NetComm®
www.netcomm.com.au

NB12WD

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 are clearly stated in Appendix D

Table of Contents

1.Introduction

The NB12WD MyComms Gateway is a powerful all-in-one device that incorporates an ADSL2+ Broadband Router, an 11g Wireless Access Point, VoIP Gateway, USB print server, as well as a DECT handset for all your VoIP needs. It is best suited for residential or business users who want to integrate all of the listed features in one compact device.

The NB12WD VoIP feature allows calls to be routed anywhere in the world, significantly reducing or eliminating long distance call charges. You can even make phone calls when your PC is turned off. The NB12WD also delivers high quality calls during periods of heavy Internet use, by employing Layer 3 policy-based Quality of Service (QoS), which prioritises your voice packets. With NetComm's NB12WD, you have all of your Internet, networking and communication needs integrated into one stylish desktop unit eliminating the clutter of many separate devices

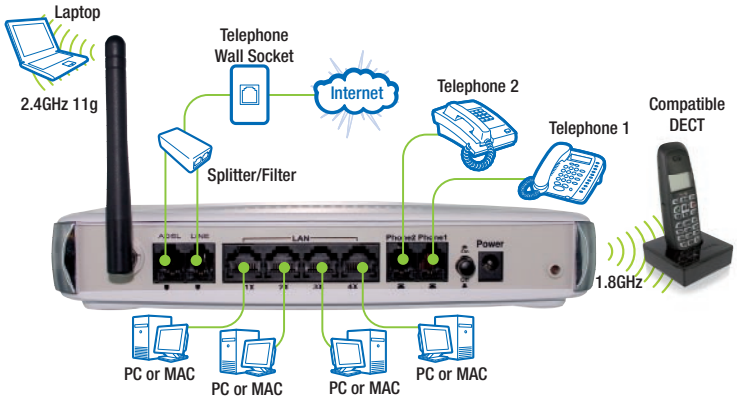
1.1 Features

- ADSL2+ Broadband Router
- 802.11g wireless access point (backward compatible with 802.11b)
- VoIP gateway with 2 phone ports
- FXO "lifeline" port
- 4 10/100 Ethernet LAN ports
- Built-in USB print server
- Layer 3 policy-based QoS, IP QoS, ToS
- Built-in 1.8GHz Gap compatible DECT base station with support for 2 DECT lines and up to 5 handsets
- DECT handset
- WEP encryption
- WPA and WPA2
- Static Route/RIP/RIP v2 routing functions
- NAT/PAT
- DHCP server/client/relay
- VPN/PPTP/L2TP/IPSec pass through

For a complete list of features, please consult Appendix D: Specifications.

1.2 Application

The diagram below depicts a typical application of the **NB12WD** series.



1.3 Front Panel LED Indicators

The front panel LED indicators are shown and explained below.

LED	Color	Mode	Function
POWER	Green	On	The NB12WD is powered up.
		Off	The NB12WD is powered down.

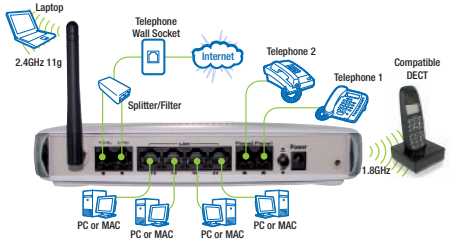
WLAN	Green	On	The wireless module is ready.
		Off	The wireless module is switched off.
		Blink	Data transmitting or receiving over wireless.
PHONE1	Green	On	The FXS Phone 1 is off hook.
		Off	The FXS Phone 1 is on hook.
PHONE2	Green	On	The FXS Phone 2 is off hook.
		Off	The FXS Phone 2 is on hook.
DECT1	Green	On	DECT Line 1 in use
		Off	DECT Line 1 idle
DECT2	Green	On	DECT Line 2 in use
		Off	DECT Line 2 idle
LAN 4x~1x	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over Ethernet.
LINE	Green	On	FXO (pass through) Line is off hook.
		Off	FXO Line is on hook.
ADSL	Green	On	The ADSL link is established.
		Off	The ADSL link is not established.
		Blink	The ADSL link is training or traffic is passing through ADSL.
Side Panel			
USB	Green	On	A USB link is established
		Off	A USB link is not established
		Blink	Data transmitting or receiving over USB
DECT	Green	On	NB12WD is in register mode for DECT
		Off	NB12WD is not in register mode for DECT
		Blink	NB12WD is in paging mode for DECT

Installation

2.Installation

2.1 Hardware Installation

Follow the instructions below to complete the hardware installation.



Connecting your device

1. With the supplied Ethernet cable, connect your computer to any LAN port on your NB12WD.
2. Connect your telephone wall socket to an ADSL Splitter/Filter (not supplied).
3. With one of the supplied telephone cables, connect the socket labeled **ADSL** on your NB12WD to the socket labeled **ADSL** on your ADSL Splitter/Filter (not supplied).
4. If you wish to use Lifeline backup function, please ensure that:
   a. the **Line** port of the NB12WD is connected to the socket labeled **phone** on the ADSL Splitter/Filter

AND

   b. Please also ensure that your telephone handset is connected to one of the ports on your NB12WD labeled **Phone1** or **Phone2**.
5. Connect the supplied Power Adapter to the wall power outlet and to the socket labeled **Power** on the NB12WD.
6. Switch on your NB12WD at the power outlet and press the on/off button to the **on** position and wait 1 minute for it to power up.
7. Open a web-browser on your computer and browse to **192.168.1.1**.
8. When asked for a username and password, enter the default of **admin** into both fields.
9. Select **Quick Setup** from the menu on the left, and follow the instructions to establish your internet connection.

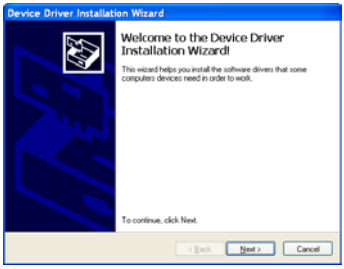
2.2 USB Driver Installation

Note: Connection via Ethernet is strongly recommended as the main wired connection method

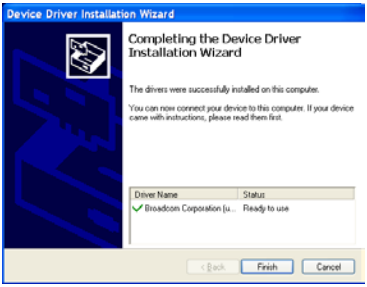
Windows XP USB Instructions

1: Do NOT connect your USB cable before installing the USB driver on your computer. Insert the NB12WD manual and driver installation disc, and select "USB Driver Installation" from the CD Menu (If the CD fails to autorun the menu, open the CD folder, browse to the 'USB installation' folder, and double-click the file named 'setup.exe'.

Once the Device Driver Installation Wizard opens, click **Next**.



2: Wait a moment for the driver to install, and then click **Finish**.

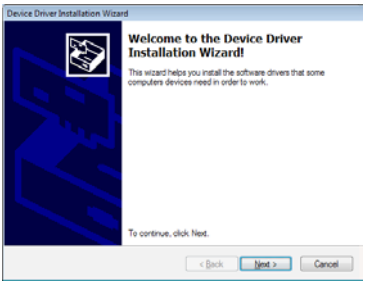


3: Next connect your USB cable from your computer to your NB12WD. Windows XP will take several seconds to recognize the device, and to automatically configure the driver. After this is complete, your NB12WD via USB has been set up and is ready to use.

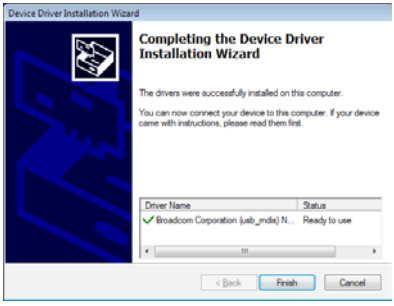
Windows Vista USB Instructions

1: Do NOT connect your USB cable before installing the USB driver on your computer. Insert the NB12WD manual and driver installation disc, and select “USB Driver Installation” from the CD Menu (If the CD fails to autorun the menu, open the CD folder, browse to the ‘USB installation’ folder, and double-click the file named ‘setup.exe’.

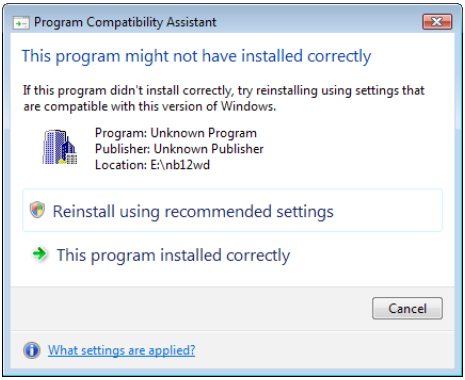
Once the Device Driver Installation Wizard opens, click **Next**.



2: Click **Finish**.



3. If you see a warning that the program might not have installed correctly, please click “This program installed correctly” as shown below.



4: Connect your USB cable from your computer to your NB12WD. Windows Vista will take several seconds to recognize the device, and to automatically configure the driver. After this is complete, your NB12WD via USB has been set up and is ready to use.

Mac OSX 10.X USB Instructions

MacOSX has a compatible driver pre-installed. To use the NB12WD with MacOSX via USB, simply plug the cable in, and your NB12WD is ready to use.

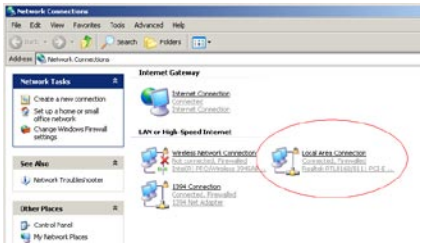
Web User Interface

3. Web User Interface

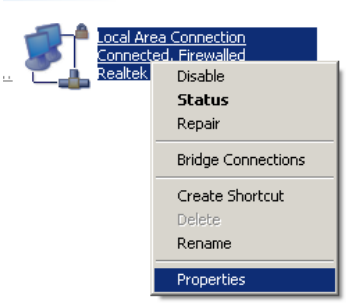
This section describes the setup procedure to access the web user interface using Windows XP.

3.1 TCP/IP Settings

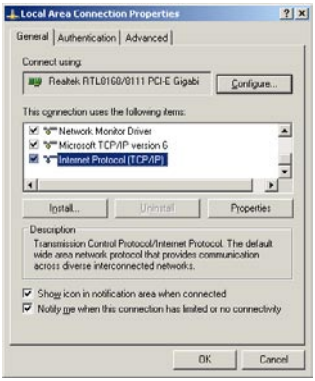
- Enter [Start Menu], select [Control panel], select [Network].

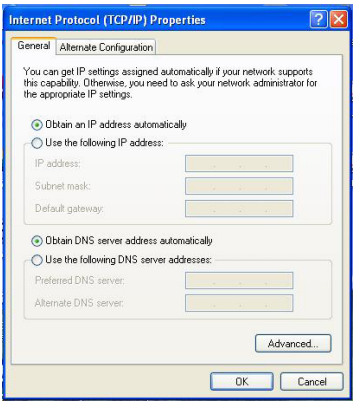


- Select [Local Area Connection]) icon=>select [properties]



- Select [Internet Protocol (TCP/IP)] =>Click [Properties].





- Select the [General] tab.
- Please select both
  - Obtain an IP address automatically
  - Obtain DNS server address automatically

3.2 Login Procedure

Follow these steps to login to the web user interface.

