

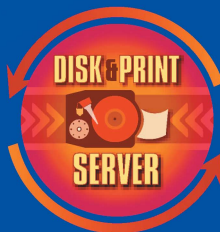
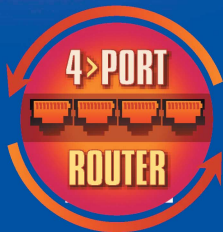
**NetComm**™  
Broadband Solutions

**NB620W** ➤ SUPER-G Wireless Gateway



# SUPER-G Wireless Gateway

- Broadband wireless router for cable or ADSL modems
- Triple Security – NAT, SPI/DOS and WPA
- Web content filtering
- USB 2.0 Host Ports for Disk and Print Serving
- Universal Plug & Play (UPnP)
- Virtual Server/Port Forwarding
- VPN Passthrough
- Easy Configuration & Setup
- Works with all Operating Systems



**NB620W** ➤ **User Guide**

## Legal & Regulatory Information

This manual is copyright. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the Copyright Act, no part may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Limited. NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product.

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 meets 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 direction 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 intended 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.

## Important rules for safe operation

In addition to the careful attention devoted to quality standards on the manufacture of network products, safety is a major factor in the design of every product. However, safety is your responsibility, too. This section lists the gateway and accessory equipment. Please read them carefully before operation and using the gateway.

- Read and follow instructions- You should read all the safety and operating instructions before operating the gateway.
- Retain Instructions- You should save all the safety and operating instructions, for future reference.

- Heed Warnings- Comply with all warning messages on the product and within operating instructions.
- Check Power Sources- Operate this product only from the type of power source indicated on the product's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Be Careful of Overloading- Do not overload wall outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard. Periodically examine the cord, and if its appearance indicates damage or deteriorated insulation, have it replaced by your service technician.
- Protect Power Cords - Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit from the product.
- Check Ventilation - Slots and openings in the enclosure are provided for ventilation to ensure reliable operation of the product and to protect it from overheating. Do not block or cover these openings, never block these openings by placing the product on a bed, sofa, rug, or other similar surface. Never place this product near or over a radiator or heater, or any other heat source (including amplifiers). Do not place this product in a built-in installation, such as bookcase or equipment rack, unless you provide proper ventilation.
- Do Not Use Accessories - Do not use attachments, unless they are recommended by your vendor, as they may cause electrical or fire hazards.
- Use the Recommended Power Adaptor - You must use the power adaptor that comes with your product.
- Do Not Use Near Water - Do not use this product near water. For example, near a swimming pool, bathtub, washbowl, and the like.
- Do Not place near high temperature source - For example near a steamer, kitchen range fire, and the like.
- Use Caution in Mounting This Product - Do not place this product on an unstable surface support. The product may fall, causing serious injury to a child or adult, as well as serious damage to the product.
- Unplug Power Before Cleaning - Do not use liquid cleaner or aerosol cleaner. Use a damp cloth for cleaning.
- Keep Objects Out of Openings - Never push objects of any kind into this product through openings, as they may touch dangerous voltage or "short-out" parts, which could result in a fire or electric shock. Never spill liquid on the product.
- Protect From Lighting - For added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet, and disconnect the cable system. This will prevent damage to the product due to lightning and power line surges.
- Turn Off the Power Switch between DC plugs Off and On.
- Do Not Remove Covers - Do not attempt to service this product yourself, as opening or removing covers may expose you to dangerous voltage or hazards.

Chapter 1 Introduction .....	5
1.1 Product Overview .....	5
1.2 Features and benefits .....	6
1.3 What's in the package? .....	7
1.4 Connecting the NetComm Super-G Wireless Gateway .....	8
1.5 Device .....	9
1.6 Factory Default .....	10
Chapter 2 Configuring your Computers .....	12
2.1 Overview .....	12
2.2 Configuring Windows 98 and Millennium PCs .....	13
2.3 Configuring Windows 2000 PCs .....	15
2.4 Configuring Windows XP PCs .....	17
Chapter 3 Configuring the Wireless Gateway .....	19
3.1 Basic Configuration .....	20
3.2 Advanced Items .....	31
3.3 Management .....	48
Chapter 4 Configuring Printer Sharing .....	53
4.1 Configuring Printer Sharing on Windows98 SE or Millennium PCs .....	53
4.2 Configuring Printer Sharing on Windows 2000 .....	57
4.3 Configuring NB620W Printer Sharing on Windows XP PCs .....	62
Appendix A: Technical Specifications .....	67
Appendix B: Frequent Asked Questions .....	71
Appendix C: Troubleshooting .....	73
Appendix D: DDNS Update Status Messages .....	74
Appendix E: Cable Connections .....	75
RJ-45 Network Ports .....	75
Twisted pair cables .....	75
Straight and crossover cable configuration .....	76
RJ11 connector and cable .....	76
605 to RJ-11 adapter .....	77
USB cable .....	77
9 Pin (RS-232 ) Serial Cable .....	77
Appendix F: Registering your NetComm Product .....	78
Customer Information .....	79
Product Warranty .....	80
Limitations of Warranty .....	81

---

## Chapter 1 Introduction

### 1.1 Product Overview

Thank you for purchasing the NetComm NB620W Super-G Wireless Gateway. The NB620W is a state-of-the-art Wireless Gateway with the latest in advanced broadband wireless connectivity. Now it's simple and cost-effective to build a local network with Internet access using wired or wireless technology.

The NB620W features the latest 802.11g wireless standard for high speed transfer rates up to 54Mbps, as well as a Atheros' Super G mode to turbocharge your transfer rates. The NB620W is backwards compatible with 11Mbps, 802.11b wireless networks and carries a built-in 4 port 10/100 Base-TX Ethernet Switch.

The NB620W introduces three levels of security to keep those intruders and hackers out of your wired or wireless network. The combination of NAT and SPI/DOS (Stateful Packet Inspection/Denial of Service) firewall technology, the latest WEP (Wireless Encryption Protocols) and WPA (WiFi Protection Access – PSK and Radius) ensures the safety of your network PCs and their data.

Working with any Operating System that supports TCP/IP, including Windows, Apple Macintosh and Linux, the NB620W Web-based user interface facilitates easy set up and ongoing administration.

The NB620W also features two USB 2.0 ports for Disk and Print Serving. Simply connect a supported USB 1.1 or 2.0 printer to the built-in USB host and all authorised users can use this printer, via both the LAN and wireless LAN. You can also connect any USB hard or Flash drive to the other USB port to make the data available to authorised users on the local LAN as well as wireless users.

This reference manual assumes that the reader has an installed Ethernet card in the computer to be connected and has basic to intermediate computer and Internet skills. However, basic Computer Networking, Internet, and Firewall technology information is available from the NetComm Web site. See [www.netcomm.com.au](http://www.netcomm.com.au).

## 1.2 Features and benefits

### The NetComm NB620W Super-G Wireless Gateway

- Four 10/100M Base TX ports for PC or LAN connection and one 10/100M Base TX WAN port for broadband connection
- 802.11g Wireless Access Point supports up to 54Mbps
- Atheros' Super G wireless mode – turbocharge your transfer rates.
- Supports automatic hacker pattern detection to block malicious intrusions
- Network Address Translation (NAT) conceals private network from the Internet
- VPN pass through allows secure communication protocols
- Web-based user interface for easy installation, configuration and management
- Virtual Server/Port Forwarding allows outside users to access internal servers via the Internet
- Administrators can block specific users' Internet access by UPI (User Profile Identification)
- Supports UPnP for easy device discovery and advanced Internet applications
- USB 2.0 Host port for LPR Print sharing
- USB 2.0 Host port for file sharing
- 3-YEAR WARRANTY WHEN YOU REGISTER ONLINE

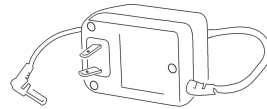
## 1.3 What's in the package?

Your NB620W Package should contain the following items:

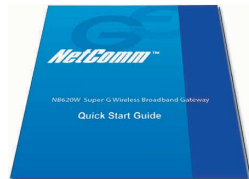
- NB620W Super-G Wireless Broadband Gateway with 4-port Switch



- Power Adapter



- Quick Installation Guide



- Package Contents Note



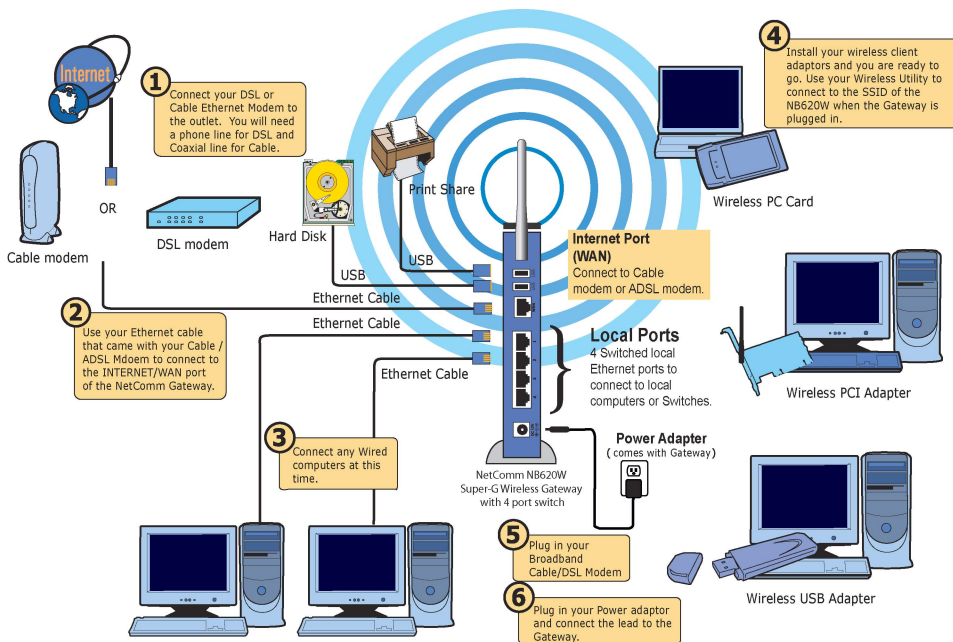
- CRS813 - Manuals and On-Line Tutorial CD



Please contact your dealer if any of the above listed items are missing or damaged.

## 1.4 Connecting the NetComm Super-G Wireless Gateway

A typical Internet access application of the NB620W Gateway is shown below:



### Connecting your Gateway

#### Site Selection

Before installation, select the Wireless Gateway location. Proper placement of the Gateway is critical to ensure optimum radio range and performance. You can use the Site Survey Utility to help you to determine the best location. Typically, the best location to place your Gateway is at the center of your wireless coverage area. Try to place your mobile stations within the line of sight. Obstructions may impede performance of the Gateway.

#### Connect the Ethernet Cables

##### WAN (Internet) Port

Connect to your broadband (Cable Modem or ADSL Modem) access equipment.

##### LAN (Local) Ports

Connect via ethernet cable to your local server or workstations (PCs).

##### Connect the USB printer and storage device

Connect the USB printer and USB storage device to the USB 2.0 host ports, power on the printer and storage device. You can access them right after the Gateway starts up. Please note that you can have one printer and one storage device at a time, two storage devices or two printers will not work on this Gateway.



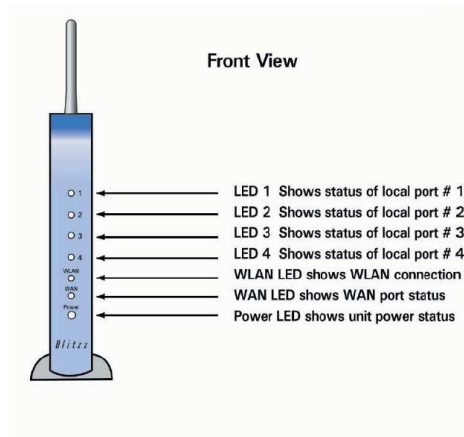
## Connect the Power Cable

Connect the power adapter to the power socket on the Gateway, and plug the other end of the power into an electrical outlet. The Gateway will be powered on and all five indicators on the top panel will flash in sequence to test the functionality of the indicators.

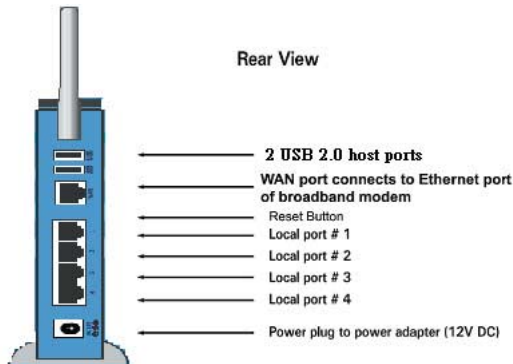
## 1.5 Device

The NB620W has 5 ports and 7 LEDs for connection and administrative purposes.

### 1.5.1 NB620W Front Panel



### 1.5.2 NB620W Back Panel



## 1.6 Factory Default

Reset Button. Press and hold the reset button for more than 7 seconds; the gateway will be restored to factory default values. All of your saved configurations will be gone, so please backup your current configuration before using the Reset Button..

### 1.6.1 Log-in

#### User Name

The default username of the NB620W is "admin".

#### Password

The default password of the NB620W is "admin". It is highly recommended that you setup your own password to prevent unauthorized access to the Gateway's settings.

#### First time login

You can directly access the configuration manager home page after you enter the IP address: 192.168.1.1 and the default username and password.

