

NB5540

Wireless Firewall Router

54Mbps WIRELESS FIREWALL VPN ROUTER WITH 10/100 4-PORT SWITCH



Active
SPI & DoS
Firewall

5 VPN
End
Points

54
Mbps
Wireless

All-in-one advanced firewall, 2.4GHz wireless & VPN router

User Guide

Router

Contents

Quick Start Section

Default Settings & Facts	4
NetComm Wireless Firewall Router Quick Start	5
One page setup for Telstra Bigpond Cable	6
One page setup for Optus Cable	7
One page setup for most ADSL services	8
Introduction	9
Chapter 1: Getting to know your NetComm 11G Wireless Firewall Router	11
1-1 About NetComm 11G Wireless Firewall Router	11
1-2 Contents of the NetComm 11G Wireless Firewall Router Package	12
1-3 Features of the NetComm 11G Wireless Firewall Router	12
Chapter 2: Hardware Installation & Setup	13
2-1 Rear Panel & Connections	13
2-2 Front Panel LEDs	14
2-3 System Requirements and Setup	15
2-4 Installing the TCP/IP Protocol for Windows	15
2-5 Fixed IP Addresses Configuration	18
2-6 Macintosh Setup	20
Chapter 3: Internet Access	22
3-1 Prepare your network information	22
3-2 Web-based User Interface	23
3-3 Initial Configuration – Setup	24
Chapter 4: Advanced Applications	28
4-1 Firewall	28
4-2 DHCP Configuration	29
4-3 Web Control	30
4-4 ToD Control	31
4-5 Access Control	32
4-6 Port Forwarding Settings	34
4-7 Special Application (Port Triggering)	36
4-8 Dynamic Routing	37
4-9 Static Routing	37
4-11 Administration Settings	41
4-12 Status Monitor	43
4-13 DMZ Host	44
4-14 Log	45
4-15 VPN Passthrough	46
4-16 Dynamic DNS (DDNS)	47

4-17 Universal Plug and Play	49
4-18 Back Up and Restore	53
4-19 Upgrade Firmware	55
4-20 Diagnostics (Ping & Tracert)	56
Chapter 5: Configuring IPSec/VPN Tunnels	58
5-1 VPN/IPSec Introduction	58
5-2 VPN Application Types	60
5-3 VPN / IPSec Setup	61
5-4 Example1: Tunnel between Two VPN Routers	65
5-5 Example2: Tunnel between VPN Router-and-VPN Client with Fix IP	65
5-6 Example3: Tunnel between VPN Router-and-VPN Client with dynamic IP	66
Chapter 6: Configuring IPSec on Windows 2000/XP	67
6-1 Environment	67
6-2 Steps in Windows 2000/XP	67
6-3 Steps in Cable/DSL Firewall Router	79
Chapter 7: Trouble Shooting	81
Hardware	81
Client Side (Computers)	82
Appendix A: Frequently Asked Questions	82
Appendix B: Technical Specifications	84
Appendix C: Glossary	85
Appendix D: Registering your NetComm Product	88
Contact Information	88
Trademarks and Notices	88
Product Warranty	91
Limitations of Warranty	91

Default Settings & Facts

The following lists the default settings of your NetComm Wireless 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 Wireless 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 (12VDC, 1.0Amps, Center pole positive) with your NetComm Wireless Firewall Router.

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

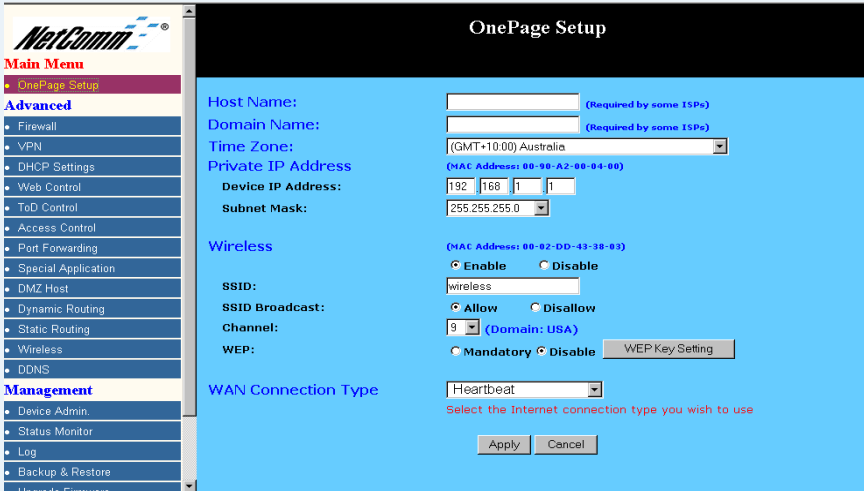
Web: www.netcomm.com.au

NetComm Wireless Firewall Router Quick Start

The following Quick Start pages are intended to be used by an advanced user to quickly configure the NetComm Wireless 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 Wireless 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 Wireless Firewall Router and ensure you have a link. Connect your Cable modem (supplied by your ISP) to the WAN port of the NetComm Wireless 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 Wireless Firewall Router's default IP (192.168.1.1). The main menu of the router should open displaying the **“One Page Setup”**.

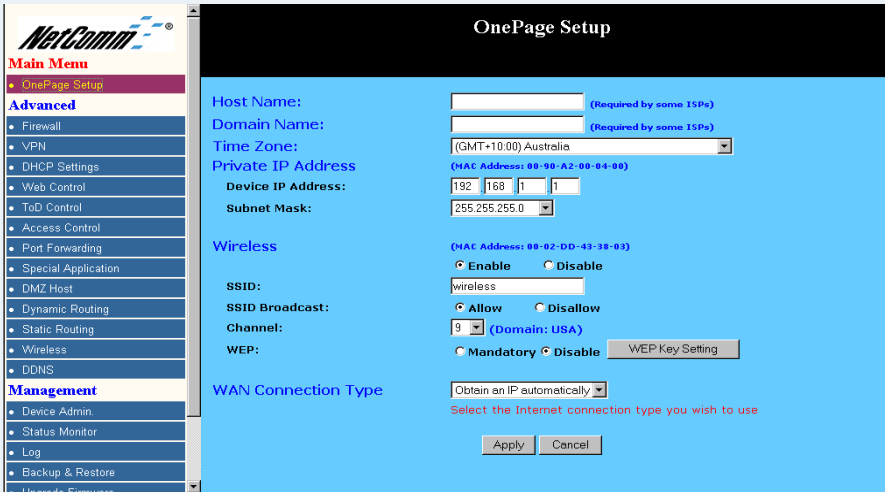


Note: You may be prompted for a log-in, there is no User Name and the Password is "admin".

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 Wireless 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 Wireless 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

1. Connect your computer to one of the four LAN ports on the NetComm Wireless 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 Wireless Firewall Router's default IP (192.168.1.1). The main menu of the router should open displaying the **“One Page Setup”**.



NetComm OnePage Setup

Main Menu

- OnePage Setup

Advanced

- Firewall
- VPN
- DHCP Settings
- Web Control
- ToD Control
- Access Control
- Port Forwarding
- Special Application
- DMZ Host
- Dynamic Routing
- Static Routing
- Wireless
- DDNS

Management

- Device Admin
- Status Monitor
- Log
- Backup & Restore
- Upgrade Firmware

Host Name: (Required by some ISPs)

Domain Name: (Required by some ISPs)

Time Zone: (GMT+10.00) Australia

Private IP Address (MAC Address: 00-00-A2-00-04-00)

Device IP Address: 192 | 168 | 1 | 1

Subnet Mask: 255.255.255.0

Wireless (MAC Address: 00-02-DD-43-38-03)

Enable Disable

SSID: wireless

SSID Broadcast: Allow Disallow

Channel: 9 (Domain: USA)

WEP: Mandatory Disable WEP Key Setting

WAN Connection Type: Obtain an IP automatically

Select the Internet connection type you wish to use

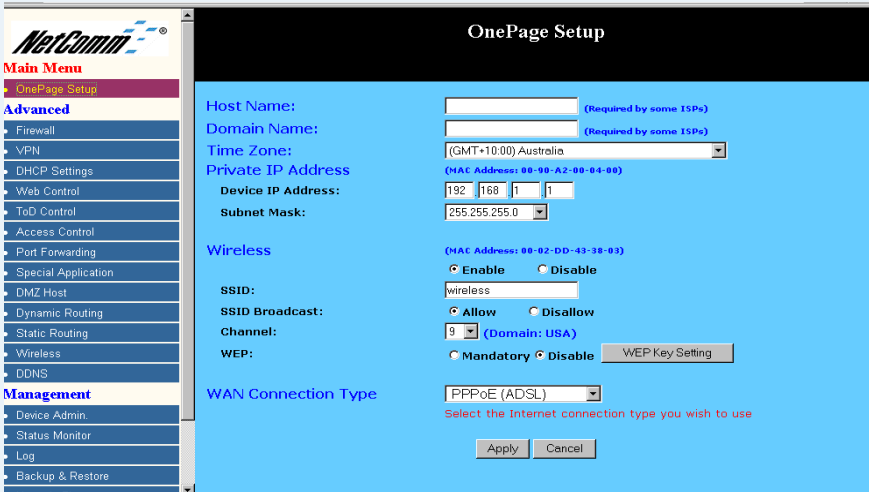
Apply Cancel

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 **“Obtain an IP automatically (E.g. Optus cable)”**.
5. Optus cable does not require a **“User Name”** and **“Password”** as it uses the modem's MAC address to identify you to 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 Wireless 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 Wireless 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 Wireless Firewall Router and ensure you have a link. Connect your ADSL modem (supplied by your ISP) to the WAN port of the NetComm Wireless 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 Wireless Firewall Router's default IP (192.168.1.1). The main menu of the router should open displaying the “One Page Setup”.



The screenshot shows the NetComm OnePage Setup web interface. On the left is a navigation menu with categories: Main Menu (OnePage Setup, Advanced, Management), Advanced (Firewall, VPN, DHCP Settings, Web Control, ToD Control, Access Control, Port Forwarding, Special Application, DMZ Host, Dynamic Routing, Static Routing, Wireless, DDNS), and Management (Device Admin, Status Monitor, Log, Backup & Restore). The main content area is titled "OnePage Setup" and contains the following fields:

- Host Name: [] (Required by some ISPs)
- Domain Name: [] (Required by some ISPs)
- Time Zone: (GMT+10:00) Australia
- Private IP Address: (MAC Address: 88-90-A2-00-04-00)
- Device IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- Wireless: (MAC Address: 88-92-DD-43-38-03)
 - Enable (selected) / Disable
 - SSID: wireless
 - SSID Broadcast: Allow (selected) / Disallow
 - Channel: 9 (Domain: USA)
 - WEP: Mandatory (selected) / Disable (WEP Key Setting button)
- WAN Connection Type: PPPoE (ADSL)

Below the fields is a note: "Select the Internet connection type you wish to use" and two buttons: Apply and Cancel.

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 Wireless 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 Wireless 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 11G Wireless Firewall Router. The NetComm 11G Wireless Firewall Router is designed to provide advanced networking security and network resource sharing, with an integrated 802.11g wireless AP and 4-port 10/100 Mbps switch. 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. Configured as a DHCP server, the NetComm 11G Wireless 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 11G Wireless 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 11G Wireless 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 11G Wireless 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 11G Wireless Firewall Router.

Chapter 1: Get to know your NetComm 11G Wireless Firewall Router

This chapter describes the package contents and provides a list of features of the NetComm 11G Wireless Firewall Router.

Chapter 2: Hardware Installation & Setup

This chapter describes the steps for hardware installation of the NetComm 11G Wireless Firewall Router.

Chapter 3: Internet Access

This chapter describes the steps for basic configuration and start up of the NetComm 11G Wireless Firewall Router.

Chapter 4: Advanced Applications

This chapter describes how to configure advanced functions in order to get the most from your NetComm 11G Wireless Firewall Router.

Chapter 5: Configuring IPSec VPN

This chapter describes IPSec VPNs and explains how to configure your Router.

Chapter 6: Configuring IPSec on Windows 2000/XP

This chapter describes how to configure IPSec on Windows 2000/XP

Chapter 7: Trouble Shooting

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

Chapter 1: Getting to know your NetComm 11G Wireless Firewall Router

This chapter describes the package contents and provides a list of features of the NetComm 11G Wireless Firewall Router.

1-1 About NetComm 11G Wireless Firewall Router

The *NetComm 11G Wireless Firewall Router* is a hybrid product, which combines Ethernet technology and wireless access into a single stand-alone unit. The device allows you take advantage of both security and fast connections. All computers, whether on your Wireless network or on your wired 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.

Wireless LAN

Wireless Local Area Network systems (WLANs) transmit and receive data through the air by using radio frequency (RF). This offers advantages, such as mobility, ease of installation, and scalability, over traditional wired systems.

- **Mobility:** WLANs combine data connectivity with user mobility. This provides users with access to the network anywhere in their organization. For example, users can roam from a conference room to their office without being disconnected from the LAN. This would be impossible with a wired network.
- **Ease of Installation:** Eliminating the need to deploy network cable in walls and ceiling, installing WLANs is easy for both novice and expert users alike.
- **Scalability:** WLAN topologies are easy to change in various ways from peer-to-peer networks for a small group of users to full infrastructure networks for hundreds of users roaming over a broad area.

Wireless LANs can be set as "Ad-hoc" network and "Infrastructure" network. Unlike the "Ad-hoc network", where users on the LAN send data directly to each other, the "Infrastructure" network includes an access point and users on the "Infrastructure" network send data to that dedicated access point. NetComm Wireless 11G Router uses "Infrastructure" network, where each wireless LAN PC within the range of the access point can communicate with other wireless LAN PCs within the range.

1-2 Contents of the NetComm 11G Wireless Firewall Router Package

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

- NetComm 11G Wireless Firewall Router
- Power Adapter - 12VDC, 1.0Amps Center Pole Positive
- This Manual

1-3 Features of the NetComm 11G Wireless Firewall Router

Your NetComm 11G Wireless Firewall Router contains the following features that make it excellent for network connections.

- Provides wireless access roaming, best access point selection, loading balance, network traffic filtering included in wireless roaming function.
- Provides 64bits/128bits key WEP (Wired Equivalent Privacy) wireless data encryption to secure wireless communication.
- Fully supports 802.11 open and shared key authentications.
- 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 (Port Forwarding).
- 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 11G Wireless 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 11G Wireless Firewall Router.



Connecting your Router

1. Plug one end of the UTP cable into the WAN port, the other into the RJ45 Ethernet jack on your ADSL or Cable modem.
2. Connect a computer, with a Network Interface Card installed, to one of the four LAN Ports.
3. Connect the external power supply to the NetComm 11G Wireless Firewall Router.
4. 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.

Note: *Auto MDI is available on all five ports. A special cross over cable or “uplink” port to join the router to another hub or switch is not required as the ports are self-adjusting.*

2-2 Front Panel LEDs

The following figure shows the front view of the NetComm 11G Wireless Firewall Router.



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

Power:	Green	On when power is on.
Diag:	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.

For WLAN

Enable /Activity:	Green	The Links LED illuminates when the wireless option is enabled. When the wireless option is disabled (through the web-based utility), the LED is off. Blinking when there is wireless connection activity.
--------------------------	-------	--

For WAN port & LAN ports (x4)

Link/Act & 10/100:	Green	On when a successful 100Mbps connection is made through the corresponding port. Blinking when data is flowing through this port.
	Yellow	On when a successful 10Mbps connection is made through the corresponding port. Blinking when data is flowing through 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.
4. TCP/IP network protocol.
5. Web browser, such as Microsoft Internet Explorer or Netscape Navigator.

2-4 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”**.

