NetComm®

ADSL Integrated Gateway

ADSL

User Guide

NB5580W & NB5580

Australia connects with NetComm®

Contents

Quick Start Section

The following Quick Start pages are intended to be used by an advanced user to quickly configure the NetComm NB5580/W. It assumes that you are familiar with *Networking* and that you already have an ADSL enabled phone line. If you need further explanation, please refer to the more detailed sections of this document. This guide presumes that your NetComm NB5580/W is set to factory defaults (See *Resetting* if required).

The NB5580 is available in either standard or wireless versions. If you have purchased the NB5580W, refer to 4.10 Wireless or Chapter 7 - Security for information on setting up the wireless component of your Router.

Product naming conventions

This manual covers both the NB5580 and NB5580W ADSL integrated Gateways.

Where feature and functions are common to both models the product will be refered to as the NB5580/W.

Features and functions dedicated to the NB5580W - Wireless model are shown separately.

Package Contents

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

- NB5580 ADSL Integrated Gateway

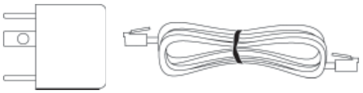
OR

- NB5580W ADSL Integrated Gateway with Wireless with Removable Omni directional 2dBi Antenna

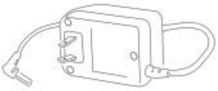
- Package Contents Note and this User Guide

- Cat-5 RJ45 Straight-through Ethernet Cable

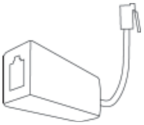
- RJ11 ADSL Line Cord and RJ11 to 605 ADSL Line adaptor



- Plug Pack 12VDC, 1.0A



- Microfilter



- Rubber Feet

Check the contents of your package and, if any parts are missing or damaged, please contact your Dealer.

Default Settings & Facts for the NB5580 & NB5580W

The following lists the default settings of your NetComm NB5580/W.

Note: It is highly recommended that you enable security settings such as WEP, and change default administration passwords and SNMP strings before connecting your NB5580 to your network or the Internet.

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 NB5580/W 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 loose 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.

Note: Both types of reset require the NB5580/W to be powered up before the reset button is pressed.

Power

Ensure that you only use the Power Adaptor supplied (12VDC, 1.0Amps, Center pole positive) with your NetComm NB5580/W.

One page setup for most ADSL services

1. Connect your computer to one of the four LAN ports on the NetComm NB5580/W and ensure you have a link. Connect your ADSL enabled line to the ADSL port of the NetComm NB5580/W using the RJ11 cable supplied.
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 NB5580/W's default IP (192.168.1.1). The main menu of the router should open displaying the **"One Page Setup"**.

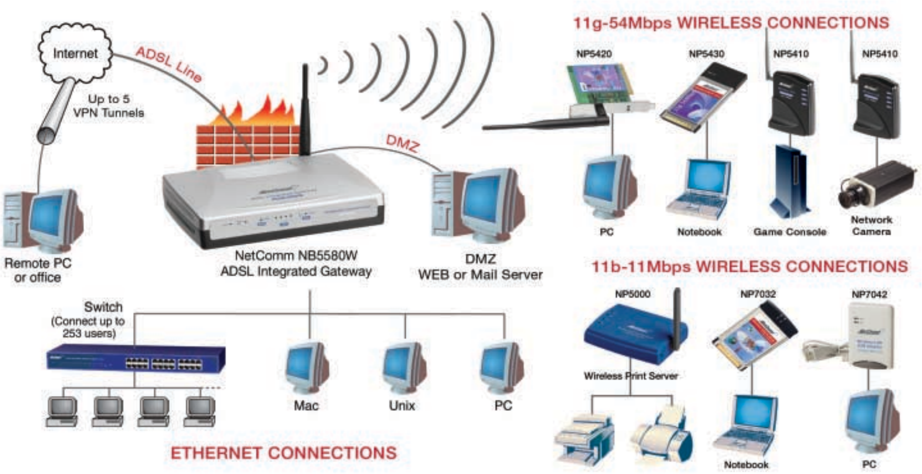
Note: You may be prompted for a log-in, there is no User Name and the default Password is "admin".

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 NB5580/W 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 NB5580/W'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 NB5580/W.

Available in either standard (NB5580) or wireless (NB5580W) models, the NetComm NB5580/W is designed to provide advanced networking security and network resource sharing, with a 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 above diagram shows the NB5580W (Wireless Model).

The wireless model (NB5580W) also provides an integrated 802.11g wireless AP thereby expanding your network to include your Wireless LAN (WLAN).

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 NB5580/W 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 NB5580/W is equipped with a 4-port 10M/100Mbps auto-sensing switch, dedicating a possible100Mbps to each and every ethernet connected computer.

With a web-based UI (User Interface), this NetComm NB5580/W 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 NB5580/W. 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 NB5580/W.

Chapter 1: Get to know your NetComm NB5580/W

This chapter describes the package contents and provides a list of features of the NetComm NB5580/W.

Chapter 2: Hardware Installation & Setup

This chapter describes the steps for hardware installation of the NetComm NB5580/W. Please note that there are separate instructions for both the NB5580 and the NB5580W.

Chapter 3: Internet Access

This chapter describes the steps for basic configuration and start up of the NetComm NB5580/W.

Chapter 4: Advanced Applications

This chapter describes how to configure advanced functions in order to get the most from your NetComm NB5580/W.

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: Security

This chapter is provides guidelines to secure your network.

Chapter 8: Trouble Shooting

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

Chapter 1: Getting to know your NetComm NB5580/W

This chapter describes the package contents and provides a list of features of the NetComm NB5580/W.

1-1 About NetComm NB5580/W

The NetComm NB5580/W combines an ADSL Modem with a Router, including an Active Firewall and VPN security. There are two versions of this product;

- **NB5580** (ADSL modem / Router / Firewall / VPN)
- **NB5580W** (ADSL modem / Router / Firewall / VPN / Wireless Access Point)

All computers (whether connected wirelessly or via Ethernet) can seamlessly share one ADSL internet account as well as share data (Files, Printers and other network services) between themselves locally or to a remote office / user (via a VPN tunnel).

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 (only applicable for the wireless model - NB5580W)

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 NB5580W 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 Features of the NetComm NB5580/W

Standard Features of the NB5580 & NB5580W

- Integrated ADSL Modem supports - Auto, G.DMT, G.LITE, ANSI T1.413
- Supports PPPoE, PPPoA, Static & Dynamic IP, Classical IP & Bridge using LLC Encapsulation.
- Active Firewall featuring Stateful Packet Inspection (SPI) and prevention of DoS attack
- Network Address Translation (NAT max 1000 simultaneous connections)
- 5 Integrated VPN Tunnel End points.
- Multi-session VPN Pass-through or NATTraversal (PPTP & IPSec)
- Universal Plug and Play - allows Internet Apps to auto configure ports
- Ping Diagnostics (LAN & WAN)
- Trace Route Diagnostics
- Back up & Restore Configuration
- Intruder detection, Traffic & Event Logging - viewable Online.
- Logging / Alarms can be sent to Syslog or Email server.
- Access Control - filter by IP / MAC / URL keyword
- Access Control - filter Proxy / Java / ActiveX / Cookie.
- Access Control - Time of Day filter with exception IP address.
- Dynamic DNS for hosting server on Dynamic Public IP address.
- DHCP Server for LAN
- DNS Relay / Forwarding
- Port Range Forwarding (Virtual Server)
- Port Triggering (Special Applications like P2P programs)
- Demilitarised Zone Host (DMZ) & Multi DMZ for hosting Web/Mail servers
- Web Based configuration and Administration
- Remote Internet Administration (changeable HTTP Port Number)
- SNMP support (4 communities, Enable / Disable)
- Dynamic Routing (RIP 1 & 2, independently control Tx/Rx)
- Static Routing (editable DEST, MASK, GW, HOP, IF)
- Flash Firmware Upgradeable
- 4 Port Ethernet Switch on LAN side.
- WAN MAC spoofing (change WAN MAC)
- WAN MTU value setting.
- 3 YEAR WARRANTY

Extra Features of the NB5580W (Wireless version)

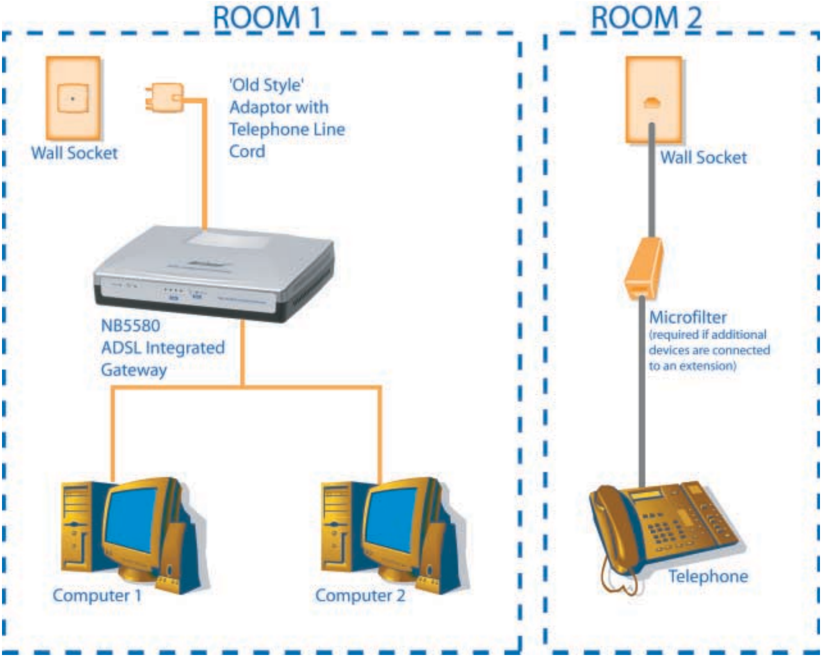
- Integrated 54Mbps Wireless Access Point (802.11g/b compatible)
- Wireless Encryption - WEP 64bit & 128bit, upgradeable to WPA.
- SSID Wireless Beacon - Enable / Disable.
- Wireless Access Control - up to 64 allowed MACs

1-3 Do I need a Micro filter?

Micro filters are used to prevent common telephone equipment, such as phones, answering machines and fax machines, from interfering with your ADSL service. If your ADSL enabled phone line is being used with any other equipment other than your ADSL Modem then you will need to use one Micro filter for each phone device.

Splitters may be installed when your ADSL line is installed or when your current phone line is upgraded to ADSL. If your telephone line is already split you will not need to use a Microfilter - check with your ADSL service provider if you are unsure.

Each micro filter is connected in-line with your telephone or fax machine so that all signals pass through it. Telephones and/or facsimiles in other rooms that are using the same extension will also require Microfilters. The following diagram gives an example of connecting your ADSL Modem/Router using a Microfilter.


ROOM 1
ROOM 2
Wall Socket
'Old Style' Adaptor with Telephone Line Cord
NB5580 ADSL Integrated Gateway
Computer 1
Computer 2
Wall Socket
Microfilter (required if additional devices are connected to an extension)
Telephone

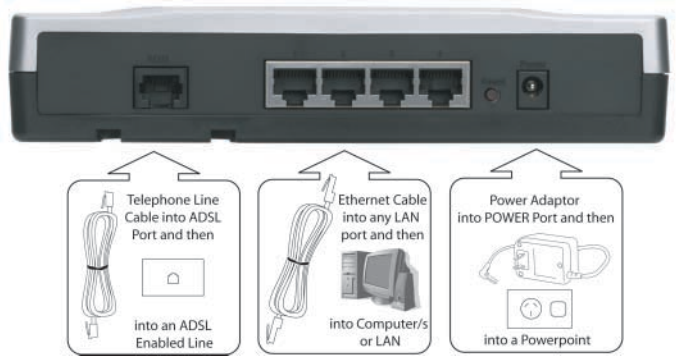
A suitable Microfilter can be purchased from NetComm or your Service Provider, if required. If installing a POTS Splitter, refer to Appendix F: EM1180 ADSL POTS Splitter Installation Guide for more information.

Chapter 2: Hardware Installation & Setup

This chapter provides information about your NetComm NB5580/W's physical features and gives step-by-step installation instructions.

2-1 Connecting your NB5580 to your LAN

Note: It is recommended that you connect your NB5580 to only one computer to configure it BEFORE connecting it to the rest of your network. This will allow you to enable/disable the DHCP server and change other settings that may conflict with exisiting Network devices.


Telephone Line Cable into ADSL Port and then
into an ADSL Enabled Line
Ethernet Cable into any LAN port and then
into Computer/s or LAN
Power Adaptor into POWER Port and then
into a Powerpoint

If using the NB5580 as a desktop unit, fix the Rubber Feet provided.

Plug the Power pack into a power point and into the power socket of the NB5580.

Connect your ADSL line (Telephone line) into the ADSL socket of the NB5580.

Note: If your telephone line has an ADSL splitter installed you must connect the NB5580 to the line/wall socket designated for ADSL use. If your Telephone line does not have an ADSL splitter you must connect Microfilters in-line with each telephone device you intend to use on the Telephone line. See the Section on ADSL Filters / Splitters in the Appendix of this manual.

Connect your computers (with Network Interfaces) to any of the four Ethernet LAN sockets on the back of the NB5580. If you wish to connect more than four computers you should connect one of the LAN sockets to your Network Hub or Switch. Check that the Ethernet sockets used have their respective LAN link lights on.

Note: Auto MDI is available on all four ports. A special cross over cable or "uplink" port to join the router to another hub or switch is not required as the NB5580 ports are self adjusting.

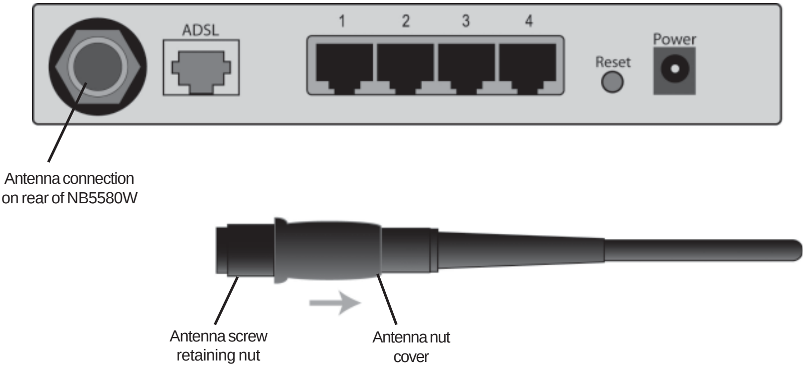
You should now be able to access and configure the NB5580/W via a web browser. See the Configuration section of this manual for more information.

2-2 Connecting your NB5580W to your LAN

***Note:** It is recommended that you connect your NB5580W to only one computer to configure it BEFORE connecting it to the rest of your network. This will allow you to enable/disable the DHCP server and change other settings that may conflict with exisiting Network devices. It is also recommended that you disable the Wireless function (NB5580W only)*

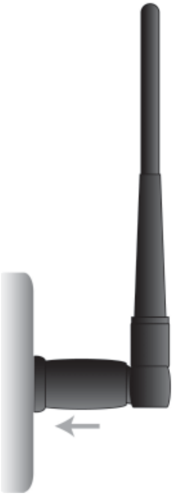
Connecting the Antenna

Pull back the Antenna nut cover to reveal the screw retaining nut. Place the screw retaining nut over the antenna connection on the rear of the NB5580W and turn it clockwise.


ADSL
1
2
3
4
Reset
Power
Antenna connection on rear of NB5580W
Antenna screw retaining nut
Antenna nut cover

***Note:** Do not over-tighten the attaching nut - but do make sure that you have screwed it all the way to its end. Once completed slide the black screw nut cover completly over the retaining nut before trying to bend the antenna to 90 degrees.*

Return the cover and bend the antenna to a 90º angle.

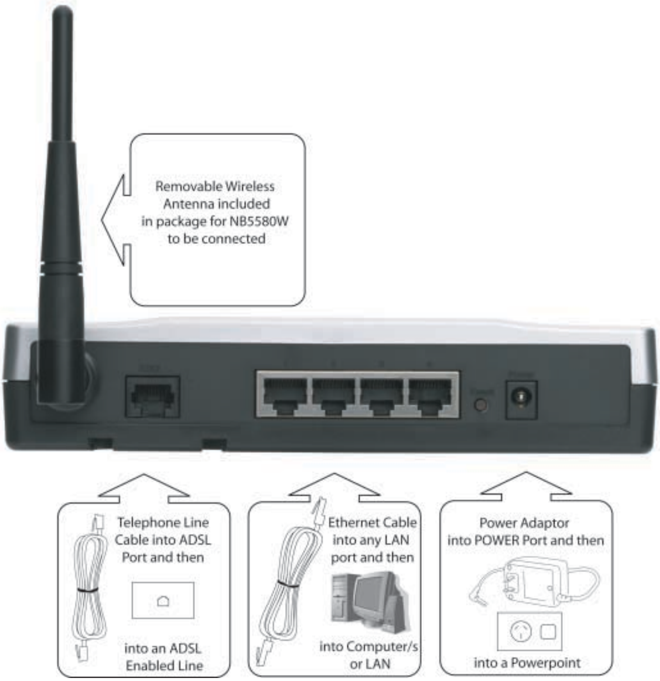


***Note:** Please note that you may have to rotate the complete antenna assembly to do this and have the antenna pointing vertically.*

If using the NB5580W as a desktop unit, fix the Rubber Feet provided.

Plug the Power pack into a power point and into the power socket of the NB5580W.

Connect your ADSL line (Telephone line) into the ADSL socket of the NB5580W.


Removable Wireless Antenna included in package for NB5580W to be connected
Telephone Line Cable into ADSL Port and then
into an ADSL Enabled Line
Ethernet Cable into any LAN port and then
into Computer/s or LAN
Power Adaptor into POWER Port and then
into a Powerpoint

***Note:** If your telephone line has an ADSL splitter installed you must connect the NB5580W to the line/wall socket designated for ADSL use. If your Telephone line does not have an ADSL splitter you must connect Microfilters in-line with each telephone device you intend to use on the Telephone line. See the Section on ADSL Filters / Splitters in the Appendix of this manual.*

Connect your computers (with Network Interfaces) to any of the four Ethernet LAN sockets on the back of the NB5580W. If you wish to connect more than four computers you should connect one of the LAN sockets to your Network Hub or Switch. Check that the Ethernet sockets used have their respective LAN link lights on.

***Note:** Auto MDI is available on all four ports. A special cross over cable or "uplink" port to join the router to another hub or switch is not required as the NB5580W ports are self adjusting.*

You should now be able to access and configure the NB5580W via a web browser. See the Configuration section of this manual for more information.

2-3 Front Panel LEDs for the NB5580

The following figure shows the front view of the NetComm NB5580.

