

# User Guide



**NB600W**  
Super-G Wireless Gateway

## 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.

## Contents

---

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.....	9
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 .....	33
3.3 Management.....	49
Appendix A: Technical Specifications .....	56
Appendix B: Frequent Asked Questions.....	60
Appendix C: Troubleshooting .....	62
Appendix D: DDNS Update Status Messages.....	63
Appendix E: Cable Connections .....	64
RJ-45 Network Ports .....	64
Straight and crossover cable configuration .....	65
RJ11 connector and cable .....	66
605 to RJ-11 adapter .....	66
Appendix F: Registering your NetComm Product .....	67
Customer Information .....	68
Product Warranty.....	69
Limitations of Warranty .....	70

---

## Chapter 1 Introduction

### 1.1 Product Overview

Thank you for purchasing the NetComm NB600W Super-G Wireless Gateway. The NB600W 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 NB600W 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 NB600W is backwards compatible with 11Mbps, 802.11b wireless networks and carries a built-in 4 port 10/100 Base-TX Ethernet Switch.

The NB600W 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 NB600W Web-based user interface facilitates easy set up and ongoing administration.

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 NB600W 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
- 3-YEAR WARRANTY WHEN YOU REGISTER ONLINE

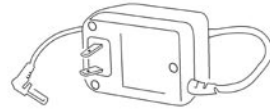
## 1.3 What's in the package?

Your NB600W Package should contain the following items:

- NB600W Super-G Wireless Broadband Gateway with 4-port Switch



- Power Adapter



- Quick Installation Guide



- Package Contents Note



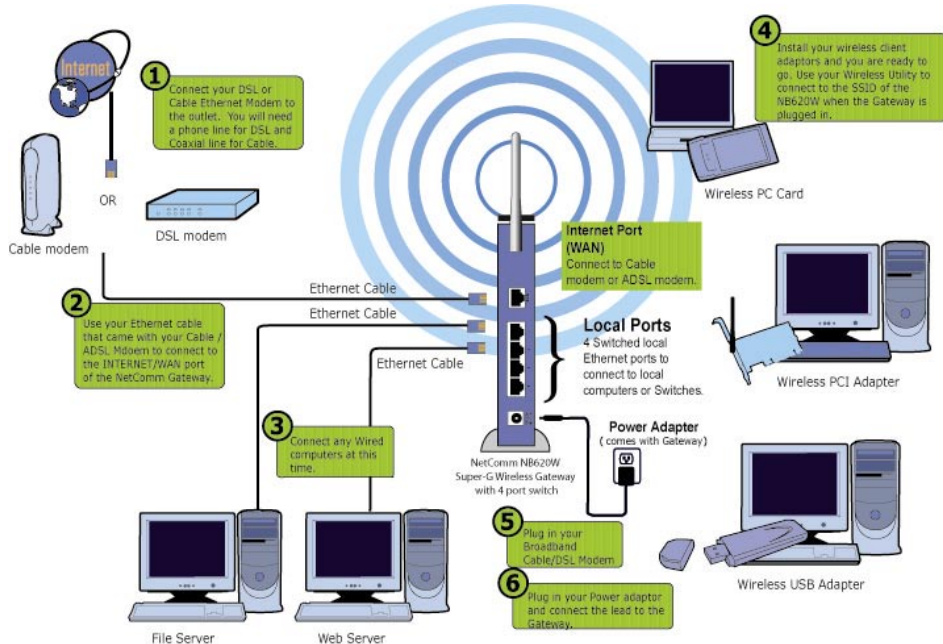
- Installation CD



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 NB600W 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 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.



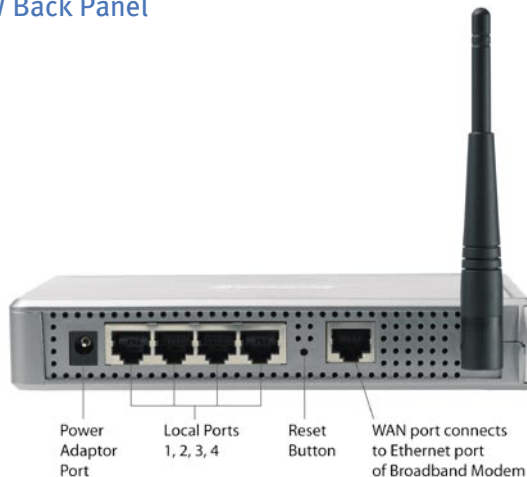
## 1.5 Device

The NB600W has 5 ports and 7 LEDs for connection and administrative purposes.

### 1.5.1 NB600W Front Panel



### 1.5.2 NB600W 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 NB600W is “admin”.

### Password

The default password of the NB600W 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 NB600W Gateway. Hold the button in at least 10 seconds. The NB600W 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 NB600W 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>	NB600W
<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 NB600W Gateway.

To do this, you need to configure your PC's network settings to obtain an IP 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 cannot find it on the desktop, click the Start button). Then choose Properties in the menu; the system information will identify which operating system you are using.



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

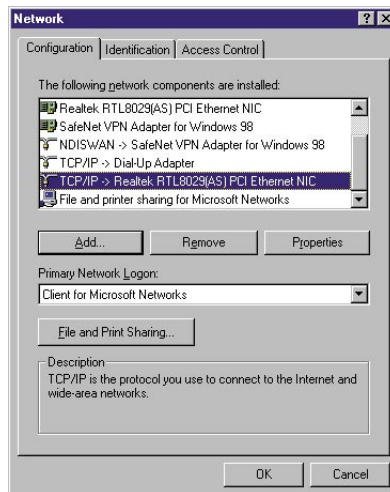
The following pages tell you, step by step, how to configure your network settings based on the type of Windows operating system you are using. Make sure that an Ethernet or wireless adapter (also known as a network adapter) has been successfully installed in each PC you will configure. Once you've configured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

## 2.2 Configuring Windows 98 and Millennium PCs

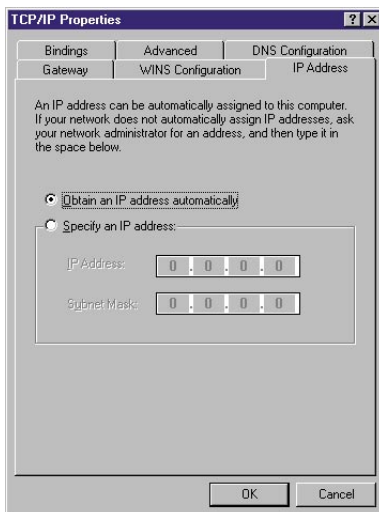
1. Click the Start button. Select Settings and click the Control Panel icon. Double-click the Network icon.