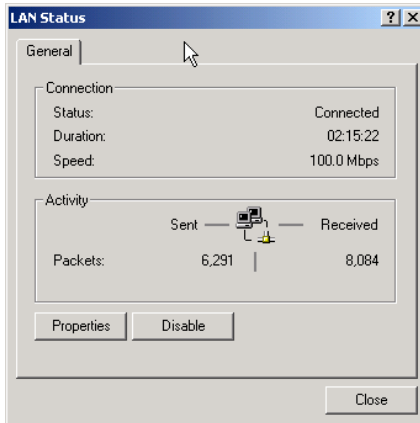


Double-click the **“Network”** icon. Your Network window should appear. Select the **“Configuration”** tab.

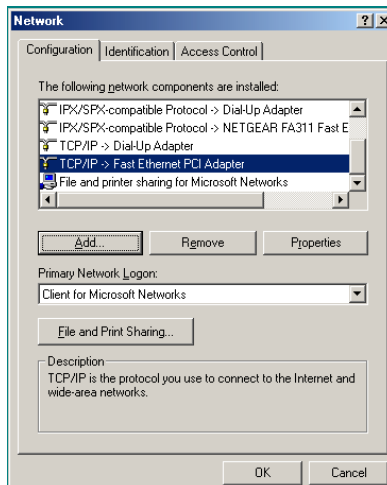
Note: For Windows 2000 & Windows XP the settings can be reached by clicking the “Local Area Connection” icon on the right bottom side of your desktop screen.



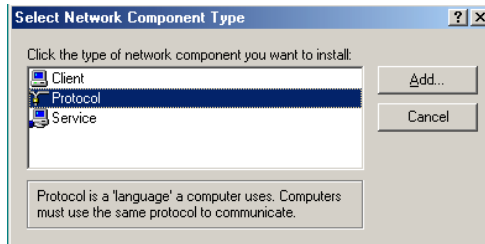
In the “Local Area Connection Status” window, click “Properties” button then your Network window will appear.



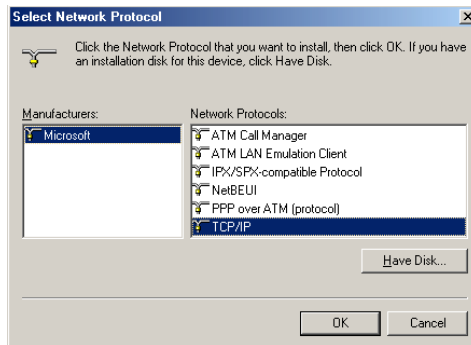
2. Check whether the TCP/IP Protocol has already been installed and bound to your Network Interface Card.



- 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”**.



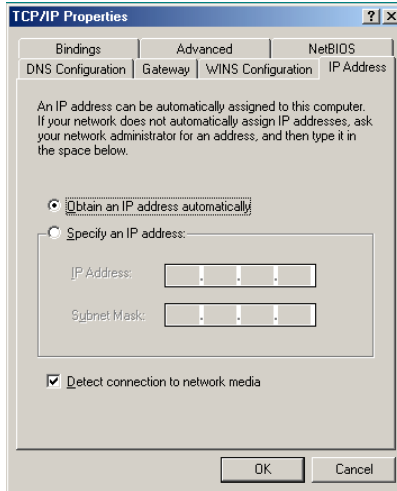
4. Highlight **“Microsoft”** under the list of manufacturers.



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

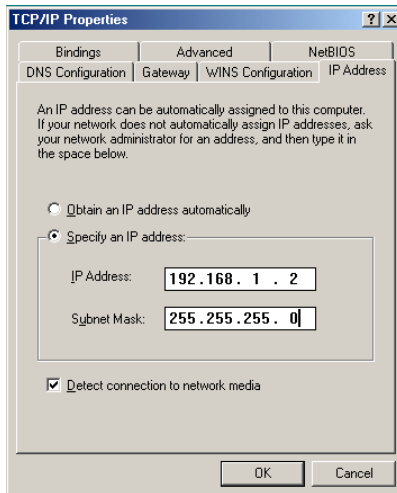
5. After a few seconds, you will be brought back to the Network window. The TCP/IP Protocol should now be on the list of installed network components (refer to point 2).
6. Click the **“Properties”** button.

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



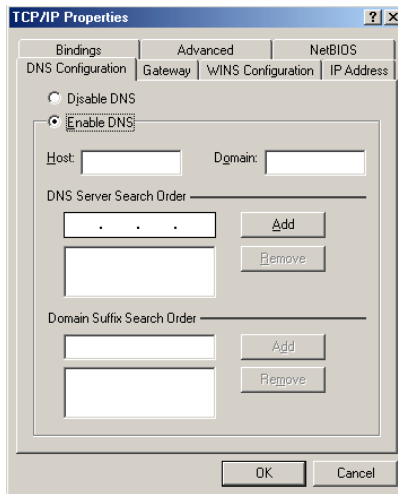
7. Select “**Obtain an IP address automatically**”. Click “**OK**”. Restart your computer to complete the TCP/IP installation.

2-5 Fixed IP Addresses Configuration



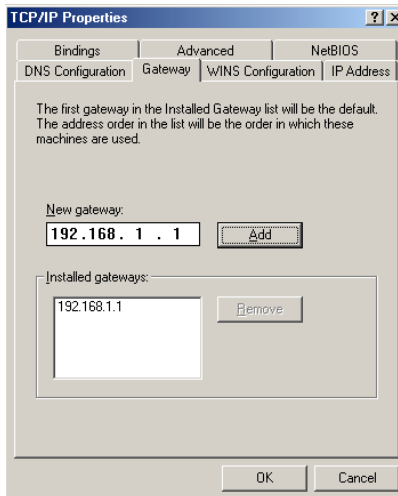
Fixed IP addresses may be assigned to network devices for many reasons, such as the server computers or printers which are consistently accessed by multiple users. To set up computers with fixed IP Addresses, go to the “**IP Address**” tab of the “**TCP/IP Properties**” window as shown above.

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 11G Wireless 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 11G Wireless 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.

2-6 Macintosh Setup

This section 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.

Hardware Connections

Connect your Macintosh computer to your NetComm 11G Wireless 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.

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 11G Wireless Firewall Router's DHCP server.

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.

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 11G Wireless 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.

NetComm 11G Wireless Firewall Router Configuration

To configure your NetComm 11G Wireless 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*.

Adding NetComm 11G Wireless Firewall Router to Existing Network

If the NetComm 11G Wireless 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 11G Wireless 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 11G Wireless 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 11G Wireless Firewall Router (refer to the above section).

Chapter 3: Internet Access

This chapter describes the procedures necessary to configure the basic functions and to start up your NetComm 11G Wireless Firewall Router. On successful completion of these procedures, you will be able to access the Internet via your NetComm 11G Wireless Firewall Router.

3-1 Prepare your network information

In order to allow a quick reference point when setting up your NetComm 11G Wireless 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: _____

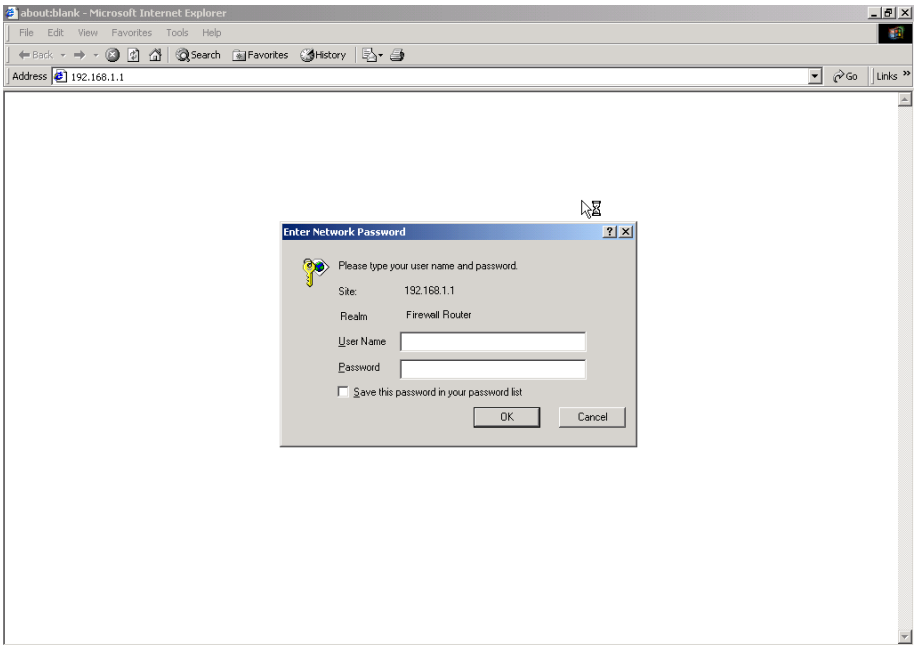
Password: _____

3-2 Web-based User Interface

The NetComm 11G Wireless 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 11G Wireless 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: *This password should be changed via the Administration page immediately.*



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

When making changes to the settings, click on the **“Apply”** button before moving to another page. The router will reboot and refresh the screen in 5 seconds. Continue the session by selecting more menu items.



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.



The screenshot shows the 'OnePage Setup' configuration interface. It includes the following fields and options:

- Host Name:** A text input field with a note '(Required by some ISPs)'.
- Domain Name:** A text input field with a note '(Required by some ISPs)'.
- Time Zone:** A dropdown menu currently set to '(GMT+10:00) Australia'.
- Private IP Address:** A section containing:
 - Device IP Address:** Four input fields with values 192, 168, 1, 1.
 - Subnet Mask:** A dropdown menu with value 255.255.255.0.
- Wireless:** A section containing:
 - Wireless:** A section header with a note '(MAC Address: 00-02-DD-43-30-03)'.
 - Enable/Disable:** Radio buttons for 'Enable' (selected) and 'Disable'.
 - SSID:** A text input field with value 'wireless'.
 - SSID Broadcast:** Radio buttons for 'Allow' (selected) and 'Disallow'.
 - Channel:** A dropdown menu with value '9' and a note '(Domain: USA)'.
 - WEP:** Radio buttons for 'Mandatory' and 'Disable'.
 - WEP Key Setting:** A button.

- **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.

Wireless

Check "**Disable**", "**Mixed**" or "**G-only**" to make the wireless LAN function active or select to support 11b/11g mixed mode or 11g only.

- **SSID** As the acronym for Service Set Identifier, SSID is the unique name shared among all clients and Wireless Broadband Router in a same wireless network. The SSID must be identical for all points and must not exceed 32 characters.
- **SSID Broadcast** Router will broadcast the SSID to let WLANs clients easily search and connect to this wireless router by leaving this item as default setting "Allow". Click "Disallow" to disable the broadcast.
- **Channel** Select the appropriate channel number from the drop-down. The permissible channels are different from Regulatory Domains. Make sure that all nodes in the same wireless LAN network use the same channel, or the channel usage is automatic when a connection between client and access point are made.

-
- **WEP** As the acronym for Wired Equivalent Privacy, WEP 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 insure data security. To code/decode the data transmission, all points must use the identical key. To make the WEP encryption active or inactive, select "Mandatory" or "Disable".
 - **WEP Key Setting** As the WEP is active, click the button of "WEP Key Setting" to go to the setting page. Select "64Bit" or "128Bit" encryption algorithm from the drop-down list. There are two ways to generate WEP key:
 1. **Passphrase** Enter a alphanumeric text string in this column then click "Generate" button, and four 64-bit or 128-bit encryption key will be created automatically.
 2. **You can enter the WEP key manually.**

You may need to enter the WEP key manually in case to join the existing wireless network. However, if not, the Pass phrase method is recommended. If you are not sure which way to use, check with your network administrator.
 - **Default TX Key** Select one of the four keys to be the encryption key you are going to use in the wireless network. To be sure that all the points in a same wireless network have to have the same encryption key.

Click "**Apply**" after making any changes.

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 (eg Optus Cable)

Obtain IP automatically is the default option for the router. If your ISP automatically assigns the IP addresses and other values to the NetComm 11G Wireless 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' dropdown menu is selected. Below it, there are input fields for 'Specify WAN IP Address', 'Subnet Mask', 'Default Gateway Address', and three 'DNS' entries. Each field is represented by a grid of four small input boxes. The 'Subnet Mask' field is pre-filled with '255', '255', '255', and '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 dropdown, there are fields for 'User Name' (containing 'username@isp.net.au') and 'Password' (masked with asterisks). There are two radio button options: 'Connect on Demand: Max Idle Time 5 Min.' (which is selected) and 'Keep Alive: Redial Period 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 is the amount of time the router will remain connected after network traffic has ceased. This function is for PPPoE only and is mainly used for security.
- **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.

HeartBeat

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

- **User Name** Enter the user name as provided by your ISP.
- **Password** Enter the password as provided by your ISP.



The screenshot shows the WAN Connection Type configuration page. The 'WAN Connection Type' is set to 'HeartBeat(Telstra Cable)'. The 'Heart Beat Server' section has two radio buttons: 'Connect on Demand: Max Idle Time 5 Min.' and 'Keep Alive: Redial Period 30 Sec.'. The 'Apply' and 'Cancel' buttons are at the bottom.

- **Heart Beat Server** When you select the "HeartBeat (eg Telstra Cable)" option for your WAN connection type in the NetComm router One-Page Setup, you may also need to specify the Heart Beat Server's IP address.

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 11G Wireless 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** 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. Temporarily disable this option if you have a particularly sensitive Internet application that does not function through the router.
- **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 if your browser is using a proxy because the router only sees the connection to the proxy and then the proxy connects to yahoo. If you block the use of proxies then all connections must be made directly through the router.

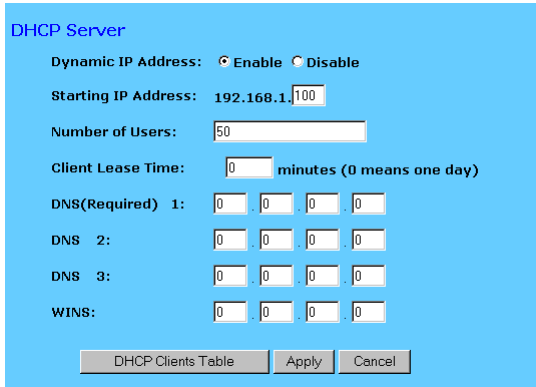
Java & Active X are programming languages for web pages. However, some Trojan programs are also written in these programming languages. If you deny either of these, you may not be able access some parts of web sites.

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 be blocked by the router if the “Deny” option is selected.

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.



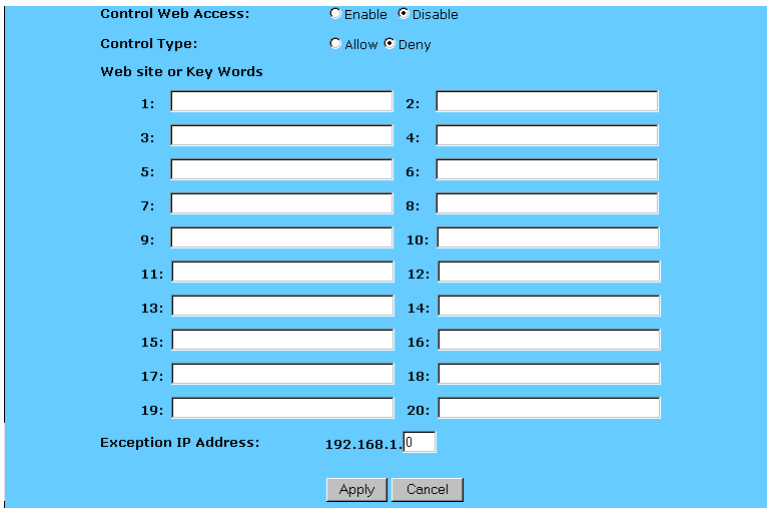
Note: The DHCP Server can support a maximum pool of 253 IP Addresses.

- **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.
- **Client Lease Time** Enter the number of time that DHCP clients (The PCs on LAN side) can use the IP Addresses assigned by Router's DHCP server. Before the time is up, DHCP clients have to request to renew the DHCP information.
- **DNS** The IP Address of the Domain Name Server, which is currently used. Multiple DNS IP settings are common. The first DNS entry will be use in most cases.
- **DHCP Clients Table** Click the DHCP Clients Table button to show current DHCP client information.

