



# User Guide

# Contents

|   |           |
|---|-----------|
| <b>About the Router</b> .....                     | <b>5</b>  |
| Requirements.....                                 | 6         |
| Package Contents.....                             | 6         |
| Device Design.....                                |           |
| Front.....  | 7         |
| Back.....   | 8         |
| <b>Getting Started</b> .....                      | <b>10</b> |
| Planning Your Network.....                        | 10        |
| Configuring TCP/IP Settings.....                  | 11        |
| Setup the Device.....                             | 12        |
| Connecting to the Internet.....                   | 13        |
| Connecting Via Quick Setup.....                   | 13        |
| Connecting Wireless Devices.....                  | 14        |
| Web User Interface.....                           | 15        |
| Accessing the Web User Interface.....             | 15        |
| Menus.....  | 15        |
| <b>Device Info</b> .....                          | <b>17</b> |
| Device Info > Summary.....                        | 17        |
| Device Info > WAN.....                            | 17        |
| Device Info > Statistics.....                     | 18        |
| Device Info > Statistics > LAN.....               | 18        |
| Device Info > Statistics > WAN.....               | 18        |
| Device Info > Statistics > ATM.....               | 19        |
| Device Info > Statistics > ADSL.....              | 19        |
| Device Info > Route.....                          | 20        |
| Device Info > ARP.....                            | 20        |
| Device Info > DHCP.....                           | 20        |
| <b>Quick Setup</b> .....                          | <b>22</b> |
| <b>Advanced Setup</b> .....                       | <b>25</b> |
| Advanced Setup > WAN.....                         | 26        |
| Advanced Setup > LAN.....                         | 28        |
| Advanced Setup > NAT.....                         | 28        |
| Advanced Setup > NAT > Virtual Servers.....       | 29        |
| Advanced Setup > NAT > Port Triggering.....       | 29        |
| Advanced Setup > NAT > DMZ Host.....              | 29        |
| Advanced Setup > NAT > ALG.....                   | 29        |
| Advanced Setup > Security.....                    | 29        |
| Advanced Setup > Security > IP Filtering.....     | 30        |
| Outgoing IP Filtering.....                        | 30        |
| Incoming IP Filtering.....                        | 32        |
| Advanced Setup > Security > Parental Control..... | 32        |

|   |           |
|---|-----------|
| Advanced Setup > Quality of Service .....                       | 33        |
| Advanced Setup > Quality of Service > Queue Configuration ..... | 33        |
| Advanced Setup > Quality of Service > QoS Classification .....  | 34        |
| Advanced Setup > Routing .....                                  | 35        |
| Advanced Setup > Routing > Default Gateway .....                | 35        |
| Advanced Setup > Routing > Static Route .....                   | 35        |
| Advanced Setup > Routing > RIP .....                            | 35        |
| Advanced Setup > DNS .....                                      | 36        |
| Advanced Setup > DNS > DNS Server .....                         | 36        |
| Advanced Setup > DNS > Dynamic DNS .....                        | 36        |
| Using DynDNS.org .....  | 37        |
| Using TZ0 .....   | 37        |
| Advanced Setup > DSL .....                                      | 38        |
| Advanced Setup > Port Mapping .....                             | 38        |
| <b>Wireless (NB7Plus4W only) .....</b>                          | <b>40</b> |
| Wireless > Basic .....  | 41        |
| Wireless > Security .....                                       | 41        |
| Wireless > MAC Filter .....                                     | 42        |
| Wireless > Wireless Bridge .....                                | 42        |
| Wireless > Advanced .....                                       | 43        |
| Wireless > Station Info .....                                   | 43        |
| <b>Diagnostics .....</b>  | <b>45</b> |
| <b>Management .....</b>   | <b>47</b> |
| Management > Settings .....                                     | 47        |
| Management > Settings > Backup .....                            | 48        |
| Management > Settings > Update .....                            | 48        |
| Management > Settings > Restore Default .....                   | 48        |
| Management > System Log .....                                   | 49        |
| Management > TR-069 Client (NB7Plus4W only) .....               | 49        |
| Management > Internet Time .....                                | 50        |
| Management > Access Control .....                               | 51        |
| Management > Access Control > Services .....                    | 51        |
| Management > Access Control > IP Addresses .....                | 51        |
| Management > Access Control > Passwords .....                   | 52        |
| Management > Update Software .....                              | 53        |
| Management > Save/Reboot .....                                  | 53        |
| Safety Precautions .....  | 53        |
| <b>Appendix</b>   |           |
| How to change the security on the NB7Plus4W .....               | 55        |
| WEP encryption .....  | 56        |
| WPA2 encryption .....   | 56        |
| How to Bridge my NB7 Series Modem .....                         | 57        |

# About the Router



# About the Router

Your router offers an easy way of integrating your computer and other network devices into a single network. Here are some of the benefits you can obtain from using the router in your home or office:

**Integrated Modem Feature:** Your router is an ideal solution for high speed Internet connectivity. It is capable of handling the fastest data transfer speed from your Internet provider and sharing this within your local network devices.

**Strong Security:** Your router utilizes built-in firewall security to block service attacks. For added flexibility, it can be modified to allow specific applications to pass through while blocking intrusive threats at the same time.

**Intuitive User Interface:** Applying changes on the router settings can be done easily using a Web browser. The router uses a simplified user interface that allows you to apply the configurations you want for the various features of the router.

Your router will serve as the central figure in establishing your local area network (LAN) by using a combination of hardware and software. The hardware includes the cables, wireless access points, and Ethernet ports that create the path to connect your devices. The software part includes the applications that manage the flow of information in these devices.

You can complete the basic installation and Internet connection within 8 minutes. Some more time is needed if you intend to utilize more advanced functions but it can be worth it. Advanced features like port forwarding will help you create your own web server to store your Web site, Dynamic DNS allows you to access your network from the Internet, and remote access enables you to configure your router settings from different locations.

Once installation is complete, it will be much easier for you to enjoy voice communication, high speed Internet, and data/audio/video sharing within your network.

## Requirements

Your computer must meet the following minimum requirements.

- Any operating system can be used
- Internet Explorer 6.0 or Firefox 2.0
- Ethernet network adapter
- An active DSL Internet account

## Package Contents

Package contents are listed below. For any missing items, please contact your dealer immediately. Product contents vary for different models.

- Router
- Ethernet cable
- Telephone cable
- 12V 1A DC Power Adapter
- Easy Start Guide

## Device Design – Front



| Label        | Action               | Description                          |
|--------------|----------------------|--------------------------------------|
| POWER        | Off                  | No power is supplied to the device   |
|              | Steady light         | Connected to an AC power supply      |
| ETHERNET 1-4 | Off                  | No Ethernet connection               |
|              | Steady light         | Connected to an Ethernet port        |
|              | Blinking light       | Transmitting/Receiving data          |
| Wireless     | Off                  | Access point is disabled             |
|              | Steady light         | Access point is enabled              |
|              | Blinking light       | Transmitting/Receiving data          |
| DSL          | Off                  | No DSL signal                        |
|              | Blinking light       | Establishing DSL signal              |
|              | Steady light         | DSL signal is established            |
| INTERNET     | Off                  | No Internet connection               |
|              | Green light          | Connected to the Internet            |
|              | Green Blinking light | Transmitting/Receiving data          |
|              | Red Blinking light   | Cannot establish Internet connection |

## Device Design – Back



| Label             | Description  |
|-------------------|--|
| DSL               | Connecting the telephone cable                           |
| ETHERNET 1-4      | Connecting with computers/devices through Ethernet cable |
| RESET             | Resetting the device. Press for 10 seconds to reset.     |
| POWER (12V 1A DC) | Connecting with the 12V 1A DC power adapter              |
| ON/OFF            | Switching the device on/off                              |
| Antenna           | Sending/receiving wireless signals                       |