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

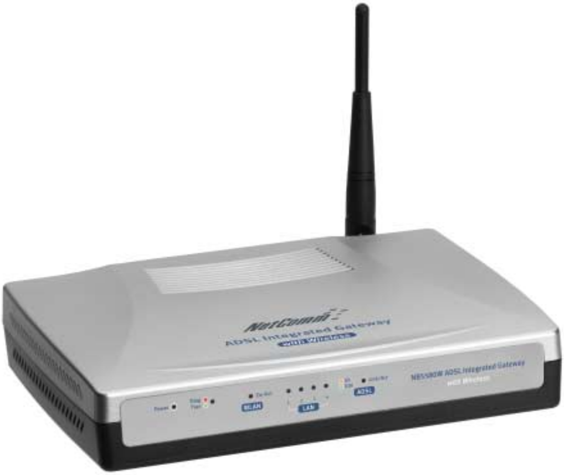
Power:	Green	On when power is on.
Diag:	Red	Lights up during system check when the power is initially connected. If the Router is working properly, the light should switch off after the diagnostic has been completed.

For 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.

2-4 Front Panel LEDs for the NB5580W

The following figure shows the front view of the NetComm NB5580W.



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.

Yellow — On when a successful 10Mbps connection is made through the corresponding port.
Blinking when data is flowing through this port.

Chapter 3: Internet Access

This chapter describes the procedures necessary to configure the basic functions and to start up your NetComm NB5580/W. On successful completion of these procedures, you will be able to access the Internet via your NetComm NB5580/W.

3-1 Prepare your network information

In order to allow a quick reference point when setting up your NetComm NB5580/W, it is suggested you complete the table below with the necessary information, which should be supplied by your ISP:

(✓ tick indicates common minimal requirements)

Host Name: ____

Domain Name: ____

✓ **Public IP address allocation:**

□ DHCP (Obtain IP Address automatically), or

□ Static IP

IP Address (if static): ________.________.________.________

Subnet Mask (if static): ________.________.________.________

Default Gateway (if static): ________.________.________.________

DNS Server Primary: ________.________.________.________

DNS Server Secondary (optional): ________.________.________.________

DNS Server Third (optional): ________.________.________.________

✓ **WAN type:**

□ PPPoE

□ PPPoA

□ Classical IP

□ LLC Encapsulation - Static IP

□ LLC Encapsulation - Dynamic IP

□ Modem / Bridge using LLC Encapsulation

✓ ISP Account Username (if PPPoE/A): ____

✓ ISP Account Password (if PPPoE/A): ____

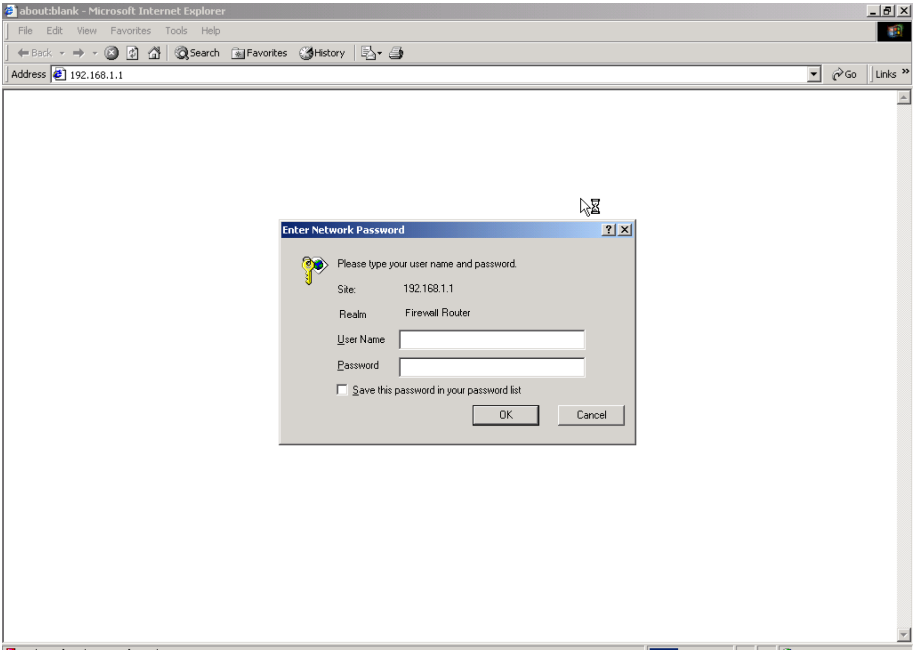
3-2 Web-based User Interface

The NetComm NB5580/W uses a Web based User Interface for configuration, when you have made your changes to a particular page of the configuration you must click "APPLY" at the bottom of that page to save your changes before you go to configuration another page.

To Start configuring your NB5580/W:

Type http://192.168.1.1 into your Web browser (Internet Explorer or Netscape) address field then 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.



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm Firewall Router

User Name

Password

□ Save this password in your password list

about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address 192.168.1.1
Go
Links
OK
Cancel

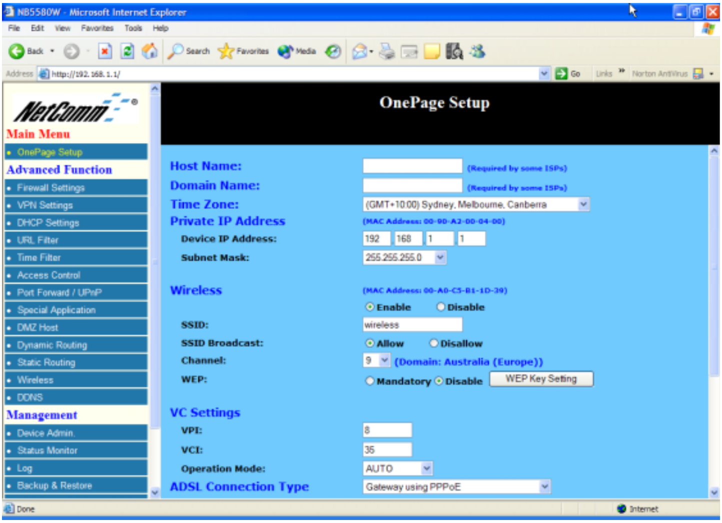
Note: ***This password should be changed via the Administration page immediately. The password can be reset by restoring the factory defaults with the Reset button.***

Settings are successful.

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.

The One-page setup screen is used to configure the most common settings to get your NB5580/W connected to the internet and sharing that connection with your LAN / WLAN. Below is quick list of only the settings which are critical and where you should find the information to correctly configure theses settings:



OnePage Setup

Host Name: (Required by some ISPs)

Domain Name: (Required by some ISPs)

Time Zone: (GMT+10:00) Sydney, Melbourne, Canberra

Private IP Address (MAC Address: 00-90-A2-00-04-00)

Device IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

Wireless (MAC Address: 00-A0-C5-B1-1D-39)

● Enable ○ Disable

SSID: wireless

SSID Broadcast: ● Allow ○ Disallow

Channel: 9 (Domain: Australia (Europe))

WEP: ○ Mandatory ● Disable

VC Settings

VPI: 8

VCI: 35

Operation Mode: AUTO

ADSL Connection Type: Gateway using PPPoE

***Note:** 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.*

Quick Settings to get you started

Private IP address / Device IP address - This is the IP address that will be used to configure the NB5580/W and it is also the IP address that your Computers will use as there Gateway IP address to access the Internet through the NB5580/W. Your Network Administrator can advise if this IP address should be changed (i.e. if the default 192.168.1.1 is already used)

Subnet Mask - This is the subnet mask that accompanies the Device IP address. Your Network Administrator can advise if this IP address should be changed but the default of 255.255.255.0 is recommended.

Wireless Enable / Disable (NB5580W only) - For security you should Disable the Wireless function before connecting the NB5580W to your network, you can enable the wireless function when you are happy with your wireless security settings.

SSID (NB5580W only) - You should change your SSID to be something unique but non-descript, it can be any name upto 32 characters. This SSID must be choosen for the configuration of any Wireless Clients you wish to connect to the NB5580W.

VC Settings / VPI / VCI - Most typical ADSL services in Australia use VPI = 8 and VCI = 35. Check with your ISP to confirm what values you need to set for your specific ADSL service.

ADSL Connection Type - Most Typical ADSL services in Australia use “Gateway using PPPoE” or “Gateway Using PPPoA”. Check with your ISP to confirm which connection type best suits your ADSL service.

Note: When you have specified the above settings don't forget to click the “Apply” button at the bottom of the page.

Other Less Commonly Used Settings

- **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. This will be used to date stamp you log files.

Wireless (only applicable for the NB5580W)

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.Because the NB5580W is the central point in your Infrastructure mode Wireless Network it is where you decide what will be the network name (SSID) that your Wireless Client adapters must look for or 'lock onto'. When your Wireless Client devices are in Infrastructure mode and come into range of your NB5580W they will look for a matching SSID and change their channel to match the NB5580W if WEP encryption is turned on they will also use their WEP keys to transfer data to and from the NB5580W.

Note: For security it is advised that your SSID be unique but non-descript of your Company or location. i.e. Do not use your Company name or Address as your SSID. Your SSID should be changed from defaults to provide additional security and to prevent conflicts with neighboring WLANs

- **SSID Broadcast (Beacon)** - The NB5580W's built-in Access point broadcasts it's presence to Wireless Client Adapters automatically, this feature can be disabled to assist in hiding your WLAN from the casual browser, however disabling your SSID broadcast does not make your WLAN more secure. NetComm recommend leaving this feature enabled for ease of use.
- **Channel** - Different countries have different numbers of available channels, Your NB5580W is factory set to the Australian (European) domain. Wireless Client adapters that have a matching SSID will automatically match the Channel that you set in your NB5580W. To decide which channel to use in your NB5580 it is recommended that you choose a channel that is not the same or numerically close to any existing or neighboring WLAN channel.
- **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

The ADSL Connection type sets the way your NB5580/W works with the ADSL Service supplied by your ISP. The Most common choice for this setting is either Gateway using PPPoE or Gateway using PPPoA these will work for most ISP's ADSL services and will safely share your Internet access with your LAN:

- Gateway using PPPoE
- Gateway using PPPoA
- Gateway using Classical IP
- Gateway using LLC Encaps. (Dynamic IP)
- Gateway using LLC Encaps. (Static IP)
- Router using Classical IP
- Modem using LLC Encaps.

Gateway, *Router* and *Modem* are different *working modes* that the NetComm NB5580/W can use. It is highly recommended that you use the Gateway mode, which is NAT enabled. It not only allows LAN users to share a single IP Address, but also protects your LAN network from outside intruders. If the NetComm NB5580/W is set to the Router mode or the Modem mode, all the computers in the LAN will have to be assigned fixed public IP Addresses. The Router mode allows users to specify which routing path data packets should take. If using the Modem mode, most functions of the NB5580/W are not used and you will need to use a second router or computer to authenticate your ISP account.

LLC Encaps, *Classical IP*, *PPPoE*, and *PPPoA* are *connection modes* that use different protocols to create the initial session between your NetComm NB5580/W and ISP’s equipment. Your ISP may indicate the connection mode you should set. If you don’t know which one to choose, connect your ISP to get this information.

Gateway using PPPOE

Choose this setting if:

1. You want to employ NAT to share Internet access for all of your computers, as well as protect them from outside intruders.
2. Your ISP uses PPPoE as connection mode. You can find more information in the RFC 2516 standard.

- **User Name** Enter the user name your ISP provide to you.
- **Password** Enter the password your ISP provide to you.
- **Connect-on-demand** Is a utility to trigger the PPPoE session to connect if in a disconnected state when Internet access is being attempted. Select this function and enter the number of minutes you wish to wait after network idle time in the "**Max Idle Time"** location. This function is for PPPoE only.
- **Keep Alive** This function keeps your PPPoE connection always on even during a period of no WAN activity. In some situations the PPPoE session cannot be restored immediately after disconnection because the ISP's system may need time to restore. Check with your ISP to ascertain how much time is required before the router starts to re-build the PPPoE session and enter this into the "**Redial Period**" field.

Gateway using PPPOA

Choose this setting if:

1. You want to employ NAT to share Internet access for all of your computers, as well as protect them from outside intruders.
2. Your ISP uses **PPPoA** as its connection mode. You can find more information in the RFC 2684 standard.

- **User Name** Enter the user name your ISP provide to you.
- **Password** Enter the password your ISP provide to you.
- **Connect-on-demand** Is a utility to trigger the PPPoA session to connect if in a disconnected state when Internet access is being attempted. Select this function and enter the number of minutes you wish to wait after network idle time in the "**Max Idle Time"** location.
- **Keep Alive** This function keeps your PPPoA connection always on even it sites idle. However, in some situation, PPPoA session cannot be built immediately after disconnection because the system on ISP site may need a little time to restore. You may need to check your ISP to get the information that how much time it need to wait before the router start to re-build the PPPoE session and fill it in the "**Redial Period**".

Gateway using Classical IP

Choose this setting to meet the following conditions:

1. You want to employ NAT to share Internet access for all of your computers, as well as protect them from outside intruders.
2. Your ISP uses **Classical IP** connection type (use LLC encapsulation and routing protocol) and provides you with one or more IP addresses when you apply for the service. You can find more information in the RFC 2684 standard.

- **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.

Gateway using LLC Encaps. (Dynamic IP)

This connection type is the default setting of the NetComm NB5580/W. Choose this setting if:

1. You want to employ NAT to share Internet access for all of your computers, as well as protect them for outside intruders.
2. Your ISP uses LLC Encapsulation and DHCP to assign IP addresses when you connect. (LLC encapsulation allows multiplexing of multiple protocols over a single ATM virtual connection (VC). You can find more information in the RFC 2684 standard.)

Gateway using LLC Encaps. (Static IP)

Choose this setting according if :

1. You want to employ NAT to share Internet access for all of your computers, as well as protect them for outside intruders.
2. Your ISP uses LLC Encapsulation and provides you with one or more IP addresses when you apply for the service. You can find more information in the RFC 2684 standard.

- **Specify WAN IP Address** Enter one 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.

Router using Classical IP

Choose this setting if:

1. You want this device acting as a router without NAT function.
2. Your ISP uses **Classical IP** connection type (use LLC encapsulation and routing protocol) and provides you one or more IP addresses when you apply for the service. You can find more information in the RFC 2684 standard.

- **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.

Note: You have to set public IP address for each of your LAN computers if you select this connection type.

Modem using LLC Encaps.

Choose this setting if:

1. You want this device acting as an ADSL modem. (i.e. when being plugged into another broadband router or a computer running your ISP's software)
2. Your ISP uses LLC encapsulation.

Your ISP may use DHCP to provide an IP address or provide you one or more IP addresses, as well as advising you to use PPPoA or PPPoE connection modes.

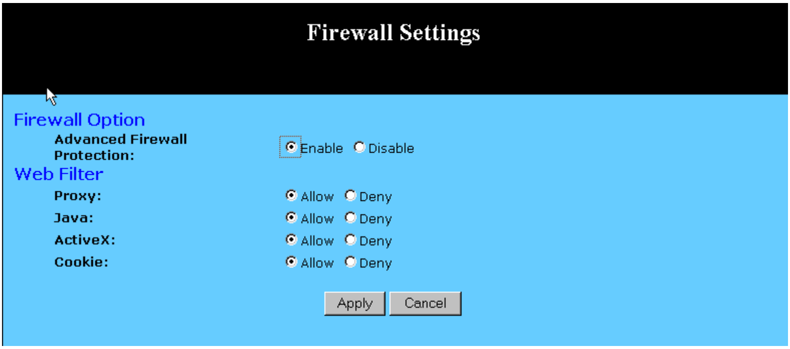
When you have properly configured the Setup page, click "**Apply**". Your Router will then attempt to connect to the Internet. If you experience problems, please refer to the trouble shooting section before contacting NetComm Technical Support.

Chapter 4: Advanced Applications

This chapter provides information on how to set up and use the advanced features of your NetComm NB5580/W.

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 Settings

Firewall Option

Advanced Firewall Protection: ● Enable ○ Disable

Web Filter

Proxy: ● Allow ○ Deny

Java: ● Allow ○ Deny

ActiveX: ● Allow ○ Deny

Cookie: ● Allow ○ Deny

- **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. When the firewall is enabled it will block against the following attacks:
  - DoS
  - DDoS
  - Ping of Death
  - LAND
  - IP Spoofing
  - SYN Slug
  - IP Smurfing

  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 NB5580/W to block the access of 216.115.102.76 that is the IP address of www.yahoo.com, it will fail to block successfully 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.

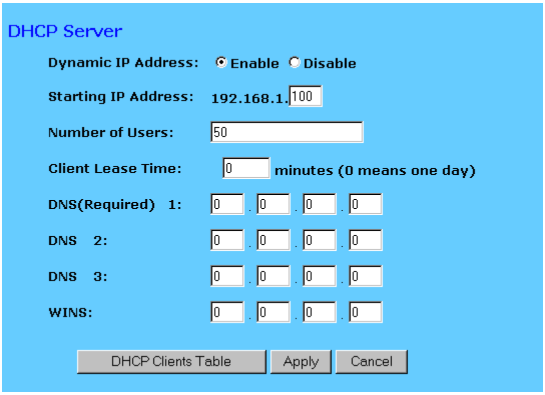
Java & **Active X** are programming languages for web pages. However, some Trojan programs are also written in these programming languages. If you deny either of these, you may not be able to access some parts of web sites.

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.



DHCP Server

Dynamic IP Address: ● Enable ○ Disable

Starting IP Address: 192.168.1.100

Number of Users: 50

Client Lease Time: 0 minutes (0 means one day)

DNS(Required) 1: 0 . 0 . 0 . 0

DNS 2: 0 . 0 . 0 . 0

DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

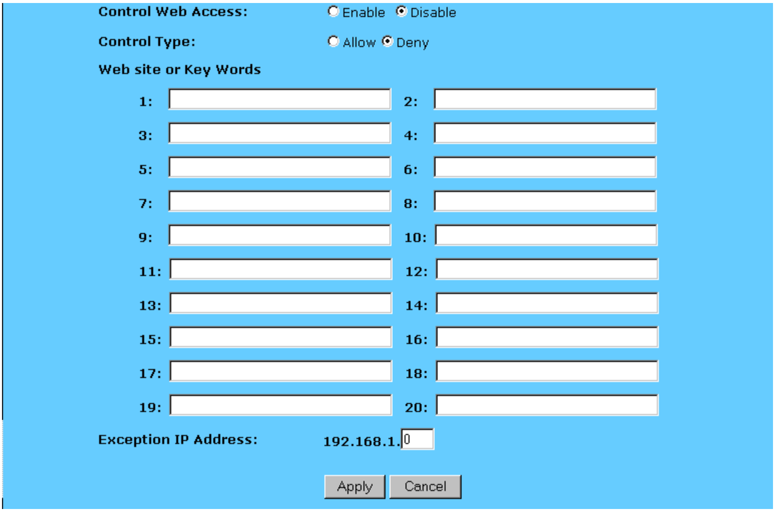
Note: The DHCP Server can support a maximum pool of 253 IP Addresses.

- **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 used in most cases.
- **DHCP Clients Table** Click the DHCP Clients Table button to show current DHCP client information. Such as what IP addresses are already being used, etc.