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”.



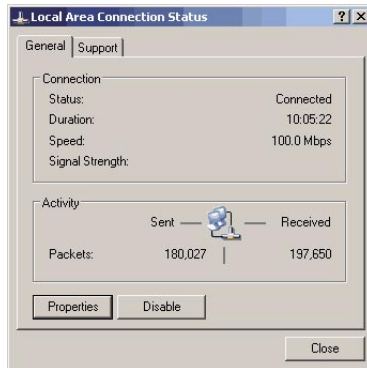
4. Now click the Gateway tab, and verify that the Installed Gateway field is blank. Click the OK button.



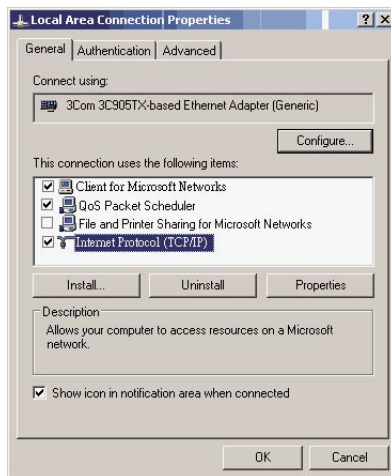
5. Click the OK button again. Windows may ask you for the original Windows installation disk or additional files. Check for the files at c:\windows\options\cabs, or insert your Windows CD-ROM into your CD-ROM drive and check the correct file location, e.g., D:\win98, D:\win9x, etc. (If “D” is the letter 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

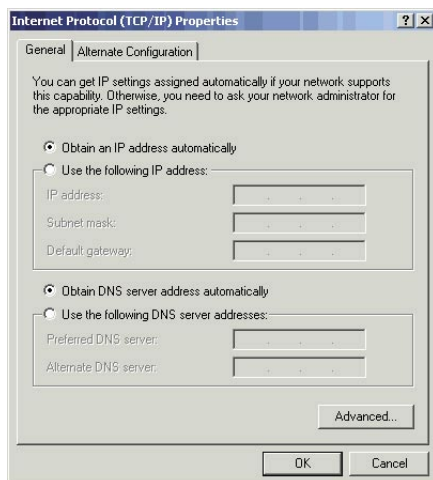
1. Click the Start button. Select Settings and click the Control Panel icon. Double-click Network and Dial-up Connections icon.
2. Select the Local Area Connection icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the Local Area Connection.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



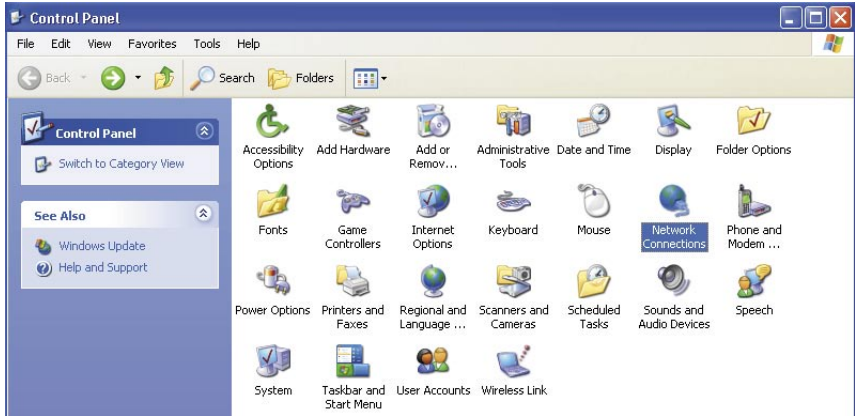
5. Restart your computer.



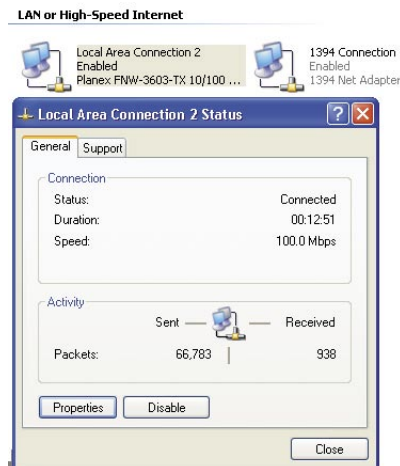
## 2.4 Configuring Windows XP PCs

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.



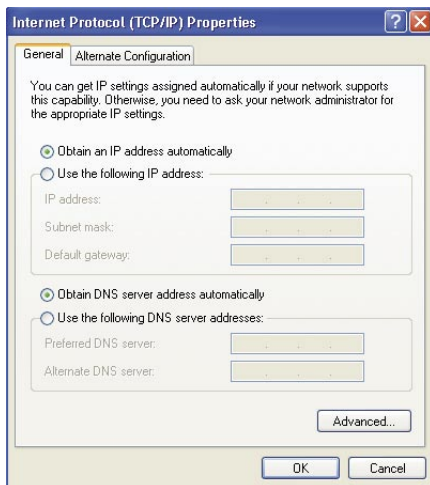
2. Select the Local Area Connection icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the Local Area Connection. Click the Properties button.



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 Gateway's IP address, please type `http://<the new IP address of the gateway>.`)

## Chapter 3 Configuring the Wireless Gateway

The NB600W 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 NB600W Wireless Gateway.

### Accessing the Configuration Manager

The Configuration Manager is a number of pre-installed web-based pages in the NB600W 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 NB600W. Just configure your PCs to accept the network information automatically. The NB600W 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 NB600W 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 to 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.

The screenshot displays the configuration interface for a NetComm Super-G Wireless Firewall Router. The left sidebar contains a navigation menu with the following items: Setup Wizard, Internet Port, Local Port, Wireless LAN, Advanced, Access Control List, Content Filtering, Dynamic DNS, Firewall, Remote Management, Static Routes, UPnP, Virtual Server, Management, Access Log, Factory Reset, Firmware Upgrade, Network Status, Save Configuration, Time, and Help .. The main content area is titled 'You Are Now In > Internet Port > Telstra BigPond Configuration'. It features a dropdown menu for 'Protocol' set to 'Telstra BigPond (BigPond Configuration)'. Below this are input fields for 'Server IP Address' (four empty boxes), 'User Name' (a long text box), 'Password' (a text box), and 'Confirm Password' (a text box). The 'MAC Address' is displayed as '00 - 01 - 38 - 3A - F8 - CE', with a checkbox labeled 'Copy from this PC' next to it. At the bottom of the form are 'Save' and 'Undo' buttons.