# Getting Started

# Getting Started

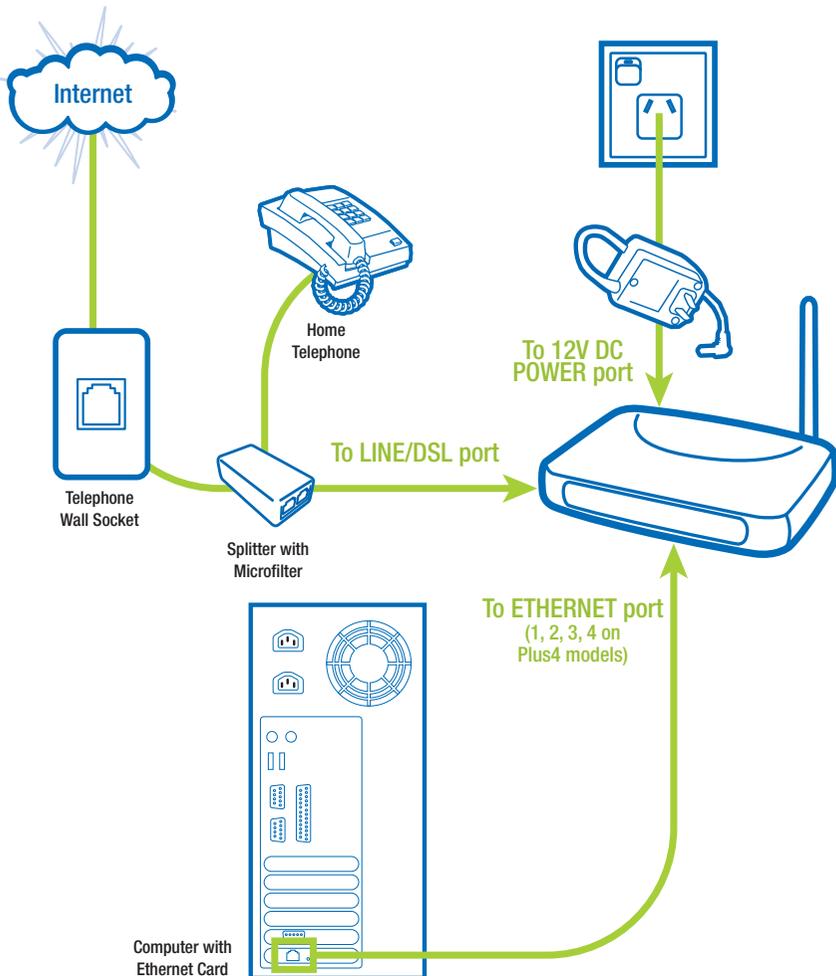
Setting up the device is easy. The diagram below provides an outline of the steps needed to complete the installation. Brief descriptions appear beside each step. Detailed instructions are provided in the subsequent pages.

## Setup the Device

When installing the router, find an area where there are enough electrical outlets for the router, the main computer, and your other computer devices.

To setup the router:

1. Plug one end of the Ethernet cable from the router's ETHERNET port and then plug the other end into the Ethernet port in your computer.
2. If you have another device you need to connect to the router, use another Ethernet cable. Plug one end of the Ethernet cable from the computer's Ethernet port and then plug the other end into an available Ethernet port in the router.
3. Plug one end of the telephone cable from the ADSL Filter's ADSL port and then plug the other end into the router's DSL port. (see **Do I need a Microfilter** on page 12)
4. Connect the power adapter from the router's 12V 1A DC port into the electrical outlet.
5. Push the power button into the on position.



## Do I need a Microfilter?

An ADSL Microfilter filters out ADSL signals to allow ADSL and regular Voice Calls to share a single telephone line.

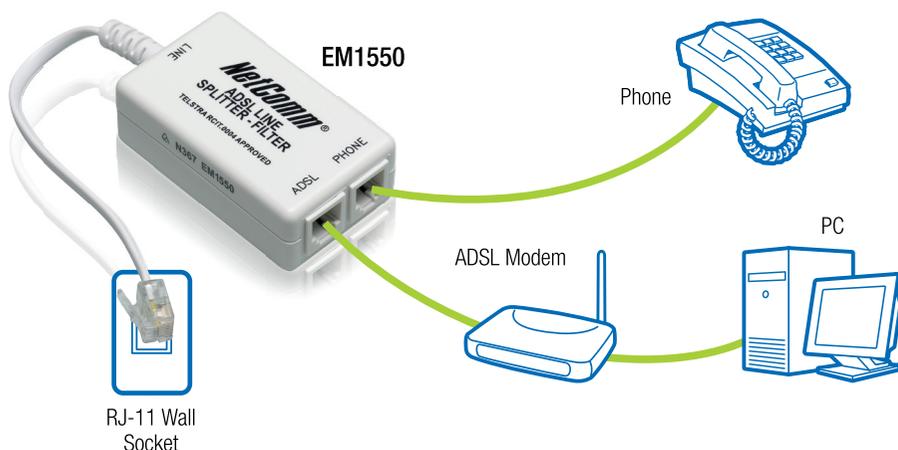
Any equipment sharing your ADSL telephone line, other than an ADSL modem must be connected to a telephone jackpoint via a microfilter. Examples of such non-ADSL equipment that MUST connect through a microfilter are :

- Telephone Handset
- Fax Machine
- Foxtel digital set
- Back to base alarm
- Modem (non adsl)
- Caller display unit
- Other devices that have an integral modem

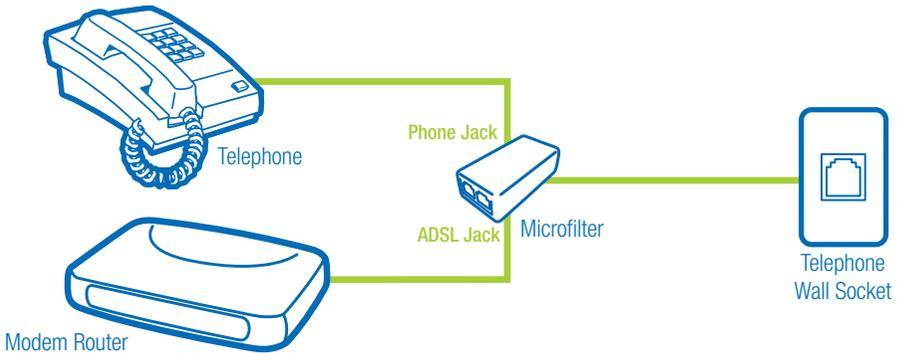
Failure to connect ALL non-ADSL equipment via a microfilter may result in loss of the data link whenever a call is made or answered. In many cases the link will also be lost when a call is received even if it is not answered.

NetComm Recommends our EM1550 ADSL2+ Microfilter to get the most out of your ADSL2+ connection

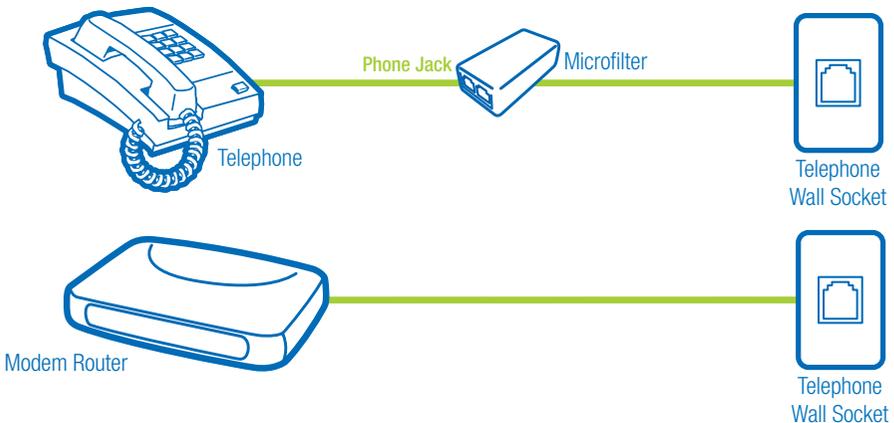
## How do I connect a Microfilter?



If you are connecting the modem to a wall socket where there is already a phone, you will need to use an ADSL Microfilter. Connect the Modem and Phone into the Microfilter as shown bellow. All other phones will need a Microfilter attached between the phone and the wall socket.



If you are connecting the modem to one phone socket and the telephone to another socket. You will not need a Microfilter for the modem but you will need one for ALL the telephone sockets.



## Web User Interface

The Web Interface is used to configure the router settings.

### Accessing the Web User Interface

To access the Web User Interface:

1. Open your browser.
2. Enter 192.168.1.1 and then press Enter.
3. Enter the User name and Password, and then click OK. The default User name and Password is admin.