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

4-3 URL Filter

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: ○ Enable ● Disable

Control Type: ○ Allow ● Deny

Web site or Key Words

1:		2:	
3:		4:	
5:		6:	
7:		8:	
9:		10:	
11:		12:	
13:		14:	
15:		16:	
17:		18:	
19:		20:	

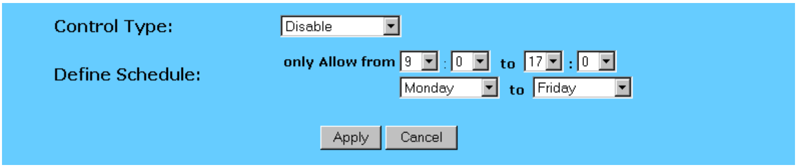
Exception IP Address: 192.168.1.0

- **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 only specific websites listed. In contrast, to restrict users on the network to access the websites listed, check "Deny" 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 the URL Filter.

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

4-4 Time Control

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



Control Type: Disable

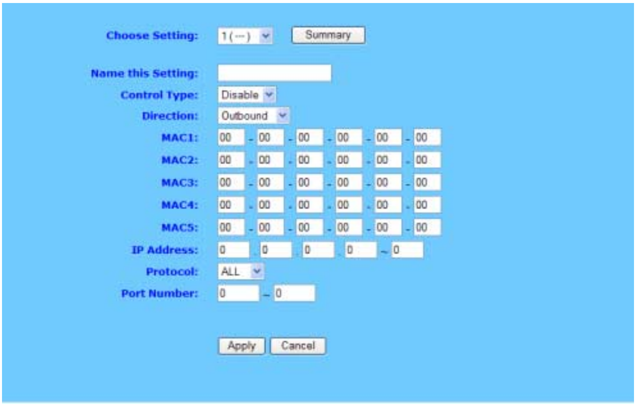
Define Schedule: only Allow from 9 : 0 to 17 : 0
Monday to Friday

- **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 Port Forwards (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.



Choose Setting: 1 (---)
Name this Setting:
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

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.

- **Choose Setting** 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.
- **Control Type** Select "Enable" to limit users/computers access to specific applications you set on this rule. Select "Disable" to restrict the users/computers access to specific applications you set on this rule.
- **Name this Setting** 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: 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.

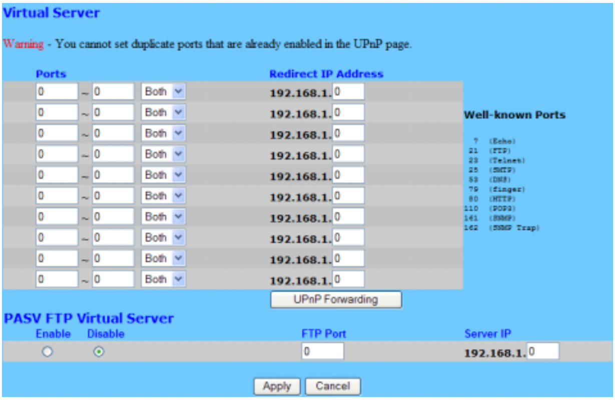
Click the "**Apply**" button after making any changes, or click the "**Cancel**" button to exit the screen without saving any changes.

Note: To allow or deny access by URL, refer to the section on URL Filter.

4-6 Port Forwarding / UPnP 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 NB5580/W 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.

Note: Please refer to section 4-17 Universal Plug'n'Play for alternatives to Port Forwarding



Virtual Server

Warning - You cannot set duplicate ports that are already enabled in the UPnP page.

Ports				Redirect IP Address
0	~	0	Both	192.168.1. 0
0	~	0	Both	192.168.1. 0
0	~	0	Both	192.168.1. 0
0	~	0	Both	192.168.1. 0
0	~	0	Both	192.168.1. 0
0	~	0	Both	192.168.1. 0
0	~	0	Both	192.168.1. 0
0	~	0	Both	192.168.1. 0
0	~	0	Both	192.168.1. 0
0	~	0	Both	192.168.1. 0

Well-known Ports

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

PASV FTP Virtual Server

Enable	Disable	FTP Port	Server IP
○	●	0	192.168.1. 0

Note: Your NetComm NB5580/W 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 NB5580/W'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.***

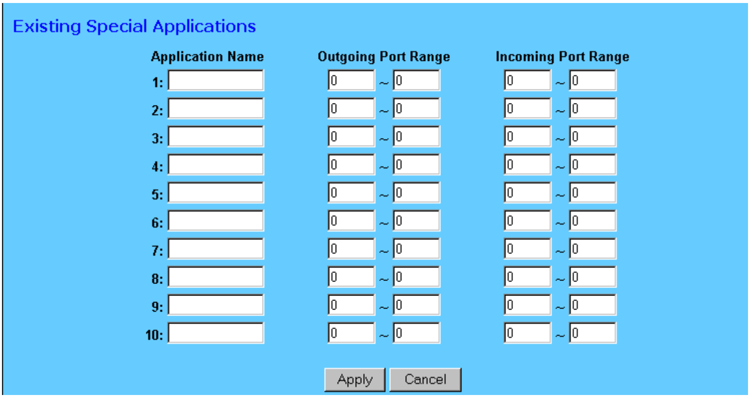
The following table lists the protocols and port ranges that are used by some common applications:

Note: Port 8080 on the Public IP address is typically used for Remote Management and must be change in the Admin Page if you wish to use this port for another service

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) ”C:\Program Files\Quake III Arena\quake3.exe” +set net_port 27660 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:		0 ~ 0	0 ~ 0
2:		0 ~ 0	0 ~ 0
3:		0 ~ 0	0 ~ 0
4:		0 ~ 0	0 ~ 0
5:		0 ~ 0	0 ~ 0
6:		0 ~ 0	0 ~ 0
7:		0 ~ 0	0 ~ 0
8:		0 ~ 0	0 ~ 0
9:		0 ~ 0	0 ~ 0
10:		0 ~ 0	0 ~ 0

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 NB5580/W 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 NB5580/W.
- **Incoming Control** Enter the port number or range of numbers the inbound packets carry.

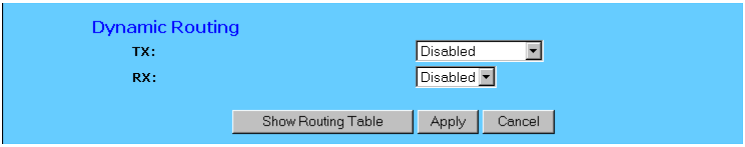
Click "**Apply**" after making any changes.

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 NB5580/W to exchange routing information with other routers in the network. Enabling this feature is likely to enhance performance of your NetComm NB5580/W when used in a multi routed network.



Dynamic Routing

TX: Disabled

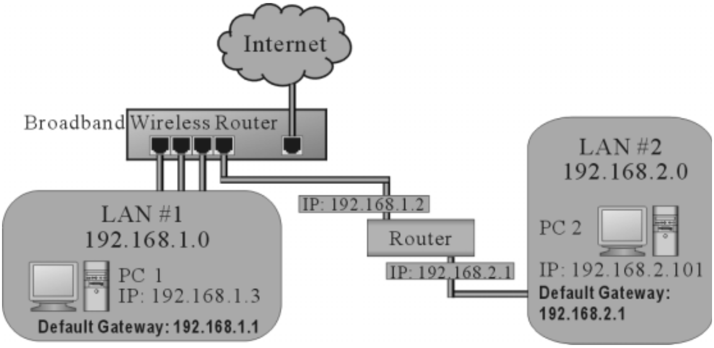
RX: Disabled

- **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.

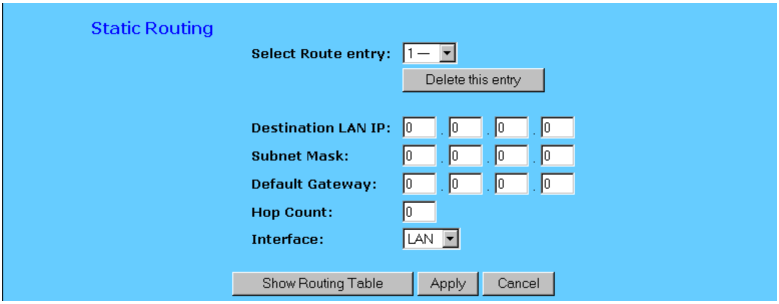
Click **“Apply”** after making any changes.

4-9 Static Routing

The Static Routing feature allows computers that are connected to the NetComm NB5580/W 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 NB5580/W through another router (destination LAN). Up to 20 route entries may be entered into the NetComm NB5580/W. 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 NB5580/W via another router while PC1 in LAN#1 is connected to the NetComm NB5580/W directly. Without configuring the Static Routing function, the two computers would not be able to communicate with each other.


Static Routing

Select Route entry: 1 —

Destination LAN IP: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Default Gateway: 0 . 0 . 0 . 0

Hop Count: 0

Interface: LAN

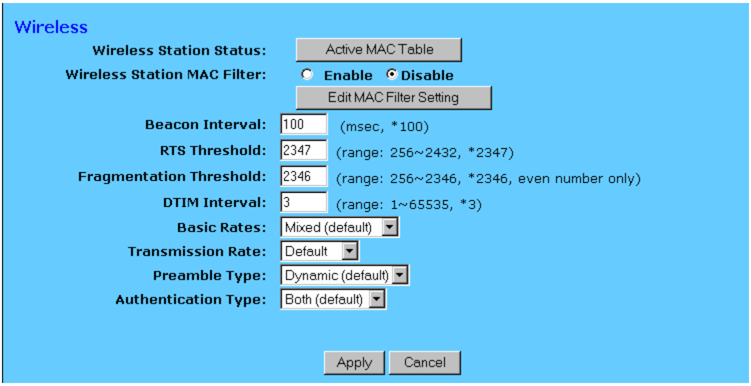
- **Select Route entry** Select the route entry number from 1 to 20 that you wish to configure.
- **Destination LAN IP** and **Subnet Mask** Enter the IP Address and Subnet Mask of the destination LAN that the immediate LAN is to communicate with. Taking the above diagram as an example, enter ***192.168.2.0*** 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 (only applicable for the NB5580W)

This setting page allows you to configure advanced wireless functions of your NB5580W. 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

Wireless Station Status:

Wireless Station MAC Filter: ○ Enable ● Disable

Beacon Interval: 100 (msec, *100)

RTS Threshold: 2347 (range: 256~2432, *2347)

Fragmentation Threshold: 2346 (range: 256~2346, *2346, even number only)

DTIM Interval: 3 (range: 1~65535, *3)

Basic Rates: Mixed (default)

Transmission Rate: Default

Preamble Type: Dynamic (default)

Authentication Type: Both (default)

- **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.

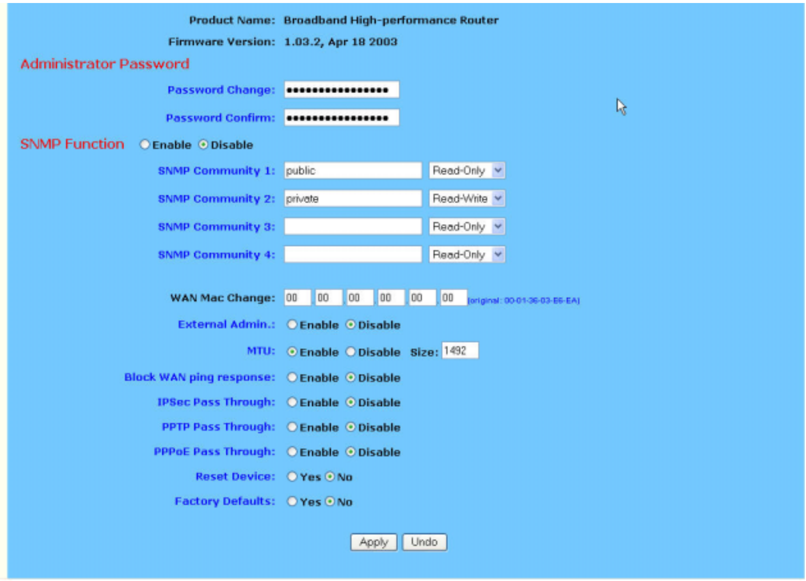
- **RTS Threshold** RTS packet is use to account for potential hidden stations. This feature allows you to set the size of RTS packet.

- **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 NB5580/W

This feature allows the administrator to manage the NetComm NB5580/W 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 NB5580/W. If the **“Password”** is left blank, all users on your LAN/WLAN can access the router simply by entering the unit’s IP Address into their web browser’s location window.



Product Name: Broadband High-performance Router

Firmware Version: 1.03.2, Apr 18 2003

Administrator Password

Password Change: ••••••••••••••••

Password Confirm: ••••••••••••••••

SNMP Function ○ Enable ● Disable

SNMP Community 1: public Read-Only

SNMP Community 2: private Read-Write

SNMP Community 3: Read-Only

SNMP Community 4: Read-Only

WAN Mac Change: 00 00 00 00 00 00 (original: 00-01-36-03-E6-EA)

External Admin.: ○ Enable ● Disable

MTU: ● Enable ○ Disable Size: 1492

Block WAN ping response: ○ Enable ● Disable

IPSec Pass Through: ○ Enable ● Disable

PPTP Pass Through: ○ Enable ● Disable

PPPoE Pass Through: ○ Enable ● Disable

Reset Device: ○ Yes ● No

Factory Defaults: ○ Yes ● No

- **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 funcitonality 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 NB5580/W 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.

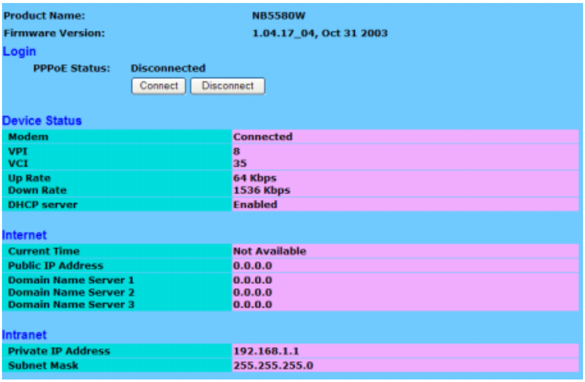
- **MTU** Check **“Enable”** if you want to limit the incoming and outgoing packet size for the router. Enter the maximum packet size you wish to set in the **“Size”** column. This can assist with the transmission of emails with attachments, etc.
- **Block WAN ping response** This option is enabled by 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.



Product Name: NB5580W

Firmware Version: 1.04.17_04, Oct 31 2003

Login

PPPoE Status: Disconnected

Device Status

Modem	Connected
VPI VCI	8 35
Up Rate Down Rate	64 Kbps 1536 Kbps
DHCP server	Enabled

Internet

Current Time	Not Available
Public IP Address	0.0.0.0
Domain Name Server 1 Domain Name Server 2 Domain Name Server 3	0.0.0.0 0.0.0.0 0.0.0.0

Intranet

Private IP Address	192.168.1.1
Subnet Mask	255.255.255.0

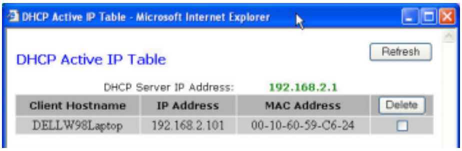
- **Login** This column shows the login information of your WAN connection. You can manually initiate a connection or a disconnection by clicking the buttons. However, if you initiate a disconnection here, the "**Connect-on-Demand**" will not function until the connection button is clicked. Note that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

  DHCP Release: Click this button to 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 - Microsoft Internet Explorer

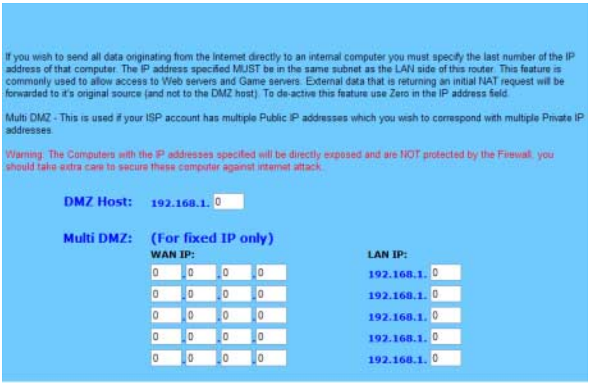
DHCP Active IP Table

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	□

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.



If you wish to send all data originating from the Internet directly to an internal computer you must specify the last number of the IP address of that computer. The IP address specified MUST be in the same subnet as the LAN side of this router. This feature is commonly used to allow access to Web servers and Game servers. External data that is returning an initial NAT request will be forwarded to it's original source (and not to the DMZ host). To de-active this feature use Zero in the IP address field.

Multi DMZ - This is used if your ISP account has multiple Public IP addresses which you wish to correspond with multiple Private IP addresses.

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 computer against internet attack.

DMZ Host: 192.168.1. 0

Multi DMZ: (For fixed IP only)

WAN IP:	LAN IP:
0 . 0 . 0 . 0	192.168.1. 0
0 . 0 . 0 . 0	192.168.1. 0
0 . 0 . 0 . 0	192.168.1. 0
0 . 0 . 0 . 0	192.168.1. 0
0 . 0 . 0 . 0	192.168.1. 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 you 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.

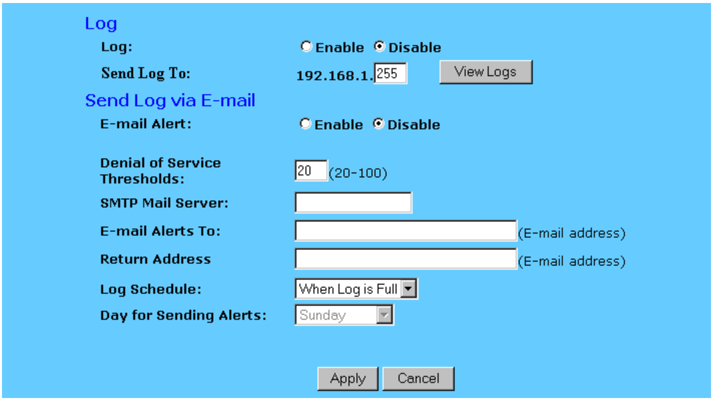
Multi DMZ

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: When Log is Full

Day for Sending Alerts: Sunday

- **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 to** 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.

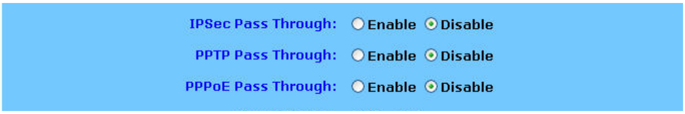
  Weekly The alert e-mail will be sent by each week. When this item is select.
- Day of Sending Alert When "Weekly" is selected as Log Schedule, you can select which day in a week to send the alert e-mail.

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).



IPSec Pass Through: ○ Enable ● Disable

PPTP Pass Through: ○ Enable ● Disable

PPPoE Pass Through: ○ Enable ● Disable

The NetComm NB5580/W 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.