#### Forgot your password?

If you forget the password, you can reset the device to its factory setting. Press the "Reset" button on the back panel of the NB620W Gateway. Hold the button in at least 10 seconds. The NB620W will revert to its default settings. Then, you can configure the Gateway again.

#### Security

It is recommended that you change the admin password and disable wireless, remote management and UPnP until you require these functions or you take suitable security measures (e.g. Set WEP Keys).

### 1.6.2. Management / Gateway Address

The NB620W gateway address, also the address for management utility, is 192.168.1.1. Please login the Management Utility or setup your gateway on this address. [Please refer to Chapter 3 Configuring the Wireless Gateway for more information.]

If your computer supports Microsoft Universal Plug and Play (UPnP), once the Gateway is plugged into the same physical network, your station will detect it.

## 1.6.3 Default Values

The default values are:

<b>User Name:</b>	admin
<b>Password:</b>	admin
<b>WAN/Internet Port:</b>	DHCP client enabled
<b>Local IP address:</b>	192.168.1.1
<b>Subnet mask:</b>	255.255.255.0
<b>DHCP server:</b>	Enable
<b>DHCP start address:</b>	192.168.1.2
<b>Number of DHCP clients:</b>	128
<b>Wireless:</b>	Enabled
<b>SSID:</b>	NB620W
<b>Channel:</b>	11
<b>Operation Mode:</b>	802.11b/g mixed
<b>WEP security:</b>	No
<b>Remote Management:</b>	Disable
<b>UPnP:</b>	Disable

## Chapter 2 Configuring your Computers

### 2.1 Overview

The instructions in this chapter will help you configure each of your computers to be able to communicate with the NB620W Gateway.

To do this, you need to configure your PC's network settings to obtain an address automatically, so your PC can function as a DHCP client. Computers use IP address to communicate with the Gateway and each other across a network, such as the Internet.



First, find out which Windows operating system your computer is running. You can find out by right clicking My computer on your desktop (if you can not find it on the desktop, click the Start button). Then choose contents in the menu, the system information tells you which operating system you are using.



You may need to do this for each computer you are connecting to the Gateway.

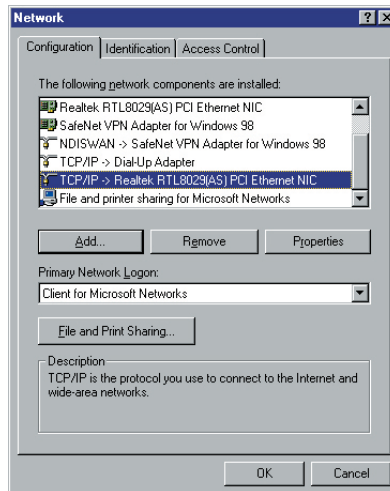
The following pages tell you, step by step, how to configure your network settings based on the type of Windows operating system you are using. Make sure that an Ethernet or wireless adapter (also known as a network adapter) has been successfully installed in each PC you will configure. Once you've configured your computers, continue to "Chapter 3: Configuring the Wireless Gateway".

## 2.2 Configuring Windows 98 and Millennium PCs

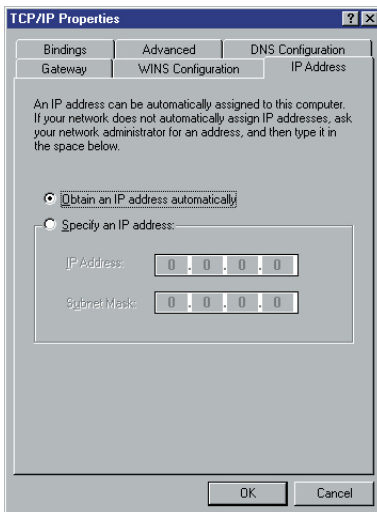
1. Click the Start button. Select Settings and click the Control Panel icon. Double-click the Network icon.



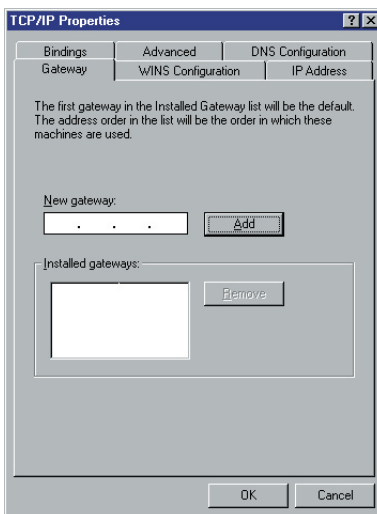
2. On the Configuration tab, select the TCP/IP line for the applicable Ethernet adapter. Do not choose a TCP/IP entry whose name mentions DUN, PPPoE, VPN or AOL. If the word TCP/IP appears by itself, select that line. Click the Properties button.



3. Click the IP Address tab. Select “Obtain an IP address automatically”.



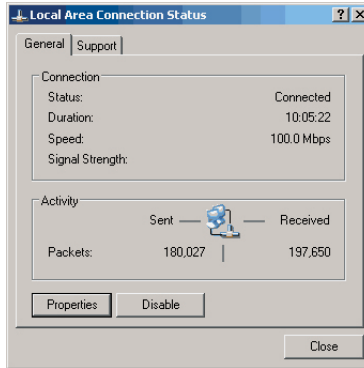
4. Now click the Gateway tab, and verify that the Installed Gateway field is blank. Click the OK button.



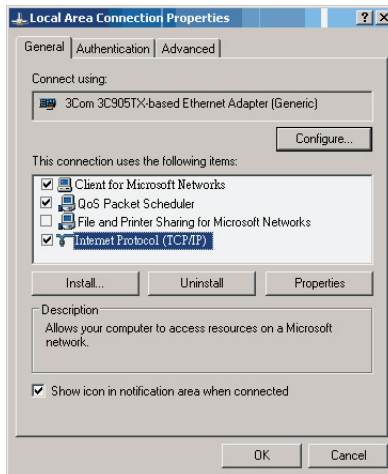
5. Click the OK button again. Windows may ask you for the original Windows installation disk or additional files. Check for the files at `c:\windows\options\cabs`, or insert your Windows CD-ROM into your CD-ROM drive and check the correct file location, e.g., `D:\win98`, `D:\win9x`, etc. (If "D" is the letter of your CD-ROM drive).
6. Windows may ask you to restart your PC. Click the Yes button. If Windows does not ask you to restart, restart your computer anyway.

## 2.3 Configuring Windows 2000 PCs

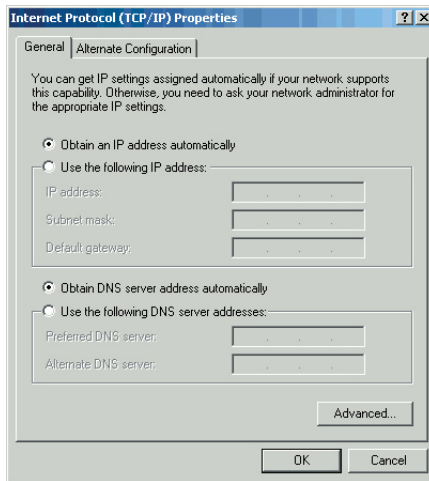
1. Click the Start button. Select Settings and click the Control Panel icon. Double-click Network and Dial-up Connections icon.
2. Select the Local Area Connection icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the Local Area Connection. Click the Properties button.



3. Make sure the box next to Internet Protocol (TCP/IP) is checked. Highlight Internet Protocol (TCP/IP), and click the Properties button.



4. Select Obtain an IP address automatically. Once the new window appears, click the OK button. Click the OK button again to complete the PC configuration.



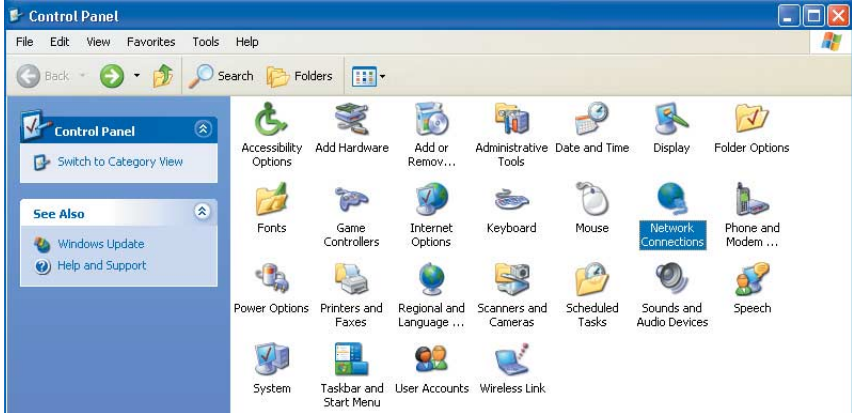
5. Restart your computer.



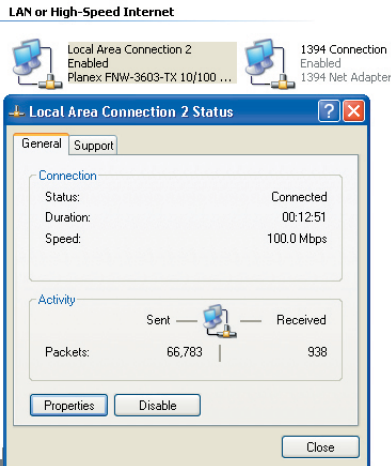
## 2.4 Configuring Windows XP PCs

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

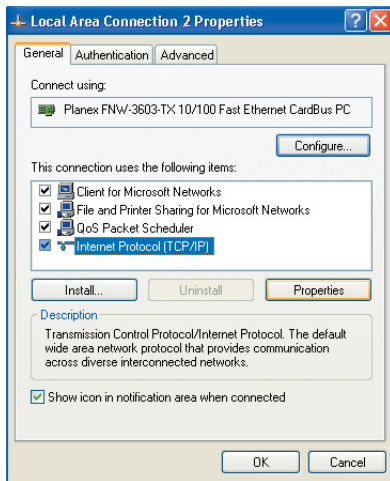
1. Click the Start button and then the Control Panel icon. Click the Network and Internet Connections icon. Then click the Network Connections icon.



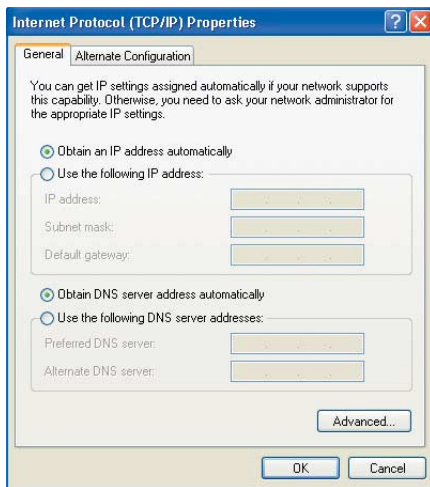
2. Select the Local Area Connection icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the Local Area Connection. Click the Properties button.



3. Make sure the box next to Internet Protocol (TCP/IP) is checked. Highlight Internet Protocol (TCP/IP), and click the Properties button.



4. Select Obtain an IP address automatically. Once the new window appears, click the OK button. Click the OK button again to complete the PC configuration.



After you have obtained an IP address, please access the Gateway by typing `http://192.168.1.1` to configure the Gateway. (If you have changed the route's IP address, please type `http://<the new IP address of the gateway>`.)

## Chapter 3 Configuring the Wireless Gateway

The NB620W Wireless Gateway includes a pre-installed web-based configuration tool, which provides an interface to manage and configure the device to meet the requirements of your network. You can access the Configuration Manager through your web browser from any computer, which has a network connection with the NB620W Wireless Gateway.

### Accessing the Configuration Manager

The Configuration Manager is a number of pre-installed web-based pages in the NB620W Wireless Gateway. To access the Configuration Manager you will need:

- A computer equipped with Ethernet or WLAN network adapter. The IP address of your computer needs to be setup in the same subnet as the NB620W. Just configure your PCs to accept the network information automatically. The NB620W will assign an IP for your PC when connecting. (If you don't know how to setup the IP configuration, please refer to Chapter 2: Configuring your PCs.)
- A web browser installed on the PC. The program is designed to work best with Microsoft Internet Explorer version 5.0, Netscape Navigator version 4.7, or later versions.

You can access the program from any computer connected to the NB620W Wireless Gateway via the LAN or Wireless ports. To login to the Configuration Manager:

- 1.) From any LAN computer, open your web browser and type the following URL in the web address (or location) box. Press <Enter>

**http://192.168.1.1**

A login screen displays:



- 2.) Type "admin" as the user name and leave the password blank if it is your first time logging in. Click on OK get login to the Configuration Manager.

**Note:** You can change the password at any time. For security reason, we recommend you change your password the first time you login.

## 3.1 Basic Configuration

The basic configuration contains Internet Port, Local Port and the Wireless LAN configurations. After you have finished setting up the basic items, the gateway will work for most scenarios.

### 3.1.1 Internet Port

The Internet Port section contains information to allow your modem to connect to the Internet. You will need to configure this section with the settings that have been assigned and provided by your ISP.

#### DHCP Configuration

The DHCP is the default service for the Internet Port section. This means that you will get the IP address from the ISP automatically. Choose this type of Protocol for Optus Cable.