## 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 also.



**NetComm® Super-G Wireless Firewall Router**

You Are Now In > Internet Port > DHCP Configuration

Setup Wizard

Internet Port  
Local Port  
Wireless LAN

Advanced  
Access Control List  
Content Filtering  
Dynamic DNS  
Firewall  
Remote Management  
Static Routes  
UPnP  
Virtual Server

Management  
Access Log  
Factory Reset  
Firmware Upgrade  
Network Status  
Save Configuration  
Time

Help ..

Protocol: DHCP(Dynamic IP Configuration for Cable)

Host Name: XG6640g

Domain Name:

☐ Use Static DNS

Primary: . . . .

Secondary: . . . .

MAC Address: 00 . 01 . 38 . 3A . F8 . CE

☐ Copy from this PC: . . . .

Save Undo

Field	Description
<b>Host Name/Domain Name</b>	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.
<b>Use Static DNS</b>	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.)
<b>MAC address</b>	Some ISPs require a specific MAC address. 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.

**NetComm® Super-G Wireless Firewall Router**

You Are Now In > Internet Port > PPPoE Configuration

**Setup Wizard**

- Internet Port
- Local Port
- Wireless LAN
- Advanced**
- Access Control List
- Content Filtering
- Dynamic DNS
- Firewall
- Remote Management
- Static Routes
- UPnP
- Virtual Server
- Management**
- Access Log
- Factory Reset
- Firmware Upgrade
- Network Status
- Save Configuration
- Time
- Help ..

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** . **01** . **38** . **3A** . **F8** . **CE**

☐ Copy from this PC:  .  .  .

**Save** **Undo**

Field	Description
<b>Host Name/Domain Name</b>	ISPs generally require the host name and domain name as identification. If these are not required, assign on your own or leave blank.
<b>User Name</b>	Enter your username.
<b>Password &amp; Confirm Password</b>	Enter your password and confirm again in the fields for the login to the ISP.
<b>Service Name</b>	Enter the ISP specified service name or assign one of your own if the Service Name is not specified.
<b>Packet Size (MTU)</b>	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.
<b>Disconnect after idle time</b>	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.

Field	Description
<b>Enable Unnumbered PPP Connection</b>	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.
<b>Use Static DNS</b>	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.)
<b>MAC address</b>	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”.

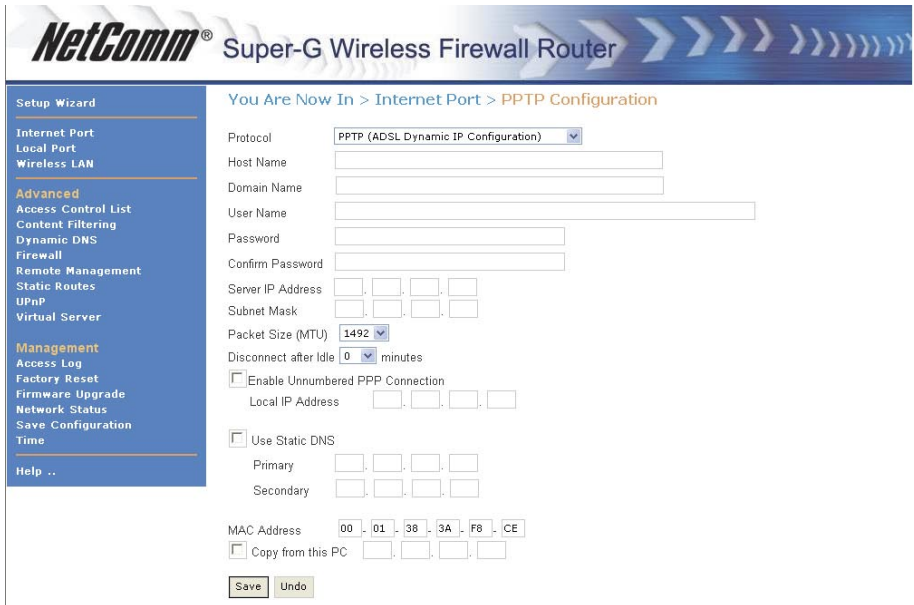
The screenshot shows the NetComm Super-G Wireless Firewall Router web interface. The top banner displays the NetComm logo and the product name. Below the banner, a navigation menu on the left lists various setup options: Setup Wizard, Internet Port, Local Port, Wireless LAN, Advanced (Access Control List, Content Filtering, Dynamic DNS, Firewall, Remote Management, Static Routes, UPnP, Virtual Server), Management (Access Log, Factory Reset, Firmware Upgrade, Network Status, Save Configuration, Time), and Help. The main content area is titled 'You Are Now In > Internet Port > Static IP Configuration'. It features a 'Protocol' dropdown menu set to 'Static IP Configuration'. Below this are input fields for 'Host Name', 'Domain Name', 'IP Address', 'Submask', 'Gateway', 'Primary DNS', and 'Secondary DNS'. Each of these fields is represented by a small grid of input boxes. At the bottom, there is a 'MAC Address' field with a dropdown menu showing '00', '01', '38', '3A', 'F8', and 'CE', followed by a checkbox labeled 'Copy from this PC'. 'Save' and 'Undo' buttons are located at the bottom left of the form area.

Field	Description
<b>Host Name/Domain Name</b>	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.
<b>IP Address</b>	Enter the IP address of the gateway's Internet port. Please use the ISP specified address.
<b>Subnet mask</b>	Enter the subnet mask supplied by your ISP.
<b>Gateway</b>	Your ISP will assign a gateway address for you. If you can not find one, please contact your ISP.
<b>Primary DNS</b>	Enter the domain name server of the ISP.
<b>Secondary DNS</b>	The back up domain name server can be left blank if necessary.
<b>MAC address</b>	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.



**NetComm® Super-G Wireless Firewall Router**

You Are Now In > Internet Port > PPTP Configuration

Setup Wizard

- Internet Port
- Local Port
- Wireless LAN

Advanced

- Access Control List
- Content Filtering
- Dynamic DNS
- Firewall
- Remote Management
- Static Routes
- UPnP
- Virtual Server

Management

- Access Log
- Factory Reset
- Firmware Upgrade
- Network Status
- Save Configuration
- Time

Help ..