1: Open an Internet browser (e.g. Microsoft Internet Explorer) and enter the default IP address for the router in the URL address field at top. For example, if the IP address is 192.168.1.1, enter "http://192.168.1.1".

2: Next, you will be prompted to enter your user name and password. Enter **admin** as the user name and **admin** as the password, and then click **OK**. These values can be changed later (see section 9.6.3).

3: After successfully logging in, you will reach the Quick Setup menu.

3.3 Default Settings

The following list shows the factory default settings for this router.

- LAN port IP address: 192.168.1.1
- Local administrator account name: admin
- Local administrator account password: admin
- Local non-administrator account name: user
- Local non-administrator account password: user
- Remote WAN access: disabled (except for ICMP)
- NAT and firewall:Disabled for MER, IPoA and Bridge modes Enabled for PPPoE and PPPoA modes
- DHCP server on LAN interface: enabled
- WAN IP address: none
- Wireless access: enabled
- SSID: NetComm Wireless
- Wireless authentication: enabled Password a1b2c3d4e5
- Annex M disabled

This router supports the following connection types.

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoA)
- MAC Encapsulated Routing (MER)
- IP over ATM (IPoA)
- Bridging
- Half Bridge (PPP IP Extension)

Technical Note:

The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Default screen, section 9.1.3.

Your **NB12WD** has a Quick Setup page configured for easy access via PPPoE. All you need to do is enter the Username and Password issued by your ISP, and click the 'Save & Reboot' button to establish your internet connection.


Quick Setup

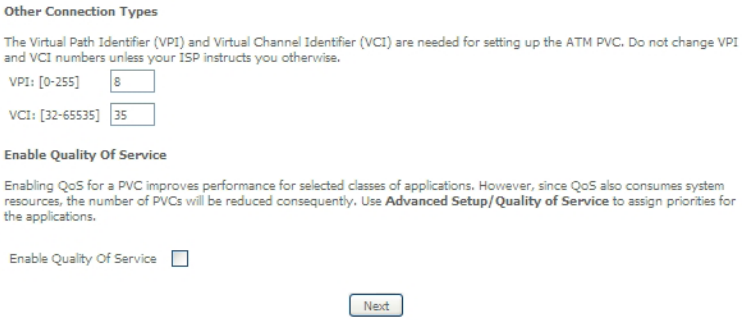
4. Quick Setup

If you have a different connection type, please select the **Click here for other connection types** button and follow the instructions to configure your advanced connection. For more information about configuring an advanced WAN connection, please see section 6.1.

4.1 Manual Quick Setup

1: Click **Quick Setup** and select the **click here for other connection types** button to enable manual configuration.

After clicking the button the following screen appears.

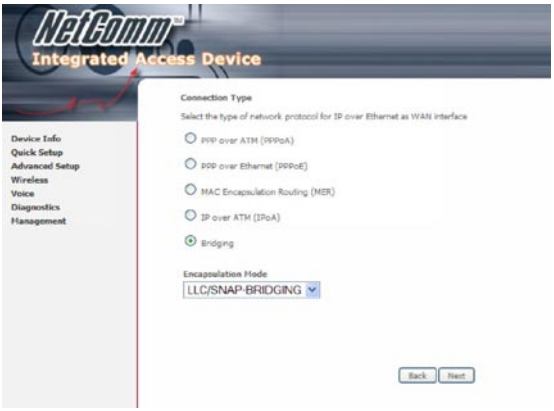


2: Enter the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) values. Select Enable Quality Of Service if required and click Next.

3: Choose an Encapsulation mode.

Choosing different connection types provides different encapsulation modes.

- PPPoA- VC/MUX, LLC/ENCAPSULATION
- PPPoE- LLC/SNAP BRIDGING, VC/MUX
- MER- LLC/SNAP-BRIDGING, VC/MUX
- IPoA- LLC/SNAP-ROUTING, VC MUX
- Bridging- LLC/SNAP-BRIDGING, VC/MUX

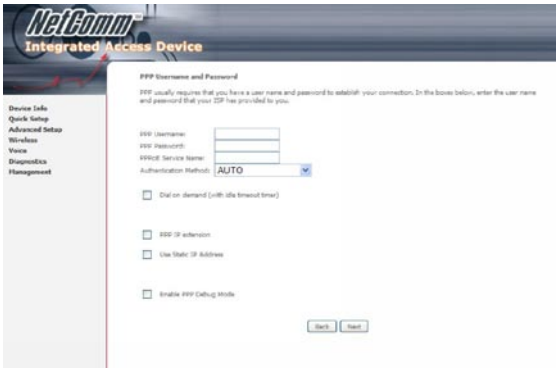


NOTE: The sections that follow describe the PVC setup procedure further. Choosing different connection types pops up different settings requests. Enter appropriate settings that are required by your service provider.

4.1.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE)

Follow Steps 1 through to 3 of Manual Quick Setup

4: Select the PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE) radio button and click Next. The following screen appears.



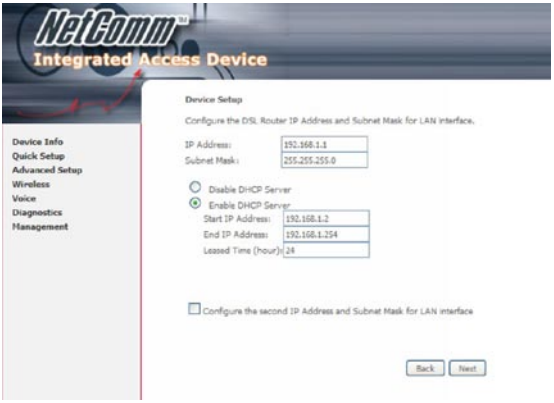
Field	Description
PPP Username/PPP Password	The PPP Username and the PPP password requirement are dependent on the particular requirements of the ISP or the DSL service provider. The web user interface allows a maximum of 256 characters for the PPP username and a maximum of 32 characters for PPP password
PPPoE service name	PADI requests contain a service label. Some PPPoE servers (or BRAS) of ISP check this service label to make a connection NOTE: No service name for PPPoA
Disconnect if no activity	The router can be configured to disconnect if there is no activity for a period of time by selecting the Dial on demand check box. When the checkbox is ticked, you need to enter the inactivity timeout period. The timeout period ranges from 1 minute to 4320 minutes
PPP IP Extension	The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specially requires this setup, do not select it

The PPP IP Extension supports the following conditions	Allows only one PC on the LAN
	The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the router has a single IP address to assign to a LAN device
	NAT and firewall are disabled when this option is selected
	The router becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address
	The router extends the IP subnet at the remote service provider to the LAN PC. That is, the PC becomes a host belonging to the same IP subnet
	The router bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the router's LAN IP address
Use Static IP Address	Unless your service provider specially requires this setup, do not select it.
	If selected, enter your static IP address.
Enable PPP Debug Mode	Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. But this is for debug, please don't enable in normal usage

5: Click **Next** to display the following screen.

Field	Description
Enable IGMP Multicast checkbox	Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers
Enable WAN Service checkbox	Tick this item to enable the ATM service. Untick it to stop the ATM service
Service Name	This is user-defined

6: After entering your settings, select Next. The following screen appears.

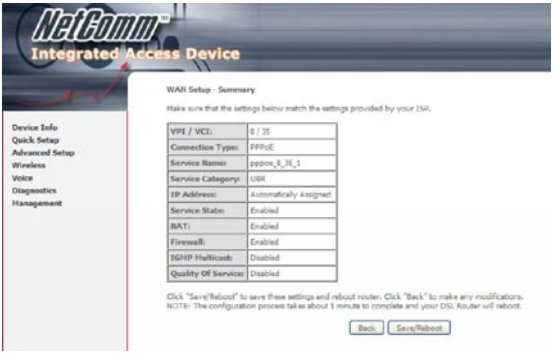


This screen allows the user to configure the LAN interface IP address, subnet mask and DHCP server. If the user would like this router to assign dynamic IP address, DNS server and default gateways to other LAN devices, select the button Enable DHCP server and enter the Start and End IP addresses and DHCP leased time.

To configure a secondary IP address for the LAN port, tick the checkbox shown.

7: Click **Next** to continue. To enable the wireless function, tick the checkbox (as shown), input a new SSID (if desired) and click Next.

8: Click Next to display the WAN Setup-Summary screen that presents the entire configuration summary. Click Save/Reboot if the settings are correct. Click Back if you wish to modify the settings.

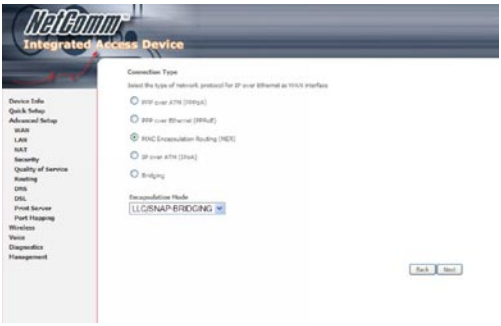


9: After clicking **Save/Reboot**, the router will save the configuration to flash memory and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info screen automatically.

4.1.2 MAC Encapsulation Routing (MER)

Follow Steps 1 through to 3 of Manual Quick Setup

4: Select the MAC Encapsulation Routing (MER) radio button and click Next.



The following screen appears.

Enter information provided to you by your ISP to configure the WAN IP settings.

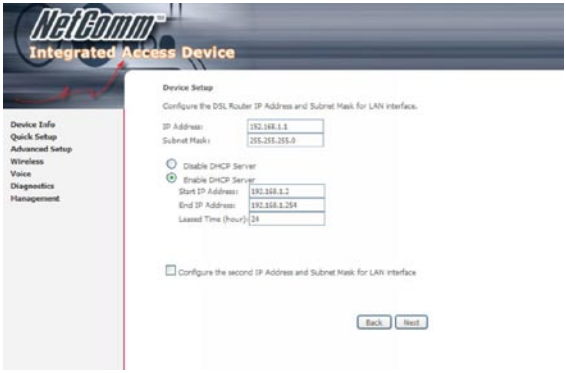
NOTE: DHCP can be enabled for PVC in MER mode if Obtain an IP address automatically is chosen. Changing the default gateway or the DNS affects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.

If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address" field. The ISP will provide the values to enter in these fields.

5: Click **Next** to display the following screen.

Field	Description
Enable NAT	If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be de-selected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will be gone
Enable Fullcone NAT	This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address
Enable Firewall	If the firewall checkbox is selected, the Security submenu will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will be gone
Enable IGMP Multicast	Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers
Enable WAN Service	Tick the checkbox to enable the WAN service. If this item is not selected, you will not be able to use the WAN service
Service Name	This is User-defined

6: Upon completion click **Next**. The following screen appears.



Consult the following paragraphs for more details about these settings.

The Device Setup screen allows the user to configure the LAN interface IP address and DHCP server. If the user would like this router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices, select the radio box **Enable DHCP** server to enter the starting IP address and end IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

NOTE: If NAT is enabled, Enable DHCP Server Relay won't display.

To configure a secondary IP address for the LAN port, tick the checkbox shown.

7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown), input a new SSID (if desired) and click **Next.**

The following screen will display.

8: The WAN Setup-Summary screen presents the entire configuration summary. After clicking **Save**, the router will save the configuration to flash memory and reboot. Click **Back** if you wish to modify the settings. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the **Device Info** screen automatically.

4.1.3 IP Over ATM

Follow Steps 1 through to 3 of Manual Quick Setup

4: Select the IP over ATM (IPoA) radio button and click **Next**.

The following screen appears.