Click the "**Apply**" button after making any changes, or click the "**Cancel**" button to exit the screen without saving any changes.

4-3 Web Control

This feature allows you to restrict LAN users access to specific web sites. To block a site, you can enter either a complete URL (Internet address) or keywords included in the URL.

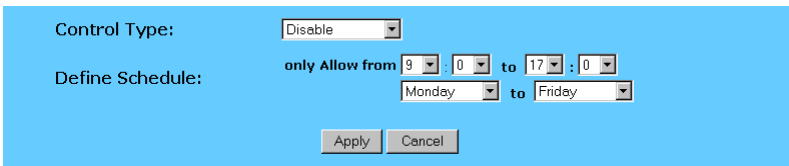


- **Control Web Access** Check "Enable" or "Disable" to make this function active or inactive.
- **Control Type** Check "Allow" to allow users on the network to access specific website listed on the location only. In contrast, to restrict users on the network to access the website listed on the location, check "Block" in this item.
- **Web site or Key Words** Enter either a complete URL (Internet address) or keywords included in the URL.
- **Exception IP Address** Enter the IP Address of LAN PC that will not be restricted by this rule.

Click the "**Apply**" button after making any changes, or click the "Cancel" button to exit the screen without saving any changes.

4-4 ToD Control

This feature allows you to limit connection availability according to a nominated time schedule.



Control Type:

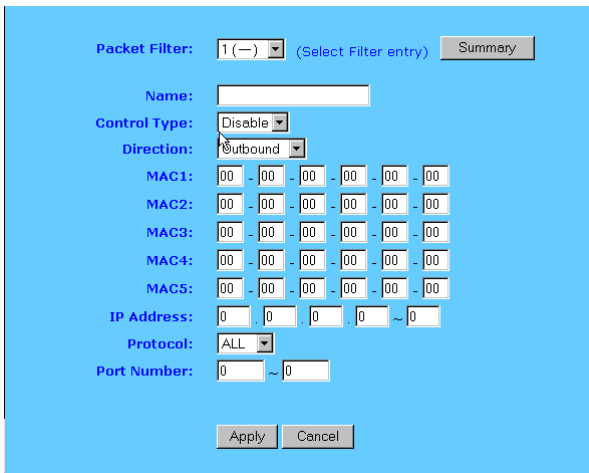
Define Schedule: **only Allow from** : to :
 to

- **Control Type** Select the control type from the drop down list and make this function active. Select "Block Outbound" to restrict the connection to the Internet from your LAN. Select "Block Inbound" to restrict any external connections from Internet to your LAN servers that were set as virtual servers or as DMZ host. Select "Block Both" to restrict both incoming and outgoing connections. Select "Disable" to turn off this function.
- **Define Schedule** Set a period of time with beginning and ending from the drop down list.

Click the "**Apply**" button after making any changes, or click the "**Cancel**" button to exit the screen without saving any changes.

4-5 Access Control

The Access Control feature allows administrators to block certain users from accessing the Internet or specific applications. Network administrators can restrict access of up to five groups of specified network users/computers. You can identify users/computers either by IP Address or by MAC Address. To effectively block by IP Address the computers you wish to block must only be able to operate on a fixed IP address and you must know the IP Address of each computer.



Packet Filter: 1 (-) (Select Filter entry) Summary

Name:

Control Type: Disable

Direction: Outbound

MAC1: 00 - 00 - 00 - 00 - 00 - 00

MAC2: 00 - 00 - 00 - 00 - 00 - 00

MAC3: 00 - 00 - 00 - 00 - 00 - 00

MAC4: 00 - 00 - 00 - 00 - 00 - 00

MAC5: 00 - 00 - 00 - 00 - 00 - 00

IP Address: 0 0 0 0 ~ 0

Protocol: ALL

Port Number: 0 ~ 0

Apply Cancel

Alternatively you can identify the computers you wish to block by MAC Address. This is more effective because a MAC Address is physically locked to a computer and not easily changed, however, blocking by MAC address is more laboursome as each filter must be individually set and filtering by MAC address ranges can not be done because MAC addresses are rarely consecutive.

- **Packet Filter** Select the number of policy rules you want to configure. There are up to 10 rules you can set. Note that these rules are sequenced. Rule 1 has higher priority than Rule 2 and so forth.
- **Status** Select "Allow" to limit users/computers access to specific applications you set on this rule. Select "Deny" to restrict the users/computers access to specific applications you set on this rule.
- **Name** For each rule, you can enter up to 15 characters to identify it.
- **Direction** Choose the initial network data traffic direction you wish to block. Select "LAN" if you want to block LAN side users/PCs set in the following "MAC" and "Source IP" fields to access certain applications on the Internet. Select "WAN" if you want to block WAN side users/PCs set in the following "MAC" and "Source IP" fields to access certain PCs on your LAN side.

- **MAC** This item allows network administrators to use the MAC addresses of PCs to restrict users/computers from accessing the specific application you set in this rule. A MAC address is short for Media Access Control Address and is a hardware address that uniquely identifies each node on network. Enter the MAC addresses of the computers you wish to allow/block in each field.
- **IP Address** This item allows network administrators to use IP Address of PCs to restrict users/computers from accessing the certain applications you set in this rule. Enter the range of IP addresses if you want them to be included in a controlled group with the same access limitation.

Note that if you set both "MAC" and "Source IP" in one rule, the PCs which have the MAC addresses matching in "MAC" field and their IP addresses matching in the "Source IP" field will be allowed/blocked for certain applications.

- **Protocol** Select the protocol type as "TCP" or "UDP" from the drop down list. If you are not sure which one to choose, select "Both".
- **Port Number** Enter the range of port numbers that are used by the applications you wish to be blocked. For example, port 80 usually is used as destination port number when you access a web page. Note that if you don't enter any value in the "MAC" and "Source IP" column but enter the port number, for example "80", in "Destination Port", it means all the users/PCs will be allowed/denied access to certain applications related to this port, for example "web browsing".
- **Summary** Click this button to display a summary page showing all the current rules you have set.

Click the "**Apply**" button after making any changes, or click the "**Cancel**" button to exit the screen without saving any changes.

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

4-6 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 11G Wireless 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 and that your internal servers do not use a DHCP client.

UPnP Function: Enable Disable
 UPnP Control: Enable Disable

Application Name	Ext.Port	Protocol		Int. Port	IP Address	Enable
		TCP	UDP			
FTP	21	<input checked="" type="radio"/>	<input type="radio"/>	21	192.168.1.0	<input type="checkbox"/>
Telnet	23	<input checked="" type="radio"/>	<input type="radio"/>	23	192.168.1.0	<input type="checkbox"/>
SMTP	25	<input checked="" type="radio"/>	<input type="radio"/>	25	192.168.1.0	<input type="checkbox"/>
DNS	53	<input checked="" type="radio"/>	<input type="radio"/>	53	192.168.1.0	<input type="checkbox"/>
TFTP	69	<input checked="" type="radio"/>	<input type="radio"/>	69	192.168.1.0	<input type="checkbox"/>
finger	79	<input checked="" type="radio"/>	<input type="radio"/>	79	192.168.1.0	<input type="checkbox"/>
HTTP	80	<input checked="" type="radio"/>	<input type="radio"/>	80	192.168.1.0	<input type="checkbox"/>
POP3	110	<input checked="" type="radio"/>	<input type="radio"/>	110	192.168.1.0	<input type="checkbox"/>
NNTP	119	<input checked="" type="radio"/>	<input type="radio"/>	119	192.168.1.0	<input type="checkbox"/>
SNMP	161	<input checked="" type="radio"/>	<input type="radio"/>	161	192.168.1.0	<input type="checkbox"/>
msmsgs	42215	<input checked="" type="radio"/>	<input type="radio"/>	9833	192.168.1.101	<input checked="" type="checkbox"/>
msmsgs	20959	<input checked="" type="radio"/>	<input type="radio"/>	7839	192.168.1.102	<input checked="" type="checkbox"/>
	0	<input type="radio"/>	<input checked="" type="radio"/>	0	192.168.1.0	<input type="checkbox"/>
	0	<input type="radio"/>	<input checked="" type="radio"/>	0	192.168.1.0	<input type="checkbox"/>

Note: Your NetComm 11G Wireless Firewall Router supports only one forward to one IP Address for each port (service).

- Set up a network computer to act as a server and configure each with a fixed LAN IP Address in the same subnet as the LAN subnet of the router.
- In the “One Page Setup” screen, ensure the “**Private IP Address**” is set to the NetComm 11G Wireless 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.

Note: You can only forward an external port once, therefore UPnP port settings and Portforwarding settings must not overlap or conflict:

- Use UPnP settings for any preprogrammed ports and where internal port is different from external port (i.e. Port Translation)
- Use Port forwarding for ports that are not common and do not need translation.

The following table lists 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
E-Donkey	TCP	4661, 4662, 4663
	UDP	4665
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)
	TCP	6901 (Voice)
PC Anywhere host	TCP	5631
	UDP	5632
Quake 2	UDP	27910
Quake III	UDP	27660 (first player)
	UDP	"C:\Program Files\Quake III Arena\quake3.exe" +set net_port 27660
	UDP	27661 (second player)
Telnet Server	TCP	23
Web Server	TCP	80

4-7 Special Application (Port Triggering)

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 11G Wireless 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 11G Wireless Firewall Router.
- **Incoming Control** Enter the port number or range of numbers the inbound packets carry.

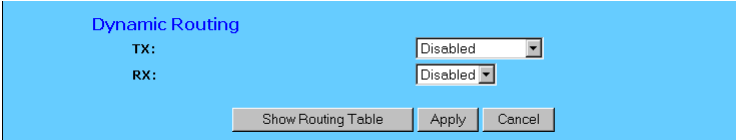
Click “**Apply**” after making any changes.

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

4-8 Dynamic Routing

The Dynamic Routing feature allows your NetComm 11G Wireless Firewall Router to exchange routing information with other routers in the network. Enabling this feature is likely to enhance performance of your NetComm 11G Wireless Firewall Router when used in a multi routed network.

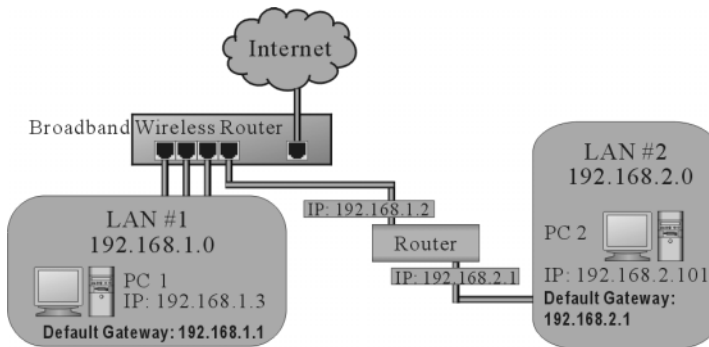


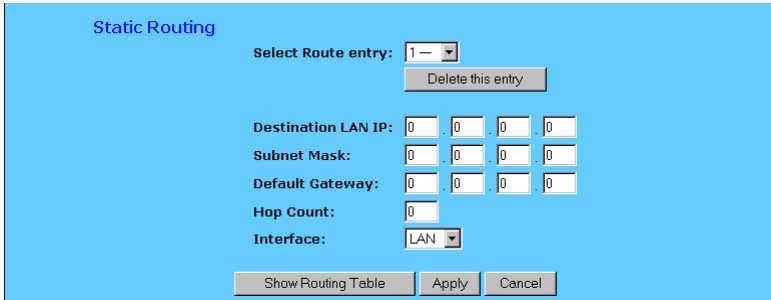
- **TX** From the drop-down list, select one of the routing information types, “**RIP-1**”, “**RIP-1 Compatible**”, or “**RIP-2**”, to enable the “**TX**” (transmit) function. “**RIP-1**” is the protocol used by older routers and newer routers should use “**RIP-2**”. “**RIP-1 Compatible**” serves to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

4-9 Static Routing

The Static Routing feature allows computers that are connected to the NetComm 11G Wireless 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 11G Wireless Firewall Router through another router (destination LAN). Up to 20 route entries may be entered into the NetComm 11G Wireless 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 11G Wireless Firewall Router via another router while PC1 in LAN#1 is connected to the NetComm 11G Wireless Firewall Router directly. Without configuring the Static Routing function, the two computers would not be able to communicate with each other.

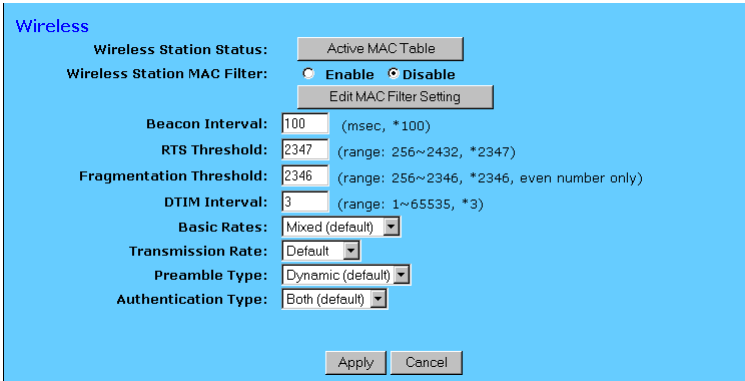
- **Select Route entry** Select the route entry number from 1 to 20 that you wish to configure.
- **Destination LAN IP** and **Subnet Mask** Enter the IP Address and Subnet Mask of the destination LAN that the immediate LAN is to communicate with. Taking the above diagram as an example, enter *192.168.2.0* 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.

4-10 Wireless

This setting page allows you to configure advanced wireless functions. To set those items needs more technology background. Unless you really understand those technical terms, it would be better to leave them as default setting.



- **Wireless Station Status** The "Active MAC Table" shows the MAC addresses of wireless clients, which have the same ESSID and WEP key with Broadband Wireless Router. When the "MAC Filter" function is disabled, the background color is gray.

Click the "Active MAC Table" button will display all MAC addresses of wireless nodes on your WLAN.

If the MAC Filter function is enabled and the MAC addresses showing in this table have been entered into the "Edit MAC Filter" table, the background color of those MAC addresses will be green. Otherwise, it should be red. If the MAC addresses have been blocked (check the Filter field beside the MAC address in Edit MAC Filter table), the background color will be yellow.

- **Wireless Station MAC Filter** This function allows you to restrict wireless users to access Internet.

Click "Edit MAC Filter Setting" button to open the edit table.

Wireless MAC Entry There are 32 sets divided into four groups in this function. You can choose each group by selecting from the pop-down list. Enter the MAC addresses of the computers you wish to block in the columns and click the Filter field beside the MAC address, and then that user will be blocked to link to WLAN and Internet. If the "Filter" field isn't checked, that MAC address won't be blocked. The MAC address entered here should be 12 continue alphanumeric digits without "-" in between. Click "Apply" to save these changes.

- **Beacon Interval** It's the signal sent periodically by wireless access point to provide synchronization among the stations in wireless LAN.
- **RTS Threshold** RTS packet is use to account for potential hidden stations. This feature allows you to set the size of RTS packet.

- **Fragmentation Threshold** If the length of data frame needing transmission exceeds the fragmentation threshold you set in the column, the data frame will be fragmented. If there is significant interference or high utilization in your wireless network, the smaller fragmentation value can increase the reliability transmission. However, it is more efficient to set the large fragment size.
- **DTIM Interval** DTIM is the acronym of delivery traffic indication message. It determines how often the MAC Layer forward multicast traffic.
- **Basic rate** Leave "Mixed" as default setting to compatible with different wireless standard or select other rates you wish to use to connect with specific wireless standard devices. .
- **Transmission Rates** Leave "Default" setting or select other speed you wish to use.
- **Preamble Type** Leave "Dynamic" as default setting or select other type to compatible with special setting your client devices use.
- **Authentication Type** Select either Open System or Share Key as authentication type. If you are not sure, select both.

