



N600 Dual Band WiFi Gigabit Modem Router with Voice



NB16WV-02
USER GUIDE

Copyright

Copyright©2013 NetComm Wireless Limited. All rights reserved.

The information contained herein is proprietary to NetComm Wireless Limited. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NetComm Wireless Limited.



Please note: This document is subject to change without notice.

Save Our Environment

When this equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separately from domestic waste.

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

Please be responsible and protect our environment.

This manual covers the following products:

NetComm Wireless NB16WW-02

DOCUMENT VERSION	DATE
1.0 Initial document release	1 May 2013
1.1 Updated to include WPS button function description	24 November 2014
1.2 Updated to NCMZO_1016_04231050	6 May 2015
1.3 Updated Dial Plan section with dial plan syntax	1 September 2016

Table 1 - Document Revision History

Table of Contents

Overview	5
Introduction.....	5
Target Users.....	5
Prerequisites.....	5
VoIP Telephony Requirements.....	5
Notation.....	5
Product Introduction	6
Product Overview.....	6
Package Contents.....	6
Product Features.....	7
Physical Dimensions and Indicators	8
LED Indicators.....	8
Physical Dimensions.....	9
NB16WV-02 Default Settings.....	9
Interfaces	10
Safety and Product Care	11
Transport and Handling	11
Installation and Configuration of the NB16WV-02	12
Placement of your NB16WV-02.....	12
Avoid obstacles and interference.....	12
Cordless Phones.....	12
Choose the “Quietest” Channel for your Wireless Network.....	12
Hardware installation.....	13
Connecting via a cable.....	13
Connecting wirelessly.....	13
Telephone Setup.....	13
Web Based Configuration Interface	14
First-time Setup Wizard.....	14
ADSL.....	15
Mobile Broadband.....	16
WAN.....	16
Basic View.....	21
Status.....	21
Wireless 2.4GHz.....	22
Wireless 5GHz.....	22
Mobile Broadband.....	23
ADSL.....	23
Advanced Configuration.....	25
Status.....	25
Network Setup.....	26
Forwarding Rules.....	44
Security Settings.....	48
Advanced Settings.....	55
VoIP Settings.....	67
Call Features.....	73
NAS Settings.....	78
Toolbox.....	83
Additional Product Information	85
Establishing a wireless connection.....	85
Windows XP (Service Pack 3).....	85
Windows Vista.....	85
Windows 7.....	85
Windows 8/8.1.....	85
Mac OSX 10.6.....	85
Troubleshooting.....	86
Using the indicator lights (LEDs) to Diagnose Problems.....	86
Technical Data	86
Electrical Specifications.....	86
Environmental Specifications / Tolerances.....	86
Legal & Regulatory Information	87

Intellectual Property Rights.....	87
Customer Information	87
Consumer Protection Laws.....	87
Product Warranty	88
Limitation of Liability.....	88
Contact.....	89

Overview

Introduction






This manual provides information related to the installation, operation, and utilisation of the NB16WW-02.

Target Users




The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

Prerequisites

Before continuing with the installation of your NB16WW-02, please confirm that you comply with the minimum system requirements below.

-  An activated ADSL, activated 3G, or configured Ethernet WAN connection.
-  Computer with Windows, Macintosh, or Linux-based operating systems with a working Ethernet adapter with TCP/IP Protocol installed.
-  A Web Browser such as Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Safari etc.
-  Wireless Computer System Requirements:
 -  Computer with a working 802.11b, 802.11g or 802.11n wireless adapter.

VoIP Telephony Requirements

-  Standard analogue PSTN or cordless PSTN phone handset (DECT) with an RJ-11 port.
(ISDN phone handsets are not supported)
-  RJ-11 to RJ-11 phone connectivity cable
-  Subscription to a VoIP Service by a VoIP Service Provider using SIP version 1.0 or 2.0 (Session Initiation Protocol)

Notation

The following symbols are used in this manual:



Indicates a note requiring attention.



Indicates a note providing a warning.



Indicates a note providing useful information.

Product Introduction

Product Overview

- Powerful dual-band wireless router with support for ADSL and 3G/4G Mobile Broadband.
- Creates instant Wireless hotspots to share the Internet connection of a 3G/4G USB modem or DSL/Cable connection.
- Supports Wireless N standard with data speeds up to 600Mbps.
- One Gigabit WAN port for alternate wired Internet connection (DSL/Cable/Satellite via Ethernet).
- Four Gigabit LAN ports to connect wired devices like PCs or gaming consoles.
- One RJ-11 port to connect an analogue telephone for use with a VoIP service.
- Ensures connectivity and business continuity with auto Internet failover from ADSL to Ethernet WAN or 3G Mobile Broadband.
- Easy Wi-Fi Protected Setup (WPS) by the single touch of a button to establish a secure wireless connection
- Full Wireless security - WEP, WPA, WPA2.
- Browser based interface for configuration and management: OS independent and easy to use.
- File server (FTP / NAS).
- Download assistant.
- Web HDD function.

Speeds are dependent on network coverage. See your 3G provider coverage maps for more details. The total number of Wi-Fi users can also affect data speeds. Maximum wireless signal rate and coverage values are derived from IEEE Standard 802.11g and 802.11n specifications. Actual wireless speed and coverage are dependent on network and environmental conditions included but not limited to volume of network traffic, building materials and construction/layout.

Package Contents

The NB16WW-02 package consists of:

- N600 Dual Band WiFi Gigabit Modem Router with Voice - NB16WW-02.
- Quick Start Guide.
- Power Supply Unit.
- Ethernet Cable (RJ-45).
- Phone Cable (RJ-11).
- Wireless Security Card.
- Warranty Card.

If any of these items are missing or damaged, please contact NetComm Wireless Support immediately by visiting the NetComm Wireless Support website at: <http://www.netcommwireless.com/contact-forms/support>

Product Features

The NetComm NB16WW-02 integrates an ADSL modem, dual-band wireless LAN, full Gigabit Ethernet interface and multi-functional USB port into one unit. Connection to the Internet is achieved through the ADSL modem, a 3G/4G service, fixed line or via a connection to the NB16WW-02's Ethernet WAN port, providing you with the flexibility to choose how you access the Internet.

The NB16WW-02's automatic failover ensures you are always connected by activating the 3G/4G connection should the ADSL or Ethernet WAN connection drop out.

Users are able to share a single Internet connection via both a wired and wireless connection to the NB16WW-02. With a built in antennas providing a 2 transmit, 2 receive (2T2R) 802.11n concurrent dual band wireless access point, this router provides theoretical combined wireless speeds of up to 600Mbps.

On top of this, the NB16WW-02 has four gigabit LAN ports for high-speed wired connections to multiple devices. The NB16WW-02 allows you to simply insert a 3G/4G USB Modem with SIM card and utilise 3G/4G Mobile Broadband for Internet connectivity.

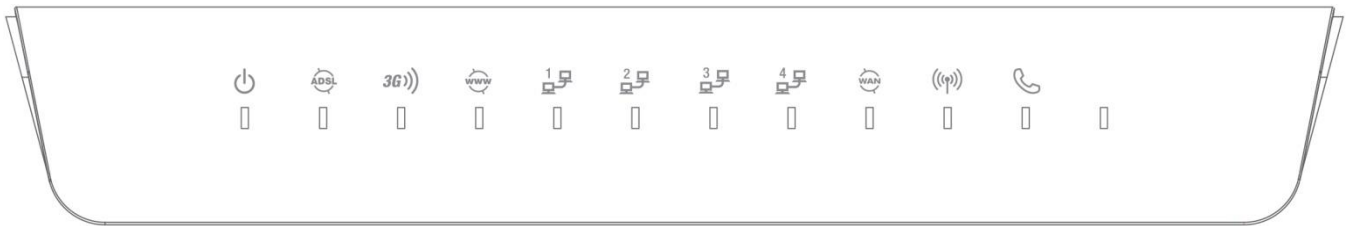
Integrated VoIP telephony enables the NB16WW-02 to offer a highly cost efficient solution for making interstate or overseas calls using the mobile broadband connection, especially in locations that lack fixed line infrastructure or as an alternative to traditional landline based Internet services. All you require is a traditional analogue/cordless phone and an activated account with a VoIP service provider.










The NB16WW-02 also includes advanced security features such as VPN pass-through, a wide array of wireless security options and a built in firewall.

Physical Dimensions and Indicators

LED Indicators

The NB16WV-02 has been designed to be placed on a desktop. All of the cables exit from the rear for easy organization. The display is visible on the front of the NB16WV-02 to provide you with information about network activity and the device status. See below for an explanation of each of the indicator lights.



LED INDICATOR	ICON	COLOUR	DEFINITION
Power		Off	The NB16WV-02 is powered off
		Blue	The NB16WV-02 is powered on and operating normally
		Blue Flashing	The NB16WV-02 is starting up
ADSL		Off	No ADSL configuration present
		Blue	The NB16WV-02 is connected to the Internet via an xDSL service
		Blue Flashing	The NB16WV-02 is attempting to connect to the xDSL service
3G		Off	No 3G/4G configuration present (or no 3G/4G dongle plugged in)
		Red	SIM Error
		Red Flashing	3G/4G connection failed - Retrying
		Blue	The NB16WV-02 is connected to the Internet via a 3G/4G service
WWW		Blue Flashing	The NB16WV-02 is attempting to connect to the 3G/4G service
		Off	No Internet configuration present
		Red	The NB16WV-02 is connected via a 3G service
		Flashing Red	Data is being sent or received via the 3G service
LAN 1-4		Blue	The NB16WV-02 is connected via an xDSL service
		Flashing Blue	Data is being sent or received via the xDSL service
		Purple	The NB16WV-02 is connected via an Ethernet WAN service
		Flashing Purple	Data is being sent or received via the Ethernet WAN service
WAN		Off	No device is connected to the Ethernet LAN port
		Blue	A device is connected to the Ethernet LAN port
		Flashing Blue	Data is being sent or received via the Ethernet LAN port
WIFI		Off	No device is connected to the Ethernet WAN port
		Blue	A device is connected to the Ethernet WAN port
		Flashing Blue	The NB16WV-02 is attempting to connect to the Ethernet WAN port
VoIP		Off	WiFi is disabled on the NB16WV-02
		Blue	WiFi is enabled on the NB16WV-02
		Flashing Blue	The NB16WV-02 is waiting for a WPS PBC client connection
VoIP		Off	No VoIP service is configured
		Blue	The NB16WV-02 is registered with the configured VoIP service
		Flashing Blue	The NB16WV-02 is attempting to connect to the configured VoIP service

Physical Dimensions

The following page lists the physical dimensions of the NB16WW-02.



NB16WW-02 DIMENSIONS	
Length	215 mm
Width	145 mm
Height	37 mm
Weight	403 grams

NB16WW-02 Default Settings

The following tables list the default settings for the NB16WW-02.

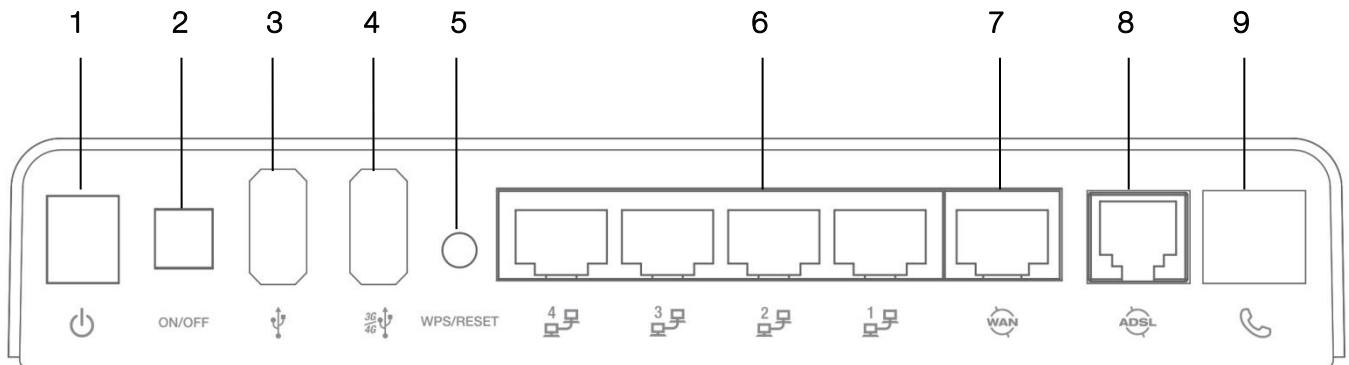
LAN (MANAGEMENT)	
Static IP Address:	192.168.20.1
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.20.1

WIRELESS (WI-FI)	
SSID:	(Refer to the included Wireless Security Card)
Security:	WPA2-PSK (w AES encryption)
Security Key:	(Refer to the included Wireless Security Card)

NB16WW-02 WEB INTERFACE ACCESS	
Username:	admin
Password:	admin

Interfaces




The following interfaces are available on the NB16WV-02:



NUMBER	INTERFACE	DESCRIPTION
1	Power Jack	Connection point for the included power adapter. Connect the power supply here.
2	Power button	Turns the NB16WV-02 on or off.
3	USB 2.0 (File Sharing)	Connect a USB based storage device here.
4	USB 2.0 (3G/4G Modem)	Connect a 3G/4G USB modem here.
5	WPS button	Activate the WiFi WPS function. a) Hold for 1-3 seconds then release to trigger the 2.4GHz WPS b) Hold for 4-6 seconds then release to trigger the 5GHz WPS c) Hold for 15 seconds then release to reset the NB16WV-02 to factory default settings.
6	LAN 1-4	Gigabit Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.
7	WAN	Gigabit WAN port for connection to a WAN network.
8	ADSL	Use the provided RJ-11 cable to connect the router to the telephone line operating your xDSL service.
9	Telephone	Phone port for a standard PSTN analogue telephone handset. Connect a phone to this port to make use of a VoIP service.

Safety and Product Care

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, 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.
-  To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are unobstructed.



WARNING

Disconnect the power line from the device before servicing.

Transport and Handling

When transporting the NB16WV-02, it is recommended to return the product in the original packaging. This ensures the product will not be damaged.



In the event the product needs to be returned, ensure it is securely packaged with appropriate padding to prevent damage during courier transport.

Installation and Configuration of the NB16WV-02

Placement of your NB16WV-02



The wireless connection between your NB16WV-02 and your WiFi devices will be stronger the closer your connected devices are to your NB16WV-02. Your wireless connection and performance will degrade as the distance between your NB16WV-02 and connected devices increases. This may or may not be directly noticeable, and is greatly affected by the individual installation environment.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between three to five meters from the NB16WV-02 in order to see if distance is the problem.









Please note: While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning; if you are concerned that your network is not operating at its maximum effectiveness, this checklist may help.

If you experience difficulties connecting wirelessly between your Wi-Fi Devices and your NB16WV-02, please try the following steps:

-  In multi-storey homes, place the NB16WV-02 on a floor that is as close to the centre of the home as possible. This may mean placing the NB16WV-02 on an upper floor.
-  Try not to place the NB16WV-02 near a cordless telephone that operates at the same radio frequency as the NB16WV-02 (2.4GHz).





Avoid obstacles and interference

Avoid placing your NB16WV-02 near devices that may emit radio "noise," such as microwave ovens. Dense objects that can inhibit wireless communication include:

-  Refrigerators
-  Washers and/or dryers
-  Metal cabinets
-  Large aquariums
-  Metallic-based, UV-tinted windows
-  If your wireless signal seems weak in some spots, make sure that objects such as those listed above are not blocking the signal's path (between your devices and the NB16WV-02).

Cordless Phones

If the performance of your wireless network is impaired after considering the above issues, and you have a cordless phone:

-  Try moving cordless phones away from your NB16WV-02 and your wireless-enabled computers.
-  Unplug and remove the battery from any cordless phone that operates on the 2.4GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering with the NB16WV-02.
-  If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your NB16WV-02 to channel 11. See your phone's user manual for detailed instructions.
-  If necessary, consider switching to a 900MHz or 5GHz cordless phone.

Choose the "Quietest" Channel for your Wireless Network

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with your wireless network. Use the Site Survey capabilities found in the Wireless Utility of your wireless adapter to locate any other wireless networks that are available (see your wireless adapter's user manual), and switch your Router and computers to a channel as far away from other networks as possible.

Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighbouring cordless phones or other wireless devices.

Hardware installation

1. Connect the power adapter to the Power socket on the back of the NB16WV-02.
2. Plug the power adapter into the wall socket and switch on the power.
3. Wait approximately 60 seconds for the NB16WV-02 to power up.

Connecting via a cable

1. Connect the yellow Ethernet cable provided to one of the ports marked 'LAN' at the back of the NB16WV-02.
2. Connect the other end of the yellow Ethernet cable to your computer.
3. Wait approximately 30 seconds for the connection to establish.
4. Open your Web browser, and enter <http://192.168.20.1> into the address bar and press enter.
5. Follow the steps to set up your NB16WV-02.

Connecting wirelessly

1. Ensure Wi-Fi is enabled on your device (computer/laptop/Smartphone).
2. Scan for wireless networks in your area and connect to the network name that matches the Wireless network name configured on the NB16WV-02.



Note: Refer to the included Wireless Security Card for the default SSID and wireless security key of your NB16WV-02

3. When prompted for your wireless security settings, enter the Wireless security key configured on the NB16WV-02.
4. Wait approximately 30 seconds for the connection to establish.
5. Open your Web browser, and enter <http://192.168.20.1> into the address bar and press Enter.
6. Follow the steps to set up your NB16WV-02.