NOTE: DHCP is not supported over IPoA. The user must enter the IP address or WAN interface for the default gateway setup and the DNS server addresses provided by the ISP.

5: Click **Next**. The following screen appears.

Field	Description
Enable NAT	If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox should be de-selected. When the system comes back after reboot, the NAT submenu will be gone
Enable Firewall	If the firewall checkbox is selected, the Security submenu will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will be gone

6: Click **Next** to display the following screen.

The Device Setup screen allows the user to configure the LAN interface IP address and DHCP server. If the user would like this router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices. Select the button Enable DHCP server on the LAN to enter the starting IP address and end IP address and DHCP lease time.

The Device Setup screen allows the user to configure the LAN interface IP address and DHCP server. If the user would like this router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices. Select the radio box **Enable DHCP** server on the LAN to enter the starting IP address and end IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

NOTE: If NAT is enabled, Enable DHCP Server Relay won't display.

To configure a secondary IP address for the LAN port, click the box as shown below.

7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown), input a new SSID (if desired) and click **Next**.

The following screen will be displayed.

8: The WAN Setup-Summary screen presents the entire configuration summary. After clicking **Save/ Reboot**, the router will save the configuration to the flash memory, and reboot. Click **Back** if you wish to modify the settings. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the **Device Info** screen automatically.

4.1.4 Bridging

4: Select the Bridging radio button and click **Next**. The following screen appears. To use the bridge service, tick the **Enable Bridge Service** checkbox and enter a service name (user defined).

5: Click the **Next** button to continue. Enter the IP address for the LAN interface. The default IP address is 192.168.1.1. The LAN IP interface in bridge operating mode is needed for local users to manage the router. Notice that there is no IP address for the WAN interface in bridge mode, and technical support cannot access the router remotely.

6: Click **Next** to continue. To enable the wireless function, select the radio button (as shown), input a new SSID (if desired) and click **Next**.

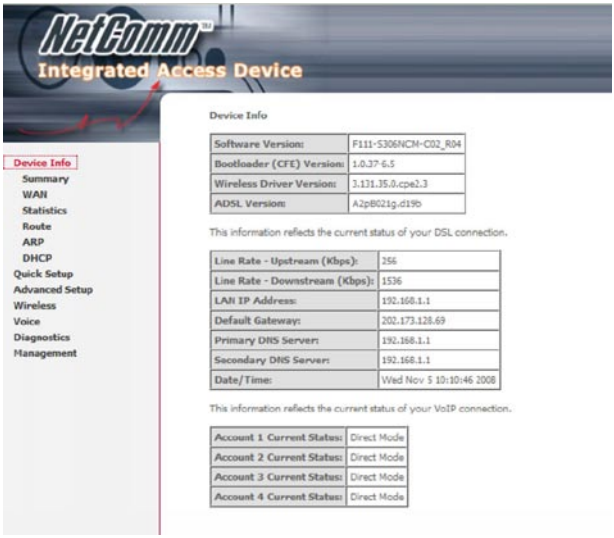
The following screen will be displayed.

7: The WAN Setup-Summary screen presents the entire configuration summary. After clicking **Save/ Reboot**, the router will save the configuration to the flash memory, and reboot. Click **Back** if you wish to modify the settings. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the **Device Info** screen automatically.


Device Info

5. Device Info

Select **Device Info** from the main menu to display Summary information as below.



5.1 WAN

Select WAN from the Device Info menu to display the status of all configured PVC(s).

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; enable if VoIP services are being used
State	Enable/Disable this WAN connection
Status	The status of this connection
IP Address	The IP address of this connection

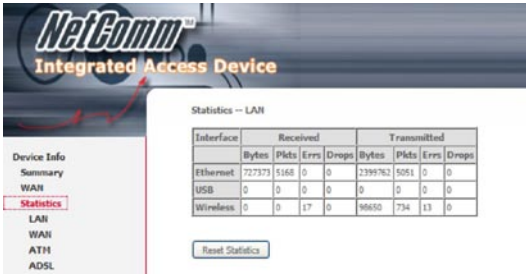
5.2 Statistics

This submenu provides statistics for LAN, WAN, ATM, ADSL connections.

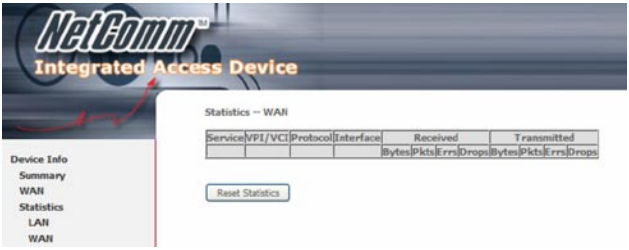
NOTE: These statistics refresh every 10 seconds.

5.2.1 LAN Statistics

The Network Statistics screen shows interface statistics for Ethernet and Wireless interfaces. (The Network Statistics screen shows interface statistics of LAN. Eg; Here provides byte transfer, packet transfer, Error and Drop statistics for the LAN interface.)



5.2.2 WAN Statistics



Service		Shows the service type
VPI/VCI		Shows the values of the ATM VPI/VCI
Protocol		Shows the connection type
Interface		Shows connection interfaces
Received/Transmitted	- Bytes	Rx/TX (receive/transmit) packet in Byte
	- Pkts	Rx/TX (receive/transmit) packets
	- Errs	Rx/TX (receive/transmit) packets with errors
	- Drops	Rx/TX (receive/transmit) dropped packets

ADSL

The figure below shows the ATM statistics screen when using ADSL.

5.2.3 ATM Statistics (ADSL)

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 HEX error
In Invalid Vpi Vci Errors	Number of cells received with an unregistered VCC address.
In Port Not Enable 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.

5.2.4 ADSL Statistics

The following graphic shows the ADSL Network Statistics screen. The **Reset** button (located at the bottom of the screen) can be used to reset statistics. The bit error rate can be tested by clicking the **ADSL BER Test** button.

Consult the table that follows for field descriptions.

Field	Description
Mode	Line Coding format (e.g. G.dmt, G.lite, T1.413, ADSL2)
Type	Channel type (Interleave or Fast)
Line Coding	Trellis On/Off
Status	Lists the status of the ADSL 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.

n G.DMT mode the following section is inserted here.

K	Number of bytes in DMT frame
R	Number of check bytes in RS code word
S	RS code word size in DMT frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

In ADSL2+ mode the following section is inserted here.

MSGc	Number of bytes in overhead channel message
B	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in FEC Data Frame
T	Max Data Frames over sync bytes
R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

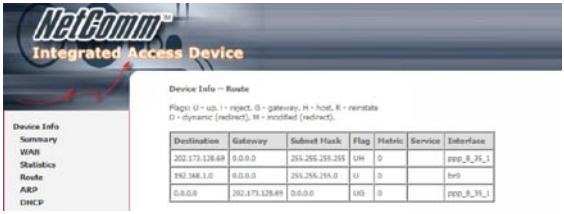
Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

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 Cells	Total number of ATM cells (including idle and data cells)
Data Cells	Total number of ATM data cells
Bit Errors	Total number of bit errors

In ADSL2+ mode the following section is inserted here.

Total ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

5.3 Route

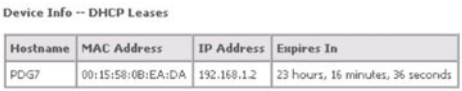


Clicking on 'Device Info', then 'Route' shows the advanced route configuration of your NB12WD

5.4 ARP

Clicking on 'Device Info', then 'ARP' shows the current ARP table (The automatic mapping of IP Addresses to MAC addresses) on the NB12WD.

5.5 DHCP

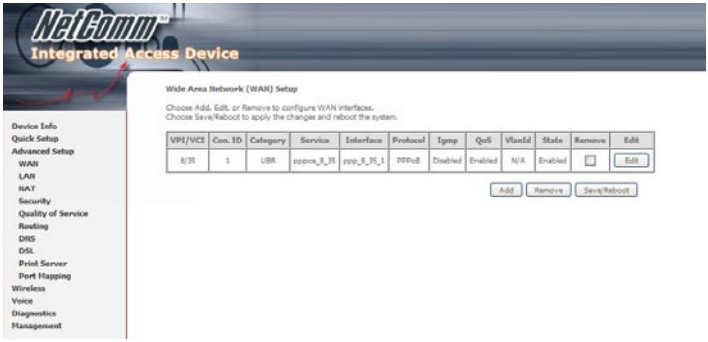


Clicking on 'Device Info', then 'DHCP' shows the current DHCP lease table of your NB12WD. This table shows the IP addresses that have been assigned by the NB12WD, to which devices they have been assigned, and when the DHCP lease will expire.

Advanced Setup

6. Advanced Setup

This chapter explains the Advanced Setup menu options outlined below.



NOTE: The selections available on this menu are based on configured connection settings and/or user account privileges. For example, NAT is not an available option in Bridge mode and may be disabled in MER or IPoA.

6.1 WAN

This screen allows for the advanced configuration of WAN interfaces.

- To Add a WAN connection, click the **Add** button. To edit an existing connection, click the **Edit** button next to the connection.
- To remove a connection select its radio button under the Remove column in the table and click the **Remove** button under the table.
- **Save/Reboot** activates the new configuration.

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; enable if VoIP services are being used.
State	Enable/Disable this WAN connection
Status	The status of this connection
IP Address	The IP address of this connection

6.1.1 MSP

Multi-Service over PVC (MSP) supports multiple protocols over a single connection. As with the PPPoE, Bridge and MER protocols can coexist, while IPoA and PPPoA are not supported. This function supports remote management by bridge protocol in addition to multimedia applications over a single PVC.

Configuring MSP is a two-part process:

Part 1 - Create multiple PVCs (One Bridge + multiple PPPoE / One MER)

Part 2 - Use Port Mapping to connect LAN / WAN interfaces

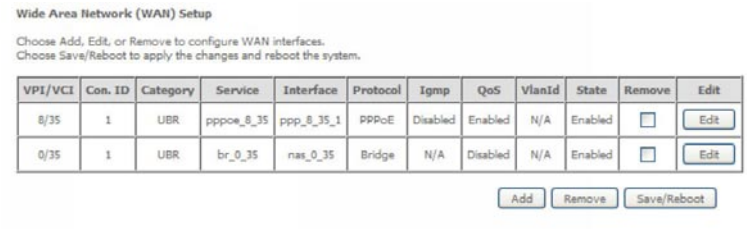
NOTE: The example below shows how to configure a Bridge / PPPoE MSP connection. Use the same process for Bridge / MER MSP connections.

If QoS is configured on the first MSP connection, it will be configured by default for all subsequent connections.

If a MSP connection is removed every other MSP connection should be removed to avoid port mapping configuration problems.

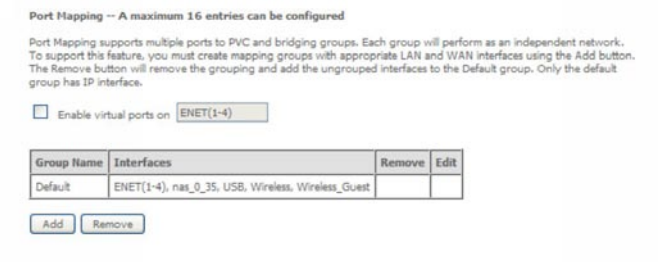
Part 1 – Create Multiple PVCs

On the Advanced Setup – WAN screen, create one PPPoE connection and one Bridge connection on the MSP supporting PVC. The screen will display as follows.



Part 2

Go to Advanced Setup – Port Mapping screen (see section 6.10 Port Mapping) and select the Enable Virtual Ports checkbox. The screen will display as follows.

