NetComm®
www.netcomm.com.au

NB8WVPN User Guide

Preface

This manual provides information related to the installation, operation, and application of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be broken or malfunctioning, please contact technical support for immediate service by email at technicalsupport@netcomm.com.au

For product update, new product release, manual revision, or software upgrades, please visit our website at http://www.NetComm.com.au

Important Safety Instructions

With reference to unpacking, installation, use and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

CAUTION:

- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

WARNING

- Disconnect the power line from the device before servicing.
- Power supply specifications

Copyright

NOTE:This document is subject to change without notice.

Save Our Environment

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

Table of Contents

1.Overview

Thank you for purchasing the NetComm NB8WVPN ADSL2+ Router. NetComm is proud to introduce this device incorporating ADSL2+ and Wireless in a single compact unit. The NB8WVPN is truly a 'broadband communications gateway' that, when attached to the appropriate ISP services, will enable multiple broadband communications streams to run concurrently into your home or office. Wireless and ethernet data services can be delivered and distributed to multiple PCs at the same time, while the gateway can be managed via 'Quality of Service' (QoS) controls to ensure that priority is given to the traffic of your choice.

Let's look at some of the capabilities offered by the NB8WVPN in brief:

ADSL Broadband The NB8WVPN offers the next generation of broadband ADSL technology with ADSL2/2+, which boosts ADSL's performance significantly,improves interoperability, and supports new applications, services and deployment conditions.

Wireless In addition to fast, standard 802.11g-based wireless, the NB8W incorporates Broadcom's state-of-the-art XPress and Afterburner technology to radically improve the performance of wirelessly-connected devices.

QoS With the addition of bandwidth-hungry applications to the SOHO/Home network the NB8WVPN has not overlooked one of the most important features for a home Internet gateway – Quality of Service (QoS) The QoS implementation in the NB8WVPN is extremely sophisticated allowing you to prioritise data on your network according to rules you make.

2.NB8WVPN Package Contents

Your **NB8WVPN** contains the following items:

- **NB8WVPN** Broadband Communications Gateway
- 18VDC 1A Power Supply
- RJ11 ADSL Line Connection Cable
- RJ45 Cat 5 Ethernet cable
- Installation CD
- Quick Start Guide

Selected terminology used in this manual

POTS	A telephone line used for a standard phone-line and service will be referred to as POTS (=Plain Old Telephone Service)
Pass-through Line	The line that connects the NB8WVPN to a POTS line may be referred to as a pass-through line
RJ11	Telephone cables may be referred to as RJ11 which is the format of the connection plug used for telephones
Ethernet	Local area network traffic will be carried by standard Category 5 cable referred to as Ethernet
RJ45	Ethernet cables may also be referred to as 'RJ45' which is the format of the connection plug used for network devices
LAN	Local Area Network
WLAN	Wireless Local Area Network

3. Minimum System Requirements

Different aspects of the **NB8WVPN** have different requirements, so let's look at them in turn. We'll start with your computer, which ought to match the following requirements if you are to enjoy the benefits of a high-speed ADSL connection and use of Wireless Networking.

PC Requirements:

- Any computer running Windows 98/2000/Me/XP Vista or Macintosh OSX
- Ethernet or Wireless Network card
- CD-ROM drive
- Web browser e.g.
  - Internet Explorer 5.1 (or better)
  - Netscape Navigator
  - Mozilla FireFox 1.0.4 (or better)

ADSL Requirement:

- ADSL broadband connection to an ISP (Internet Service Provider)
- ADSL Splitter/Filter (see below for details)

Note: Connection at ADSL2 or 2+ rate depends on the service offered by your ISP; the device will operate at standard ADSL rates in the absence of the 2 or 2+ service. Consult your ISP for details.

Wireless Requirements

- Wireless Network Interface Card (NIC) for each intended computer
- Wireless enabled computer

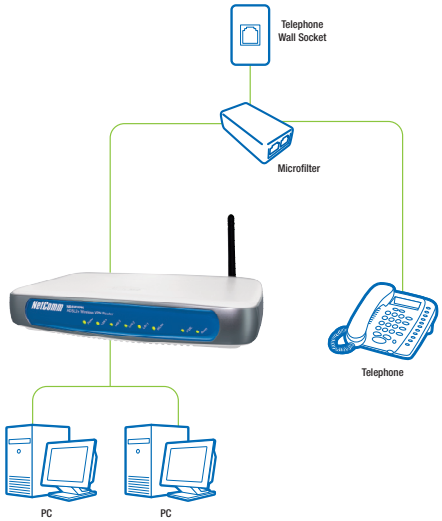
Do I need a micro filter?

Micro filters are used to prevent interference between phones and fax machines,and your ADSL service. If your ADSL-enabled phone line is being used with any equipment other than your ADSL Modem then you will need to use one Micro filter for each phone device in use.Telephones and/ or facsimiles in other rooms that are using the same line will also require Microfilters.The following diagram gives an example of connecting your ADSL Modem/ Router using a Microfilter. A suitable Microfilter can be purchased from NetComm or your Service Provider, if required.

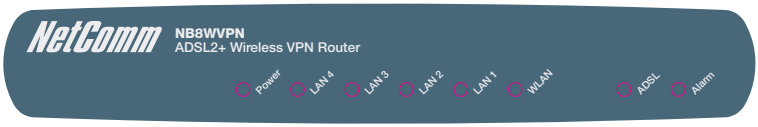
A central splitter may be installed with your ADSL service or when your current phone line is upgraded to ADSL. If your telephone line is already split you will not need to use a Microfilter on each device.- Check with your ADSL or phone service provider if you are unsure as to whether a splitter is installed at your premises.

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

A suitable Microfilter can be purchased from NetComm or your Service Provider,if required.



The front panel LED indicators are shown and explained below.



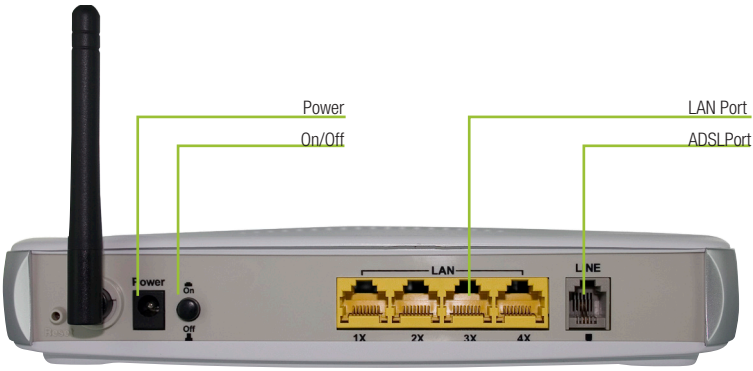
Getting to Know the **NB8WVPN**

It is recommended that you take a moment to acquaint yourself with the indicator lights, ports and default settings of the **NB8WVPN** prior to commencing with installation.

LED Indicators

LED	Colour	Mode	Function
POWER	Green	On	The router is powered up
		Off	The router is powered down
ADSL	Green	On	The ADSL Link is established
		Off	The ADSL Link is not established
	Green	Blink	The ADSL line is training or trafficis passing through
LAN 1x ~4x	Green	On	Ethernet link is established
		Off	Ethernet link is not established
	Green	Blink	Data transmitting/receiving over Ethernet
WLAN	Green	On	Wireless module is ready
		Off	Wireless module is not installed
	Green	Blink	Data transmitting/receiving over Wireless
ALARM	Red	On	The ADSL link is terminated
		Off	Normal operating status

Back Panel Ports



Port Name	Function
Reset	Reset button. Depress for 10 seconds to return your NB8WVPN to its default settings
Antenna	Wireless LAN antenna
Power	Connect the power adaptor that comes with your NB8WVPN
Power Button	Press to power on / off your NB8WVPN
4 x LAN	4 x 10/100 Base-T Ethernet jack (RJ-45) to connect to your Ethernet Network card or Ethernet Hub / Switch
ADSL	Telephone jack (RJ-11) to connect to your Telephone Wall Socket (ADSL line)

4.Default Settings

Default Settings

The following are the default LAN (Local Area Network), and WAN (Wide Area Network) settings.

LAN (Management)

- Static IP Address: 192.168.1.1;
- Subnet Mask: 255.255.255.0;
- Default Gateway: blank;

WAN (Internet)

- Empty: Once you have run through 'ADSL Quick Setup' you will have a saved WAN connection;
- Default connection type: PPPoE (most common for Australian ISPs);
- VPI / VCI: 8 / 35;

Modem Access

- Username: admin
- Password: admin

4.1 Restore Factory Default Settings

Restore Factory Defaults will reset the **NB8WVPN** to its factory default configuration.Occasions may present themselves where you need to restore the factory defaults on your **NB8WVPN** such as:

- You have lost your username and password and are unable to login to your **NB8WVPN**'s web configuration page;
- You have purchased your **NB8WVPN** from someone else and need to reconfigure the device to work with your ISP;
- You are asked to perform a factory reset by NetComm Support staff

In order to restore your **NB8WVPN** to its factory default settings, please follow these steps:

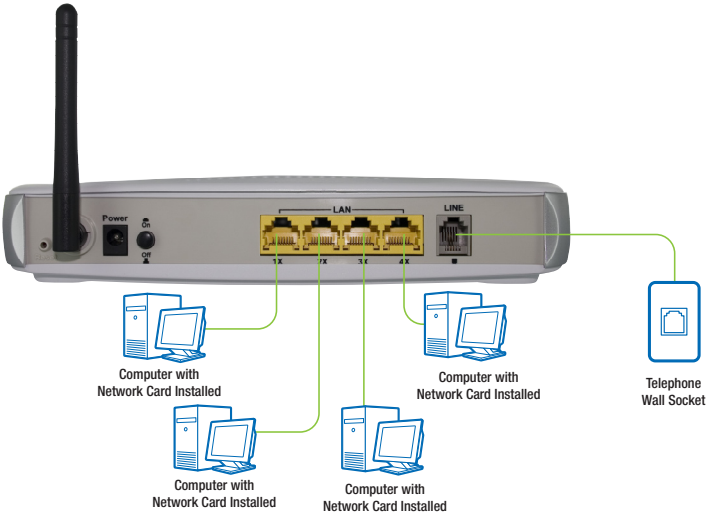
- Ensure that your **NB8WVPN** is powered on (for at least 10 seconds);
- Use a paper clip or a pencil tip to depress the reset button for ten seconds and release. At this point, the reset is in progress. Do not power off the unit at this point;
- When indicator lights return to steady green, reset is complete. The default settings are now restored. The entire process takes about 45 seconds to complete;
- Once you have reset your NB8WVPN to its default settings you will be able to access the device's configuration web interface using http://192.168.1.1 with username 'admin' and password 'admin';

5.Connecting the NB8WVPN

The diagram below shows you how to connect the NB8WVPN to your PC, ADSL and POTS service.

The initial set-up is required to get the **NB8WVPN** up and running:

1. Connecting the cables between **NB8WVPN**, PC and telephone(s) and power on
2. Establish ADSL connection
3. Set up Wireless



5.1 Connecting the Cables

Note: If you wish to link to the NB8WVPN wirelessly at the outset, see 3. Establishing a Wireless Connection below.

The **NB8WVPN** can be connected via an Ethernet cable.

To connect to your ADSL Router, you need to have either an Ethernet Port present on your Computer/Notebook.