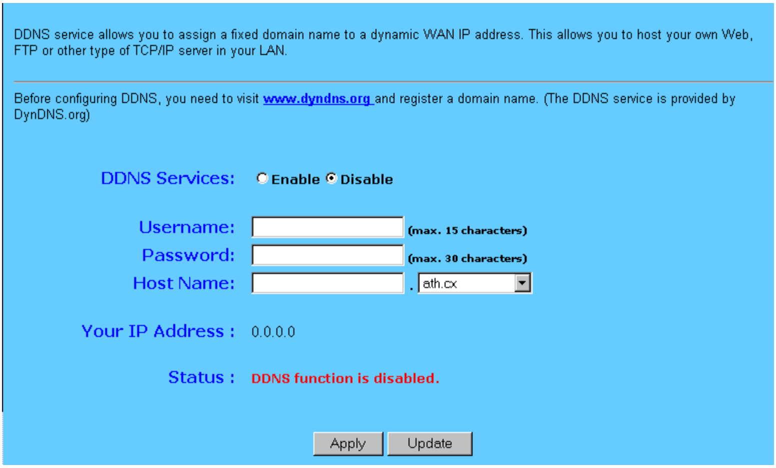
4-16 Dynamic DNS (DDNS)

"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

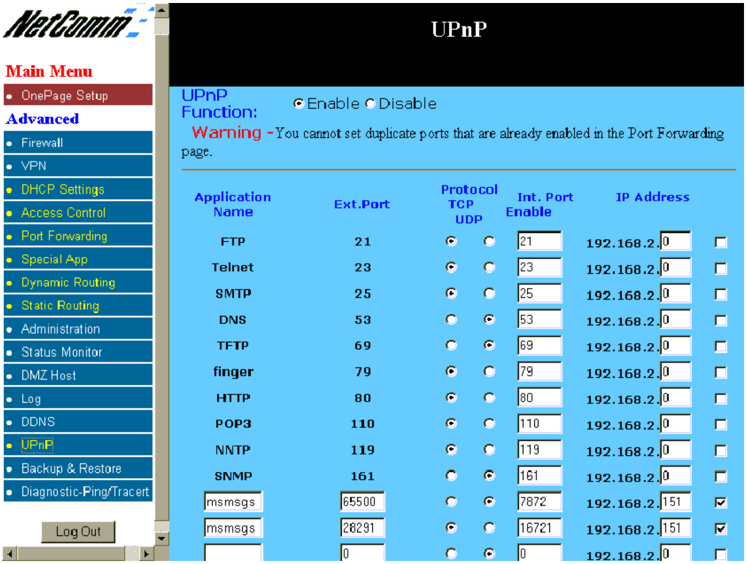
Universal Plug and Play is a system designed to make computers, computer equipment and home appliances work together seamlessly. Currently the biggest advantage of having UPnP integrated into your router is that this will assist your router in allowing complex Internet applications such as MSN Messenger© 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.*



UPnP

UPnP Function: ● Enable ○ Disable

Warning - You cannot set duplicate ports that are already enabled in the Port Forwarding page.

Application Name	Ext.Port	Protocol TCP	Protocol UDP	Int. Port	IP Address	Enable
FTP	21	●	○	21	192.168.2.0	□
Telnet	23	●	○	23	192.168.2.0	□
SMTP	25	●	○	25	192.168.2.0	□
DNS	53	○	●	53	192.168.2.0	□
TFTP	69	○	●	69	192.168.2.0	□
finger	79	●	○	79	192.168.2.0	□
HTTP	80	●	○	80	192.168.2.0	□
POP3	110	●	○	110	192.168.2.0	□
NNTP	119	●	○	119	192.168.2.0	□
SNMP	161	○	●	161	192.168.2.0	□
msmsgs	65500	○	●	7872	192.168.2.151	☑
msmsgs	28291	●	○	16721	192.168.2.151	☑
	0	○	●	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.

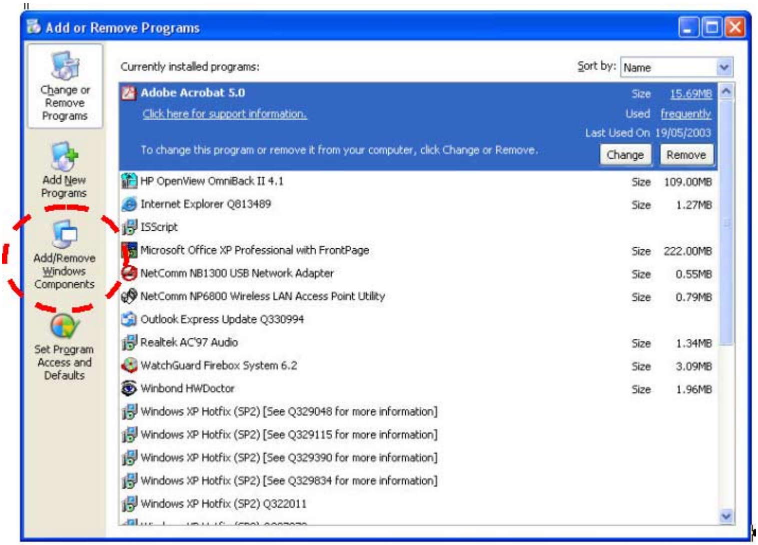
Adding UPnP to Windows XP

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.

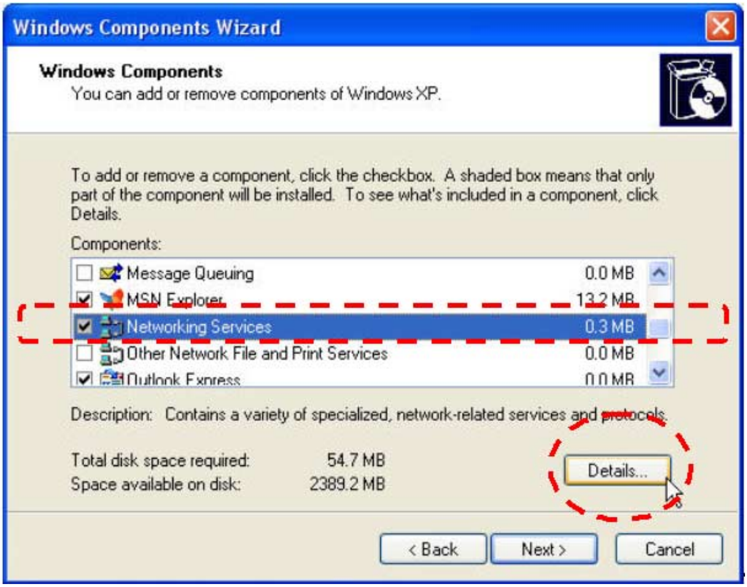

Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
Change
Remove

Currently installed programs: Sort by: Name

Adobe Acrobat 5.0 Size 15.69MB
Click here for support information. Used frequently
Last Used On 19/05/2003
To change this program or remove it from your computer, click Change or Remove.

HP OpenView OmniBack II 4.1	Size	109.00MB
Internet Explorer Q813489	Size	1.27MB
ISScript		
Microsoft Office XP Professional with FrontPage	Size	222.00MB
NetComm NB1300 USB Network Adapter	Size	0.55MB
NetComm NP6800 Wireless LAN Access Point Utility	Size	0.79MB
Outlook Express Update Q330994		
Realtek AC'97 Audio	Size	1.34MB
WatchGuard Firebox System 6.2	Size	3.09MB
Winbond HWDoctor	Size	1.96MB
Windows XP Hotfix (SP2) [See Q329048 for more information]		
Windows XP Hotfix (SP2) [See Q329115 for more information]		
Windows XP Hotfix (SP2) [See Q329390 for more information]		
Windows XP Hotfix (SP2) [See Q329834 for more information]		
Windows XP Hotfix (SP2) Q322011		

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



Windows Components Wizard

Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

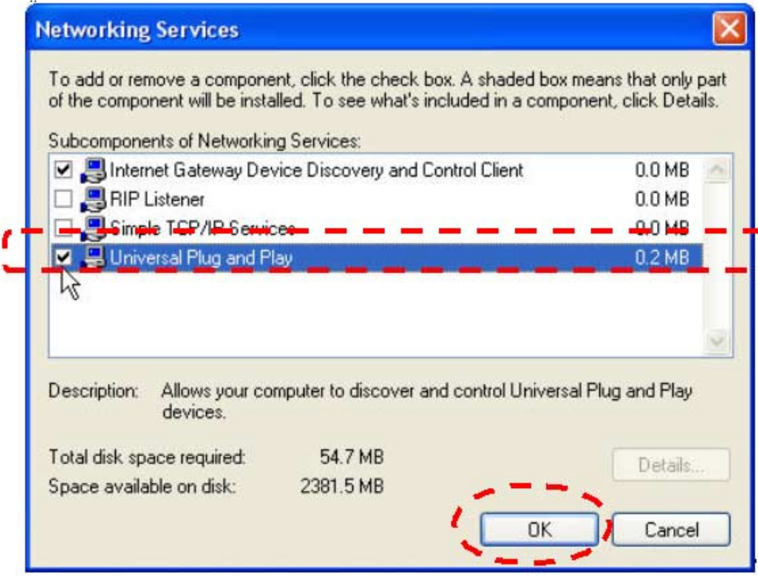
☐	Message Queuing	0.0 MB
☑	MSN Explorer	13.2 MB
☑	Networking Services	0.3 MB
☐	Other Network File and Print Services	0.0 MB
☑	Outlook Express	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 54.7 MB

Space available on disk: 2389.2 MB

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



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

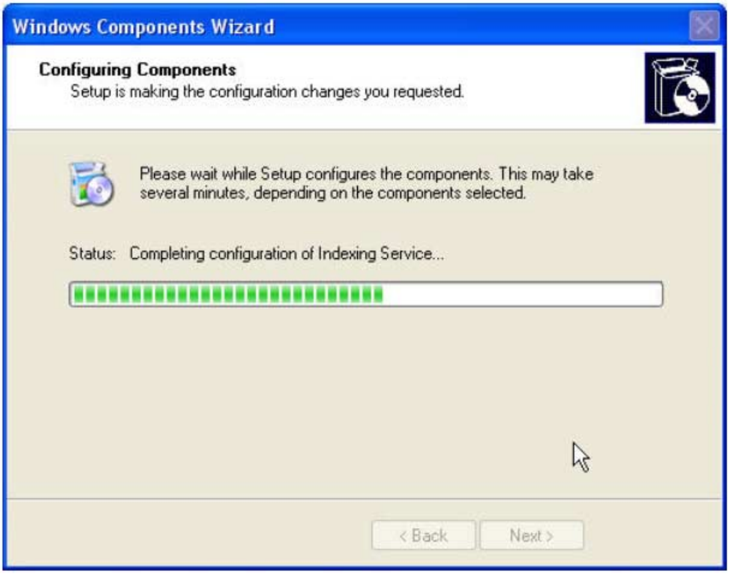
☑	Internet Gateway Device Discovery and Control Client	0.0 MB
☐	RIP Listener	0.0 MB
☐	Simple TCP/IP Services	0.0 MB
☑	Universal Plug and Play	0.2 MB

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 54.7 MB

Space available on disk: 2381.5 MB

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



Windows Components Wizard

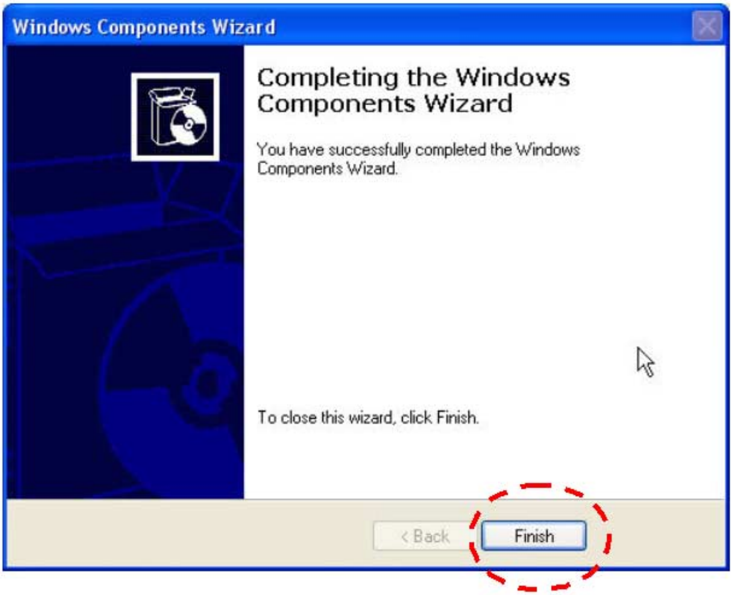
Configuring Components

Setup is making the configuration changes you requested.

Please wait while Setup configures the components. This may take several minutes, depending on the components selected.

Status: Completing configuration of Indexing Service...

6. Click Finish to close the Wizard.



Windows Components Wizard

Completing the Windows Components Wizard

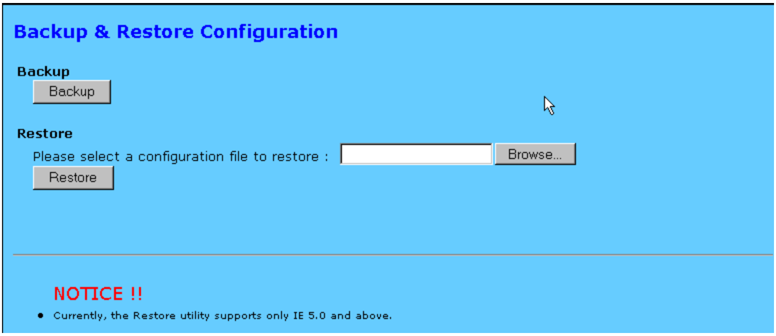
You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

4-18 Back Up and Restore

The NB5580/W 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.***



Backup & Restore Configuration

Backup

Restore

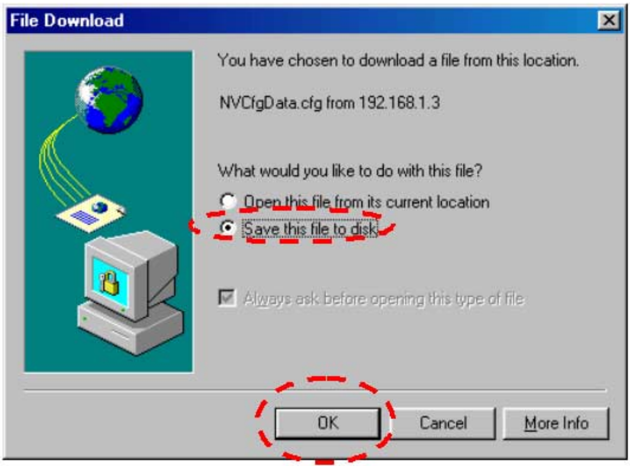
Please select a configuration file to restore :

NOTICE !!

- Currently, the Restore utility supports only IE 5.0 and above.

To Back up your router;

1. Click the Backup button. When the File download window opens select Save this file to disk. Click OK



File Download

You have chosen to download a file from this location.

NVCfgData.cfg from 192.168.1.3

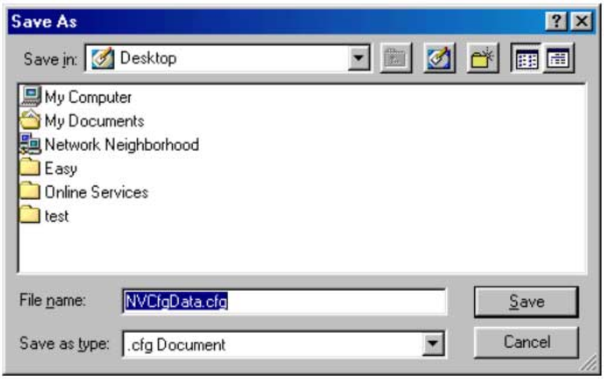
What would you like to do with this file?

○ Open this file from its current location

● Save this file to disk

☑ Always ask before opening this type of file

2. Choose the location where you would like to store the file and enter the file name (leave the .cfg extension). Click Save.



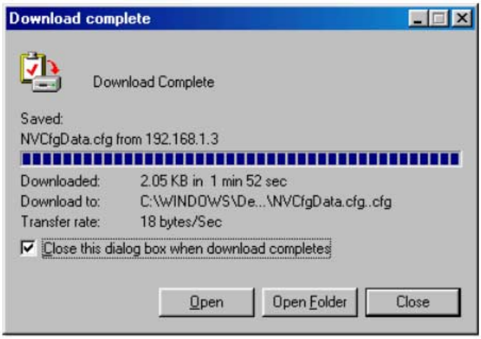
Save As

Save in: Desktop

File name: NVCfgData.cfg

Save as type: .cfg Document

3. If required when the download is complete click the Close button.



Download complete

Download Complete

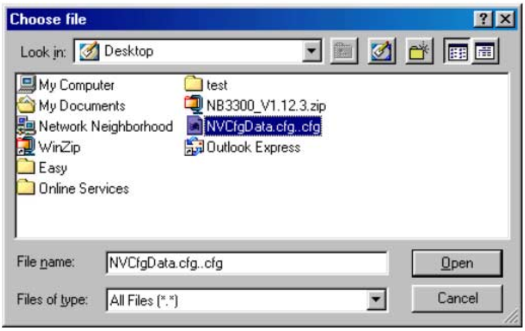
Saved:
NVCfgData.cfg from 192.168.1.3

Downloaded: 2.05 KB in 1 min 52 sec
Download to: C:\WINDOWS\De...\NVCfgData.cfg..cfg
Transfer rate: 18 bytes/Sec

☑ Close this dialog box when download completes

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.



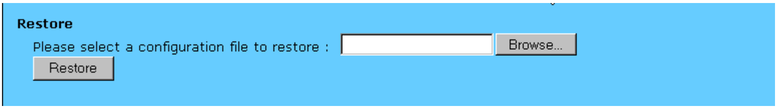
Choose file

Look in: Desktop

File name: NVCfgData.cfg..cfg

Files of type: All Files (*.*)

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.



Restore

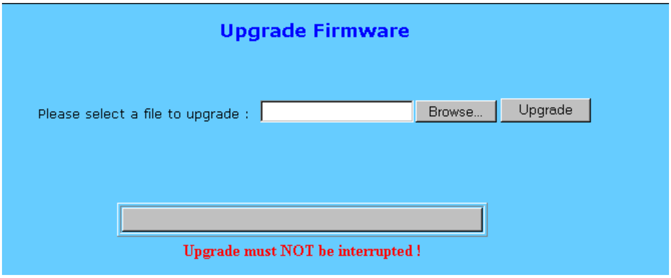
Please select a configuration file to restore :

4. 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.



Upgrade Firmware

Please select a file to upgrade :

Upgrade must NOT be interrupted !