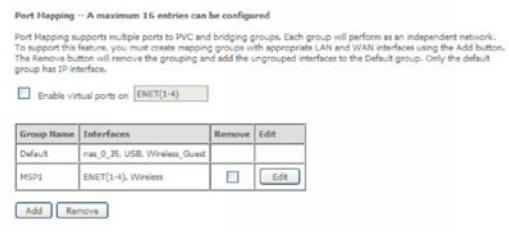


NOTE: Only hardware ports and bridge PVCs are listed as interfaces. The bridge interface is shown as "nas_x_y_z" where x=port, y=vpi, and z=vci.

To continue, click the **Add** button at the bottom of the screen shown above.

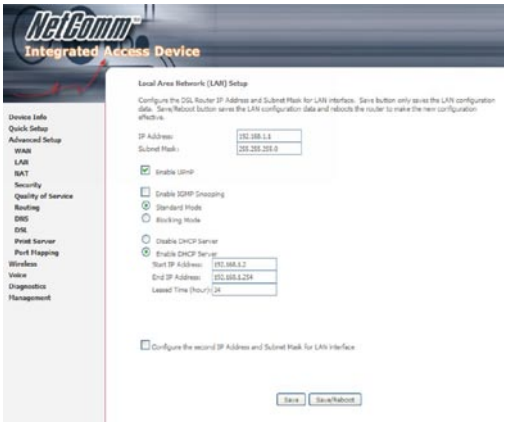
On the screen shown below, select the bridge connection and one Ethernet virtual port (ENET 1-4). Enter a group name, such as “MSP1”, and click **Save/Apply**.

If successfully configured, the Port Mapping screen will display as follows.



6.2 LAN

Use this screen to configure LAN interface settings.



NOTE: NAT is enabled so Enable UPnP is shown above while DHCP Server Relay is hidden. Consult the field descriptions below for more details.

Field	Description
IP Address	Enter the IP address for the LAN port
Subnet Mask	Enter the subnet mask for the LAN port
Enable UPnP	Tick the box to enable Universal Plug and Play. This option is hidden when NAT disabled or if no PVC exists
Enable IGMP Snooping	Enable by ticking the box
Standard Mode	In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group – even if IGMP snooping is enabled
Blocking Mode	In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group
DHCP Server	To enable DHCP, select Enable DHCP server and enter starting and ending IP addresses and the leased time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN

DHCP Server Relay	Enable with checkbox and enter DHCP Server IP address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address. This option is hidden if NAT is enabled
Configure the second IP address by ticking the checkbox shown	
IP Address	Enter the secondary IP address for the LAN port
Subnet Mask	Enter the secondary subnet mask for the LAN port

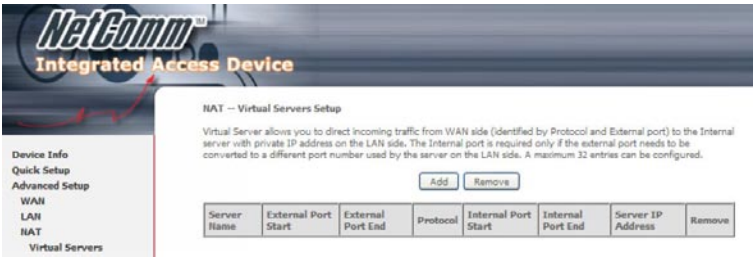
NOTE: The Save button saves new settings to allow continued configuration while the Save/Reboot button not only saves new settings but also reboots the device to apply the new configuration (i.e. all new settings).

6.3 NAT

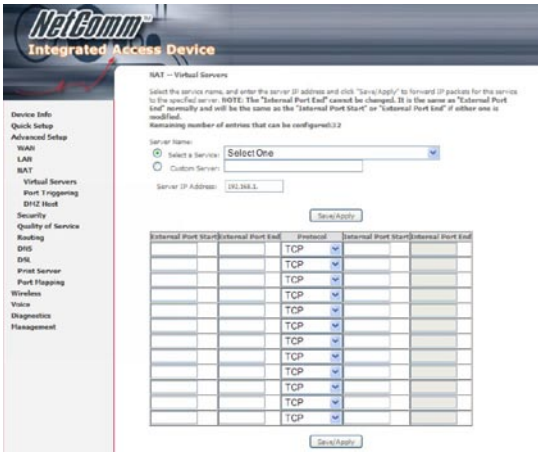
To display this option, NAT must be enabled in at least one PVC shown on the Advanced Setup - WAN screen. (NAT is not an available option in Bridge mode)

6.3.1 Virtual Servers

Virtual Servers allow 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 32 entries can be configured.



To add a Virtual Server, click **Add**. The following screen will be displayed.



Select a Service	User should select the service from the list.
or	or
Custom Server	User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.

6.3.2 Port Triggering

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

To add a Trigger Port, simply click the **Add** button. The following will be displayed.

Select an Application	
Or Custom Application	User can select the application from the list. Or enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Protocol	User can select from: TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Protocol	User can select from: TCP, TCP/UDP or UDP.

6.3.3 DMZ Host

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

Enter the DMZ Host IP address and click **Save/Apply** to activate DMZ host.

Clear the IP address field and click **Save/Apply** to deactivate DMZ host.

6.4 Security

To display this option, the Firewall checkbox must be enabled in at least one PVC shown on the Advanced Setup - WAN screen.

NOTE: For a more technical discussion of this topic see Appendix B: Firewall.

6.4.1 IP Filtering

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

Outgoing

The default setting for all Outgoing traffic is **ACCEPTED**.

To add a filtering rule, click the **Add** button. The following screen will be displayed.

Filter Name	Type a name for the filter rule.
Protocol	User can select: TCP, TCP/UDP, UDP or ICMP
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source subnet mask.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination Port (port or port:port)	Enter destination port number or range.

Incoming

The default setting for all Incoming traffic is Blocked.

To add a filtering rule, click the **Add** button. The following screen will be displayed.

To configure the parameters, please reference the Outgoing table above. The Incoming IP Filter applies only to the PVCs selected at the bottom of the screen in the WAN Interfaces list. Only PVCs configured in routing mode (PPPoE, PPPoA, MER, or IPoA) with firewall enabled are available for selection.

6.4.2 Parental Control

This allows parents, schools, and libraries to set access times for Internet use.

To add a time of day restriction click **Add**. The following screen will display.

User Name	Name of the Filter.
Browser's or Other MAC Address	Displays MAC address of the device on which the WUI is running or another MAC address.
Days of the week	Days when restrictions are applied. Click the checkbox under the days of the week.
Start/End Blocking Time	The times when restrictions start and stop.

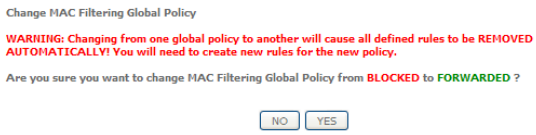
NOTE: Parental Control must be activated to use Internet Time. Also, this menu item is not displayed when in Bridge mode since the router would not be able to connect to the NTP time server.

6.4.3 Mac Filtering

Mac Filtering allows access to be restricted/allowed based on a MAC address.

Note: Mac Filtering is only available for Bridged mode.

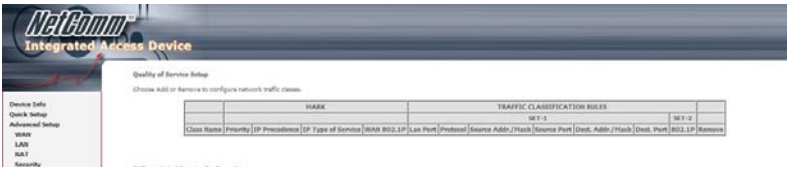
To Change Policy, Click the **Change Policy** button. The following screen will be displayed.



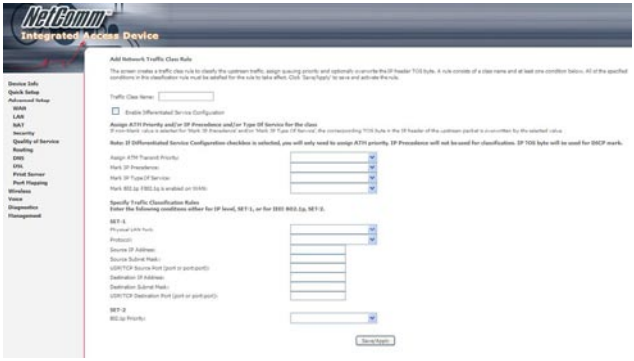
To add a MAC Filtering rule, Click **Add**. The following screen will display.

Click **Save/Apply** to save and activate the filter.

6.5.1 QoS Classification



Click **Add** to configure network traffic classes.



Click **Save/Apply** to save and activate the rule.

Traffic Class Name	Enter name for traffic class.
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.
Mark IP Type Of Service	Select either: Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay
Mark 802.1p if 802.1q is enabled on WAN	Select between 0-7. The higher the digit shows the higher the priority.

SET-1	
Physical LAN Port	Select between ENET(1-4), USB, Wireless and 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 or port range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number or port range.
SET-2	
802.1p Priority	Select between 0-7. The lower the digit shows the higher the priority

6.6 Routing

6.6.1 Default Gateway

If the **Enable Automatic Assigned Default Gateway** checkbox is selected, this router will accept the first received default gateway assignment from the DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway and/or WAN interface. Click **Save/Apply**.

NOTE: After enabling Automatic Assigned Default Gateway, you must click the Save/Apply button to put it into effect. The router will reboot.

6.6.2 Static Route

This screen lists the configured static routes and allows for the configuration of static routes. Choose Add or Remove to configure the static routes.

To add static route, click the **Add** button to display the following screen. Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click **Save/Apply** to add the entry to the routing table.

6.6.3 RIP

To activate RIP for the router, select the Enabled radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the Enabled checkbox for the interface. Click **Save/Apply** to save settings and start/stop RIP (based on Global RIP mode).

6.7 DNS

6.7.1 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 the Save button to save the new configuration. You must reboot the router to make the new configuration effective.

6.7.2 Dynamic DNS

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

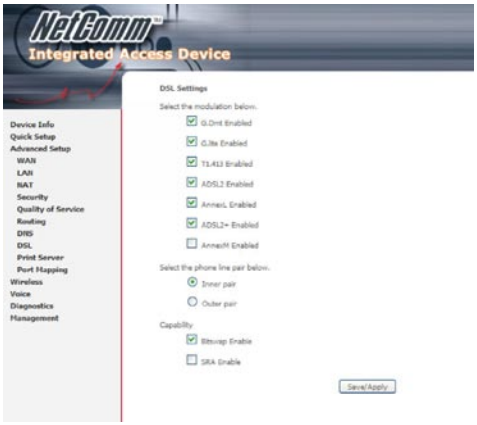
NOTE: The Add and Remove buttons will only be displayed if the CPE has already been assigned an IP address from the remote server.

To add a dynamic DNS service, click **Add** and the following screen will display.

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.

6.8 DSL

This screen is used to select ADSL modulations and capabilities.



The following table describes these DSL settings

Option	Description
G.dmt	Sets G.Dmt if you want the system to use G.Dmt mode.
G.Lite	Sets G.Lite if you want the system to use G.Lite mode.
T1.413	Sets the T1.413 if you want the system to use T1.413 mode.
ADSL2	The router can support the functions of ADSL2.
AnnexL	The router can support/enhance the long loop test.
ADSL2+	The router can support the functions of ADSL2+.
AnnexM	Enables a higher “upstream” data rate, by making use of some downstream channels.
Inner Pair	Reserved only
Outer Pair	Reserved only
Bitswap Enable	Allows bitswapping function
SRA Enable	Allows seamless rate adaptation

6.9 Print Server

This router is equipped with one high-speed USB2.0 host connection. With software support, users can connect USB devices such as a printer to the router. For this software release, only the print server is supported.