## Menus

The Web User Interface includes the following menus:

- Device Info
- Quick Setup
- Advanced Setup
- Wireless
- Diagnostics
- Management



# Device Info



# Device Info

## Device Info > Summary

Summary provides an overview of the operating parameters used in your device.

### Device Info

|                           |                        |
|---------------------------|------------------------|
| Board ID:                 | 96338L-2M-8M           |
| Base MAC Address:         | 02:10:18:01:00:01      |
| Firmware Version:         | 95.2.6                 |
| Software Version:         | 3.10L.01.A2pB022g.d20e |
| Bootloader (CFE) Version: | 1.0.37-8.7             |

This information reflects the current status of your DSL connection.

|                                |             |
|--------------------------------|-------------|
| Line Rate - Upstream (Kbps):   |             |
| Line Rate - Downstream (Kbps): |             |
| LAN IP Address:                | 192.168.1.1 |
| Default Gateway:               |             |
| Primary DNS Server:            | 192.168.1.1 |
| Secondary DNS Server:          | 192.168.1.1 |

To view Summary:

1. Select Device Info.
2. Click Summary.

## Device Info > WAN

WAN displays a summary of the WAN connection settings.

| Port/VPI/VCI | Con. ID | Category | Service | Interface | Protocol | Igmp | QoS | State | Status | IP Address |
|--------------|---------|----------|---------|-----------|----------|------|-----|-------|--------|------------|
|--------------|---------|----------|---------|-----------|----------|------|-----|-------|--------|------------|

To view WAN:

1. Select Device Info.
2. Click WAN.

## Device Info > Statistics

Statistical information is provided and displayed by LAN, WAN, ATM, and ADSL.

### Device Info > Statistics > LAN

LAN displays a statistical summary of the data transaction for each interface.

#### Statistics -- LAN

| Interface | Received |      |      |       | Transmitted |      |      |       |
|-----------|----------|------|------|-------|-------------|------|------|-------|
|           | Bytes    | Pkts | Errs | Drops | Bytes       | Pkts | Errs | Drops |
| Ethernet  | 539405   | 4215 | 0    | 0     | 1473477     | 3926 | 0    | 0     |
| USB       | 0        | 0    | 0    | 0     | 0           | 0    | 0    | 0     |

Reset Statistics

To view LAN statistics:

1. Select Device Info.
2. Click Statistics > LAN.

### Device Info > Statistics > WAN

WAN displays a statistical summary of the data transaction for each connection.

#### Statistics -- WAN

| Service | VPI/VCI | Protocol | Interface | Received |      |      |       | Transmitted |      |      |       |  |  |
|---------|---------|----------|-----------|----------|------|------|-------|-------------|------|------|-------|--|--|
|         |         |          |           | Bytes    | Pkts | Errs | Drops | Bytes       | Pkts | Errs | Drops |  |  |
|         |         |          |           |          |      |      |       |             |      |      |       |  |  |

Reset Statistics

To view LAN statistics:

1. Select Device Info.
2. Click Statistics > WAN.

## Device Info > Statistics > ATM

Asynchronous Transfer Mode (ATM) displays a statistical summary of the data transaction for the ATM interface.

| ATM Interface Statistics |            |           |            |               |                           |                           |               |               |                        |                      |               |
|--------------------------|------------|-----------|------------|---------------|---------------------------|---------------------------|---------------|---------------|------------------------|----------------------|---------------|
| In Octets                | Out Octets | In Errors | In Unknown | In Hec Errors | In Invalid Vpi Vci Errors | In Port Not Enable Errors | In PTI Errors | In Idle Cells | In Circuit Type Errors | In OAM RM CRC Errors | In GFC Errors |
| 0                        | 0          | 0         | 0          | 0             | 0                         | 0                         | 0             | 0             | 0                      | 0                    | 0             |

| AAL5 Interface Statistics |            |               |                |           |            |             |              |
|---------------------------|------------|---------------|----------------|-----------|------------|-------------|--------------|
| In Octets                 | Out Octets | In Ucast Pkts | Out Ucast Pkts | In Errors | Out Errors | In Discards | Out Discards |
| 0                         | 0          | 0             | 0              | 0         | 0          | 0           | 0            |

| AAL5 VCC Statistics |              |                |                     |               |
|---------------------|--------------|----------------|---------------------|---------------|
| VPI/VCI CRC Errors  | SAR Timeouts | Oversized SDUs | Short Packet Errors | Length Errors |
|                     |              |                |                     |               |

To view ATM statistics:

1. Select Device Info.
2. Click Statistics > ATM.

## Device Info > Statistics > ADSL

ADSL displays a statistical summary of the ADSL connection.

Statistics -- ADSL

|                          |           |  |
|--------------------------|-----------|--|
| Mode:                    |           |  |
| Type:                    |           |  |
| Line Coding:             |           |  |
| Status:                  | Link Down |  |
| Link Power State:        | L0        |  |
| DownstreamUpstream       |           |  |
| SNR Margin (dB):         |           |  |
| Attenuation (dB):        |           |  |
| Output Power (dBm):      |           |  |
| Attainable Rate (Kbps):  |           |  |
| Rate (Kbps):             |           |  |
| Super Frames:            |           |  |
| Super Frame Errors:      |           |  |
| RS Words:                |           |  |
| RS Correctable Errors:   |           |  |
| RS Uncorrectable Errors: |           |  |
| HEC Errors:              |           |  |
| OCF Errors:              |           |  |
| LCD Errors:              |           |  |
| Total Cells:             |           |  |
| Data Cells:              |           |  |
| Bit Errors:              |           |  |
| Total ES:                |           |  |
| Total SES:               |           |  |
| Total UAS:               |           |  |

To view ADSL statistics:

1. Select Device Info.
2. Click Statistics > ADSL.

## Device Info > Route

Route displays the routing rules implemented in the router.

### Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate  
D - dynamic (redirect), M - modified (redirect).

| Destination | Gateway | Subnet Mask   | Flag | Metric | Service | Interface |
|-------------|---------|---------------|------|--------|---------|-----------|
| 192.168.1.0 | 0.0.0.0 | 255.255.255.0 | U    | 0      |         | br0       |

To view Route:

1. Select Device Info.
2. Click Router.

## Device Info > ARP

Address Resolution Protocol (ARP) displays the HW address of each IP device.

### Device Info -- ARP

| IP address  | Flags    | HW Address        | Device |
|-------------|----------|-------------------|--------|
| 192.168.1.2 | Complete | 00:11:43:B7:E7:F2 | br0    |

To view ARP:

1. Select Device Info.
2. Click ARP.

## Device Info > DHCP

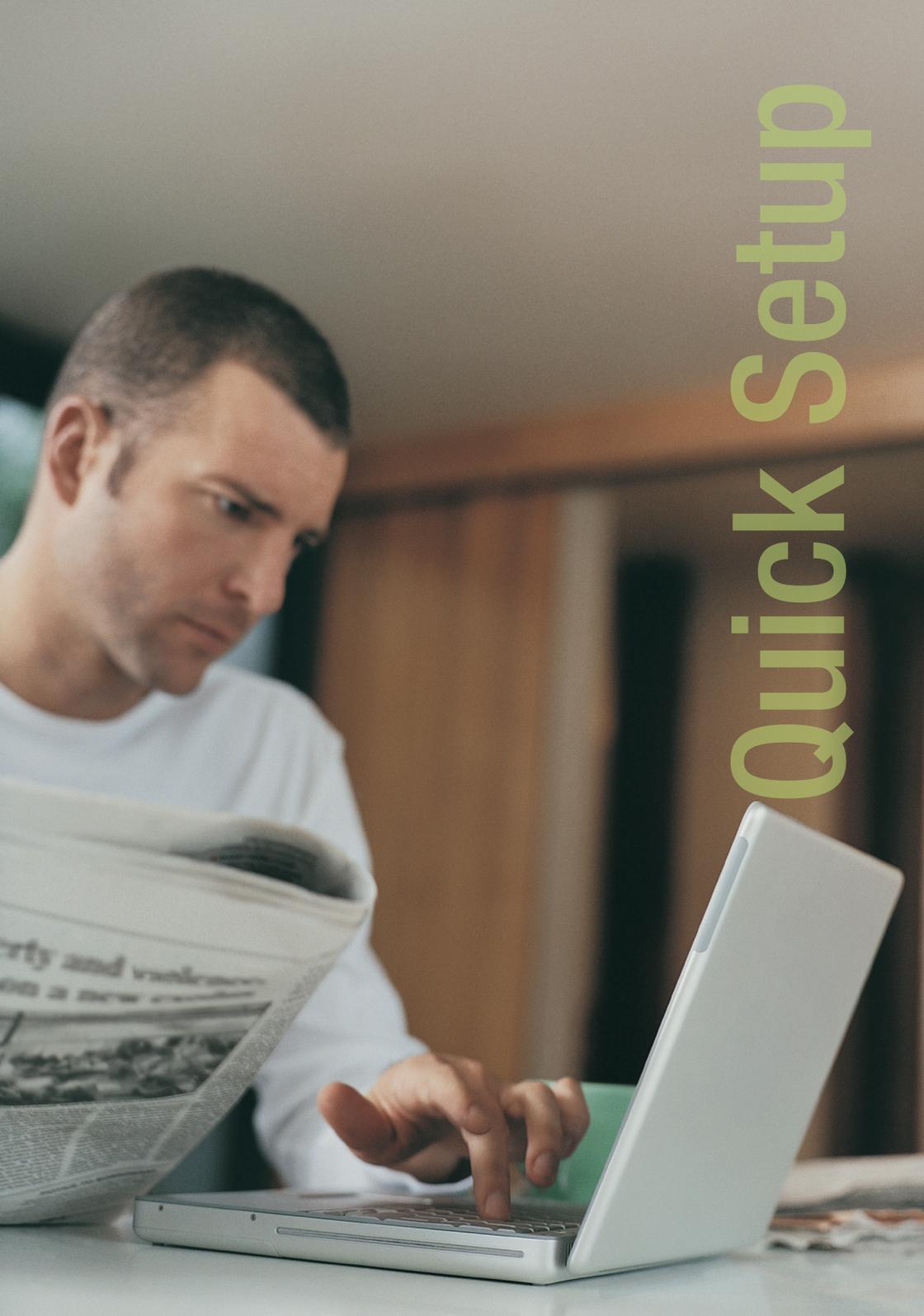
DHCP displays all the DHCP clients connected to the router.

### Device Info -- DHCP Leases

| Hostname   | MAC Address       | IP Address  | Expires In                       |
|------------|-------------------|-------------|----------------------------------|
| mycomputer | 00:11:43:B7:E7:F2 | 192.168.1.2 | 23 hours, 56 minutes, 58 seconds |

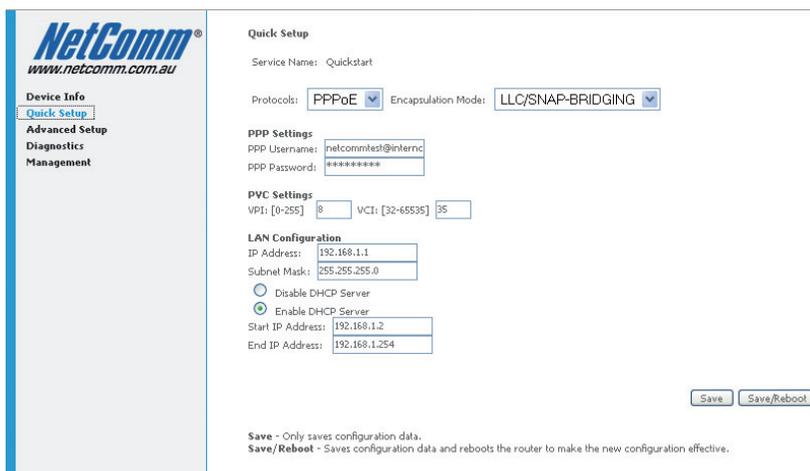
To view DHCP:

1. Select Device Info.
2. Click DHCP.



# Quick Setup

# Quick Setup



**NetComm**<sup>®</sup>  
www.netcomm.com.au

Device Info  
**Quick Setup**  
Advanced Setup  
Diagnostics  
Management

**Quick Setup**

Service Name: Quickstart

Protocols: **PPPoE** Encapsulation Mode: **LLC/SNAP-BRIDGING**

**PPP Settings**  
PPP Username: netcommtest@internc  
PPP Password: \*\*\*\*\*

**PVC Settings**  
VPI: [0-255] 0 VCI: [32-65535] 35

**LAN Configuration**  
IP Address: 192.168.1.1  
Subnet Mask: 255.255.255.0  
 Disable DHCP Server  
 Enable DHCP Server  
Start IP Address: 192.168.1.2  
End IP Address: 192.168.1.254

**Save** - Only saves configuration data.  
**Save/Reboot** - Saves configuration data and reboots the router to make the new configuration effective.

Quick Setup is used to establish an Internet connection.

To connect to the Internet via the Web Interface:

1. Open your browser.
2. Enter 192.168.1.1 and then press **Enter**.
3. Enter the User name and Password, and then click **OK**.

The default User name and Password is **admin**.

4. Select **Quick Setup**.

**Quick Setup**

Service Name: Quickstart

Protocols:  Encapsulation Mode:

**PPP Settings**

PPP Username:

PPP Password:

**PVC Settings**

VPI: [0-255]  VCI: [32-65535]

**LAN Configuration**

IP Address:

Subnet Mask:

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

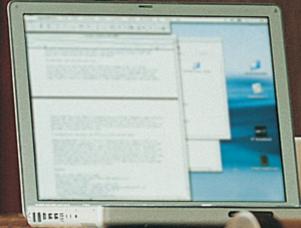
**Wireless Settings**

Enable Wireless:

Enter the wireless network name (also known as SSID).  
SSID:

5. Enter the connection settings
  - a. Enter the PPP Username and Password (provided by your ISP)
  - b. Check **Enable Wireless**
  - c. Enter a unique SSID (the SSID is your wireless network name and should be changed to a name you can recognise when scanning for wireless signals)
6. Click **Save/Reboot**.

# Advanced Setup



# Advanced Setup



## Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.

Choose Save/Reboot to apply the changes and reboot the system.

| Port/VPI/VCI | Con. ID | Category | Service    | Interface    | Protocol | Igmp     | QoS     | State   | Remove                   | Edit                                |
|--------------|---------|----------|------------|--------------|----------|----------|---------|---------|--------------------------|-------------------------------------|
| 0/8/35       | 1       | UBR      | quickstart | ppp_0_8_35_1 | PPPoE    | Disabled | Enabled | Enabled | <input type="checkbox"/> | <input type="button" value="Edit"/> |

Advanced Setup provides configuration options for other router functions.

## Advanced Setup > WAN

This screen provides a summary of the current WAN interfaces you have configured. If you have connected the NB7/NB7Plus4W to an ADSL connection through the ADSL Quick Setup interface, details of the connection will be summarized here.

### Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.  
Choose Save/Reboot to apply the changes and reboot the system.

| Port/VPI/VCI  | Con. ID | Category | Service | Interface | Protocol | Igmp | QoS | State | Remove | Edit |
|---|---------|----------|---------|-----------|----------|------|-----|-------|--------|------|
| <input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Save/Reboot"/> |         |          |         |           |          |      |     |       |        |      |

To create a new WAN connection:

1. Select Advanced Setup.
2. Click WAN.
3. Click Add.
4. Enter the connection settings:
  - a. Enter the ATM PVC Configuration, QoS Setting, and then click Next.

**ATM PVC Configuration**  
This screen allows you to configure an ATM PVC (define DORF and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [1-255]

VCI: [2-65535]

AutoCheckDPC

WAN Mode - Enable Multiple Protocols Over a Single PVC

Service Category: **URR/WithoutPCR** ▼

**Enable Quality Of Service**  
Enabling packet-level QoS for a PVC improves performance for selected classes of applications... QoS cannot be set for GBR and Realtime VBR... QoS consumes system resources, therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service

- b. Select the Connection Type, Encapsulation, and then click Next.