Click Apply after making any changes.

4-11 Administration Settings

This feature allows the administrator to manage the NetComm 11G Wireless 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 11G Wireless 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.
- **SNMP Function** The NetComm router is equipped with SNMP functionality to allow it to be monitored and managed with a central SNMP management suite. SNMP is disabled by default, if enabled the community strings should be changed for security.
- **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 11G Wireless 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.
- **Block WAN ping response** This option is enabled by default for security. This means the router will not respond to pings sent to it by other computers on the internet. You can alter this to help with diagnostics.
- **IPSec Pass Through** This option needs to be enabled if a computer on the LAN wishes to use a IPSec VPN client to tunnel ‘through’ the router and out to the Internet.
- **PPPoE Pass Through** This option needs to be enabled if a computer on the LAN wishes to use a PPPoE client to tunnel ‘through’ the router and out to the Internet.
- **PPTP Pass Through** This option needs to be enabled if a computer on the LAN wishes to use a PPTP client to tunnel ‘through’ the router and out to the Internet.
- **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.

4-12 Status Monitor

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

- **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 release the IP address obtained from the ISP’s DHCP server.
 - DHCP Renew:** Click this button to re-acquire an IP address from the ISP’s 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.

DHCP Active IP Table			
DHCP Server IP Address: 192.168.2.1			
Client Hostname	IP Address	MAC Address	Delete
DELLW98Laptop	192.168.2.101	00-10-60-59-C6-24	<input type="checkbox"/>

4-13 DMZ Host

The DMZ Host application allows unrestricted 2-way communication between a single LAN PC and other Internet users or servers. This application is useful for supporting special-purpose services such as video-conferencing and gaming, that require proprietary client software and/or 2-way user communication.

will open all in/out accesses for one LAN computer, especially for **Internet game** application. Besides, this is useful for those LAN computers that host TCP/IP services that should be fully exposed to the public network. Please enter one LAN IP Address in the LAN IP field. (0 is inactive)

DMZ Host: 192.168.1.

Multi DMZ: (For fixed IP only)

WAN IP:	LAN IP:
<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>	192.168.1. <input type="text" value="0"/>
<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>	192.168.1. <input type="text" value="0"/>
<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>	192.168.1. <input type="text" value="0"/>
<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>	192.168.1. <input type="text" value="0"/>
<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>	192.168.1. <input type="text" value="0"/>

To use this application, you must first obtain a fixed Public IP Address from your ISP. Note that in order to provide unrestricted access, the Firewall provided by the Broadband Security Router to protect this port is disabled, thus creating a potentially serious security risk.

It is recommended that this application is disabled when it is not in use by entering "0" in the "DMZ Host" field.

The Multi DMZ allows you to map the public IP addresses to your LAN PCs, should you get more than one public IP address from your ISP. This function is useful to set up your servers, such as an FTP server, web server, and so on, with public IP addresses, but still keep them within your LAN group.

With the public IP addresses, Internet users will access your servers more easily and those servers can still communicate with other PCs in your LAN by using Network Neighborhood.

DMZ Host

1. Before setting up a LAN PC to act as a DMZ Host, you should configure it using a fixed IP Address.
2. In the "One Page Setup" screen, ensure the Private IP Address is set to the Broadband Security Router's default setting of 192.168.1.1. In the Public IP Address area, select "Specify an IP Address", and then enter the IP Address and other necessary information provided by your ISP.
3. Click the "DMZ Host" option in the Advanced Menu and enter the fixed IP Address of the Exposed Host PC in the "DMZ Host" IP Address location. Remember, entering "0" will disable this application.

Multi DMZ

1. Enter the valid public IP address in "WAN IP" column. Next, enter the private IP address of the PC that you wish to map to in "LAN IP" field. Up to five public IP addresses can be entered.
2. Click the "Apply" button after making any changes, or click the "Cancel" button to exit the screen without saving any changes.

Warning: The Computers with the IP addresses specified will be directly exposed and are NOT protected by the Firewall, you should take extra care to secure these computers against internet attack.

4-14 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

Log: Enable Disable

Send Log To: 192.168.1.255

Send Log via E-mail

E-mail Alert: Enable Disable

Denial of Service Thresholds: 20 (20-100)

SMTP Mail Server:

E-mail Alerts To: (E-mail address)

Return Address: (E-mail address)

Log Schedule: ▾

Day for Sending Alerts: ▾

- **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. This computer must run a suitable "syslog" application (a copy of such an application can be downloaded from the NetComm website).
- **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.
- **Denial of Service Thresholds** The threshold is used to determine the attempt of establishing connection is DoS attack or not.
- **SMTP Mail Server** The domain name of IP Address of your ISP's outgoing e-mail server.

You may find this information when you apply for e-mail service from your ISP.

- **E-mail Alert** Enter the e-mail address you wish to send to.
- **Return Address** Enter the e-mail address you wish to send to if the alert e-mail cannot be sent to the address above.
- **Log Schedule** Select from the drop down list that when you wish the alert e-mail will be send:

When Log is Full The alert e-mail will be sent when log space is full. They are about 30 entries.

Hourly The alert e-mail will be sent by each hour.

Daily The alert e-mail will be sent by each day at midnight.

Weekly The alert e-mail will be sent by each week. When this item is select.

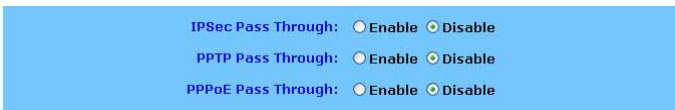
- **Day of Sending Alert** When "Weekly" is selected as Log Schedule, you can select which day in a week to send the alert e-mail.

Click the "**Apply**" button after making any changes, or click the "**Cancel**" button to exit the screen without saving any changes.

Note: *You must enable the log and click apply before you can use the "View Logs" button.*

4-15 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). The NetComm 11G Wireless Firewall Router supports up to fifty PPTP or IPSec VPN Passthrough sessions depending throughput available and tunnel load.



Note: *VPN Passthrough can be enabled or disabled in the administration page. Depending on your VPN service you may need to disable Active Firewall to allow VPN Pass through.*

4-16 Dynamic DNS (DDNS)

"DDNS" is an acronym for Dynamic Domain Name Service. Whenever you set up the web servers, mail servers, or sometimes ftp servers, you need "Domain Name" to help Internet users reach your servers easily.

Internet actually runs on IP Addresses which are numerical order, for example "66.37.215.53". These IP Address identify the location of each device connected to Internet. However, the human brain does not easily remember this numbering system, so a system that allocate domain name such as "www.dyndns.org" provides an easier method. If you type "66.37.215.53" or "www.dyndns.org" in the web browser's address bar, the browser will show the same web page. This is because both methods relate to the same web server. The "Domain Name Servers" used to manage the Internet will translate "www.dyndns.org" into the IP Address "66.37.215.53" in order to allow your browser to find the web server and display the correct web page in your browser.

If your "WAN Connection Type", as shown in One Page Setup section, is "Obtain IP Address Automatically", "PPPoE", or "PPTP" with dynamic IP address assigned by ISP, it will cause an error when you set up the public computer servers in your LAN side PCs. Internet users may not be able to reach your servers because your WAN side IP address may change each time you initiate the connection to your ISP. The DDNS function will help to map your IP address to your domain name when your ISP assigns a new dynamic IP Address.

Note that this DDNS function acts as the client appliance of DDNS service and is only able to be use in conjunction with the service provided by DynDNS.org. Before you begin using this function, you will need to apply to DynDNS.org to be able to use the service. Please visit www.dyndns.org for further information.

DDNS service allows you to assign a fixed domain name to a dynamic WAN IP address. This allows you to host your own Web, FTP or other type of TCP/IP server in your LAN.

Before configuring DDNS, you need to visit www.dyndns.org and register a domain name. (The DDNS service is provided by DynDNS.org)

DDNS Services: Enable Disable

Username: (max. 15 characters)

Password: (max. 30 characters)

Host Name: . ath.cx

Your IP Address : 0.0.0.0

Status : DDNS function is disabled.

Dynamic Domain Name Service is a feature that allows you to map a domain name to a public IP address automatically. The advantage of this function is that even if your ISP assigns your router a different IP address every day - people and computers can reference your internal network (if VPN, Port forward or DMZ settings are made) via your domain name without the need to know your Public IP address. The router is designed to use the Web site www.dyndns.org which offers up to 5 free Dynamic domain names per user.

- **DDNS Service** Check the "Enable" option if you wish to activate this function.
- **Username** After you have applied for the DDNS service from DynDNS.org, you will be issued with a Username. Enter this username in the "Username" field.
- **Password** DynDNS.org, will also issue you with a password. Enter the detail in the "Password" field.
- **Host Name** DynDNS.org, will provide you with a Host Name. Enter this name in the "Host Name" field.
- **Your IP Address** This will display the IP Address currently assigned by your ISP.
- **Status** This display the current status of the DDNS function.

Click the "Apply" button after making any changes, or click the "Cancel" button to exit the screen without saving any changes.

This function is a handy compliment to the following features of the router;

- **VPN** - you can direct another VPN device to reference your Router by specifying the Fully Qualified Domain Name (FQDN) that is specified in the DDNS setup.
- **Port forwarding** - if you wish to host a web server on your LAN the public can access it via a domain name URL (E.g. <http://router.mine.nu/default.htm>) rather than typing in the real public IP address in the URL (E.g. <http://203.147.250.73/default.htm>)
- **DMZ** - Similarly to above if you are using the DMZ host function to allow external access to a game server, web server, etc, you can provide a domain name (E.g. UT2003.mine.nu) for your friends to enter into the game.

To setup DDNS follow these steps;

1. Go to www.dyndns.org and register an account and a Dynamic domain name.
2. Log into your router and select DDNS from the menu.
3. Enter your DDNS Username, Password and Domain name as chosen during your registration. Click Apply.
4. You will need to click Update to make your first update.

4-17 Universal Plug and Play

Universal Plug and Play is a system designed to make computers, computer equipment and home appliances work together seamlessly. Currently the biggest advantage of having UPnP integrated into your router is that this will assist your router in allowing complex Internet applications such as MSN Messenger© work over Network Address Translation (NAT) without the need to setup Port forwards or DMZ. The biggest advantage of this is that the port mapping is dynamic so you do not need to specify the IP address of the computer running MSN Messenger and it should be possible to run the application on two separate machines on the same LAN that share a UPnP gateway.

To enable UPnP simply follow these steps;

1. Open the UPnP window from the left hand menu.
2. Select Enable at the top of the window and then click Apply at the bottom.

The preprogrammed ports on the UPnP page offer the option to perform Port forwarding with Translation, this means that it will 'Translate' an external public port to a different internal port and IP address.

Note: *You can only forward an external port once, therefore UPnP port settings and Portforwarding settings must not overlap or conflict. The use of UPnP does reduce the security of your network by automatically allowing applications (and potentially trojans) to open ports in your router. You should assess this risk before enabling UPnP.*

Application Name	Ext. Port	Protocol TCP UDP	Int. Port Enable	IP Address
FTP	21	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	21	192.168.2.0
Telnet	23	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	23	192.168.2.0
SMTP	25	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	25	192.168.2.0
DNS	53	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	53	192.168.2.0
TFTP	69	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	69	192.168.2.0
finger	79	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	79	192.168.2.0
HTTP	80	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	80	192.168.2.0
POP3	110	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	110	192.168.2.0
NNTP	119	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	119	192.168.2.0
SNMP	161	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	161	192.168.2.0
mmsgs	65500	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	7872	192.168.2.151
mmsgs	26291	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	16721	192.168.2.151
	0	<input type="radio"/> TCP <input type="radio"/> UDP	0	192.168.2.0

- Use UPnP settings for any preprogrammed ports and where internal port is different from external port (i.e. Port Translation)
- Use Port forwarding for ports that are not common and do not need translation.

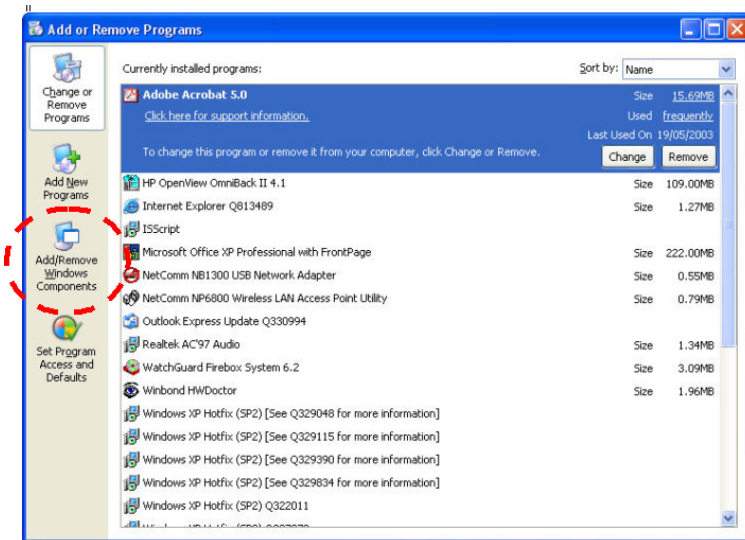
Adding UPnP to Windows XP

Currently the only version of Windows to feature UPnP is Windows XP, and it is not installed by default. As UPnP becomes more common you should be able to control more and more devices via the UPnP software in Windows. To add UPnP capability to your Windows XP computer follow the steps below;

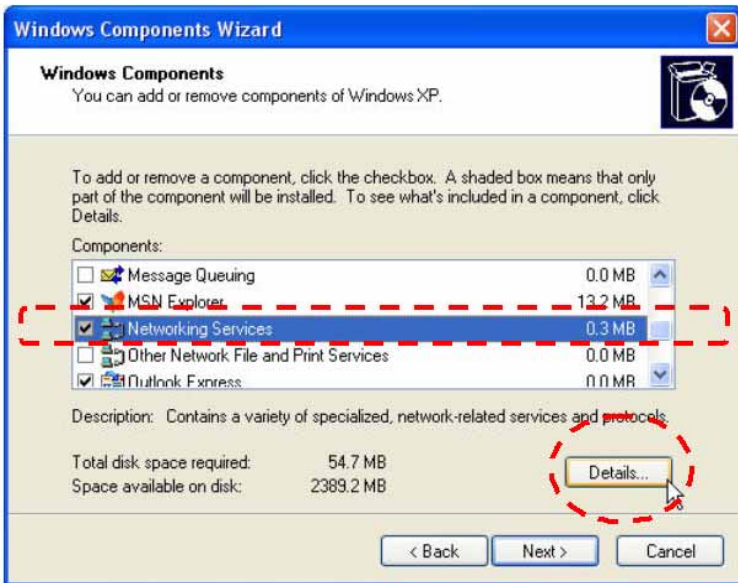
Note: For more information please consult Microsoft's website.

Hint: Look for the red circles denoting where to click.

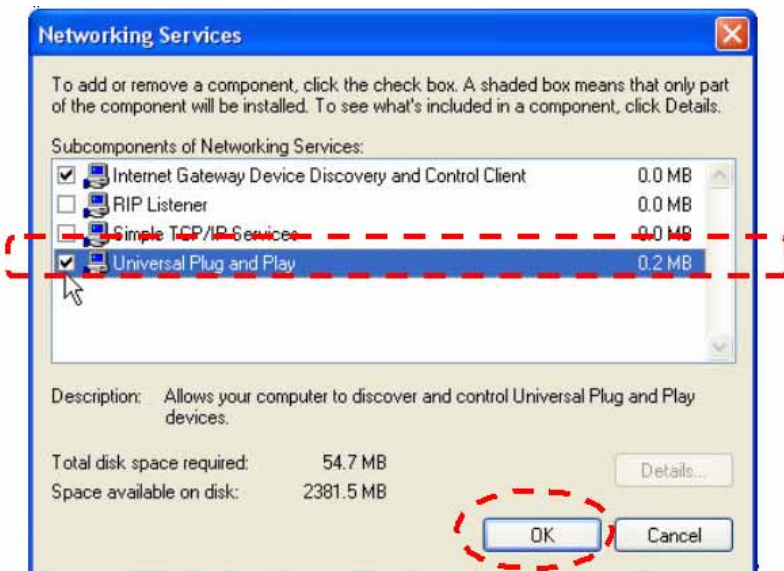
1. Open Control Panel and select Add or Remove Programs
2. Choose the Add/Remove Windows Components icon on the left hand side.