Telephone Setup

1. Insert the RJ-11-to-RJ-11 cable that comes delivered with your telephone into the FXS Phone Port (RJ-11) of the NB16WV-02.
2. Make sure the other end of the cable is plugged firmly into the RJ-11 port of your telephone.
3. Follow the steps to setup your VoIP account details.

Web Based Configuration Interface

Interface

First-time Setup Wizard

Please follow the steps below to configure your NB16WV-02 Wireless router via the web based configuration wizard.

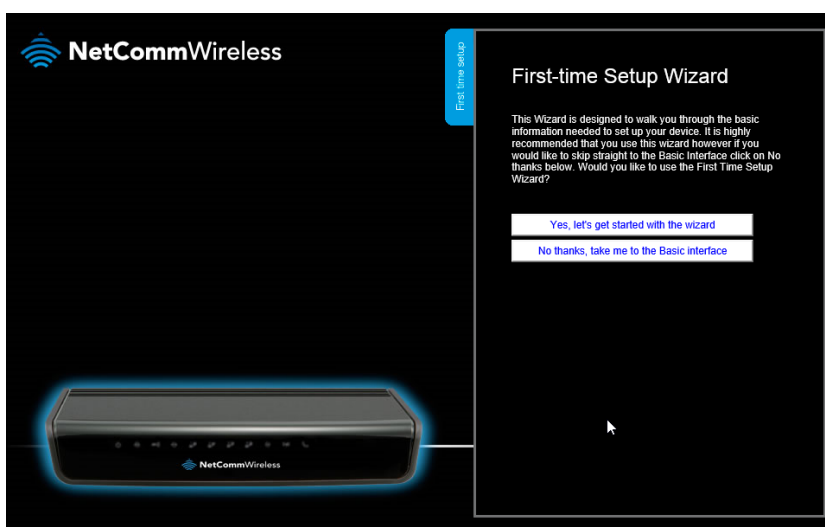
Open your web browser (e.g. Internet Explorer/Firefox/Safari) and type <http://192.168.20.1/> into the address bar at the top of the window.

At the login screen, type **admin** in the username and password field, then click the **Login** button.

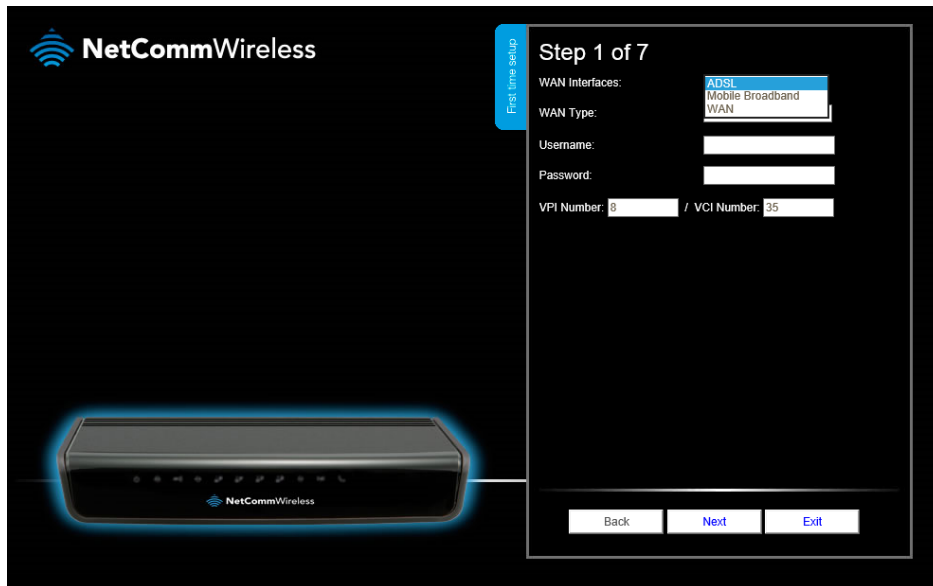


Note: admin is the default username and password for the unit.




1. Click on **Yes, let's get started with the wizard.**



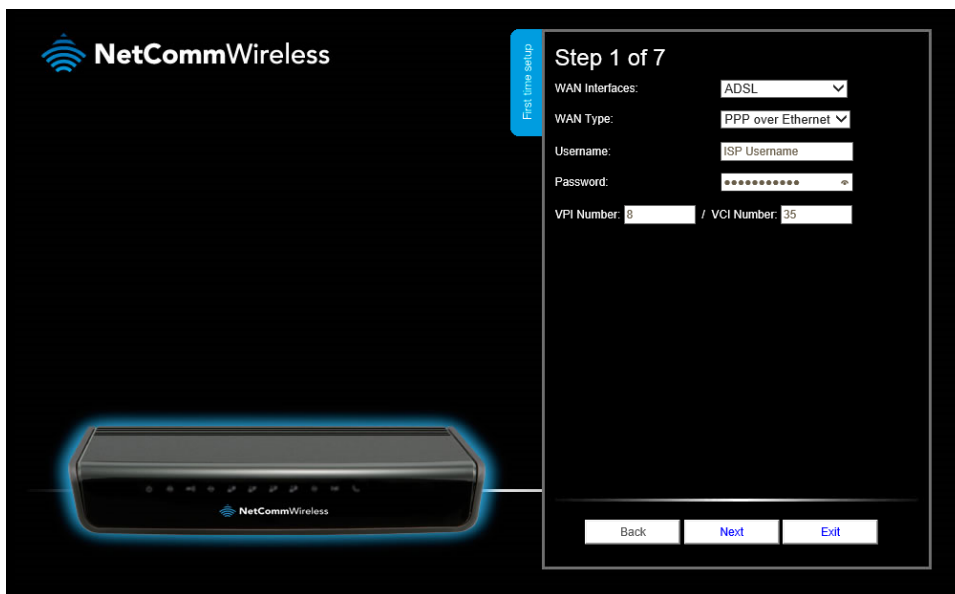
The wizard assists you in configuring the router and entering the information required to setup your Internet connection.





2. From the **WAN Interface** pull down menu, select the type of Internet connection you would like to use. You can select from:


-  ADSL
-  Mobile Broadband
-  WAN

ADSL



- a. Select the type of ADSL connection. You can select from:
 -  PPP over ATM (or PPPoA)
 -  PPP over Ethernet (or PPPoE)
- b. Enter the Username and Password as supplied by your Internet Service Provider.
- c. Enter the appropriate VCI and VPI as supplied by your Internet Service Provider.
- d. Click **Next** to continue.

Mobile Broadband



Step 1 of 7

WAN Interfaces:

Country:

Service Provider:

Network Name (APN):

Username:

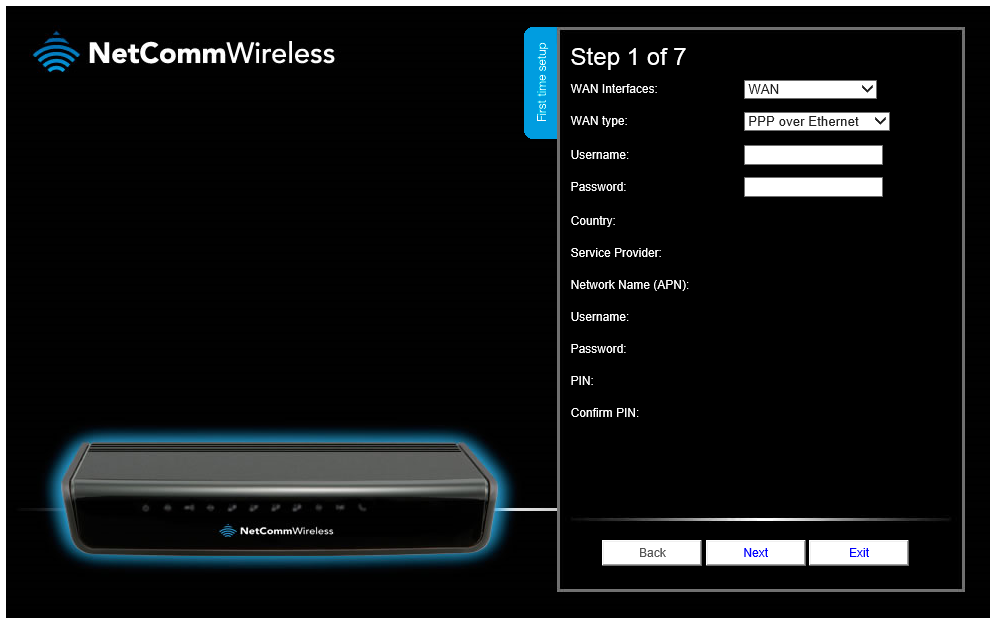
Password:

PIN:

Confirm PIN:

- Select your country and mobile broadband service provider from the list.
- Check that the APN displayed is correct as per the information provided by your mobile broadband provider.
- If your carrier requires you to log on to the network, enter the authentication criteria in the Username and Password fields.
- If your SIM requires a PIN, enter it in the PIN and Confirm PIN fields.
- Click **Next** to continue.

WAN



Step 1 of 7

WAN Interfaces:

WAN type:

Username:

Password:

Country:

Service Provider:

Network Name (APN):

Username:

Password:

PIN:

Confirm PIN:

Select the type of WAN connection:

Dynamic IP Address

- Enter the Host Name (Optional)
- Enter the MAC Address of your device which is registered with the ISP

Static IP Address

- a. Enter the Static IP Address.
- b. Enter the Static Subnet Mask.
- c. Enter the Static Gateway.
- d. Enter the Static Primary and Secondary DNS.

PPP over Ethernet (or PPPoE)

Enter the PPPoE Username and Password supplied by your service provider.

PPTP

- a. Enter the Server IP Address/Name.
- b. Enter the PPTP Account and PPTP Password.

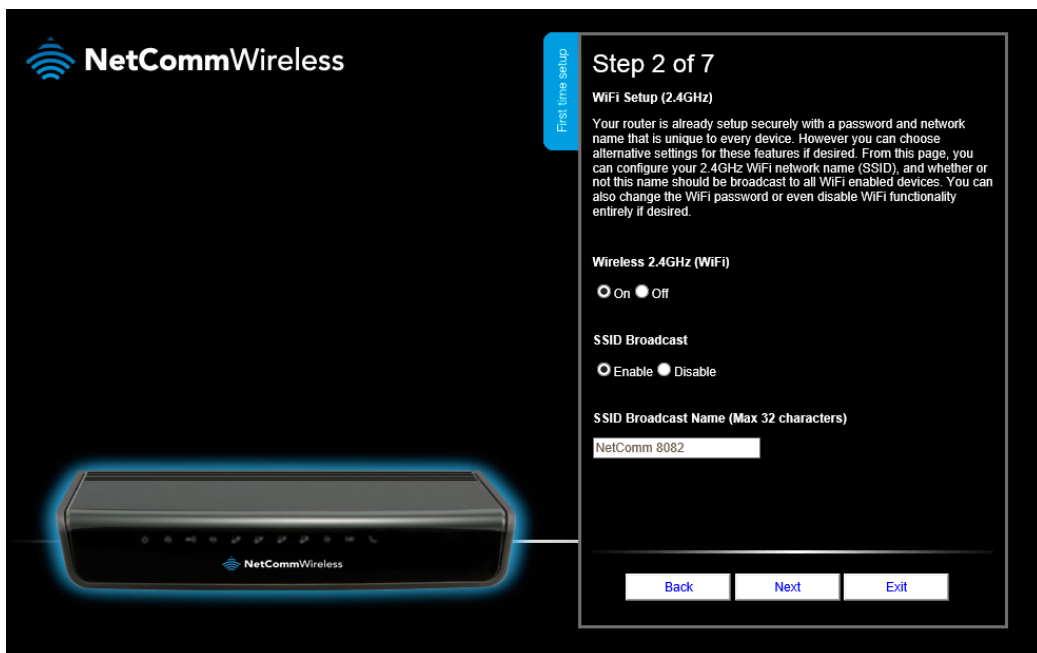
L2TP

- a. Enter the Server IP Address/Name.
- b. Enter the PPTP Account and PPTP Password.


Click **Next** when you have entered the required details.

3. If you want to change the 2.4GHz Wireless network settings, you can do so on this page. You can enable or disable the Wireless network, select whether to broadcast your SSID or not and change the Wireless network name. Change the settings as needed and click **Next**.

(If you wish to use the default settings, click **Next**)



4. You can change the WiFi 2.4GHz security key if you wish by using the **Security Key Type** drop down list and then typing in a new security key in the **Security Key** field. The Security key must be at least 8 characters long. Click **Next** to continue.



NetCommWireless

Step 3 of 7

Router Security

A **WiFi 2.4GHz** Security Key is already set-up with your Router, however you can change that key here if desired. You can also change the security type below. To connect to the Router via WiFi you will need to enter the Security Key into your device.

Security Key Type

WPA2-PSK

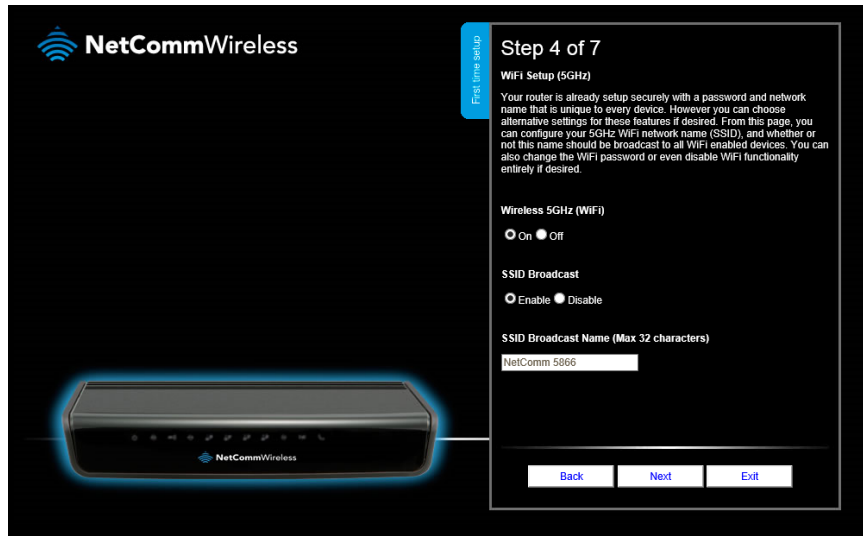
Security Key (Minimum of 8 characters)

jodamefiga

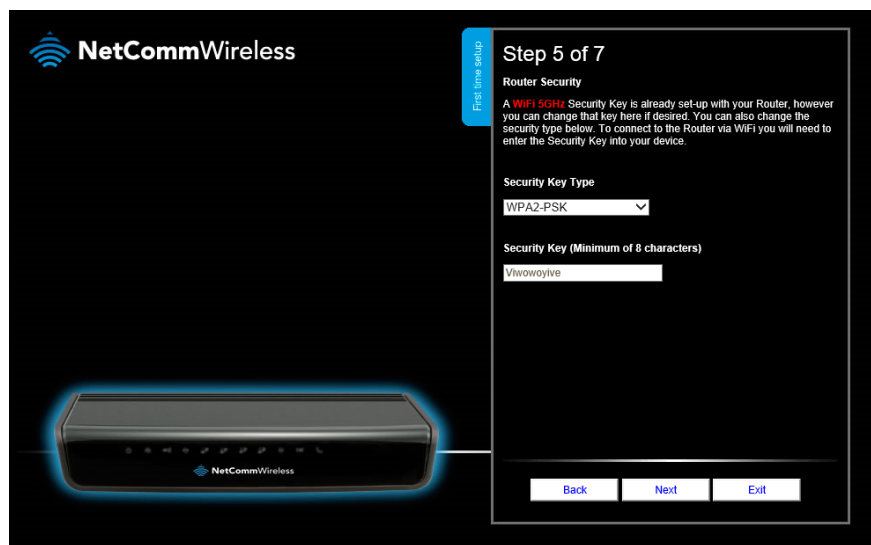
Back Next Exit

- If you want to change the 5GHz Wireless network settings, you can do so on this page. You can enable or disable the Wireless network, select whether to broadcast your SSID or not and change the Wireless network name. Change the settings as needed and click **Next**.

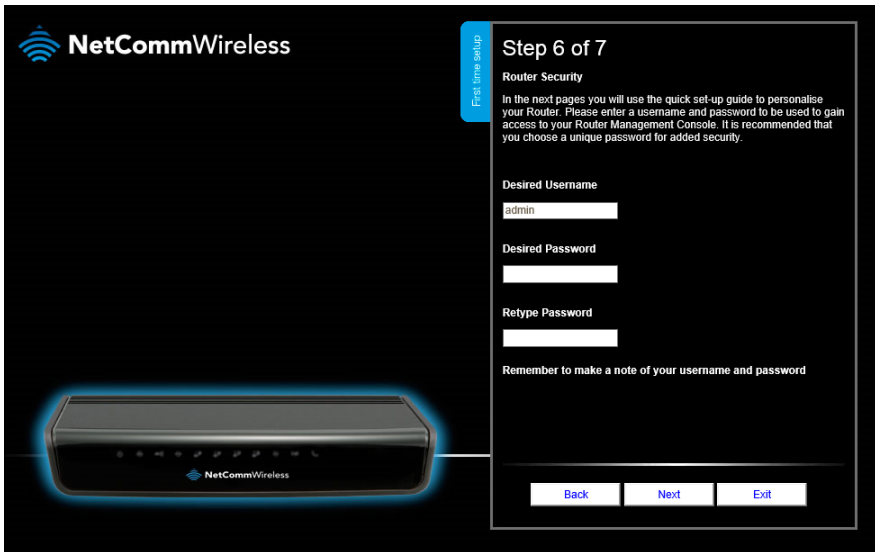
(If you wish to use the default settings, click **Next**)



- You can change the WiFi 5GHz security key if you wish by using the **Security Key Type** drop down list and then typing in a new security key in the **Security Key** field. The Security key must be at least 8 characters long. Click **Next** to continue.