**Connection Type**  
Select the type of network protocol for IP over Ethernet as WAN interface

PPP over ATM (PPPoA)  
 PPP over Ethernet (PPPoE)  
 MAC Encapsulation Routing (MER)  
 IP over ATM (IPoA)  
 Bridging

**Encapsulation Mode**  
**LLC/SNAP-BRIDGING** ▼

- c. If PPPoE is selected enter in the username and password then click next

**PPP Username and Password**

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPP Service Name:

Authentication Method: **AUTO**

Dial on demand (with idle timeout timer)

Idle timer (seconds) (Default): [ 4000 ]

PPP IP extension

Advanced PPP

Non-PPP IP Address:

Non-PPP Net Mask:

Use Static IP Address

IP Address:

Retry PPP password on authentication error

Enable PPP Debug Mode

Bridge PPPd Frame Between WAN and Local Port (Default Enabled)

- d. Enable IGMP multicast if needed, then click next

**Enable IGMP Multicast, and WAN Service**

Enable IGMP Multicast

Enable WAN Service

Service Name:

[Back](#) [Next](#)

- e. Check the settings. Click Back to apply modifications.

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP:

|                    |                        |
|--------------------|------------------------|
| PORT / VPI / VCI   | 0 / 8 / 35             |
| Connection Type    | PPPoE                  |
| Service Name       | pppoe_0_0_35_1         |
| Service Category   | USB                    |
| IP Address         | Automatically Assigned |
| Service State      | Enabled                |
| NAT                | Enabled                |
| Firewall           | Enabled                |
| IGMP Multicast     | Disabled               |
| Quality Of Service | Disabled               |

Click "Save" to save these settings. Click "Back" to make any modifications.  
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

[Back](#) [Save](#)

5. Click Save.



## Advanced Setup > NAT > Port Triggering

Some applications require that the specific ports in the router's firewall be opened for access by the remote parties. For instance, an application uses port 25 for requests and port 113 for replies. If a computer on the LAN connects to port 25 on a remote server hosting this application, using Port Triggering on the router, incoming connections to port 113 (from the remote server) could be redirected to the PC which initiated the request. A maximum of 32 entries can be configured.

**NAT - Port Triggering Setup**

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the Firewall when an application on the LAN initiates a TCP/IP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

| Application | Trigger  | Open       | Remove   |
|-------------|----------|------------|----------|
| Name        | Protocol | Port Range | Protocol |
|             | Start    | End        | Start    |
|             |          |            |          |

Click Add to setup Port Triggering.

**NAT - Port Triggering**

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it. Remaining number of entries that can be configured: 32

Application Name:

Select an application:

Custom application:

| Trigger Port | Start | End | Trigger | Protocol | Open Port | Start | End | Protocol |
|--------------|-------|-----|---------|----------|-----------|-------|-----|----------|
|              |       |     | TCP     | ▼        |           |       |     | TCP      |
|              |       |     | TCP     | ▼        |           |       |     | TCP      |
|              |       |     | TCP     | ▼        |           |       |     | TCP      |
|              |       |     | TCP     | ▼        |           |       |     | TCP      |
|              |       |     | TCP     | ▼        |           |       |     | TCP      |
|              |       |     | TCP     | ▼        |           |       |     | TCP      |
|              |       |     | TCP     | ▼        |           |       |     | TCP      |
|              |       |     | TCP     | ▼        |           |       |     | TCP      |

## Advanced Setup > NAT > DMZ Host

If a computer is assigned as a DMZ Host, it will receive all the data from the Internet that does not belong to the list of applications configured as a Virtual Server. Enter the LAN IP address of the PC you wish to set as DMZ Host in the DMZ Host IP Address. If you need to disable the DMZ Host, just clear the DMZ Host IP Address field, and then click Save/Apply.

**Note:** DMZ exposes your computer to the Internet and will be vulnerable to malicious attacks.

**NAT - DMZ Host**

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

## Advanced Setup > NAT > ALG

### ALG

Select the ALG below.

SIP Enabled

An Application Layer Gateway (ALG) allows two or more simultaneous VoIP phone calls to be made by VoIP clients through this router.

## Advanced Setup > Security

### Advanced Setup > Security > IP Filtering

The router supports IP Filtering which allows you to easily set up rules to control incoming and outgoing Internet traffic. The router provides two types of IP filtering: Outgoing IP Filtering and Incoming IP Filtering.

#### Outgoing IP Filtering

By default, the router allows all outgoing Internet traffic from the LAN but by setting up Outgoing IP Filtering rules, you can block some users and/or applications from accessing the Internet.

**Outgoing IP Filtering Setup**

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

| Filter Name  | Protocol | Source Address / Mask | Source Port | Dest. Address / Mask | Dest. Port | Remove |
|--|----------|-----------------------|-------------|----------------------|------------|--------|
| <input type="button" value="Add"/> <input type="button" value="Remove"/> |          |                       |             |                      |            |        |

To create a new outgoing IP filter, click Add. The Add IP Filter-Outgoing page will be displayed.

**Add IP Filter -- Outgoing**

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Key in the following parameters:

|   |  |
|---|--|
| <b>Filter Name</b>                        | Key in the name of the filter rule.  |
| <b>Protocol</b>                           | Select the IP protocol to block.   |
| <b>Source IP Address/Subnet Mask</b>      | Enter the IP address of the PC on the LAN to block.                              |
| <b>Source Port</b>                        | Enter the port number used by the application to block.                          |
| <b>Destination IP Address/Subnet Mask</b> | Enter the IP address of the remote server to which connection should be blocked. |
| <b>Destination Port</b>                   | Enter the destination port number used by the application to block.              |

Click Save/Apply to take effect the settings. The new rule will then be displayed in the Outgoing IP Filtering table list.

To delete the rule, click Remove checkbox next to the selected rule, and click Remove.

## Incoming IP Filtering

By default, when NAT is enabled, all incoming IP traffic from WAN is blocked except for responses to requests from the LAN. However, some incoming traffic from the Internet can be accepted by setting up Incoming IP Filtering rules.

**Incoming IP Filtering Setup**

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

| Filter Name | VPI/VCI | Protocol | Source Address / Mask | Source Port | Dest. Address / Mask | Dest. Port | Remove |
|-------------|---------|----------|-----------------------|-------------|----------------------|------------|--------|
|             |         |          |                       |             |                      |            |        |

To create a new incoming IP filter, click Add. The Add IP Filter-Incoming page will be displayed.

**Add IP Filter -- Incoming**

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

**WAN Interfaces (Configured in Routing mode and with firewall enabled only)**  
 Select at least one or multiple WAN interfaces displayed below to apply this rule.

Select All

pppoe\_0\_35\_1/ppp\_0\_35\_1

Key in the following parameters:

|   |   |
|---|---|
| <b>Filter Name</b>                        | Key in the name of the filter rule.                                       |
| <b>Protocol</b>                           | Select the IP protocol to allow.  |
| <b>Source IP Address/Subnet Mask</b>      | Enter the IP address of the remote server from which to allow connection. |
| <b>Source Port</b>                        | Enter the port number used by the application to allow.                   |
| <b>Destination IP Address/Subnet Mask</b> | Enter the IP address of the PC on the LAN to which connection is allowed. |
| <b>Destination Port</b>                   | Enter the destination port number used by the application to allow.       |

Click Save/Apply to take effect the settings. The new rule will then be displayed in the Incoming IP Filtering table list.

To delete the rule, click Remove checkbox next to the selected rule, and click Remove.

## Advanced Setup > Security > Parental Control

Parental Control allows you to apply router access restrictions among LAN devices within specific times in a day. A maximum of 16 restriction rules can be created.

Time of Day Restrictions -- A maximum 16 entries can be configured.

| Username   | MAC | Mon | Tue | Wed | Thu | Fri | Sat | Sun | Start | Stop | Remove |
|--|-----|-----|-----|-----|-----|-----|-----|-----|-------|------|--------|
| <input type="button" value="Add"/> <input type="button" value="Remove"/> |     |     |     |     |     |     |     |     |       |      |        |

To add restrictions, click Add. This opens the Time of Day Restriction page. Click Start to enable a restriction or click Stop to disable the rule.

To delete a restriction, click Remove checkbox next to the selected restriction, and click Remove.