Connecting your NB8WVPN ADSL Modem via ETHERNET

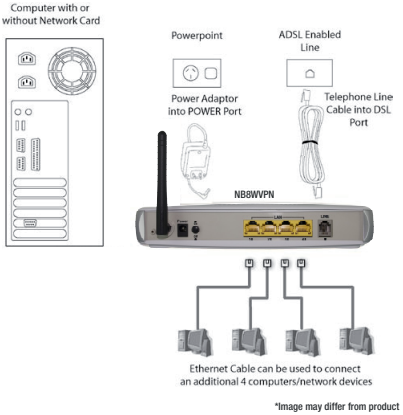


*Image may differ from product

1. Connect your **NB8WVPN** to either a computer directly or a network hub or switch using CAT5 ethernet cables.
2. Connect the power pack to the ADSL Router and switch on the power button.
3. Ensure that there is a LAN link light on the **NB8WVPN**.
4. Ensure that the computer you intend to use has an IP address in the same subnet as the **NB8WVPN** ADSL Router. (e.g. the **NB8WVPN**'s default IP is 192.168.1.1 - your computer should be on 192.168.1.100 or similar.) If you have DHCP enabled on your computer, the **NB8WVPN** will assign your computer a suitable IP address.
5. Ensure that your computer has a LAN link light.
6. Connect one end of the ADSL phone line to the **NB8WVPN** ADSL Router and the other end to the wall socket.

5.2 Establishing an ADSL connection via PPPoE

Having physically connected your **NB8WVPN**, the next step is to establish your ADSL connection to the Internet, via your ISP.

Nearly all Australian ISPs connect their clients via a standard method called PPPoE (Point-to-Point Protocol over Ethernet). Your **NB8WVPN** has a 'Quick Setup' page configured for easy access via PPPoE, so all you need do is enter the Username and Password issued by your ISP, click the 'Save & Connect' button and connection will follow. This sequence will be explained here.

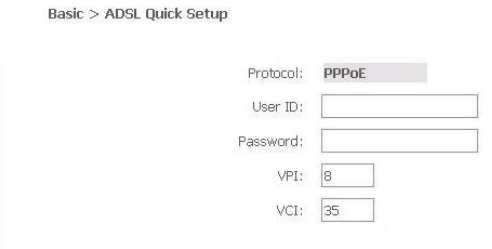
Note: If you are not using a PPPoE connection type, then consult the section under Advanced>WAN for details of choosing another connection type (e.g. PPPoA, Static, Bridge, etc.). If unsure, follow the steps in this section first.

At this point you must have your NB8WVPN connected according to Section 1, above, with your PC connected to the NB8WVPN via Ethernet cable. You must also have your ISP-supplied username and password on hand.

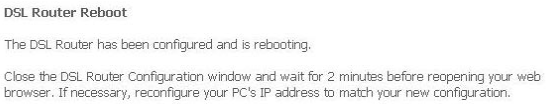
1. For Windows users, insert the accompanying CD into your CD-ROM drive. An autorun screen should appear. Click the 'Configure NB8WVPN'button;

Note: If you do not have a CD-ROM or are running a non-Windows OS, you can access the NB8WVPN Configuration page by opening a web browser and entering http://192.168.1.1 into the Address / Location field.If you are not able to access the login screen by this means, go to the section titled 'Computer Hardware Configuration'for instructions and come back here when this is completed. Otherwise, proceed to next.

2. Enter the username **'admin'** and password '**admin**' and click **'OK'**;
3. The following web page is displayed:



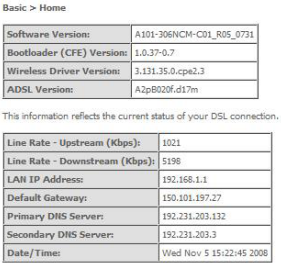
4. Enter your PPPoE User ID and PPPoE Password and click the "**Save & Reboot**" button. Do not adjust the VPI or VCI fields unless your ISP has instructed you to do so.The **NB8WVPN** will apply all of the settings in approximately 2 minutes.


DSL Router Reboot

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

5. After trying to connect the Basic > Home screen appears:


Basic > Home

Software Version:	A101-306NCM-C01_R05_0731
Bootloader (CFE) Version:	1.0.37-0.7
Wireless Driver Version:	3.131.35.0.cpe2.3
ADSL Version:	A2pB020f.d17m

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	1021
Line Rate - Downstream (Kbps):	5198
LAN IP Address:	192.168.1.1
Default Gateway:	150.101.197.27
Primary DNS Server:	192.231.203.132
Secondary DNS Server:	192.231.203.3
Date/Time:	Wed Nov 5 15:22:45 2008

5.3 Establishing your Wireless Connection

Wireless networking provides an alternative connection to using Ethernet cable. Wireless access is enabled by default on your **NB8WVPN** with the following default settings:

- Wireless network name (SSID): '**NetComm Wireless**';
- Security: WEP (64-bit) HEX key: '**a1b2c3d4e5**';

Note: For advanced wireless settings of your NB8WVPN refer to the section entitled "Advanced Settings" in this User Guide.

If you have a wireless Ethernet card on your PC, you can connect to your **NB8WVPN** by following these steps:

1. Connect the NB8WVPN as in the diagram above, except for Point 1;
2. Enable the wireless connectivity of your PC;
3. Search for available wireless networks;
4. The default name (SSID) of the **NB8WVPN's** wireless network, '**NetComm Wireless**', will appear;
5. Connect to the SSID '**NetComm Wireless**' and when prompted, enter the default HEX password which is **a1b2c3d4e5**;
6. Proceed with '**Establishing an ADSL link via PPPoE**' above.

Computer Hardware Configuration

This section provides instructions for configuring the TCP/IP(Network) settings on your computer to work with your Modem. These steps are only required if you are having trouble accessing your Modem.

Windows Vista PCs

1. In the Windows task bar, click the Start button, and then click Control Panel.
2. Click on Network & Sharing Center. (Classic View only).
3. Click Manage Network Connections in the menu on the left.
4. In the LAN or High-Speed Internet window, right-click on the icon corresponding to your network interface card (NIC) and select Properties. (Often, this icon is labelled Local Area Connection).
5. The Local Area Connection dialog box displays with a list of currently installed network items. Ensure that the check box to the left of the item labelled Internet Protocol (TCP/IP) is checked. Select Internet Protocol TCP/IP and click on Properties.
6. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labelled Obtain an IP address automatically. Also click the radio button labelled Obtain DNS server address automatically.

7. Click OK twice to confirm your changes, and close the Control Panel.

Windows® XP PCs

1. In the Windows task bar, click the Start button, and then click Control Panel.
2. Click on Network & Internet Connections icon. (Category mode only).
3. Click the Network Connections icon.
4. In the LAN or High-Speed Internet window, right-click on the icon corresponding to your network interface card (NIC) and select Properties. (Often, this icon is labelled Local Area Connection).
5. The Local Area Connection dialog box displays with a list of currently installed network items. Ensure that the check box to the left of the item labelled Internet Protocol (TCP/IP) is checked. Select Internet Protocol TCP/IP and click on Properties.
6. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labelled Obtain an IP address automatically. Also click the radio button labelled Obtain DNS server address automatically.
7. Click OK twice to confirm your changes, and close the Control Panel.

Windows 2000 PCs

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the Start button, point to Settings, and then click **Control Panel**.
2. Double-click the **Network** and **Dial-up** Connections icon.
3. In the **Network** and **Dial-up** Connections window, right-click the **Local Area Connection** icon, and then select **Properties**.
4. In the Local Area Connection Properties dialog box, select **Internet Protocol** (TCP/IP), and then click **Properties**
5. In the **Internet Protocol** (TCP/IP) Properties dialog box, click the **radio** button labelled **Obtain an IP address automatically**. Also click the **radio** button labelled **Obtain DNS server address automatically**.
6. Click **OK** twice to confirm and **save** your changes, and then close the **Control Panel**.

Windows Me PCs

1. In the Windows task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. Click on **View All Control Panel Options**.
3. Double-click the **Network** icon.

4. The **Network Properties** dialog box displays with a list of currently installed network components. If the list includes **Internet Protocol** (TCP/IP), then the protocol has already been enabled. Skip to step 10.
5. If **Internet Protocol** (TCP/IP) does not display as an installed component, click **Add**…
6. In the **Select Network Component Type** dialog box, select **Protocol**, and then click **Add**…
7. Select **Microsoft** in the Manufacturers box.
8. Select **Internet Protocol** (TCP/IP) in the Network Protocols list, and then click **OK**. You may be prompted to install files from your Windows ME installation CD or other media. Follow the instructions to install the files. If prompted, click **OK** to restart your computer with the new settings.

Next, configure the PC to accept IP information assigned by the modem:

9. Follow steps 1 – 4 above..
10. In the Network Properties dialog box, select TCP/IP, and then click **Properties**.

If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.

11. In the TCP/IP Settings dialog box, click the **radio** button labelled Obtain an IP address automatically.
12. Click **OK** twice to confirm and save your changes,and then close the Control Panel.

Windows 95, 98 PCs

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the **Start** button, point to Settings, and then click **Control Panel**.
2. Double-click the **Network** icon.
3. The Network dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled. **Skip to step 9**.
4. If TCP/IP does not display as an installed component, click **Add**… The **Select Network Component Type** dialog box displays.
5. Select **Protocol**, and then click **Add**… The **Select Network Protocol** dialog box displays.
6. Click on **Microsoft** in the Manufacturers list box, and then click **TCP/IP** in the Network Protocols list box.
7. Click **OK** to return to the Network dialog box, and then click **OK** again. You may be prompted to install files from your Windows95/98 installation CD.Follow the instructions to install the files.
8. Click **OK** to restart the PC and complete the TCP/IP installation.

Next, configure the PCs to accept IP information assigned by the Modem:

9. Follow steps **1 – 3 above**.
10. Select the network component labelled TCP/IP, and then click **Properties**. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
11. In the TCP/IP Properties dialog box, click the **IP** Address tab.
12. Click the **radio** button labelled Obtain an IP address automatically.
13. Click **OK** twice to confirm and save your changes.You will be prompted to restart Windows.
14. Click **Yes**.

Note: For detailed information regarding the advanced features of this product, refer to the Advanced Settings sections.

Your **NB8WVPN** has many advanced features that you may want or need to use in the future. Let's start by taking a look at the menus in the web interface.

1. Login to the **NB8WVPN** web interface (http://192.168.1.1);
2. Enter your username & password (default is 'admin' / 'admin');

The **NB8WVPN** has the following main menu items:

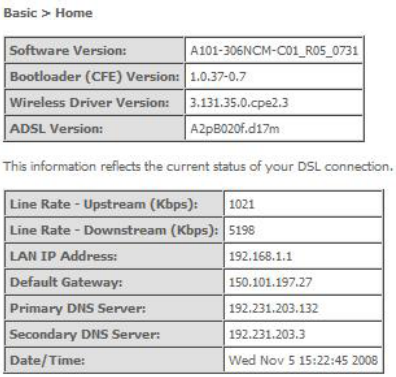
- Basic
- Wireless
- Management
- Advanced
- Status

Let's explore these menus in detail.