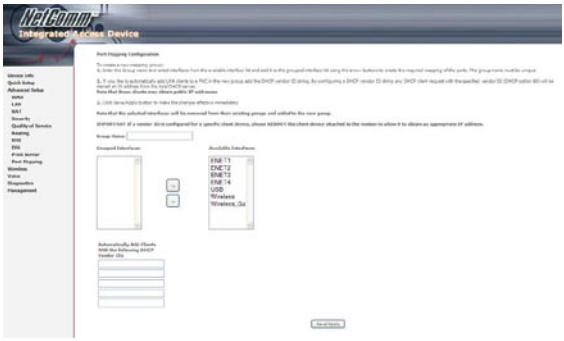
NOTE: Please refer to Appendix A: Printer Server for detailed setup instructions.

6.10 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 checkbox, all of the LAN interfaces will be put together as a default group.

To add a port mapping group, 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 with the arrow buttons .

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 PortMapping is enabled.

There are 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 is for PPPoE and the others are for IP set-top box (video). The LAN interfaces are ENET1, ENET2, ENET3, ENET4, Wireless and USB. Port mapping configuration is:

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

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

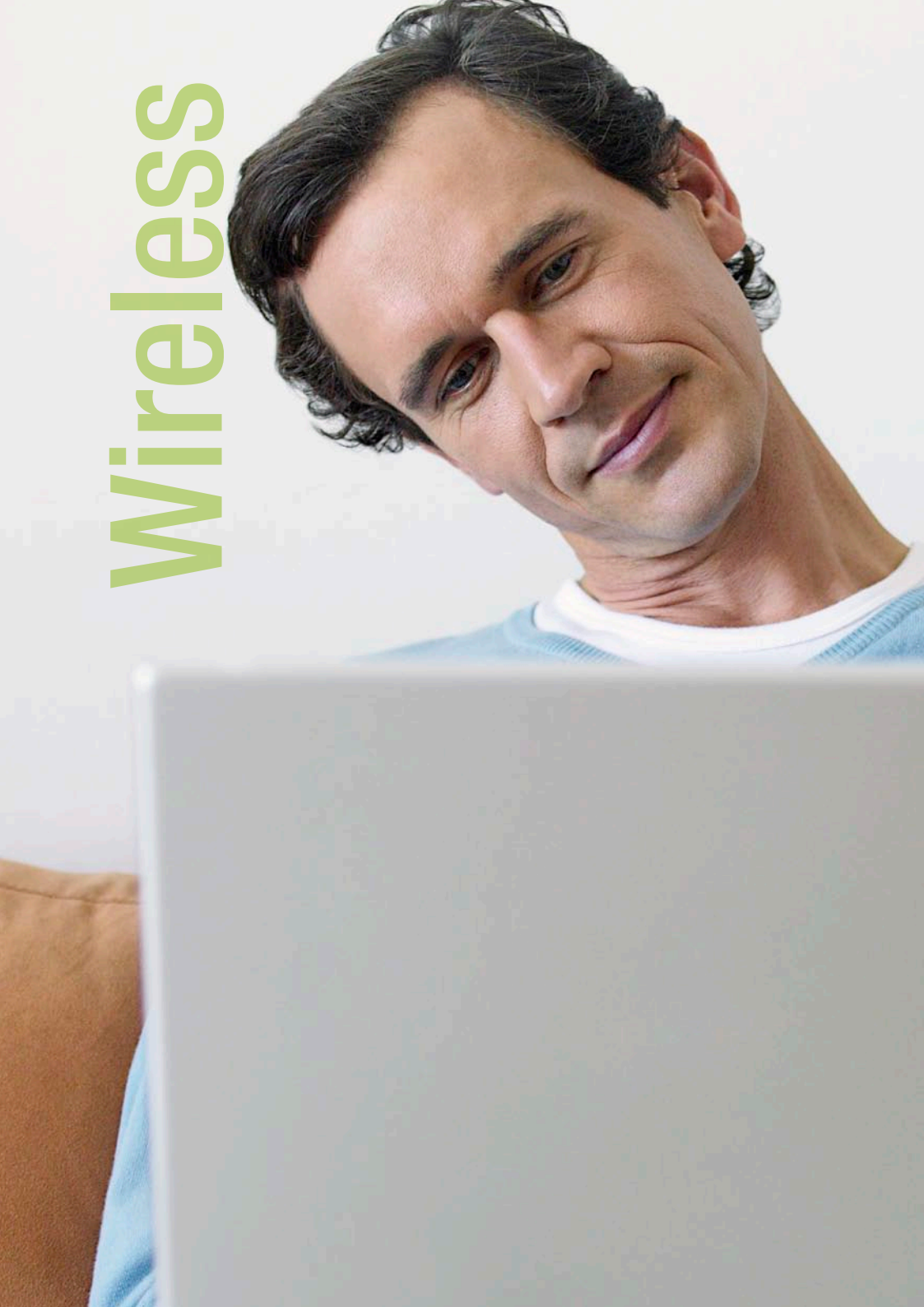
On the LAN side, the PC can get IP address from CPE DHCP server and access the Internet via PPPoE (0/33).

If the set-top box was connected with interface “ENET1” and send a deco request with vendor id “Video”, the CPE deco server would forward this request to ISP’s deco server. Then the CPE will change the PortMapping configuration automatically.

The PortMapping configuration would become:

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

Wireless



7. Wireless

The Wireless dialog box allows you to enable the wireless capability, hide the access point, set the wireless network name and restrict the channel set.

7.1 Basic

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

Click **Save/Apply** to configure the basic wireless options.

Option	Description
Enable Wireless	A checkbox that enables or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, and County settings. The default is Enable Wireless.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. If you do not want the access point to be automatically detected by a wireless station, this checkbox should be de-selected. The station will not discover this access point. To connect a station to the available access points, the station must manually add this access point name in its wireless configuration. In Windows XP, go to the Network>Programs function to view all of the available access points. You can also use other software programs such as NetStumbler to view available access points.
SSID	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access. The naming conventions are: Minimum is one character and maximum number of characters: 32 bytes.
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Each county listed in the menu enforces specific regulations limiting channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13

7.2 Security

Security settings are used to prevent unauthorized connection to your network. This can be as basic as a neighboring 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 practice 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 NB12WD wireless network.

Quick Security Setup 1: WEP Security

Your NB12WD has WEP (Wired Equivalent Privacy) encryption enabled by default. Your network will not be available to passer-by or non-authorized users, and any workstation wishing to connect to your NB12WD 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: NetComm 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.

This page will also allow you to change the Network Authentication and 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 settings is required, go to Wireless>Security and select WPA-PSK from the Network Authentication drop-down menu. Enter a network key of your choice in the WPA Pre-Shared Key field; this can be from 8 to 63 characters and contain special characters and spaced. And change the WPA Group Rekey Interval to 3600.

Select TKIP for WPA Encryption and leave WEP Encryption 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).

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 NB12WD 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 unauthorized 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 is 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, an algorithm then generates a series of keys based on the entered values.

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

WEP and WPA

"WEP" stands for Wired 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-specialized 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

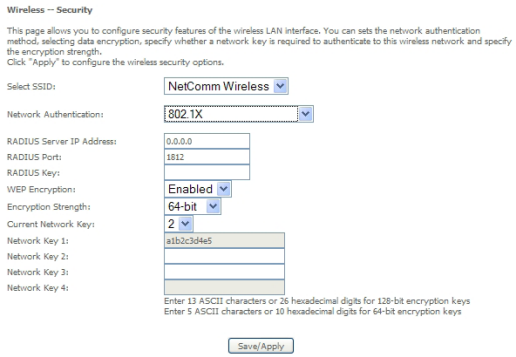
Network Authentication specifies the type of network authentication. The default value is 'Open'.

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 NB12WD.

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 requires a RADIUS server to provide client authentication. WPA also requires specification of the '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, the rekeying (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 NB12WD and the wireless clients. This shared secret can be between 8 and 63 characters and can include special characters and spaces.

For maximum security, 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 NB12WD.

WPA2

'WPA Pre-authentication' support in WPA2 allows a client to pre-authenticate with the NB12WD 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, video, or VoIP will all break without fast roaming.

'Network Re-Auth Interval' is the interval specified (seconds) that the wireless client needs to re-authenticate with the NB12WD.

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 NB12WD. 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.

7.3 MAC Filter

This option allows access to the router to be restricted based upon MAC addresses. Every network device has a unique 48-bit MAC address. This is usually shown as xx:xx:xx:xx:xx:xx, where xx are hexadecimal numbers. When MAC address filtering is enabled, it restricts the devices that can connect to your access point.

To add a MAC Address filter, click the **Add** button shown below.

To delete a filter, select it from the table below and click the **Remove** button.

Option	Description
MAC Restrict Mode	Disabled: MAC filtering function is disabled. Allow: Permits PCs with listed MAC addresses to connect to access point. Deny: Prevents PCs with listed MAC from connecting to the access point.
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. A maximum of 60 MAC addresses can be added. Every network device has a unique 48-bit MAC address. This is usually shown as xx:xx:xx:xx:xx:xx, where xx are hexadecimal numbers.

After clicking the **Add** button, the following screen appears.

Enter the MAC address in the box provided and click **Save/Apply**.

7.4 Wireless Bridge

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

7.5 Advanced

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

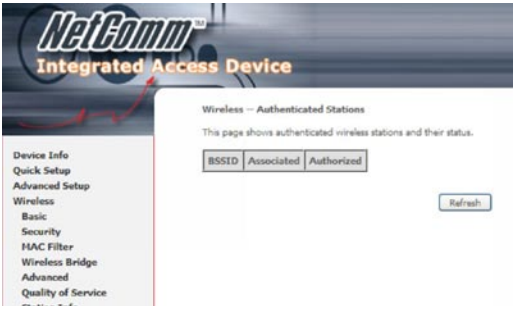
Click **Apply** to configure the advanced wireless options.

Option	Description
AP Isolation	1. Prevents clients PC from seeing one another in My Network Places or Network Neighborhood 2. Prevents one wireless Client communicating with another wireless Client
Band	The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network. The two standards apply to the 2.4 GHz frequency band. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting multicast packet transmit rate.
Basic Rate	Setting basic transmit rate.
Fragmentation Threshold	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. Enter a value between 256 and 2346. 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. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC 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 AP 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 access point. By default, radio NICs passively scan all RF channels and listen for beacons coming from access points to find a suitable access point. Before a station 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)
Xpress TM Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.

54g TM Mode	Set the mode to 54g Auto for the widest compatibility. Select the mode to 54g Performance for the fastest performance among 54g certified equipment. Set the mode to 54g LRS if you are experiencing difficulty with legacy 802.11b equipment.
54g Protection	In Auto mode the router 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 cooperate with the legacy. Long preamble interoperates 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.

7.6 Station Info

This screen shows authenticated wireless stations and their status.



MAC	**Lists the MAC address of all the stations.**
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.
SSID	Lists which SSID of the Router that the stations connect to.
Interface	Lists which interface of the Router that the stations connect to.