- If you want to change the system username or password, enter the new username in the **Desired Username** field and then enter the new password into both the **Desired Password** and **Retype Password** fields and then click **Next**. (If you do not wish to change the password, leave the fields blank and click **Next**).



NetCommWireless

Step 6 of 7

Router Security

In the next pages you will use the quick set-up guide to personalise your Router. Please enter a username and password to be used to gain access to your Router Management Console. It is recommended that you choose a unique password for added security.

Desired Username
admin

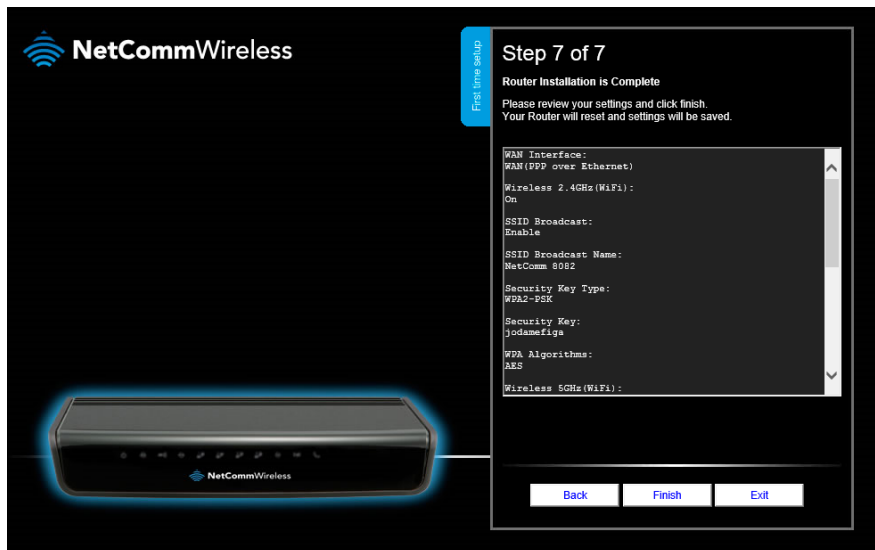
Desired Password
[]

Retype Password
[]

Remember to make a note of your username and password

Back Next Exit

- Confirm the setup information and click **Finish** if everything is correct. You can also click **Back** to go back and change any of the previously configured settings.



NetCommWireless

Step 7 of 7

Router Installation is Complete

Please review your settings and click finish. Your Router will reset and settings will be saved.

WAN Interface:
WAN (PPP over Ethernet)

Wireless 2.4GHz (WiFi):
On

SSID Broadcast:
Enable

SSID Broadcast Name:
NetComm 8082

Security Key Type:
WPA2-PSK

Security Key:
Jodamefiga

WPA Algorithms:
AES

Wireless 5GHz (WiFi):

Back Finish Exit









When you click Finish, the wizard applies your settings and the Advanced Status view is displayed. Your Dual Band WiFi Modem Router is ready to use.

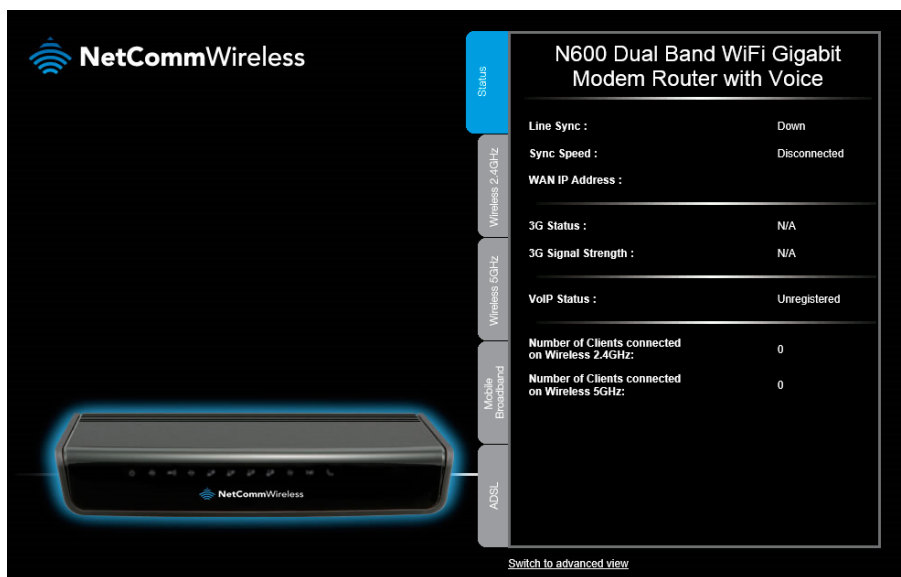
Basic View

When you log in to the router, the Basic View is displayed. Basic View gives you the most important information at a glance.

Status





The Status tab displays the following information:

-  ADSL Line Status
-  ADSL Sync Speed
-  The current WAN IP Address
-  3G Status
-  3G Signal Strength
-  VoIP Service Status (If configured)
-  Number of clients connected on Wireless 2.4GHz
-  Number of clients connected on Wireless 5GHz

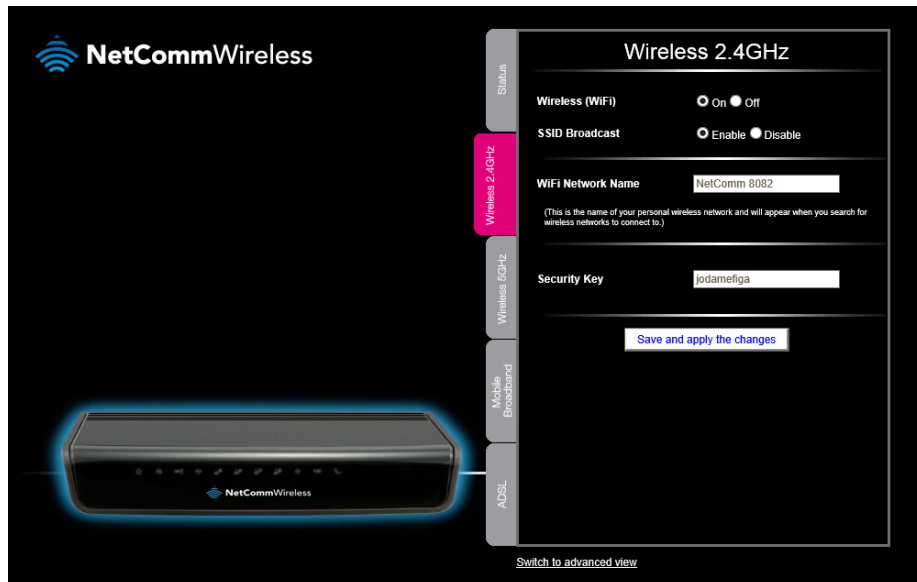


Wireless 2.4GHz

The wireless tab displays the following options for the 2.4GHz network:





-  Turn Wireless (WiFi) on or off
-  Turn SSID Broadcast on or off
-  Set the SSID (WiFi Network Name)
-  Set the Wireless Security Key

If you make any changes to the Wireless 2.4GHz configuration, Click the **Save and apply the changes** button to make these changes active.



Wireless 5GHz

The wireless tab displays the following options for the 5GHz network:







-  Turn Wireless (WiFi) on or off
-  Turn SSID Broadcast on or off
-  Set the SSID (WiFi Network Name)
-  Set the Wireless Security Key

If you make any changes to the Wireless 5GHz configuration, Click the **Save and apply the changes** button to make these changes active.



Mobile Broadband

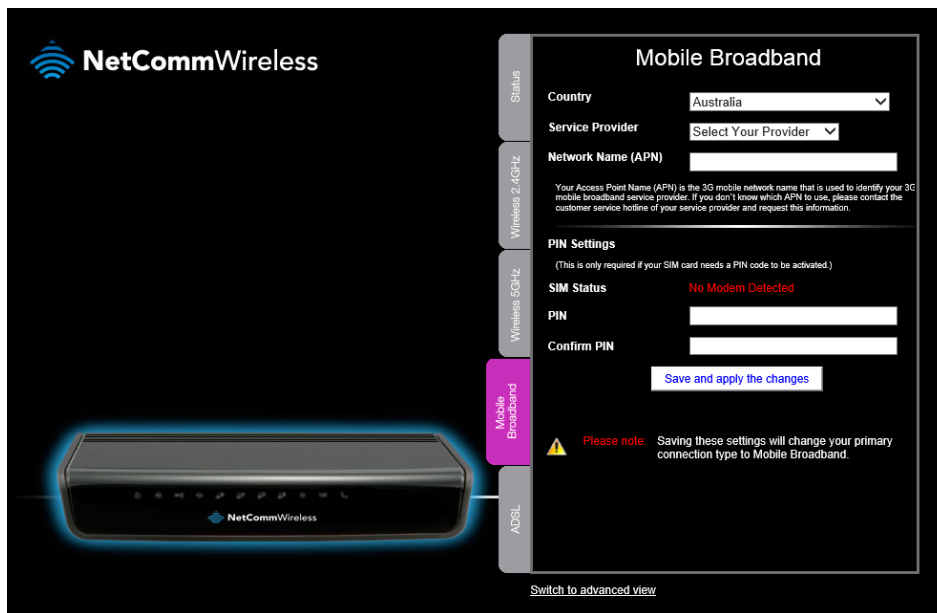
The following configuration options are available on the Mobile Broadband tab:

-  Country
-  Service Provider
-  Network Name (APN)
-  SIM Status
-  PIN
-  Confirm PIN

To configure your 3G/4G (Mobile Broadband) connection, select the applicable Country and Service Provider. The Network Name (APN) should be automatically filled with the correct APN. Please verify this with the information supplied by your 3G/4G provider.

The SIM Status will show if a PIN is required to use your SIM. If it is, enter the SIM PIN into the **PIN** and **Confirm PIN** fields.






If you make any changes to the 3G configuration, click the **Save and apply the changes** button to make these changes active.



Note: Saving any configuration changes on this page will make the Mobile Broadband connection the primary method of connecting to the Internet and disable other connection types. To enable Mobile broadband as a secondary failover, please configure Mobile Broadband in the Advanced View.



ADSL

The following configuration options are available on the ADSL tab:

-  Username
-  Password
-  Protocol
-  VPI Number
-  VCI Number

To configure your ADSL connection, enter the username and password as supplied by your ADSL service Provider.

Select the applicable protocol for your ADSL service. You can select from:

-  PPP over Ethernet (or PPPoE)
-  PPP over ATM (or PPPoA)

Enter the VPI Number (usually 8 for an ADSL service in Australia) and the VCI Number (usually 35 for an ADSL service in Australia) as supplied by your ADSL service Provider.

If you make any changes to the ADSL configuration, click the **Save and apply the changes** button to make these changes active.



NetCommWireless

ADSL Settings

ADSL Connection:
Please enter your ADSL authentication details supplied by your ISP into the fields below, and click **Save and apply the changes**

Username

Password

Protocol **PPP over Ethernet** ▼

VPI Number

VCI Number

Save and apply the changes

Please note: Saving these settings will change your primary connection type to ADSL (PPPoE and PPPoA).

[Switch to advanced view](#)

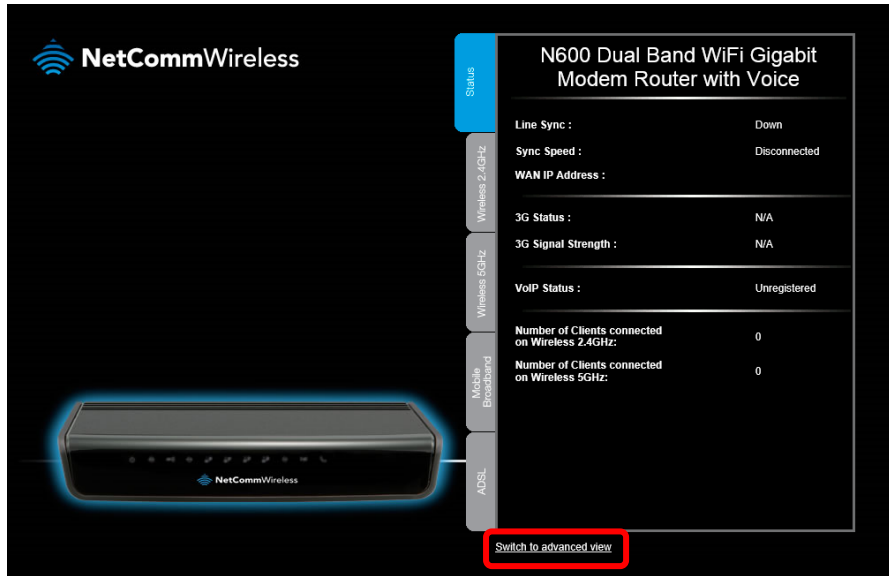


Note: Saving any configuration changes on this page will make the ADSL connection the primary method of connecting to the Internet and disable other connection types.

Advanced Configuration

To access the advanced configuration options of your NB16WW-02, you need to log in to the web configuration and change to Advanced view.

To do this, open your web browser (e.g. Internet Explorer/Firefox/Safari), type <http://192.168.20.1/> into the address bar at the top of the window and press the Enter key.




At the login screen, type **admin** in the Username and Password field and click the Login button.



Note: admin is the default username and password for the unit.

Click on the **Switch to Advanced View** link at the bottom of the page. The Advanced Status page is displayed.

Status

N600 Dual Band WiFi Gigabit Modem Router with Voice - NB16WW-02  [Switch to basic view](#)

Status [Network Setup](#) [Forwarding Rules](#) [Security Settings](#) [Advanced Settings](#) [VoIP Settings](#) [NAS Settings](#) [Toolbox](#)

Wireless 2.4GHz Status

Item	WLAN Status	Sidenote
Wireless 2.4GHz mode	Enable	(B/G/N Mixed)
SSID	NetComm 8082	
Channel	Auto	
Security	WPA2-PSK	(AES)
MAC Address		00:60:64:9E:AC:E2

Wireless 5GHz Status

Item	WLAN Status	Sidenote
Wireless 5GHz mode	Enable	(A/N Mixed)
SSID	NetComm 5866	
Channel	Auto	
Security	WPA2-PSK	(AES)
MAC Address		00:60:64:9E:AC:E3

VoIP Status

Item	Status	Sidenote
VoIP	Unregistered	Interface: PVC0

Statistics Information

Statistics of WAN	Inbound	Outbound
Octets	0	0
Unicast packets	0	0
Multicast packets	0	0

[ADSL Modem Status](#) [View Log...](#) [Clients List...](#) [NAT Status...](#) [Refresh](#)
 Device Time: Wed, 06 May 2015 11:29:35 +1000

ITEM	DESCRIPTION
Wireless 2.4GHz Status	
Wireless 2.4GHz mode	The status of the 2.4GHz wireless radio.
SSID	The SSID of the 2.4GHz wireless network.
Channel	The channel number in use by the 2.4GHz radio.
Security	The form of authentication in use on the router for the 2.4GHz wireless network. Side note shows the encryption method used.
MAC Address	The unique identifier assigned to your 2.4GHz wireless interface.
Wireless 5GHz Status	
Wireless 5GHz mode	The status of the 5GHz wireless radio.
SSID	The SSID of the 5GHz wireless network.
Channel	The channel number in use by the 5GHz radio.
Security	The form of authentication in use on the router for the 5GHz wireless network. Side note shows the encryption method used.
MAC Address	The unique identifier assigned to your 5GHz wireless interface.
VoIP Status	
VoIP	The registration status of the VoIP function. Side note indicates the interface that VoIP is currently assigned to.
Statistics Information	
Octets	The number of data bytes which have passed into and out of the router.
Unicast packets	The number of unicast packets which have passed into and out of the router.
Multicast packets	The number of multicast packets which have passed into and out of the router.

Network Setup

Network Setup

This page allows you to configure the ADSL, Mobile Broadband and Ethernet WAN (Wide Area Network) connection settings on the NB16WW-02.