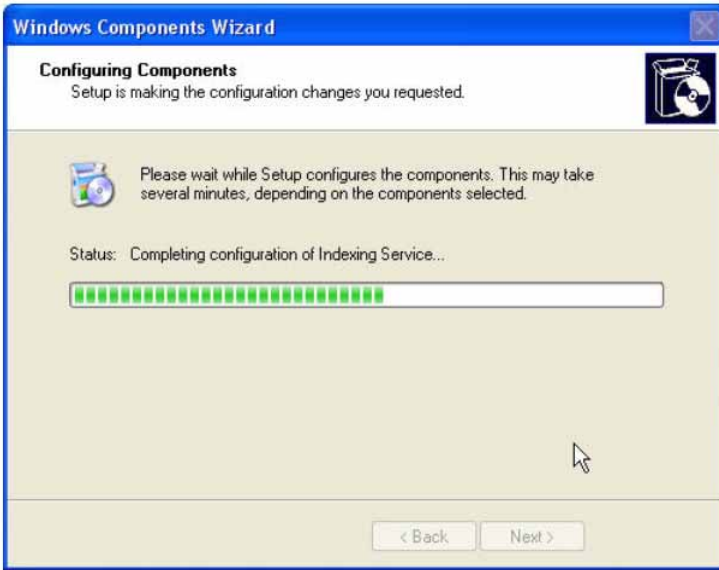
- When the Windows Components wizard open scroll down to find and select Networking services. Then click Details.



- Ensure that Universal Plug and Play is ticked and then click OK.



5. Wait for Windows to copy files and make changes.



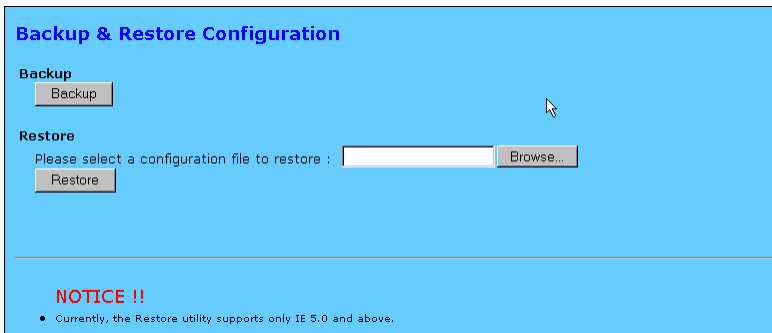
6. Click Finish to close the Wizard.



4-18 Back Up and Restore

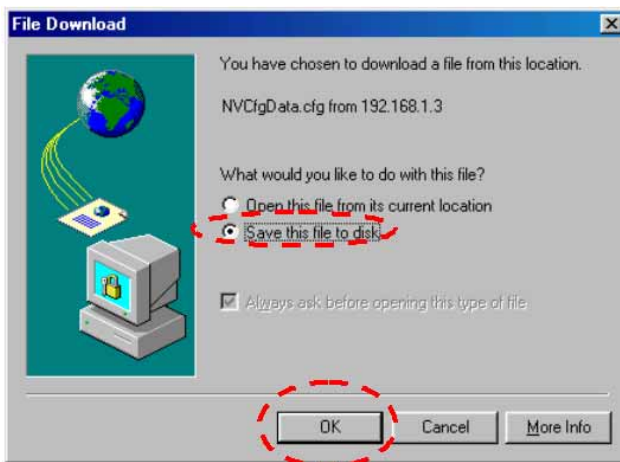
The NB5540 has the ability to store the current configuration to a file. This information can then be restored to the router at a later date.

Note: *Your router's configuration should be kept secret and in a secure location to prevent unwanted access to password or network topology information. Currently you should only use Internet Explorer version 5.0 or above to back up your router.*



To Back up your router;

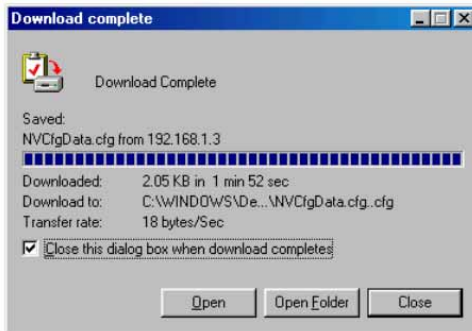
1. Click the Backup button. When the File download window opens select Save this file to disk. Click OK
2. Choose the location where you would like to store the file and enter the file name (leave the .cfg extension). Click Save.
3. If required when the download is complete click the Close button.



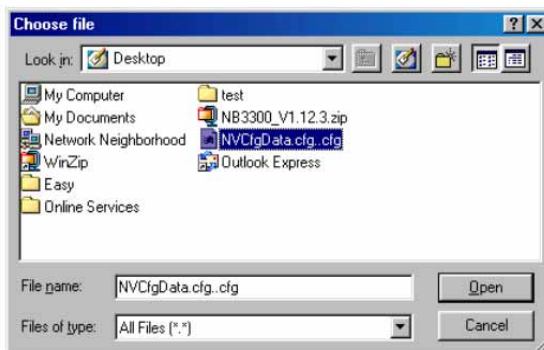
To Restore your Router's configuration;



1. Log into the router and click the Backup and Restore menu item from the left hand menu.



2. Click the Browse button to open a Choose file window, search and select your previously backed up file. Click Open.
3. When you return to the Backup & Restore screen you should see the file path in the white field. Click the Restore button to start the configuration upload.



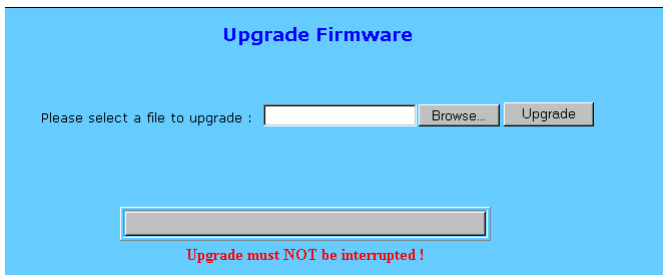


- Once the upload is complete the router should reboot and implement the new configuration. The IP address and subnet of the could now be different, perform a "IPconfig Release and renew" to check if the browser menu stops responding.

Note: *You may not be able to restore a configuration that was backed up from a different version of firmware. It is strongly advised that you try to match the firmware version in your router to the version from which the backup file was made.*

4-19 Upgrade Firmware

This setting page allows you to upgrade the latest version firmware to keep your router up-to-date. Before you upgrade the firmware, you have to get the latest firmware and save it on the PC you use to configure the router.



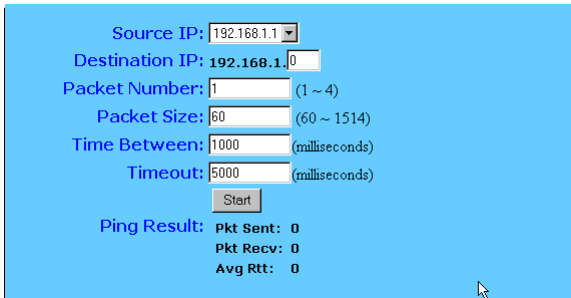
- **Select a file to upgrade** Enter path of the latest firmware you saved on the PC. You can choose "Browsing" to view the folders and select the firmware.
- **Upgrade** After you enter or select the path, click "Upgrade" to proceed firmware upgrade process. Please note that don't power off the router during the firmware upgrading.

4-20 Diagnostics (Ping & Tracert)

The Ping / Trace Route Diagnostics can be independently selected by clicking on either "Ping" or "Tracert" on the left hand menu. These features are handy tools for diagnosing network faults and ISP service faults.

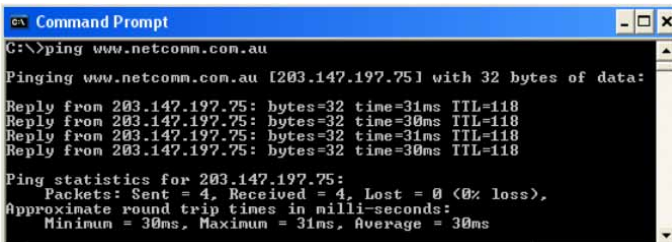
Ping - Operates in a similar way to most Ping utilities, It will send a ping via the ICMP protocol and receive a response from the target if it is configured to respond. You can choose if the ping originates from the LAN (Private) side of the router or from the WAN (Public) side of the router.

Note: *Just because a computer does not respond to a ping doesn't mean it is not functional or on the same IP address. Computers and routers can be configured to NOT respond to pings and yet they can still transfer TCP / IP data. Most Windows default installations will respond to a Ping.*



Source IP: 192.168.1.1
Destination IP: 192.168.1.0
Packet Number: 1 (1 ~ 4)
Packet Size: 60 (60 ~ 1514)
Time Between: 1000 (milliseconds)
Timeout: 5000 (milliseconds)
Start
Ping Result: Pkt Sent: 0
Pkt Recv: 0
Avg Rtt: 0

Hint: For testing WAN (internet) connectivity it is handy to perform a DOS ping to a website from a computer that has confirmed internet access to obtain a IP number for your router test see the screen shot below;



```
ex Command Prompt
C:\>ping www.netcomm.com.au

Pinging www.netcomm.com.au [203.147.197.75] with 32 bytes of data:

Reply from 203.147.197.75: bytes=32 time=31ms TTL=118
Reply from 203.147.197.75: bytes=32 time=30ms TTL=118
Reply from 203.147.197.75: bytes=32 time=31ms TTL=118
Reply from 203.147.197.75: bytes=32 time=30ms TTL=118

Ping statistics for 203.147.197.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 30ms, Maximum = 31ms, Average = 30ms
```

Ping example 1 - Testing Router connectivity to a local computer.

1. Leave the source IP to be the LAN IP address of the router.
2. Enter the last number set of the IP address of your local target computer (eg 192.168.1.100).
3. Set your number of test packets to send (either 1, 2, 3 or 4).
4. Leave packet size as default 60 bytes.
5. Leave time between packets as default 1 second (1000 milliseconds).
6. Leave time out as default 5 seconds (5000 milliseconds).
7. Click Start.
8. Check that packets Received equal at least 1 for confirmation of a successful ping. Packet loss can be determined by comparing packets sent to packets received.

Ping example 2 - Testing Internet connectivity (your router's connection to the Internet)

1. Change the source IP to be the WAN IP address of the router.
2. Enter the whole IP address of your target computer (E.g. use the number you discovered in the hint above such as 203.147.197.75).
3. Set your number of test packets to send (either 1, 2, 3 or 4)
4. Leave packet size as default 60 bytes.
5. Leave time between packets as default 1 second (1000 milliseconds).
6. Leave time out as default 5 seconds (5000 milliseconds).
7. Click Start.
8. Check that packets received equals at least 1 to confirm a good ping response. Total packet loss can be determined by comparing packets sent to packets received.

Trace Route - Operates in a way to most Trace Route programs and is used to Trace all the routing points from the Source (the Router) to the Destination (The IP address entered).



Note: *Not all routers in an IP path will allow self identification hence you may see some hops along the way left as blanks. Also it is possible that the final destination may not respond to the Trace Route Query even though it exists and can exchange data via TCP / IP.*

Chapter 5: Configuring IPSec/VPN Tunnels

5-1 VPN/IPSec Introduction

The VPN Router creates secure communications between sites without the expense of leased site-to-site lines. A VPN tunnel is a combination of authentication, encryption, tunneling and access control technologies used to transport traffic over the Internet or any insecure network. IPSec (Internet Protocol Security) is an industry-standard protocol suite that provides confidentiality, data integrity and authentication at the IP Layer to offer secure communications across a public network like the Internet.

IPSec Components

IPSec contains the following protocols:

- Encapsulating Security Payload (ESP):
Provides confidentiality, authentication, and integrity.
- Authentication Header (AH):
Provides authentication and integrity.
- Internet Key Exchange (IKE):
Provides key management and Security Association (SA)

Security Association (SA)

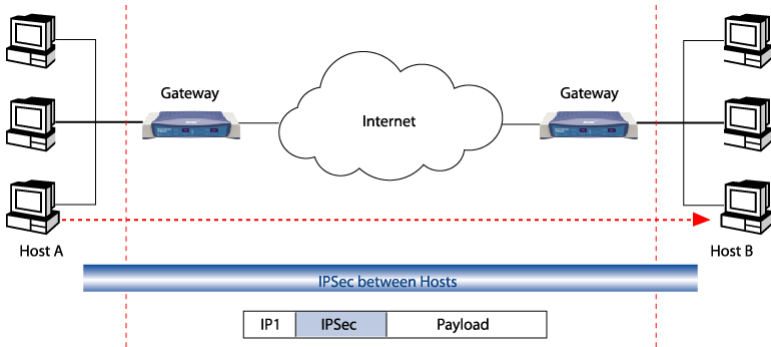
An SA provides data protection for unidirectional traffic as defined in the IPSec protocols. An IPSec tunnel typically consists of two unidirectional SAs, which together provide a protected, full-duplex data channel.

IPSec can be used in tunnel mode or transport mode. Typically, the tunnel mode is used for gateway-to-gateway IPSec tunnel protection, while transport mode is used for host-host IPSec tunnel protection. A gateway is a device that monitors and manages incoming and outgoing network traffic and routes the traffic accordingly. A host is a device that sends and receives network traffic.

Transport Mode

The transport mode IPSec implementation encapsulates only the packet's payload. The IP header is not changed. After the packet is processed with IPSec, the new IP packet contains the old IP header (with the source and destination IP addresses unchanged) and the processed packet payload.

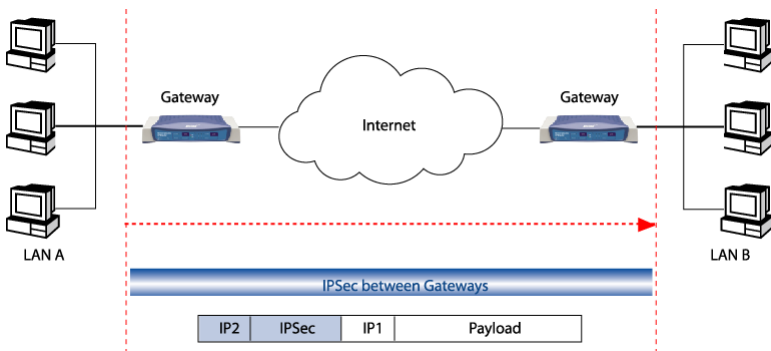
Tunnel Mode



The tunnel mode IPSec implementation encapsulates the entire IP packet.

The entire packet becomes the payload of the packet that is processed with IPSec. A new IP header is created that contains the two IPSec gateway addresses. The gateways perform the encapsulation/decapsulation on behalf of the hosts. Tunnel mode ESP prevents an attacker from analyzing the data and deciphering it, as well as knowing who the packet is from and where it is going.

Key Management



IPSec uses the Internet Key Exchange (IKE) protocol to facilitate and automate the SA setup and the exchange of keys between parties transferring data. IPSec requires that keys be re-created, or refreshed, frequently so that the parties can communicate securely with each other. IKE manages the process of refreshing keys; however, a user can control the key strength and the refresh frequency. Refreshing keys on a regular basis ensures data confidentiality between sender and receiver.