Protocol	<input type="text" value="DHCP(Dynamic IP Configuration for Cable)"/>
Host Name	<input type="text"/>
Domain Name	<input type="text"/>
<input type="checkbox"/> Use Static DNS	
Primary	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Secondary	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
MAC Address	<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>
<input type="checkbox"/> Copy From This PC	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="button" value="Save"/>	<input type="button" value="Undo"/>

**Host Name/Domain Name.** Some cable ISPs require the host name and domain name as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, you can assign your own or leave it blank and it will work.

**Use Static DNS.** If you want to use your own DNS instead of the one provided by your ISP, check this box, and type the IP address of the DNS in the field. (At least one in the primary field.)

**MAC address.** Some ISPs allow you to connect to them with a specified MAC address only. You can enter the MAC address manually or copy it from a PC which is attached to the Local Port. Simply type in its IP address and the gateway will copy the MAC address from that PC. The gateway comes with the factory default MAC address. You do not need to change the default value if the ISP is not checking the MAC address of your Internet Port.

## PPPoE Configuration

Most DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish an Internet connection. If you are connected to the Internet through a DSL line, check with your ISP to see what protocol they use.

### You Are Now In > Internet Port > PPPoE Configuration

Protocol PPPoE (ADSL Dynamic IP Configuration)

Host Name

Domain Name

User Name

Password

Confirm Password

Service Name

Packet Size (MTU) 1492

Disconnect After Idle 0 Minutes

Enable Unnumbered PPP Connection

Local IP Address  .  .  .

Use Static DNS

Primary  .  .  .

Secondary  .  .  .

MAC Address 00 . 02 . D8 . 00 . 00 . 31

Copy From This PC  .  .  .

Save Undo

**Host Name/Domain Name.** Some ISPs require the host name and domain name as identification. If it is not specified, assign on your own or leave it as blank.

**User Name, Password, Confirm Password.** Enter your username, password and confirm again in the fields for the login to the ISP.

**Service Name.** Enter the ISP specified service name or assign one of your own if the Service Name is not specified.

**Packet Size (MTU).** The Maximum Transmission Unit of an IP packet. The default value is 1492 Bytes. If your ISP requires a special value, please select from the pull down menu. The default value will work for most cases. Otherwise, contact your ISP for the MTU value.

**Disconnect after idle time.** The PPPoE connection will be disconnected by the gateway automatically when there is no Internet traffic for the idle time specified. The idle time of “0” means an always-on connection. The default value is “0” minute.

**Enable Unnumbered PPP Connection.** Check this box and enter the IP address of the unnumbered connection. Contact your ISP if you are unsure if this feature is required for your PPPoE connection.

**Use Static DNS.** If you want to use your own DNS instead of the one provided by your ISP, click the checkbox and type the IP address of the DNS in the field. (At least one for the primary field.)

**MAC address.** Some ISPs allow you to connect to them with a specified MAC address only. You can enter the MAC address manually or copy it from a PC which is attached to the Local Port. Simply type in its IP address and the gateway will copy the MAC address from that PC. The gateway comes with the factory default MAC address. You do not need to change the default value if the ISP is not checking the MAC address of your Internet Port.

## Static IP Configuration

If you connect to the Internet using a permanent IP address, please select Static IP Configuration from the pull down menu and fill the ISP specified values in the fields.

**Note:** If your ISP requires a PPPoE type connection, you should NOT use " Static IP Config".

Protocol	<input type="text" value="Static IP Configuration"/>
Host Name	<input type="text"/>
Domain Name	<input type="text"/>
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Submask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Gateway	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Primary DNS	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Secondary DNS	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
MAC Address	<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>
<input type="checkbox"/> Copy From This PC	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="button" value="Save"/>	<input type="button" value="Undo"/>

**Host Name/Domain Name.** Some ISPs require the host name and domain name as identification. If it is not specified, assign on your own or leave it as blank.

**IP Address.** Enter the IP address of the gateway's Internet port. Please use the ISP specified address.

**Subnet mask.** Enter the subnet mask supplied by your ISP.

**Gateway.** Your ISP will assign a gateway address for you. If you can not find one, please contact your ISP.

**Primary DNS.** Enter the domain name server of the ISP.

**Secondary DNS.** The back up domain name server can be left blank if necessary.

**MAC address.** Some ISPs allow you to connect to them with a specified MAC address only. You can enter the MAC address manually or copy it from a PC which is attached to the Local Port. Simply type in its IP address and the gateway will copy the MAC address from that PC. The gateway comes with the factory default MAC address. You do not need to change the default value if the ISP is not checking the MAC address of your Internet Port.

## PPTP Configuration

Some older modems use a PPTP connection instead of PPPoE. This connection uses a PPP session to connect to your ISP. After the connection between the ISP and your modem is established, you are able to use your modem to connect to the Internet.

### You Are Now In > Internet Port > PPTP Configuration

Protocol

Host Name

Domain Name

User Name

Password

Confirm Password

Server IP Address

Subnet Mask

Packet Size (MTU)

Disconnect After Idle  Minutes

Enable Unnumbered PPP Connection

Local IP Address

Use Static DNS

Primary

Secondary

MAC Address

Copy From This PC

**Host Name/Domain Name.** Some ISPs required the host name and domain name as identification. If this has not been specified, assign on your own or leave it as blank.

**User Name, Password, Confirm Password.** Enter your username, password and confirm again in the fields for the login to the ISP.

**Server IP.** Your modem's IP address. You must set your computer to be the same domain as your modem (For example, if your modem's IP address is 192.168.0.1 and the subnet mask is 255.255.255.0, your PC must be configured as 192.168.0.x, where the x is from 2 to 254, and the subnet mask should be same as the modem's 255.255.255.0). You will be able to access your modem. Use "ping <your modem's IP>" in the command line of your PC to test your configuration.. If you don't know the modem's IP address, please refer to the modem's manual or consult your ISP.



**Packet Size (MTU).** The Maximum Transmission Unit of an IP packet. The default value is 1492 Bytes. If your ISP requires a special value, select this from the pull down menu. The default value will work for most cases. Alternatively, contact your ISP for a specified value.

**Disconnect after idle time.** The PPPoE connection will be disconnected by the gateway automatically when there is no Internet traffic for the idle time specified. An idle time of “0” means an always-on connection. The default value is “0” minute.

**Enable Unnumbered PPP Connection.** When unnumbered function is used in PPTP, check this box and enter the IP address of the unnumbered connection. Check with your ISP if you are unsure.

**Use Static DNS.** If you want to use your own DNS instead of the one provided by your ISP, check this box and enter the IP address of the DNS in the field. (At least one for the primary field.)

**MAC address.** Some ISPs allow you to connect to them with a specified MAC address only. You can enter the MAC address manually or copy it from a PC which is attached to the Local Port. Simply type in its IP address and the gateway will copy the MAC address from that PC. The gateway comes with the factory default MAC address. You do not need to change the default value if the ISP is not checking the MAC address of your Internet Port.

## 3.1.2 Local Port

Configure your gateway's Local Port IP address here. The Local Port must be a private IP address. (10.x.x.x, 192.x.x.x are reserved for LAN use).

The screenshot shows the configuration interface for the Local Port. The breadcrumb trail is "You Are Now In > Local Port". The "Private Network" section contains fields for IP Address (192.168.1.1) and Subnet Mask (255.255.255.0). The "DHCP Server" section includes a checked "DHCP Server Enable" checkbox, a Start IP Address field (192.168.1.2), a Number Of IP Address field (128), a Lease Time dropdown menu (24 Hours), a "Setup" button for Static DHCP IP & MAC Address, and a WINS Server field. At the bottom of the form are "save" and "Undo" buttons.

**Subnet Mask.** The subnet mask determines the number of computers that are allowed in this network. A class C network with the subnet mask 255.255.255.0 allows maximum 253 users (the gateway is already using the 192.168.1.1) in your local area network. Usually a class C network is satisfactory for a local network.

**DHCP server.** To enable the DHCP server, please click the check box. The DHCP server assigns dynamic IP address to the clients.

**Start IP address.** Specify the start of the IP address for DHCP users. The default value is 192.168.1.2. (Please make sure there is no fixed IP address within the range you assigned here on the LAN, otherwise the DHCP client cannot get the IP address correctly.)

**Number of IP address.** Assign the number of users allowed to use the DHCP service. The default value is 128 users.

**Lease Time.** A DHCP user's PC gets the IP address with a lease time. When the lease time is expired, the user's PC must connect to the DHCP server to request the dynamic IP address again. When there are lots of mobile users using DHCP service in your network, select an appropriate time to make sure you manage the IP addresses well, because when the user turns his computer off and leaves, the gateway might not be aware of that IP address is vacant, thus that IP address will be idle there until the lease time expired. The default value of the lease time is 168hours.

**WINS Server.** The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter the WINS server's IP Address here. Otherwise, leave it as blank.

**Static DHCP IP & MAC Address.** Click Setup in the Local port configuration page to setup the Static DHCP IP. You can assign a fixed IP address to a DHCP client. Put the PC's IP address and MAC address in the fields and click Add to add it to the list. Use Delete or Delete all to manage the list.

## 3.1.3 Wireless LAN

Click Enable Wireless Access to enable the wireless function of the gateway.

The screenshot shows the 'Wireless Lan' configuration page. The 'Basic' section includes a checked 'Enable Wireless Access' checkbox, an SSID field containing 'NB620W', an unchecked 'Hide SSID' checkbox, a 'Region' dropdown menu showing '--- Select Region ---', a 'Channel' dropdown menu showing '11', and an 'Operation Mode' dropdown menu showing '802.11b/g mixed'. Below this is an 'Enable Wireless Access List' section with an unchecked checkbox and a 'Setup Access List' button. The 'Security Mode' dropdown menu is set to 'Disable'. At the bottom of the page are 'Save' and 'Undo' buttons.

**SSID.** (Service Set Identifier.) The SSID is the network name shared among all points in the wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 characters (use any characters on the keyboard).

**Hide SSID.** The gateway will not broadcast its SSID or the SSID of any device connecting to it. Hiding the SSID makes your wireless network more secure as, unless the wireless user knows the SSID in advance, they cannot connect to the gateway. (Some old wireless LAN cards do not support this function. Please contact your wireless card vendor for new firmware.)

**Region.** Select the region for your location.

**Channel.** Select an appropriate channel from the list. The default channel is 11. All devices in your wireless network must be set to the same channel.

**Operation Mode.** There are four operation modes Auto, Super-G, 802.11b/g and 802.11b only. When in Auto mode, you can use either Super G wireless network interface cards or regular 802.11g wireless network interface cards connect to the gateway. If all wireless clients are using Super G, the gateway will serve the clients at the maximum speed. If one or more of the clients use 802.11g or 802.11b connecting to the gateway, the gateway will be in 802.11b/g mixed mode. At Super-G, the channel will be fixed at 6, the regular 802.11g and 802.11b clients cannot connect to the gateway when in this mode. The default value is in 802.11b/g mixed mode, you can use both 802.11b and 802.11g's wireless network interface card to connect to the gateway. If you want to support only 802.11b, choose 802.11b only.

**Enable Wireless Access List.** Check the box to enable the wireless access control list. Only users in the access list can connect to the wireless network when enabled. Click Setup Access List to configure the list.

**Wireless Security.** It is strongly recommended to use one of the Wireless Security modes to protect your local network.

The gateway supports four different types of security modes for your network: WEP (Wire Equivalence Protection) encryption, WPA (Wi-Fi Protected Access) Pre-Shared key, WPA RADIUS (Remote Access Dial In User Service) and 802.1x RADIUS.

To enable Security Settings, choose one of the security modes you desired.

**WEP:** There are three levels of WEP encryption, 64-bit, 128-bit and 152-bit.

Security Mode

**WEP Security**

WEP Encryption

Key Format

Passphrase

Key 1

Key 2

Key 3

Key 4

The higher the encryption bit, the more secure your network, however, speed is sacrificed at higher bit levels. To utilize WEP, select the desired encryption bit, and enter a passphrase then click generate. You might enter the WEP key in HEX or ASCII form.

**WPA Pre-Shared Key:** There are two encryption options for WPA Pre-Shared Key, TKIP and AES. TKIP stands for Temporal Key Integrity Protocol. TKIP utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers. AES stands for Advanced Encryption System, which utilizes a symmetric 128-Bit block data encryption.

Channel

Operation Mode

Enable Wireless Access List

Security Mode

**WPA Pre-Shared Key Security**

WPA Algorithms

WPA Shared Key

Group Key Renewal  Seconds

To use WPA Pre-Shared Key, enter a password in the WPA Shared Key field between 8 and 63 characters long. You may also enter a Group Key Renewal time between 0 and 99,999 seconds. The default value is 1800 seconds. When the group key renewal time expired, the gateway will change the wireless secret key automatically to enhance the security of the wireless.

Security Mode

## WPA RADIUS Security

WPA Algorithms

RADIUS Server Address

RADIUS Port

Shared Key

Group Key Renewal  Seconds

**WPA RADIUS:** WPA RADIUS uses an external RADIUS server to perform user authentication. To use WPA RADIUS, choose Auto, TKIP or AES for the WPA algorithm, enter the IP address of the RADIUS server, the RADIUS Port (default is 1812) and the shared secret from the RADIUS server.

Security Mode

## 802.1x RADIUS Security

RADIUS Server Address

RADIUS Port

Shared Key

Group Key Renewal  Seconds

**802.1x RADIUS:** The 802.1x RADIUS utilizes a RADIUS server for authentication. To utilize RADIUS, enter the IP address of the RADIUS server, the RADIUS Port (default is 1812) and the shared secret from the RADIUS server.