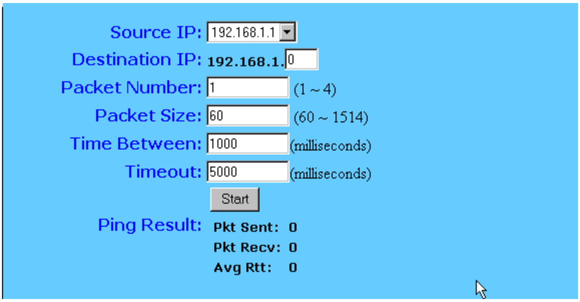
- **Select a file to upgrade** Enter path of the latest firmware you saved on the PC. You can choose "Browsing" to view the folders and select the firmware.
- **Upgrade** After you enter or select the path, click "Upgrade" to proceed firmware upgrade process. Please note that don't power off the router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

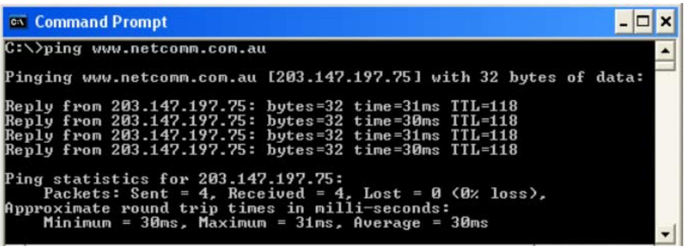
Timeout: 5000 (milliseconds)

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 via another router or modem to obtain a IP number for your router test see the screen shot below;