ADSL

Ethernet over ATM (RFC1483 bridged) with NAT

Item	Setting
WAN Interface	ADSL <input type="button" value="▼"/> PVC0 <input type="button" value="▼"/> <input type="radio"/> Active <input checked="" type="radio"/> Inactive <input type="button" value="PVCs Summary"/>
WAN Type	Ethernet Over ATM (RFC 1483 Bridged) with NAT <input type="button" value="▼"/>
Remote Host for keep alive	<input type="text"/>
IP Mode	Dynamic IP Address <input type="button" value="▼"/>
Host Name	<input type="text"/> (optional)
ISP registered MAC Address	<input type="text"/> <input type="button" value="Clone"/>
NAT	<input checked="" type="checkbox"/> Enable
Data Encapsulation	VCmux <input type="button" value="▼"/>
VPI Number	0 <input type="text"/> (range: 0~255)
VCI Number	100 <input type="text"/> (range: 1~65535)
Schedule type	UBR <input type="button" value="▼"/>
Multicast	Disable <input type="button" value="▼"/>
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable 1 <input type="text"/> (range: 1~4094)

OPTION	DEFINITION
WAN Interface	The interface to configure. When ADSL is selected you may select a permanent virtual circuit (PVC) from 0 to 7.
WAN Type	The type of ADSL connection to use.
Remote Host for keep alive	A host name to use for the keep alive function. This host will be used to send a ping request in order to keep the connection alive.
IP Mode	Select to use either a static or dynamically assigned IP address for your connection. When selecting to utilise a static IP address, you will also need to enter the WAN IP Address, WAN Subnet Mask and WAN Default gateway in use for the connection <i>(Refer to your ISP for more information).</i>
Host Name	Set the hostname for your connection <i>(Optional - Refer to your ISP for more information).</i>
ISP Registered MAC Address	You can change the WAN port MAC address if needed to clone your 3G modem <i>(Optional - Refer to your ISP for more information).</i>
NAT	This option enables or disables "Network Address Translation" for this connection type.
Data Encapsulation	Select the Data Encapsulation required by your ISP <i>(Refer to your ISP for more information).</i>
VPI Number	Enter the VPI provided by your ISP <i>(This will usually be 8 for Australia or 0 for New Zealand)</i>
VCI Number	Enter the VCI provided by your ISP <i>(This will usually be 35 for Australia or 100 for New Zealand)</i>
Schedule Type	Select the data schedule type required by your ISP <i>(Refer to your ISP for more information).</i>
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.

IP over ATM (RFC1483 routed)

Item	Setting
WAN Interface	ADSL <input type="button" value="▼"/> PVC0 <input type="button" value="▼"/> <input type="radio"/> Active <input checked="" type="radio"/> Inactive <input type="button" value="PVCs Summary"/>
WAN Type	IP over ATM (RFC 1483 Routed) <input type="button" value="▼"/>
Remote Host for keep alive	<input type="text"/>
IP Mode	Dynamic IP Address <input type="button" value="▼"/>
Host Name	<input type="text"/> (optional)
ISP registered MAC Address	<input type="text"/> <input type="button" value="Clone"/>
NAT	<input checked="" type="checkbox"/> Enable
Data Encapsulation	VCmux <input type="button" value="▼"/>
VPI Number	0 <input type="text"/> (range: 0~255)
VCI Number	100 <input type="text"/> (range: 1~65535)
Schedule type	UBR <input type="button" value="▼"/>
Multicast	Disable <input type="button" value="▼"/>
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable <input type="text" value="1"/> (range: 1~4094)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
WAN Interface	The interface to configure. When ADSL is selected you may select a permanent virtual circuit (PVC) from 0 to 7.
WAN Type	The type of ADSL connection to use.
Remote Host for keep alive	A host name to use for the keep alive function. This host will be used to send a ping request in order to keep the connection alive.
IP Mode	Select to use either a static or dynamically assigned IP address for your connection. When selecting to utilise a static IP address, you will also need to enter the WAN IP Address, WAN Subnet Mask and WAN Default gateway in use for the connection <i>(Refer to your ISP for more information).</i>
Host Name	Set the hostname for your connection <i>(Optional - Refer to your ISP for more information).</i>
ISP Registered MAC Address	You can change the WAN port MAC address if needed to clone your 3G modem <i>(Optional - Refer to your ISP for more information).</i>
NAT	This option enables or disables "Network Address Translation" for this connection type.
Data Encapsulation	Select the Data Encapsulation required by your ISP <i>(Refer to your ISP for more information).</i>
VPI Number	Enter the VPI provided by your ISP <i>(This will usually be 8 for Australia or 0 for New Zealand)</i>
VCI Number	Enter the VCI provided by your ISP <i>(This will usually be 35 for Australia or 100 for New Zealand)</i>
Schedule Type	Select the data schedule type required by your ISP <i>(Refer to your ISP for more information).</i>
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.

PPP over Ethernet

Item	Setting
WAN Interface	ADSL <input type="button" value="▼"/> PVC0 <input type="button" value="▼"/> <input type="radio"/> Active <input checked="" type="radio"/> Inactive <input type="button" value="PVCs Summary"/>
WAN Type	PPP over Ethernet <input type="button" value="▼"/>
Remote Host for keep alive	<input type="text"/>
IPv6 Dualstack	<input type="checkbox"/> Enable
Username	<input type="text"/>
Password	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Service Name	<input type="text"/> (optional)
Assigned IP Address	<input type="text"/> (optional)
MTU	0 <input type="text"/> (0 is auto)
NAT	<input checked="" type="checkbox"/> Enable
Data Encapsulation	LLC <input type="button" value="▼"/>
VPI Number	8 <input type="text"/> (range: 0~255)
VCI Number	35 <input type="text"/> (range: 1~65535)
Schedule type	UBR <input type="button" value="▼"/>
Multicast	Disable <input type="button" value="▼"/>
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable 1 <input type="text"/> (range: 1~4094)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
WAN Interface	The interface to configure. When ADSL is selected you may select a permanent virtual circuit (PVC) from 0 to 7.
WAN Type	The type of ADSL connection to use.
Remote Host for keep alive	A host name to use for the keep alive function. This host will be used to send a ping request in order to keep the connection alive.
IPv6 Dualstack	Enables IPv6 Dual stack which allows IPv4 and IPv6 to run side-by-side without encapsulating one protocol within the other.
Username	The account name given to you by your ISP.
Password	The password given to you by your ISP. <i>(For security, this field appears blank. If you don't want to change the password, leave it empty)</i>
Primary DNS	This feature allows you to manually assign a Primary DNS Server <i>(Optional - Refer to your ISP for more information).</i>
Secondary DNS	This feature allows you to manually assign a Secondary DNS Server <i>(Optional - Refer to your ISP for more information).</i>
Service Name	Enter the service name if your ISP requires it <i>(Optional - Refer to your ISP for more information).</i>
Assigned IP Address	Enter the IP address assigned to your service. This is usually left blank.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
NAT	This option enables or disables "Network Address Translation" for this connection type.
Data Encapsulation	Select the Data Encapsulation required by your ISP <i>(Refer to your ISP for more information).</i>
VPI Number	Enter the VPI provided by your ISP <i>(This will usually be 8 for Australia or 0 for New Zealand)</i>
VCI Number	Enter the VCI provided by your ISP <i>(This will usually be 35 for Australia or 100 for New Zealand)</i>
Schedule Type	Select the data schedule type required by your ISP <i>(Refer to your ISP for more information).</i>
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.

[PPP over ATM](#)

Item	Setting
WAN Interface	ADSL <input type="button" value="v"/> PVC0 <input type="radio"/> Active <input checked="" type="radio"/> Inactive <input type="button" value="PVCs Summary"/>
WAN Type	PPP over ATM <input type="button" value="v"/>
Remote Host for keep alive	<input type="text"/>
IPv6 Dualstack	<input type="checkbox"/> Enable
Username	<input type="text"/>
Password	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Service Name	<input type="text"/> (optional)
Assigned IP Address	<input type="text"/> (optional)
MTU	0 (0 is auto)
NAT	<input checked="" type="checkbox"/> Enable
Data Encapsulation	VCMux <input type="button" value="v"/>
VPI Number	0 (range: 0~255)
VCI Number	100 (range: 1~65535)
Schedule type	UBR <input type="button" value="v"/>
Multicast	Disable <input type="button" value="v"/>
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable 1 (range: 1~4094)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
WAN Interface	The interface to configure. When ADSL is selected you may select a permanent virtual circuit (PVC) from 0 to 7.
WAN Type	The type of ADSL connection to use.
Remote Host for keep alive	A host name to use for the keep alive function. This host will be used to send a ping request in order to keep the connection alive.
IPv6 Dualstack	Enables IPv6 Dual stack which allows IPv4 and IPv6 to run side-by-side without encapsulating one protocol within the other.
Username	The account name given to you by your ISP.
Password	The password given to you by your ISP. <i>(For security, this field appears blank. If you don't want to change the password, leave it empty)</i>
Primary DNS	This feature allows you to manually assign a Primary DNS Server <i>(Optional - Refer to your ISP for more information).</i>
Secondary DNS	This feature allows you to manually assign a Secondary DNS Server <i>(Optional - Refer to your ISP for more information).</i>
Service Name	Enter the service name if your ISP requires it <i>(Optional - Refer to your ISP for more information).</i>
Assigned IP Address	Enter the IP address assigned to your service. This is usually left blank.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
NAT	This option enables or disables "Network Address Translation" for this connection type.
Data Encapsulation	Select the Data Encapsulation required by your ISP <i>(Refer to your ISP for more information).</i>
VPI Number	Enter the VPI provided by your ISP <i>(This will usually be 8 for Australia or 0 for New Zealand)</i>
VCI Number	Enter the VCI provided by your ISP <i>(This will usually be 35 for Australia or 100 for New Zealand)</i>
Schedule Type	Select the data schedule type required by your ISP <i>(Refer to your ISP for more information).</i>
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.

RFC 1483 Bridged

Item	Setting
WAN Interface	ADSL <input type="checkbox"/> PVC0 <input type="checkbox"/> Active <input checked="" type="radio"/> Inactive <input type="button" value="PVCs Summary"/>
WAN Type	RFC 1483 Bridged <input type="button" value="v"/>
Remote Host for keep alive	<input type="text"/>
Data Encapsulation	VCMux <input type="button" value="v"/>
VPI Number	<input type="text" value="0"/> (range: 0~255)
VCI Number	<input type="text" value="100"/> (range: 1~65535)
Schedule type	UBR <input type="button" value="v"/>
Multicast	Disable <input type="button" value="v"/>
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable <input type="text" value="1"/> (range: 1~4094)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

Mobile Broadband

Item	Setting
WAN Interface	Mobile Broadband <input type="radio"/> Active <input checked="" type="radio"/> Inactive
Country	Australia
Service Provider	Select Your Provider
APN	<input type="text"/>
PIN Code	<input type="text"/> (optional)
Dial Number	<input type="text"/>
Username	<input type="text"/> (optional)
Password	<input type="text"/> (optional)
Authentication Type	<input checked="" type="radio"/> Auto <input type="radio"/> PAP <input type="radio"/> CHAP
Primary DNS	<input type="text"/> (optional)
Secondary DNS	<input type="text"/> (optional)
Allowed Connection Time	<input checked="" type="radio"/> Always <input type="radio"/> By Schedule
MTU	1500 (0 is auto)
Keep Alive	<input checked="" type="radio"/> Disable <input type="radio"/> LCP Echo Request Interval <input type="text" value="10"/> seconds Max. Failure Time <input type="text" value="3"/> times <input type="radio"/> Ping Remote Host Host IP <input type="text"/> Interval <input type="text" value="60"/> seconds
Multicast	Disable
IGMP Snooping	<input type="checkbox"/> Enable

OPTION	DEFINITION
WAN Interface	The interface to configure. When Mobile Broadband is selected, you may also configure whether the connection is active or inactive.
Country	Select your country from the list. This will shorten the APN list to those in your selected country.
Service Provider	Select your mobile broadband service provider from the list. This will then enable you to select the correct APN for the mobile broadband service in use.
APN	Enter the APN for your mobile broadband service. This should be automatically filled in after selecting your country and 3G provider name. If the wrong APN is shown, enter the correct APN for your mobile broadband service
PIN Code	Enter the Pin Code for your SIM card (if required).
Dial Number	This number is required to connect to your mobile broadband service. <i>(Unless advised otherwise by NetComm Wireless Technical Support, this setting should not be changed)</i>
Username	The username provided by your mobile broadband service provider to enable access to your mobile broadband service.
Password	The password provided by your mobile broadband service provider to enable access to your mobile broadband service.
Authentication Type	Choose the appropriate authentication type for your mobile broadband service.
Primary DNS	Manually assign a Primary DNS Server.
Secondary DNS	Manually assign a Secondary DNS Server.
Allowed Connection Time	This setting enables you to configure when the mobile broadband connection may be active. By default it is set to "Always". If you select "By Schedule" you can select a schedule rule or create a new one. See the next page for details on creating a schedule rule.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
Keep Alive	There are three keep alive options to select from: <ul style="list-style-type: none"> ▪ Disable: Disable the keep alive function. ▪ LCP Echo Request: The NB16WW-02 will automatically verify the connection is active. Set the interval and Max number of failures to determine when the connection is up or down. ▪ Ping Remote Host: The NB16WW-02 will ping the chosen host IP to verify the connection is active. Set the host IP address and the interval between ping tests.
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.

Creating a connection schedule for Mobile Broadband

To create a new schedule rule:

1. Select the **By Schedule** option then click the **Add New Schedule** button.

Allowed Connection Time	<input type="radio"/> Always <input checked="" type="radio"/> By Schedule Schedule Rule# Add New Rule... Add New Schedule...
-------------------------	---





The schedule creation window appears.

Item		Setting	
Name of Rule 1		<input type="text" value="Demonstration Rule"/>	
Policy		<input type="text" value="Inactivate"/> except the selected days and hours below.	
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	<input type="text" value="Monday"/>	<input type="text" value="09:00"/>	<input type="text" value="17:00"/>
2	<input type="text" value="Tuesday"/>	<input type="text" value="09:00"/>	<input type="text" value="17:00"/>
3	<input type="text" value="Wednesday"/>	<input type="text" value="09:00"/>	<input type="text" value="17:00"/>
4	<input type="text" value="Thursday"/>	<input type="text" value="09:00"/>	<input type="text" value="17:00"/>
5	<input type="text" value="Friday"/>	<input type="text" value="09:00"/>	<input type="text" value="17:00"/>
6	<input type="text" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
7	<input type="text" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
8	<input type="text" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Close"/>			

2. Enter a name for the rule in the **Name of Rule 1** field.
3. Using the **Policy** drop down list, select whether the connection should be **Active** or **Inactive** except for the selected days and hours below. This is the default behaviour of the connection for the times not specified.
4. In the **Week Day** column, use the drop down lists to select a day of the week for which to create a schedule and in the **Start Time (hh:mm)** and **End Time (hh:mm)** fields, enter the time in 24 hour format for the schedule to apply.
5. Repeat step 4 for each day a rule is to be created.
6. Click the **Save** button.

Ethernet WAN

WAN Type: You can select from the following WAN types:-

-  Dynamic IP
-  Static IP
-  PPP over Ethernet
-  PPTP
-  L2TP

Dynamic IP Address

Item	Setting
WAN Interface	Ethernet WAN <input type="radio"/> Active <input checked="" type="radio"/> Inactive
WAN Type	Dynamic IP Address
Remote Host for keep alive	<input type="text"/>
Host Name	<input type="text"/> (optional)
ISP registered MAC Address	<input type="text"/> <input type="button" value="Clone"/>
NAT	<input checked="" type="checkbox"/> Enable
Multicast	Disable
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable <input type="text" value="3"/> (range: 1~4094)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
WAN Interface	The interface to configure. When Mobile Broadband is selected, you may also configure whether the connection is active or inactive.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
Remote Host for keep alive	A host name to use for the keep alive function. This host will be used to send a ping request in order to keep the connection alive.
Host Name	Set the hostname for your connection (Optional - Refer to your ISP for more information).
ISP Registered MAC Address	You can change the WAN port MAC address if needed to clone your 3G modem (Optional - Refer to your ISP for more information).
NAT	This option enables or disables "Network Address Translation" for this connection type.
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.

Static IP Address

Item	Setting
WAN Interface	Ethernet WAN <input type="radio"/> Active <input checked="" type="radio"/> Inactive
WAN Type	Static IP Address
Remote Host for keep alive	<input type="text"/>
WAN IP Address	<input type="text"/>
WAN Subnet Mask	<input type="text"/>
WAN Gateway	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
NAT	<input checked="" type="checkbox"/> Enable
Multicast	Disable
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable <input type="text" value="3"/> (range: 1~4094)

OPTION	DEFINITION
WAN Interface	The interface to configure. When Mobile Broadband is selected, you may also configure whether the connection is active or inactive.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
Remote Host for keep alive	A host name to use for the keep alive function. This host will be used to send a ping request in order to keep the connection alive.
WAN IP Address	The static IP address assigned to you by your internet service provider.
WAN Subnet Mask	The subnet mask of the IP address assigned to you by your internet service provider.
WAN Gateway	The WAN Gateway provided to you by your internet service provider.
Primary DNS	This feature allows you to manually assign a Primary DNS Server <i>(Optional - Refer to your ISP for more information).</i>
Secondary DNS	This feature allows you to manually assign a Secondary DNS Server <i>(Optional - Refer to your ISP for more information).</i>
NAT	This option enables or disables "Network Address Translation" for this connection type.
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.

PPP over Ethernet

Item	Setting
WAN Interface	Ethernet WAN <input type="radio"/> Active <input checked="" type="radio"/> Inactive
WAN Type	PPP over Ethernet
Remote Host for keep alive	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Service Name	<input type="text"/> (optional)
Assigned IP Address	<input type="text"/> (optional)
MTU	<input type="text" value="0"/> (0 is auto)
NAT	<input checked="" type="checkbox"/> Enable
Multicast	Disable
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable <input type="text" value="3"/> (range: 1-4094)

OPTION	DEFINITION
WAN Interface	The interface to configure. When Mobile Broadband is selected, you may also configure whether the connection is active or inactive.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
Remote Host for keep alive	A host name to use for the keep alive function. This host will be used to send a ping request in order to keep the connection alive.
Username	The account name given to you by your ISP.
Password	The password given to you by your ISP.
Primary DNS	This feature allows you to manually assign a Primary DNS Server <i>(Optional - Refer to your ISP for more information).</i>
Secondary DNS	This feature allows you to manually assign a Secondary DNS Server <i>(Optional - Refer to your ISP for more information).</i>
Service Name	Enter the service name if your ISP requires it <i>(Optional - Refer to your ISP for more information).</i>
Assigned IP Address	Enter the IP address assigned to your service. This is usually left blank.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
NAT	This option enables or disables "Network Address Translation" for this connection type
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.