## 3.2 Advanced Items

The gateway's advanced configuration allows you to manage your gateway.

### 3.2.1 Advanced Setup → → → Access Control List

The Access Control List allows you to define Internet access rules for LAN users.

Pass  Block

**Schedule**  
 Always  By Schedule  
 Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday  
 Time Period  To   
 Time Period  To

#	Application	Server IP Address
*****	Please Select You Want	*****

**User Group.** All LAN users can be defined and divided into several groups; each group can have different Internet access behavior depending on your configuration. To define the user group, click Define Group. (Define Group options are introduced below.)

**Service.** Select service from the pull down menu and specify the services you want to offer or block to the users. If you can not find the service you require, click Define Application. (The Define Application options are introduced below.)

**Pass / Block.** Click the radio button to define whether this group user's access from the application to the Internet should be forwarded or blocked.

**Schedule.** Rules can be applied using a schedule that you can define. The radio button Always means the rules are running all the time. By schedule means the rules are applied to the times and days you click below.

Monday thru Sunday allows you to select the days that you want the access control to be active.

When an access control rule is successfully added, it will be appended to the list. Use the Delete or Delete all tabs to manage the list.

## Define Group - Options

Group Name

Every IP Address

This IP Address  .  .  .

IP Address Range  .  .  .  To  .  .  .

#	IP Address
***** Please Select You Want *****	

**Group Name.** Define a group name for each group such as 'sales', 'R&D' or 'accounting'. Click the radio button to choose which IP addresses you want to include in this group.

**Every IP address.** Selecting this will include all the IP addresses in your network.

**This IP address.** To specify the IP addresses one at a time, simply type in the IP address you want to add into the fields.

**IP Address Range.** For a range of IP addresses, specify the starting and ending ranges of the IP addresses into the fields.

Click Add to add your settings to the list. You can check all your IP address settings in this group by watching this list. To manage the list, click on the rows in the list, and then click delete. Click Delete All to delete all IP address from the list.

After you have defined the user groups, return to the Access control list menu.



## Define Application - Options

Application   
 Protocol    
 Port Range  Single  Range  
 Port Number  To

#	Application	Protocol	Ports
*****	Please Select You Want		*****

**Application name.** Define the name of the application you want to define.

**Protocol.** Select TCP or UDP for the protocol of the application.

**Port Range.** Define the port range, either Single or a Range, and then put the port number into the fields. Click Add to finish the setting. You can check the applications you have already defined in the list. Use the Delete or Delete all tabs to manage the list.

After you have defined your applications, please return to the Access Control List menu, and choose the application from the pull down menu.

## 3.2.2 Advanced Setup → → Content filtering

The content filtering feature allows you to block users from browsing certain web-sites or downloading specific file types.

You Are Now In > Advanced Setup > Content Filtering

Keyword

**Keyword**

Block URLs By Keyword  
 Block URLs With IP Address  
 Block Java Applets  
 Block ActiveX Controls  
 Block Cookies

Block Download Executable Files With Extension:  
 .bat  .com  .dll  .exe  .pif  .scr

Block Download Compressed Files With Extension:  
 .arc  .arj  .cab  .rar  .sit  .zip

Block Download Audio/Video Files With Extension:  
 .asf  .au  .avi  .mov  .mp3  .mpeg  .mpg  
 .ra  .ram  .rm  .wav  .wm  .wma  .wmv

**Schedule**  
 Always  By Schedule  
 Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday  
Time Period  To   
Time Period  To

Trust User  .  .  .

**Block URLs By Keyword.** Type the key words in the field Keyword then click add. Check the box to active the URL blocking function. Use delete or delete all to manage the list of keywords.

**Block URLs With IP Address.** Check this box to block users typing IP addresses in the URL field.

**Block Java Applets.** This setting will block all Java applets sent from the web site you are visiting or external web sites.

**Block ActiveX Controls.** This setting will block all ActiveX controls sent from the web site you are visiting or external web sites.

**Block Cookies.** This setting will block all cookies sent from the web site you are visiting or external web sites.

**Block Downloading Files with Extension.** Check the file types you want to block the users from downloading.

**Schedule.** To enable filtering functions by schedule, select the day and time.

Choose Always to enable the filtering all the time.

**Trusted users.** Type in the trusted user's IP in the field. The trusted user will not be affected by any defined content filtering rules.

## 3.2.3 Advanced Setup →→→ Dynamic DNS

The gateway offers a Dynamic Domain Name System (DDNS) feature. The DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other servers behind the gateway. Before you can use this feature, you need to sign up for DDNS service at [www.dyndns.org](http://www.dyndns.org) or other DDNS service providers.

Enable Dynamic DNS

**DDNS Account**

Choose From List

Enter Your Account Name

User Name

Password

Wildcard Enable

Mail Exchanger   Backup MX

Update Status : **STS**

**Enable Dynamic DNS.** Check the box to enable the DDNS service.

**DDNS Account.** The hostname you want to use. Type the first part of the name in the input box, and select the second part of the name from the pull-down menu. This allows you to have anything.dyndns.org, anythingelse.homeunix.com, etc.

**User Name, Password.** These DDNS services require you to login, please enter your DDNS registered name and password here.

**Wild Card Enable.** If you want 'anything\_here.yourhost.dyndns.org' to work (i.e. for addresses like [www.yourhost.dyndns.org](http://www.yourhost.dyndns.org)), check the Enable Wildcard box.

**Mail Exchanger.** If you wish to use a mail exchanger, put its hostname into the Mail Exchanger field.

**Backup MX.** If you need to backup the Mail Exchanger's address while you login to the DDNS service provider every time, please click the checkbox.

**Update Status.** Returns the status of your DDNS service- please check the status of the DDNS service here. If you received an error message from a problem other than your configuration, please contact your DDNS service provider. Please refer to the Appendix E for all Update Status messages.

Click the "Update" to check your current status of the DDNS service, or click "Refresh" to refresh the web page displayed.

### 3.2.4 Advanced Setup →→→ Firewall

**DoS Attack Threshold.** When the gateway suffers a continuous attack from the Internet (Which is considered an abnormal connection that makes many connection requests in a limited time to consume or exhaust the memory of the gateway.), the gateway will drop this traffic from the attack sources instead of responding to them like normal internet traffic. Please select your own threshold bandwidth from the attack source on the Internet by clicking the radio button (Normally when you have less bandwidth to the Internet, you will have a correspondingly smaller DoS Attack Threshold.) Otherwise the DoS function will not work properly.

**DoS Attack Threshold**

2 Mbps Or Above
  1-2 Mbps
  Under 1 Mbps

E-Mail Alarm

Block Request From Wan Port  
 Block Ping From Wan Port  
 Block PPTP, L2TP, IPSec Request  
 Block UPnP Request From Wan Port  
 Use This DMZ Host  .  .  .

**Block Request from WAN Port.** The block request from WAN port feature reinforces your network security by hiding your network ports; this makes it difficult for others to intrude onto your network. This feature is enabled by default. However, if you host servers on your LAN, you cannot enable this feature since it will block users from the Internet from reaching servers on your LAN.

**Block Ping from WAN port.** This feature can prevent your network from being "pinged", or detected by other Internet users.

**Block PPTP, L2TP, IPSec Request.** This feature blocks all VPN connection requests from hosts outside your network.

**Use the DMZ host.** The DMZ feature allows one local network user to be exposed to the Internet to use special-purpose services, such as Internet gaming or videoconferencing. DMZ forwards all the ports to this computer, exposing it entirely to the Internet. This is not recommended for extended uses.

Enable Email Alarm

Mail Server  Port No.

Subject

Send Mail To

Return Address

**E-Mail Log**

Log Full  Everyday

Time

The E-mail alarm feature enables you to receive the gateway access log through emails regularly. Click the checkbox, if you want to receive these e-mails from the gateway.

**Mail Server.** This is the e-mail server address on your network or on the Internet. The mail server specified should relay your mails without user name and password login, otherwise the mail cannot be sent. The standard SMTP port for sending e-mails is 110. Change it if you have special settings, otherwise leave it as the default.

**Subject.** The subject you enter will appear as the subject of the e-mails that the gateway will send to you. This allows the user to identify by subject which mail is from the gateway.

**Send mail to.** Please enter your e-mail address or the e-mail address you want the gateway send to.

**Return address.** If your gateway cannot send to the recipient successfully and is bounced back, or users want to be able to reply to the message through e-mail, then this address will be where the mail is sent to.

**E-mail log.** You can specify the behavior of the gateway when sending e-mail logs. By clicking the radio button "Log Full", the e-mails will be sent only when the log stored in the gateway is full. The other option "Everyday", will have the gateway send e-mails on a daily basis, whether there are messages or not.

**Time.** Please specify the time you would like the gateway to send these e-mails everyday.

## 3.2.5 Advanced Setup →→→ Remote Management

User Name

Password

Confirm Password

Enable Management Via Wan Port    Web Port

Allow Management Form PC

MAC Address 1 -----

MAC Address 2 -----

Send System Log To This PC    ...

**User Name, Password, Confirm Password.** You can change the user name and password of the gateway here. Type in your new user name, then your password and confirm it. Click save to change the username and password. To increase protection, please use passwords of more than 6 characters and no simple phrases. After you changed the user name and password, the gateway will require you to login with the new user name and password immediately.

It is strongly recommended you change the user name and password from the default value to your own setting when you first access the gateway. The default value is very easy for unauthorized persons to guess.

**Enable Management from WAN port.** The remote management feature can be enabled or disabled by checking this checkbox. When enabled, the user from the Internet can configure the gateway via the web.

**Web Port.** The well-known port for web access is 80; if you have your own web site on your LAN for Internet access, please assign another number that is unique to your virtual server settings so that other users do not stumble onto your remote WAN management screen.

**Allow Management From PC.** Check this box to restrict management access from the LAN. Only the PC with the MAC address you specify here can manage the gateway. If you key in the wrong MAC address and press "Save" by mistake, your PC will lose access to the gateway. If this happens, you will need to press the reset button (on the rear side of the gateway) for 5 seconds to restore the gateway to its factory default values.

**Send System Log To this PC.** The gateway will send the system logs to the PC with the IP address specified here.

## 3.2.6 Advanced Setup →→→ Static Routes

Destination Network / Host  .  .  .

Subnet Mask  .  .  .

Gateway  .  .  .

Add Undo

#	Dest. Net/Host	Subnet Mask	Gateway	Interface

Delete All Delete

When you have more than one network on your LAN, and you want to route certain IP addresses of the network to another network, add them into the static routing table.

**Destination Network / Host.** The destination network is the address of the remote network or host, which you want to assign a static route to.

**Subnet Mask.** The Subnet Mask determines which portion of a destination IP address is the network portion, and which portion is the host portion.

**Gateway.** This is the IP address of the gateway device that allows for connection between the Gateway and the remote network or host.



## 3.2.7 Advanced Setup →→→ UPnP

Enable UPnP

Save

**Enable UPnP.** To enable UPnP click the checkbox. UPnP is a function that allows the gateway to self-discover, self-configure and communicate easily with other devices on the network.

## 3.2.8 Advanced Setup → Virtual Server

The virtual server allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

You Are Now In > Advanced Setup > Virtual Server

Application:

Server IP Address:  .  .  .

#	Application	Server IP Address

**Application.** Choose the application in the pull down menu; if you cannot find the application you want in the list, please click the Define Application button to define one of your own.

**Server IP address.** Enter the server address for the application you selected above. Then click Add to proceed. It will then be shown in the list.

### Define Application - Options

Application:

Protocol:

Port Range:  Single  Range

Port Number:  To

#	Application	Protocol	Ports

Some applications need specified ports opened for Internet connection, such as games, Instant Messengers and so on.

**Application.** Type in the application name that is easy to remember and identify.

**Protocol.** Select TCP or UDP. If you are not sure which one to use, check the application manual.

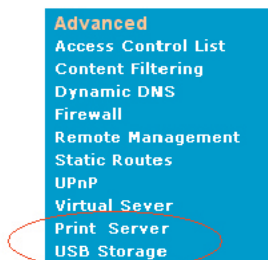
**Port Range.** Choose Single if there is one port to be opened, or choose Range for a range of port numbers.

**Port Number.** Type in the Port number or Port range.

Click Add to finish your setting and it will be updated to the list.

## 3.2.9 Advanced Setup → → Print Server

In NB620W's advanced menu, you will see the Print Server and USB Storage option.



When there is no Printer connected to the Gateway's USB port, or if the power to that printer is off, the printer status shows Model name: None and Status: Off-Line.



To install a printer, use a USB cable and connect the printer to either one of the USB ports. Power on the printer. You will see the Printer Status change in the printer status field. If the printer is still not identified, please check the USB cable and power supply of the printer.

The default port for the print server is 515. If you want to change it, please use a port number which is larger than 1024, otherwise that might conflict with other services. Click Save to save the settings if you have changed the LPD Server Port.



### 3.2.10 Advanced Setup → USB Storage

When there is no USB storage device hooked up to the NB620W Gateway, you will see the status all shown with Not Available or Not Attached. The Super User can create and delete files or directories, while a regular User can only upload or download files. After you finished the configurations, click Save.