6.Basic

6.1 Basic>Home

The first page you see after you have successfully setup your **NB8WVPN** is the Basic > Home which provides a summary of the status of your **NB8WVPN**:


Basic > Home

Software Version:	A101-306NCM-C01_R05_0731
Bootloader (CFE) Version:	1.0.37-0.7
Wireless Driver Version:	3.131.35.0.cpe2.3
ADSL Version:	A2pB020f.d17m

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	1021
Line Rate - Downstream (Kbps):	5198
LAN IP Address:	192.168.1.1
Default Gateway:	150.101.197.27
Primary DNS Server:	192.231.203.132
Secondary DNS Server:	192.231.203.3
Date/Time:	Wed Nov 5 15:22:45 2008

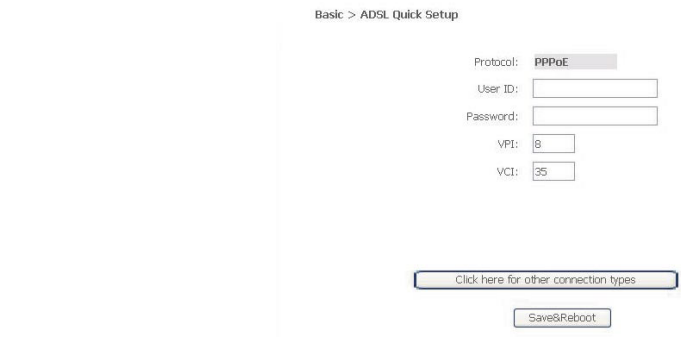
Field Description

Field	Description
Software Version	The current version of software (firmware) loaded into your NB8WVPN
Bootloader (CPE) Version	The version of the bootloader
Wireless Driver Version	The version of the wireless driver
ADSL Version	The version of the ADSL chip
Line Rate – Upstream	The upstream line rate in Kbps (e.g. 256Kbps)
Line Rate – Downstream	The downstream line rate in Kbps. (e.g. 1500 Kbps)
LAN IP Address	The IP address to access the NB8WVPN on the LAN side
Default Gateway	The default gateway that your NB8WVPN communicates with
Primary DNS Server	The primary DNS server IP address
Secondary DNS Server	The secondary DNS server IP address

6.2 Basic>ADSL Quick Setup

The **NB8WVPN** can be opened in a Web Browser window of a computer attached to the device by entering the Web address http://192.168.1.1. Enter User ID: admin and password: admin.

The 'ADSL Quick Setup' page will then be displayed when the device is first started, or if you have deleted your WAN connection settings or reset the **NB8WVPN** to factory defaults. The '**ADSL Quick Setup**' screen appears as follows:



Field	Description
User ID	The PPPoE username issued by your ISP (e.g. user@isp.com.au)
Password	The PPPoE password issued by your ISP
Save & Reboot	This button saves your settings, reboots the NB8WVPN and connects to the Internet. Once completed you will be returned to the 'Basic > Home' page

Click on **Save & Reboot**, close the browser window and wait several minutes. Then re-open browser window, if you are not automatically re-directed, then log into **NB8WVPN** again following the steps above. You will then see the Basic > Home page indicating your ADSL service status. Proceed to configure Wireless, if required.

NOTES:

* PPPoE (Point to Point Protocol over Ethernet) is the standard connection method for Australian ISPs.

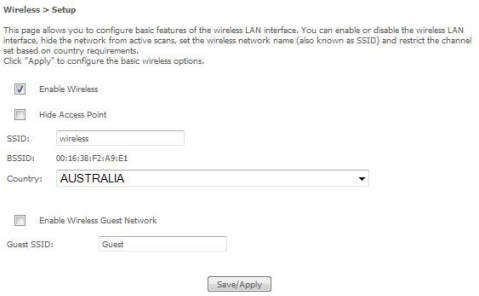
** ADSL is 'UP': this means the ADSL Sync Light must be steady green

If you do not have a PPPoE connection you can click on the link 'Click Here for Other Connection Types...' which will take you to the page from where you can select a different connection type.

7.Wireless

7.1 Wireless Setup

The **NB8WVPN** serves as an 802.11g Wireless Access Point, with enhanced capabilities provided by Broadcom's XPressTM technology. The first screen in the Wireless menus is as follows:



Field	Enter
Enable Wireless	Check Enable Wireless to turn on wireless transmission
Hide Access Point	If this is checked, wireless clients will need to know the SSID (=wireless network name) if they wish to join the network. If Hide Access point is unchecked, the SSID will be broadcast to any wireless client in range
SSID	'Station Set Identifier',or network name; replace with name of your choice. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, the wireless client will not be able to join the network. Min one character, max 32.
BSSID	The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point) and in Independent BSS or ad-hoc networks, the BSSID is generated randomly.
Country	Defaults to Australia

When settings are entered, click **Save/Apply**

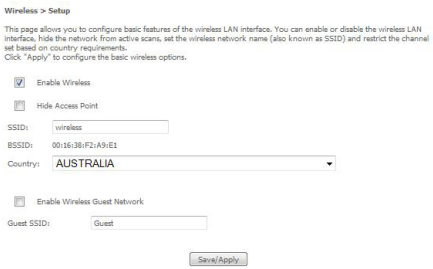
7.2 Wireless Security Quick Setup

Security settings are used to prevent unauthorised connection to your network. This can be as basic as a neighbouring user who detects and is able to connect through your wireless network, right through to actual malicious interference or 'hacking'. Whatever the case, it is a good practise to be aware of and to use wireless network security to safeguard your data and your network

Prior to considering the details of wireless security – provided later – the Quick Security Setup explains how to implement basic security on your **NB8WVPN** wireless network.

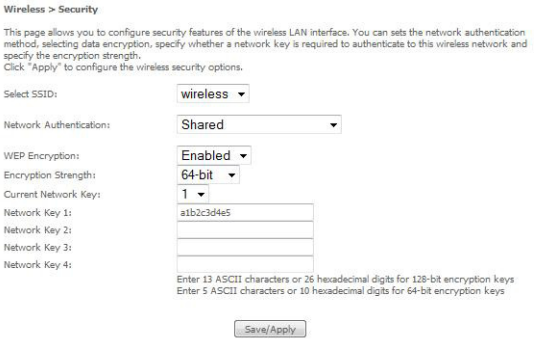
Quick Security Setup 1: WEP Security

Your **NB8WVPN** has WEP (Wired Equivalent Privacy) encryption enabled by default. Your network will not be available to passer-by or non-authorised users, and any workstation wishing to connect to your NB8WVPN must know the SSID (wireless network name) and WEP key values.



- Turn on **wireless**, and set the **SSID** or wireless network name in the Wireless Setup Screen:
- Default SSID: wireless. This can continue to be used or changed to the name of your choice.
- Next, click on **Wireless>Security**. You should see that WEP encryption is enabled by default.
- Click on **Set Encryption Key** button to either check, or change, the WEP encryption key:

  Default WEP Key: a1b2c3d4e5



You are able to change these values however it is strongly recommended that security is not turned off. It is also recommended that your SSID or network name not advertise your actual name but be kept 'generic' or anonymous.
Note: WEP Security is the appropriate choice if the network clients that wish to connect include 802.11b standard NICs.

Quick Security Setup 2 – WPA-PSK

If a stronger network security setting is required, go to Wireless>Security and select WPA-PSK from the Network Authentication drop-down menu. Enter a Network Key of your own choice; this can be from 8 to 63 characters and contain special characters and spaces.

- Select **TKIP** from **WPA encryption**
- Leave WEP as **disabled**.

Users wishing to connect to your network will need to know the SSID name and the WPA Pre-Shared Key.

Note: Wireless client network cards must be WPA-compliant to connect to your network; if in doubt check the wireless client network card documentation, or use WEP security (above).

7.3 Wireless Security in Detail

The following provides a detailed summary of wireless terms and acronyms and more in-depth explanations of the topic. It assumes little prior knowledge of wireless networking and is aimed at providing background for the terminology used in the **NB8WVPN** Wireless Security screens.

Warning: Wireless Networking is a technically challenging subject!

Authentication and Encryption

The two major aims of wireless network security are:

1. to prevent unauthorised persons from joining the network and
2. to prevent interception of network data or 'eavesdropping'. These aims are accomplished by:
   - Authentication: establishes the identity of those seeking to join the network
   - Encryption: ensures that data is protected in such a way that those outside the network cannot access it.

Network Keys

The term 'network key' is often used in the context of wireless networking. The Network Key can be a text string, although in some systems network keys are generated from a 'pass-phrase' which is entered in one field from which up to four keys are derived in fields underneath the entry field.

In all cases, the Wireless Router/Access Point and the workstations wishing to connect must use the same Network Key which needs to be communicated to clients prior to connection.

'Re-keying' refers to the frequency with which network keys are changed; for security purposes, they need to be changed frequently in case they re-occur frequently enough to identify them.

In some wireless systems, network keys are entered by a variety of means including:

- ASCII – any letter, number, or punctuation mark but no special characters
- Hex – Letters A-F, Numbers 0-9 only
- Pass phrase – enter a phrase in the top field of a set of fields, analgorithm then generates a series of keys based on the entered values.

These methods have been standardised in the later implementations of Wireless Security and are easier to use in WPA.

WEP and WPA

'WEP' stands for Wireless Equivalent Privacy and was the original wireless security method. Over time it was found to be vulnerable to attacks based on de-coding the 'keys' used to encrypt the data. While no longer recommended for enterprise-level security, WEP is certainly secure from casual interception and will repel any non-specialised attempt to join the network or intercept data; it can be penetrated with various kinds of software tools and techniques but these are beyond the capability of the average computer user.

'WPA' stands for Wi-Fi Protected Access and is an improvement on WEP. WPA2 offers further refinements to WPA.

WPA and WPA2 both comprise a number of different wireless security elements and methods that can be adapted to a variety of situations depending on the requirements. A lot of what is provided is applicable to enterprise-level wireless networking, in other words, suitable for businesses who wish to deploy strict security methods and policies for their employees. Accordingly, these technologies will exceed the requirements of home users.

An important element of WPA security is a RADIUS server (stands for Remote Access Dial-in User Service). The RADIUS server typically sits in the server room of a business or department and authenticates and manages user requests for connection. Home users will generally never have to bother about RADIUS server details.

In nearly all cases, the default security method, which is WEP, or WPA-PSK will provide adequate security for home wireless networks.

Other wireless security elements shall be explained in context below.

Network Authentication

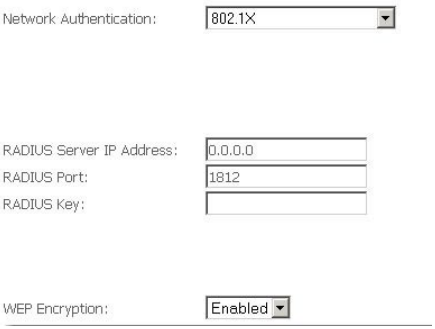
Network Authentication specifies the type of network authentication.The default value is'Open'.

Open:	Under Open System authentication, any wireless station can request authentication.
Shared:	Under Shared Key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel (i.e. verbally). To use Shared Key authentication, you must have a network key assigned to the clients trying to connect to your NB8WVPN.

802.1X

802.1X security requires the presence of a RADIUS server, and specification of the IP address of a RADIUS server, the port on which to connect to it, and the Shared Key used to authenticate with it.

Disregard this security setting unless you are setting up or connecting to a RADIUS server.



WPA

WPA also requires a RADIUS server to provide client authentication. 802.1X also requires specificationofthe'WPA Group Rekey Interval' which is the rate that the RADIUS server sends a new Group Key out to all clients. The Re-Keying process is part of WPA's enhanced security. This method also requires specification of the IP address of a RADIUS server, the port on which to connect to the RADIUS server, and the shared key used to authenticate with the RADIUS server.

WPA-PSK

WPA-PSK is a special mode of WPA providing strong encryption without access to a RADIUS server.

In this mode encryption keys are automatically changed (rekeyed) and authentication re-established between devices after a specified period referred to as the 'WPA Group Rekey Interval'.

WPA-PSK is far superior to WEP and provides stronger protection for the home/SOHO user for two reasons: first, the process used to generate the encryption key is very rigorous and second, there keying (or key changing) is done very quickly. This stops even the most determined hacker from gathering enough data to identify the key and so break the encryption.