PPTP

Item	Setting
WAN Interface	Ethernet WAN <input type="radio"/> Active <input checked="" type="radio"/> Inactive
WAN Type	PPTP
Remote Host for keep alive	<input type="text"/>
IP Mode	Dynamic IP Address
Server IP Address/Name	<input type="text"/>
PPTP Account	<input type="text"/>
PPTP Password	<input type="text"/>
Connection ID	<input type="text"/> (optional)
MTU	0 (0 is auto)
MPPE	<input type="checkbox"/> Enable
Multicast	Disable
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable <input type="text" value="3"/> (range: 1~4094)

OPTION	DEFINITION
WAN Interface	The interface to configure. When Mobile Broadband is selected, you may also configure whether the connection is active or inactive.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
Remote Host for keep alive	A host name to use for the keep alive function. This host will be used to send a ping request in order to keep the connection alive.
IP Mode	Select to use either a static or dynamically assigned IP address for your connection. When selecting to utilise a static IP address, you will also need to enter the PPTP IP Address, PPTP Subnet Mask and PPTP Default gateway in use for the connection <i>(Refer to your PPTP administrator for more information).</i>
Server IP Address/Name	Enter the PPTP server name or IP Address.
PPTP Account	Enter the PPTP username supplied by your PPTP administrator.
PPTP Password	Enter the PPTP password supplied by your PPTP administrator.
Connection ID	Enter an Optional name to identify the PPTP connection.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
MPPE	Select to enable or disable the MPPE security extensions for the PPTP connection.
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.

L2TP

Item	Setting
WAN Interface	Ethernet WAN <input type="radio"/> Active <input checked="" type="radio"/> Inactive
WAN Type	L2TP
Remote Host for keep alive	<input type="text"/>
IP Mode	Dynamic IP Address
Server IP Address/Name	<input type="text"/>
L2TP Account	<input type="text"/>
L2TP Password	<input type="text"/>
MTU	0 (0 is auto)
MPPE	<input type="checkbox"/> Enable
Multicast	Disable
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable <input type="text" value="3"/> (range: 1-4094)

OPTION	DEFINITION
WAN Interface	The interface to configure. When Mobile Broadband is selected, you may also configure whether the connection is active or inactive.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
Remote Host for keep alive	A host name to use for the keep alive function. This host will be used to send a ping request in order to keep the connection alive.
IP Mode	Select to use either a static or dynamically assigned IP address for your connection. When selecting to utilise a static IP address, you will also need to enter the L2TP IP Address, L2TP Subnet Mask and L2TP Default gateway in use for the connection <i>(Refer to your PPTP administrator for more information).</i>
Server IP Address/Name	Enter the L2TP server name or IP Address.
L2TP Account	Enter the L2TP username supplied by your L2TP administrator.
L2TP Password	Enter the L2TP password supplied by your L2TP administrator.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
MPPE	Select to enable or disable the MPPE security extensions for the L2TP connection.
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which VLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.

DHCP Server

This page allows you to change the Dynamic Host Configuration Protocol (DHCP) server settings on the NB16WW-02. The DHCP Server enables computers or devices connecting to the NB16WW-02 to automatically obtain their network configuration settings. By default, the DHCP server is enabled.

The **LAN IP Address** and **Subnet Mask** fields offer the ability to configure the IP address of the router locally and the subnet mask.

Item	Setting
DHCP Server	DHCP <input type="radio"/> Disable <input checked="" type="radio"/> Enable
LAN IP Address	<input type="text" value="192.168.20.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
IP Pool Starting Address	<input type="text" value="100"/>
IP Pool Ending Address	<input type="text" value="200"/>
Lease Time	<input type="text" value="86400"/> Seconds
Domain Name	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Primary WINS	<input type="text"/>
Secondary WINS	<input type="text"/>
Gateway	<input type="text"/> (optional)

OPTION	DEFINITION
DHCP Server	Enable or disable the DHCP server.
LAN IP Address	The local IP address of the NB16WW-02. <i>(The computers on your network must use this IP address as their Default Gateway. You can change it if necessary.)</i>
Subnet Mask	Enter the subnet mask for use on the local network. This would usually be set to 255.255.255.0.
IP Pool Starting/Ending Address	Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool
Lease Time	Length of the DHCP lease time
Domain Name	Optional, this information will be passed to the client
Primary DNS	Optional, this information will be passed to the client
Secondary DNS	Optional, this information will be passed to the client
Primary WINS	Optional, this information will be passed to the client
Secondary WINS	Optional, this information will be passed to the client
Gateway	Optional, this information will be passed to the client

When you have finished configuring the DHCP Server settings, click **Save** to save your settings. If you want to cancel any changes you have made before saving them, click the **Undo** button.

Use the **Clients List** button to check the DHCP client list. The **Fixed Mapping** button allows you to map a specific IP address to a specific MAC address. The following pages describe these features in more detail.

DHCP Client List

This is the list of currently connected devices using DHCP.

DHCP Clients List					
IP Address	Host Name	MAC Address	Type	Lease Time	Select
192.168.20.2	Ethernet PC1	1A-2B-3C-4D-5E-6F	Wired	23:59:32	<input checked="" type="checkbox"/>

If you wish to assign permanent IP address for a particular DHCP client (or device), select the appropriate DHCP client by clicking in the "Select" box, and click on "Add to Fix Map Table". This will ensure the clients current IP address is reserved.

DHCP Fixed Mapping

DHCP Fixed Mapping allows you to reserve a specific IP address for a specific device.

DHCP clients -- select one -- ID --

ID	MAC Address	IP Address	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

The DHCP Server will reserve a specific IP for a device based on that device's unique MAC address.

You can enter a new fixed mapping by entering the MAC address of the device and the IP address you wish to allocate to it.

To locate your device's unique MAC address, please refer to your device's user manual.

Select the **Enable** checkbox to activate the DHCP fixed mapping entry.

Wireless 2.4GHz

The Wireless 2.4GHz page allows you to configure the options related to the 2.4GHz wireless network of the router.

Item	Setting
Wireless Module (2.4GHz)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID (SSID)	<input type="text" value="NetComm 3714"/>
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	<input type="text" value="Auto"/>
Wireless Mode	<input type="text" value="B/G/N mixed"/>
Authentication	<input type="text" value="WPA2-PSK"/>
802.1X	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Encryption	<input type="text" value="AES"/>
Pre-shared Key	<input type="text" value="Zulujuatile"/>

OPTION	DEFINITION
Wireless Module (2.4GHz)	Select to enable or disable the 2.4GHz Wireless network function of the NB16WV-02.
Network ID (SSID)	Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. <i>(Please refer to the included Wireless Security Card insert for your default SSID)</i>
SSID Broadcast	The router will broadcast the SSID so that wireless clients can find the wireless network.
Channel	The wireless radio channel in use by your network.
Wireless Mode	Choose B/G Mixed, B only, G only, and N only, G/N Mixed or B/G/N mixed. <i>(The factory default setting is B/G/N mixed)</i>
Authentication	<p>You may select from the following authentication types to secure your wireless network:</p> <ul style="list-style-type: none"> ▪ Open ▪ Shared ▪ Auto ▪ WPA ▪ WPA-PSK ▪ WPA2 ▪ WPA2-PSK ▪ WPA/WPA2 ▪ WPA-PSK/WPA2-PSK. <p>WPA-PSK/WPA2-PSK is a newer type of security. This type of security gives a more secure network compared to WEP. Use TKIP Encryption Type for WPA-PSK and AES for WPA2-PSK.</p> <p>Please enter the key in the "Pre-share Key". The key needs to be more than 8 characters and less than 63 characters. It can be any combination of letters and numbers.</p> <p><i>(Please refer to the included Wireless Security Card insert for your default WPA-PSK2 key)</i></p>
802.1X	When Authentication is set to Open , you can enable 802.1X which enables Extensible Authentication Protocol (EAP) over wired or wireless networks.
Encryption	Select the type of encryption for your network. These options vary depending on the type of Authentication selected.



Note: The configuration for WPA-PSK and WPA2-PSK is identical. Additionally, disabling SSID broadcast will not increase your WiFi network's security. Hidden SSID networks can be unmasked with specific network tools.

After configuring wireless security, you also need to configure your wireless adapter to use the same security settings before you can connect wirelessly. Not all wireless adapters support WPA-PSK/WPA2-PSK/WPA/WPA2 security. Please refer to your wireless adapter user guide for more information. (Many drivers for Window XP wireless network adapters do not support WPA2.) It is strongly recommended that you set up wireless security such as WPA2-PSK (when the wireless client supports WPA2) in order to secure your network.

Click **Save** to save these settings or click **Undo** to cancel.

Wireless 5GHz

The Wireless 5GHz page allows you to configure the options related to the 5GHz wireless network of the router.

Item	Setting
Wireless Module (5GHz)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID(SSID)	<input type="text" value="NetComm 2691"/>
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	<input type="text" value="Auto"/>
Wireless Mode	<input type="text" value="A/N mixed"/>
Authentication	<input type="text" value="WPA2-PSK"/>
802.1X	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Encryption	<input type="text" value="AES"/>
Pre-shared Key	<input type="text" value="qijixulifa"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting..."/> <input type="button" value="WPS Setup..."/> <input type="button" value="Wireless Client List..."/>	

OPTION	DEFINITION
Wireless Module (5GHz)	Select to enable or disable the 5GHz Wireless network function of the NB16WW-02.
Network ID (SSID)	Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. <i>(Please refer to the included Wireless Security Card insert for your default SSID)</i>
SSID Broadcast	The router will broadcast the SSID so that wireless clients can find the wireless network.
Channel	The wireless radio channel in use by your network.
Wireless Mode	Choose A only, N only or A/N Mixed. <i>(The factory default setting is A/N Mixed)</i>
Authentication	<p>You may select from the following authentication types to secure your wireless network:</p> <ul style="list-style-type: none"> ▪ Open ▪ Shared ▪ Auto ▪ WPA ▪ WPA-PSK ▪ WPA2 ▪ WPA2-PSK ▪ WPA/WPA2 ▪ WPA-PSK/WPA2-PSK. <p>WPA-PSK/WPA2-PSK is a newer type of security. This type of security gives a more secure network compared to WEP. Use TKIP Encryption Type for WPA-PSK and AES for WPA2-PSK.</p> <p>Please enter the key in the "Pre-share Key". The key needs to be more than 8 characters and less than 63 characters. It can be any combination of letters and numbers.</p> <p><i>(Please refer to the included Wireless Security Card insert for your default WPA-PSK2 key)</i></p>
802.1X	When Authentication is set to Open , you can enable 802.1X which enables Extensible Authentication Protocol (EAP) over wired or wireless networks.
Encryption	Select the type of encryption for your network. These options vary depending on the type of Authentication selected.



Note: Disabling SSID broadcast will not increase your WiFi network's security. Hidden SSID networks can be unmasked with specific network tools.

Change Password

This page allows you to change the NB16WW-02 web configuration password.

Item	Setting
Username	<input type="text" value="admin"/> (*Change this if you need to change Username.)
Old Password	<input type="password"/>
New Password	<input type="password"/>
Reconfirm	<input type="password"/>

Type in the old password (the factory default username and password is **admin**) and then type in the new password. Re-enter the new password in the **Reconfirm** field and click **Save**.

We recommend that you change your router's username and password for security reasons. You should record your new username and password for future reference. In the case that you forget your username or password, you can restore the router to the factory default settings via the reset button. This will restore the username and password to "admin", however all preconfigured settings will be lost.




Forwarding Rules

The Forwarding Rules page allows you to configure the port forwarding management on the router. Click on any of the menu items on the left to access the respective settings page.

Forwarding rules are a necessary feature as by default NAT (Network Address Translation) will automatically block incoming traffic from the Internet to the LAN unless a specific port mapping exists in the NAT translation table. Because of this, NAT provides a level of protection for computers that are connected to your LAN.

However this also creates a connectivity problem when you want to make LAN resources available to Internet clients. For example, to play network games or host network applications.

There are three ways to work around NAT and to enable certain LAN resources available from the Internet:

-  **Port Forwarding**
-  **Port Triggering**
-  **DMZ Host**

Port Forwarding

A virtual server is defined as a Service Port, and all requests to this port will be redirected to the computer specified by the Server IP.

Port Forwarding can also work with Scheduling Rules, and give you more flexibility on Access control.



Note: For further instructions on scheduling rules, please refer to the "Scheduling" section later in this guide

Well known services -- select one -- <input type="button" value="Copy to"/> ID -- <input type="button" value="v"/>						
Item		Setting				
Port Forwarding Mode		Single Mode <input type="button" value="v"/>				
ID	External Port	Server IP	Internal Port	Protocol	Enable	Use Rule#
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
11	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
12	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
13	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
14	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
15	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
16	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
17	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
18	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
19	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
20	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="button" value="v"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>						

For example, if you have an FTP server (the default port is 21 using TCP for FTP) at 192.168.1.10, a Web server (the port is 80 and 81) and an Authentication server (port 2008) at 192.168.20.40, and a VPN server (the default port is 1723 via UDP for PPTP VPN) at 192.168.20.60, then you would need to specify the following virtual server mappings:



Note: At any given time, only one IP address can be bound to a particular Service Port. Port range can be entered by separating the first and last port by a colon. (e.g. for port 8080 to port 8090 inclusive, enter 8080:8090)

ID	EXTERNAL PORT	SERVER IP	INTERNAL PORT	PROTOCOL	ENABLE	USE RULE#
1	21	192.168.1.10	21	TCP	✓	(0) Always
2	80:81	192.168.20.40	80:81	Both	✓	(0) Always
3	2008	192.168.20.40	2008	TCP	✓	(0) Always
3	1723	192.168.20.60	1723	UDP	✓	(0) Always

Click **Save** to save the settings or **Undo** to cancel.

Port Triggering

Some applications like online games, video conferencing and Internet telephony require multiple connections to the internet. As such, these applications cannot work with a pure NAT router such as the NB16WW-02.

Popular applications -- select one -- ID --

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

The Port Triggering feature allows some of these applications to work with this router.



Note: Please check if your application is compatible with port triggering first. If this fails to make the application work, try to configure that computer as the DMZ host instead. Each port can only be used by 1 host machine at a time. If the port is occupied by an existing host, port triggering/forwarding/DMZ for that port will not work.

(For further instructions on setting up a DMZ host, please refer to the “Miscellaneous” section below)

OPTION	DEFINITION
Trigger	The outbound port number that will be triggered by the application.
Incoming Ports	When the trigger packet is detected, the inbound packets sent to the specified port numbers will be allowed to pass through the firewall to the triggering host.
Enable	Select to enable or disable the configured special application entry.

Port triggering opens an incoming **port** when your computer is using a specified outgoing **port** for specific traffic.

The NB16WW-02 also provides predefined settings for some popular applications.

To use the predefined settings, select your application from the “**Popular applications**” drop down list, select an unused ID from the list and then click **Copy to**. The predefined settings will then be added to the list.

Click **Save** to save the settings or **Undo** to cancel.

Miscellaneous

A Demilitarized Zone (DMZ) Host is a computer without the protection of firewall. It allows that particular computer to be exposed to unrestricted 2-way communication to the internet. It is mostly used for Internet games, Video conferencing, Internet telephony and other special applications.

Universal Plug and Play (UPnP) allows UpnP enabled host computers to automatically edit port mapping allowing NAT traversal for the host's requesting applications.

Item	Setting	Enable
DMZ Mode	Single Mode ▾	
IP Address of DMZ Host	<input type="text"/>	<input type="checkbox"/>
UPnP setting		<input checked="" type="checkbox"/>

To enable DMZ, enter the IP address of the computer you want to be live on the internet and select the **Enable** option.



Note: This feature should be used only when required as it exposes the selected machine to the greater Internet without security.

If ports are used in port forwarding/triggering, traffic through these ports will be directed to the port forwarding/triggering host PC, not to the DMZ host.

OPTION	DEFINITION
DMZ Mode	Select from Single Mode or Multi Mode. Single Mode uses the currently active connection type for the DMZ host while Multi Mode allows you to specify which connection type should be placed in the DMZ.
IP Address of DMZ Host	Enter the IP address of the computer you wish to put in the DMZ.
UPnP Setting	The device supports UPnP. If enabled, UPnP capable LAN clients can automatically edit port mapping entries for its own applications.

Click **Save** to save the settings or **Undo** to cancel.

Security Settings

The Security Settings page allows you to configure the security management on the router such as Packet filters and MAC Control. The following pages describe the various security options available

Status

The Status page lists any currently configured filtering for the Outbound, Inbound and Domain filters.