You Are Now In > Advanced Setup > USB Storage

---

**Storage Status**

Device Vendor : N/A  
 Device Product : N/A  
 Disk : N/A  
 Disk Status : No Attached Disk

---

**FTP Server Configuration**

FTP Server  Port  (Default Is 21)  
 MAX User Login   
 Connection Timeout  Minute  
 Anonymous Account Login   
 Remote Access From WAN

---

**FTP Server User List**

UserName	Password	MaxLogin	Policy
<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="B"/>

(B:Browser D:Download U:Upload C:Create E:Delete)

#	UserName	Password	Max.Login	Policy

To hook up a USB storage device, you just need to connect the USB cable to either one of the USB host ports available on the NB620W Gateway. You will see the Storage Status change shortly. If the device is not detected, please check the USB cable link. If the USB storage device does not have an external power, please make sure the device consumes power lower than 2.5W. If the device is still not detected, please use an external power for the USB storage device.

## Storage Status

Device Vendor : DMI  
Device Product : USB 2.0 Storage Adaptor  
Disk Vendor: FUJITSU Model: MHN2200AT  
Disk Status : **Connected.**  
Please Press Unload Button First Before Unplug USB Storage.

Remove Disk

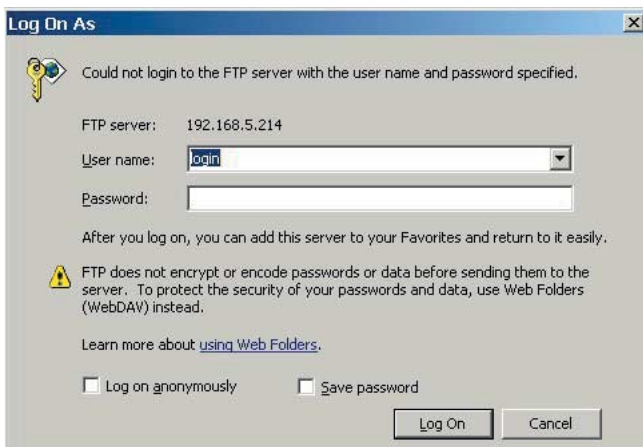
To remove the USB storage device, please click Remove Disk button. Wait until the Disk Status changes to Disconnected. You can then unplug the cable from USB host ports of the Gateway. If you click Remove Disk while there are users still accessing the storage device, you will be advised that it cannot be removed. Wait until noone is accessing the storage device and you can then you can click Remove Disk again to remove the USB storage.

## Storage Status

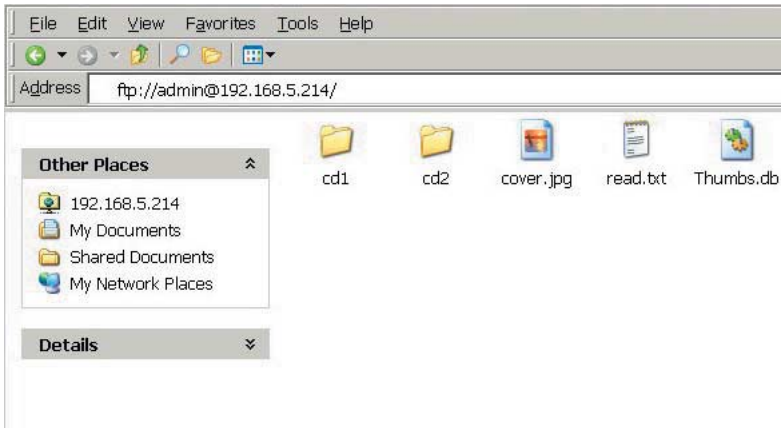
Device Vendor : DMI  
Device Product : USB 2.0 Storage Adaptor  
Disk Vendor: FUJITSU Model: MHN2200AT  
Disk Status : **Disconnected.**  
You Can Unplug USB Now.

Remove Disk

To access the storage, use the browser, type FTP://[user name]@[Internet IP] in the address field. You will see a popup login screen. You may login as the super user or the regular user.



After logged in, you will see the listed files and directories on the storage device.



When you login with Super User, you can create and delete files or directories, while a regular User can only upload or download files.

**Max User Login.** The Gateway allows a total of 8 users (including super user, regular user, and anonymous user) to access the storage device simultaneously.

**Connection Timeout.** The amount of time that a user can be connected before it wil timeout..

**Anonymous Account Login.** Allow users to login without any authorization.

**Policy.** To classify user what is allowed or denied.

## 3.3 Management

These management features are provided to allow you to effectively manage your gateway.

### 3.3.1 Management Access Log

Date/Time	Source	Destination Name	MAC	Protocol
2003/9/18 12:00 PM	211.21.90.92/1234	192.168.5.51/80	11-22-33-44-55-66	TCP

Refresh

The Access Log allows you to browse the gateway's traffic after a period of time and then log the records to files for future reference. (Need access log software? Please look though APPENDIX F SYSLOG SOFTWARE). Click the Refresh button to renew the list for the most current records.

### 3.3.2 Management Factory Reset

Click the Reset button to set all configurations to factory default.

(Please push the reset button at the rear side of the gateway for 7 seconds to reset the gateway.)

Reset Router To Factory Default 

The default values are:

<b>User Name:</b>	admin
<b>Password:</b>	admin
<b>WAN/Internet Port:</b>	DHCP client enabled
<b>Local IP address:</b>	192.168.1.1
<b>Subnet mask:</b>	255.255.255.0
<b>DHCP server:</b>	Enable
<b>DHCP start address:</b>	192.168.1.2
<b>Number of DHCP clients:</b>	128
<b>Wireless:</b>	Enabled
<b>SSID:</b>	NB620W
<b>Channel:</b>	11
<b>Operation Mode:</b>	802.11b/g mixed
<b>WEP security:</b>	No
<b>Remote Management:</b>	Disable
<b>UPnP:</b>	Disable



## 3.3.3 Management → Firmware Upgrade

File Name  Browse

Upgrade Undo

---

Firmware can be upgraded by clicking the Upgrade button after browsing for the firmware, which you can download from the NetComm website when available. Do not upgrade your firmware unless you are experiencing problems with the gateway. After a successful upgrade, the modem will reboot by itself, you current page will be reloaded to the first page of the configuration.

## 3.3.4 Management → → Network Status

The network status shows the Service Type, IP address, Subnet mask, Gateway, DNS and MAC address of your WAN.

### Internet

<b>Wan Protocol :</b>	Static IP
<b>PPPoE Connection Status :</b>	Link Down
<b>PPPoE Connection Time :</b>	
<b>IP Address :</b>	211.75.41.42
<b>Subnet Mask :</b>	255.255.255.248
<b>Gateway :</b>	211.75.41.41
<b>Primary DNS :</b>	168.95.1.1
<b>Secondary DNS :</b>	168.95.192.1
<b>Domain Name :</b>	
<b>MAC Address :</b>	00:01:38:13:22:49

Refresh

Connect/Release      Disconnect/Renew

Session List      User List

**Refresh.** Click this button to display the latest information.

**Connect/Renew.** When using PPPoE or PPTP, you can click this button to establish a connection to the Internet port.

**Disconnect/Release.** Click here to break the Internet port connection.

When using DHCP, please click Disconnect / Release to release your current IP address, and click Connect / Renew to get a new IP address from the DHCP server.

### User List

IP	MAC IP	Host Name	Expire Time
192.168.5.10	00-02-A8-00-00-01	Test	Expire

Refresh

The user list shows users who are using the DHCP service, including their IP address, MAC address, Host Name and the Expiration Time of the leased IP address. Click Refresh to update the latest users list.

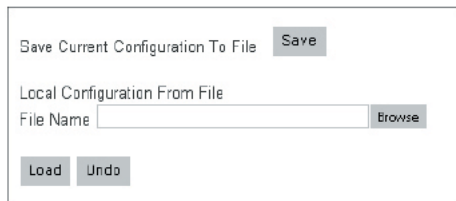
## Session List

UDP/TCP	Src.IP	Port	Dest.IP	Port	Timeout
TCP	192.168.5.27	3071	192.168.5.254	80	9
UDP	192.168.5.168	3027	168.95.1.1	53	170
TCP	192.168.5.240	1428	168.95.4.73	110	144
TCP	192.168.5.43	1637	206.16.0.113	80	17
TCP	192.168.5.168	3289	204.71.201.141	80	67
TCP	192.168.5.43	1639	206.65.183.140	80	27
TCP	192.168.5.168	3290	204.71.200.37	80	82
TCP	192.168.5.43	1672	192.168.5.254	80	48
TCP	192.168.5.43	1654	216.73.85.29	80	77
TCP	192.168.5.43	1670	192.168.5.254	80	48

[Previous](#)[Next](#)[Refresh](#)

List the sessions currently established. By watching the session list, you will be able to observe who is using the Internet service, what type of services are used and other information for you to monitor your network. The session list also helps you to debug Internet connection problems. Click Previous or Next to browse for the whole list.

## 3.3.5 Management →→ Save Configuration



Save Current Configuration To File

Local Configuration From File

File Name

To save your current configuration in a file on your PC, click the Save button. The system will then prompt you to choose the path for the configuration file being saved. Click Save to proceed. To load a saved configuration file from the PC, click Browse then choose the path and the file. Click Load to proceed. After a successful load, please power cycle the gateway (unplug the power core then plug back in.).

## 3.3.6 Management →→ Time



Time Zone

Use Daylight Saving Time

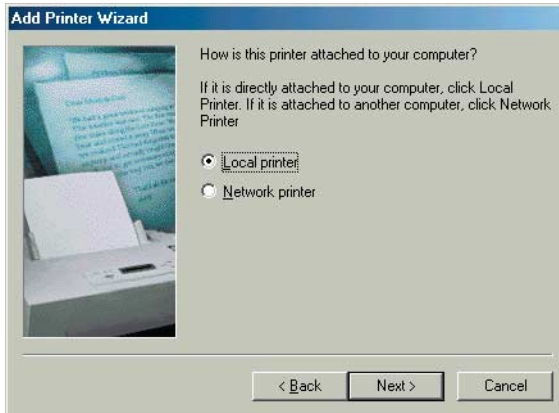
Current Time:

Change the time zone to the area you reside in. The default value is the GMT-8.00 Pacific Time (USA/Canada). When in the daylight saving period, please check the Use Daylight Saving Time box.

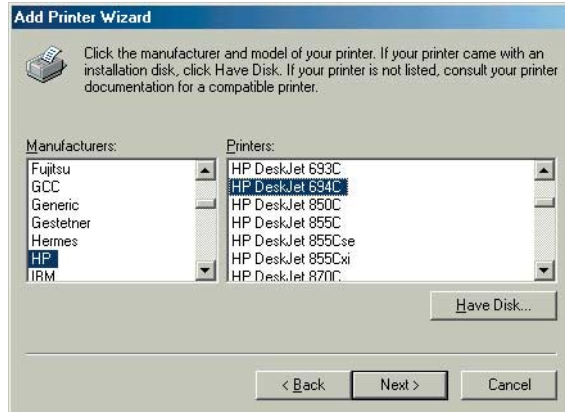
## Chapter 4 Configuring Printer Sharing

### 4.1 Configuring Printer Sharing on Windows98 SE or Millennium PCs

1. After you have installed the third party print monitor system, run the Add Printer Wizard from Start -> Setup -> Printers -> Add a Printer. Select Local Printer and then click Next.

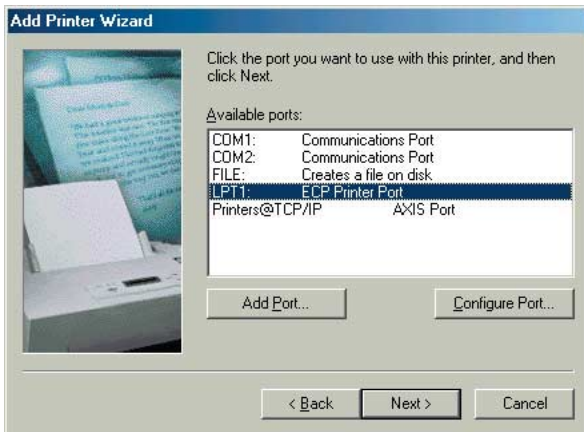


2. Select the printer manufacturer and type that you want to hook up with the NB620W to install the driver or click Have Disk for the drivers on your disk or a CD-ROM.



- Note:** Microsoft Windows 98 or ME does not support the LPR protocol which is needed to enable the printer serving function of NB620W to operate. If you are using Windows 98 or ME, you must install a third party LPR Utility driver to allow Windows 98 or ME to redirect your print job to an IP address. Please visit <http://www.axis.com/techsup/software/> to download their free Print Monitor for Windows. If you are running a Windows 2000 or XP system, you will not need this third party utility as these two operating systems support the LPR Protocol as standard.