7.7 About SIP & VoIP

Voice Settings

The NB12WD has the ability to connect two regular telephones via the Phone1 and Phone2 ports on the rear of the unit and provides a number of sophisticated call-management functions such as call forward, call waiting, call transfer and so on. The following section provides further details of how to set up VoIP services, and then how to use the advanced telephony functions offered by the NB12WD.

Note: You can use separate VoIP accounts from your VoIP Service Provider but not separate accounts with different VSPs. This means that you can configure your NB12WD to provide two telephone extensions.

VoIP services are usually provided through a standard technology called SIP, briefly described as follows.

About SIP

SIP, the Session Initiation Protocol, is a signalling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. SIP is the Internet Engineering Task Force standard for multimedia conferencing over the Internet. SIP is designed to address the functions of signalling and session management within a packet-switched network. Signalling allows call information to be carried across network boundaries while session management provides the ability to control the qualities and attributes of an end-to-end call.

The Session Initiation Protocol is a peer-to-peer protocol. There are four components in the SIP standard:

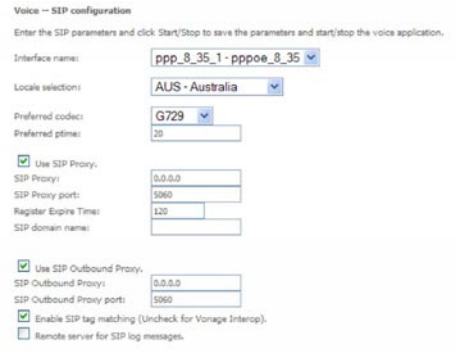
- User Agent (UA)
- Proxy Server
- Registar Server
- Redirect Server

In effect, this means that when you sign up for a VoIP account based on a SIP server, your 'VoIP' number and account details are managed by the SIP server at the VoIP Service Provider premises; by entering your SIP details (e.g. 'sip.serviceprovider.com') along with your VoIP/SIP account number and your account password, you are 'registered' with the service and able to make VoIP calls in practically the same way as with a traditional phone service (but for a much lower cost.)

Voice Menu 1

Enter your VoIP details in the NB12WD through the Voice menu.

Clicking on the Voice Menu will retrieve the following screen:

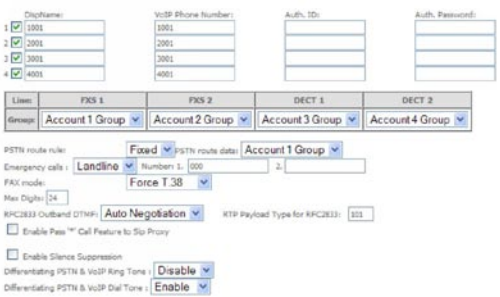


Entries in these fields are as follows:

Field	Value
Interface name	Current WAN connection; if you have set up your PPPoE connection to your ISP, this will display the current WAN connection.
Preferred codec	Value recommended by your VSP; default is G.729.
Preferred ptime	Value recommended by your VSP; default is 20.
Use SIP proxy	This box must be checked to activate the SIP registration process.
SIP Proxy	Enter SIP proxy IP address provided by your VSP.
SIP proxy port	Default is 5060. Leave as default unless directed to enter another value by VSP.
SIP proxy Domain	Set SIP proxy domain name; usually the same as SIP Proxy unless directed otherwise by VSP.
SIP Outbound Proxy:	Leave disable unless directed by VSP.
Enable SIP tag Matching:	Remote server for SIP Message: This box must be checked to activate the SIP Message logging. Leave as default unless directed otherwise by VSP.
Register Expire Time	Value recommended by your VSP; default is 120 (seconds).

Voice Menu 2

The lower part of the Voice entries screen provides fields in which details of your VoIP telephone number(s) are entered, along with several other VoIP parameters.



The NB12WD provides for two telephone 'extensions'. If you have one VoIP number and one telephone handset, plug this phone into Port 1 and enter the VoIP details in fields labelled with 1… .

If you have two handsets and one VoIP number then enter the same details in fields 1. and 2., above. In this configuration, both handsets will operate in tandem in the same way as two handsets on an ordinary POTS line.

Notes: for 1 account and 2 handsets. Not all VoIP Service Provider support that function.

If you have two or more different VoIP accounts from the same VSP, separate details may be entered for each account.

Field	Means
DispName	Will appear in telephone LCD display (if present)
Extension	VoIP Phone Number. The SIP client phone number.
Auth Id	VoIP account ID, a.k.a. SIP ID or VoIP Phone Number
Auth Password	Account password
PSTN Call Route	Incoming PSTN calls to ring on. Set the PSTN to ring on phone1 or phone2.
Emergency Calls:	Emergency calls default to PSTN connection.
Max Digits	Leave as default – refers to maximum length of digit string
RFC2833 Outband DTMF	Value recommended by your VSP; default is Auto Negotiation
RTP Payload Type for RFC2833	Value recommended by your VSP; default is 101

Enable Phone Hotline (1&2)	Hotline function will automatically connect to a stipulated VoIP or PSTN phone number; if the box is checked and a number is entered, the nominated phone will ring as soon as the handset is lifted.
Enable pass "*"Call Feature to SIP Proxy:	Tick to enable the NB12WD to pass "*" key press to the SIP Proxy
FAX Mode:	Leave as default unless directed by VSP
Differentiating PSTN & VoIP Ring Tone.	To differentiate ring tone for PSTN and VoIP calls.
Differentiating PSTN & VoIP Dial Tone.	To differentiate dial tone for PSTN and VoIP calls.
Enable Silence Suppression	Leave as default unless directed by VSP

Field	Means
Enable Account 1 call waiting.	To enable Call waiting feature on Account 1.
Enable Account 2 call waiting.	To enable Call waiting feature on Account 2.
Enable Account 3 call waiting.	To enable Call waiting feature on Account 3.
Enable Account 4 call waiting.	To enable Call waiting feature on Account 4.
Call forward Type:.	To enable call forward on accounts 1- 4. Calls to the account will be forwarded to the nominated phone number in "Call Forward Phone Number" field.
Signaling and Media QoS.	Leave as default unless instructed by your VoIP Service Provider.

Once you have input these settings, click Apply and Save VoIP Parameters which will save your settings and attempt to register the NB12WD with your VSP.

Click on Device Info to check the status of your VoIP service. In the Device Info-Summary window, you will see the following status indicators:

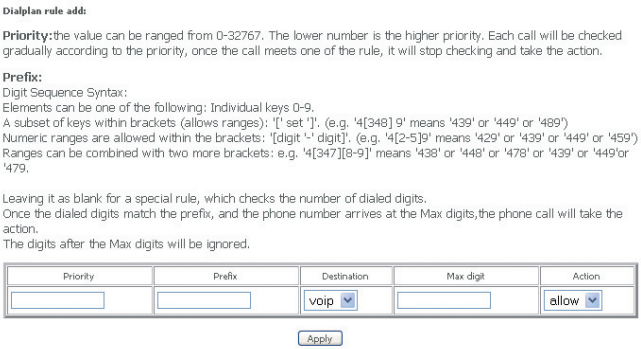
VoIP Status Indicator	Means
Direct Mode	VoIP is available but you are not connected to a SIP service. You are only able to make VoIP calls by entering IP details of remote device.
SIP Registration Fail	Usually indicates Invalid VoIP/SIP User ID and Password (= VoIP phone number and Authorisation Code). Check VoIP entries and try again.
SIP Registration Success	Connected to VSP; ready for VoIP phone calls. In this case you will hear a normal dial-tone.

Voice > Dial Plan

The NB12WD supports two types of Dial Plan. Outgoing Dial Plan works for both VoIP and PSTN connection and Incoming Dial Plan that only works for VoIP connection. Click on their respective link on the menu to access the configuration page.

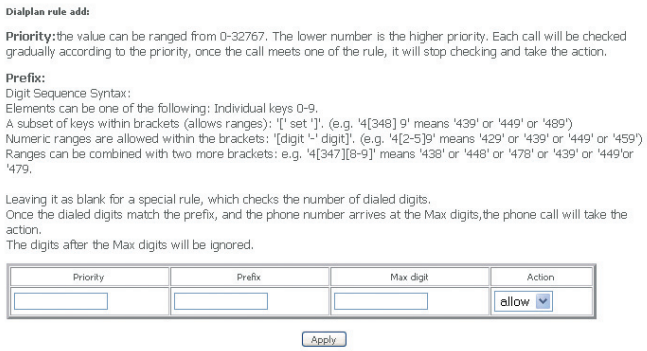
Voice > Dial Plan > Outgoing

Click the Add button to add a new Outgoing Dial Plan Rule.



Voice > Dial Plan > Incoming

Click the Add button to add a new Incoming Dial Plan Rule.



Voice > Dial Plan > Advance

This feature allows you to set advance Dial Plan.

Click the Add button to add a new rule.

Priority:	The value can be ranged from 0-32767. The lower number is the higher priority. Each call will be checked gradually according to the priority, once the call meets one of the rule, it will stop checking and take the action.
Prefix:	When the input numbers match the prefix numbers of the rule, the system will first delete the number of prefix defined in the DeleteDigit on the input number and then insert the digital numbers defined in the InsertDigit prior to the left number, and then call out with the recombination number.
MinDigit and MaxDigit:	The value can be ranged from 1-24. It defined the range of the number of the final adding number, for example, if the prefix is "123", the DeleteDigit is 1, and InsertDigit is "29998261". The system will firstly delete the number of the prefix, then the number will become as 23, and then insert 29998261 prior to 23, then the number will be "2999826123". Therefore, the MinDigit can be configured from 1 to 10 and the MaxDigit can be configured bigger than 10.
DeleteDigit:	Enter the number of prefix digit that you want to delete.
InsertDigit:	Enter the number you want to insert.

Examples:

index	Priority	Prefix	MinDigit	MaxDigit	DeleteDigit	InsertDigit
10	1	2	8	1	29998261	
20	23	1	8	2	29998261	
30	4567	1	9	3	29998261	

Example 1: when the user enter 123, the system will firstly delete the first number of the prefix, then the number will become as 23, and then insert 29998261 prior to 23, then the call-out number will be 2999826123.

Example 2: when the user enter 234, the system will firstly delete the first 2 number of the prefix, then the number will become as 4, and then insert 29998261 prior to 4, then the call-out number will be 299982614.

Example 3: when the user enter 456789, the system will firstly delete the first 3 number of the prefix, then the number will become as 789, and then insert 29998261 prior to 789, then the call-out number will be 29998261789.

Making Telephone Calls

To make a call, simply dial the number.

To dial an IP address directly, dial the IP address digits, using keypad * as the dot. Complete the address with a final * or #. When using IP address dialing it is not possible to specify which line at a gateway is called, so the gateway always routes IP-address dialed calls to the first line.

Network busy tone (fast busy) will be played for unknown or unreachable destinations.

To answer calls, simply pick up the phone or press the handsfree button.

Call Hold

To put a call on hold, press flash then hang up (optional). To return to the original call, press flash or pick up the phone. The phone will issue a short ring burst every 30 seconds or so while on-hook to remind you that a call is on hold.

Call Transfer

- To transfer a call, press flash then dial the new number.
- To transfer immediately, hang up (blind transfer).
- To transfer with consultation, wait for the party to answer, consult, and then hang up.
- To abort the transfer (if the third party does not answer), press flash to return to the original call.

Conference Calling

To turn a two-party call into a three-party conference call, press flash and dial the third party. Wait for the party to answer, then press flash.

To drop the third party and return to a two-party call, press flash again. To drop yourself out of the conference, hang up. The call will be transferred (so that the other two parties remain connected to each other). In conference mode, the conference initiator performs the audio bridge/mixing function – there are two voice streams established.