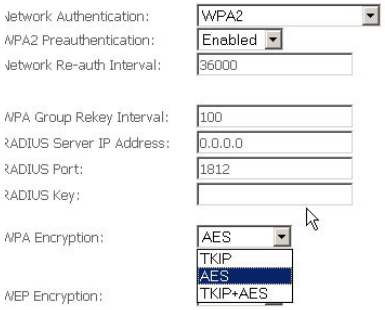
WEP is confusing because of the various types of 'network keys' vendors use (HEX, ASCII, or passphrase) and because home users mix and match equipment from multiple vendors, all using different types of keys. But WPA-PSK employs a consistent, easy to use method to secure your network. This method uses a passphrase (also called a shared secret) that must be entered in both the NB8WVPN and the wireless clients. This shared secret can be between 8 and 63 characters and can include special characters and spaces. The 'WPA Pre-Shared Key' should be a random sequence of either keyboard characters (upper and lowercase letters, numbers, and punctuation) at least 20 characters long, or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long.

Note: The less obvious, longer and more 'random' your 'WPA Pre-Shared Key', the more secure your network.

Note the following 'WPA Encryption' options:

TKIP:	The Temporal Key Integrity Protocol (TKIP) takes over after the initial shared secret is entered in your wireless devices and handles the encryption and automatic rekeying.
AES:	WPA defines the use of Advanced Encryption Standard (AES) as an additional replacement for WEP encryption. Because you may not be able to add AES support through a firmware update to your existing wireless clients / equipment, support for AES is optional and is dependent on vendor driver support.
TKIP+AES:	This will allow either TKIP or AES wireless clients to connect to your NB8WVPN.

WPA2



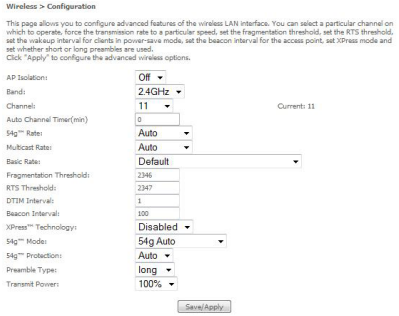
'WPA Pre-authentication' support in WPA2 allows a client to pre-authenticate with the **NB8WVPN** toward which it is moving, while maintaining a connection to the access point it's moving away from. This new capability allows the roaming to occur in less than 1/10th of a second while a traditional roam without PMK caching and pre-authentication would take more than one second. Time-sensitive applications like Citrix or video will all break without fast roaming.

'Network Re-Auth Interval' is the interval specified (seconds) that the wireless client need store-authenticate with the **NB8WVPN**.

For the remainder of the fields required, see above.

WPA2-PSK:	Same as WPA-PSK, but you can only use AES with WPA2 and not WPA.
Mixed WPA2/WPA:	Enables WPA2 or WPA wireless clients to connect to the NB8WVPN. Requires a RADIUS server to authenticate the wireless clients.
Mixed WPA2/WPA-PSK:	Enables WPA2 and WPA clients to authenticate using a PSK (Pre-Shared Key) instead of a RADIUS server.

To enter advanced settings for the wireless network hosted by the **NB8WVPN**, click on Wireless > Configuration:



Many of these fields may not need to be altered and may require interpretation by a network engineer.

Field Name	About
AP Isolation	'On': 'wireless clients associated with the access point will only be able to communicate with the Access Point
	'Off': wireless clients associated with the Access Point will be able to connect to each other 'peer-to-peer
Band	[Not alterable by end-user]
Channel	The default channel is 11. The 802.11b/g network is divided into 13 channels in Australia. Each channel broadcasts on a slightly different frequency; if you are getting interference from adjacent wireless networks, make a note of the channels that these are operating on and change your channel accordingly.
Auto Channel Timer Rate	Default rate is 'Auto' and operates at the 54 Mbps data rate when possible but drops to lower rates when necessary, dependent on signal strength and the capacity of the client stations.
Multicast Rate	Leave at default setting 'Auto' unless there is a specific requirement for multicast.
Basic Rate	Leave as default
Fragmentation Threshold	Enter a value between 256 (min) and 2346 (max).
	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented.
	If you experience a high packet error rate, try to slightly increase your 'Fragmentation Threshold'. The value should remain at its default setting of 2346 unless you are troubleshooting wireless network issues. Setting the 'Fragmentation Threshold' too low may result in poor performance.

RTS Threshold	Request To Send, set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS (Clear To Send) mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC (Network Interface Card) transmits smaller packet without using RTS/CTS.
	The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM), also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the NB8WVPN has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions. Each beacon transmission identifies the presence of an wireless client (or access point). By default, WLAN passively scan all RF channels and listen for beacons coming from access points to findasuitableaccess point.
	Before a station (wireless client) enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
	The entered value is represented in ms. Default is 100. Acceptable entry range is 1 to 0xffff (65535).
XpressTM Technology	Select 'enable' to activate in-built XpressTM Technology 1
54gTM Mode.	Select the mode to '54g Auto' for the widest compatibility. Select the mode to '54g Performance' for the fastest performance with 54g certified equipment. Set the mode to '54g LRS' if you are experiencing difficulty communicating with legacy 802.11b equipment
54g Protection.	In 'Auto' mode the NB8WVPN will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection 'Off' to maximize 802.11g throughput under most conditions
Preamble Type	Short preamble is intended for application where maximum throughput is desired but it doesn't co-operate with the legacy. Long preamble inter-operates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999
Transmit Power	The Router will set different power output (by percentage) according to this selection.

1. About XpressTM Technology

XpressTM Technology is a Broadcom innovation that dramatically improves wireless performance for suitably equipped client workstations while ensuring compatibility with 802.11b and 802.11g devices. Basically, XpressTM will communicate at the maximum rate sustainable for each class of device, and also provide very fast data transfer rates with other XpressTM-compatible network devices allowing a total theoretical bandwidth of 108Mbps.

If you are communicating with XpressTM-equipped wireless network client machines, enable XpressTM ; otherwise, don't enable.

7.4 Wireless > Mac Filter

The Wireless > MAC Filter page displays the following:

This function allows wireless access to be restricted or allowed based on the MAC address of the client device. When MAC address filtering is enabled, access is restricted to the clients that are listed as allowing to connect to the **NB8WVPN**.

Note: PROCEED CAREFULLY with this feature because if you deny or exclude your own MAC address you will lose contact with the device and need to re-set the device and restore your details.

MAC filtering is enabled for a list of specific MAC addresses and can be set to Deny or Allow.

Field Name	Comment
MAC Restrict Mode	Off – disables MAC filtering.
	Allow– permits access for the specified MAC address.
	Deny – Rejects access for specified MA Caddress.
	Click the 'Save/Apply' button when done.
Add / Remove	To Add or Remove a MAC address use these buttons.

How to find your MAC address

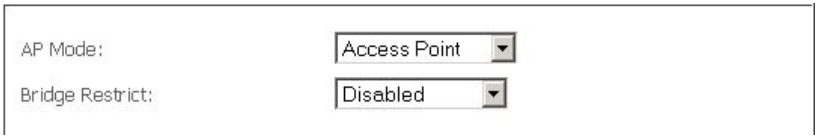
Go to Start>Run. Enter CMD and press enter. At the command prompt, type IPCONFIG/ALL.

The MAC address is referred to as a 'physical address' by Windows. It is always in the format of six groups of two characters separated by a hyphen. If the NB8WVPN does not recognise the address as valid, enter the values separated by a colon : instead of a hyphen.

7.5 Wireless > Wireless Bridge

Wireless bridge mode is used to provide a wireless link between WLAN segments to provide greater coverage or to extend network size and reach. If a wireless router is used in bridge mode, then Access Point functionality is disabled. Network Bridges operate to 'bridge' two network segments on the 'physical' or MAC link layer. This section describes how to configure the **NB8WVPN** in bridge mode.

To access the Wireless Bridge feature click on Wireless> Wireless Bridge:

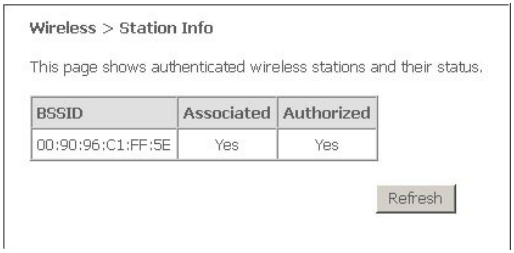


Above, default setting for **NB8WVPN** to act as Access Point.

Field Name	Comment
AP Mode	Allows you to choose between Access Point or Wireless Bridge mode.
Bridge Restrict	If AP Mode is set to Bridge, and this fieldsettoEnabled, it allows you to specify from choice of available bridge(s).
Bridge Restrict disabled	Any wireless bridge within range may connect.
Enabled (Scan)	Scans for available wireless bridges and displays MAC address of any that it has found. Click 'Refresh' to initiate scan if required, then select bridge of choice.

7.6 Wireless > Station Info

This page shows the MAC address of authenticated wireless stations that are connected to the **NB8WVPN** and their status. In the example below there is one workstation attached to the wireless network.



8.Management

8.1 Management > Device Settings > Backup

Backup enables you to save a copy of the NB8WVPN configurationfile.This can be re-loaded tor estore your settings should you need to reset the device to its factory defaults.

The default file name is back up settings.conf, or give it an explanatory name (e.g.NB8WVPNHome.conf) and save it to somewhere safe on your computer.

8.2 Management > Device Settings > Update

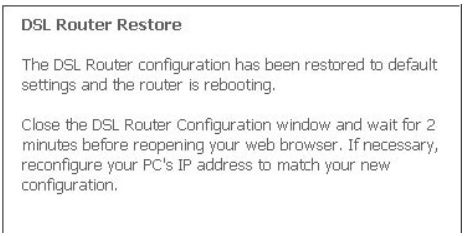
The Update option under 'Management > Device Settings' enables you to load a previously saved configuration file.Click on browse, navigate to the.config file and then click on update settings to restore settings.

8.3 Management > Device Settings > Restore Default

Clicking the 'Restore Default Configuration 'button in the Management>Restore Settings screen will restore the original factory default settings on your **NB8WVPN**.

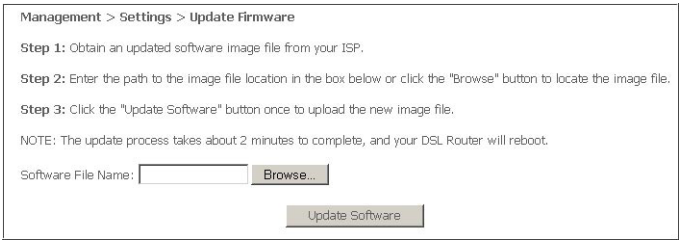
Note 1: This entry has the same effect as the hardware reset-to-default button on the rear of the NB8WVPN. The NB8WVPN hardware and the boot loader support the reset to default button. If the reset button is continuously pushed for more than 5 seconds, the boot loader will erase the entire configuration data saved on the flash memory.

Note 2: Restoring system settings requires a system reboot. This necessitates that the current Web UI session be closed and restarted.



8.4 Management > Device Settings > Update Firmware

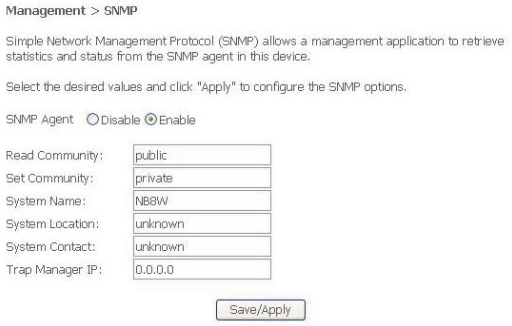
The 'Update Firmware' screen allows you to obtain an updated firmware image file from NetComm. Manual software upgrades from a locally stored file can be uploaded using this screen by selecting a firmware file saved to your hard-disk and clicking the 'Update Firmware' button.



8.5 Management > SNMP

The Simple Network Management Protocol (SNMP) allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this, the administrator typically runs an SNMP management station program such as MIB browser on a local host to obtain information from the SNMP agent, in this case the **NB8WVPN** (if SNMP enabled). An SNMP 'community' performs the function of authenticating SNMP traffic.A 'community name' acts as a password that is typically shared among SNMP agents and managers.