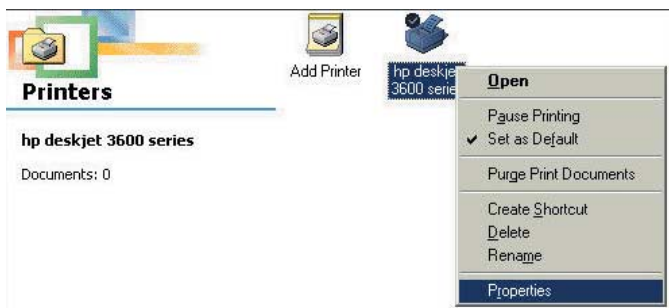
3. When you see this page, click LPT1 ECP Printer Port and then Next



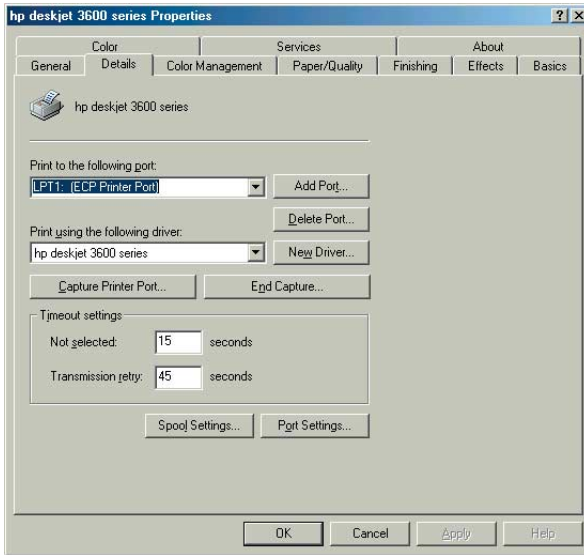
4. Type the name for the printer and then click Finish.



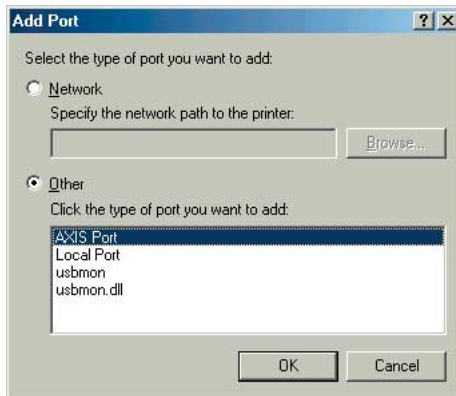
5. After completing the above steps, go to Start->Settings->Printer and right click on the printer you just added. Select Properties.



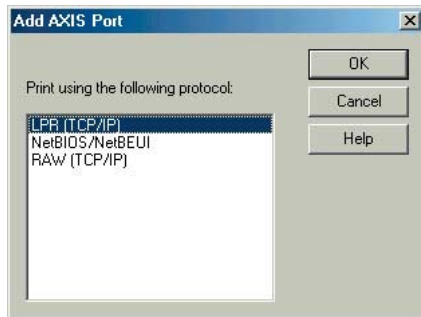
- Click on Details Tab and then click the Add Port button.



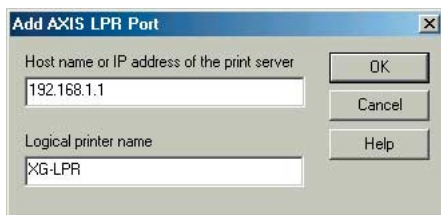
- Click on Other, select NB620W Port and then click OK.



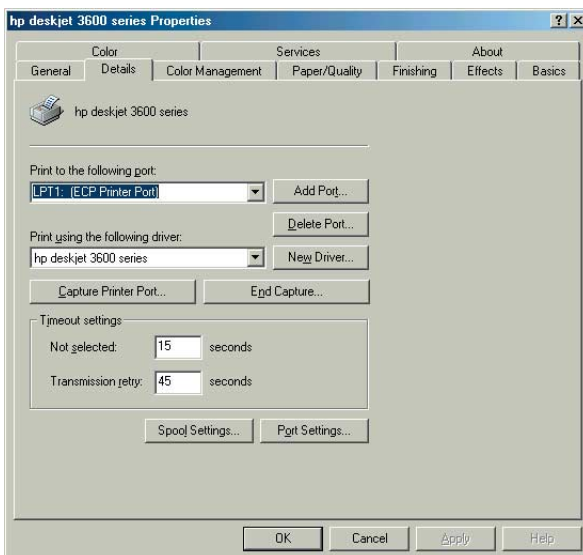
8. Select LPR (TCP/IP) and then click OK.



9. Type in the NB620W's IP address or host name (print server's IP address) in the Host name or IP address of the print server field and give it a name in the field Logical printer name. Click OK.



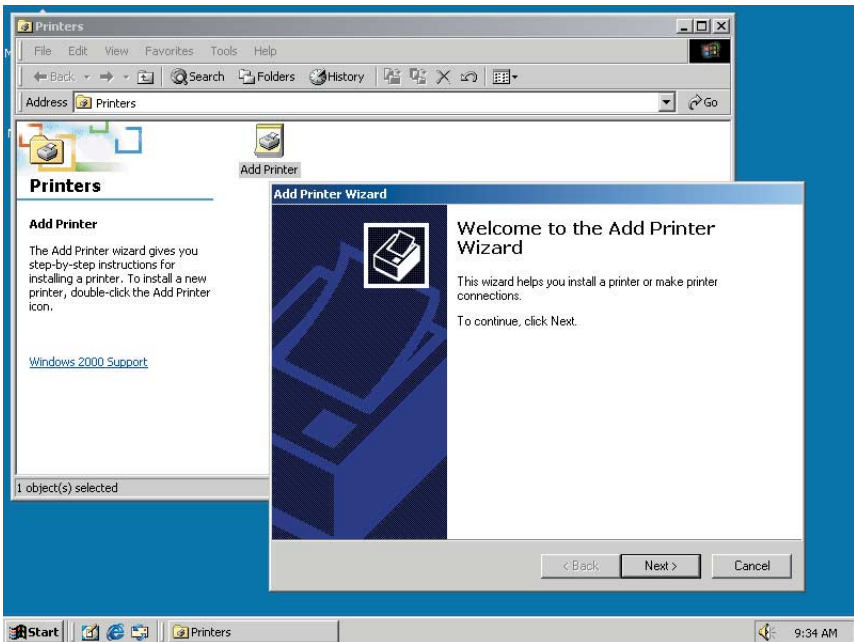
10. After you have added a new printer with a new port, select the printer name and port from the “Print to the following port” pull down menu. Finally, click OK to finish the configuration on Windows98 or ME. Now you can use the printer via the NB620W Gateway.



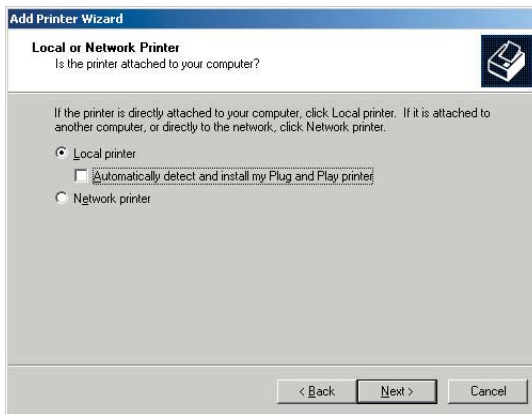


## 4.2 Configuring Printer Sharing on Windows 2000

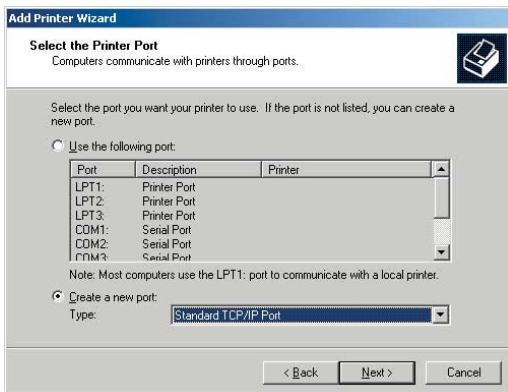
1. Please go to Start -> Setup -> Printers -> Add Printer, and click Next.



2. Choose Local printer and uncheck the box “Automatically detect and install my Plug and Play printer” and then click next.



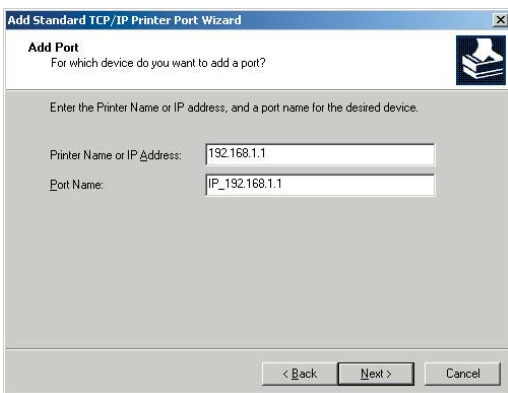
3. Click “Create a new port” and select Standard TCP/IP Port from the list then. Click Next.



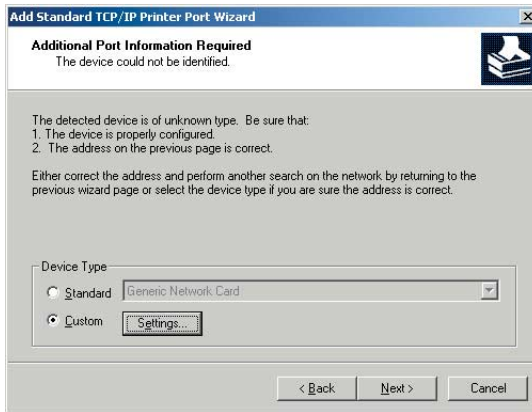
4. Click Next.



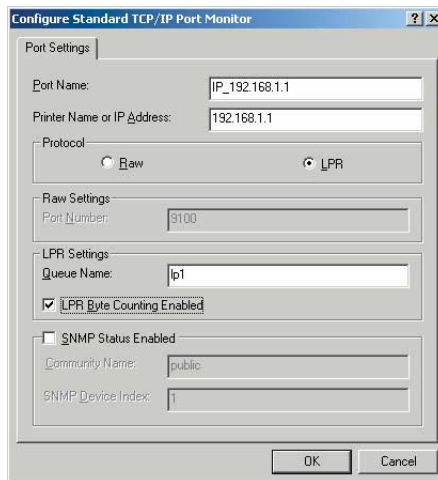
5. Type in the IP address or NETBIOS name of the NB620W Gateway in the Printer Name or IP Address field. The Port Name will be generated itself. Click Next.



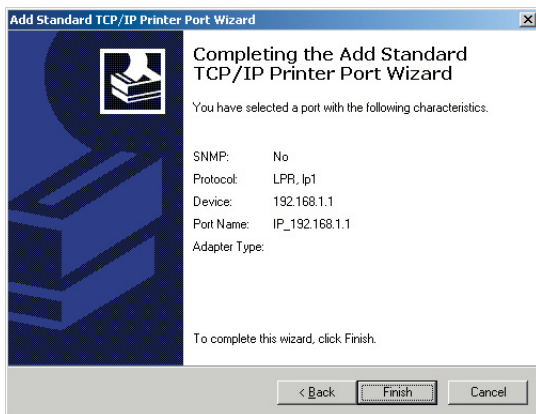
- Choose Custom and click the Settings button.



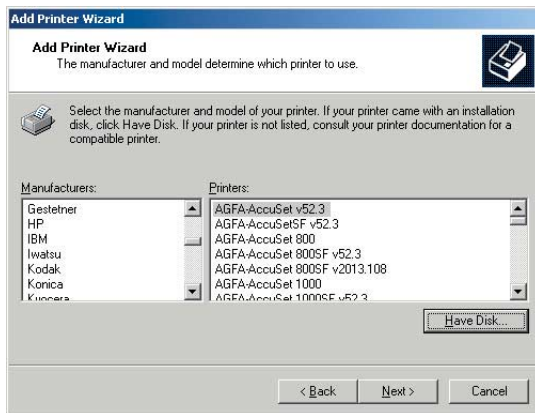
- In the Protocol field, click on LPR protocol, and give it a queue name such as “lp1” (can be any). Check the LPR Byte Counting Enabled box. Click OK.



8. Click Finish.

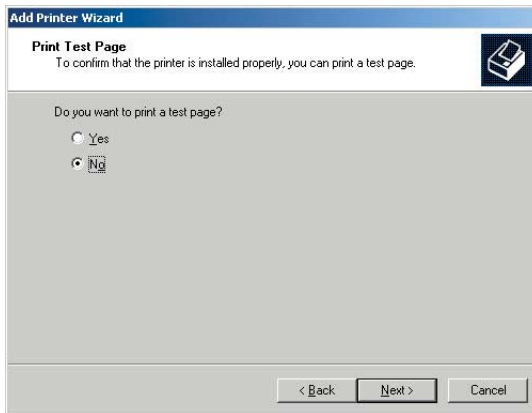


9. You have selected your printer port and protocol, and now you need to install the printer driver on your PC.

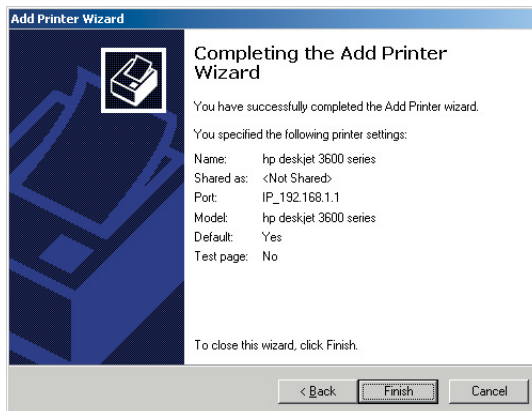


Click Have Disk if you can not find your printer model listed and use the driver CD that came with the printer.