### Time of Day Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

Browser's MAC Address   
 Other MAC Address   
(xxxxxxxxxxxx)

Days of the week   
 Click to select

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Key in the following parameters:

|   |  |
|---|--|
| <b>User Name</b>                                  | Enter a descriptive name for the restriction.                          |
| <b>Browser's MAC Address or Other MAC Address</b> | Enter the device MAC Address.  |
| <b>Days of the week</b>                           | Click to select the days on which to apply the restriction.            |
| <b>Start Blocking Time (hh:mm)</b>                | Enter the time when the restriction will be enabled (00:00 to 23:59).  |
| <b>End Blocking Time (hh:mm)</b>                  | Enter the time when the restriction will be disabled (00:00 to 23:59). |

## Advanced Setup > Quality of Service

Quality of Service allows certain applications to gain priority over other applications in where a continuous flow of data packets is required. For example if someone is talking on a VoIP call and someone else starts downloading a large file the VoIP call traffic will gain priority over the download so they VoIP call will go uninterrupted.

QoS gives you the capability to specify the level of priority to be provided for specific applications. By default, QoS is not enabled.

### QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Save/Apply' button to save it.

**Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.**

**Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.**

Enable QoS

Select Default DSCP Mark:

Save/Apply

## Advanced Setup > Quality of Service > Queue Configuration

QoS Queue Configuration -- A maximum 16 entries can be configured.

| Interfacename                 | Description | Precedence | Queue Key | Enable | Remove |
|-------------------------------|-------------|------------|-----------|--------|--------|
| <p>Add Remove Save/Reboot</p> |             |            |           |        |        |

Click Add to create a QoS Queue Configuration.

### QoS Queue Configuration

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. **Note: Lower integer values for precedence imply higher priority for this queue relative to others** Click 'Save/Apply' to save and activate the filter.

Queue Configuration Status:

Queue:

Queue Precedence:

Save/Apply

## Advanced Setup > Quality of Service > QoS Classification

You can add or remove QoS Classification rules.

### Quality of Service Setup

Choose Add or Remove to configure network traffic classes.

| MARK   |           |          |             | TRAFFIC CLASSIFICATION RULES |          |      |                   |             |                  |            |                       |                      |        |       |                |        |      |
|--|-----------|----------|-------------|------------------------------|----------|------|-------------------|-------------|------------------|------------|-----------------------|----------------------|--------|-------|----------------|--------|------|
| Class Name   | DSCP Mark | Queue ID | 802.1p Mark | LAN Port                     | Protocol | DSCP | Source Addr./Mask | Source Port | Dest. Addr./Mask | Dest. Port | Source MAC Addr./Mask | Dest. MAC Addr./Mask | 802.1p | Order | Enable/Disable | Remove | Edit |
| <input type="button" value="Add"/> <input type="button" value="Save/Apply"/> |           |          |             |                              |          |      |                   |             |                  |            |                       |                      |        |       |                |        |      |

Click Add to create a Network Traffic Class Rule.

### Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

### Assign ATM Priority and/or DSCP Mark for the class

If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the corresponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.

Assign Classification Queue:

Assign Differentiated Services Code Point (DSCP) Mark:

Mark 802.1p if 802.1q is enabled:

### Specify Traffic Classification Rules

Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.

#### SET-1

Physical LAN Port:

Protocol:

Differentiated Services Code Point (DSCP) Check:

IP Address:

Source Subnet Mask:

UDP/TCP Source Port (port or port:port):

Destination IP Address:

Destination Subnet Mask:

UDP/TCP Destination Port (port or port:port):

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

#### SET-2

802.1p Priority:

## Advanced Setup > Routing

### Advanced Setup > Routing > Default Gateway

The Enable Automatic Assigned Default Gateway checkbox is ticked by default. The router will accept the first received Default Gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s).

#### Routing -- Default Gateway

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

Enable Automatic Assigned Default Gateway

### Advanced Setup > Routing > Static Route

Use this if your LAN consists of multiple subnets and you want to manually define the data transmitting paths

#### Routing -- Static Route (A maximum 32 entries can be configured)

| Destination | Subnet Mask | Gateway | Interface | Remove   |
|-------------|-------------|---------|-----------|--|
|             |             |         |           | <input type="button" value="Add"/> <input type="button" value="Remove"/> |

To create a new Static Route, click Add. The Routing-Static Route Add page will shows up.

#### Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.

Destination Network Address:

Subnet Mask:

Use Gateway IP Address

Use Interface

The key settings for adding a new Static Route are explained:

|                                    |  |
|------------------------------------|--|
| <b>Destination Network Address</b> | Enter the network address to which the data packets are to be sent.  |
| <b>Subnet Mask</b>                 | Enter the subnet mask for this destination.  |
| <b>Use Gateway IP Address</b>      | If you wish to use a specific gateway to reach the destination network, select this checkbox and then enter the IP address of the gateway. |
| <b>Use Interface</b>               | If you wish to use a particular WAN interface, select the checkbox and select the interface.   |

Click Save/Apply to take effect the settings. To delete an entry from the list, click its corresponding Remove button.

### Advanced Setup > Routing > RIP

#### Routing -- RIP Configuration

To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by giving a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

Global RIP Mode  Disabled  Enabled

| Interface     | VPI/VCI | Version | Operation | Enabled                             |
|---------------|---------|---------|-----------|-------------------------------------|
| br0           | (LAN)   | 2       | Active    | <input checked="" type="checkbox"/> |
| ppp_0_0_100_1 | 0/0/100 | 2       | Passive   | <input type="checkbox"/>            |

## Advanced Setup > DNS

### Advanced Setup > DNS > DNS Server

DNS (Domain Name System) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Therefore, each time you type a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system consists of a network of DNS servers. If one DNS server does not know how to translate a particular domain name, it asks another one and so on until the correct IP address is returned.

If you select the Enable Automatic Assigned DNS checkbox, the router will receive and use the DNS Server assigned by your ISP.

To use your preferred DNS servers, disable the Enable Automatic Assigned DNS checkbox and key in the IP address of your Primary DNS server. Adding a Secondary DNS server is optional.

#### DNS Server Configuration

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'save' button to save the new configuration. You must reboot the router to make the new configuration effective.

Enable Automatic Assigned DNS

Save

### Advanced Setup > DNS > Dynamic DNS

The router offers a Dynamic Domain Name System (DDNS) feature. 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 server behind the router.

Before using this feature, you need to sign up for DDNS service providers. The router supports these popular Dynamic DNS service providers:

- www.dyndns.org
- www.tzo.com

Click Add to create a Dynamic DNS setting.

#### Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

| Hostname | Username | Service | Interface | Remove |
|----------|----------|---------|-----------|--------|
|----------|----------|---------|-----------|--------|

Add Remove

## Using DynDNS.org

Key in the following parameters:

- D-DNS provider      Select DynDNS.org.
- Hostname             Enter the hostname.
- Interface             Select an interface.
- DynDNS Settings    Enter your dyndns.org Username and password.

### Add dynamic DDNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider     

Hostname            

Interface            

**DynDNS Settings**

Username            

Password            

## Using TZO

Key in the following parameters:

- D-DNS provider      Select TZO.
- Hostname             Enter the hostname.
- Interface             Select an interface.
- TZO Settings         Enter your TZO e-mail and key.

### Add dynamic DDNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider     

Hostname            

Interface            

**TZO Settings**

Email                

Key

## Advanced Setup > DSL

The DSL page allows you to select the modulation, the phone line pair and the capability.

**DSL Settings**

Select the modulation below.

G.Dmt Enabled  
 G.lite Enabled  
 T1.413 Enabled  
 ADSL2 Enabled  
 AnnexL Enabled  
 ADSL2+ Enabled  
 AnnexM Enabled

Select the phone line pair below.

Inner pair  
 Outer pair

Capability

Bitwap Enable  
 SRA Enable

## Advanced Setup > Port Mapping

Port Mapping allows you to create groups composed of the various interfaces available in your router.

**Port Mapping -- A maximum 16 entries can be configured**

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

| Group Name | Enable/Disable | Remove | Edit | Interfaces | Enable/Disable                      |
|------------|----------------|--------|------|------------|-------------------------------------|
| Default    |                |        |      | USB        | <input checked="" type="checkbox"/> |
|            |                |        |      | ENET       | <input checked="" type="checkbox"/> |

Click Add to create a port mapping group.