Protocol: **PPTP (ADSL Dynamic IP Configuration)**

Host Name:

Domain Name:

User Name:

Password:

Confirm Password:

Server IP Address:

Subnet Mask:

Packet Size (MTU): **1492**

Disconnect after Idle: **0** minutes

☐ Enable Unnumbered PPP Connection

Local IP Address:

☐ Use Static DNS

Primary:

Secondary:

MAC Address: **00** **01** **38** **3A** **F8** **CE**

☐ Copy from this PC:

**Save** **Undo**

Field	Description
<b>Host Name/Domain Name</b>	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.
<b>User Name</b>	Enter your username.
<b>Password &amp; Confirm Password</b>	Enter your password and confirm again in the fields for the login to the ISP.
<b>Server IP</b>	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.

Field	Description
<b>Packet Size (MTU)</b>	he 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.
<b>Disconnect after idle time</b>	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.
<b>Enable Unnumbered PPP Connection</b>	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.
<b>Use Static DNS</b>	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.)
<b>MAC address</b>	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).



Field	Description
<b>Subnet Mask</b>	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.
<b>DHCP server</b>	To enable the DHCP server, please click the check box. The DHCP server assigns dynamic IP address to the clients.
<b>Start IP address</b>	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.)
<b>Number of IP address</b>	Assign the number of users allowed to use the DHCP service. The default value is 128 users.

Field	Description
<b>Lease Time</b>	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 168 hours.
<b>Static DHCP IP &amp; MAC Address</b>	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.
<b>WINS Server</b>	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 blank.

### 3.1.3 Wireless LAN

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



Field	Description
<b>SSID</b> (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).
<b>Hide SSID</b>	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. If necessary contact your wireless card vendor for new firmware.)
<b>Region</b>	Select the region for your location.
<b>Channel</b>	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.
<b>Operation Mode</b>	<p>There are four operation modes Auto, Super-G, 802.11b/g and 802.11b only.</p> <p>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.</p>

Field	Description
	<p>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.</p>
<b>Enable Wireless Access List</b>	<p>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.</p>
<b>Security Mode</b>	<p>It is strongly recommended to use one of the Wireless Security modes to protect your local network.</p> <p>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.</p> <p>To enable Security Settings, choose one of the security modes you desired.</p> <div> <div>Security Mode</div> <div>WEP Encryption</div> </div> <div> <div>WEP Security</div> <div> <div>WEP Encryption</div> <div>64 bit(5 characters or 10 digits)</div> </div> <div> <div>Key Format</div> <div>HEX</div> </div> <div> <div>Passphrase</div> <div>55</div> <div>Generate</div> </div> <div> <div><input checked="" type="radio"/> Key 1</div> <div>E7F27D0179</div> </div> <div> <div><input type="radio"/> Key 2</div> <div>B8F4828525</div> </div> <div> <div><input type="radio"/> Key 3</div> <div>375C50FC4E</div> </div> <div> <div><input type="radio"/> Key 4</div> <div>88BD22D834</div> </div> <div> <div>Save</div> <div>Undo</div> </div> </div>
<b>WEP</b>	<p>There are three levels of WEP encryption, 64-bit, 128-bit and 152-bit.</p> <p>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.</p>

## Field

## Description

### 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.

### 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

#### WPA RADIUS Security

WPA Algorithms

RADIUS Server Address

RADIUS Port

Shared Key

Group Key Renewal  Seconds

Field	Description
<b>802.1x RADIUS</b>	<p>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.</p> <p>Security Mode <span>802.1x RADIUS</span></p> <p><b>802.1x RADIUS Security</b></p> <p>RADIUS Server Address <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/></p> <p>RADIUS Port <span>1812</span></p> <p>Shared Key <input type="text"/></p> <p>Group Key Renewal <span>1800</span> Seconds</p> <p><span>Save</span> <span>Undo</span></p>



## 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.



The screenshot shows the NetComm Super-G Wireless Firewall Router configuration interface. The top banner reads "NetComm® Super-G Wireless Firewall Router". Below the banner, a navigation bar indicates "You Are Now In > Advanced Setup > Access Control List".

On the left is a sidebar menu with the following items:

- Setup Wizard
- Internet Port
- Local Port
- Wireless LAN
- Advanced**
  - Access Control List
  - Content Filtering
  - Dynamic DNS
  - Firewall
  - Remote Management
  - Static Routes
  - UPnP
  - Virtual Server
- Management**
  - Access Log
  - Factory Reset
  - Firmware Upgrade
  - Network Status
  - Save Configuration
  - Time
- Help ..

The main configuration area for "Access Control List" includes:

- User Group:** A dropdown menu with a "Define Group" button next to it.
- Application:** A dropdown menu showing "FTP (TCP 21)" with a "Define Application" button next to it.
- Blocking Schedule:**
  - Radio buttons for "Always" (selected) and "by schedule".
  - Days of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday (all are unchecked).
  - Time Period: Two dropdowns showing "0:00" to "1:00".
  - "Add" and "Undo" buttons.
- Table:** A table with columns "#", "Application", and "Blocking Schedule". The table is currently empty.
- Buttons:** "Delete All" and "Delete" buttons at the bottom of the table.

#### Field

#### Description

#### User Group

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

#### Application

Select the application 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.)

#### Blocking Schedule

Rules can be applied using a defined schedule. 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 define. 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

**NetComm® Super-G Wireless Firewall Router**

You Are Now In > Advanced Setup > Access Control List > Define Group

Group Name

☒ Every IP Address

☐ This IP Address

☐ IP Address Range     To

#	IP Address

Field	Description
<b>Group Name</b>	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.
<b>Every IP address</b>	Selecting this will include all the IP addresses in your network.
<b>This IP address</b>	To specify the IP addresses one at a time, simply type in the IP address you want to add into the fields.
<b>IP Address Range</b>	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

**NetComm® Super-G Wireless Firewall Router**

**Setup Wizard**  


---

Internet Port  
Local Port  
Wireless LAN  


---

**Advanced**  
Access Control List  
Content Filtering  
Dynamic DNS  
Firewall  
Remote Management  
Static Routes  
UPnP  
Virtual Server  


---

**Management**  
Access Log  
Factory Reset  
Firmware Upgrade  
Network Status  
Save Configuration  
Time

You Are Now In > Advanced Setup > Access Control List > Define Application

Application:   
Protocol: TCP  
Port Range: ☒ Single ☐ Range  
Port Number:  to   

Add
Undo

#	Application	Protocol	Ports
<div style="border: 1px solid #ccc; width: 100%; height: 100%;"></div>			

Delete

Field	Description
<b>Application name</b>	Define the name of the application you want to define.
<b>Protocol</b>	Select TCP or UDP for the protocol of the application.
<b>Port Range/Port Number</b>	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.