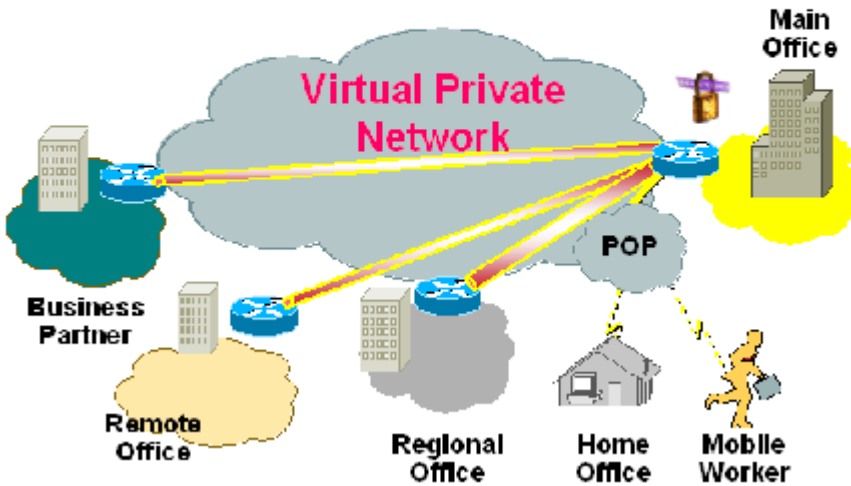
5-2 VPN Application Types

VPNs address the following applications

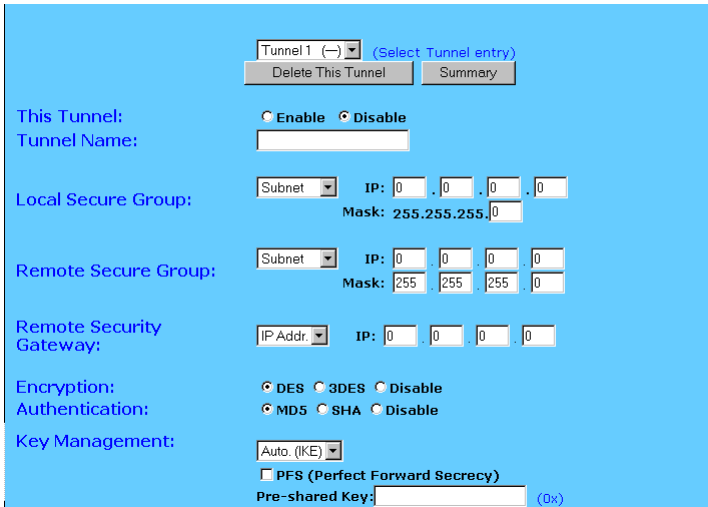
- Provide telecommuting workers with access to central office resources.
- Interconnect branch offices to enable corporate intranets.
- Connect business partners over the Internet with significant cost savings.

Virtual: Encapsulation 

Private: Security 



5-3 VPN / IPSec Setup



1. Select the tunnel you wish to create in the **Select Tunnel Entry** drop-down box. It is possible to create up to 70 simultaneous tunnels.

Then select **Enable** to enable the tunnel.

Once the tunnel is enabled, enter the name of the tunnel in the **Tunnel Name** field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

2. Under **Local Secure Group** and **Remote Secure Group**, you may choose one of five options:

- **Subnet** - If you select Subnet (which is the default), this will allow all computers on the local subnet to access the tunnel. In the example shown below, all Local Secure Group computers with IP Addresses 192.168.1.xxx will be able to access the tunnel. All Remote Secure Group computers with IP Addresses 192.168.2.xxx will be able to access the tunnel.



When using the Subnet setting, the default value of 0 should remain in the last octet of the **IP** and **Mask** fields.

- **IP Address** - If you select IP Address, only the computer with the specific IP Address that you enter will be able to access the tunnel. In the example shown below, only the computer with IP Address 192.168.1.101 can access the tunnel from this end. Only the computer with IP Address 192.168.2.51 can access the tunnel from the remote end.



This Tunnel: Enable Disable

Tunnel Name: tunnel_1

Local Secure Group: IP Addr IP: 192 . 168 . 1 . 101

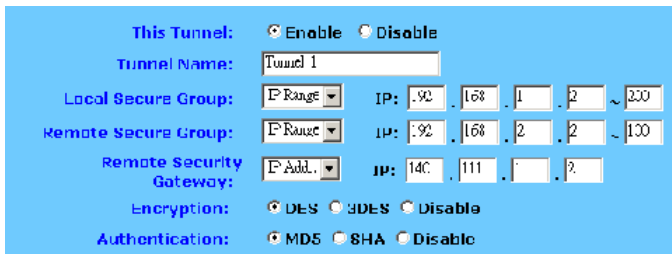
Remote Secure Group: IP Addr IP: 192 . 168 . 2 . 51

Remote Security Gateway: IP Addr IP: 140 . 111 . . . 2

Encryption: DES 3DES Disable

Authentication: MD5 SHA Disable

- **IP Range** - If you select IP Range, it will be a sort of combination of Subnet and IP Address. You can specify a range of IP Addresses on the Subnet which will have access to the tunnel. In the example shown below, all computers on this end of the tunnel with IP Addresses between 192.168.1.2 and 192.168.1.200 can access the tunnel from the local end. Only computers assigned an IP Address between 192.168.2.2 and 192.168.2.100 can access the tunnel from the remote end.
- **Host** – If you select Host, the value should be set the same as the Remote Security Gateway setting
- **Any** – When this option is selected, this Gateway accepts requests from any IP address such as remote users, mobile users or telecommuters using dynamic IP.



This Tunnel: Enable Disable

Tunnel Name: Tunnel 1

Local Secure Group: IP Range IP: 192 . 168 . 1 . 2 ~ 200

Remote Secure Group: IP Range IP: 192 . 168 . 2 . 2 ~ 100

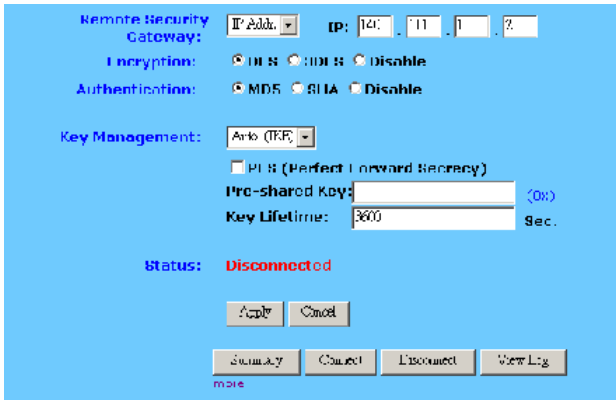
Remote Security Gateway: IP Addr IP: 140 . 111 . . . ?

Encryption: DES 3DES Disable

Authentication: MD5 SHA Disable

- Under Remote Security Gateway, enter the *Public* IP Address of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Router, a VPN Server, or a host with VPN software. In the example shown above, the IP Address of the Remote Security Gateway is 140.111.1.2. This IP Address may either be **static** or **dynamic**, depending on the settings of the remote VPN device. When connecting between two routers the remote security gateway will be the public (WAN) IP address of the remote router as given on the status page or by the remote ISP.
- Using **Encryption** also helps make your connection more secure. There are two different types of encryption: **DES** or **3DES**. You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting **Disable**. In our example shown below, DES (which is the default) has been selected.

5. **Authentication** acts as another level of security. There are two types of authentication: **MD5** and **SHA**. As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to **Disable** authentication. In the screen below, MD5 (the default) has been selected.



Remote Security Gateway: IP Addr: [] IP: [10] . [11] . [1] . [?]

Encryption: DES 3DES Disable

Authentication: MD5 SHA Disable

Key Management: Auto (IKE)

PFS (Perfect Forward Secrecy)

Pre-shared Key: [] (OK)

Key Lifetime: 3600 Sec.

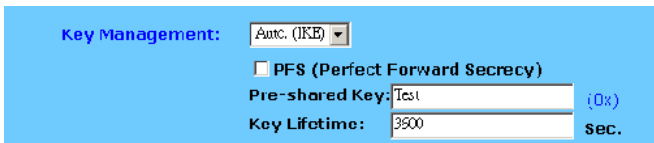
Status: **Disconnected**

Apply Cancel

Summary Connect Disconnect View Log

more

6. In order for any encryption to occur, the two ends of the tunnel must agree on the type of encryption and the way the data will be decrypted. This is done by sharing a “key” to the encryption code. Under Key Management, you may choose Auto (IKE) and enter a series of numbers or letters in the Pre-shared Key field. In the example shown below, the word Test is used. Based on this word (which **MUST** be entered at both ends of the tunnel) a code is generated to scramble (encrypt) the data being transmitted over the tunnel, where it is unscrambled (decrypted). You may use any combination of up to 23 numbers or letters in this field. No special characters or spaces are allowed. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you’d like the key to be used, or leave it blank for the key to last indefinitely.



Key Management: Auto (IKE)

PFS (Perfect Forward Secrecy)

Pre-shared Key: Test (OK)

Key Lifetime: 3600 Sec.

Similarly, you may choose Manual Keying, which allows you to generate the code yourself. Enter your code into the Encryption KEY field. Then enter an Authentication KEY into that field. These fields must both match the information that is being entered in the fields at the other end of the tunnel. The example shown below displays some sample entries for both the Encryption and Authentication Key fields. Again, up to 23 alphanumeric characters are allowed to create this key.

The Inbound SPI and Outbound SPI fields are different, however. The Inbound SPI value set here must match the Outbound SPI value at the other end of the tunnel. The Outbound SPI here must match the Inbound SPI value at the other end of the tunnel. In the example (see above), the Inbound SPI and Outbound SPI values shown would be opposite on the other end of the tunnel. Only numeric characters can be used in these fields.

Key Management: Manual

Encryption KEY: (U>)

Authentication KEY: (0>)

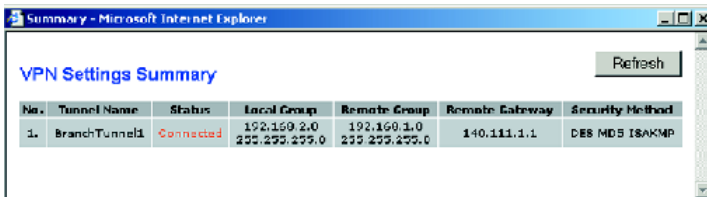
Inbound SPI: (0)

Outbound SPI: (0)

Once you are satisfied with all your settings, click the Apply button. If you make any mistakes, clicking the Cancel button will exit the screen without saving any changes, provided that you have not already clicked the Apply button.

After the VPN device is set up at the other end of the tunnel, you may click the Connect button to use the tunnel. This assumes that both ends of the tunnel have a physical connection to each other (e.g., over the Internet, physical wiring, etc.). After clicking the Connect button, click the Summary button. If the connection is made, the screen shown below will appear:

Under Status, the word Connected should appear if the connection is successful. The other fields reflect the information that you entered on the VPN screen to make the connection. If Disconnected appears under Status, some problem exists that prevents the creation of the tunnel.



- Double-check all the values you entered on the VPN screen to make sure they are correct.
- Check the status page of both the local router and the remote device and ensure the public IP addresses are the same as entered for the remote security gateway.

If, for any reason, you experience a temporary disconnection, the connection will be re-established as long as the settings on both ends of the tunnel stay the same.

To get more details concerning your tunnel connection, click the View Log button.

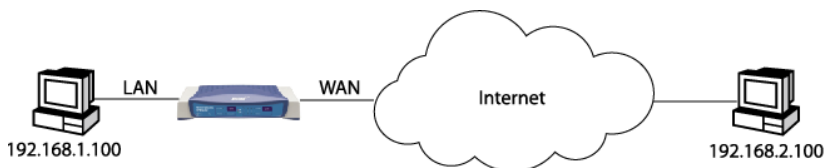
The VPN Log screen displays successful connections, transmissions and receptions, and the types of encryptions used. Once you no longer have need of the tunnel, simply click the Disconnect button on the bottom of the VPN page.

5-4 Example1: Tunnel between Two VPN Routers



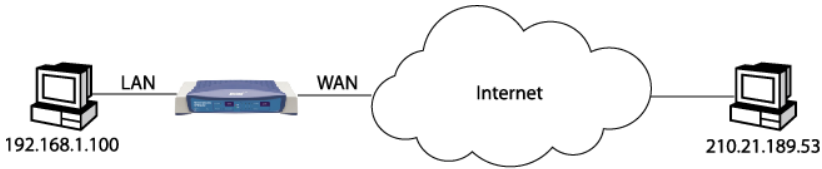
	VPN Router #1	VPN Router #2
LAN IP:	92.168.1.1	192.168.2.1
WAN IP:	210.241.239.77	211.21.189.53
Default Gateway:	210.241.239.73	211.21.189.49
	Tunnel 1	Tunnel 1
This Tunnel:	Enable	Enable
Local Secure Group:	Subnet 192.168.1.0, 255.255.255.0	Subnet 192.168.2.0, 255.255.255.0
Remote Secure Group:	Subnet 192.168.2.0, 255.255.255.0	Subnet 192.168.1.0, 255.255.255.0
Remote Security Gateway:	211.21.189.53	210.241.239.77
Encryption:	DES	DES
Authentication:	MD5	MD5
IPSec:	ISAKMP	ISAKMP
PFS:	Off	Off
IKE Pre-share KEY:	MyTest	MyTest

5-5 Example2: Tunnel between VPN Router and VPN Client with Fix IP



	VPN Router #1	
LAN IP:	192.168.1.1	
WAN IP:	210.241.239.77	IP: 140.111.1.2
Default Gateway:	210.241.239.73	140.111.1.1
	Tunnel 1	Tunnel 1
This Tunnel:	Enable	Enable
Local Secure Group:	Subnet 192.168.1.0, 255.255.255.0	IP: 140.111.1.2
Remote Secure Group:	IP: 140.111.1.2	Subnet 192.168.1.0, 255.255.255.0
Remote Security Gateway:	140.111.1.2	140.111.1.1
Encryption:	DES	DES
Authentication:	MD5	MD5
IPSec:	ISAKMP	ISAKMP
PFS:	Off	Off
IKE Pre-share KEY:	MyTest	MyTest

5-6 Example3: Tunnel between VPN Router-and-VPN Client with dynamic IP



VPN Router #1

LAN IP: 192.168.1.1
 WAN IP: 210.241.239.77
 Default Gateway: 210.241.239.73

Tunnel 1

This Tunnel: Enable
 Local Secure Group: Subnet 192.168.1.0, 255.255.255.0
 Remote Secure Group: IP: Any
 Remote Security Gateway: Any
 Encryption: DES
 Authentication: MD5
 IPSec: ISAKMP
 PFS: Off
 IKE Pre-share KEY: MyTest

Win2000 Professional Safenet Cisco VPN Client

IP: 210.21.189.53
 210.21.189.49

Tunnel 1

Enable
 IP: 211.21.189.53
 Subnet 192.168.1.0, 255.255.255.0
 210.241.239.77
 DES
 MD5
 ISAKMP
 Off
 MyTest

Chapter 6: Configuring IPsec on Windows 2000/XP

This chapter 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>

6-1 Environment

Windows XP or Windows 2000 Server

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

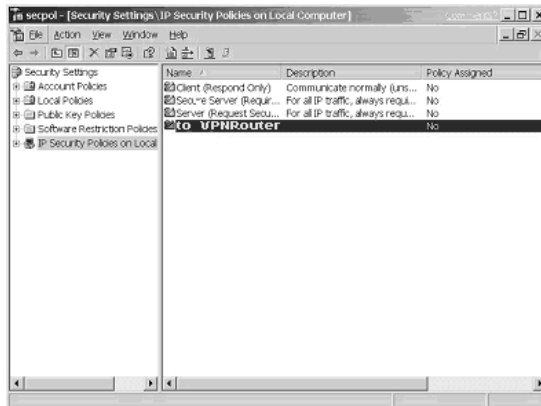
IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

6-2 Steps in Windows 2000/XP

6-2.1 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**.