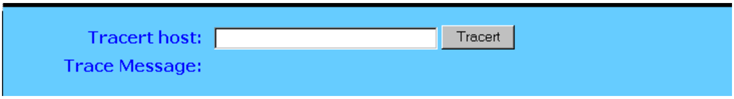
```
C:\>ping www.netcomm.com.au

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)

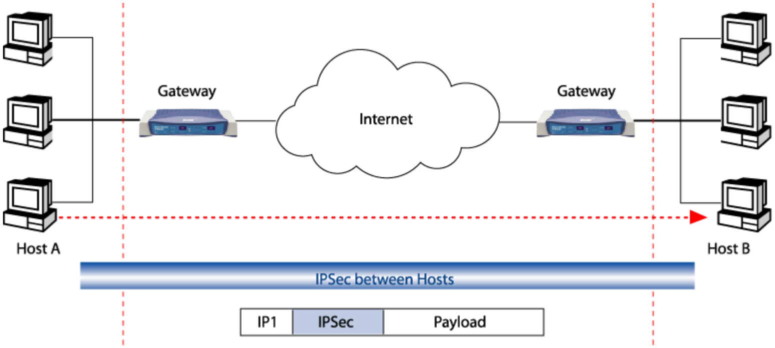
An SA provides data protection for unidirectional traffic as defined in the IPSec protocols. An IPSec tunnel typically consists of two unidirectional SAs, which together provide a protected, full-duplex data channel.

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.

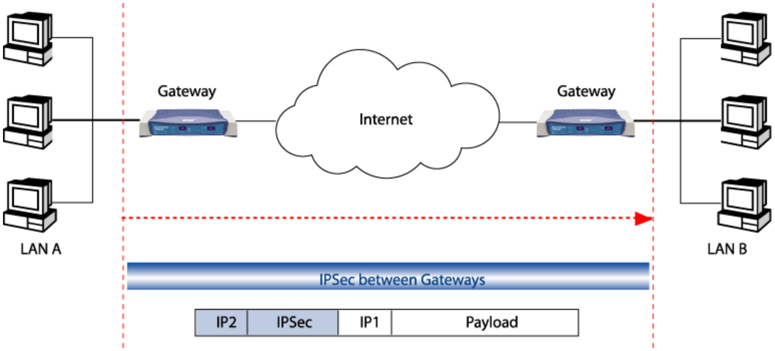
Tunnel Mode



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

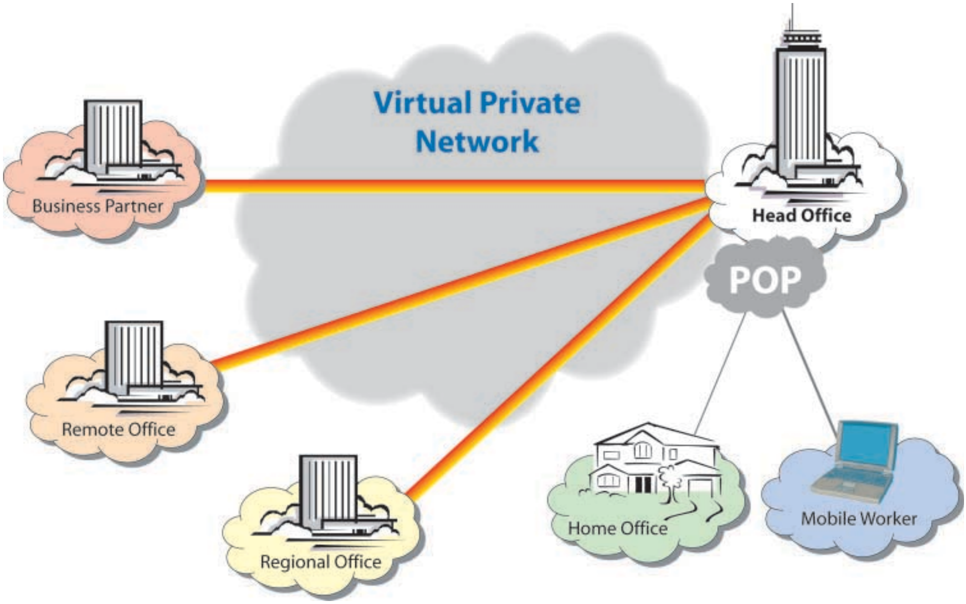


IPSec uses the Internet Key Exchange (IKE) protocol to facilitate and automate the SA setup and the exchange of keys between parties transferring data. IPSec requires that keys be re-created, or refreshed, frequently so that the parties can communicate securely with each other. IKE manages the process 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.

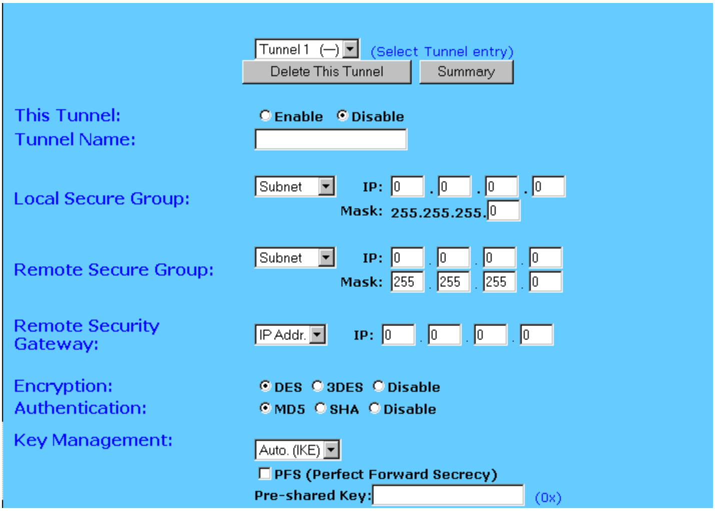
5-2 VPN Application Types

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.



5-3 VPN / IPSec Setup



Tunnel 1 (--) ▾ (Select Tunnel entry)

This Tunnel: ○ Enable ● Disable

Tunnel Name:

Local Secure Group: Subnet ▾ IP: 0 . 0 . 0 . 0 Mask: 255.255.255.0

Remote Secure Group: Subnet ▾ IP: 0 . 0 . 0 . 0 Mask: 255 . 255 . 255 . 0

Remote Security Gateway: IP Addr. ▾ IP: 0 . 0 . 0 . 0

Encryption: ● DES ○ 3DES ○ Disable

Authentication: ● MD5 ○ SHA ○ Disable

Key Management: Auto. (IKE) ▾

☐ PFS (Perfect Forward Secrecy)

Pre-shared Key: (0x)

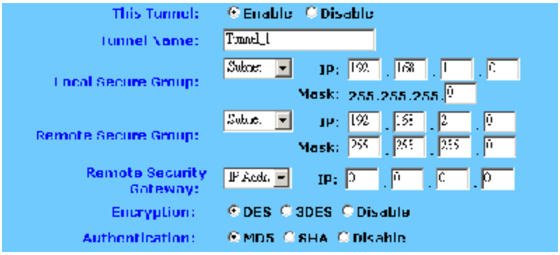
1. Select the tunnel you wish to create in the **Select Tunnel Entry** drop-down box. It is possible to create up to 70 simultaneous tunnels.

   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.



This Tunnel: ● Enable ○ Disable

Tunnel Name: Tunnel_1

Local Secure Group: Subnet ▾ IP: 192 . 168 . 1 . 0 Mask: 255.255.255.0

Remote Secure Group: Subnet ▾ IP: 192 . 168 . 2 . 0 Mask: 255 . 255 . 255 . 0

Remote Security Gateway: IP Addr. ▾ IP: 0 . 0 . 0 . 0

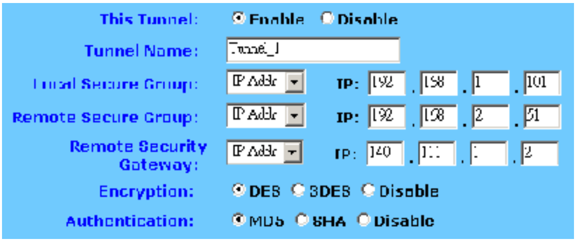
Encryption: ● DES ○ 3DES ○ Disable

Authentication: ● MD5 ○ SHA ○ Disable

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

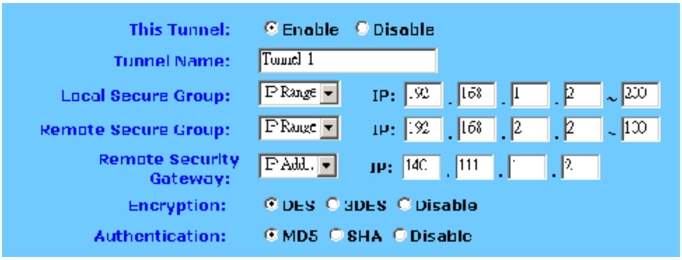
Remote Secure Group: IP Addr ▾ IP: 192 . 168 . 2 . 51

Remote Security Gateway: IP Addr ▾ IP: 140 . 111 . 1 . 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 telecommutors 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

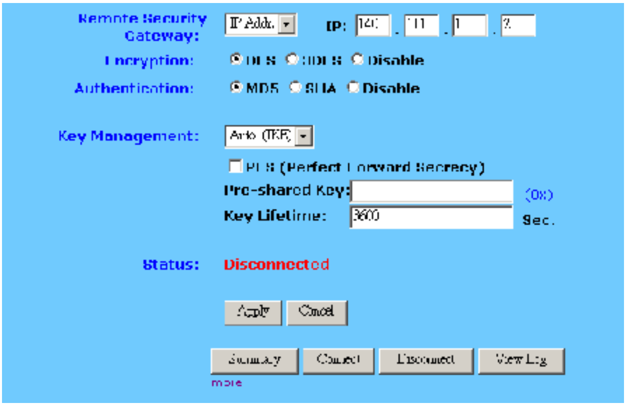
Remote Security Gateway: IP Addr. ▾ IP: 140 . 111 . 1 . 2

Encryption: ● DES ○ 3DES ○ Disable

Authentication: ● MD5 ○ SHA ○ Disable

3. 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.

4. 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.



Remote Security Gateway: IP Addr. IP: 140 . 11 . 1 . 2

Encryption: ● DES ○ 3DES ○ Disable

Authentication: ● MD5 ○ SHA ○ Disable

Key Management: Auto (IKE)

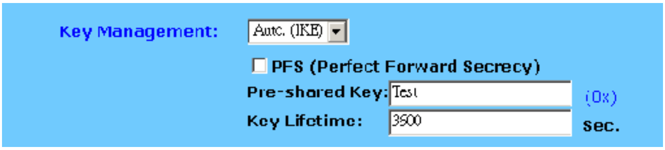
□ PFS (Perfect Forward Secrecy)

Pre-shared Key: (0x)

Key Lifetime: 3600 Sec.

Status: Disconnected

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.



Key Management: Auto. (IKE)

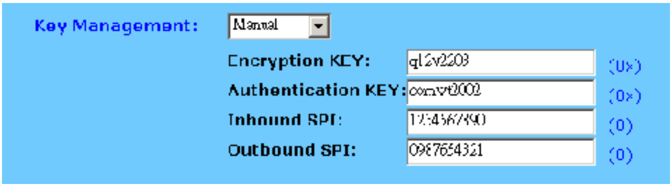
□ PFS (Perfect Forward Secrecy)

Pre-shared Key: Test (0x)

Key Lifetime: 3600 Sec.

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.

   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.



Key Management: Manual

Encryption KEY: ql2v2203 (0x)

Authentication KEY: comvt2002 (0x)

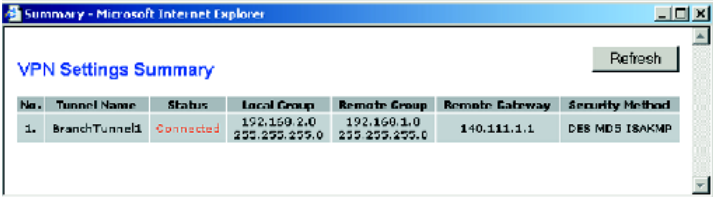
Inbound SPI: 1234567890 (0)

Outbound SPI: 0987654321 (0)

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.

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:



VPN Settings Summary

No.	Tunnel Name	Status	Local Group	Remote Group	Remote Gateway	Security Method
1.	BranchTunnel1	Connected	192.168.2.0 255.255.255.0	192.168.1.0 255.255.255.0	140.111.1.1	DES MD5 ISAKMP

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.

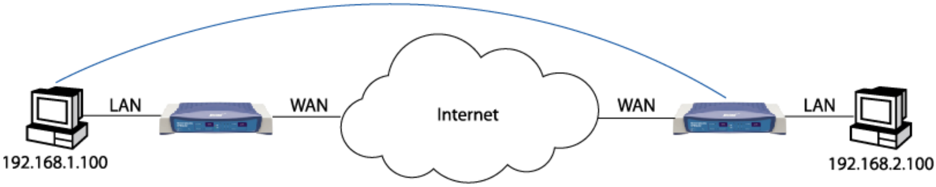
- Double-check all the values you entered on the VPN screen to make sure they are correct.
- Check the status page of both the local router and the remote device and ensure the public IP addresses are the same as entered for the remote security gateway.

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.

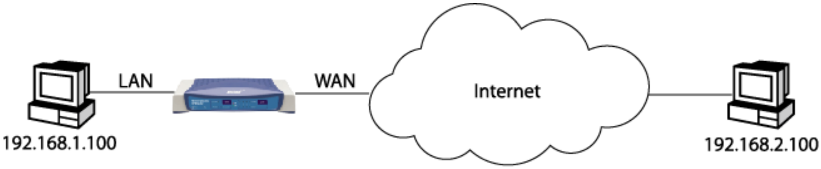
The VPN Log screen displays successful connections, transmissions and receptions, and the types of encryptions used. Once you no longer have need of the tunnel, simply click the Disconnect button on the bottom of the VPN page.

5-4 Example1: Tunnel between Two VPN Routers



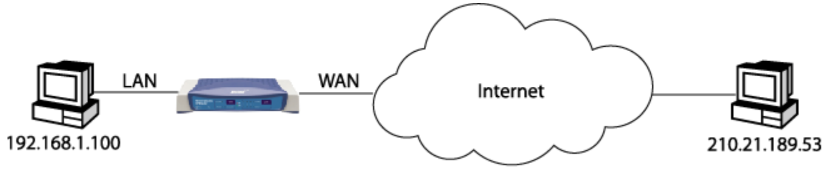
	VPN Router #1	VPN Router #2
LAN IP:	92.168.1.1	192.168.2.1
WAN IP:	210.241.239.77	211.21.189.53
Default Gateway:	210.241.239.73	211.21.189.49
	Tunnel 1	Tunnel 1
This Tunnel:	Enable	Enable
Local Secure Group:	Subnet 192.168.1.0, 255.255.255.0	Subnet 192.168.2.0, 255.255.255.0
Remote Secure Group:	Subnet 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	Win2000 Professional Safenet Cisco VPN Client
LAN IP:	192.168.1.1	
WAN IP:	210.241.239.77	IP: 210.21.189.53
Default Gateway:	210.241.239.73	210.21.189.49
	Tunnel 1	Tunnel 1
This Tunnel:	Enable	Enable
Local Secure Group:	Subnet 192.168.1.0, 255.255.255.0	IP: 211.21.189.53
Remote Secure Group:	IP: Any	Subnet 192.168.1.0, 255.255.255.0
Remote Security Gateway:	Any	210.241.239.77
Encryption:	DES	DES
Authentication:	MD5	MD5
IPSec:	ISAKMP	ISAKMP
PFS:	Off	Off
IKE Pre-share KEY:	MyTest	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 NB5580/W. 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 2000Server

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

Subnet Mask: 255.255.255.0

ADSL Integrated Gateway

WAN

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

Subnet Mask: 255.255.255.0

LAN

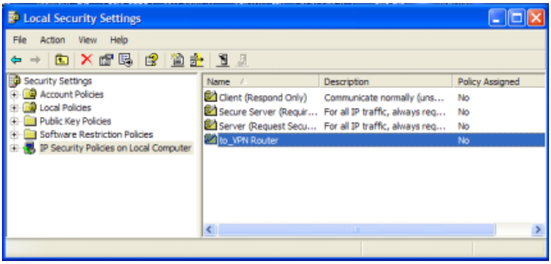
IP Address: 192.168.1.1

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**").



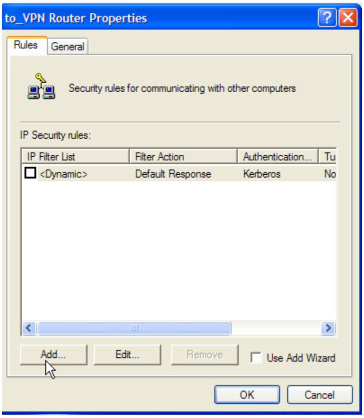
Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (uns...	No
Secure Server (Requir...	For all IP traffic, always req...	No
Server (Request Secu...	For all IP traffic, always req...	No
to_VPN Router		No

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→VPN Router" and "VPN Router→WinXP".

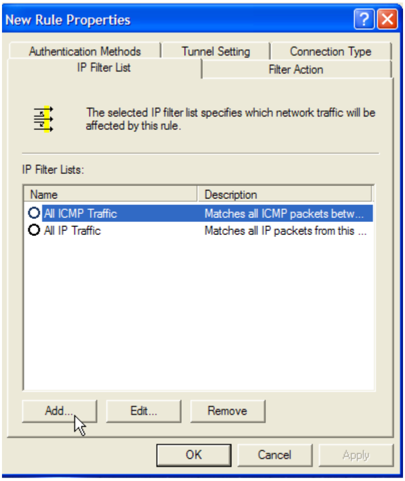
[Filter List 1] WinXP→ VPN Router

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



IP Filter List	Filter Action	Authentication...	Tu
☐ <Dynamic>	Default Response	Kerberos	No

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



New Rule Properties

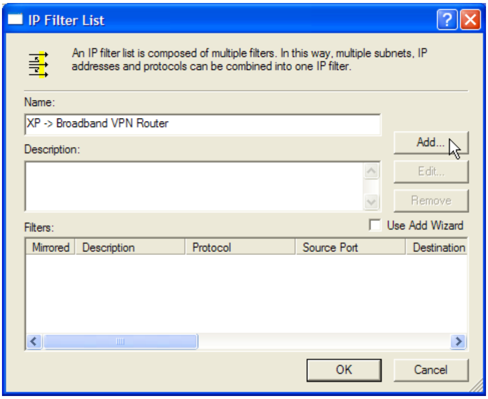
Authentication Methods | Tunnel Setting | Connection Type | IP Filter List | Filter Action

The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...

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



IP Filter List

An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name:
XP -> Broadband VPN Router

Description:

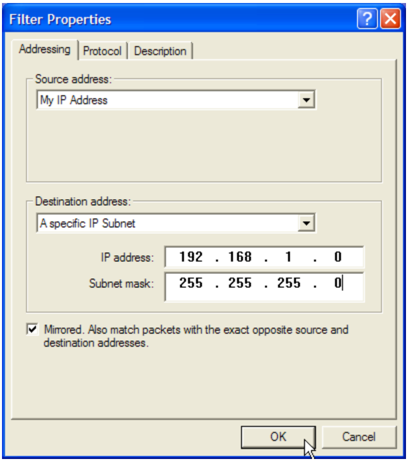
Filters:

□ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination

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.



Source address: My IP Address

Destination address: A specific IP Subnet

IP address: 192 . 168 . 1 . 0

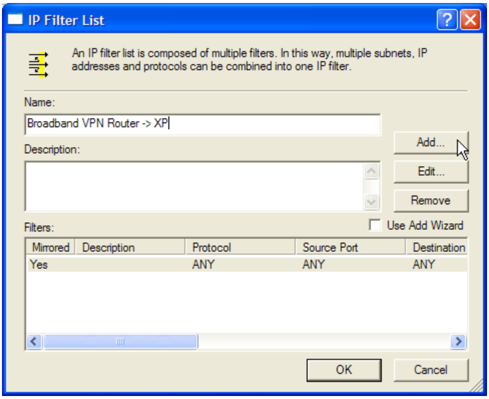
Subnet mask: 255 . 255 . 255 . 0

☑ Mirrored. Also match packets with the exact opposite source and destination addresses.

7. Click **OK** button. Then click **OK**(for WinXP) or **Close** (for Win2000) button on the **IP Filter List** window.

[Filter List 2] Broadband VPN Router→WinXP

8. On the **IP Filter List** tab, click the **Add** button.
9. Type an appropriate name **"Broadband VPN Router→XP"** for the filter list, click to clear the **Use Add Wizard** check box, and then click **Add**.



An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: Broadband VPN Router -> XP

Description:

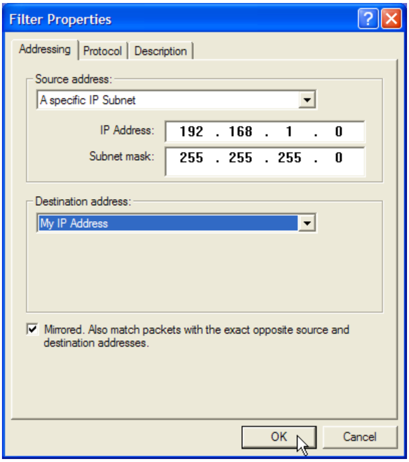
Filters:

□ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY

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.



Filter Properties

Addressing | Protocol | Description

Source address: A specific IP Subnet

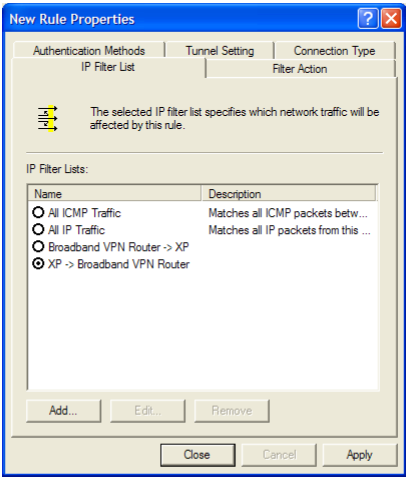
IP Address: 192 . 168 . 1 . 0

Subnet mask: 255 . 255 . 255 . 0

Destination address: My IP Address

☑ Mirrored. Also match packets with the exact opposite source and destination addresses.

13. Click **OK**, and then click **OK**.



New Rule Properties

Authentication Methods | Tunnel Setting | Connection Type | IP Filter List | Filter Action

The selected IP filter list specifies which network traffic will be affected by this rule.

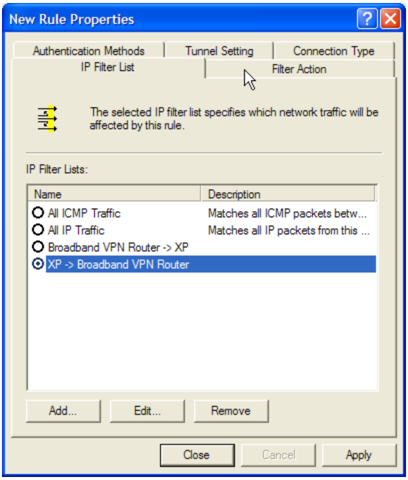
IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
○ Broadband VPN Router -> XP	
● XP -> Broadband VPN Router	

6-2.3 Configure Individual Rule of 2 Tunnels

[Tunnel 1] WinXP→Broadband VPN Router

1. From the **IP Filter List** tab, click the filter list **“XP→Broadband VPN Router”**.

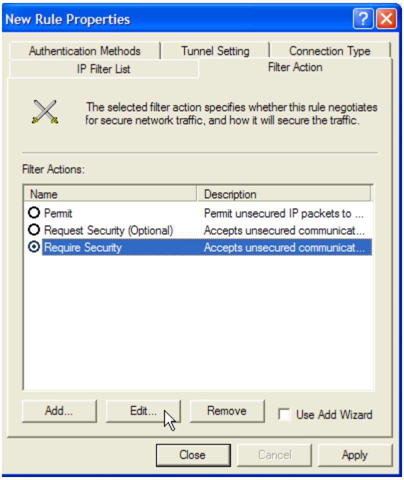


The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
○ Broadband VPN Router -> XP	
● XP -> Broadband VPN Router	

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



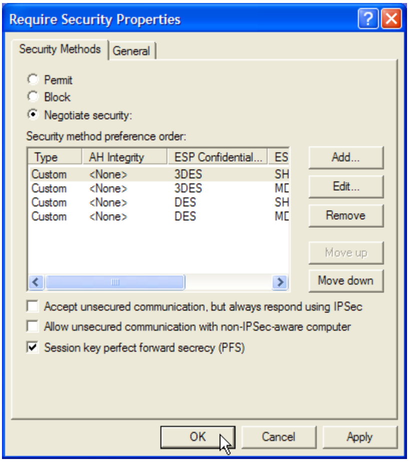
The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

Filter Actions:

Name	Description
○ Permit	Permit unsecured IP packets to ...
○ Request Security (Optional)	Accepts unsecured communicat...
● Require Security	Accepts unsecured communicat...

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 ADSL Integrated Gateway, and then click the **OK** button.



Require Security Properties

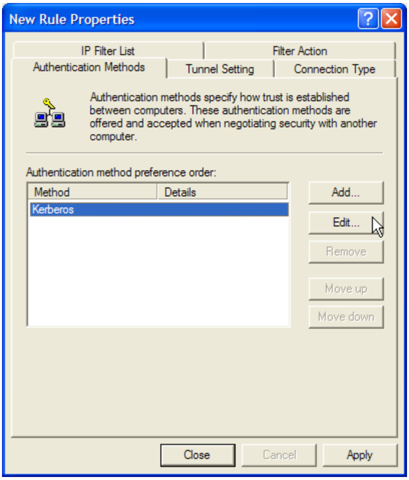
○ Permit
○ Block
● Negotiate security:

Security method preference order:

Type	AH Integrity	ESP Confidential...	ES
Custom	<None>	3DES	SH
Custom	<None>	3DES	MD
Custom	<None>	DES	SH
Custom	<None>	DES	MD

□ Accept unsecured communication, but always respond using IPSec
□ Allow unsecured communication with non-IPSec-aware computer
☑ Session key perfect forward secrecy (PFS)

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

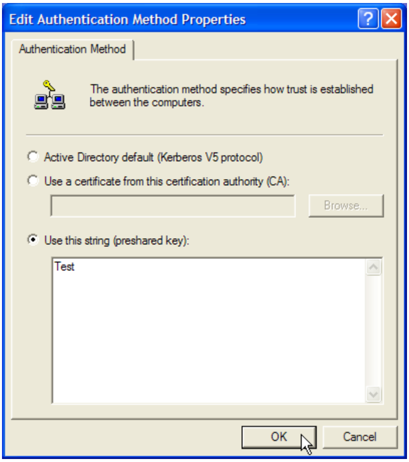


New Rule Properties

Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Kerberos	



Edit Authentication Method Properties

Authentication Method

The authentication method specifies how trust is established between the computers.

○ Active Directory default (Kerberos V5 protocol)

○ Use a certificate from this certification authority (CA):

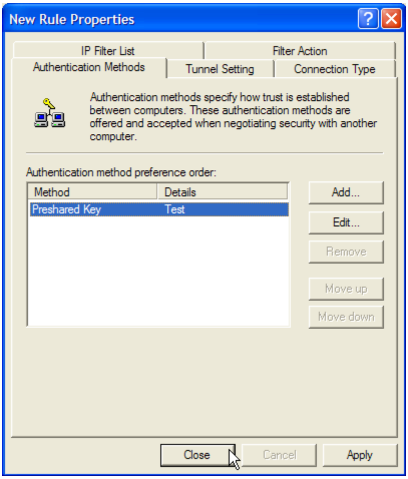
Browse...

● Use this string (preshared key):

Test

OK Cancel

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



New Rule Properties

IP Filter List | Filter Action | Authentication Methods | Tunnel Setting | Connection Type

Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

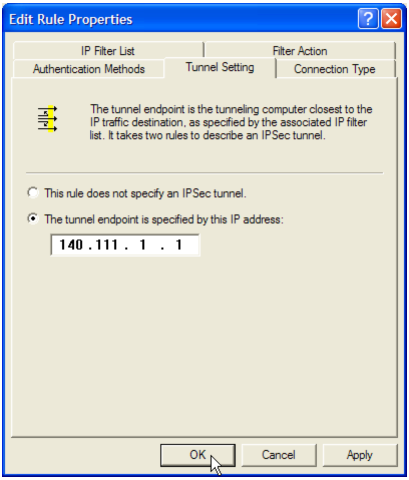
Method	Details
Preshared Key	Test

Add... Edit... Remove Move up Move down

Close Cancel Apply

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

7. 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 ADSL Integrated Gateway.



Edit Rule Properties

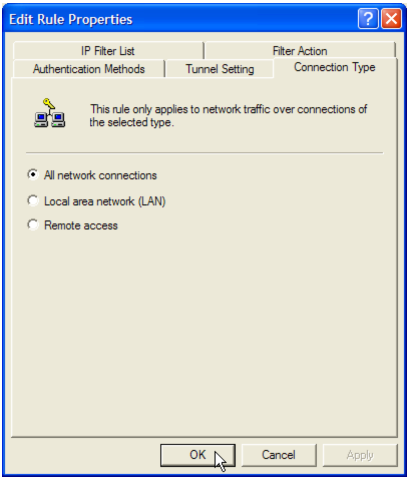
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.

○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP address:

140 . 111 . 1 . 1

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



Edit Rule Properties

This rule only applies to network traffic over connections of the selected type.

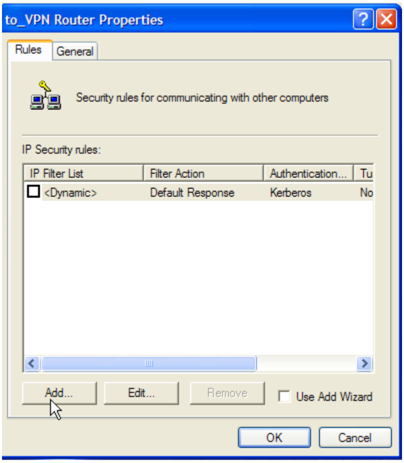
● All network connections

○ Local area network (LAN)

○ Remote access

[Tunnel 2] VPN Router→ WinXP

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



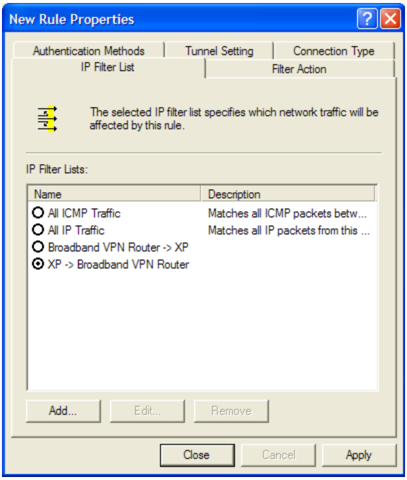
Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
□ <Dynamic>	Default Response	Kerberos	No

□ Use Add Wizard

10. On the **IP Filter List** tab, click the filter list **“Broadband VPN Router→XP”**.

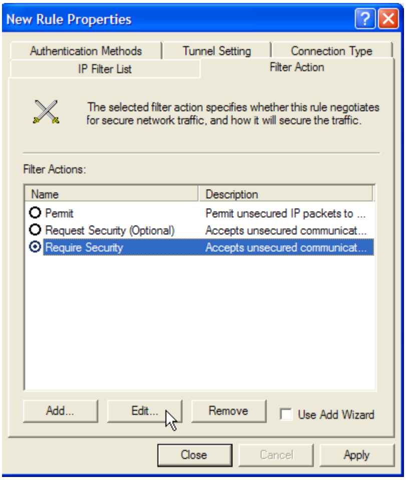


The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
○ Broadband VPN Router -> XP	
● XP -> Broadband VPN Router	

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



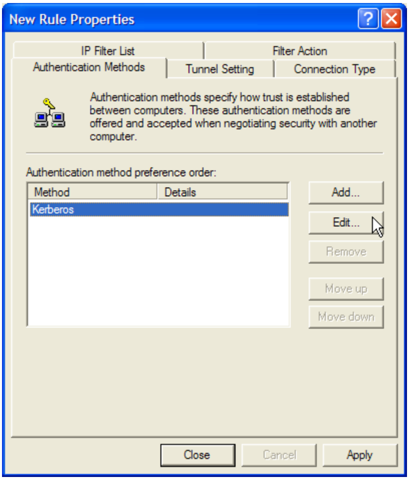
New Rule Properties

The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

Filter Actions:

Name	Description
○ Permit	Permit unsecured IP packets to ...
○ Request Security (Optional)	Accepts unsecured communicat...
● Require Security	Accepts unsecured communicat...

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



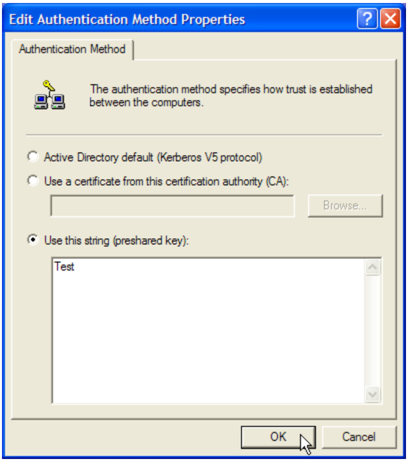
New Rule Properties

Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Kerberos	

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



Edit Authentication Method Properties

Authentication Method

The authentication method specifies how trust is established between the computers.

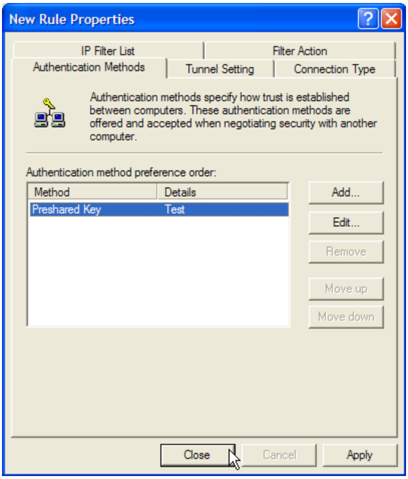
○ Active Directory default (Kerberos V5 protocol)

○ Use a certificate from this certification authority (CA):

● Use this string (preshared key):

Test

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



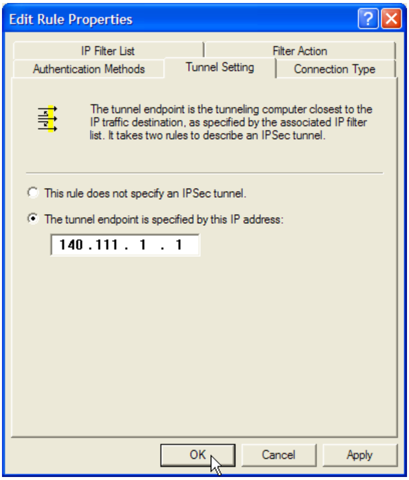
New Rule Properties

Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Preshared Key	Test

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



Edit Rule Properties

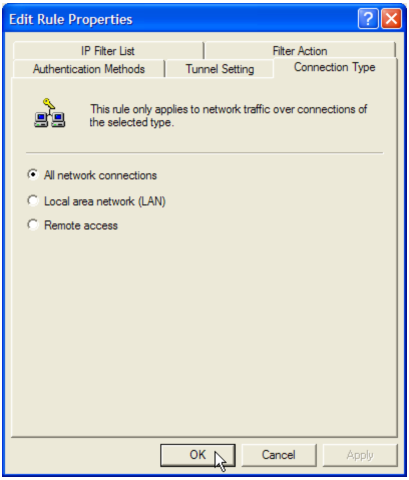
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.

○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP address:

140 . 111 . 1 . 1

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



Edit Rule Properties

This rule only applies to network traffic over connections of the selected type.

● All network connections

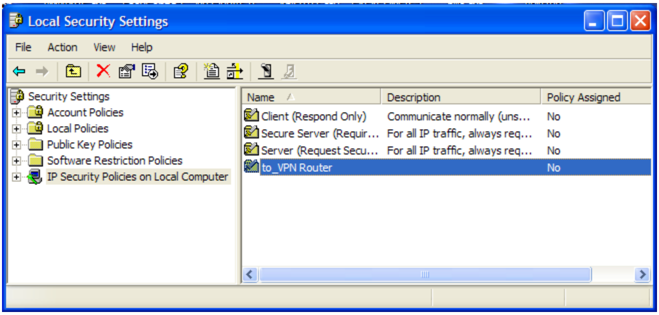
○ Local area network (LAN)

○ Remote access

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.

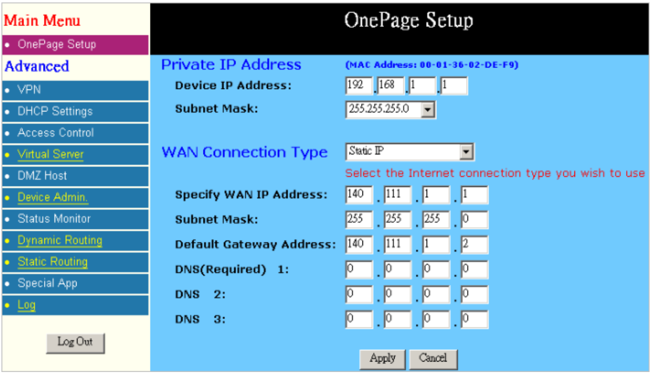


Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (uns...	No
Secure Server (Requir...	For all IP traffic, always req...	No
Server (Request Secu...	For all IP traffic, always req...	No
to_VPN Router		No

6-3 Steps in ADSL Integrated Gateway

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.



Private IP Address (MAC Address: 00-01-36-02-DE-F9)

Device IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

WAN Connection Type: Static IP

Select the Internet connection type you wish to use

Specify WAN IP Address: 140 . 111 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway Address: 140 . 111 . 1 . 2

DNS(Required) 1: 0 . 0 . 0 . 0

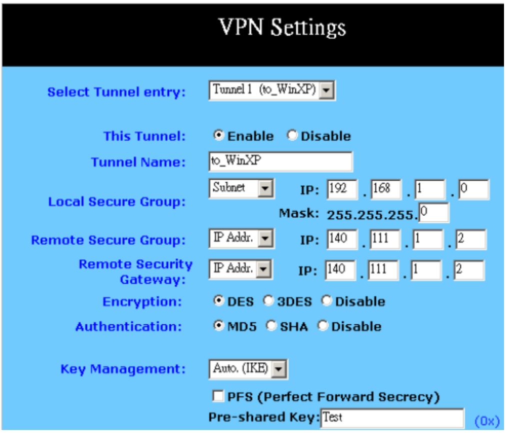
DNS 2: 0 . 0 . 0 . 0

DNS 3: 0 . 0 . 0 . 0

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.

6-3.2 VPN Screen

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



VPN Settings

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 (0x)

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: Security

This chapter provides guidance to ensure that security is maintained during installation and operation of your NetComm NB5580/W.

Your NB5580/W comes with default settings that reach a balance between immediate operability and security. However we recommend that you review the following features to ensure that your NB5580/W is as secure as your network and interoperability settings will allow.

Below is a list of the areas that need your attention to secure your NB5580/W from unauthorised access - these areas or features are;

- Physical Security
- Wireless Security (**NB5580W only**)
- Administration Password
- SNMP Community Strings
- Remote Configuration via HTTP
- Block WAN Ping Response
- DMZ Host
- Port Forwarding
- Dynamic Routing (RIP Configuration)
- Special Application
- VPN Settings
- Remote Security Gateway
- Encryption & Authentication
- Access Control
- Universal Plug 'n Play
- Logging

Physical Security

Physical security should be considered because if a malicious person has physical access to the unit they can damage it, steal it, reset it to factory defaults or just sabotage it to allow them remote access later on.

Note: Your Admin password can be deleted with physical access.

Wireless Security (NB5580W only)

The NB5580W has a Wireless Access Point built-in and enabled by default. If you do not wish to use this feature at this time you should disable it. Connecting your NB5580W to your Network in default mode will allow any wireless client in range to freely access your LAN devices as well as your Internet service. If you intend on using Wireless access you should consider enabling WEP, enabling MAC Filtering and disabling the SSID broadcast feature to enhance your network security.