Item	Status		
Outbound Filter	Disable		
Local Client	Only Deny Remote Host	Service	Working Time
Item	Status		
Inbound Filter	Disable		
Remote Host	Deny Remote Host to access	Service	Working Time
Item	Status		
Domain Filter	Disable		
Domain	Access		
All other Domains	Yes		
<input type="button" value="Refresh"/>			

Packet Filters

The Packet Filter enables you to control what packets are allowed to pass through the router. There are two types of packet filter, Outbound Packet Filter which applies to all outbound packets and the Inbound Packet Filter which only applies to packets that are destined for a LAN clients only.





Note: To ensure the filter is applied to the correct PC, you must first assign a fixed IP address to the intended LAN clients. Please refer to DHCP Fixed Mapping for instructions. For further instructions on setting up MAC Level Filtering, please refer to the "MAC Control" section below

Outbound Filter:




To enable an Outbound Filter, tick the **Enable** tick box at the top of the page.

Item		Setting		
Outbound Packet Filter		<input type="checkbox"/> Enable		
<input checked="" type="radio"/> Allow all data through the router except data that matches the specified rules. <input type="radio"/> Deny all data through the router except data that matches the specified rules.				
ID	Source IP	Destination IP : Ports	Enable	Use rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
<input type="button" value="First page"/> <input type="button" value="Previous page"/> <input type="button" value="Next page"/> <input type="button" value="Last page"/> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Inbound Filter..."/> <input type="button" value="MAC Level..."/>				

There are two types of filtering policies:

-  Allow all data traffic to pass except those that match the specified rules.
-  Deny all data traffic to pass except those that match the specified rules.

You can specify up to 48 filtering rules for each direction (Inbound or Outbound). For each rule you will need to define the following:

-  Source IP address
-  Source port
-  Destination IP address
-  Destination port
-  Protocol: TCP or UDP or both.
-  Use Schedule Rule#

For source or destination IP address, you can define a single IP address (192.168.1.1) or a range of IP addresses (192.168.1.100-192.168.20.200). Leaving these fields empty implies all IP addresses are matched.

For source or destination port, you can also define a single port (80) or a range of ports (1000-1999). Use the prefix "T" or "U" to specify either the TCP or UDP protocol e.g. T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. Leaving this field empty implies all ports are matched.

The Packet Filter also works with Scheduling Rules, and gives you more flexibility on Access control.



Note: For further instructions on scheduling rules, please refer to the "Scheduling" section later in this guide

Click **Save** to save the settings or **Undo** to cancel. [Inbound Filter](#)

To access the Inbound Packet Filter page, click on the **Inbound Filter** button on the bottom of the Outbound Filter page. All the settings on this page are the same as those for the Outbound Filter shown on the previous page.

Item		Setting		
Inbound Packet Filter		<input type="checkbox"/> Enable		
<input checked="" type="radio"/> Allow all data through the router except data that matches the specified rules. <input type="radio"/> Deny all data through the router except data that matches the specified rules.				
ID	Source IP	Destination IP : Ports	Enable	Use rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
<input type="button" value="First page"/> <input type="button" value="Previous page"/> <input type="button" value="Next page"/> <input type="button" value="Last page"/> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Outbound Filter..."/> <input type="button" value="MAC Level..."/>				

Click **Save** to save the settings or **Undo** to cancel.

Domain Filters

Domain Filters enable you to prevent users from accessing specific domain addresses.

To enable the Domain Filter, select the "Enable" tick box at the top of the page.

Item		Setting
Domain Filter		<input type="checkbox"/> Enable
Log DNS Query		<input type="checkbox"/> Enable
Privilege IP Addresses Range		From <input type="text"/> To <input type="text"/>

ID	Domain Suffix	Action	Enable
1	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
10	* (all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-

OPTION	DEFINITION
Domain Filter	Select to enable or disable domain filtering.
Log DNS Query	Enable this if you want to log when someone accesses filtered URLs.
Privilege IP Addresses Range	Set a group of computers that has unrestricted access to the internet.



Note: To enable a privileged IP address range, please first assign DHCP fixed mapping to the intended computer.

To set a Domain Filter, you need to specify the following:

OPTION	DEFINITION
Domain Suffix	Please type the suffix of the URL that needs to be restricted. For example, ".com", "xxx.com".
Action	The router action that you want when someone is accessing a URL that matches the specified domain suffix. Select Drop to block the access and/or select Log to log this access.
Enable	Select to enable the rule.

Click **Save** to save the settings or **Undo** to cancel.

URL Blocking

URL Blocking blocks LAN computers from connecting to a pre-defined website. The major difference between the Domain Filter and URL Blocking is that Domain Filtering requires you to input a suffix (e.g. xxx.com, yyy.net) while URL Blocking only requires you to input a keyword.

To enable URL Blocking, select the **Enable** option at the top of the page.

Item		Setting	
URL Blocking		<input type="checkbox"/> Enable	
ID	URL	Enable	
1	<input type="text"/>	<input type="checkbox"/>	
2	<input type="text"/>	<input type="checkbox"/>	
3	<input type="text"/>	<input type="checkbox"/>	
4	<input type="text"/>	<input type="checkbox"/>	
5	<input type="text"/>	<input type="checkbox"/>	
6	<input type="text"/>	<input type="checkbox"/>	
7	<input type="text"/>	<input type="checkbox"/>	
8	<input type="text"/>	<input type="checkbox"/>	
9	<input type="text"/>	<input type="checkbox"/>	
10	<input type="text"/>	<input type="checkbox"/>	
<input type="button" value="Save"/> <input type="button" value="Undo"/>			

To set a URL Blocking rule, you need to specify the following:

OPTION	DEFINITION
URL	If any part of the Website's URL matches the pre-defined word then the connection will be blocked. For example, you can use pre-defined word "sex" to block all websites if their URLs contain the pre-defined word "sex".
Enable	Tick to enable the rule.

Click **Save** to save the settings or **Undo** to cancel.

MAC Control (Access Control List)

MAC Control allows you to modify access rights for different users and restrict specific MAC address from associating with your NB16WW-02.

To enable MAC Address Control, select the **Enable** option at the top of the page.

Item	Setting		
MAC Address Control	<input type="checkbox"/> Enable		
<input type="checkbox"/> Connection control	Wireless and wired clients with C checked can connect to this device; and allow unspecified MAC addresses to connect.		
<input type="checkbox"/> Association control	Wireless clients with A checked can associate to the wireless LAN; and allow unspecified MAC addresses to associate.		
DHCP clients -- select one -- <input type="button" value="Copy to"/> ID -- <input type="button" value="ID"/>			
ID	MAC Address	C	A
1	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value=" << Previous"/> <input type="button" value=" Next >>"/> <input type="button" value=" Save"/> <input type="button" value=" Undo"/>			

Two types of MAC Control are available:

OPTION	DEFINITION
Connection control (C column)	Use this to control which clients (wired and wireless) can connect to the unit. If a client is denied access to connect to this device, it means the client cannot access the Internet or any other network resource/host. Choose to allow or deny clients with MAC addresses that are not in the list to connect to this device.
Association control (A column)	Check Association Control to control which wireless client can associate with the unit. If a client is denied access to associate with the unit, it means the client cannot send or receive any data via this device's WiFi. Choose to allow or deny the clients with MAC addresses that are not in the list to associate to the wireless LAN.



Note: Click the "Next Page" or the "Previous Page" buttons to see the entire list.



Note: The Media Access Control (MAC) address control list does not provide absolute control/security, MAC addresses can be changed from factory assigned value with certain tools, allowing impersonation of a specific network device. Also known as MAC spoofing.

Click **Save** to save the settings or **Undo** to cancel.

Miscellaneous

This page allows you to change various security settings on the unit.

Item	Setting	Enable
Administrator Time-out	<input type="text" value="300"/> seconds (enter 60 seconds or greater)	<input checked="" type="checkbox"/>
Remote Administration	<input type="text"/> / <input type="text"/> : <input type="text"/>	<input type="checkbox"/>
Discard PING from WAN side		<input checked="" type="checkbox"/>
DoS Attack Detection	<input type="checkbox"/> Log	<input checked="" type="checkbox"/>
Keep WAN in stealth mode		<input checked="" type="checkbox"/>

OPTION	DEFINITION
Administrator Time-out	The period of time with no activity in the web configuration page to logout automatically, untick to disable this feature.
Remote Administrator Host/Subnet:Port	Normally only Intranet users can browse the built-in web pages to perform administration tasks. This feature enables you to perform administration tasks from a remote host. If this feature is enabled, only the specified IP address can perform remote administration.
Discard PING from WAN side	When this feature is enabled, your router will not respond to ping requests from remote hosts.
DoS Attack Detection	When this feature is enabled, the router will detect and log where the DoS attack comes from on the Internet.
Keep WAN in stealth mode	When this feature is enabled, the router will not respond to port scans, making it less susceptible to discovery and attacks.



Note: If the specified IP address is 0.0.0.0, any host can connect to the router to perform administration tasks. You can also use a subnet mask (/nn) to specify a group of trusted IP addresses for example, "10.1.2.0/24".

When Remote Administration is enabled, the web server port will be shifted to default port 80.

To change the Remote Administration web server port, enter the desired port number to the last field.

Eg. Port 8080

 / :

Denial of Service (DoS) Attack Detection. When enabled, the router can detect the following (and more) DoS attack types:

-  SYN Attack
-  WinNuke
-  Port Scan
-  Ping of Death
-  Land Attack

Enable Log to record DoS attack details.

Click **Save** to save the settings or **Undo** to cancel.

Advanced Settings

The Advanced Settings page allows you to configure the advanced settings on the router such as the System log, Dynamic DNS and SNMP options.

Status

The Status page displays the current System time, and lists any configured Dynamic DNS (DDNS) accounts, any Static or Dynamic Routes added or any Quality of Service (QoS) rules in place.

Item	Status			
System Time	Thu, 01 Jan 2009 14:05:16 +1000			
Item	Status			
DDNS	Disable			
Provider	-			
Item	Status			
Dynamic Routing	Disable			
Static Routing	Disable			
Destination	Subnet Mask	Gateway	Hop	
Item	Status			
QoS Control	Disable			
Local Client	Remote Host	Service	Priority	Working Time
<input type="button" value="Refresh"/>				

System Log

This enables you to set up the system log features of the router. You can also choose to send the system log to a remote syslog server (via a UDP connection) or email a copy to a recipient.

Item	Setting	Enable
IP address for syslog server	<input type="text"/>	<input type="checkbox"/>
Email address to send syslog to		<input type="checkbox"/>
• SMTP Server : port	<input type="text"/> : <input type="text"/>	
• SMTP Username	<input type="text"/>	
• SMTP Password	<input type="text"/>	
• E-mail addresses	<input type="text"/>	
• E-mail subject	<input type="text"/>	

OPTION	DEFINITION
IP Address for remote System Logs (syslog)	The IP address of the syslog server where the system log data will be sent. Click the "Enable" checkbox to enable this function.
Email address to send syslog to	Click the "Enable" checkbox to enable this function.
SMTP Server : port	Enter the IP address or fully qualified domain name (FQDN) and port for the selected email server.
SMTP Username	The SMTP username required to send email <i>(if required)</i> .
SMTP Password	The SMTP password required to send email <i>(if required)</i> .
Email Addresses	Enter the email addresses to send a copy of the current syslog to.
Email Subject	Enter the email subject to show on any sent emails.
View Log...	View the current system log.
Email Log Now	Email the current syslog to the entered email addresses.

Dynamic DNS




The Dynamic DNS feature enables users to set a static domain name for their internet connection even when the ISP only provides a dynamic IP address.

By mapping the host name to the current public IP address of the router, users who want to connect to the router or any services behind the router from the internet can just use the Dynamic DNS hostname instead of the IP Address which might change every time the router connects to the Internet.

Before you can use a Dynamic DNS service, you need to register an account on one of the many supported Dynamic DNS providers such as DynDNS.org, TZO.com or dhs.org.

Item	Setting
DDNS	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Provider	<input type="text" value="DynDNS.org(Dynamic)"/>
Host Name	<input type="text"/>
Username / E-mail	<input type="text"/>
Password / Key	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

After registering the account, the Dynamic DNS provider will provide you with the following details:

-  Host Name
-  Username/Email
-  Password/Key

To enable the Dynamic DNS feature on the unit, select the **Enable** option, choose the appropriate Dynamic DNS Provider and enter the details supplied by your Dynamic DNS provider.

Click **Save** to save the settings or **Undo** to cancel.

QoS

Quality of Service (QoS) provides different priority to different users or data flows. It can also guarantee a certain level of performance.

Item	Setting
QoS	Disable ▾
WAN Interface	PVC0 ▾
QoS Mode	Smart-QoS ▾
Bandwidth of Upstream	<input type="text"/> Kbps (Kilobits per second)
Bandwidth of Downstream	<input type="text"/> Kbps (Kilobits per second)

Item	Select	Setting
Game	<input type="checkbox"/>	<input type="text"/> 0 %
Chat	<input type="checkbox"/>	<input type="text"/> 0 %
VoIP	<input type="checkbox"/>	<input type="text"/> 0 %
P2P	<input type="checkbox"/>	<input type="text"/> 0 %
Video	<input type="checkbox"/>	<input type="text"/> 0 %
Web	<input type="checkbox"/>	<input type="text"/> 0 %

OPTION	DEFINITION
QoS	Use the drop down list to Enable or Disable QoS.
WAN Interface	Use the drop down list to select the interface to which QoS should apply.
QoS Mode	Use the drop down list to select the type of QoS to apply. Smart-QoS lets the router decide on the best settings based on the types of service you select below and the percentage setting assigned to each type of service. Higher percentages give a higher quality of service for that service type.
Bandwidth of Upstream	Enter the upstream bandwidth in Kilobits per second of your connection so that the router can calculate the best QoS settings.
Bandwidth of Downstream	Enter the downstream bandwidth in Kilobits per second of your connection so that the router can calculate the best QoS settings.

The lower section of the screen lets you manually assign a percentage of bandwidth to the different service types. If you manually assign QoS, the total percentage must add up to 90%. The remaining 10% of bandwidth is reserved for other types of network traffic.

For advanced QoS configuration, use the **QoS Mode** drop down list to select **User-defined QoS Rule** to display the QoS rules table. Click the **Add A New Rule** button to configure a new QoS rule.

Item	Setting
Rule	<input checked="" type="checkbox"/> Enable
Class	IP ▾
Class Info - IP	<input type="text"/> ~ <input type="text"/>
Function	PRI ▾
Function data - Priority	<input type="text"/>
Direction	In ▾
Schedule	(0) Always ▾

OPTION	DEFINITION
Rule	Select to enable or disable the QoS rule.
Class	Select the class of traffic you would like to prioritise.
Class Info	Enter the range of IP addresses of the class.
Function	Select the function of the rule. You can select from Priority, Max Rate, Session, Drop, Log or Alert.
Function data - Priority	Enter a priority value from 1 to 6 with 1 being the highest.
Direction	Select the direction of traffic to prioritise. Available options include In, Out or Both.
Schedule	Select a schedule for the new rule to apply. Previously created schedules are visible here or you can select the rule to always apply.



Note: For further instructions on scheduling rules, please refer to the "Scheduling" section later in this guide

Click on **Save** to store your setting or **Undo** to discard your changes.

SNMP

SNMP (Simple Network Management Protocol) is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

Item	Setting
Enable SNMP	<input type="checkbox"/> Local <input type="checkbox"/> Remote
Get Community	<input type="text"/>
Set Community	<input type="text"/>
IP 1	<input type="text"/>
IP 2	<input type="text"/>
IP 3	<input type="text"/>
IP 4	<input type="text"/>
SNMP Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c
WAN Access IP Address	<input type="text"/>

OPTION	DEFINITION
Enable SNMP	You must check Local, Remote or both to enable SNMP function. If Local is checked, this device will only respond to requests from LAN connected hosts. If Remote is checked, this device will respond to requests from the WAN connection.
Get Community	Sets the community string your device will respond to for Read-Only access.
Set Community	Sets the community string your device will respond to for Read/Write access.
IP 1, IP 2, IP 3, IP 4	Input your SNMP Management host IP here. You will need to configure the address where the device should send SNMP Trap messages to.
SNMP Version	Please select proper SNMP Version that your SNMP Management software supports.
WAN Access IP Address	You can limit remote access to a specific IP address by entering it here.



Note: If "Remote" access is enabled, the default setting of 0.0.0.0 means any IP obtain SNMP protocol Information.

Click the **Save** button to store your setting or the **Undo** button to discard your changes.

Routing

Routing tables allow you to determine which physical interface address to use for outgoing IP data. If you have more than one router and subnet, you will need to configure the routing table to allow packets to find the proper routing path and allow different subnets to communicate with each other.

These settings are used to setup the static and dynamic routing features of the NB16WW-02.

Item		Setting				
Dynamic Routing		<input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2				
Static Routing		<input checked="" type="radio"/> Disable <input type="radio"/> Enable				
ID	Destination	Subnet Mask	Gateway	Hop	Enable	
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	
<input type="button" value="Save"/> <input type="button" value="Undo"/>						

Dynamic Routing:

Routing Information Protocol (RIP) will exchange information about different host destinations for working out routes throughout the network.



Note: Only select RIPv2 if you have a different subnet in your network. Otherwise, select RIPv1.

Static Routing:

For static routing, you can specify up to 8 routing rules.

You need to enter the **destination IP address**, **subnet mask**, **gateway**, and **hop** for each routing rule, then enable the rule by selecting the **Enable** checkbox.

Click the **Save** button to store your setting or the **Undo** button to discard your changes.