The 'System Log' option under the Status menu allows you to view the system event log, or to configure the 'System Log' options.



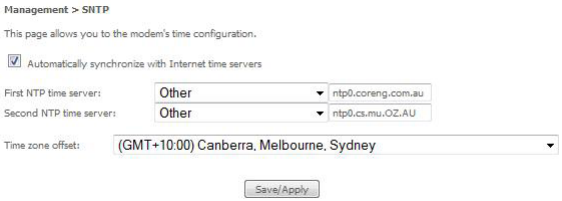
Field	Means
Read Community	Read device settings.
Set Community	Read and change device settings.
System Name	Default = NB8WVPN.
System Location	User-defined value.
System Contact	User-defined value.
Trap Manager IP	IP Address of admin machine.

8.6 Management > SNTP

The SNTP option under Management menu configures the NB8WVPN's time automatically by synchronizing with Internet time servers.

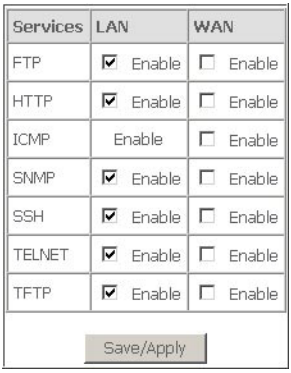
Note: The NB8WVPN is configured to Australian EST by default.

Tick the corresponding box displayed on the screen. Then click **Save/Apply**.



Management > Access Control > Services

The Services Option limits or enables selective access via the LAN or WAN via the following services:



Enable the service by checking the corresponding box and clicking **SAVE/APPLY**. You will note that all services are enabled for LAN clients and disabled for WAN clients by default.

CAUTION: If you disable HTTP access from the LAN then you may not be able to open the NB8WVPN in your Web Browser!

EXAMPLE 1: You need to access your **NB8WVPN** via the Internet from a remote location through a Web browser. Method: enable WAN access for HTTP and click Save and Apply. Then enter the address http://[WAN_IP_NB8WVPN] in the browser address bar of the remote machine.

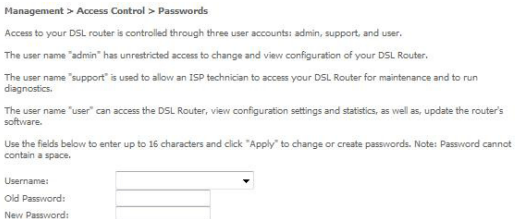
EXAMPLE 2: Assume that you already have a web server on your LAN behind the **NB8WVPN** that people connect to from the Internet. You have entered a 'Port Forwarding' entry that forwards incoming traffic on the WAN on port 80 to the LAN IP of the web server on port 80 (default for HTTP traffic). If you enable HTTP WAN access to the **NB8WVPN** you will be notified that the default port to access the **NB8WVPN** has been updated to port 8080. Therefore, your web server will not need to be reconfigured, and you can access your **NB8WVPN** on the WAN side using address http://WAN_IP_OF_NB8WVPN:8080. The same applies for other services that use conflicting ports setup in your **NB8WVPN**.

Management > Access Control > IP Addresses

The IP Addresses option limits the Access>Services by IP address. If the Access Control Mode is enabled, only the listed IP addresses can access the **NB8WVPN** for the specified services. Before the service is enabled, specify the IP addresses by clicking the Add button and entering the address details. Enter the IP address and click **Apply** to allow access.

Management > Access Control > Password

This page allows you to change the password for all user accounts. Please choose the account you wish to change, type the old password and put in the new password.



8.7 Management > Save/Reboot

The **Save/Reboot** option saves the current configuration and reboots the **NB8WVPN**.Close the **NB8WVPN**'s Configuration window and wait for 2minutes before reopening your web browser.If necessary, reconfigure your PC's IP address to match your new configuration if you have disabled the DHCP server running in your **NB8WVPN** (see Computer Hardware Configuration).

9.Advanced

9.1 Advanced > WAN

Clicking on the 'Advanced' menu displays the following:

VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	VlanId	State	Remove	Edit
8/35	1	UBR	pppoe_8_35	ppp_8_35_1	PPPoE	Disabled	Enabled	N/A	Enabled	☐	Edit

This screen provides a summary of the current WAN interfaces you have configured. If you have connected the **NB8WVPN** to ADSL through the ADSL Quick Setup interface, details of the connection will be summarised here.

Setting up a WAN profile goes through a set of steps which establishes connection parameters covering the following:

Field	Means
VPI/VCI	Always 8/35 in Australia
Con. ID	Sequence number of connection (e.g. 1,2…)
Category	ATM Service Category; leave as default
Service	Name of connection: give this a name you will recognise (e.g. ISP name)
Interface	Current WAN interface name
Protocol	Bridge or Router Mode
IGMP	Enable/Disable IGMP proxy
QoS	Enable/Disable QoS
VLAN ID	The VLAN ID of this PVC
State	Enable/Disable this WAN connection

Once settings are entered, click **Save**. Connection status can be checked under **Status>Diagnostic**s.

Choosing a WAN Profile

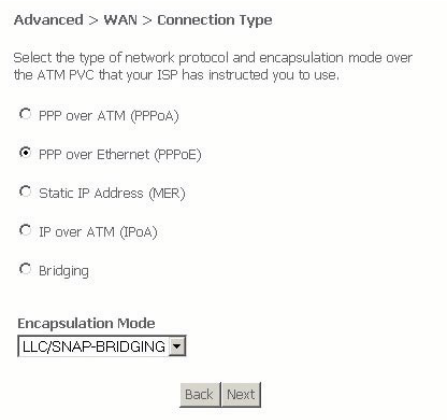
In the event that you wish to set up several connection profiles on your **NB8WVPN** for use in different locations OR with different ADSL services

- click '**Add**' to add the next connection profile
- Repeat set up steps above

You are able to cycle through connection profiles in the Status>Diagnostics window; if more than one WAN profile exists, a button will displayed for Next Connection in the sequence.

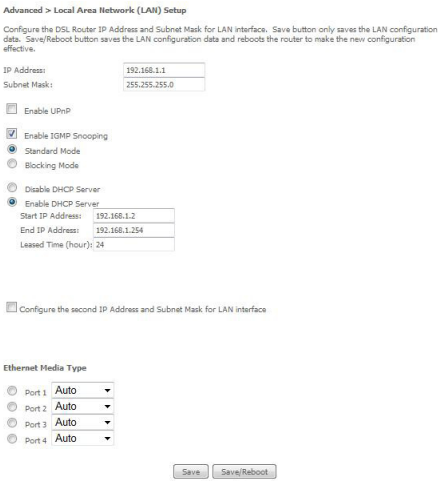
Alternative Connection Types (Inc PPPoA)

In the event that you wish to set up an alternative connection type, for example a PPPoA connection rather than the more common PPPoE type, this is done in the following screen which is accessed from Advanced>WAN>New. Select required connection type, click on **Next** and follow the prompts.



9.2 Advanced > LAN

Configure the **NB8WVPN**'s LAN IP address and sub net mask. Save button only saves the LAN configuration data.**Save/Reboot** button saves the LAN configuration data and reboots the **NB8WVPN** to make the new configuration effective.



Field	Means
LAN IP Address	Default: 192.168.1.1. The LAN IP address of your NB8WVPN.
LAN Subnet Mask	Default: 255.255.255.0. The subnet mask of your NB8WVPN. A subnet mask is used to determine what subnet an IP address belongs to. For more information on subnetting see http://www.ralphb.net/IPSubnet/.

Field	Means
Enable UPnP	Universal plug and play (UPnP) allows traffic to pass through the NB8WVPN for applications using the UPnP protocol. This feature requires one active WAN connection. In addition, the client connecting to the NB8WVPN should support this feature.
	UPnP also supports NAT Traversal which can automatically solve many NAT-related communications problems. UPnP enables applications to assign dynamic port mappings to the NB8WVPN and delete them when connections are complete.
	A typical example is the MSN Messenger application that runs on Windows. Instead of manually setting up the port mappings UPnP enables MSN Messenger to make the request to the NB8WVPN which will setup these ports dynamically. When MSN Messenger is closed the port openings will be removed from the NB8WVPN's configuration.
	Configure the second IP address and subnet mask for LAN interface. It is possible to configure a second IP address to access the NB8WVPN on. Once this box is checked you are able to enter the IP address and subnet mask.
Disable DHCP Server	Disables the DHCP server. Only to be done if Static IP address is set up.
Enable DHCP Server	Default: Enabled.
Start IP Address	Default: 192.168.1.2. The first IP address that will be issued to the first DHCP client connecting to the NB8WVPN using Ethernet cable or wirelessly.
End IP Address	Default: 192.168.1.254. The last IP address in the DHCP pool to be issued to DHCP clients connecting to the NB8WVPN.
Lease Time	Default: 24 hours. The time an IP address is assigned to a client before behind renewed.
Enable IGMP Snooping	IGMP specifies how a host can register a router in order to receive specific multicast traffic. IGMP Snooping allows the NB8WVPN to capture IGMP frames. When your NB8WVPN hears an IGMP report from a host for a given multicast group it adds the host's port number for that group. When the NB8WVPN hears an IGMP Leave, it removes the host's port from the table entry.
	Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic-thatis,itis forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group. IGMP Snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your NB8WVPN.
Save	Save the settings.
Save / Reboot	Save and reboot with the settings applied.

Advanced > NAT > Explanation

NAT stands for Network Address Translation, a process which converts private IP addresses of a computer on the internal private network to one or more public IP addresses for the Internet. NAT changes the packet headers to the new address and keeps track of each session; when packets come back from the Internet, it performs the reverse conversion to the IP address of the client machine.

Web applications operate through 'open ports' on devices attached to the Internet by initiating a query which opens a 'communication session' with the host through the open port. The presence of the NAT device prevents this process from occurring, as the NAT only admits incoming packets that have been elicited by an outgoing request; other packets are discarded.

However this causes connectivity problems, as any requests originating from applications on the other side of the NAT device - such as requests generated by network gaming and conferencing applications - will not be able to locate a port, and therefore a host, with which to communicate, as their requests are discarded by the NAT. Hence the terms 'opening', 'forwarding' and 'mapping' ports: these processes add information to the NAT table which allows the NAT router to direct incoming requests from selected applications to the appropriate port.

So Port Mapping tells the NAT router: 'when a request arrives which is intended for TCP port 1357, don't discard it, but direct it to such-and-such a port'. The port-mapping process invokes advanced routing functionality to 'bind' the Port Mapping request to the LAN client from which it originated.

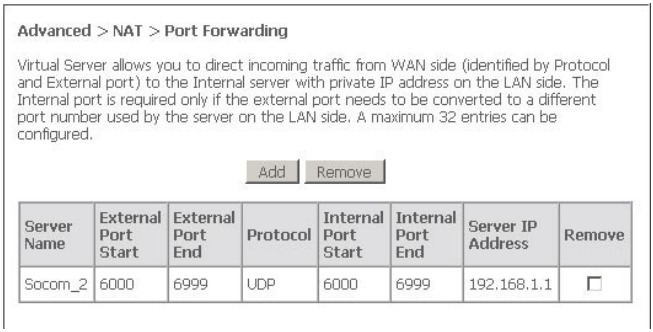
A basic NAT operation is depicted in this illustration:

Advanced > NAT > Port Forwarding

Note: This option is not available if your NB8WVPN is in Bridge mode.