Call Waiting

If call waiting is enabled on a line (see feature codes), and you hear the call waiting tone during a call, press flash to answer the second call. The first call is automatically placed on hold. To switch between calls, press flash again.

- To disable the call waiting feature, dial *60.
- To enable the call waiting feature, dial *61.
- Call forward feature settings (Busy or All) takes priority over the call waiting feature.
- Call waiting feature is ignored on new incoming calls if there is already a call on hold or in conference.

Call Forward Number

- To set the call forward number, dial *74 then the number. Note that this does not actually enable forwarding; to do so, select the call forward action as described below.
- To disable all call forwarding features, dial *70

Call Forward No Answer

To enable call forward on no answer, dial *71. Incoming calls will be forward if unanswered for 18 seconds.

Call Forward Busy

To enable call forward if busy, dial *72. Incoming calls will be immediately forwarded if the phone is off-hook.

Call Forward All

- To enable call forward for all calls, dial *73.
- To disable the “forward all calls” feature, dial *75. Previous settings for Call Forward Busy or No Answer are not modified.

Call Return

To place a call to the last known incoming caller (unanswered or not), dial *69.

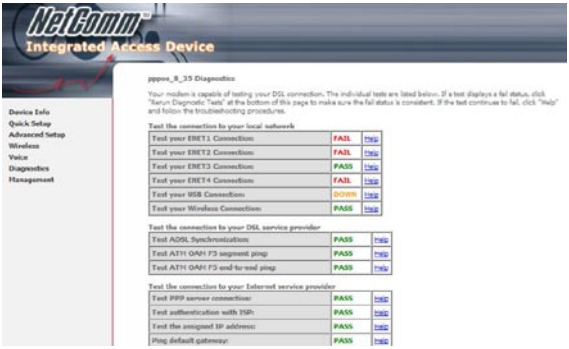
Redial

To redial the last outgoing number, dial *68 or press the redial key on your handse

Diagnostics

8.Diagnostics

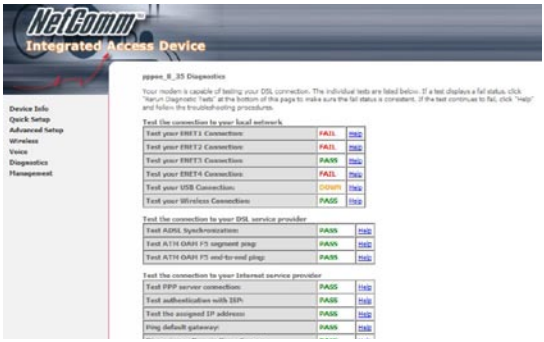
The Diagnostics menu provides feedback on the connection status of the router and the DSL link. The individual tests are listed below. If a test displays a fail status, click Rerun Diagnostic Tests at the bottom of this screen to make sure the fail status is consistent. If the test continues to fail, click Help and follow the troubleshooting procedures provided onscreen.



Test	Description
Ethernet Connection	Pass: Indicates that the Ethernet interface from your computer is connected to the LAN port of your router. Fail: Indicates that the router does not detect the Ethernet interface on your computer.
Wireless Connection	Pass: Indicates that the Wireless interface from your computer is connected to the wireless network. Down: Indicates that the router does not detect the wireless network.
ADSL Synchronization	Pass: Indicates that the router has detected an ADSL signal from the telephone company. Fail: Indicates that the router does not detect a signal from the telephone company's DSL network.

Additional tests are added here based upon connection type.

An example is provided below of the diagnostics screen for a PPPoE connection.



Ping Default Gateway	Pass: Indicates that the device can communicate with the first entry point to the network. It is usually the IP address of the ISP local router. Fail: Indicates that the device was unable to communicate with the first entry point on the network. It may not have an effect on your Internet connectivity. Therefore, if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.
Ping Primary Domain Name Server	Pass: Indicates that the device can communicate with the primary Domain Name Server (DNS). Fail: Indicates that the device was unable to communicate with the primary Domain Name Server (DNS). It may not have an effect on your Internet connectivity. Therefore, if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.

If multiple PVCs are configured you will have the option of testing each one in turn.

Click the Next Connection button at the bottom of the screen to do so.

Management

9. Management

9.1 Settings

The Management section includes the following functions and processes.

Settings	Internet Time
System Log	Access Control
SNMP Agent	Update Software
TR-069 Client	Save/Reboot

The Settings option allows you to back up your settings to a file, retrieve the setting file, and restore the settings.

9.1.1 Backup

The Backup option under Management > Settings saves your router configurations to a file on your PC. Click Backup Settings in the main menu. You will be prompted to define the location of the backup file to save. After choosing the file location, click Backup Settings. The file will then be saved to the assigned location.

9.1.2 Update

This option updates your router settings using a previously saved settings file.

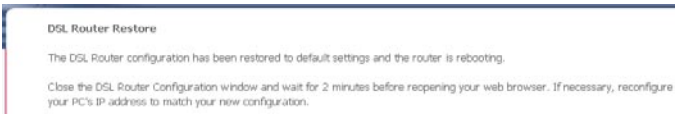
9.1.3 Restore Default

Clicking the Restore Default Configuration option in the Restore Settings screen can restore the original factory installed settings (see section 3.3 Default Settings).

NOTE 1: This option has the same effect as the hardware reset-to-default button on the rear panel of the router. The device board hardware and the boot loader support the reset to default button. If the reset button is pressed for more than 10 seconds, the configuration data will be erased.

NOTE 2: Restoring system settings requires a system reboot. The current Web UI session must be closed and restarted. Before restarting it, the IP configuration may need to be configured with a static IP address.

After the Restore Default Configuration button is selected, the following screen appears. Close the window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC IP address to match your new configuration.



9.2 System Log

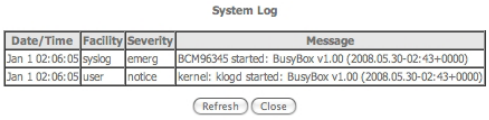
The System Log option under Management > Settings allows you to view the system events log, or to configure the System Log options. The default setting of system log is disabled. Follow the steps below to enable and view the system log.

1: Click **Configure System Log** to display the following screen.

2: Select from the desired Log options described in the following table, and then click **Save/Apply**.

Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, tick Enable and then Apply button.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the device SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging," which is the lowest critical level. The following log levels are • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the View System Log screen for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote syslog server or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

3: Click **View System Log**. The results are displayed as follows.



9.3 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 NB12WD(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.

To enable SNMP, change the setting for "SNMP Agent" to "Enable".

Field	Means
Read Community	Read device settings.
Set Community	Read and change device settings.
System Name	Default = NB12WD.
System Location	User-defined value.
System Contact	User-defined value.
Trap Manager IP	IP Address of admin machine.

9.4 TR-069 Client

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

Option	Description
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
Connection Request Authentication	Enable/Disable authentication of ACS making a Connection Request to the CPE.
Connection Request User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Connection Request Password	Password used to authenticate an ACS making a Connection Request to the CPE.
Get RPC Methods	This method may be used by a CPE or ACS to discover the set of methods supported by the ACS or CPE it is in communication with. This list may include both standard TR-069 methods (those defined in this specification or a subsequent version) and vendor-specific methods. The receiver of the response MUST ignore any unrecognized methods. Click this button to force the CPE to establish an immediate connection to the ACS.

9.5 Internet Time

The Internet Time option under the Management submenu configures the time settings of the device. To automatically synchronize with Internet time servers, tick the corresponding box displayed on this screen shown below.

First NTP time server: Select the required server.

Field	Description
Second NTP time serve	Select second time server, if required
Time zone offset	Select the local time zone

Configure these options and then click **Save/Apply** to activate.

9.6 Access Control

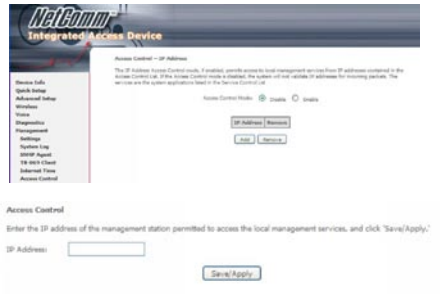
The Access Control option under the Management menu configures three access-related parameters: Services, IP Address and Passwords.

9.6.1 Services

The Services option limits or opens the access services over the LAN or WAN. These services are provided FTP, HTTP, ICMP, SSH, TELNET, and TFTP. Enable the service by checking the item in the corresponding checkbox, and then click **Save/Apply**.

9.6.2 Access IP Addresses

The IP Addresses option limits access by IP address. If Access Control Mode is enabled, only the IP addresses listed here can access the router. Before enabling it, configure the IP addresses by clicking the **Add** button. Enter the IP address and click **Apply** to allow the PC with this IP address to manage the device.



9.6.3 Passwords

The Passwords option configures the access passwords for the router. Access to your router is controlled through three user accounts: admin, support, and user.

- admin has unrestricted access to change and view the configuration of your router. It is the top administrative account.
- support is intended to allow limited access so that a technical support representative can conduct maintenance and run diagnostics.
- user provides the least access control but allows for viewing configuration settings and statistics, as well as, updating software.

Use the fields below to enter up to 16 characters and click **Save/Apply** to change or create passwords. See section 3.3 Default Settings for the default passwords.

9.7 Update Software

The Update Software screen allows you to update the software of the device. Manual software upgrades from a locally stored file can be performed using the following screen. Your ISP will provide this file to you, if necessary.

9.8 Save and Reboot

The Save/Reboot button saves the configurations and reboots the router. After clicking it, wait for 2 minutes before attempting to use the user interface. You may need to close and restart the web browser if it does not refresh automatically. You may need to reconfigure your PC IP address to match your new configuration. In this case, see section 3.1 TCP/IP Settings for detailed instructions.

Appendix

Appendix A: Printer Server

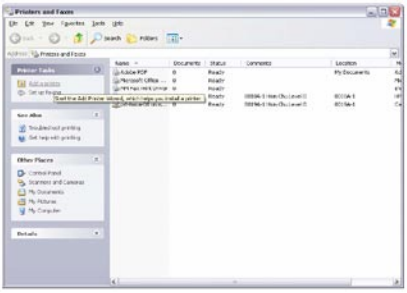
These steps explain the procedure for enabling the Printer Server.

1: Enable Print Server from Web User Interface.

Select **Enable on-board print server** checkbox and enter Printer name and Make and model

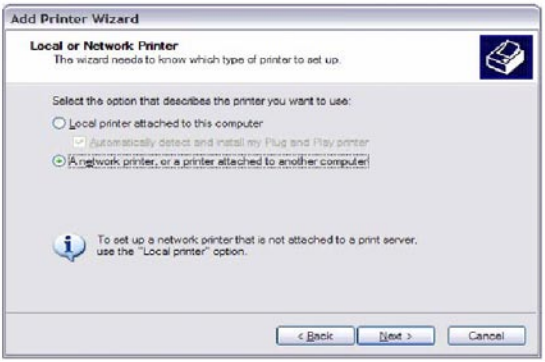
NOTE: The Printer name can be any text string up to 40 characters. The Make and model can be any text string up to 128 characters.

2: Go to the Printers and Faxes application in the Control Panel and select the Add a printer function (as located on the side menu below).



3: Click **Next** to continue, when you see the dialog box below.

4: Select Network Printer and click **Next**.