**NetComm® Super-G Wireless Firewall Router**

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 ☐ .gif ☐ .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 ☐ Tuesday ☐ Friday ☐ Saturday ☐ Sunday

Time Period 0:00 to 1:00

Time Period 0:00 to 1:00

Trust User

Field	Description
<b>Block URLs By Keyword</b>	Type the key words in the field Keyword then click add. Check the box to activate the URL blocking function. Use delete or delete all to manage the list of keywords.
<b>Block URLs With IP Address</b>	Check this box to block users typing IP addresses in the URL field.
<b>Block Java Applets</b>	This setting will block all Java applets sent from the web site you are visiting or external web sites.
<b>Block ActiveX Controls</b>	This setting will block all ActiveX controls sent from the web site you are visiting or external web sites.

Field	Description
<b>Block Cookies</b>	This setting will block all cookies sent from the web site you are visiting or external web sites.
<b>Block Download File</b>	Available for Executable, Compressed and Audio/Video files. Check the file types you want to block the users from downloading.
<b>Schedule</b>	<p>To enable filtering functions by schedule, select the day and time.</p> <p>Choose Always to enable the filtering all the time.</p>
<b>Trust User</b>	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.

The screenshot shows the NetComm Super-G Wireless Firewall Router web interface. The top banner displays the NetComm logo and the product name. Below the banner, a navigation menu on the left lists various setup options: Setup Wizard, Internet Port, Local Port, Wireless LAN, Advanced, Access Control List, Content Filtering, Dynamic DNS, Firewall, Remote Management, Static Routes, UPnP, Virtual Server, Management, Access Log, Factory Reset, Firmware Upgrade, Network Status, Save Configuration, Time, and Help. The main content area is titled 'You Are Now In > Advanced Setup > Dynamic DNS'. It contains a checkbox for 'Enable Dynamic DNS', a 'DDNS account' section with a dropdown menu (currently showing 'ath.cx'), a text input for 'user name', and a text input for 'Password'. There is also a checkbox for 'Wildcard Enable', a text input for 'Mail Exchanger', and a checkbox for 'Backup MX'. At the bottom, there are 'Save' and 'Undo' buttons, and an 'Update Status' section with 'Update' and 'Refresh' buttons.

Field	Description
<b>Enable Dynamic DNS</b>	Check the box to enable the DDNS service.
<b>DDNS Account</b>	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. Enter your account name.
<b>User Name, Password</b>	These DDNS services require you to login, please enter your DDNS registered name and password here.
<b>Wild Card Enable</b>	If you want 'anything_here.yourhost.dyndns.org' to work (i.e. for addresses like www.yourhost.dyndns.org), check the Enable Wildcard box.
<b>Mail Exchanger</b>	If you wish to use a mail exchanger, put its hostname into the Mail Exchanger field.
<b>Backup MX</b>	If you need to backup the Mail Exchanger's address while you login to the DDNS service provider every time, please click the checkbox.

Field	Description
<b>Update Status</b>	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 D 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.

Field	Description
<b>DoS Attack Threshold</b>	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.
<b>Block Request from WAN Port</b>	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.
<b>Block Ping from WAN port</b>	This feature can prevent your network from being “pinged”, or detected by other Internet users.
<b>Block PPTP, L2TP, IPSec Request</b>	This feature blocks all VPN connection requests from hosts outside your network.
<b>Block UPnP Request from WAN Port</b>	This feature blocks all UPnP requests from hosts outside your network.



Field	Description
<b>Use the DMZ host.</b>	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 continuous use.

## Email Alarm - Options

The screenshot shows the NetComm Super-G Wireless Firewall Router web interface. The breadcrumb trail indicates the user is in 'Advanced Setup > Firewall > Email Alarm'. On the left is a navigation menu with categories: Setup Wizard, Internet Port, Local Port, Wireless LAN, Advanced (with sub-items: Access Control List, Content Filtering, Dynamic DNS, Firewall, Remote Management, Static Routes, UPnP, Virtual Server), Management (with sub-items: Access Log, Factory Reset, Firmware Upgrade, Network Status, Save Configuration, Time), and Help. The main content area has the title 'You Are Now In > Advanced Setup > Firewall > Email Alarm'. It contains a checkbox for 'Enable Email Alarm', input fields for 'Mail Server', 'Port No.' (set to 25), 'Subject', 'Send Mail To', and 'Return Address'. Below this is an 'E-Mail Log' section with radio buttons for 'Log Full' (selected) and 'Everyday', a 'Time' dropdown set to '00:00 AM', and 'Save' and 'Undo' buttons.

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.

Field	Description
<b>Mail Server</b>	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.
<b>Port No</b>	The standard SMTP port for sending e-mails is 110. Change it if you have special settings, otherwise leave it as the default.
<b>Subject</b>	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.
<b>Send Mail To</b>	Enter the e-mail address you want the gateway send to.

Field	Description
<b>Return Address</b>	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.
<b>E-mail log</b>	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.
<b>Time</b>	Please specify the time you would like the gateway to send these e-mails everyday.

## 3.2.5 Advanced Setup ➔ Remote Management

The screenshot shows the NetComm Super-G Wireless Firewall Router web interface. The top banner displays the NetComm logo and the product name. Below the banner, a navigation menu on the left lists various setup options: Setup Wizard, Internet Port, Local Port, Wireless LAN, Advanced (highlighted), Access Control List, Content Filtering, Dynamic DNS, Firewall, Remote Management, Static Routes, UPnP, Virtual Server, Management (highlighted), Access Log, Factory Reset, Firmware Upgrade, Network Status, Save Configuration, Time, and Help. The main content area is titled 'You Are Now In > Advanced Setup > Remote Management'. It contains fields for User Name (set to 'admin'), Password (masked with dots), and Confirm Password. Below these are buttons for 'Change Login Password' and 'Undo'. Further down, there is a 'Web Management Port' field set to '80' (default 80), followed by checkboxes for 'Enable Management Via Wan Port' and 'Allow Management from PC'. Below these are MAC Address 1 and MAC Address 2 fields, each with a grid of input boxes. A checkbox for 'Send System Log to this PC' is also present. At the bottom are 'Save' and 'Undo' buttons.