10. You can click Yes to print out a test page or click No to save paper and ink.



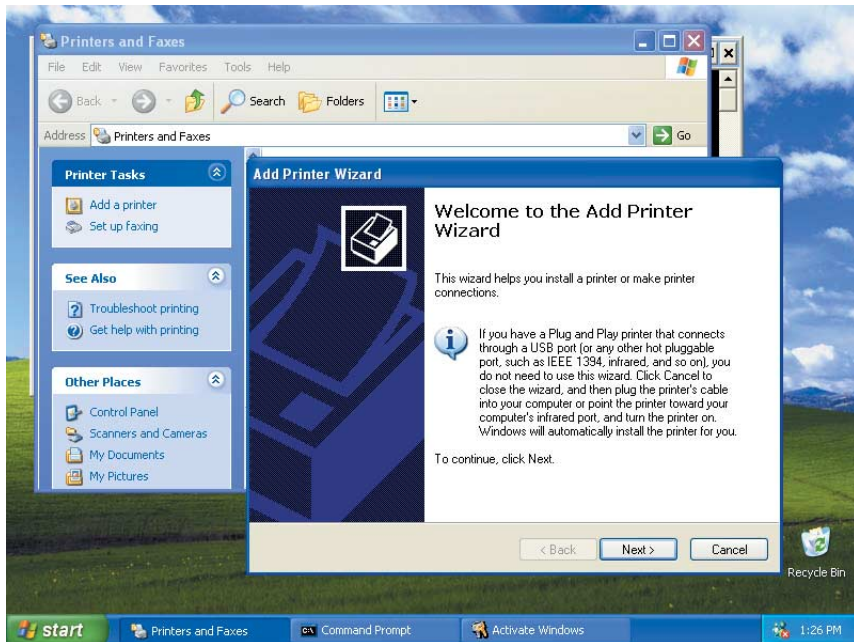
11. Then click Next.



12. Click Finish. The Setup is completed. You can use the printer that is hooked up to the NB620W Gateway's USB port.

## 4.3 Configuring NB620W Printer Sharing on Windows XP PCs

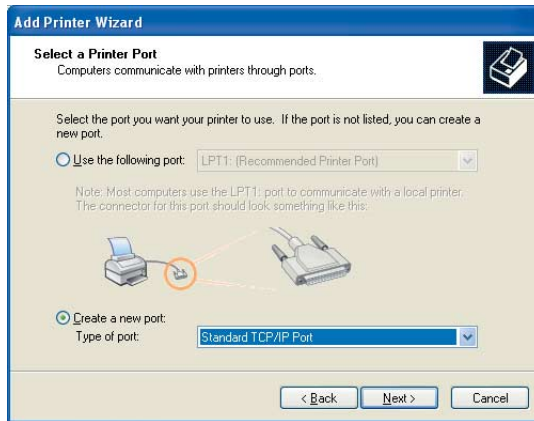
1. Please go to Start -> Setup -> Printers -> Add Printer, and click Next.



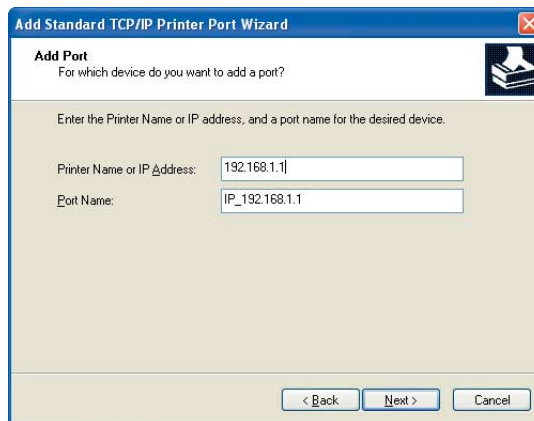
2. Choose Local printer and uncheck the box “Automatically detect and install my Plug and Play printer?” and then click next.



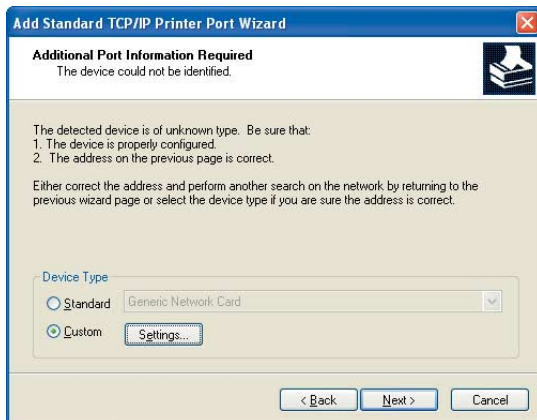
- Click Create a new port and select Standard TCP/IP Port from the list and then click Next.



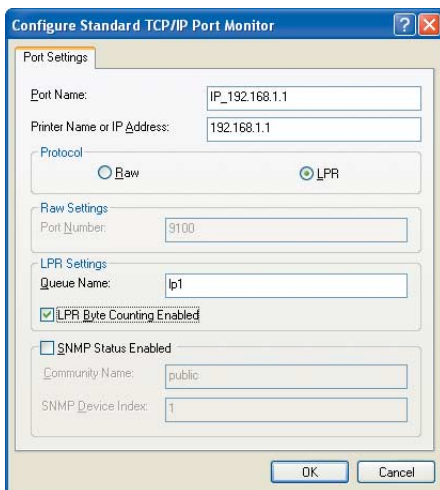
- Click Finish.
- Type in the IP address or NETBIOS name of the NB620W Gateway in the Printer Name or IP Address field. The Port Name will be generated itself. Click Next.



6. Choose Custom and Click the Settings button.

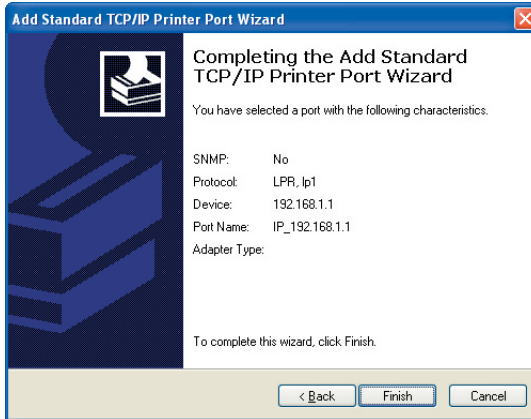


7. In the Protocol field, click on LPR protocol and give it a queue name lp1 (can be any). Check the LPR Byte Counting Enabled box. Click OK.

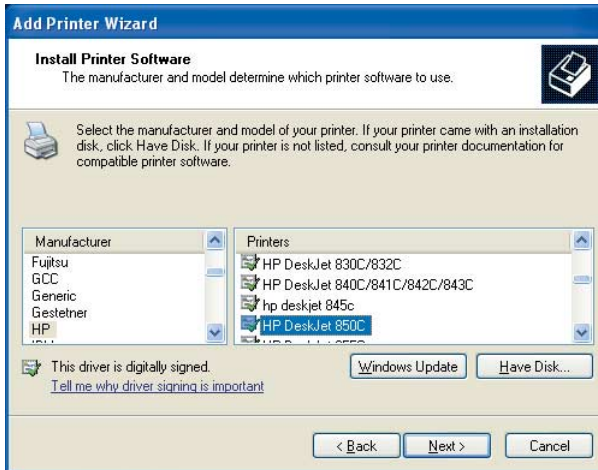




- Click Finish.

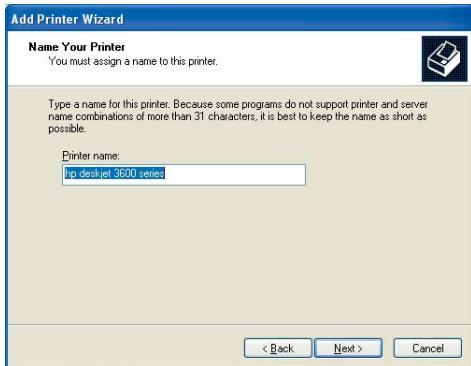


- You have selected your printer port and protocol. Now you need to install the printer driver on your PC.

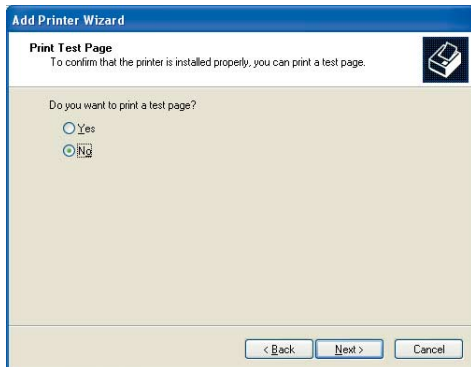


Click Have Disk if you can not find your printer model listed and use the driver CD that came with the printer.

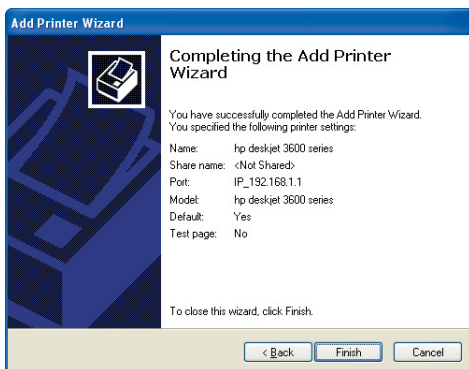
10. Give the printer a name, and then click Next.



11. You can click Yes to print out a test page or click No to save paper and ink. Then click Next.



12. Click Finish. The Setup is completed. You can use the printer via the NB620W Gateway's USB port.



## Appendix A: Technical Specifications

<b>Standard:</b>	IEEE 802.3, 802.3u, 802.11g and 802.11b
<b>Channels:</b>	11 Channels: US, Canada 13 Channels: Europe, Australia 14 Channels: Japan
<b>Access Interface</b>	WAN: One 10/100 Base TX port, Auto sensing, Auto MDIX, RJ-45 connector LAN: Four 10/100 Base TX ports, Auto sensing, Auto MDIX, RJ-45 connector Wireless: External Antenna, Frequency: 2.412~2.484 GHz, support 14 channels, data rates supports 6, 9, 12, 18, 24, 36, 48 and 54 Mbps auto fallback function,
<b>LED Indicators</b>	PWR: Green LED, indicates power and operation DIAG: Green LED, indicates hardware abnormal operation LAN 10/100: indicates LAN port connection, yellow, 10Mbps, green, 100Mbps WAN 10/100: indicates ISP connection WLAN : Green LED, indicates Wireless LAN function
<b>Reset Button</b>	(Factory default-setting button)
<b>Environment</b>	Operation Temperature: 0°C ~ 45°C Operation Humidity: 5% ~ 95% Storage Temperature: -20~+85°C Storage Humidity: 5%~95%
<b>Power</b>	AC Adapter: Input 240VAC; Output 24 VDC/0.5 Amps Maximum power consumption: 10 Watts
<b>Dimensions</b>	180mm x 143mm x 40.5mm (W x D x H)
<b>Certificates</b>	C-Tick N367

## Hardware

### Access Interface

- WAN: One 10/100 Base TX port, Auto sensing, Auto MDIX, RJ-45 connector
- LAN: Four 10/100 Base TX ports, Auto sensing, Auto MDIX, RJ-45 connector
- Wireless: External Antenna, Frequency: 2.412~2.484 GHz, support 13 channels, data rates supports 6, 9, 12, 18, 24, 36, 48 and 54 Mbps auto fallback function, Super-G Wireless Mode.

### LED Indicators

- LED1 shows status of local port #1
- LED2 shows status of local port #2
- LED3 shows status of local port #3
- LED4 shows status of local port #4
- WLAN LED shows Wireless LAN connection
- WAN LED shows WAN/Internet port status
- Power LED shows unit power status

**Reset Button** (Factory default-setting button)

Two USB 2.0 Host ports (For Disk and Print serving)

### Environment

- Operation Temperature: 0°C ~ 45°C
- Operation Humidity: 5% ~ 95%
- Storage Temperature: -20~+85°C
- Storage Humidity: 5%~95%

### Power

- AC Adapter: Input 240VAC; Output 24VDC/0.5 Amps
- Maximum power consumption: 10 Watts

### Dimensions & Weight

- 180mm x 143mm x 40.5mm (W x D x H)

### Certificates

- C-Tick N367

## Software

### Networking /Transport layer protocol

- 802.1D Bridge for LAN and Wireless bridging
- DHCP server
- PPPoE, Telstra BigPond, DHCP client and Fixed IP for broadband DSL/ Cable ISP connection (eg Optus Cable)
- MAC address spoofing
- Static routes
- DNS proxy
- Dynamic DNS for dynamic IP based domain name service
- NTP client for network time synchronization
- 802.11g Access Point

### Firewall/NAT

- Stateful packet inspection
- DoS attack prevention
- Virtual Server/Port Forwarding
- One DMZ host
- IP packet filtering with scheduling (MAC based access control list)
- Event logging and e-mail alert for DoS attack
- ALG support including: IPSec, PPTP, L2TP, H.323, SIP, NetMeeting, MS Messenger, RealPlayer, Quick Time (ICQ, CuSeeMe, VDO Live, Quake III, Diablo II, Age of Empire II)

### Wireless Security

- Supports 40/64,128 and 152-bit WEP encryption
- MAC based access control list
- Wireless Access Control (SSID)
- Wi-Fi Protected access (WPA) compatible (Pre-shared Key)
- 802.1x

### Web Contents Filtering

- Supports true proxy-based URL blocking with scheduling

## Management

- Web-based configuration wizard
- Web-based firmware upgrade, configuration profile backup/restore
- Remote Management
- Supports Windows-based syslog viewer
- Supports UPnP

## File sharing support

- Supported OS: USB support needed - Windows 98se, Me, 2000 and XP
- Management Tool: Web-Based

## Printing supported features

- Supported OS: Native Windows 2000 & XP LPR Protocol, Win95, 98 & Me with 3rd Party LPR Client, (Not supplied)
- Supported Networks: LPR Print Server
- Management Tool: Web-Based

## Appendix B: Frequent Asked Questions

### Q: What is a "dynamic IP address"?

A: An IP address from your ISP which is assigned via DHCP and is therefore not guaranteed to remain the same. Some cable modem Internet providers provide IP address assignments which rarely change, but the addresses assigned are still considered to be dynamic, not static.