Administration Password

Your Admin Password gives you complete control over the NB5580/W it should NEVER be left as default because it can allow access from a Web browser on both your LAN and possibly the Internet. You should change your Administration Password to something complex and involving many UPPER and lower case Characters. Some examples of suitable passwords in growing complexity are;

fa11en4you	<- mixing words and numbers, replacing letters with numbers.
Buz911B0xzero	<- as above but using upper and lower case as well.
SecN@tC0mmwillyou	<- The '0' is a zero, the use of '@' instead of 'e'

To change your Admin password choose the 'Device Admin' option on the menu. Enter your new password twice, once in each field and then click the submit button

Note: For security your password's characters will be replaced with dots so no one can see you type it on the screen.

SNMP

Simple Network Management Protocol is used to manage devices on networks from a central location. SNMP is disabled by default and you should not enable it unless you wish to use it. The authentication for SNMP is based on 'Community Strings' these are like passwords and should be treated as such when it comes to security. If you want to use SNMP on your NB5580/W you should change all your community strings (both public and private) to more secret names with more complexity.

Remote Configuration via HTTP

The HTTP server built into the NB5580/W is used to allow you to view and edit configuration pages via a web browser from anywhere on the Internet. You can set the NB5580/W to allow this information to be viewed or changed via the WAN (Internet). The default is to NOT allow Remote configuration (Administration) via the Internet, this can be changed in the Device admin page. You can also change the port that the service runs on (default is port 8080) but this means when you access your NB5580/W you will need to include the different port when you type its IP address E.g;

http://192.168.1.1:8080

Block WAN Ping Response

Most Devices running TCP/IP protocols will respond to a Ping, this makes diagnosis of Networking problems easier to fault find. However responding to a Ping request to your Public (WAN) IP address makes you an easier target for hackers. The NB5580/W is set to disregard a ping from the internet by default, if you need to enable this feature for diagnosis of a problem please remember to Enable the Block again when testing is complete.

DMZ Host

The DeMilitarized Zone Host setting is used to specify the IP address of a computer (Host) that will deal with any data received from the internet that is not a response to an internal computer's request (via NAT). This data would normally be 'dropped' by the NB5580/W but if you wish to allow external access to a particular internal computer, this option is used to 'expose' the 'Host' to raw connections from the internet.

The DMZ host feature is most commonly used to allow Internet users access to a Web server or Game server.

Note: To secure your network you should ensure that the DMZ host feature is disabled. If you need to use the DMZ host feature you should ensure the computer with the IP address specified is secured with a secondary software or hardware firewall.

Port Forwarding

This feature is similar to the DMZ host feature except it allows individual ports on the public Internet IP address to be forwarded to a private IP address. This is most commonly used to allow Internet users to access a Web service on port 80 etc.

To secure your NB5580/W you should not have port forwards that are not being used. Any port forwards that have been configured should only specify the IP address of secure computers.

Dynamic Routing (RIP)

RIP is disabled by default, you should only enable RIP if you want your NB5580/W to accept routing information from other LAN routers or if you want it to share it's routing information with other router's. As always the less information a 'Hacker' can find out about your system the less chance the hacker has of finding an exploit for your system. Ensure RIP is disabled if you do not need to use it.

Special Application (Port Triggering)

The ‘Special Application’ settings of your router allows specific ports to be opened by ‘triggering’. This means that if you specify ports on the Special Applications menu these ports will be monitored and allowed to pass more easily through the Firewall/NAT engine should a special Internet application require more direct access. While Programs like Peer to Peer (P2P) file sharing programs, On-line games etc can use these triggered ports you must be aware that these programs could subsequently allow access to your LAN or atleast the computer they are running on. If you do not need Special Applications triggered ports leave these fields blank.

VPN

Your router has VPN tunnel endpoints built-in these can allow full Network access to your entire LAN Subnet, a IP address range or just a single IP address (Computer).

Local Secure Group

To ensure the highest level of network security is maintained it is best to set your “Local Secure Group” to be the minimal number of IP addresses required for the purpose of the VPN tunnel.

E.g. If the VPN tunnel is only used for using Remote Desktop Connection to a Windows XP computer on an IP address of 192.168.1.200 then limit the Local Security settings to the following;

(Subnet / IP range / IP Address) = IP Address

IP = 192.168.1.200

MASK = Not Applicable (because an IP was specified)

Note: Don’t forget any changes you make in the ‘Local Secure Group’ will need to be reflected in the settings for ‘Remote Secure Group’ in the Router/Client at the other end.

Remote Security Gateway

To further increase your security you should limit the possibilities of the Remote Security Gateway setting. This setting will need to be set to ‘ANY’ if the remote router or VPN client is going to be allocated a new Public IP address each time it connects to the Internet. ‘ANY’ is the least desirable setting for security but it may be necessary for practical reasons (e.g. ‘Road Warrior’ type VPN tunnels).

However if the VPN router / Client at the remote end is on a fixed IP address it is strongly recommended that you specify the IP address here as this will prevent hackers on other IP addresses being able to create a VPN tunnel to your Router even if the know your Preshared Key and other private settings.

Encryption & Authentication

Setting encryption (DES or 3DES) is highly desirable as this will help prevent a hacker from reading the contents of any intercepted packets. DES is a Standardised encryption method that is very strong, 3DES passes each payload through the encryption alogorithim three times to enhance its security. 3DES is the most secure setting.

Authentication (MD5 or SHA) should be used to increase security of your VPN tunnels, choose the authentication method which best suits the VPN router / Client at the other end. This will help ensure that VPN tunnels joining your Router will authenticate via a known Preshared key before a tunnel is allowed.

Preshared Keys should be made out of complex strings of characters (as per the Admin password) and keys should be different for each tunnel entered so that access rights intended for one VPN client can not be used by a different client on a different tunnel.

Access Control

The NB5580/W has Access Control functions that allow you to restrict which Network Interface Cards (NICs) or IP addresses can use the Internet and or use other NetWork services. You can use this Access control to help increase the security of your Network by only allowing known or trusted devices/employees to access the internet and other services. If you place highly restricted servers behind a secondary router on another subnet you can restrict which NICs or IP addresses (or both) are allowed access to the second subnet.

URL Filters and Web Filters are another way to help keep your network security tight, if you prevent internal computers from running Java script, Active X script etc you can help prevent the downloading and subsequent execution of potentially malicious code from being forced onto your computer via web browsing, however most modern web pages use some for of this code and this may be come restrictive. If you are using Access control measures on your router you should also block the use of Proxies as these may allow an internal user (LAN user) to circumvent your Access Control.

Universal Plug and Play

UPnP allows Internet Application running on local LAN computers to Automatically configure your router with Port Forwarding configurations that will allow specific port data to be transmitted directly to the LAN computer hosting the application.

Because UPnP effectively allows a computer to configure openings in your firewall it’self it is disabled by default in your router. Only enable UPnP if you wish to reduce your security by allowing your UPnP enabled applications to configure your router.

Logging

To maintain a secure network it is important to adapt to changes in your network environment. The best way to do this is to view the logging in your router, particularly look for items in red text as these indicate data that has been blocked by the firewall or by your Access Control filters. For easy regular monitoring use the email or Syslog features to send you log to another computer.

Chapter 8: Trouble Shooting

This chapter provides solutions to problems you may encounter during installation and operation of your NetComm NB5580/W.

Hardware

The Power LED is off.

Check the power cable is properly connected to the NetComm NB5580/W, the power adapter and the socket.

The LAN Link LED is off.

Check the computer, hub or switch is properly connected to the NetComm NB5580/W.

Check the computer's Ethernet card is properly installed.

Check the UTP cable connecting the computer to the Router is connected.

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.

Why can't I configure the NetComm NB5580/W?

First, check whether the NetComm NB5580/W is properly installed, including the LAN and WAN connections, and all devices' power.

Check the NB5580/W and the computer are on the same network segment. If you are not sure, initiate the DHCP function (Section 4-2) and set your computer to obtain an IP address automatically (Appendix B).

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 NB5580/W's default IP address of 192.168.1.1. Check also the Subnet Mask is set to 255.255.255.0

- 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 NB5580/W 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 NB5580/W'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 NB5580/W, make sure that you disable the proxy setting within your Internet browser and set your browser to access the Internet via the LAN.

What can I do if I have forgotten the password for NetComm NB5580/W?

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.

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 (Section 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 (Appendix B) 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)

I can't browse the Internet via the NetComm NB5580/W

Ensure your computer can ping or access the Router. See the previous section entitled **"Why can't I configure the NetComm NB5580/W"** for more information.

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

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 NB5580/W's settings are correct (Section 3-3).

Appendix A: Frequently Asked Questions

What is the maximum number of IP Addresses the NetComm NB5580/W can support?

The NetComm NB5580/W can support up to 253 IP Addresses usually in the range of 192.168.1.2~192.168.1.254.

Where should the NetComm NB5580/W be installed on the network?

In a typical environment, the NetComm NB5580/W should be installed between the ADSL/Cable modem and your LAN. Connect the NetComm NB5580/W to the Ethernet port of your ADSL/Cable modem, and connect your computers to the RJ45 jack on the LAN side.

Does the NetComm NB5580/W support IPX or AppleTalk?

No. The NetComm NB5580/W 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 NB5580/W can support them.

Does the NetComm NB5580/W support 100Mb Ethernet?

Yes, the NetComm NB5580/W supports both 10Mb & 100Mb Ethernet on the LAN side, but only 10Mb on the WAN side.

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.

How can NetComm NB5580/W share single user account to multiple users?

The NetComm NB5580/W 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.

What operating systems does NetComm NB5580/W series support?

The NetComm NB5580/W 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.)

Can I use multiple E-mail accounts if I use NetComm NB5580/W?

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.

Can Internet users access LAN computers?

The NetComm NB5580/W uses NAT to route all in/out band packets. All external users can only see the IP of the NetComm NB5580/W but cannot access LAN computers. The LAN computers are well protected with the NetComm NB5580/W's natural firewall (NAT). You can allow Internet users access to specific computers by using the Port Forwarding, DMZ Host and Special Application options.

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).

Does the NetComm NB5580/W support PPTP of VPN packets pass through?

Yes. The NetComm NB5580/W supports PPTP pass through.

Does the NetComm NB5580/W series support IPsec?

Yes. The NetComm NB5580/W supports IPsec pass through.

Wireless Questions

Can I run an application from a remote computer over the wireless network?

This will depend on whether or not the application is designed to be used over a network. Most applications that are designed to work over TCP/IP ethernet newworks should run transparently over your wireless network.Consult the application's user guide to determine if it supports operation over a network.

Can I play multiplayer games with other users of the wireless network?

Yes, as long as the game supports multiple players over a LAN (local area network). Refer to the game's user guide for more information.

What are Ad-hoc and Infrastructure modes?

An Ad-hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN. An Ad-hoc wireless LAN is applicable when no AP is available or you wish to run a private network not joined to the corporate wireless network.

Because the NB5580W can only operate in Access Point mode when you wish to connect to it your Wireless client adapters (connected to your computers) MUST be set to Infrastructure mode.

What is Roaming?

Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single Access Point. Before using the roaming function, the workstation must make sure that it is the same channel number as the Access Point of the dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and Access Point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links Access Points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each Access Point and the distance of each Access Point to the wired backbone. Based on that information, the node next selects the right Access Point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original Access Point or whether it should seek a new one. When a node no longer receives acknowledgment from its original Access Point, it undertakes a new search. Upon finding a new Access Point, it then re-registers, and the communication process continues.

What is ESSID?

An Infrastructure configuration can support roaming for mobile workers. More than one Access point can be configured as an with the same SSID. Users within range of atleast one Access point could roam freely between Access points while maintaining a continuous connection to the wireless network.

What is ISM band?

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

What is DSSS? What is FHSS? And what are their differences?

Frequency Hopping Spread Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be shortduration impulse noise. Direct Sequence Spread Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Would the information be intercepted while transmitting on air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, the WLAN series offers the encryption function (WEP) to enhance security and access control. Users can set it up depending upon their needs.

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a shared-key algorithm, as described in the IEEE 802.11 standard.

What is a MACAddress?