Field	Description
<b>User Name</b>	You can change the user name and password of the gateway here. Type in your new user name.
<b>Password, Confirm Password</b>	Type in 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.
<b>Web Management Port</b>	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.
<b>Enable Management Via WAN port</b>	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.

Field	Description
<b>Allow Management from PC</b>	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.
<b>Send System Log to this PC</b>	The gateway will send the system logs to the PC with the IP address specified here.

## 3.2.6 Advanced Setup → Static Routes

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.

The screenshot shows the NetComm Super-G Wireless Firewall Router web interface. The top banner reads "NetComm® Super-G Wireless Firewall Router". Below the banner, the breadcrumb path is "You Are Now In > Advanced Setup > Static Routes". On the left is a navigation menu with categories: "Setup Wizard" (Internet Port, Local Port, Wireless LAN), "Advanced" (Access Control List, Content Filtering, Dynamic DNS, Firewall, Remote Management, Static Routes, UPnP, Virtual Server), "Management" (Access Log, Factory Reset, Firmware Upgrade, Network Status, Save Configuration, Time), and "Help ..". The main content area has input fields for "Destination Network / Host", "Subnet Mask", and "Gateway", each with a four-part IP address box. Below these are "Add" and "Undo" buttons. A table with columns "#", "Destination", "Submask", and "Gateway" is shown, with a large empty text area below it for adding routes. At the bottom are "Delete All", "Delete", and "Routing Table" buttons.

Field	Description
<b>Destination Network / Host</b>	The destination network is the address of the remote network or host, which you want to assign a static route to.
<b>Subnet Mask</b>	The Subnet Mask determines which portion of a destination IP address is the network portion, and which portion is the host portion.
<b>Gateway</b>	This is the IP address of the gateway device that allows for connection between the Gateway and the remote network or host.

The screenshot shows the NetComm Super-G Wireless Firewall Router web interface. The top banner displays the NetComm logo and the product name. Below the banner, a navigation menu on the left lists various configuration options: Setup Wizard, Internet Port, Local Port, Wireless LAN, Advanced (highlighted), Access Control List, Content Filtering, Dynamic DNS, Firewall, Remote Management, Static Routes, UPnP, and Virtual Server. Under the 'Advanced' section, there are links for Management, Access Log, Factory Reset, Firmware Upgrade, Network Status, Save Configuration, and Time. The main content area shows the breadcrumb 'You Are Now In > Management > UPnP'. A checkbox labeled 'Enable UPnP' is checked. Below the checkbox is a 'Save' button.

Field	Description
<b>Enable UPnP</b>	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.)



Field	Description
<b>Application</b>	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.
<b>Server IP address</b>	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

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

The screenshot shows the 'Define Application' screen in the NetComm Super-G Wireless Firewall Router Setup Wizard. The breadcrumb trail at the top reads: 'You Are Now In > Advanced Setup > Virtual Server > Define Application'. On the left is a navigation menu with sections: 'Setup Wizard' (Internet Port, Local Port, Wireless LAN), 'Advanced' (Access Control List, Content Filtering, Dynamic DNS, Firewall, Remote Management, Static Routes, UPnP, Virtual Server), and 'Management' (Access Log, Factory Reset, Firmware Upgrade, Network Status, Save Configuration, Time). The main area contains form fields for 'Application' (text), 'Protocol' (dropdown menu with 'TCP' selected), 'Port Range' (radio buttons for 'Single' and 'Range', with 'Single' selected), and 'Port Number' (two text boxes for 'to' and 'from'). Below these are 'Add' and 'Undo' buttons. A table with columns '#', 'Application', 'Protocol', and 'Ports' is shown, with a 'Delete' button below it.

Field	Description
<b>Application</b>	Type in the application name that is easy to remember and identify.
<b>Protocol</b>	Select TCP or UDP. If you are not sure which one to use, check the application manual.
<b>Port Range</b>	Choose Single if there is one port to be opened, or choose Range for a range of port numbers.
<b>Port Number</b>	Type in the Port number or Port range.
Click Add to finish your setting and it will be added to the list.	



## 3.3 Management

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

### 3.3.1 Management ➤ Access Log

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. Click the Refresh button to renew the list for the most current records.

**Super-G Wireless Firewall Router**

Setup Wizard

---

Internet Port

Local Port

Wireless LAN

---

Advanced

Access Control List

Content Filtering

Dynamic DNS

Firewall

Remote Management

Static Routes

UPnP

Virtual Server

---

Management

Access Log

Factory Reset

Firmware Upgrade

Network Status

Save Configuration

Time

---

Help ...