To display the NAT function, you need to have enabled the NAT feature in the WAN Setup. By default, NAT is enabled on your **NB8WVPN**

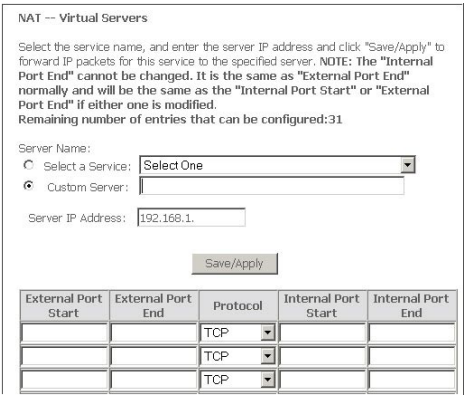
Clicking on Advanced > NAT displays the following:



The Port Forwarding feature allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

For example, you may want to setup an FTP server with IP address 192.168.1.110 on your LAN for people to connect to. The default port that an FTP server listens on is port 21. So, to this set this up you would do the following:

Click on '**Add**' .



If you are setting up a common server (e.g FTP) you can select the type of server from the dropdown list. Selecting the server will automatically configure the necessary ports:

Enter the Server's IP address (e.g. 192.168.1.110)

Click '**Save / Apply**'

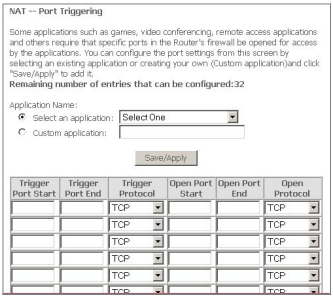
Let's take a look at the fields on this page.

Field	Means
Select a Service	Select a type of service you wish to host on your LAN.
Custom Server	Input the name for the custom server.
Server IP address	The IP address of the server on your LAN. You will notice that the first 3 octets of the address are automatically input. (e.g. 192.168.1)

Field	Means
External Port Start	The external port on the WAN side of your NB8WVPN that clients try to connect to. (e.g. port 80 on the WAN side for clients trying to connect to a web server).
External Port End	The external port end on the WAN side of your NB8WVPN that clients try to connect to. (e.g. if you are running a service that requires a range of ports to be open you would enter the last port in the range here).
Protocol	Select the protocol from the dropdown list. (e.g. if you were hosting a video service you would select UDP).
Internal Port Start	The internal port refers to the port on the server that clients try to connect to. (e.g. port 80 on the WAN side for clients trying to connect to a web server).
Internal Port End	The internal port end on the server that clients try to connect to. (e.g. if you are running a service that requires a range of ports to be open you would enter the last port in the range here).
Save / Apply	Save and Apply the settings.

Advanced > NAT > Port Triggering

Port triggering is similar to Port Forwarding however where port forwarding is tied to a specific IP address, Port triggering is dynamic and is tied to a particular application event request. The 'Custom Application' settings, or the pre-sets that are provided by the application names in the drop-down menu, allows specific ports to be opened by the named applications.The'trigger'is the out going request, which then 'opens' the ports specified in the Open Port Start-End range to enable the application to reply.

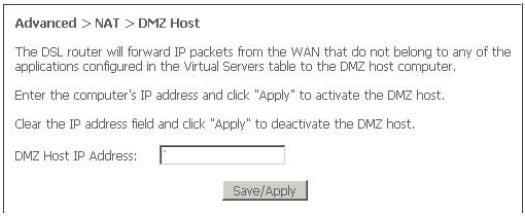


For this to work, you need to know the Outgoing Port(s) which the application uses to Send requests, and then specify the Open Port range for the reply. Some typical port ranges are as follows; for other applications, check the vendor websites.

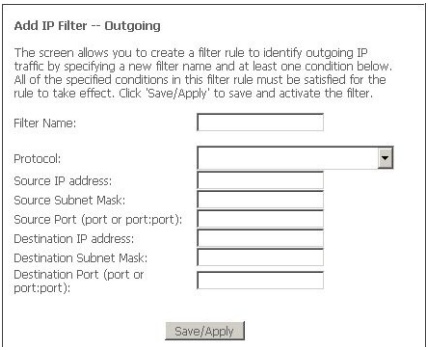
Application	Outgoing Port	Reply Port
Battle.net	6112	6112
DialPad	7175	51200, 51201,51210
ICQ	4000	4000
ICU II	2019	2000-2038, 2050-2051, 2069, 2085,3010-3030
IRC	6667	531, 6666, 6667
MSN Gaming Zone	47624	2300-2400, 28800-29000
PC to Phone	12053	12120,12122, 24150-24220
Quick Time4	554	6970-6999
wowcall	8000	4000-4020

Advanced > NAT > DMZ

A DMZ Host PC is set up 'between' your (private) LAN and the (public) WAN to allow access from the outside world to a specified and isolated zone on your network. It is most commonly used to provide access to a Web server or Game server without exposing the rest of your computers to the Internet. Enter the IP address of the DMZ computer and click 'Save/Apply'. The computer with that IP address can then serve web pages or games to the outside world, while the rest of your network remains private.



Advanced > Security > IP Filtering



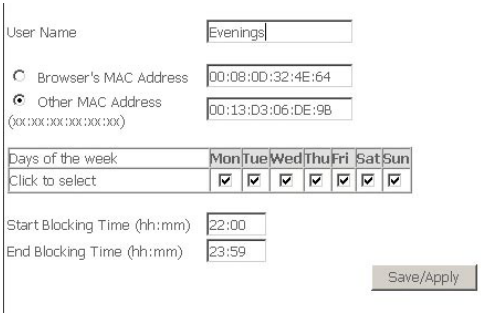
Outgoing or Ingoing IP filtering can restrict IP traffic based on various criteria.

Field Name	Comment
Filter Name	Enter name for this filter/rule
Protocol	Choose UDP/TCP or both
Source IP address	Enter source IP address
Source Subnet Mask	Enter source Subnet Mask
Source Port	Either port or port range
Destination IP address	Enter destination IP address
Destination Subnet Mask	Enter destination Subnet Mask
Destination Port	Either port or port range

Advanced > Security > Parental Control

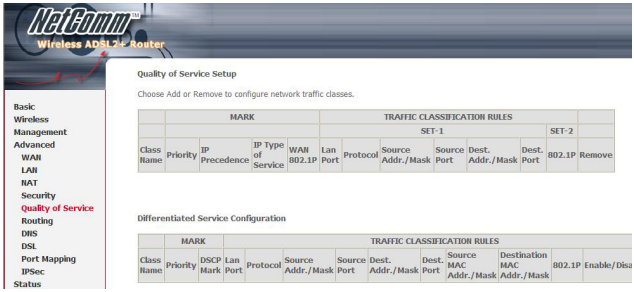
Parental Control allows **NB8WVPN** administrator to restrict access according to hours of the day. Enter target machine's MAC address and create a Rule Name (called 'User Name') and a time range. If you wish to restrict access from, say, 10:00pm until 6:30 in the morning, create two rules to cover the period 10:00-Midnight and midnight – 6:30

Parental Control: here the PC with MAC address 00:13:D3:06:DE:9B cannot access the **NB8WVPN** between 10:00pm and 11:59pm.



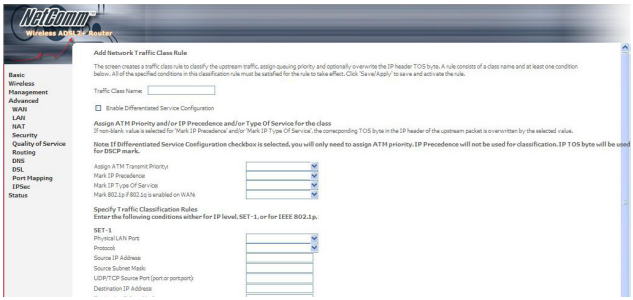
9.3 Advanced > QoS

To display the QoS function, you need to enable the QoS feature in the WAN Setup.



Choose Add to configure network traffic classes.

The following screen will be displayed:

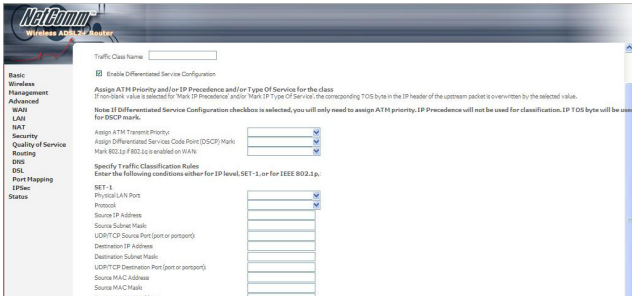


The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule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

Traffic Class Name	Enter name for traffic class.
Enable Differentiated Service Configuration	Enable Differentiated Service Configuration if required.
Assign ATM Transmit Priority	Select Low, Medium or High.
Mark IP Precedence	Select between 0-7. The lower the digit shows the higher the priority
	If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the corresponding TOS byte in the IP header of the upstream packet is overwritten by the selected value.
	Note: If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.
IP Type Of Service	Select either: Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay
	If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the corresponding TOS byte in the IP header of the upstream packet is overwritten by the selected value.
	Note: If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.
Assign Differentiated Services Code Point (DSCP) Mark	Choose the required DSCP value. Default value is "000000".
Mark 802.1p if 802.1q is enabled on WAN	Select between 0-7.

Specify Traffic Classification Rules	
Enter the following conditions either for physical LAN/Wireless port or for IP level, SET-1, or for IEEE 802.1p, SET-2	
SET-1	
Physical LAN Port	User can select from: ENET, ENET(1-4), USB, Wireless or Wireless_Guest.
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the subnet mask for the source IP address.
Source Port (port or port:port)	Enter source port number.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number.
SET-2	
802.1p Priority	Select between 0-7.

If the Enable Differentiated Service Configuration box is ticked (i.e. selected) the following screen will be displayed:



The additional Items are explained here.

Assign Differentiated Services Code Point (DSCP) Mark	The selected Code Point gives the corresponding priority to the packets that satisfies the rules set below.
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask:	This is the mask used to decide how many bits are checked in Destination MAC Address.

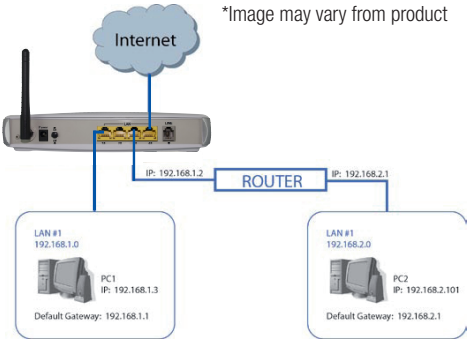
Advanced > Routing > Default Gateway

Default Gateway is checked by default and ensures that the **NB8WVPN** will accept the first received IP address assigned to it by the DHCP server to which it connects. This will generally be the ISP's server. You would only uncheck this if the **NB8WVPN** was being used in Static Routing mode (see below).