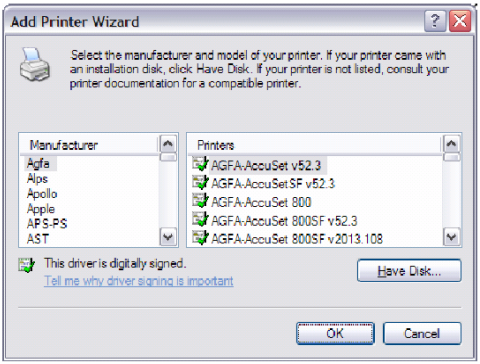


5: Select **Connect** to a printer on the Internet and enter your printer link.

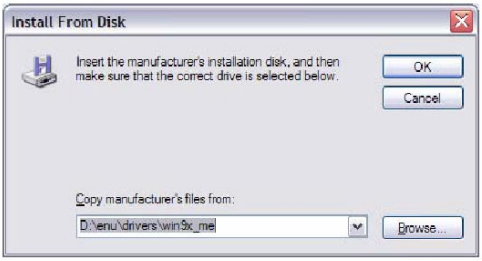
(e.g. http://192.168.1.1:631/printers/hp3845) and click **Next**.

NOTE: The printer name must be the same name entered in the web user interface "printer server setting" as in step 1.

6: Click Have **Disk** and insert the printer driver CD.



7: Select driver file directory on CD-ROM and click **OK**.

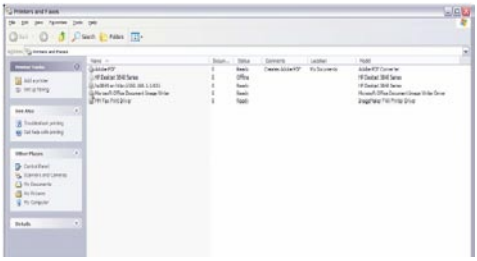


8: Once the printer name appears, click **OK**.

9: Choose Yes or No for default printer setting and click **Next**.

10: Click "**Finish**".

11: Check the status of printer from Windows Control Panel, printer window. Status should show as Ready.



Appendix B: Firewall

Stateful Packet Inspection

Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

Denial of Service attack

Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the router can withstand are: ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack and Tear Drop.

TCP/IP/Port/Interface filtering rules

These rules help in the filtering of traffic at the Network layer i.e. Layer 3. When a Routing interface is created "Enable Firewall" must be checked.Navigate to Advanced Setup -> Security -> IP Filtering, web page.

Outgoing IP Filtering: Helps in setting rules to DROP packets from the LAN interface. By default if Firewall is Enabled all IP traffic from LAN is allowed. By setting up one or more filters, particular packet types coming from the LAN can be dropped.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from: TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be dropped.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

Destination IP Address/Destination Subnet Mask: Packets with the particular "Destination IP Address/ Destination Subnet Mask" combination will be dropped.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

Examples:

1.	Filter Name	: Out_Filter1
	Protocol	: TCP
	Source Address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0
	Source Port	: 80
	Dest. Address	: NA
	Dest. Sub. Mask	: NA
	Dest. Port	: NA

This filter will Drop all TCP packets coming from LAN with IP Address/Sub. Mask 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

2.	Filter Name	: Out_Filter2
	Protocol	: UDP
	Source Address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0
	Source Port	: 5060:6060
	Dest. Address	: 172.16.13.4
	Dest. Sub. Mask	: 255.255.255.0
	Dest. Port	: 6060:7070

This filter will drop all UDP packets coming from LAN with IP Address/Sub. Mask 192.168.1.45/24 and a source port in the range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port in the range of 6060 to 7070

Incoming IP Filtering:

Helps in setting rules to ACCEPT packets from the WAN interface. By default all incoming IPtraffic from WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, particular packet types coming from the WAN can be Accepted.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from: TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be accepted.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers (portX : portY) will be accepted.

Destination IP Address/Destination Subnet Mask: Packets with the particular "Destination IP Address/ Destination Subnet Mask" combination will be accepted.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

The WAN interface on which these rules apply needs to be selected by the user.

Examples:

1.	Filter Name	: In_Filter1
	Protocol	: TCP
	Source Address	: 210.168.219.45
	Source Subnet Mask	: 255.255.0.0
	Source Port	: 80
	Dest. Address	: NA
	Dest. Sub. Mask	: NA
	Dest. Port	: NA

Selected WAN interface: mer_0_35/nas_0_35

This filter will ACCEPT all TCP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub. Mask 210.168.219.45/16 having a source port of 80 irrespective of the destination. All other incoming packets on this interface are DROPPED.

2.	Filter Name	: In_Filter2
	Protocol	: UDP
	Source Address	: 210.168.219.45
	Source Subnet Mask	: 255.255.0.0
	Source Port	: 5060:6060
	Dest. Address	:192.168.1.45
	Dest. Sub. Mask	: 255.255.255.0
	Dest. Port	: 6060:7070

This rule will ACCEPT all UDP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub. Mask 210.168.219.45/16 and a

source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC Layer Filtering:

These rules help in the filtering of traffic at the Layer 2. MAC Filtering is only effective on ATM PVCs configured in Bridge mode. After a Bridge mode PVC is created, navigate to Advanced Setup -> Security -> MAC Filtering web page.

Global Policy:

When set to Forwarded the default filter behavior is to Forward all MAC layer frames except those explicitly stated in the rules. Setting it to Blocked changes the default filter behavior to Drop all MAC layer frames except those explicitly stated in the rules.

To setup a rule:

Protocol Type: Can be PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI or IGMP.

Destination MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular destination address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Source MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular source address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Frame Direction:

LAN <=> WAN --> All Frames coming/going to/from LAN or to/from WAN.

WAN => LAN --> All Frames coming from WAN destined to LAN.

LAN => WAN --> All Frames coming from LAN destined to WAN

User needs to select the interface on which this rule is applied.

1.	Global Policy:	Forwarded
	Protocol Type:	PPPoE
	Dest. MAC Addr:	00:12:34:56:78
	Source MAC Addr:	NA
	Frame Direction:	LAN => WAN

WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule drops all PPPoE frames going from LAN-side to WAN-side with a Dest. MAC Addr. of 00:12:34:56:78 irrespective of its Source MAC Addr. on the br_0_34 WAN interface. All other frames on this interface are forwarded.

Protocol Type:	PPPoE
Dest. MAC Addr:	00:12:34:56:78:90
Source MAC Addr:	00:34:12:78:90:56
Frame Direction:	WAN => LAN

WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule forwards all PPPoE frames going from WAN-side to LAN-side with a Dest. MAC Addr. of 00:12:34:56:78 and Source MAC Addr. of 00:34:12:78:90:56 on the br_0_34 WAN interface. All other frames on this interface are dropped.

Daytime Parental Control

This feature restricts access of a selected LAN device to an outside Network through the router, as per chosen days of the week and the chosen times.

User Name: Name of the Filter.

Browser's MAC Address: Displays MAC address of the LAN device on which the browser is running.

Other MAC Address: If restrictions are to be applied to a device other than the one on which the browser is running, the MAC address of that LAN device is entered.

Days of the Week: Days of the week, when the restrictions are applied.

Start Blocking Time: The time when restrictions on the LAN device

are put into effect.

End Blocking Time: The time when restrictions on the LAN device are lifted.

Example:

User Name:	FilterJohn
Browser's MAC Address:	00:25:46:78:63:21
Days of the Week:	Mon, Wed, Fri
Start Blocking Time:	14:00
End Blocking Time:	18:00

When this rule i.e. FilterJohn is entered, a LAN device with MAC Address of 00:25:46:78:63:21 will be restricted access to the outside network on Mondays, Wednesdays and Fridays, from 2pm to 6pm. On all other days and time this device will have access to the outside Network.

Appendix C: Pin Assignments

Line Port (RJ11)

Pin	Definition	Pin	Definition
1	-	4	ADSL_TIP
2	-	5	-
3	ADSL_RING	6	-

LAN Port (RJ45)

Pin	Definition	Pin	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

Appendix D: Specifications

Back Panel

RJ11 X1 for ADSL2+, RJ45 X 4 for LAN, Reset Button X 1, Power Jack X 1, WiFi antenna, USB host/device

DSL

ADSL2+ Downstream : 24 Mbps **Upstream :** 1.3 Mbps

Standards: ITU-T G.992.5, G.992.3, G.992.1; ANSI T1.413 Issue 2; AnnexM

Standards:ITU-T G.993.2 (profiles 8a,8b,8c,8d,12a,12b,17a)

Ethernet

Standard	IEEE 802.3, IEEE 802.3u
10/100 BaseT	Auto-sense
MDI/MDX support	Yes

Wireless

Standard	IEEE802.11g, backward compatible with 802.11b
Encryption	64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption
Channels	13 Channels (Australia)
Data Rate	Up to 54Mbps

WPA/WPA2, IEEE 802.1x, MAC address filtering, Variable output power levels (10, 25, 50, 100 mW @ 22 MHz channel bandwidth)

ATM Attributes

RFC 2364 (PPPoA), RFC 2684 (RFC 1483) Bridge/Route; RFC 2516 (PPPoE);

RFC 1577 (IPoA)

Support PVCs	16
AAL type	AAL5
ATM service class	UBR/CBR/VBR
ATM UNI support	UNI 3.1/4.0
OAM F4/F5	Yes

Management

TR-069/TR-098/TR-104/TR-111, SNMP, Telnet, Web-based management, Configuration backup and restoration, Software upgrade via HTTP, TFTP server, or FTP server

Bridge Functions

Transparent bridging and learning	IEEE 802.1d
VLAN support	Yes
Spanning Tree Algorithm	Yes
IGMP Proxy	Yes

Routing Functions

Static route, RIP v1/v2, NAT/PAT, DHCP Client/Server/Relay, DNS, ARP

Security Functions

Authentication protocols: PAP, CHAP, TCP/IP/Port filtering rules, Packet and MAC address filtering, Access Control

Encryption protocol: SSH

Port triggering/Forwarding, Stateful Packet Inspection, Denial Of Service protection, Traffic Conditioning, WFQ-based Bandwidth Management, HTTP proxy

Application Passthrough

PPTP, L2TP, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box, etc

QoS: L3 policy-based QoS, IP QoS, ToS

OS Supported for USB driver

Windows Vista/2000/XP/ME/98SE

Power Supply: External power adapter 100 - 240 Vac, 15VDC / 1.6A

Environment Condition

Operating temperature: 0 ~ 50 degrees Celsius

Relative humidity: 5 ~ 95% (non-condensing)

Dimensions: 205 mm (W) x 48 mm (H) x 145 mm (D)

Kit Weight: 1 kg ~ 1 x NB12WD

1 x RJ-11 cable

1 x RJ-45 cable

1 x USB cable

1 x power adapter

1 x cd-rom

NOTE: Specifications are subject to change without notice

Linux OS comes with ssh client. Microsoft Windows does not have ssh client but there is a public domain one "putty" that you can download.

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Appendix E: SSH Client

To access the router using Linux ssh client:

From LAN: Use the router WEB UI to enable SSH access from LAN.

(default is enabled)

type: ssh -l admin 192.168.1.1

From WAN: From the router, use WEB UI to enable SSH access from WAN.

type: ssh -l support xx:xx:xx:xx (router WAN IP address)

To access the router using Windows putty ssh client:

From LAN: Use the router WEB UI to enable SSH access from LAN

(default is enabled)

type: putty -ssh -l admin 192.168.1.1

From WAN: From the router, use WEB UI to enable SSH access from WAN.

type: putty -ssh -l support xx:xx:xx:xx (router WAN IP address)

Appendix F: 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

ADSL2+ Router

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