System Time

This page allows you to change the System time setting on the NB16WW-02.

Item	Setting															
Time Zone	(GMT+10:00) Canberra, Melbourne, Sydney															
Auto-Synchronization	<input checked="" type="checkbox"/> Enable Time Server (RFC-868): 0.netcomm.pool.ntp.org															
Enable Daylight Saving	<input checked="" type="radio"/> Disable <input type="radio"/> Enable															
Daylight Saving Dates	<table border="0"> <thead> <tr> <th></th> <th>Month</th> <th>Week</th> <th>Day of Week</th> <th>Time</th> </tr> </thead> <tbody> <tr> <td>DTS Start</td> <td>Jan</td> <td>1st</td> <td>Sun</td> <td>1am</td> </tr> <tr> <td>DTS End</td> <td>Jan</td> <td>1st</td> <td>Sun</td> <td>1am</td> </tr> </tbody> </table>		Month	Week	Day of Week	Time	DTS Start	Jan	1st	Sun	1am	DTS End	Jan	1st	Sun	1am
	Month	Week	Day of Week	Time												
DTS Start	Jan	1st	Sun	1am												
DTS End	Jan	1st	Sun	1am												
<input type="button" value="Save"/> <input type="button" value="Undo"/>																
<input type="button" value="Sync with Time Server"/> <input type="button" value="Sync with my PC (Wed April 24, 2013 10:13:55)"/>																

OPTION	DEFINITION
Time Zone	Select the time zone where this device is located.
Auto-Synchronization	Select the "Enable" checkbox to enable this function.
Enable Daylight Saving	Enables or disables the router's automatic daylight saving adjustment feature.
Daylight Savings Dates	Use the drop down lists to select a daylight saving start and end date and time.
Time Server	Select a NTP time server to obtain the current UTC time from.
Sync with Time Server	Select if you want to set Date and Time by NTP Protocol.
Sync with my PC	Select if you want to set Date and Time using your computers Date and Time

Click **Save** to save the settings or **Undo** to cancel.

Scheduling

You can use scheduling to enable or disable a service at a specific time or on a specific day.

Item		Setting
Schedule		<input type="checkbox"/> Enable
Rule#	Rule Name	Action
1		<input type="button" value="Add New"/>
2		<input type="button" value="Add New"/>
3		<input type="button" value="Add New"/>
4		<input type="button" value="Add New"/>
5		<input type="button" value="Add New"/>
6		<input type="button" value="Add New"/>
7		<input type="button" value="Add New"/>
8		<input type="button" value="Add New"/>
9		<input type="button" value="Add New"/>
10		<input type="button" value="Add New"/>

Select **Enable** and then click the **Add New Rule** button.

Item		Setting	
Name of Rule 1		<input type="text"/>	
Policy		<input type="button" value="Inactivate"/> on the selected days and hours below.	
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
2	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
3	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
4	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
5	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
6	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
7	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
8	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>

Select a name for the rule and enter the details such as the day, start time or end time and click the **Save** button

In the example below, the rule is called "Work Hours" and it is only active between 08:00 and 17:30.

You are then able to select the scheduling rule name specified from the Packet Filter configuration section to perform the configured filtering at the scheduled time as per the screenshot below.

Item		Setting	
Name of Rule 1		<input type="text" value="Work Hours"/>	
Policy		<input type="button" value="Activate"/> on the selected days and hours below.	
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	<input type="button" value="Every Day"/>	<input type="text" value="08:00"/>	<input type="text" value="17:30"/>

This example would prevent any access to the IP address 66.102.11.104 from any device connected to the router, 7 days a week, only between the hours of 08:00 and 17:30.

Click the **Save** button to save the settings or the **Undo** button to cancel.

IPv6

The IPv6 page enables you to configure the settings used for an IPv6 connection (if supported by your Internet Service Provider).

Item	Setting
IPv6	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
IPv6 Interface	ADSL ▾
IPv6 Connection	DHCPv6 ▾
DNS Setting	<input checked="" type="radio"/> Obtain DNS Server address Automatically <input type="radio"/> Use the following DNS address
Primary DNS Address	<input type="text"/>
Secondary DNS Address	<input type="text"/>
LAN IPv6 Address	<input type="text"/> /64
LAN IPv6 Link-Local Address	
Autoconfiguration	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Autoconfiguration Type	Stateless ▾
Router Advertisement Lifetime	<input type="text" value="200"/> Seconds
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
IPv6	Select to enable or disable IPv6 functionality.
IPv6 Interface	Configure IPv6 for the selected interface.
IPv6 Connection	Select the type of IPv6 connection to utilise for your service. You can select from: <ul style="list-style-type: none"> ▪ Static IPv6 ▪ DHCPv6 ▪ PPPoE ▪ 6 to 4 ▪ IPv6 in IPv4 Tunnel ▪ PPPoA Select the type of connection as required by your Internet Service Provider for their IPv6 service.
DNS Setting	Select whether to automatically obtain DNS Server addresses or use the ones you manually specified.
Primary DNS Address	Enter the Primary DNS Address for the IPv6 connection.
Secondary DNS Address	Enter the Secondary DNS Address for the IPv6 connection.
LAN IPv6 Address	The IP Address to use for the IPv6 LAN interface.
LAN IPv6 Link-Local Address	The current local LAN IPv6 address of the NB16WW-02.
Autoconfiguration	Select to enable or disable IPv6 auto configuration (if supported by your Internet Service Provider). Disable IPv6 /64 Prefix delegation.
Autoconfiguraion Type	Enabling Stateless or stateful IPv6, allowing defined IPv6 /64 addressing or automatic globally unique IPv6 address.
Router Advertisement Lifetime	Enter the length of time between the router advertising its configuration on the IPv6 connection.

TR-069

The TR-069 client allows the NB16WW-02 to be automatically configured from a TR-069 server. Enter the applicable configuration options to enable the router to contact the TR-069 server and retrieve any configuration options.

Item	Setting
TR-069	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
ACS URL	<input type="text"/>
ACS Username	<input type="text"/>
ACS Password	<input type="text"/>
Connection Request Port	<input type="text" value="8099"/>
Connection Request Username	<input type="text"/>
Connection Request Password	<input type="text"/>
Inform	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Interval	<input type="text" value="900"/> seconds

OPTION	DEFINITION
TR-069	Select to enable or disable the TR-069 automatic configuration function.
ACS URL	Enter the URL of the ACS server for automatic configuration.
ACS User Name	The username required to login to the ACS server.
ACS Password	The password required to login to the ACS server.
Connection Request Port	The port number the ACS server is running on.
Connection Request Username	The username to use when a connection request is made to the CPE.
Connection Request Password	The password to use when a connection request is made to the CPE.
Inform	Select to enable or disable the Inform function for ACS connections.
Interval	Select the interval between Inform updates if Inform has been enabled.

Click the **Save** button to store any changes to the settings.

VLAN

The VLAN page provides you with the ability to create Virtual Local Area Networks (VLANs). A VLAN is layer-2 network which has been partitioned to create multiple distinct broadcast domains. The purpose of this is to isolate packets so that they may only pass between these broadcast domains via one or more routers.

Ethernet	WAN/LAN	VID	Tx TAG	
Port1	LAN	<input type="text" value="1"/>	<input type="checkbox"/>	
Port2	LAN	<input type="text" value="1"/>	<input type="checkbox"/>	
Port3	LAN	<input type="text" value="1"/>	<input type="checkbox"/>	
Port4	LAN	<input type="text" value="1"/>	<input type="checkbox"/>	
Port5	LAN	<input type="text" value="1"/>	<input type="checkbox"/>	
VLAN ID on LAN	LAN/Wireless LAN(Interface)	Tag	Type	Internet or ISP map WAN(VLAN ID)
1	Port1, Port2, Port3, Port4, Port5	No	NAT	0

OPTION	DEFINITION
Ethernet	The number of the physical port on the rear of the router for which the VLAN will be created.
WAN/LAN	The function of the port. Port 1 only functions as a WAN port.
VID	The Virtual LAN ID you want to assign to the VLAN.
Tx TAG	Selecting this option will tag packet headers with the VLAN ID.

To adjust advanced WAN VLAN settings for a particular VID, click the **WAN VLAN Settings** button. The following window is displayed:

Item	Setting
VID	<input type="text" value="1"/>
Routing Type	<input type="text" value="NAT"/>
DHCP Setting	DHCP

OPTION	DEFINITION
VID	Use the drop down list to select the VID you want to configure.
Routing Type	Use the drop down list to type of routing for the selected VID.
DHCP Setting	Displays the current DHCP setting.

Setting **Routing Type** to **Bridge** displays further options:

Item	Setting
VID	<input type="text" value="1"/>
Routing Type	<input type="text" value="Bridge"/>
WAN type	<input type="text" value="Ethernet"/>
WAN Map VLAN ID	<input type="text" value="0"/> (0 is untag)

OPTION	DEFINITION
VID	Use the drop down list to select the VID you want to configure.
Routing Type	Use the drop down list to type of routing for the selected VID.
WAN type	Use the drop down list to select which WAN type the VLAN uses.
WAN Map VLAN ID	Enter the VLAN ID to tag packets on the WAN interface.

VoIP Settings

Configurations

Service Domain

The Service Domain page is where you enter your VoIP service settings as supplied by your VoIP service provider (VSP). If you are unsure about a specific setting or have not been supplied information for a particular field, please contact your VoIP service provider to verify if this setting is needed.

Service Domain Setting	
Item	Setting
WAN Interface	Ethernet WAN ▾
Item	Setting
Display Name	<input type="text"/>
Username	<input type="text"/>
Register Name	<input type="text"/>
Register Password	<input type="text"/>
Domain	<input type="text"/>
Registrar/Proxy Server	<input type="text"/>
Use Outbound Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Outbound Proxy	<input type="text"/>
Status	Unregistered
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
Display Name	Enter the display name for your VoIP service.
User Name	Enter the User Name for your VoIP service.
Register Name	Enter the Register Name (May be called the "Auth ID") for your VoIP service.
Register Password	Enter the Register Password (May be called the "Auth Password") for your VoIP service.
Domain	Enter the Domain for your VoIP service.
Registrar/Proxy Server	Enter the Registrar or Proxy Server address for your VoIP service.
Use Outbound Server	Enable or Disable the use of an Outbound Proxy for VOIP calls.
Outbound Proxy	Enter the Outbound Proxy server address to use.
Status	The current status of your VoIP service.

Click **Save** to save your settings and connect to your VoIP service or **Undo** to discard the settings entered.

Port Setting

The Port Setting page enables you to specify a different SIP or RTP Port number to connect to your VoIP service on

Port Setting	
Item	Setting
SIP Port	<input type="text" value="5060"/> (0~65533) if set 0,it will be assigned by the system.
RTP Port	<input type="text" value="5000"/> (0~65533) if set 0,it will be assigned by the system.

OPTION	DEFINITION
SIP Port	Select the port for SIP traffic to use.
RTP Port	Select the port for RTP traffic to use.

This setting should not need to be changed unless directed to do so. Please contact your VoIP service provider to verify the port number for their VoIP Service.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Codec Setting





The Codec Setting page enables you to select which audio codec to use with your VoIP service. This information will usually be supplied by your VoIP service provider and should not need to be changed unless you are experiencing issues with VoIP call sound quality.

Codec Setting	
Item	Setting
Codec Priority 1	<input type="text" value="G.711 a-law"/> ▼
Codec Priority 2	<input type="text" value="G.729"/> ▼
Codec Priority 3	<input type="text" value="G.726 - 32"/> ▼
Codec Priority 4	<input type="text" value="G.711 u-law"/> ▼

SIP Packet Length	
Item	Setting
SIP Packet Length (G.711 & G.729)	<input type="text" value="10 ms"/> ▼

Voice VAD	
Item	Setting
Voice VAD	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
The packet length for Comfort noise packet	<input type="text" value="30"/> ms(10~50ms)

The following codec are available for use:

-  G.729
-  G.711 a-law
-  G.711 u-law
-  G.726 -32

OPTION	DEFINITION
Codec Priority 1	Set the codec you would like to try first with your VoIP service.
Codec Priority 2	Set the codec you would like to try second with your VoIP service.
Codec Priority 3	Set the codec you would like to try third with your VoIP service.
Codec Priority 4	Set the codec you would like to try fourth with your VoIP service.
G.711 & G.729 Packet Length	Adjust the packet length size. This can reduce or increase the bandwidth required and call usability for a VoIP call.
Voice VAD	Adjust the 'Voice Activity Detection' interval. This should not be adjusted unless the words in your conversation are being cut off. (This setting should not need to be changed.)
The packet length for Comfort noise packet	Set the time in milliseconds for which comfort noise is used to simulate background noise at your end of the connection.

Click **Save** to save your settings or **Undo** to discard the settings entered.

DTMF Setting

The Dual-Tone Multi-Frequency signalling (DTMF) Setting page enables you to specify which DTMF standard to use on your VoIP service.

DTMF Setting	
Item	Setting
DTMF Setting	<input checked="" type="radio"/> RFC 2833 <input type="radio"/> Inband DTMF <input type="radio"/> Send DTMF SIP Info
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

The following DTMF standards are available for use:

-  RFC 2833
-  Inband DTMF
-  Send DTMF SIP Info

This information will usually be supplied by your VoIP service provider and should not need to be changed unless you are experiencing issues with DTMF based services
(Automated Telephone services, Answering machines, etc).

OPTION	DEFINITION
DTMF Setting	Select which DTMF standard you would like to use.

Click **Save** to save your settings or **Undo** to discard the settings entered.

STUN Settings

The STUN Settings page enables you to configure settings related to using a STUN server with your VoIP service. A STUN (Session Traversal Utilities for NAT) server is used to permit NAT traversal for applications of real-time voice, video, messaging and other interactive IP communications. This information will usually be supplied by your VoIP service provider and should not be needed unless you are experiencing issues with VoIP calls or signing into your VoIP service.

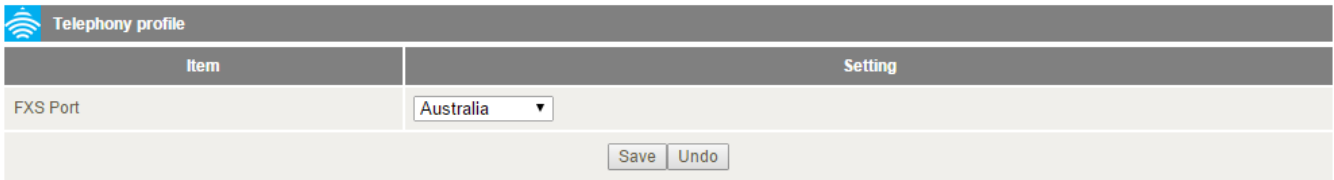
STUN Settings	
Item	Setting
SIP ALG	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
STUN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
STUN Server	<input type="text"/>
STUN Port	<input type="text"/> (80-65535)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
SIP ALG	A SIP Application Gateway provides functionality to allow VoIP traffic to pass both from the private the public and public to private side of the firewall when using network address translation (NAT).
STUN	Select to Enable or Disable the STUN server functionality of the NB16WV.
STUN Server	Enter the STUN Server address to use.
STUN Port	Enter the Port with which to connect to the STUN server on.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Telephony Profile

The Telephony Profile page enables you to configure the way the FXS phone port (RJ-11) operates.



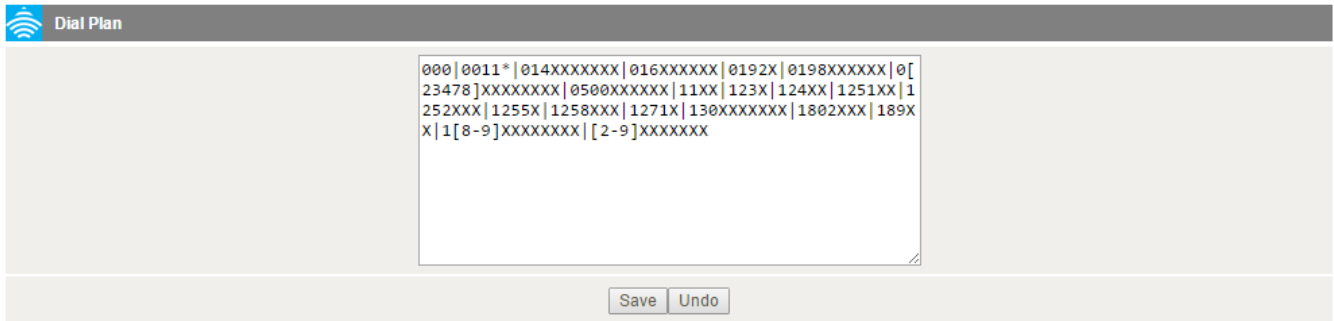
Use the drop down list to select the region closest to you to configure the FXS port operation.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Dial Plan

The Dial Plan page allows you to specify dial strings. When a dialled phone number matches a dial string, the number is dialled immediately instead of waiting for a timeout to occur.

The included default dial plan only applies to Australia. For your local dial plan, contact your VoIP service provider.



Dial plan syntax

TO SPECIFY A	ENTER THE FOLLOWING	RESULT
Separate string	(Pipe)	Separates one string from the next in the list
Digit	0 1 2 3 4 5 6 7 8 9	Identifies a specific digit (do not use #)
Range	[digit-digit]	Identifies a dialed digit within the range
Wild card	X	Matches any single digit that is dialed
Wild card	*	Matches an arbitrary number of digits
Timer	T	Indicates that an additional timeout period of 4 seconds should take place before automatic dialing starts.