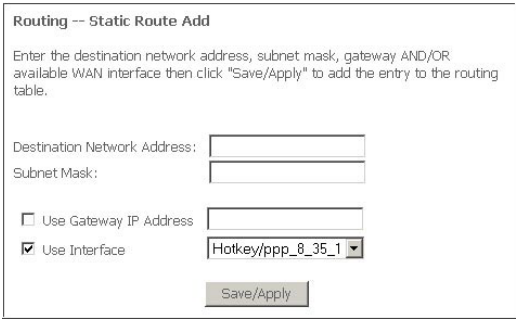
Advanced > Routing > Static Route

Static routing allows computers that are connected to the **NB8WVPN** to communicate with computers on another LAN segment which are connected to the **NB8WVPN** via another router. See diagram below for example setup:

*Image may vary from product



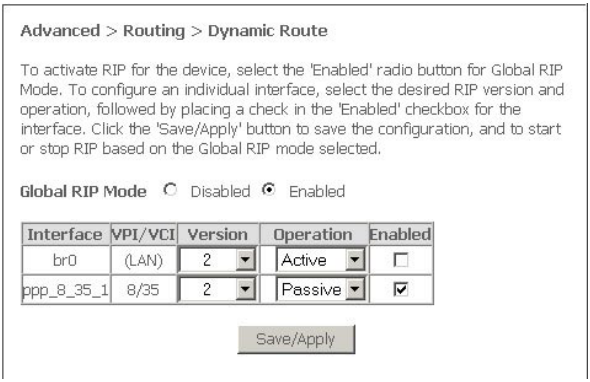
To set a static route, click add and enter the relevant details in the fields e.g.192.168.1.2



Field	Entry
Destination Network Address	LAN IP of destination address
Subnet Mask	Enter Subnet Mask for same
Use Gateway IP Address	Remote router gateway address

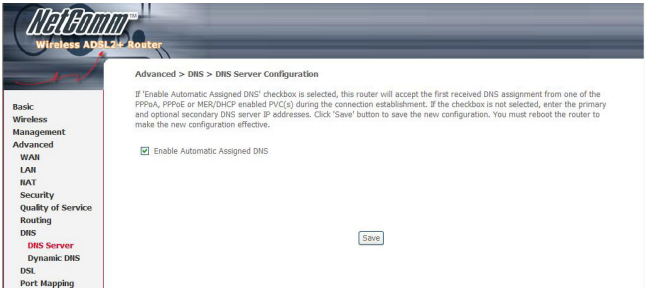
Advanced > Routing > Dynamic Route

Dynamic routing makes use of the RIP protocol to allow the **NB8WVPN** to adapt to changes in the network. RIP enables the device to determine the best route for each packet based on the 'hop count' or number of hops between Source and Destination.



Advanced > DNS > DNS Server

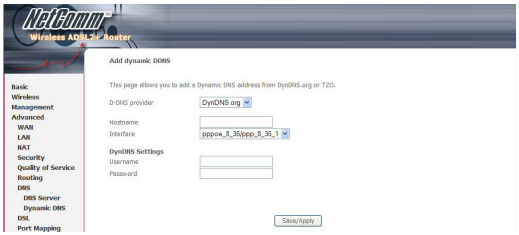
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses.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



6.7.2 Avanced > DNS > 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.

To add a dynamic DNS service, simply click the Add button. The following screen will be displayed:

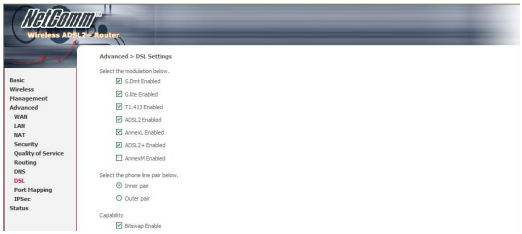


D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name for the dynamic DNS server.
Interface	Select the interface from the list
Username	Enter the username for the dynamic DNS server.
Password	Enter the password for the dynamic DNS server.

To access the DSL settings, first click On Advanced Setup and then click on DSL.

9.4 Advanced > DSL

The DSL Settings dialog box allows you to select an appropriate modulation mode.

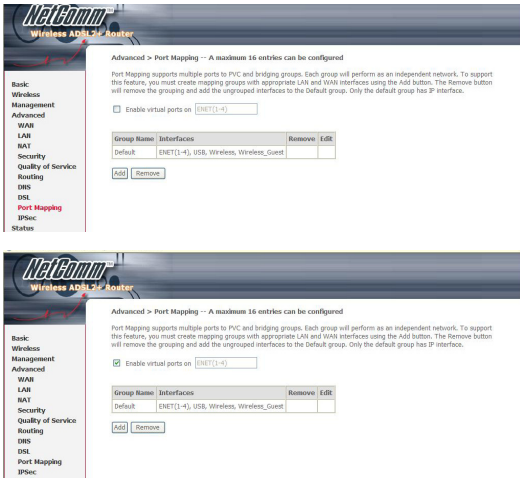


Option	Description
Auto Mode (G.dmt, G.lite or T1.413)	Sets the system auto-sense between G.Dmt, G.lite, or T1.413
G.dmt/G.lite	Sets G.Dmt/G.lite if you want the system to use either G.Dmt or G.lite mode.
T1.413	Sets the T1.413 if you want the system to use only T1.413 mode.
ADSL2 Enabled	The device can support the functions of the ADSL2.
AnnexL Enabled	The device can support/enhance the long loop test.
ADSL2+ Enabled	The device can support the functions of the ADSL2+.
AnnexM	Covers a higher “upstream” data rate version, by making use of some of the downstream channels.
Inner Pair	Reserved only
Outer Pair	Reserved only
Bitswap Enable	Allows bitswaping function
SRA Enable	Allows seamless rate adaptation

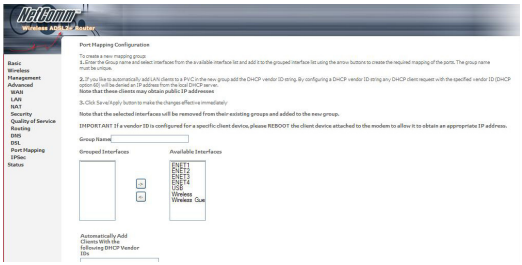
9.5 Advanced >Port Mapping

Port Mapping supports multiple port 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.

As shown below, when you tick the Enable virtual ports on, all of the LAN interfaces will be grouped together as a default.



To add a port mapping group, simply click the Add button.



To create a group from the list, first enter the group name and then select from the available interfaces on the list.

Automatically Add Clients With the Following DHCP Vendor IDs:

Add support to automatically map LAN interfaces including Wireless and USB to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when Port Mapping is enabled.

There are 4 PVCs (0/33, 0/36, 0/37, 0/38). 0/33 is for PPPoE and the others are for IP setup-box (video).

The Lan interfaces are ETH1, ETH2, ETH3, ETH4, Wireless and USB.

Port mapping configuration are:

1. Default : ENET1, ENET2, ENET3, ENET4, Wireless, Wireless_Guest and USB.
2. Video: nas_0_36, nas_0_37 and nas_0_38. The DHCP vendor ID is "Video".

The CPE's dhcp server is running on "Default". And ISP's dhcp server is running on PVC 0/36. It is for setup-box use only.

In the LAN side, PC can get IP address from CPE's dhcp server and access internet via PPPoE (0/33).

If the setup-box was connected with interface "ENET1" and send a dhcp request with vendor id "Video", CPE's dhcp server will forward this request to ISP's dhcp server.

And CPE will change the portmapping configuration automatically. The portmapping configuration will become:

1. Default : ENET2, ENET3, ENET4, Wireless, Wireless_Guest and USB.
2. Video: nas_0_36, nas_0_37, nas_0_38 and ENET1.

9.6 Configuring IPSec/VPN Tunnels

VPN/IPSec Introduction

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

IPSec Components

IPSec contains the following protocols:

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

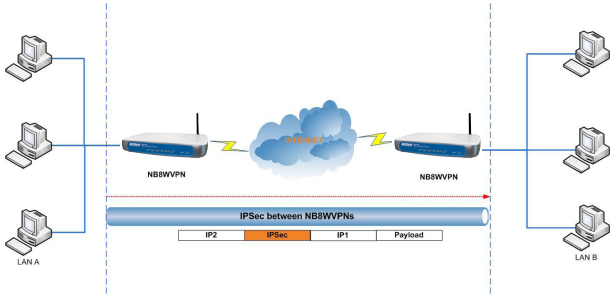
Security Association (SA)

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

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

Transport Mode

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



The tunnel mode IPSec implementation encapsulates the entire IP packet.

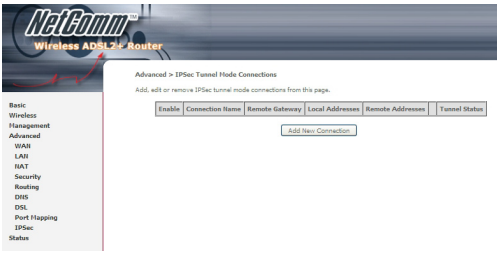
The entire packet becomes the payload of the packet that is processed with IPSec. A new IP header is created that contains the two IPSec gateway addresses. The gateways perform the encapsulation/decapsulation on behalf of the hosts. Tunnel mode ESP prevents an attacker from analyzing the data and deciphering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

Key Management

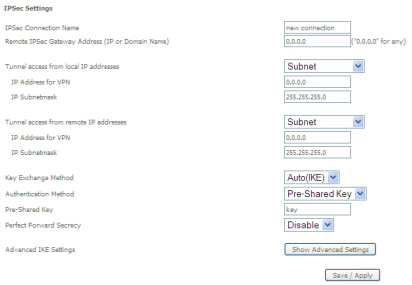
IPSec uses the Internet Key Exchange (IKE) protocol to facilitate and automate the SA setup and the exchange of keys between parties transferring data. IPSec requires that keys be re-created, or refreshed, frequently so that the parties can communicate securely with each other. IKE manages the process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

VPN / IPSec Setup

You can add, edit or remove IPSec tunnel mode connections from this page.



By clicking Add New Connection, you can add a new IPSec termination rule.



IPSec Connection Name	User-defined label
Remote IPSec Gateway Address (IP or Domain Name)	The IP address of remote tunnel Gateway, and you can use numeric address and domain name
Tunnel access from local IP addresses	It chooses methods that specify the acceptable host IP on the local side. It has single and subnet.
IP Address for VPN	If you choose “single”, please entry the host IP address for VPN. If you choose “subnet”, please entry the subnet information for VPN.
Tunnel access from remote IP addresses	It chooses methods that specify the acceptable host IP on the remote side. It has single and subnet.
IP Address for VPN	If you choose “single”, please entry the host IP address for VPN. If you choose “subnet”, please entry the subnet information for VPN.

Key Exchange Method	It has two modes. One is auto and the other is manual.
Authentication Method	It has either pre-shared key or x.509.
Pre-Shared Key	Input Pre-shared key
Perfect Forward Secrecy	Enable/disable the method that is Perfect Forward Secrecy.
Advanced IKE Settings	On IPSec Auto mode, you need to choose the setting of two phases. Click the button then choose which modes, Encryption Algorithm, Integrity Algorithm, Select Diffie-Hellman Group for Key Exchange, key time on different phases.
IPSec Connection Name	User-defined label
Remote IPSec Gateway Address (IP or Domain Name)	The IP address of remote tunnel Gateway, and you can use numeric address and domain name
Tunnel access from local IP addresses	It chooses methods that specify the acceptable host IP on the local side. It has single and subnet.
IP Address for VPN	If you choose “single”, it displays the numeric address. If you choose “subnet”, it displays two fields of numeric address and subnet mask.
Tunnel access from remote IP addresses	It chooses methods that specify the acceptable host IP on the remote side. It has single and subnet.
IP Address for VPN	If you choose “single”, it displays the numeric address. If you choose “subnet”, it displays two fields of numeric address and subnet mask.
Key Exchange Method	It has two modes. One is auto and the other is manual.
Authentication Method	It has pre-shared key and x.509.
Pre-Shared Key	Input Pre-shared key
Perfect Forward Secrecy	Enable/disable the method that is Perfect Forward Secrecy.
Advanced IKE Settings	On IPSec Auto mode, you need to choose the setting of two phases. You click the button then choose which modes, Encryption Algorithm, Integrity Algorithm, Select Diffie-Hellman Group for Key Exchange, key time on different phases.