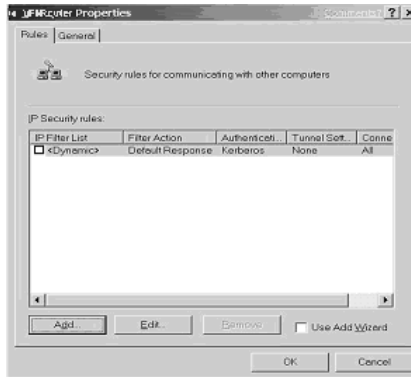


3. Click **Next**, and then type a name for your policy (for example, “**to_VPNRouter**”).
4. Deselect the **Activate the default response rule** check box, and then click **Next** button.
5. Click the **Finish** button, making sure the **Edit** check box is checked.

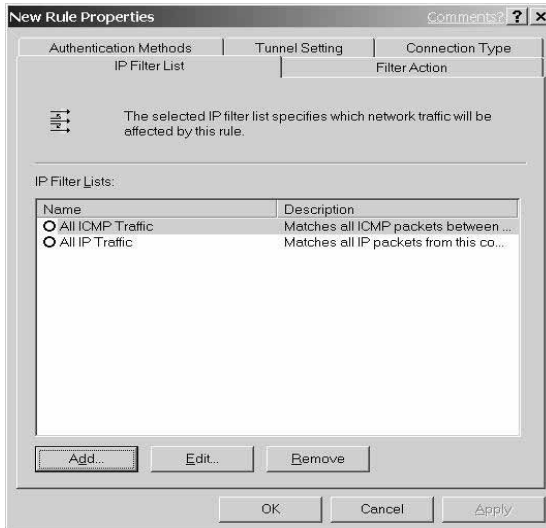
6-2.2 Build 2 Filter Lists: “WinXP→Cable/DSL Firewall Router” and “Cable/DSL Firewall Router→WinXP”.

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

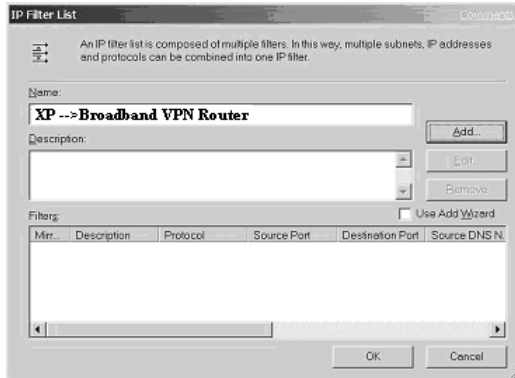
1. In the **to_VPNRouter Properties**, deselect the **Use Add Wizard** check box, and then click **Add** button to create a new rule.



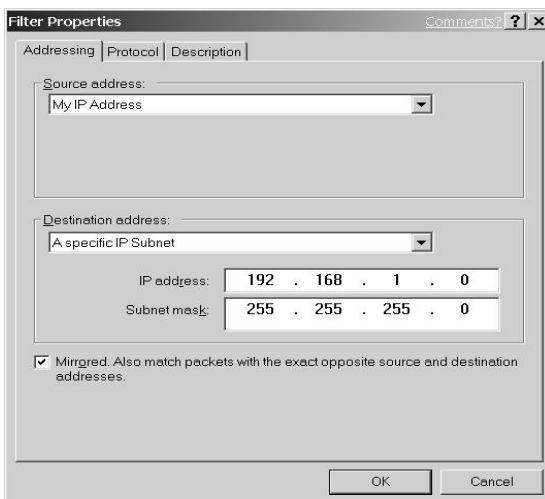
2. From the **IP Filter List** tab, click the **Add** button.



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.



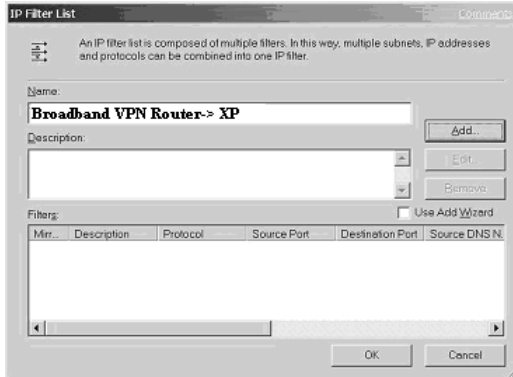
4. In the **Source address** area, click **My IP Address**.
5. In the **Destination address** field, select **A specific IP Subnet**, and fill in the **IP Address** “**192.168.1.0**” and **Subnet mask** “**255.255.255.0**”.



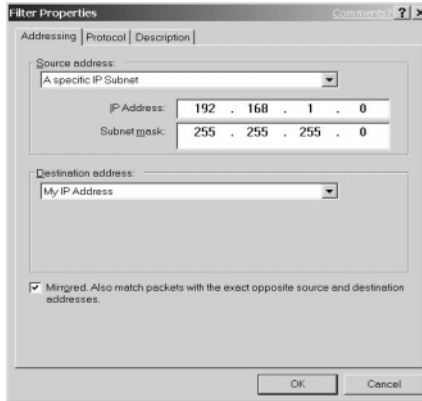
6. If you want to type a description for your filter, click the **Description** tab.
7. Click **OK** button. Then click **OK**(for WinXP) or **Close** (for Win2000) button on the **IP Filter List** window.

[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 Router→XP**” 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**.

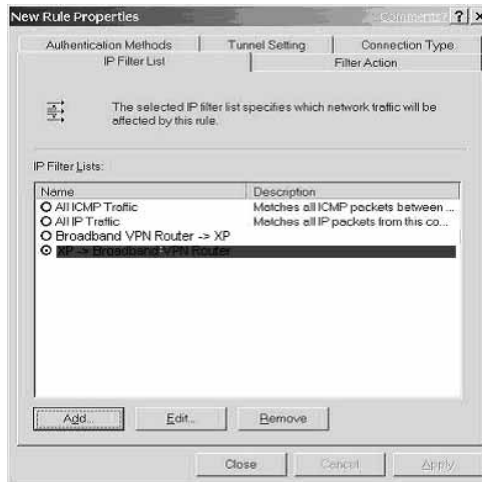


- 12. If you want to type a description for your filter, click the **Description** tab.
- 13. Click **OK**, and then click **OK**.

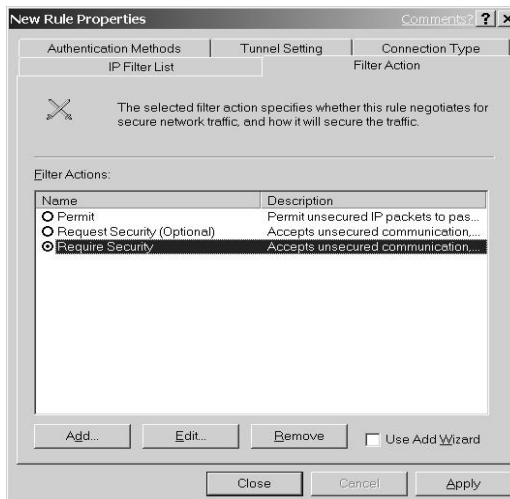
6-2.3 Configure Individual Rule of 2 Tunnels

[Tunnel 1] WinXP→Cable/DSL Firewall Router

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

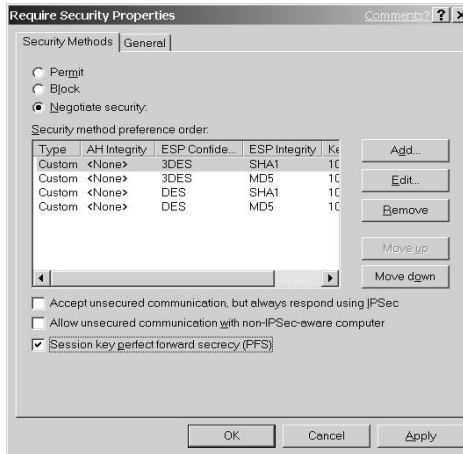


2. From the **Filter Action** tab, click the filter action “**Require Security**”, and click the **Edit** button.

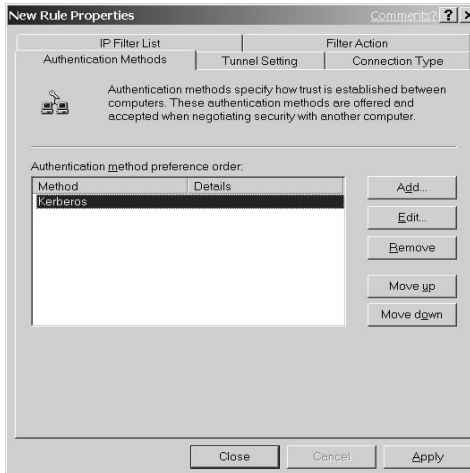


3. Check that the **Negotiate security** option is enabled, and deselect the **Accept unsecured communication**, but always respond using **IPsec** check box.

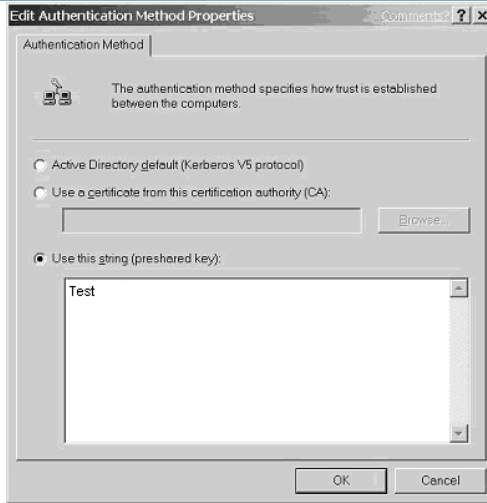
4. Select the **Session key Perfect Forward Secrecy (PFS)** and remember to check the **PFS** option on the Cable/DSL Firewall Router, and then click the **OK** button.



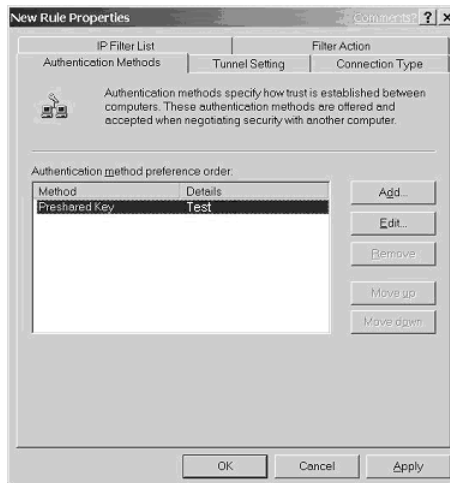
5. From the **Authentication Methods** tab, click the **Edit** button.



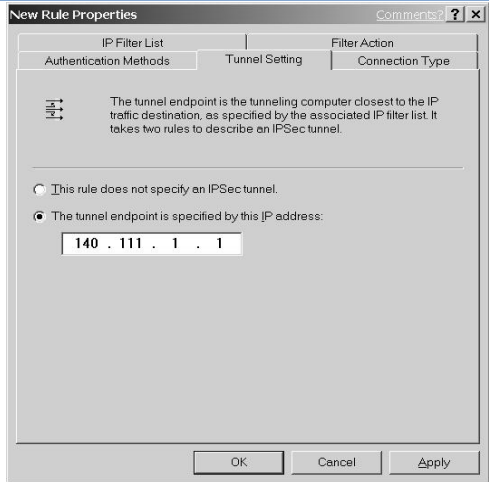
6. Change the authentication method to **“Use this string (preshared key)”**, enter the string **“Test”**, and then click the **OK** button.



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.

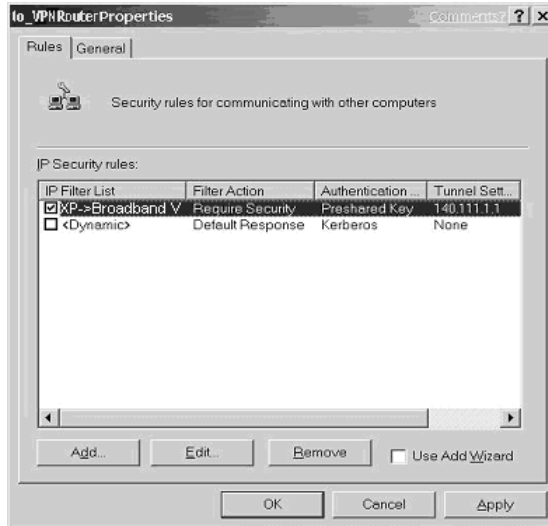


- From the **Connection Type** tab, select **All network connections**, and then click the **OK** or **Close** button to finish this rule.

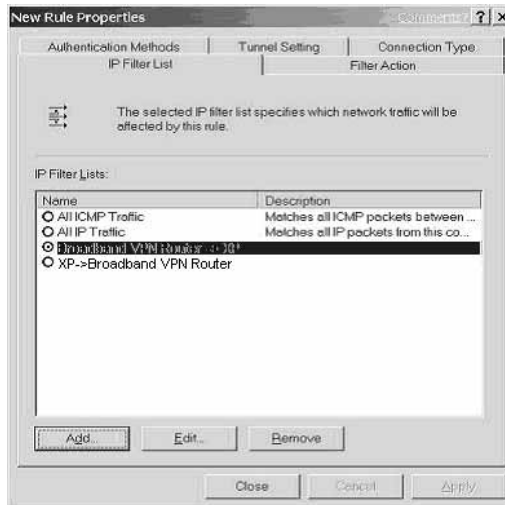


[Tunnel 2] Cable/DSL Firewall Router→ WinXP

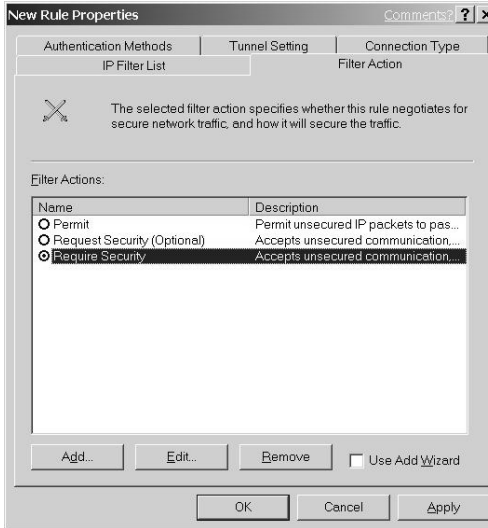
- In the **to_VPNRouter Properties**, deselect the **Use Add Wizard** check box, and then click the **Add** button to create the second IP Filter.



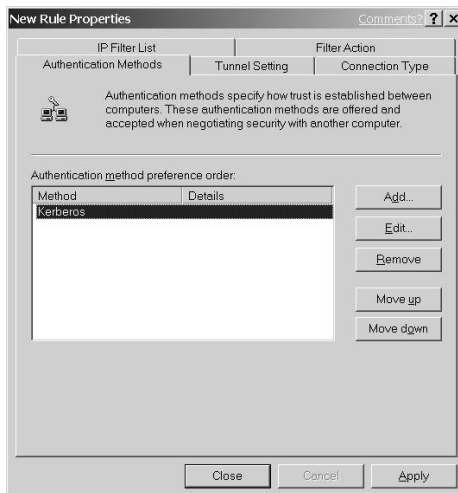
- On the **IP Filter List** tab, click the filter list **“Cable/DSL Firewall Router→XP”**.



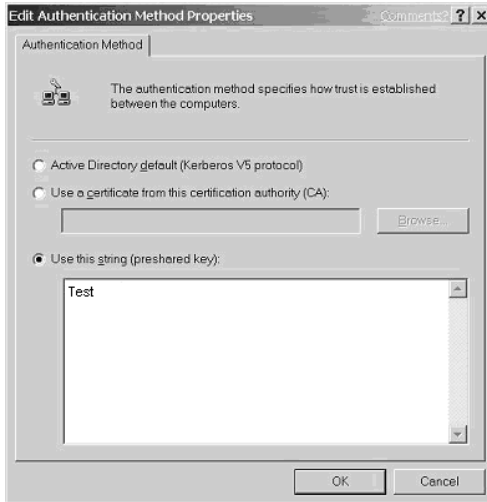
11. From the **Filter Action** tab, click the filter action **“Require Security”**.