You Are Now In > Management > Access Log

Date/Time	Source	Destination	MAC	Protocol
Dec 31 14:19:36	192.168.1.103.1099	192.168.1.1.80	00:c0:9f:25:a4:1f	TCP
Dec 31 14:18:46	192.168.1.103.1097	192.168.1.1.80	00:c0:9f:25:a4:1f	TCP
Dec 31 14:17:45	192.168.1.103.1095	192.168.1.1.80	00:c0:9f:25:a4:1f	TCP
Dec 31 14:16:56	192.168.1.103.1094	192.168.1.1.80	00:c0:9f:25:a4:1f	TCP
Dec 31 14:15:21	192.168.1.103.1091	192.168.1.1.80	00:c0:9f:25:a4:1f	TCP
Dec 31 14:13:55	192.168.1.103.1087	192.168.1.1.80	00:c0:9f:25:a4:1f	TCP
Dec 31 14:12:48	192.168.1.103.138	192.168.1.255.138	00:c0:9f:25:a4:1f	UDP
Dec 31 14:11:16	192.168.1.103.1086	192.168.1.1.80	00:c0:9f:25:a4:1f	TCP
Dec 31 14:09:57	192.168.1.103.1084	192.168.1.1.80	00:c0:9f:25:a4:1f	TCP
Dec 31 14:09:07	192.168.1.103.138	192.168.1.255.138	00:c0:9f:25:a4:1f	UDP
Dec 31 14:08:20	192.168.1.103.1080	192.168.1.1.80	00:c0:9f:25:a4:1f	TCP
Dec 31 14:07:07	192.168.1.103.1078	192.168.1.1.80	00:c0:9f:25:a4:1f	TCP
Dec 31 14:06:16	192.168.1.103.1070	192.168.1.1.80	00:c0:9f:25:a4:1f	TCP
Dec 31 14:05:04	192.168.1.103.138	192.168.1.255.138	00:c0:9f:25:a4:1f	UDP
Dec 31 14:04:07	192.168.1.103.1054	192.168.1.1.80	00:c0:9f:25:a4:1f	TCP
Dec 31 14:03:11	192.168.1.103.1047	192.168.1.1.80	00:c0:9f:25:a4:1f	TCP
Dec 31 14:02:19	192.168.1.103.138	192.168.1.255.138	00:c0:9f:25:a4:1f	UDP
Dec 31 14:01:24	192.168.1.103.1046	192.168.1.1.80	00:c0:9f:25:a4:1f	TCP
Dec 31 14:01:19	192.168.1.103.1045	192.168.1.1.53	00:c0:9f:25:a4:1f	UDP
Dec 31 14:00:43	192.168.1.103.69	255.255.255.255.67	00:c0:9f:25:a4:1f	UDP
Dec 31 14:00:37	192.168.1.103.1042	255.255.255.255.1900	00:c0:9f:25:a4:1f	UDP
Dec 31 14:00:32	192.168.1.103.138	192.168.1.255.138	00:c0:9f:25:a4:1f	UDP
Dec 31 14:00:29	192.168.1.103.1038	192.168.1.1.53	00:c0:9f:25:a4:1f	UDP
Dec 31 14:00:13	192.168.1.103.137	192.168.1.255.137	00:c0:9f:25:a4:1f	UDP
Dec 31 14:00:11	0.0.0.0.68	255.255.255.255.67	00:c0:9f:25:a4:1f	UDP

## 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.)

The default values of your NB600W 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>	NB600W
<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

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.

The screenshot shows the NetComm Super-G Wireless Firewall Router web interface. The header displays the NetComm logo and the product name. The left sidebar contains a navigation menu with sections: Setup Wizard, Internet Port, Local Port, Wireless LAN, Advanced (with sub-items: Access Control List, Content Filtering, Dynamic DNS, Firewall, Remote Management, Static Routes, UPnP, Virtual Server), Management (with sub-items: Access Log, Factory Reset, Firmware Upgrade, Network Status, Save Configuration, Time), and Help .. The main content area shows the breadcrumb 'You Are Now In > Management > Firmware Upgrade'. It displays the 'Current Firmware Version : 2.02NCT7.6640g'. There is a 'File Name' input field with a 'Browse...' button. Below these are 'Upgrade' and 'Undo' buttons. A suggestion at the bottom states: 'Suggestion : avoid upgrading firmware from Wireless LAN.'

## 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.

**NetComm® Super-G Wireless Firewall Router**

You Are Now In > Management > Network Status

**internet**

Wan Protocol : Telstra BigPond  
 Telstra BigPond Connection status : Disconnected  
 PPPoE Connection Status :  
 PPPoE Connection Time :

IP Address :  
 Subnet Mask :  
 Gateway :

Primary DNS :  
 Secondary DNS :  
 Domain Name :

MAC address : 00:01:38:3a:f8:ce

Refresh

Connect/Renew Disconnect/Release

Session List User List

Field	Description
<b>Refresh</b>	Click this button to display the latest information.
<b>Connect/Renew</b>	When using PPPoE or PPTP, you can click this button to establish a connection to the Internet port.
<b>Disconnect/Release</b>	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

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.



**NetComm® Super-G Wireless Firewall Router**

You Are Now In > Management > Network Status > **User List**

IP	MAC	Host Name	Expire Time
192.168.1.103	00:c0:9f:25:a4:1f	ASPIRE	23 hours, 36 minutes

[Refresh](#)

**Setup Wizard**

- Internet Port
- Local Port
- Wireless LAN

**Advanced**

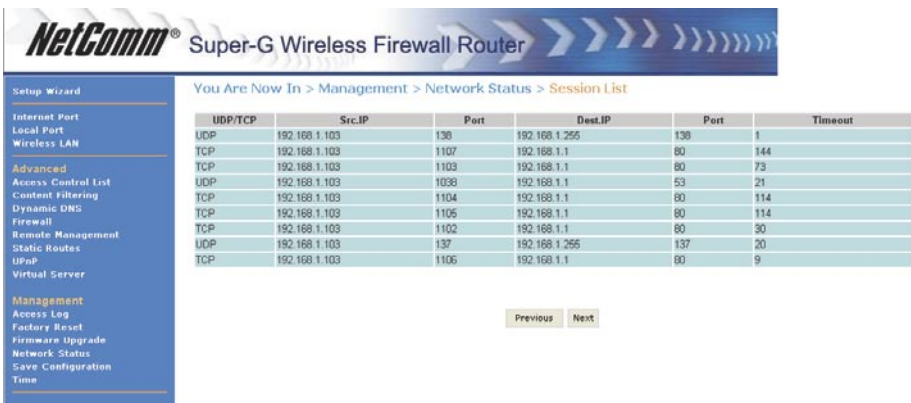
- Access Control List
- Content Filtering
- Dynamic DNS
- Firewall
- Remote Management
- Static Routes
- UPnP
- Virtual Server

**Management**

- Access Log
- Factory Reset
- Firmware Upgrade
- Network Status
- Save Configuration
- Time

## Session List

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.



**NetComm® Super-G Wireless Firewall Router**

You Are Now In > Management > Network Status > **Session List**

UDP/TCP	Src.IP	Port	Dest.IP	Port	Timeout
UDP	192.168.1.103	130	192.168.1.255	130	1
TCP	192.168.1.103	1107	192.168.1.1	80	144
TCP	192.168.1.103	1103	192.168.1.1	80	73
UDP	192.168.1.103	1038	192.168.1.1	53	21
TCP	192.168.1.103	1104	192.168.1.1	80	114
TCP	192.168.1.103	1105	192.168.1.1	80	114
TCP	192.168.1.103	1102	192.168.1.1	80	30
UDP	192.168.1.103	137	192.168.1.255	137	20
TCP	192.168.1.103	1106	192.168.1.1	80	9