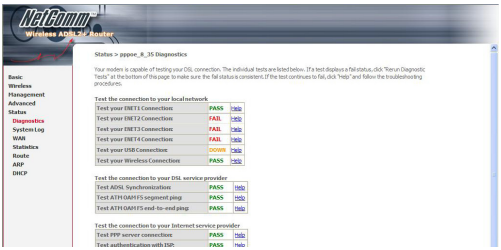
Example: Tunnel between Two VPN Routers

Parameter	NB8VPN-A	NB8VPN-B
LAN IP:	192.168.1.1	192.168.2.1
WAN IP:	210.241.239.77	211.21.189.53
Default Gateway:	210.241.239.73	211.21.189.49
Remote IPSec Gateway Address	211.21.189.53	210.241.239.77
IPSec Connection Name:	Tunnel 1	Tunnel 1
Tunnel access from local IP addresses:		
IP Address for VPN	192.168.1.0	192.168.2.0
IP Subnetmask	255.255.255.0	255.255.255.0
Tunnel access from remote IP addresses		
IP Address for VPN	192.168.2.0	192.168.1.0
IP Subnetmask	255.255.255.0	255.255.255.0
Key Exchange Method	Manual	Manual
Encryption Algorithm	DES	DES
Authentication Algorithm	MD5	MD5

10.Status

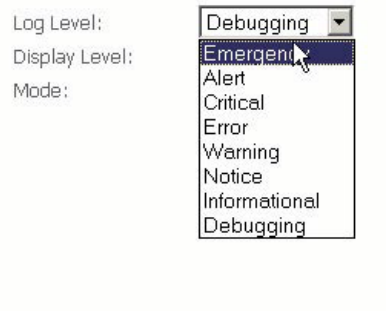
10.1 Status > Diagnostics

Self explanatory. A series of indicators about various parameters of your broadband connection. Use to troubleshoot connection problems; in event of a fail signifier, click on fail and follow troubleshooting instructions. Note the Ping Default Gateway is an optional parameter and fail may not affect connection.



10.2 Status > System Log

Click on View System Log to view entries or on Configure to set parameters for log entries. Applicable to network or device engineers and administrators.



Field Description	
Configure>Log Level	Select level of application event to log
Display Level	Select level of application event to display
Mode	Remote admin, local admin or both

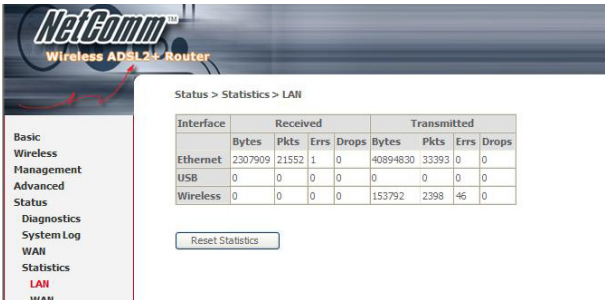
10.3 Status > WAN

Displays summary of current WAN connection including your 'Public' WAN IP (last cell in display).

VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Status	IP Address
8/35	1	UBR	pppoe_8_35	ppp_8_35_1	PPPoE	Disabled	Enabled	Enabled	Up	121.44.27.231

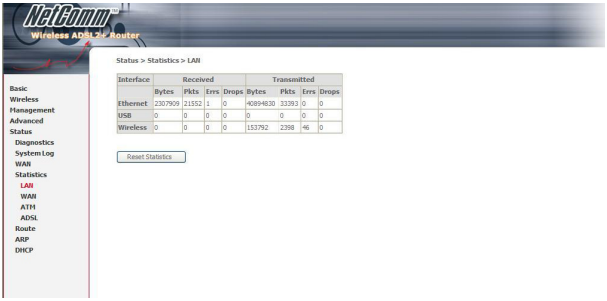
10.4 Status > Statistics

Selection of the Statistics screen provides statistics for the Network Interface of LAN, WAN, ATM, ADSL and VDSL. All statistics screens are updated every 15 seconds.

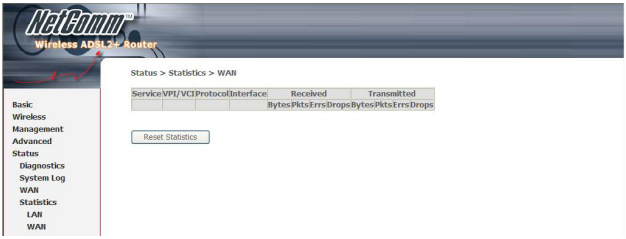


10.5 Status > LAN Statistics

The Network Statistics screen shows the interface statistics for the ATM AAL5 interface, and Ethernet interfaces. (The Network Statistics screen shows the interface statistics for the LAN interface. This provides byte transfer, packet transfer, Error and Drop statistics for the LAN interface.)



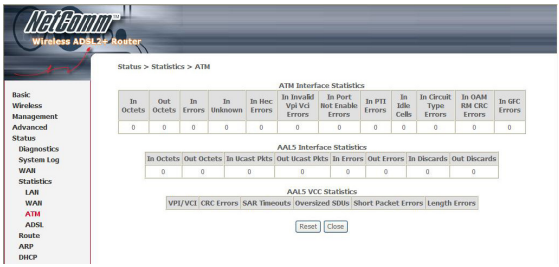
10.6 Status > WAN Statistics



Service	Shows the service type
VPI/VCI	Shows the values of the ATM VPI/VCI
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
Interface	Shows connection interfaces
Received/Transmitted - Bytes	Rx/TX (receive/transmit) packet in Bytes
- Pkts	Rx/TX (receive/transmit) packets
- Errs	Rx/TX (receive/transmit) the errored packets
- Drops	Rx/TX (receive/transmit) dropped packets

10.7 Status > ATM statistics

The following figure shows the ATM statistics screen.



ATM Interface Statistics

Field	Description
In Octets	Number of received octets over the interface
Out Octets	Number of transmitted octets over the interface
In Errors	Number of cells dropped due to uncorrectable HEC errors
In Unknown	Number of received cells discarded during cell header validation, including cells with unrecognized VPI/VCI values, and cells with invalid cell header patterns. If cells with undefined PTI values are discarded, they are also counted here.
In Hec Errors	Number of cells received with an ATM Cell Header HEC error
In Invalid Vpi Vci Errors	Number of cells received with an unregistered VCC address.
In Port Not Enabled Errors	Number of cells received on a port that has not been enabled.
In PTI Errors	Number of cells received with an ATM header Payload Type Indicator (PTI) error
In Idle Cells	Number of idle cells received
In Circuit Type Errors	Number of cells received with an illegal circuit type
In Oam RM CRC Errors	Number of OAM and RM cells received with CRC errors
In GFC Errors	Number of cells received with a non-zero GFC.

ATM AAL5 Layer Statistics over ADSL interface

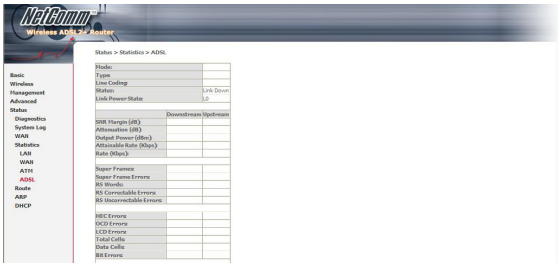
Field	Description
In Octets	Number of received AAL5/AAL0 CPCS PDU octets
Out Octets	Number of received AAL5/AAL0 CPCS PDUs octets transmitted
In Ucst Pkts	Number of received AAL5/AAL0 CPCS PDUs passed to a higher-layer
Out Ucast Pkts	Number of received AAL5/AAL0 CPCS PDUs received from a higher layer for transmission
In Errors	Number of received AAL5/AAL0 CPCS PDUs received in error. The types of errors counted include CRC-32 errors.
Out Errors	Number of received AAL5/AAL0 CPCS PDUs that could be not transmitted due to errors.
In Discards	Number of received AAL5/AAL0 CPCS PDUs discarded due to an input buffer overflow condition.
Out Discards	This field is not currently used

ATM AAL5 Layer Statistics for each VCC over ADSL interface

Field	Descriptions
CRC Errors	Number of PDUs received with CRC-32 errors
SAR TimeOuts	Number of partially re-assembled PDUs which were discarded because they were not fully re-assembled within the required period of time. If the re-assembly time is not supported then, this object contains a zero value.
Over Sized SDUs	Number of PDUs discarded because the corresponding SDU was too large
Short Packets Errors	Number of PDUs discarded because the PDU length was less than the size of the AAL5 trailer
Length Errors	Number of PDUs discarded because the PDU length did not match the length in the AAL5 trailer

10.8 Status > ADSL Statistics

The following figure shows the ADSL Network Statistics screen. Within the ADSL Statistics window, a bit Error Rate Test can be started using the ADSL BER Test button. The Reset button resets the statistics.

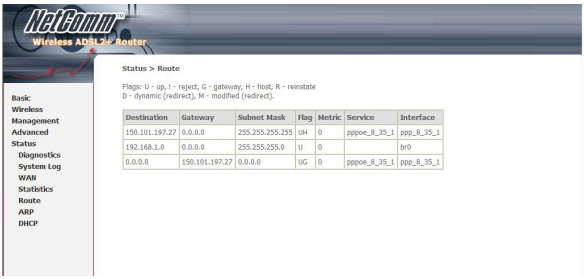


Field	Description
Mode	Modulation protocol ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2
Type	Channel type Interleave or Fast
Line Coding	DMT Trellis on
Status	Lists the status of the DSL link
Link Power State	Link output power state.
SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.
Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors
HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of out-of-cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

If you are connected to an ADSL link the following page will be displayed.

10.9 Status > Route

Summarises parameters of IP route for device.



10.10 Status > ARP

10.11 Status > DHCP

Provides summary of DHCP leases provisioned by **NB8WVPN**. Useful source to findclientmachine MAC addresses.

Status > DHCP Leases

Hostname	MAC Address	IP Address	Expires In
Toms	00:13:D3:06:DE:9B	192.168.1.3	12 hours, 46 minutes, 8 seconds
Sandra	00:08:0D:53:37:C2	192.168.1.11	18 hours, 47 minutes, 45 seconds
	00:0A:27:7C:45:58	192.168.1.4	Expired
Sirius	00:08:0D:32:4E:64	192.168.1.5	13 hours, 40 minutes, 29 seconds
acer-157fba01c8	00:0F:B0:7B:8F:25	192.168.1.15	Expired
	00:13:15:16:CC:41	192.168.1.6	21 hours, 29 minutes, 21 seconds
Sirius	00:90:96:C1:FF:5E	192.168.1.7	Expired

Appendix: Legal & Regulatory Information

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.

GNU General Public License

This product includes software code that is subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). This code is subject to the copyrights of one or more authors and is distributed without any warranty. A copy of this software can be obtained by contacting NetComm Limited on +61 2 9424 2059.

Product Warranty

The warranty is granted on the following conditions:

1. This warranty extends to the original purchaser (you) and is not transferable;
2. This warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. The customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting product to and from NetComm's nominated premises is your responsibility; and,
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.
6. The customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

The warranty is automatically voided if:

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

Limitations of Warranty

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

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

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

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

www.netcomm.com.au

NetComm®
www.netcomm.com.au

NetComm®
www.netcomm.com.au

Product Warranty

NetComm products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option, via registering your product online at the NetComm website **www.netcomm.com.au**.

Technical Support

If you have any technical difficulties with your product, please refer to the support section of our website.

www.netcomm.com.au/support

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.

NetComm®
www.netcomm.com.au

NETCOMM LIMITED PO Box 1200, Lane Cove NSW 2066 Australia
P: 02 9424 2070 **F:** 02 9424 2010
E: sales@netcomm.com.au **W:** www.netcomm.com.au

Dynalink
www.dynalink.co.nz

DYNALINK NZ 224b Bush Road, Albany, Auckland, New Zealand
P: 09 448 5548 **F:** 09 448 5549
E: sales@dynalink.co.nz **W:** www.dynalink.co.nz