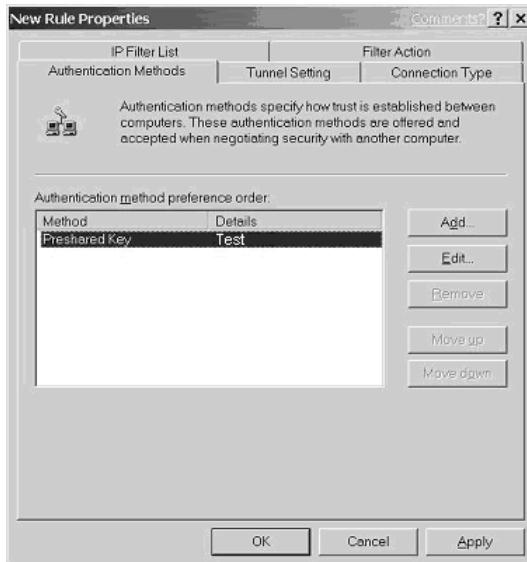
12. From the **Authentication Methods** tab, click the **Edit** button.



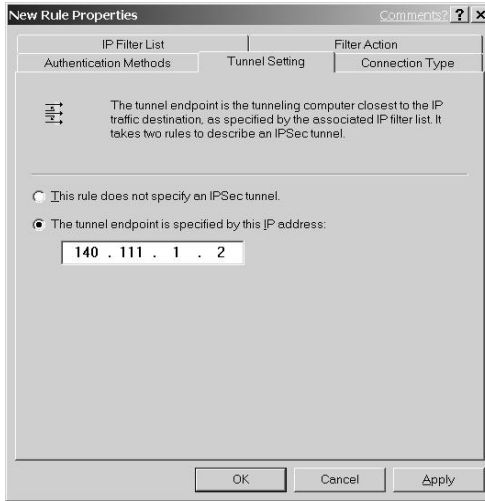
13. Change the authentication method to **“Use this string (presared key)”**, enter the string **“Test”**, and then click the **OK** button.



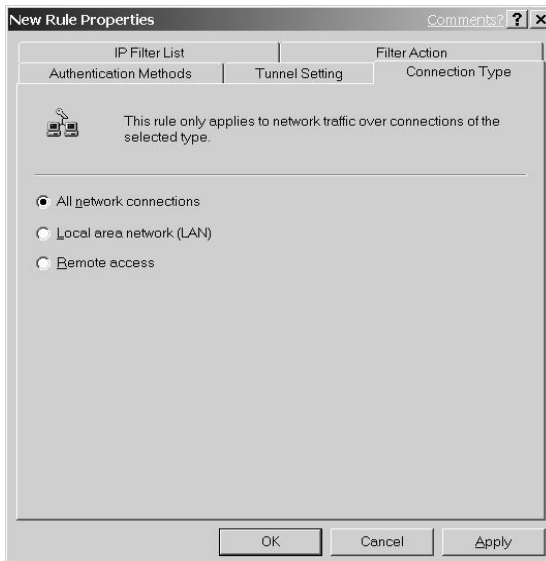
This new Preshared key will be displayed in Authentication method preference order. Click the **OK** button to continue.



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



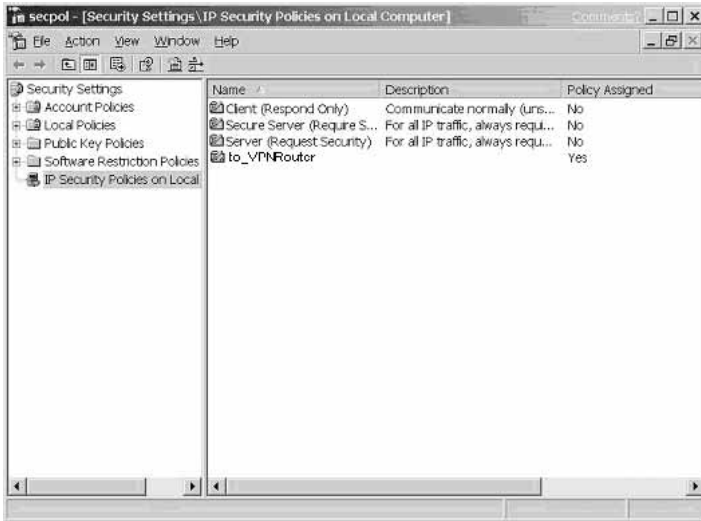
15. From the **Connection Type** tab, select **All network connections**, and then click the **OK**(for WinXP) or **Close**(for Win2000) button to finish.



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

6-2.4 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.



6-3 Steps in Cable/DSL Firewall Router

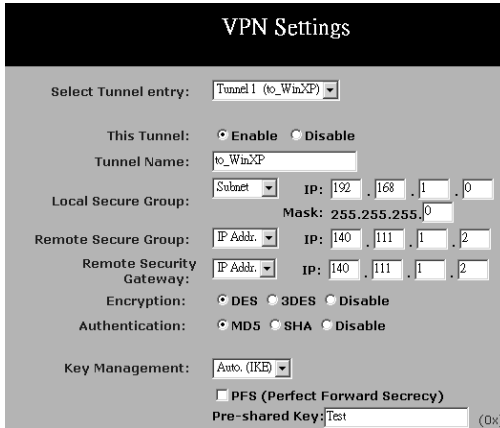
6-3.1 OnePage Setup Screen

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"> • OnePage Setup • Advanced • VPN • DHCP Settings • Access Control • Virtual Server • DMZ Host • Device Admin. • Status Monitor • Dynamic Routing • Static Routing • Special App • Log 	<p>Private IP Address (MAC Address: 00-01-36-02-DE-F9)</p> <p>Device IP Address: <input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="1"/> <input type="text" value="1"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0"/></p> <p>WAN Connection Type <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"/> <input type="text" value="111"/> <input type="text" value="1"/> <input type="text" value="1"/></p> <p>Subnet Mask: <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/></p> <p>Default Gateway Address: <input type="text" value="140"/> <input type="text" value="111"/> <input type="text" value="1"/> <input type="text" value="2"/></p> <p>DNS (Required) 1: <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/></p> <p>DNS 2: <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/></p> <p>DNS 3: <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/></p> <p style="text-align: right;"><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>

6-3.2 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 (Dx)

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 7: Trouble Shooting

This chapter provides solutions to problems you may encounter during installation and operation of your NetComm 11G Wireless Firewall Router.

Hardware

T: The Power LED is off.

Check the power cable is properly connected to the NetComm 11G Wireless 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 11G Wireless 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 11G Wireless Firewall Router?

First, check whether the NetComm 11G Wireless 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 11G Wireless 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 11G Wireless 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 11G Wireless 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 11G Wireless 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 11G Wireless Firewall Router

Ensure your computer can ping or access the Router. See the previous section entitled "Why can't I configure the NetComm 11G Wireless 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 11G Wireless Firewall Router's settings are correct (3-3).

Appendix A: Frequently Asked Questions

Q: What is the maximum number of IP Addresses the NetComm 11G Wireless Firewall Router can support?

The NetComm 11G Wireless Firewall Router can support up to 253 IP Addresses usually in the range of 192.168.1.2~192.168.1.254.

Q: Where should the NetComm 11G Wireless Firewall Router be installed on the network?

In a typical environment, the NetComm 11G Wireless Firewall Router should be installed between the ADSL/Cable modem and your LAN. Connect the NetComm 11G Wireless 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 11G Wireless Firewall Router support IPX or AppleTalk?

No. The NetComm 11G Wireless 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 11G Wireless Firewall Router can support them.

Q: Does the NetComm 11G Wireless Firewall Router support 100Mb Ethernet?

Yes, the NetComm 11G Wireless 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 11G Wireless Firewall Router share single user account to multiple users?

The NetComm 11G Wireless 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 11G Wireless Firewall Router series support?

The NetComm 11G Wireless 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 11G Wireless 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 11G Wireless Firewall Router uses NAT to route all in/out band packets. All external users can only see the IP of the NetComm 11G Wireless Firewall Router but cannot access LAN computers. The LAN computers are well protected with the NetComm 11G Wireless 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 11G Wireless Firewall Router support PPTP of VPN packets pass through?

Yes. The NetComm 11G Wireless Firewall Router supports PPTP pass through.

Q: Does the NetComm 11G Wireless Firewall Router series support IPsec?

Yes. The NetComm 11G Wireless Firewall Router supports IPsec pass through.

Appendix B: Technical Specifications

Standards	IEEE 802.11g and 802.11b standard compliant, IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX)
Ports	WAN: One 10/100 RJ-45 port LAN: Four 10/100 RJ-45 ports All ports with auto cross-over detection
Protocol	TCP/IP, UDP, NAT,DHCP, PPPoE, Heartbeat, CHAP, PAP
Maximum Users	Up to 253 users
Cabling Type	UTPCategory 5 or better
Antenna	Single external antenna with reversed SMA connector
Frequency Range	2.4-2.4835GHz (Industrial Scientific Medical Band)
Operating Channels	<i>11b Mode:</i> 11 Channels (USA, Canada) 13 Channels (Europe & Australia) 14 channels (Japan) <i>11g Mode:</i> 11 Channels (USA, Canada) 13 Channels (Europe, Japan, Australia)
Modulation	CCK for 11b mode (1, 2, 5.5, 11Mbps) OFDM for 11g mode (6, 9, 12, 24, 36, 48, 54Mbps)
Data Transmission Rate	54Mbps / 48 / 36 / 24 / 12 / 11 / 9 / 6 / 5.5 / 2 / 1 Mbps Auto Fall-Back
Access Mode	Infrastructure mode Ad-hoc mode
Roaming	IEEE 802.11 Compliant
IPSetting	WAN: DHCPclient, Static IP LAN: DHCPauto-assignment, Static IP
VPN Endpoints-IPSec	Maximum tunnels: up to 5 Local secure group: IP, Subnet or IPrange. Remote secure group: IP, Subnet, IPrange, Host or Any Remote security Gateway: IP, FQDN, Any Encryption: DES, 3DES or none Authentication: MD5, SHA or none Authentication method: Preshared key Key Management: Auto IKE (PFS or none) or Manual (Encry, Auth, In-SPI, Out SPI)
VPN Pass-through (NATtraversal)	IPSec enable/disable PPTPenable/disable Concurrent sessions: up to 50 dependent on data
Firewall & Security	Prevent Dos attack: Ping of Death, LAND, IP spoofing, SYN flood, IPSmurfing Stateful packet inspection (check inbound against outbound) NATdeny external Intruder Provides both 64-bit & 128-bit WEP Encryption ACLFilter: IP, MAC, URLkeyword Block all: Proxy, Active X, Java /script, cookies, time of day/week
Power	External, 12VDC, 1.0 Amps
Operating Temp	0 ~ 45°C
Certifications	C-Tick
System Requirements	Operating system independent – ideal for Windows, Macintosh, Linux & TCP/IPsystems

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

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

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

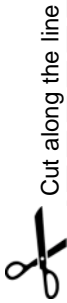
Fax: (02) 9424-2010

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.



Cut along the line

Warranty Registration Form

Date of Purchase

Name

Company

Address

..... Post Code

Tel No () Fax No ()

E-mail

The following information is vital for your warranty

Please make sure it's correct and complete.

Serial No

Model

Product Type:

PC Card

External

Internal

Other

**Make sure
you fill this
section in!**

I intend to use this product at:

Home

School/College/University

Business

Government Office

Dealer's Name

Dealer's Address

..... Post Code

Tel No () Fax No ()

How did you find out about our products?

.....

.....

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.
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.

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

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;

All-in-one advanced firewall, 2.4GHz wireless & VPN router

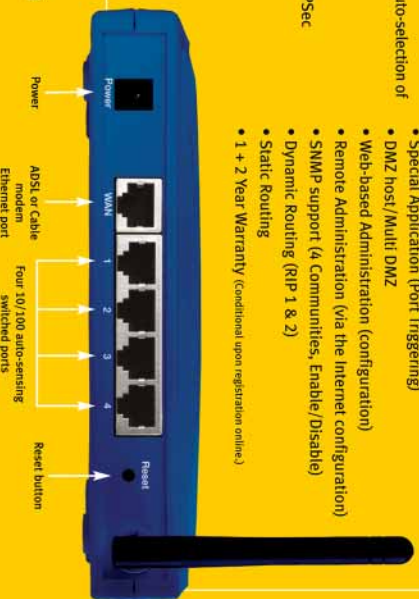
The NB5540 is designed to get Australians sharing the Internet easily, safely and wirelessly – without the need for technical expertise. Fully featured to cover a wide range of users, it includes an Active Firewall to help protect your computers from attack and 5 VPN endpoints so you can connect to the office from home or anywhere in the world via the Internet.



WIRELESS CONNECTIONS

Key Features

- One-Page-Setup (covers PPPoE ADSL, Optus cable, DHCP, Telstra Cable Heatbeat, Static IP)
- Active Firewall featuring Stateful Packet Inspection (SPI) and prevention of DOS attack. (See side panel)
- 54Mbps wireless IEEE 802.11g standard with auto-selection of optimum data rates
- Network Address Translation (NAT)
- 5 VPN Endpoints
- VPN Pass-through or NAT Traversal (PPTP & IPsec enable/disable)
- Universal Plug and Play
- Ping Diagnostics
- Trace Route Diagnostics
- Back up & Restore Configuration
- Online Log viewer/Syslog/email reporting
- DDNS (Dynamic DNS)
- DHCP Server
- Access Control (ACLs by IP/Mac/URL keyword)
- Port Forwarding
- Special Application (Port Triggering)
- DMZ host/Multi DMZ
- Web-based Administration (configuration)
- Remote Administration (via the Internet configuration)
- SNMP support (4 Communities, Enable/Disable)
- Dynamic Routing (RIP 1 & 2)
- Static Routing
- 1 + 2 Year Warranty (Conditional upon registration online)



WIRED AND WIRELESS – QUICKLY

NetComm's NB5540's integrated 802.11g wireless AP and 4-port 10/100 Mbps switch make it quick and easy to deploy wireless and wired LAN without the extra costs of a wireless access point, hub or switch. The NB5540's efficient antenna has a range of up to 150 meters and provides up to 128 bit WEP data encryption for high-level security.

KEEP YOUR OLD WIRELESS EQUIPMENT

If you already use xMbps wireless equipment it can still be used with the NB5540 because the 802.11g standard is backwards compatible with 802.11b

EASY TO USE

NetComm's web-based One-Page-Setup means you do not need to install any drivers on your computer. All you need is a web browser, such as Internet Explorer, on any computer using any Operating System and you will be able to configure your connection.

SAFELY SHARE YOUR INTERNET CONNECTION

With just one ISP account and a Cable or ADSL modem, you can allow up to 253 Windows®, Macintosh or any other Ethernet-enabled computers safe access to the Internet to send and receive emails, surf the web and so on. The Active Firewall will guard against several forms of Denial of Service attacks as well as other types of Hacking by using Stateful Packet Inspection technology. (See side panels for details)

MAKE USING THE INTERNET EASIER

Universal Plug and Play allows Internet applications such as MSN Messenger® to operate automatically over your firewall without the need for extra configuration.

JOIN NETWORKS AND COMPUTERS SECURELY

NetComm's NB5540 supports automatic VPN pass-through to allow any existing VPN client applications to continue to work through your router. Alternatively you can use the five built-in IPsec end points to join to other office networks.

FIND FAULTS EASILY

To assist in configuring your network and fault finding, NetComm has added email logging, Ping and Trace Route diagnostics to the NB5540.



NetComm is Australia's own data communications and networking solutions provider. For more information on this and other NetComm products, please visit www.netcomm.com.au

NetComm Limited, 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

Trademarks and registered trademarks are the property of NetComm Limited or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the enclosed product. Product Code: NB5540