### Port Mapping Configuration

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.  
**Note that these clients may obtain public IP addresses**

3. Click Save/Apply button to make the changes effective immediately

**Note that the selected interfaces will be removed from their existing groups and added to the new group.**

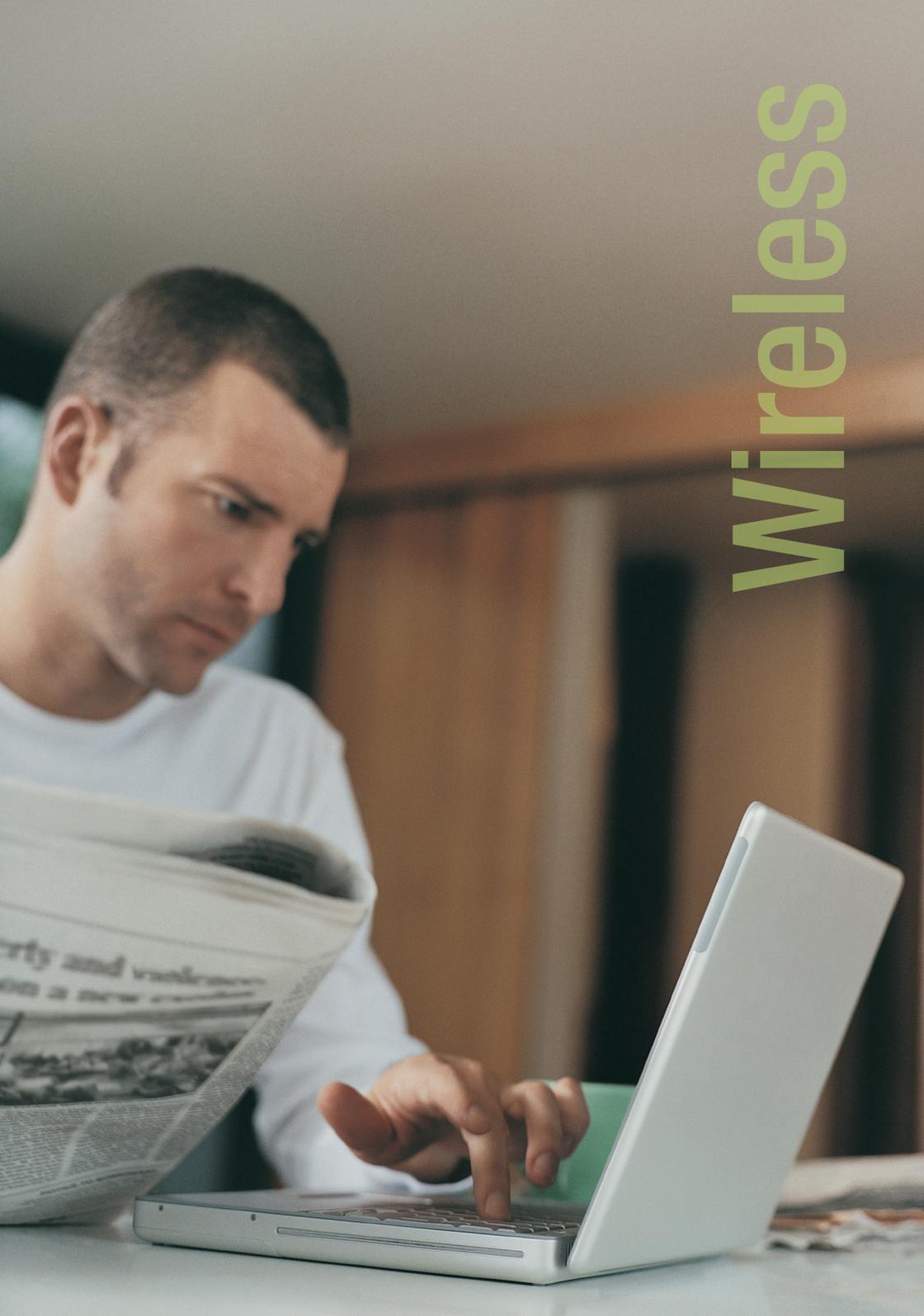
**IMPORTANT** If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

Grouped Interfaces:

Available Interfaces: ENET, USB

Automatically Add Clients With the following DHCP Vendor ID:



Wireless

# Wireless (NB7Plus4W only)

**NetComm**<sup>®</sup>  
www.netcomm.com.au

Device Info  
Quick Setup  
Advanced Setup  
**Wireless**  
Basic  
Security  
MAC Filter  
Wireless Bridge  
Advanced  
Station Info  
Diagnostics  
Management

## Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply" to configure the basic wireless options.

- Enable Wireless
- Hide Access Point
- Clients Isolation
- Disable WMM Advertise

SSID:

BSSID:

Country:

Max Clients:

- Enable Wireless Guest Network

Guest SSID:

## Wireless > Basic

The Wireless Basic page allows you to enable the wireless network and configure its basic settings.

### Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply" to configure the basic wireless options.

Enable Wireless  
 Hide Access Point  
 Clients Isolation  
 Disable WMM Advertise

SSID:   
 BSSID:   
 Country:    
 Max Clients:

Enable Wireless Guest Network  
 Guest SSID:

## Wireless > Security

The NB7Plus4W supports all encryptions within the 802.11 standard. The factory default is WEP 64bit encryption. The NB7Plus4W also supports WPA, WPA-PSK, WPA2, WPA2-PSK. (For information on setting up wireless security see [How to change the security settings page 55](#))

### Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.

#### Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network, and specify the encryption strength. Click "Save/Apply" when done.

Select SSID:    
 Network Authentication:    
 WEP Encryption:    
 Encryption Strength:    
 Current Network Key:    
 Network Key 1:   
 Network Key 2:   
 Network Key 3:   
 Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys  
 Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

## Wireless > MAC Filter

MAC Filter allows you to add or remove the MAC Address of devices which will be allowed or denied access to the wireless network.

### Wireless -- MAC Filter

MAC Restrict Mode:  Disabled  Allow  Deny

MAC Address Remove

Add Remove

Click Add to add a MAC Address.

### Wireless -- MAC Filter

Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.

MAC Address:

Save/Apply

## Wireless > Wireless Bridge

Wireless Bridge allows you to configure the router's access point as a bridge.

### Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Click "Refresh" to update the remote bridges. Wait for few seconds to update.  
Click "Save/Apply" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Refresh Save/Apply

## Wireless > Advanced

Advanced Wireless allows you to configure detailed wireless settings.

### Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click "Apply" to configure the advanced wireless options.

|                          |          |             |
|--------------------------|----------|-------------|
| Band:                    | 2.4GHz   |             |
| Channel:                 | 11       | Current: 11 |
| Auto Channel Timer(min)  | 0        |             |
| 54g™ Rate:               | Auto     |             |
| Multicast Rate:          | Auto     |             |
| Basic Rate:              | Default  |             |
| Fragmentation Threshold: | 2346     |             |
| RTS Threshold:           | 2347     |             |
| DTIM Interval:           | 1        |             |
| Beacon Interval:         | 100      |             |
| XPress™ Technology:      | Disabled |             |
| 54g™ Mode:               | 54g Auto |             |
| 54g™ Protection:         | Auto     |             |
| Preamble Type:           | long     |             |
| Transmit Power:          | 100%     |             |
| WMM(Wi-Fi Multimedia):   | Disabled |             |
| WMM No Acknowledgement:  | Disabled |             |
| WMM APSD:                | Enabled  |             |

Save/Apply

## Wireless > Station Info

This page shows the MAC address of authenticated wireless stations that are connected to the NB7Plus4W and their status

### Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

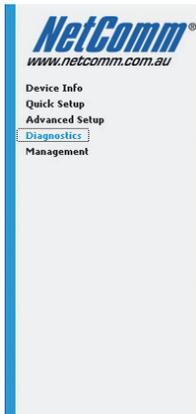
| MAC               | Associated | Authorized | SSID             | Interface |
|-------------------|------------|------------|------------------|-----------|
| 00:19:D2:32:99:CD | Yes        |            | Netcomm 7 Series | wl0       |

Refresh

# Diagnostics



# Diagnostics



## quickstart Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

### Test the connection to your local network

|                                 |      |                      |
|---------------------------------|------|----------------------|
| Test your ENET(1-4) Connection: | PASS | <a href="#">Help</a> |
|---------------------------------|------|----------------------|

### Test the connection to your DSL service provider

|                                  |      |                      |
|----------------------------------|------|----------------------|
| Test ADSL Synchronization:       | PASS | <a href="#">Help</a> |
| Test ATM OAM F5 segment ping:    | PASS | <a href="#">Help</a> |
| Test ATM OAM F5 end-to-end ping: | PASS | <a href="#">Help</a> |

### Test the connection to your Internet service provider

|                                  |      |                      |
|----------------------------------|------|----------------------|
| Test PPP server connection:      | PASS | <a href="#">Help</a> |
| Test authentication with ISP:    | PASS | <a href="#">Help</a> |
| Test the assigned IP address:    | PASS | <a href="#">Help</a> |
| Ping default gateway:            | PASS | <a href="#">Help</a> |
| Ping primary Domain Name Server: | PASS | <a href="#">Help</a> |

The router has a diagnostic feature to test your DSL connection. You can use the diagnostic menu to perform the following test functions from the router.