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs on to the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

How do I avoid interference?

Using multiple Access Points on the same channel and in close proximity to one another will generate interference. When employing multiple Access Points, be sure to operate each one on a different channel (frequency). But use the same SSID to allow seamless roaming.

How do I resolve issues with signal loss?

There is no way to know the exact range of your wireless network without testing. Every obstacle placed between an Access Point and wireless PC will create signal loss. Leaded glass, metal, concrete floors, water and walls will inhibit the signal and reduce range. Start with your Access Point and your wireless PC in the same room and move it away in small increments to determine the maximum range in your environment.

You may also try using different channels, as this may eliminate interference affecting only one channel. Additional high gain antennas can help you focus the power of your transmission to improve range in the desired area.

I have excellent signal strength, but I cannot see my network.

WEP is probably enabled on the Access Point, but not on your wireless adapter (or vice versa).

Verify that the same WEP Keys and levels (64 or 128) are being used on all nodes on your wireless network. Also we suggest you check for Wireless MAC filtering.

What is the maximum number of users the Access Point facilitates?

No more than 64, but this depends on the volume of data and may be less if many users create a large amount of network traffic.

How many channels/frequencies are available?

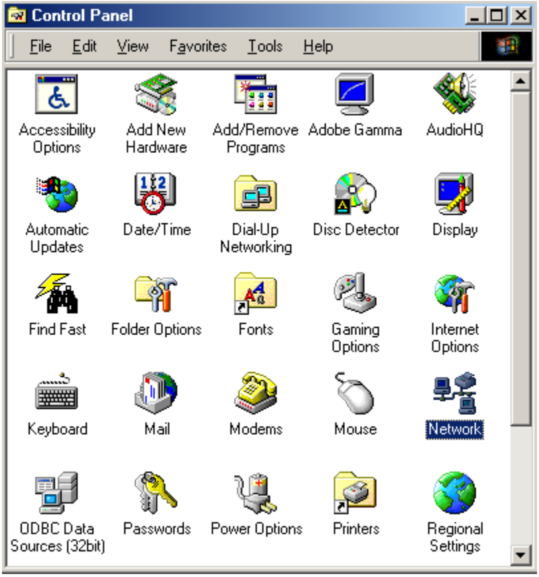
Using 802.11b or 802.11g, there are thirteen available channels in the Australian domain. Some channels may not be selectable depending on your product and regional regulations.

Appendix B: Setting up TCP/IP Protocol

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.

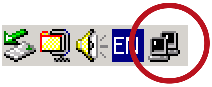
1. Click the **"Start"** button. Choose **"Settings"**, then **"Control Panel".**



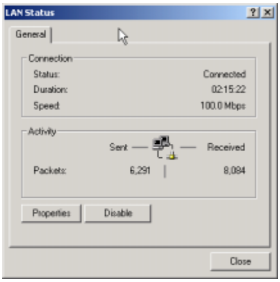
Double-click the **"Network"** icon. Your Network window should appear.

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.

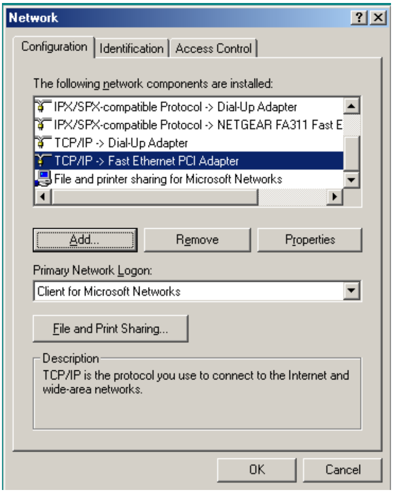


Connection
Status: Connected
Duration: 02:15:22
Speed: 100.0 Mbps

Activity
Sent — Received
Packets: 6,291 | 8,084

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

   - If yes, go to step 6.



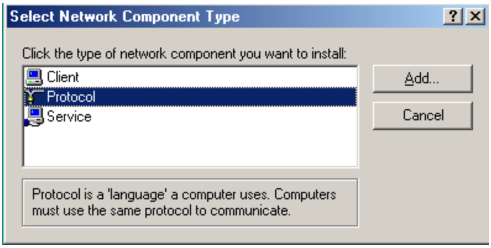
The following network components are installed:
IPX/SPX-compatible Protocol -> Dial-Up Adapter
IPX/SPX-compatible Protocol -> NETGEAR FA311 Fast E
TCP/IP -> Dial-Up Adapter
TCP/IP -> Fast Ethernet PCI Adapter
File and printer sharing for Microsoft Networks

Primary Network Logon:
Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

   - If no, click the **“Add”** button.

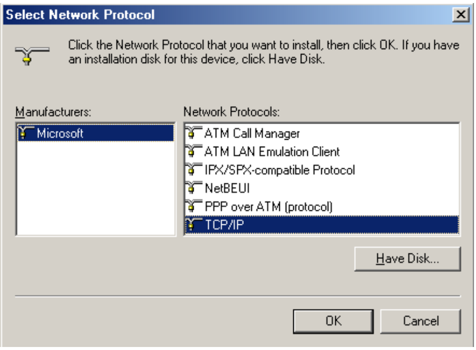
3. Double-click **“Protocol”** on the Select Network Component Type or highlight **“Protocol”** then click “**Add”**.



Click the type of network component you want to install:
Client
Protocol
Service

Protocol is a 'language' a computer uses. Computers must use the same protocol to communicate.

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



Select Network Protocol

Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this device, click Have Disk.

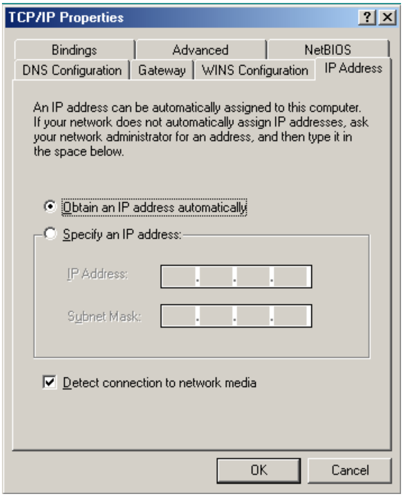
Manufacturers:
- Microsoft

Network Protocols:
- ATM Call Manager
- ATM LAN Emulation Client
- IPX/SPX-compatible Protocol
- NetBEUI
- PPP over ATM (protocol)
- TCP/IP

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.



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

☑ Detect connection to network media

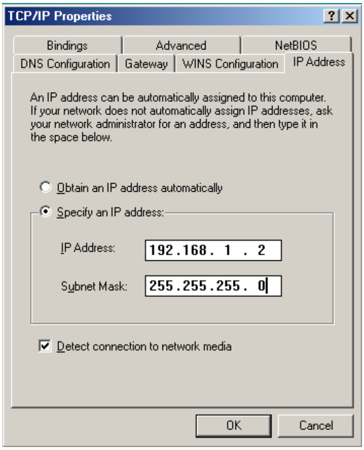
The TCP/IP Properties window consists of several tabs. Choose the **“IP Address”** tab.

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

Fixed IP Addresses Configuration

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

1. Select **"Specify an IP address"** and enter **"192.168.1.***"** in the **"IP Address"** location (where *** is a number between 2 and 254 used by the NetComm NB5580 to identify each computer), and the default **"Subnet Mask"** **"255.255.255.0"**.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically

● Specify an IP address:

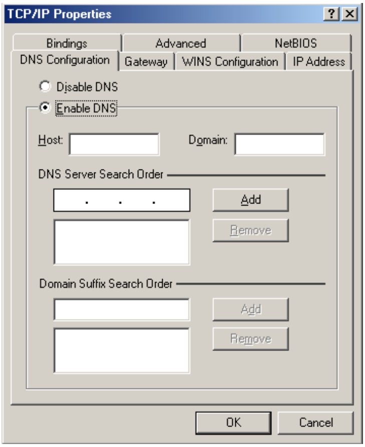
IP Address: 192.168. 1 . 2

Subnet Mask: 255.255.255. 0

☑ Detect connection to network media

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"**.



○ Disable DNS

● Enable DNS

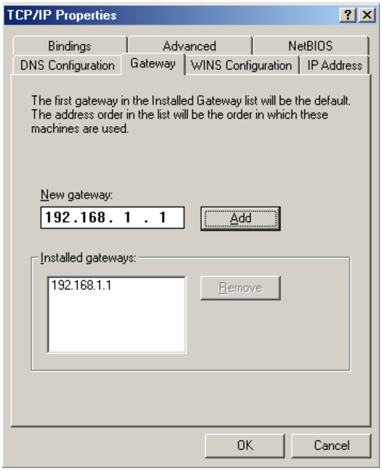
Host: Domain:

DNS Server Search Order

. . .

Domain Suffix Search Order

3. Click **"Gateway"** tab and enter the NetComm NB5580/W'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.



The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

New gateway: 192.168.1.1

Installed gateways: 192.168.1.1

Appendix C: 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 NB5580/W. 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 NB5580/W'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 NB5580/W'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 NB5580/W Configuration

To configure your NetComm NB5580/W, 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 NB5580/W to Existing Network

If the NetComm NB5580/W 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 NB5580/W.

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 NB5580/W'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 NB5580/W (refer to the above section).

Appendix D: Technical Specifications

Specifications for Wireless Model only (NB5580W)

Standards	IEEE 802.11/11g and 802.11b standard compliant, IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX)
Antenna	Single removable external antenna with reverse TNC connector
Operating Channels	*11b Mode:* 11 Channels (USA, Canada) 13 Channels (Europe & Australia) 14 channels (Japan) *11g Mode:* 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)
Access Mode	Infrastructure mode
Roaming	IEEE 802.11 Compliant
Security	64-bit & 128-bit WEP Encryption

General Specifications for both NB5580 & NB5580W

Standards	IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX)
Ports	WAN: One RJ-11 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
Frequency Range	2.4-2.4835GHz (Industrial Scientific Medical Band)
Data Transmission Rate	54Mbps / 48 / 36 / 24 / 12 / 11 / 9 / 6 / 5.5 / 2 / 1 Mbps Auto Fall-Back
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 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	A-Tick, N367
System Requirements	Operating system independent – ideal for Windows, Macintosh, Linux & TCP/IPsystems

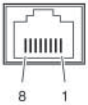
Appendix E: Cable Connections

This cable information is provided for your reference only. Please ensure you only connect the appropriate cable into the correct socket on either this product or your computer.

If you are unsure about which cable to use or which socket to connect it to, please refer to the hardware installation section in this manual. If you are still not sure about cable connections, please contact a professional computer technician or NetComm for further advice.

RJ-45 Network ports

All of the ethernet ports on the NP5580/W are 10/100 Mbps capable auto-sensing Ethernet ports. Each port supports only unshielded twisted pair (UTP) cable using an 8-pin RJ-45 plug. The Auto-uplink feature senses the connection of uplink (MDI-II) wiring using a straight-through twisted pair cable to any of the ethernet ports on the NP5580 switch to allow for connection to any port of an ethernet adapter, ethernet switch or hub.

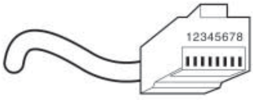


RJ-45 Connector Pin Assignment	Normal Assignment
1	Input Receive Data +
2	Input Receive Data -
3	Output Transmit Data +
6	Output Transmit Data -
4,5,7,8	Not used

Figure 1

Twisted pair cables

Figures 1 and 2 illustrate the use of straight-through and crossover twisted pair cables along with the connector.



RJ-45 plug
attached to cable

Figure 2

Straight and crossover cable configuration

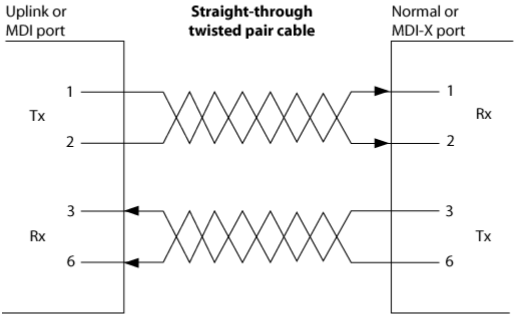


Figure 3

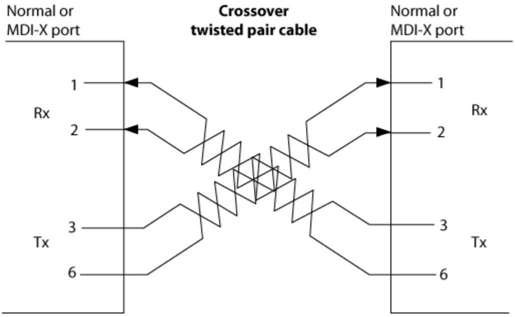
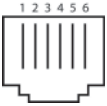


Figure 4

RJ11 connector and cable

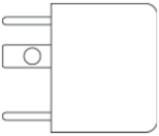
An RJ-11 connector is the small, modular plug used for most analog telephones. It has six pin slots in the head, but usually only two or four of them are used.



RJ-11 Connector Pin Assignment	Normal Assignment
1	Signal Ground
2	CTS
3	RXD
4	TXD
5	+5 Volts In
6	Signal Ground

Figure 5

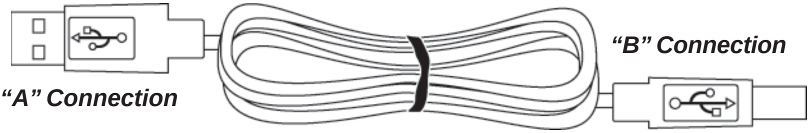
605 to RJ-11 adapter



The 605 to RJ-11adaptor is provided to comply with the older 610 Telstra wall socket. The 605 to RJ-11 adapter may be used to convert the supplied RJ-11 cable, if the older connection is required.

USB cable

A typical USB cord has an "A" connection (“upstream” to plug into the computer) and a “B” connection (“downstream” to plug into the device).



By using different connectors on the upstream and downstream ends, cable connection is simplified. The “B” connection will fit a into the “B” socket of any USB device. Similarly, any "A" connector can be plugged into any "A" socket, such as on a computer.

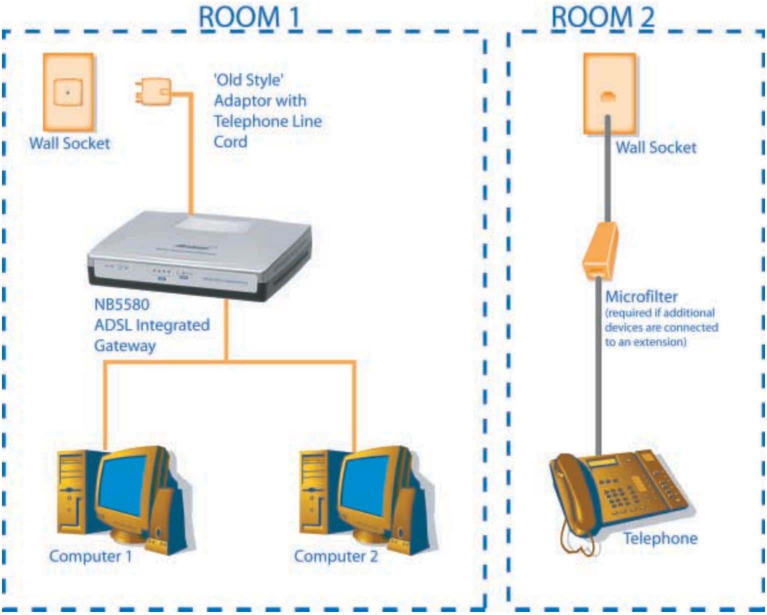
If it is a new device, the operating system auto-detects it and asks for the driver disk. If the device has already been installed, the computer activates it and starts talking to it. USB devices can be connected and disconnected at any time.

Appendix F: EM1100 ADSL Microfilter

Micro filters are used to prevent common telephone equipment, such as phones, answering machines and fax machines, from interfering with your ADSL service. If your ADSL enabled phone line is being used with any other equipment other than your ADSL Modem then you will need to use one Micro filter for each phone device.

Splitters may be installed when your ADSL line is installed or when your current phone line is upgraded to ADSL. If your telephone line is already split you will not need to use a Microfilter - check with your ADSL service provider if you are unsure.

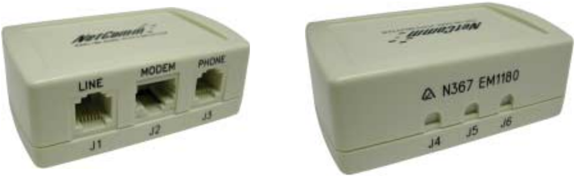
Each micro filter is connected in-line with your telephone or fax machine so that all signals pass through it. Telephones and/or facsimiles in other rooms that are using the same extension will also require Microfilters. The following diagram gives an example of connecting your ADSL Modem/Router using a Microfilter.


ROOM 1
Wall Socket
'Old Style' Adaptor with Telephone Line Cord
NB5580 ADSL Integrated Gateway
Computer 1
Computer 2
ROOM 2
Wall Socket
Microfilter
(required if additional devices are connected to an extension)
Telephone

Appendix G: EM1180 ADSL POTS Splitter Installation Guide

Features

- High quality low pass filter with optimum performance
- Surge and overload current protection
- Wall mounting facility
- Multiple input and output termination
- Additional wall outlet not required



Location for Installation

The ADSL splitter/filter should be installed into the premises telephone wiring on the customer side of any telephony connections. i.e. Before the first outlet or branching point.

Important Safety Instructions:

1. Read and understand all instructions.
2. Do not install this product near water for example, in a wet basement or near a swimming pool.
3. To reduce the risk of electric shock, do not disassemble this product. If service or repair work is required contact a qualified serviceman. Opening or removing covers may expose you to dangerous voltages or other risks. Incorrect re-assembly can cause electric shock when the appliance is subsequently used.
4. Refer servicing to qualified service personnel under the following conditions:
   - If liquid has been spilled into the product.
   - If the product does not operate correctly, i.e. If the telephone or ADSL service is disrupted by the installation of the filter.
   - If the product has been dropped or the housing has been damaged.
   - If the product exhibits a distinct change in performance.

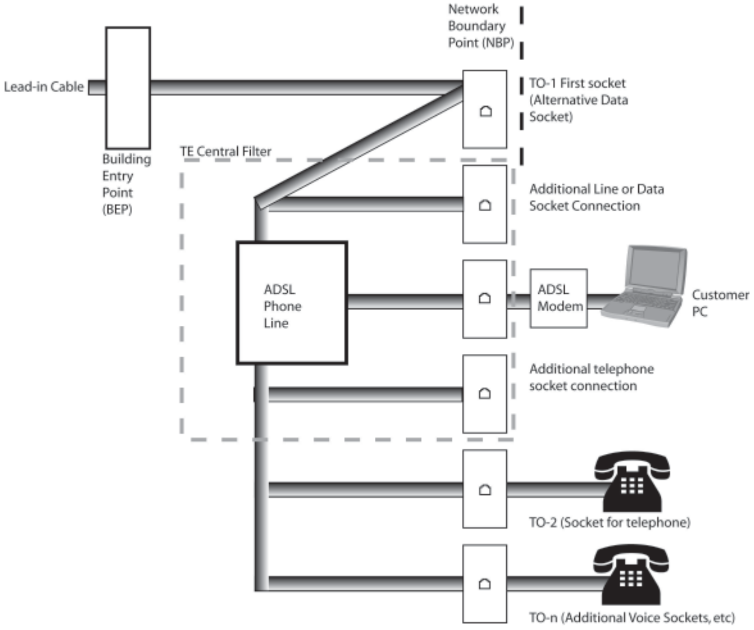
Wiring Instructions

Before you decide where to wall-mount the filter, check that all the cables can reach to their appropriate connections.

The ADSL splitter/filter may be either hard wired, or simply plugged in. If either the line, modem or the phone connection is to be hard-wired, then:

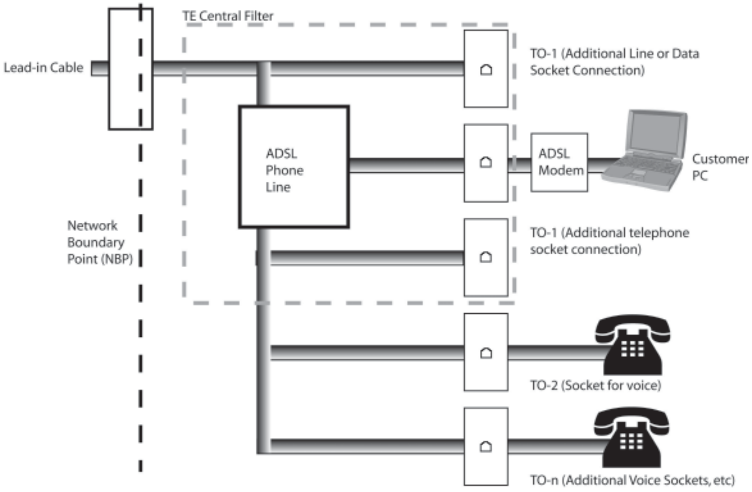
1. Lift the Wall Mount plate located on the back of the box with a flat screwdriver.
2. Remove the two screws.
3. Prepare the necessary cables by first stripping the outer cable for 25mm. Do not remove any insulation from the conductors to be terminated in the IDC.
4. Insert the conductors (2 per connector) to the relevant location on the IDC block using an IDC tool. See wiring configuration below for details.
5. Connect cable from ADSL Modem outlet to the connector marked ADSL.
6. Connect cable from in-house telephone wiring to the connector marked telephone.
7. Connect the incoming subscriber line to the connector marked LINE.
8. Secure cables with cable ties.
9. Put connector cover back in place and relocate onto the wall.

Configuration 1



Network Boundary Point (NBP)
Lead-in Cable
TO-1 First socket (Alternative Data Socket)
Building Entry Point (BEP)
TE Central Filter
Additional Line or Data Socket Connection
ADSL Phone Line
ADSL Modem
Customer PC
Additional telephone socket connection
TO-2 (Socket for telephone)
TO-n (Additional Voice Sockets, etc)

Configuration 2


TE Central Filter
Lead-in Cable
TO-1 (Additional Line or Data Socket Connection)
ADSL Phone Line
ADSL Modem
Customer PC
Network Boundary Point (NBP)
TO-1 (Additional telephone socket connection)
TO-2 (Socket for voice)
TO-n (Additional Voice Sockets, etc)

Wall Mounting Instructions

The ADSL splitter/filter can be mounted on a wall by simply suing the wall mounting plate enclosed, and suing the double sticky tape or the two screws provided.

This filter may be mounted either horizontally or vertically.

Follow these steps for screw mount:

1. Use the wall mounting plate as template to mark the two positions for holes where you wish to mount the box on the wall.
2. Drill the marked holes with a 6.0mm (0.24inch) diameter drill bit to a minimum depth of 35mm (1.38inch).
3. Insert the wall plugs into the drilled holes.
4. Position the wall mounting plate over the holes and insert the screws.
5. Position the filter over the wall mounting plate and push firmly into position until it is secured.

Connector	Function	Style	Tip	Ring
J5	Line	RJ12/IDC	Pin3	Pin4
J4	ADSL Modem	RJ45/IDC	Pin4	Pin5
J6	Local Phone	RJ123/IDC	Pin3	Pin4

Appendix H: 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.

IPAddress

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 I: 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.

Legal & Regulatory Information Copyright Information

NetComm Limited reserves the right to change the specifications and operating details of this product without notice.

NetComm is a registered trademark of NetComm Limited.

All other trademarks are acknowledged the property of their respective owners.

Customer Information

ACA (Australian Communications Authority) requires you to be aware of the following information and warnings:

(1) This unit shall be connected to the Telecommunication Network through a line cord which neets the requirements of the ACA TS008 Standard.

(2) This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACA . These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:

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

(3) The power supply that is provided with this unit is only intented for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

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.

The warranty is automatically voided if:

1. You, or someone else, use the product, or attempts to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitations of Warranty

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

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

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

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

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

NetComm
ADSL Integrated Gateway
with Wireless
Power
WLAN
LAN
ADSL
NB5580W ADSL Integrated Gateway with Wireless
ADSL Integrated Gateway
NB5580 ADSL Integrated Gateway