### Q: When should I modify the MAC address for global port settings?

A: Some ISPs identify their clients by their MAC address and host names. Entering this information allows authentication. The MAC address required for the global port settings is the adapter address for the device you are now configuring. Most ISPs use automatic registration and do not limit network MAC addresses. But, if they do, you can change your MAC address to meet their registration.

### Q: What is DMZ?

A: DMZ (demilitarized zone) is a barrier between the Internet and a company's Intranet. It is a subnet that contains a firewall and proxy server, which can be in separate servers or in one server. The firewall connects to an external firewall on the Internet side, which may be at the ISP's location and is often called a "boundary router". The double firewall architecture adds an extra measure of security for the Intranet.

### Q: What is Dynamic DNS?

A: The Dynamic DNS service is an IP Registry which provides a public central database where information such as email addresses, hostnames, Ips etc. can be stored and retrieved. This can be a solution if your DNS server uses an IP associated with dynamic IP. The Dynamic DNS service acts like an old-style phone operator: other users call the operator and ask to speak to you and the operator, who knows your extension, will make the connection. Every time your computer comes online, it will inform the Dynamic DNS server what the current IP address is. Users who need to connect to your server, through the DNS service, will be sent to the right place. Please visit <http://www.dyndns.org> for more information.

### Q: Why "Dynamic DNS"?

A: With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register with a Dynamic DNS Client to use this service. Please go to <http://www.dyndns.org> for more information.

### Q: What is Wildcard?

A: A wildcard alias is a method that is used to give your hostname multiple identities. If you were to register [yourhost.com](http://yourhost.com), everything (\*)[.yourhost.com](http://yourhost.com) would be aliased to [yourhost.com](http://yourhost.com). This includes host names such as [www.yourhost.com](http://www.yourhost.com) or [ftp.yourhost.com](http://ftp.yourhost.com). Once Wildcard feature was enabled, your host can be reached by [\\*.yourhost.dyndns.org](http://*.yourhost.dyndns.org). First, you need to register a dynamic DNS account with [www.dyndns.org](http://www.dyndns.org). To use this service, you must register with the Dynamic DNS client. The Dynamic DNS client service provider will give you a password or key. Refer to what's Dynamic DNS? Question above for more information.

## Q: What's MX (Mail Exchanger)? And why MX?

A: The Internet email system for both machines and network connections are prone to error. With this, a chain of email hubs into the email architecture is built. If the "primary" mail host goes down, instead of queuing up the mails in the unreliable host on the Internet, they get sent to the "secondary" or "backup" mail exchanger for delivery, until the primary mail server becomes functional again. In technical terms, such service is called a Backup Mail Exchanger.

## Q: What is PPPoE (PPP Over Ethernet)?

A: PPPoE is known as a dial-up DSL service. It is designed to integrate the broadband services into the current widely deployed, easy-to-use, and low-cost dial-up-access networking infrastructure. Thus, customer can get greater access speed without changing the operation concept.

## Q: What is MTU?

A: A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network such as the Internet. The Internet's Transmission Control Protocol uses the MTU to determine the maximum size of each packet in any transmission. Too large an MTU size may mean retransmissions if the packet encounters a router that can't handle that large a packet. Too small an MTU size means more header overhead and more acknowledgements that have to be sent and handled. Most computer operating systems provide a default MTU value that is suitable for most users. In general, Internet users should follow the advice of their Internet service provider (ISP) about whether to change the default value and what to change it to.

## Q: What to do if my USB storage stalls?

A: Please power off your NB620W gateway and then turn it on; the storage device will back to work. This problem usually caused by unplugging the USB storage device without unloading it first.



## Appendix C: Troubleshooting

This chapter is intended to help you troubleshoot problems you may encounter while setting up and using the NetComm NB620W. It also describes some common hardware and software problems and gives some suggestions to troubleshoot them.

### Refresh your IP address (MS Windows)

There is a tool which comes with Windows which will allow you to refresh your current IP Address. For Windows 95/98/98se/ME, click Start > Run, enter winipcfg and click OK. Select the correct Network Adaptor, click release all to release all current configuration first, then click renew all to renew the IP information again.

For Windows NT4.0/2000/XP, run ipconfig.exe in DOS mode. (ipconfig.exe/? to list all parameters). Run ipconfig /release and then run ipconfig /renew.

### IP address conflict

When you see the message box advising of an IP address conflict on any of the workstations in the network, this means two or more workstations have the same IP address. If you have setup the device as a DHCP server, on the problem workstation, please run the "winipcfg" utility, select the correct Network Adapter, click release all to release all current configuration first, then click renew all to renew the IP information again (for Windows 2000/NT4.0/XP, run ipconfig/release and then run ipconfig /renew). If the DHCP function is disabled and static IP addresses are assigned to each workstation, please double check each workstation's IP address for any duplicate IP.

### Cannot access the Internet

- Check the physical connectivity of your local network.
- Check if both the LEDs of Local and Global on the product's front panel are lit. Make sure you are using the correct cables and the cables are connected to the network devices properly.
- Check the physical connectivity of broadband device.
- Examine the LED of LAN port and the LED of the broadband signal input on the Cable Modem/xDSL Modem. If the LAN LED is off, make sure you are using the correct cables and the cables are connected to the devices properly. If the LED of the broadband signal is off, please contact your ISP.
- Check the status of this product.
- After checking the cabling, you should also check if you have entered the correct user name and password that your ISP provided. While checking, please note that the information is case sensitive.
- To check the Internet connection status, open the browser to start the web configuration, select Network Status > WAN IP Status. Check if Link Status displays "Connect successfully". If not, you may have to contact your ISP to see if their Internet service is available.
- Check the logical connectivity from your computer to the Internet.

## Appendix D: DDNS Update Status Messages

---

- (1) When starting the DDNS service.  
Updating dynamic DNS server, please wait.
- (2) When DHCP Client or PPPOE cannot get IP on the Internet Port.  
Could not resolve IP address for the device.
- (3) When DDNS update successful.  
Update dynamic DNS server successful IP: <Your Internet IP address> (eg. 211.21.190.99)  
Update dynamic DNS server successful IP: <Your Internet IP address> (eg. 211.21.190.99)  
again.  
Update successful, a feature requested is only available to donators, please donate.
- (4) When DDNS update fail.  
Update fail, cannot connect to server: members.dyndns.org  
Update fail, strange server response.  
Update fail, invalid hostname: user.dyndns.org .  
Update fail, malformed hostname: user.dyndns.org .  
Update fail, hostname: user.dyndns.org is not under your control.  
Update fail, hostname: user.dyndns.org has been blocked for abuse. You need to be logged  
in dyndns.org.  
Update fail, invalid username and password.  
Update fail, invalid parameter.  
Update fail, this user agent has been blocked.  
Update fail, too many or too few hosts found.  
Update fail, dyndns internal error, please report this number to their support people: error  
message.  
Update fail, 911!  
Update fail, 999!  
Update fail, wait response received, waiting for 60 seconds before next update.  
Update fail, error processing request  
Update fail, invalid username and password!  
Update fail, server response: server message.

## 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.

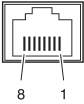
### RJ-45 Network Ports

RJ-45 Network Ports can connect any networking devices that use a standard LAN interface, such as a Hub/Switch Hub or Router. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable to connect the networking device to the RJ-45 Ethernet port. Depending on the type of connection, 10Mbps or 100Mbps, use the following Ethernet cable, as prescribed.

10Mbps: Use EIA/TIA-568-100-Category 3, 4 or 5 cable.

100Mbps: Use EIA/TIA-568-100-Category 5 cable.

**Note:** To prevent loss of signal, make sure that the length of any twisted-pair connection does not exceed 100 metres.



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.



Figure 2

## Straight and crossover cable configuration

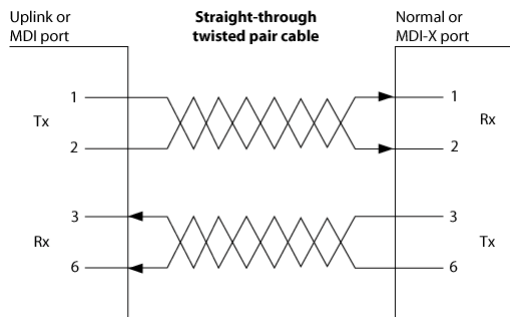


Figure 3

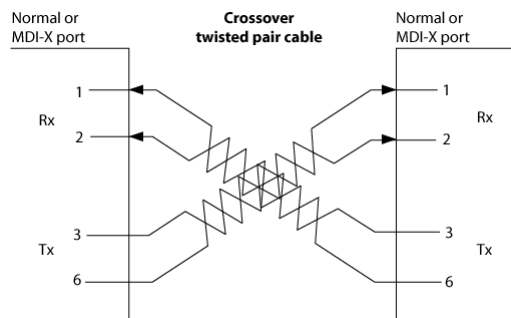


Figure 4

## 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.

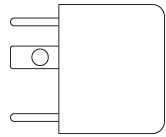


RJ-11 Connector Pin Assignment	Normal Assignment
1	Signal Ground
2	CTS
3	RXD
4	TXD
5	+5 Volts In
6	Signal Ground

Figure 5

## 605 to RJ-11 adapter

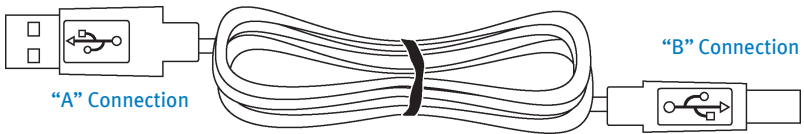
The 605 to RJ-11 adaptor is provided to comply with the older 610 Telstra wall socket. The 605 to RJ-11 adaptor may be used to convert the supplied RJ-11 cable, if the older connection is required.



## 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 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.

## 9 Pin (RS-232 ) Serial Cable

A 9 Pin (RS-232) Serial Cable may be used to connect to a serial console terminal or a PC running a terminal emulation program, such as Hyper Terminal.



Male Connector

Pin No	Name	Notes/Description No.
1	DCD	Data Carrier Detect
2	RD	Receive Data (a.k.a RxD, Rx)
3	TD	Transmit Data (a.k.a TxD, Tx)
4	DTR	Data Terminal Ready
5	SGND	Ground
6	DSR	Data Set Ready
7	RTS	Request To Send
8	CTS	Clear To Send
9	RI	Ring Indicator

## Appendix F: Registering your NetComm Product

All NetComm Limited (“NetComm”) products have a standard 12 month warranty from date of purchase against defects in manufacturing and that the products will operate in accordance with the specifications outlined in the User Guide. However some products have an extended warranty option (please refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at:

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

### 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](mailto:support@netcomm.com.au)

Fax: (+612) 9424-2010

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

### Legal & Regulatory Information

This manual is copyright. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the Copyright Act, no part may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Limited. NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product.

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 meets 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 direction 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 intended 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.

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



## Limitations of Warranty

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

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

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

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

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

## SUPER G WIRELESS GATEWAY

The NB620W is a state-of-the-art Wireless Gateway with the latest in advanced broadband wireless connectivity.

Now it's simple and cost-effective to build a local network with Internet access using wired or wireless technology. The NB620W features the latest 802.11g wireless standard for high-speed transfer rates up to 54Mbps, as well as Atheros' Super G mode to turbocharge your transfer rates. The NB620W is backwards compatible with 11Mbps, 802.11b wireless networks and carries a built-in 4 port 10/100 Base-TX Ethernet Switch.

## TRIPLE SECURITY

The NB620W introduces three levels of security to keep those intruders and hackers out of your wired or wireless network. The combination of NAT and SPI/DoS (Stateful Packet Inspection/Denial of Service) firewall technology, the latest WEP (Wireless Encryption Protocols) and WPA (WiFi Protection Access – PSK and Radius) ensures the safety of your network PCs and their data.

## WORKS WITH ANY OPERATING SYSTEM

The NB620W works with any Operating System that supports TCP/IP, including Windows®, Apple Macintosh and Linux. The NB620W can be connected to a cable or ADSL modem to access a broadband Internet service.

The Web-based user interface facilitates easy set up and administration.

## DISK & PRINT SERVER BUILT-IN

The NB620W features two USB 2.0 ports for Disk and Print Serving. Simply connect a supported USB 1.1 or 2.0 printer to the built-in USB host and all authorised users can use this printer, via both the LAN and wireless LAN.

You can also connect any hard drive or Flash drive to the other USB port to make the data available to authorised users on the local LAN as well as wireless users.

**NetComm**<sup>TM</sup>  
*Broadband Solutions*

SHARE THE  EXPERIENCE

NetComm Limited, ABN 85 002 490 486 • PO Box 1200, Lane Cove NSW 2066 Australia.  
PHONE (02) 9424 2070 • FAX (02) 9424 2010 • EMAIL [sales@netcomm.com.au](mailto:sales@netcomm.com.au) • [www.netcomm.com.au](http://www.netcomm.com.au)

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

Specifications are subject to change without notice. **Product Code: NB620W**