- Testing the connection to your local network
- Testing the connection to your DSL service provider.
- Testing the connection to your Internet service provider.

# Management



# Management



## Settings - Backup

Backup DSL router configurations. You may save your router configurations to a file on your PC.

[Backup Settings](#)

## Management > Settings

When it comes to managing the settings which you have executed to the router, you can choose to:

- Backup the settings as a configuration file stored onto your PC
- Update the current settings from a previously saved configuration file
- Erase the current settings and restore the default factory values

## Management > Settings > Backup

To backup the settings as a configuration file saved on your PC, click Backup Settings.

Select the folder where you want to save the file and key in the file name under which you want to save the settings.

### Settings - Backup

Backup DSL router configurations. You may save your router configurations to a file on your PC.

Backup Settings

## Management > Settings > Update

To import a previously saved configuration file from your PC and update the settings of your router, click Browse to locate the binary (.BIN or .IMG) upgrade file. Then click Update Settings.

### Tools -- Update Settings

Update DSL router settings. You may update your router settings using your saved files.

Settings File Name:

Update Settings

## Management > Settings > Restore Default

To restore your router to its factory default settings, click Restore Default Settings. When prompted, click OK.

Upon clicking OK, you will be prompted to follow the instruction as shown below.

### Tools -- Restore Default Settings

Restore DSL router settings to the factory defaults.

Restore Default Settings

## Management > System Log

This feature provides you a comprehensive list of log entries reporting events which you have configured for viewing.

To view the log, click View System Log.

### System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.



## Management > TR-069 Client (NB7Plus4W only)

As a TR-069 capable router, the Internet service provider can remotely update the settings of the device.

### TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply" to configure the TR-069 client options.

|   |   |
|---|---|
| Inform  | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| Inform Interval:  | <input type="text" value="300"/>                                      |
| ACS URL:  | <input type="text"/>  |
| ACS User Name:  | <input type="text" value="admin"/>                                    |
| ACS Password:   | <input type="text" value="*****"/>                                    |
| Display SOAP messages on serial console                               | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| <input checked="" type="checkbox"/> Connection Request Authentication |   |
| Connection Request User Name:   | <input type="text" value="admin"/>                                    |
| Connection Request Password:  | <input type="text" value="*****"/>                                    |

## Management > Internet Time

Enable Internet Time to automatically synchronize your time with a time server.

### Time settings

This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

First NTP time server:

Other  ntp0.coreng.com.au

Second NTP time server:

Other  ntp0.cs.mu.oz.au

Time zone offset:

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

Save/Apply

## Management > Access Control

This feature enables you manage the user access rights for remote access management based on the Services being used, IP addresses and Passwords.

### Management > Access Control > Services

Select which Services to allow and whether to allow from the LAN or the WAN.

#### Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used.

| Services | LAN  | WAN                             |
|----------|--|---------------------------------|
| FTP      | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| HTTP     | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| ICMP     | Enable                                     | <input type="checkbox"/> Enable |
| SNMP     | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| TELNET   | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| TFTP     | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |

Save/Apply

### Management > Access Control > IP Addresses

The Access Control Mode is disabled by default.

#### Access Control -- IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

Access Control Mode:  Disable  Enable

IP Address Remove

Add Remove

To allow remote management based on an authorized IP address, select Enable and click Add.

Key in the IP address of the PC from which a user will be allowed to access the web configuration menu.

Click Save/Apply to take effect the settings. Then the IP Address will be added into the table list.

To delete the existing IP address, tick the Remove checkbox next to the selected IP address in the table list and click then Remove.

#### Access Control

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

IP Address:

Save/Apply

## Management > Access Control > Passwords

When you configure the router through an Internet browser, the system requires you to enter your user name and password to validate your access permission. By default, the Username is set to "admin" and the Password to "admin".

### Access Control -- Passwords

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

Username:

Old Password:

New Password:

Confirm Password:

Save/Apply

## Management > Update Software

The router's software is stored in the FLASH memory and can be upgraded as new software is released. Click Browse to locate the software file and then click Update Software.

### Tools -- Update Software

**Step 1:** Obtain an updated software image file from your ISP.

**Step 2:** Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

**Step 3:** Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Software File Name:

## Management > Save/Reboot

This feature allows the router to enable new network configuration to take effect or to clear problems with the modem router's network connection.

**Click the button below to save and reboot the router.**

## Safety Precautions

- Do not open, service, or change any component.
- Only qualified technical specialists are allowed to service the equipment.
- Observe safety precautions to avoid electric shock
- Check voltage before connecting to the power supply. Connecting to the wrong voltage will damage the equipment.

# Appendix



# How to change the security settings

## WEP encryption

The NB7Plus4W has the WEP encryption enabled by default. To change the encryption key, please follow the steps below:

1. Connect the computer directly to the modem using an Ethernet cable.
2. Open the web configuration, <http://192.168.1.1/> from your web browser i.e. Internet explorer, Firefox.
3. At the log in screen, enter the Username and password. The default Username is "admin" and the default Password is "admin". Then click on "Login".
4. Click on "netcomm 7 series" and then click on "Security"
5. Change the Encryption Strength to either 64 bit or 128 bit.

Notes: 128bit Cipher is more secure however it will lower the data transfer speed compare to 64bit. For most home users, 64bit Cipher is adequate.

Notes: 64 bit Cipher needs 10 digits Encryption key and 128 bit Cipher needs 26 digits Encryption key.

6. Change the Network key 1 from "a1b2c3d4e5" to the new key.

Notes: WEP Encryption key can only use numbers from 0 to 9 and letters from A to F. 64 bit Cipher needs 10 digits Encryption key and 128 bit Cipher needs 26 digits Encryption key.

7. Click on "Save/Apply"

Notes: After changing the security settings, you need to remove the old wireless settings and reconfigure the wireless computer according to the new settings.

## WPA2 encryption

When a more secure connection is needed, you can change the wireless security settings on the NB7Plus4W to WPA2-PSK.

Please follow the following steps:

1. Connect the computer directly to the modem using Ethernet cable.
2. Open the web configuration, <http://192.168.1.1/> from your web browser i.e. Internet explorer, Firefox.
3. At the log in screen, enter the Username and password. The default Username is “admin” and the default password is “admin”. Then click on “Login”.
4. Click on “Wireless” and then click on “Security”
5. In the Wireless > Security page, change Network Authentication to “WPA2-PSK”
6. Enter the key in “WPA2 Pre-Shared Key” field. The key needs to be more than 8 digits and less than 63 digits and it can be any combination of letters and numbers.
7. Change the WPA2 Group Rekey Interval to “3600”
8. Click on “Save/Apply”

# How to Bridge my NB7 Series Modem

Please see the instructions below in order to bridge your NB7 Series Modem/Router:

1. Open your Web Browser (such as Internet Explorer), and enter the following numbers into the Address Bar:  
**192.168.1.1**  
If asked to login, the default username and password is **admin** and **admin**.
2. Click on **Quick Setup** from the left menu.
3. Change DHCP from **enabled** to **disabled**.
4. Select **Bridging** and then press **Save and Reboot**.

The modem will now save it's settings, and reboot itself. Please wait for 2 minutes while this process completes.

After 2 minutes, the modem will have rebooted, and will now be in Bridge Mode.

You can now connect the NB7 Series Modem into your router, and setup the router inPPPoE mode.

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

## Limitations of Warranty

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

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

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

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

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

## 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)

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

**Note:** NetComm Technical Support for this product only covers the basic installation and features outlined in the Quick Start Guide. For further information regarding the advanced features of this product, please refer to the configuring sections in the User Guide or contact a Network Specialist.