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

**Setup Wizard**

- Internet Port
- Local Port
- Wireless LAN

**Advanced**

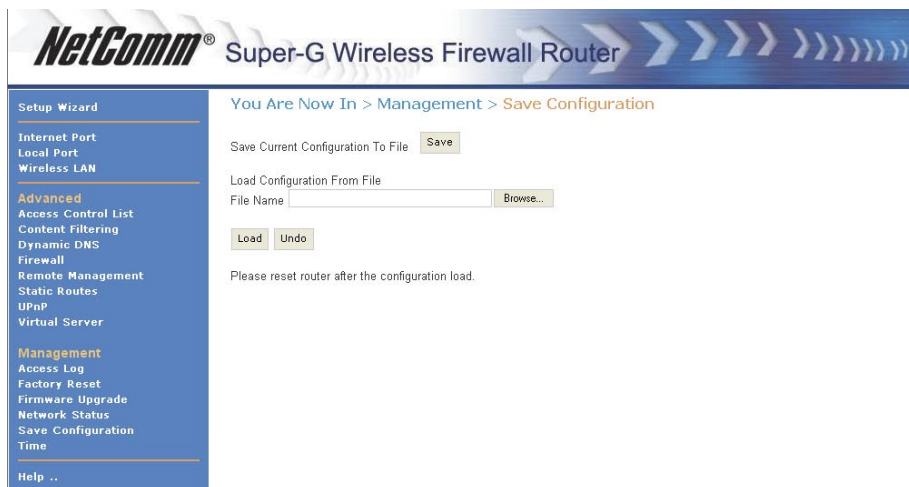
- Access Control List
- Content Filtering
- Dynamic DNS
- Firewall
- Remote Management
- Static Routes
- UPnP
- Virtual Server

**Management**

- Access Log
- Factory Reset
- Firmware Upgrade
- Network Status
- Save Configuration
- Time

## 3.3.5 Management ➤ Save Configuration

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.



The screenshot shows the NetComm Super-G Wireless Firewall Router web interface. The top banner features the NetComm logo and the product name. Below the banner, a navigation menu on the left lists various settings categories: Setup Wizard, Internet Port, Local Port, Wireless LAN, Advanced (highlighted), Access Control List, Content Filtering, Dynamic DNS, Firewall, Remote Management, Static Routes, UPnP, Virtual Server, Management (highlighted), Access Log, Factory Reset, Firmware Upgrade, Network Status, Save Configuration (highlighted), Time, and Help. The main content area displays the breadcrumb 'You Are Now In > Management > Save Configuration'. It includes a 'Save Current Configuration To File' section with a 'Save' button. Below this is a 'Load Configuration From File' section with a 'File Name' input field, a 'Browse...' button, and 'Load' and 'Undo' buttons. A note at the bottom states: 'Please reset router after the configuration load.'

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 restart the gateway (i.e. unplug the power cord and then plug it back in.).

## 3.3.6 Management ➤ 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, check the Use Daylight Saving Time box.

The screenshot shows the NetComm Super-G Wireless Firewall Router web interface. The top banner features the NetComm logo and the product name. Below the banner, a navigation bar indicates the current location: "You Are Now In > Management > Time". The left sidebar contains a menu with categories: "Setup Wizard" (Internet Port, Local Port, Wireless LAN), "Advanced" (Access Control List, Content Filtering, Dynamic DNS, Firewall, Remote Management, Static Routes, UPnP, Virtual Server), "Management" (Access Log, Factory Reset, Firmware Upgrade, Network Status, Save Configuration, Time), and "Help ..". The main content area for the "Time" page includes a "Time Zone" dropdown menu set to "(GMT-10:00) Hawaii", an unchecked checkbox for "Use Daylight Saving Time", and "Save" and "Undo" buttons. Below this, the "Current Time" is displayed as "Fri Dec 31 14:25:29 1999", with "Update" and "Refresh" buttons.

**NetComm® Super-G Wireless Firewall Router**

You Are Now In > Management > Time

Time Zone: (GMT-10:00) Hawaii

☐ Use Daylight Saving Time

Save Undo

Current Time: Fri Dec 31 14:25:29 1999

Update Refresh

**Setup Wizard**  
Internet Port  
Local Port  
Wireless LAN

**Advanced**  
Access Control List  
Content Filtering  
Dynamic DNS  
Firewall  
Remote Management  
Static Routes  
UPnP  
Virtual Server

**Management**  
Access Log  
Factory Reset  
Firmware Upgrade  
Network Status  
Save Configuration  
Time

Help ..

## 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)

### 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

## 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.

## Appendix C: Troubleshooting

This chapter is intended to help you troubleshoot problems you may encounter while setting up and using the NetComm NB600W. 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 donors, please donate.
- (4) When DDNS update fails.  
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.

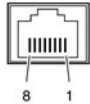
### RJ-45 Network Ports

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



Figure 2



## Straight and crossover cable configuration

There are two types of the wiring: Straight-Through Cables and Crossover Cables. Category 5 UTP/STP cable has eight wires inside the sheath. The wires form four pairs. Straight-Through Cables has same pinouts at both ends while Crossover Cables has a different pin arrangement at each end.

In a straight-through cable, wires 1,2,3,4,5,6,7 and 8 at one end of the cable are still wires 1~8 at the other end. In a crossover cable, the wires of 1,2,3,6 are reversed so that wire 1 become 3 at the other end of the cable, 2 becomes 6, and so forth.

To determine which wire is wire 1, hold the RJ-45 cable tip with the spring clip facing towards the ground and the end pointing away from you. The copper wires exposed upwards to your view. The first wire on the far left is wire 1. You can also refer to the illustrations and charts of the internal wiring on the following page.

### Straight-Through Cabling

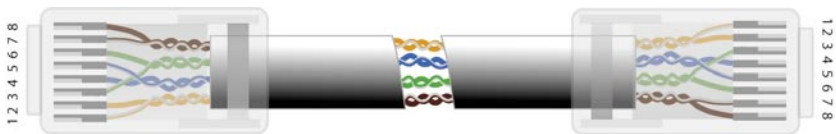


Figure 3

Wire	Becomes
1	1
2	2
3	3
6	6

### Cross-Over Cabling



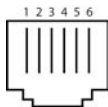
Figure 4

Wire	Becomes
1	3
2	6
3	1
6	2

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

## 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.

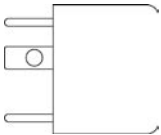


RJ-11 Connector Pin Assignment	Normal Assignment
1	Signal Ground
2	CTS
3	RXD
4	TXD
5	+5 Volts In
6	Signal Ground

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 adapter may be used to convert the supplied RJ-11 cable, if the older connection is required.



## 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.