Dial plan example

This dial plan may be used for Australia. You may copy and paste this string into the Dial Plan field on the user interface and click the **Save** button to use it.

```
000|0011*t|014XXXXXXXX|016XXXXXX|0192X|0198XXXXXX|0[23478]XXXXXXXX|0500XXXXXX|11XX|123X|124XX|1251XX|1252XXX|1255X|1258XXX|1271X|130XXXXXXX|13[1-9]XXX|1802XXX|189XX|1[8-9]XXXXXXXX|[2-9]XXXXXX|
```

OPTION	DEFINITION
000	Emergency number
0011*t	International number (After 0011, the unit allows an arbitrary number of digits and dials 4 seconds after the last digit was entered.)
0[23478]XXXXXXXX	Landline numbers with area code 02, 03, 04, 07, 08 + XXXX XXXX Mobile numbers with 04XX XXX XXX
1[8-9]XXXXXXXX	1800 and 1900 numbers
130XXXXXXXX	1300 numbers
13[1-9]XXX	13 numbers
[2-9]XXXXXX	Landline numbers without area code specified

Other Settings

The Other Settings page enables you to specify a different SIP expire time and select to enable the DNS SRV function. This information will usually be supplied by your VoIP service provider and should not need to be changed unless you are experiencing issues with VoIP calls or signing into your VoIP service.

Other Settings	
Item	Setting
SIP Expire Time	<input type="text" value="120"/> (15-86400 sec)
Use DNS SRV	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SIP ALG	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Rport	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
SIP Expire Time	Set the length of time between the NB16WV-02 refreshing its connection to your VoIP service provider
Use DNS SRV	Enable or Disable the DNS SRV function on the NB16WV-02.
SIP ALG	A SIP Application Gateway provides functionality to allow VoIP traffic to pass both from the private the public and public to private side of the firewall when using network address translation (NAT).
Rport	Rport allows a client to request that the server send the response back to the source IP address and port from which the request originated.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Call Features





The Call Features pages enable you to configure settings for features such as call waiting, call forwarding and caller ID.

Call Forward

The Call Forward page enables you to configure the type of call forwarding you would like to use and the SIP address to which any such calls should be forwarded.

Forward Setting	
Item	Setting
Type	<input type="radio"/> Always <input type="radio"/> Busy <input type="radio"/> No Answer <input checked="" type="radio"/> Disable
URL	<input type="text"/>
Call Forward Ring Time	<input type="text" value="10"/> (0~18)if set 0,it will be assigned by the system.
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

You can select from the following call forwarding conditions:

-  Always
-  Busy
-  No Answer
-  Disable

OPTION	DEFINITION
Type	Select the type of Call Forwarding you would like to use.
URL	Enter the address (Phone number) to forward VoIP calls to.
Call forwarding Ring time	Enter the amount of time the incoming call rings before call forwarding is activated.

Click **Save** to save your settings or **Undo** to discard the settings entered.

DND Setting

The DND Setting page enables you to configure Do Not Disturb (DND) mode. This will prevent calls coming through to your phone.

DND Setting	
Item	Setting
DND Always	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
DND Always	Enable or Disable the DND feature.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Caller ID

The Caller ID page enables you to configure whether your Caller ID is sent when receiving an inbound call.
(If supported by your VoIP service and phone caller ID service)




Item	Setting
Caller ID	Caller ID after 1st Ring (FSK) ▾
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
Caller ID	Select to use or Disable Caller ID.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Flash Time

The Flash Time page enables you to configure the minimum and maximum time a hook flash signal can occur for the NB16WW-02 to recognise it.


Flash Time Setting

Item	Setting
FXS Flash Signal Detect (MAX.)	<input type="text" value="1000"/> ms (100-1000)
FXS Flash Signal Detect (MIN.)	<input type="text" value="300"/> ms (100-300)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
FXS Flash Signal Detect (MAX)	Enter the maximum time (in milliseconds) to detect a hook flash.
FXS Flash Signal Detect (MIN)	Enter the minimum time (in milliseconds) to detect a hook flash.

This setting should not need to be changed unless directed to do so.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Call Waiting

The Call Waiting page enables you to utilise call waiting with your VoIP service.
(If supported by your VoIP service)

Call Waiting Setting	
Item	Setting
Call Waiting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
Call Waiting	Select to Enable or Disable the call waiting feature on the NB16WV.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Hot Line

The Hot Line page enables you to configure a telephone number which can be called without dialling any numbers at all (simply pick up the telephone handset) after the specified waiting time.

Hot Line Setting	
Item	Setting
Use Hot Line	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Hot Line Number	<input type="text"/>
Waiting time before starting Hot Line	<input type="text" value="3"/> second (1-9)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
Use Hot Line	Select to Enable or Disable the Hot Line feature of the NB16WV-02.
Hot Line Number	Enter the number to forward Hot Line calls to.
Waiting time before starting Hot Line	Enter the amount of time to wait before forwarding a call to the Hot Line number.

Click **Save** to save your settings or **Undo** to discard the settings entered.










Call Features

The Call Features page enables you to configure the dialling codes used to activate or deactivate features on your VoIP service via your handset number pad.

(If supported by your VoIP Provider and your handset.)

Call Features	
Item	Setting
Blind Call Transfer	*98
Attended Call Transfer	*02
Anonymous Call Enable	*67
Anonymous Call Disable	*67#
Anonymous Call Per Call Basis	*81
DND Enable	*78
DND Disable	*78#
Call Forwarding Enable	*72
Call Forwarding Disable	*72#
Call Return	*69

You can change the dial codes on the following VoIP service features:

-  Blind Call Transfer
-  Anonymous Call Enable
-  Anonymous Call Disable
-  Anonymous Call per Call Basis
-  DND Enable
-  DND Disable
-  Call Forwarding Enable
-  Call Forwarding Disable
-  Call Return

Click **Save** to save your settings or **Undo** to discard the settings entered.

Phone Book

The Phone Book page lets you to enter phone numbers into a database for easy calling. Phone book numbers are stored on the NB16WW-02.

ID	Name	Phone	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

The Phone Book page enables you to enter phone book entries. You are able to enter up to 140 entries.

The corresponding name is displayed when a VoIP call is received from that number.
(If supported by your VoIP service and telephone handset)

Click **Save** to save your settings or **Undo** to discard the settings entered.

To make calls using Phone Book, enter the ID number of the corresponding Phone Number, and wait for dial out wait time to elapse.

NAS Settings

The NAS Settings page enables you to configure the network area storage (NAS) function of the NB16WV-02. This function can be used to remotely access files stored on an attached USB hard drive. Click on any of the menu items to access the respective configuration page.

Disk Utility

The Disk Utility function enables you to check any attached USB storage for errors. The NB16WV will scan the attached storage and determine if there are any file system errors present. File System errors can prevent you being able to access stored content. You can also format (erase) any attached storage if needed. Simply click the appropriate button to perform either task.

Disk Total Capacity = 3941 MB

Partition	Free (MB)	Used (MB)	Total (MB)
1 [FAT32]			

*Warning! Formatting will erase all data on this partition.

Format Check Unmount

File Sharing

The File Sharing function enables the NB16WV-02 to take part in a Windows networking environment. Once configured, the attached USB Storage can be viewed from Windows by typing:

\\<Configured Name of the NB16WV-02>\Storage\
Eg, \\NAS\Storage

Files can then be dragged and dropped onto the attached USB storage.

Item	Setting
Network Attached Storage Name	NAS
Workgroup	WORKGROUP
Server Comment	samba server

Save Undo FTP Service Configuration

OPTION	DEFINITION
Network Attached Storage Name	Enter the computer name the NB16WV is to use on the network.
WorkGroup	Enter the network workgroup the NB16WV is to be a member of.
Server Comment	Enter the comment to be displayed when a list of network hosts is shown.

The File Sharing configuration also enables you to enable the built-in FTP server function and the associated settings:

Item	Setting
FTP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
FTP Port	21
FTP Max Connection per IP	2
FTP MAX Clients	5
Client Support UTF8	<input checked="" type="radio"/> Yes <input type="radio"/> No

Save Undo

OPTION	DEFINITION
FTP	Select to enable or disable the FTP server function.
FTP Port	Enter the network port the FTP server should run on.
FTP Max Connections per IP	Enter the maximum number of concurrent connections which can be used by a particular IP address.
FTP Max Clients	Enter the maximum number of clients which can connect to the FTP concurrently.
Client Support UTF8	Enable Unicode support for connected clients.

Access Control

The Access Control function provides control over which users can access any attached USB Storage. By default, the NB16WV-02 is in "Guest Mode" which means anyone can access the attached hard drive.

Item	Setting
Security Level	<input checked="" type="radio"/> Guest mode <input type="radio"/> Authorization mode
<input type="button" value="Save"/> <input type="button" value="User Configuration"/>	

Enabling “Authorization Mode” allows the creation of specific user accounts with a password to further control access permissions. To enable this, click on the **Authorization Mode** radio button and click **Save**. You can then click on the **User Configuration** button in order to create the required user accounts.

Item	Setting		
Username	<input type="text"/> (Max. 20 users)		
Password	<input type="password"/>		
ID	Username	Password	Select
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Cancel"/> <input type="button" value="Back"/>			

Add the user name and password and then click the **Add** button. Alternatively, to remove a user, click on the radio button to the right of the username and then select **Delete**.

Download Assistant

The Download Assistant enables you to schedule the NB16WW to perform a download from an Internet host.

You are able to select from two download types:

-  FTP
-  HTTP

Each type of download job requires different configuration options.

FTP

Item	Setting
Download Type	<input checked="" type="radio"/> FTP <input type="radio"/> HTTP
Job Name	<input type="text"/>
URL	<input type="text"/> Port <input type="text" value="21"/>
Save To	<input type="text" value="/C:/Downloads/FTP"/>
Login method	<input checked="" type="radio"/> Anonymous <input type="radio"/> Account
Username	<input type="text"/>
Password	<input type="text"/>
Start Time	<input type="radio"/> Schedule <input checked="" type="radio"/> At Once
Time	2013 / Apr / 24 - 16 : 44

***Please make sure the files that you download are legal before proceeding to download them.**

[E-mail Alert Configuration](#) [Save](#) [Undo](#)

OPTION	DEFINITION
Job Name	A name to identify the download job.
URL	The address to download from.
Port	The port required for the FTP server (<i>This would usually be left as 21</i>).
Save To	The location on the NB16WW to save the downloaded file to.
Login Method	Select the type of authentication required by the FTP server (<i>Selecting anonymous means a username and password are not required</i>).
Username	The username required to access the FTP server.
Password	The password required to access the FTP server.
Start Time	Select to either schedule a time for the download to begin or start the download immediately.

HTTP

Item	Setting
Download Type	<input type="radio"/> FTP <input checked="" type="radio"/> HTTP
Job Name	<input type="text"/>
URL	<input type="text"/>
Save To	<input type="text" value="/C/Downloads/HTTP"/>
Start Time	<input type="radio"/> Schedule <input checked="" type="radio"/> At Once
	Time: 2013 / Apr / 24 - 16 : 54

***Please make sure the files that you download are legal before proceeding to download them.**

[E-mail Alert Configuration](#) [Save](#) [Undo](#)

OPTION	DEFINITION
Job Name	A name to identify the download job.
URL	The address to download from.
Save To	The location on the NB16WV to save the downloaded file to.
Start Time	Select to either schedule a time for the download to begin or start the download immediately.

You can also configure the NB16WV-02 to send an e-mail on completion of the scheduled download. Click on the “E-mail Alert Configuration” button to setup this option.

Item	Setting
HTTP download alert	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
FTP download alert	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SMTP Server Address	<input type="text"/>
SMTP Server Port	<input type="text"/>
SMTP UserName	<input type="text"/>
SMTP Password	<input type="text"/>
Email Address	<input type="text"/>
Email Subject	<input type="text"/>
Reservation Disk space	<input type="text" value="200"/> MB

[Back](#) [Save](#) [Undo](#) [Test E-mail](#)

OPTION	DEFINITION
HTTP Download Alert	Select to enable or disable an alert to be sent for a completed HTTP download.
FTP Download Alert	Select to enable or disable an alert to be sent for a completed FTP download.
USB Download Alert	Select to enable or disable an alert to be sent for a completed USB download.
SMTP Server Address	Enter the address of the email server to be used to send the alerts.
SMTP Server Port	Enter the port which the email server is running on.
SMTP User Name	Enter the username required to login to the email server.
SMTP Password	Enter the password required to login to the email server.
Email Address	Enter the email address any alerts are to be sent to.
Email Subject	Enter the subject to be used on any email alerts sent out.
Reservation Disk Space	Enter the amount of disk space to reserve on the NB16WV for the specified download.

Download Status

The Download Status page enables you to monitor previously scheduled Download Assistant jobs. From this page you are able to Start, Pause, Resume or Delete any Download Assistant jobs.

There are 0 download jobs in the list.
 View **Running (0 Jobs)** Download Status

Page 1

Type	Name	Status
<input type="button" value="Pause"/> <input type="button" value="Delete"/> <input type="button" value="Resume"/> <input type="button" value="Start Now"/>		
<input type="button" value="Refresh"/>		


The View drop-down list enables you to select whether currently running jobs, waiting jobs or scheduled jobs are displayed. Once listed, click on the checkbox on the left hand side of the listed jobs and then click the appropriate function button.

Web HDD

The Web HDD function provides a web page based Windows Explorer type view of the content of any attached USB storage. Using this interface you are able to upload, download or delete files and folders as well as create directories. Click through the displayed folders to show any stored files.

You can download /upload files on Web HDD.

Current location: /

 Public

Left click on any items to select them and click the appropriate button or double click folders to view any content.

Filename

Note! Do not interrupt the process or power off the unit when it is being uploaded.

To upload files to your Web HDD. To do this, click the **Upload** button. You can then click the **Browse** button and then navigate to the file you would like to upload. Once selected, this file will be copied to the Web HDD and become available to download by connected devices.

Toolbox

The toolbox menu provides access to various settings and maintenance functions of the router.

System Info

The System Info screen displays the general settings on the router, such as the WAN type, the date and time, the log types and the log data.

Item	Setting
WAN Type	None
Display time	Thu, 01 Jan 2009 10:40:07 +1000
Log Types	<input type="checkbox"/> System <input type="checkbox"/> Attacks <input type="checkbox"/> Drop <input type="checkbox"/> Debug
<input type="button" value="Save"/> <input type="button" value="Undo"/>	
Time	Log

Page: 0/0 (Log Number: 0)

Routing Table

The Routing table displays the current routes in place on the router.

Destination	Netmask	Gateway	Flags	Interface
192.168.20.0	255.255.255.0	0.0.0.0		br0
239.0.0.0	255.0.0.0	0.0.0.0		br0
127.0.0.0	255.0.0.0	0.0.0.0		lo

Total numbers of routes :3
 Flags Meaning : G:Gateway D:Dynamic H:Host

Click the **Refresh** button to update this list.

Restore Settings

The Restore settings page allows you to restore a previously saved configuration of the router. This is handy for reverting to a working configuration when making changes to the router's settings.

Config Filename

Note! Do not interrupt the process or power off the unit when it is being upgraded.
 When the process is done successfully, the unit will be restarted automatically.

To restore the router configuration, click the **Browse** button, select the saved configuration file and then click the **Restore** button.

Firmware Upgrade

This page lets you upgrade the firmware of the router. The firmware is the system running on the router. New firmware updates are regularly made available and can fix bugs and add new features.

Firmware Filename
<input type="button" value="Choose File"/> No file chosen Current firmware version is NCMZ0.1016_04231050 . Note! Do not interrupt the process or power off the unit when it is being upgraded. When the process is done successfully, the unit will be restarted automatically.
<input type="button" value="Upgrade"/> <input type="button" value="Cancel"/>

Backup Settings

Click the **Backup Settings** menu item to save the current configuration of the router to a file for safe-keeping.

Reset to Default

Click the **Reset to Default** menu item to set the configuration of the router to the factory default settings.



Note: This will erase all configuration settings. Ensure you have a backup of your configuration before proceeding to reset to default settings.

Reboot

Click the **Reboot** menu item to restart the router.

Startup Wizard

Click the **Startup Wizard** menu item if you want to run the initial wizard that showed the first time you installed your router.

Miscellaneous

The miscellaneous page provides options to send a Wake-on-LAN packet to a specified IP, ping a specified domain name or IP address and brighten or dim the front LEDs of the router.

Item	Setting
MAC Address for Wake-on-LAN	<input type="text"/> <input type="button" value="Wake up"/>
Domain Name or IP address for Ping Test	<input type="text"/> <input type="button" value="Ping"/>
LED Settings	<input checked="" type="radio"/> Manual <input type="radio"/> By Schedule <input type="button" value="Brighten LEDs"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

Logout

The **Logout** menu item logs you out of the router.

Additional Product Information

Establishing a wireless connection

Windows XP (Service Pack 3)

1. Open the Network Connections control panel (Start -> Control Panel -> Network Connections);
2. Right-click on your Wireless Network Connection and select View Available Wireless Networks;
3. Select the wireless network listed on your included wireless security card and click Connect.
4. Enter the network key (refer to the included wireless security card for *the default wireless network key*).
5. The connection will show Connected.

Windows Vista

1. Open the Network and Sharing Center (Start > Control Panel > Network and Sharing center).
2. Click on "Connect to a network".
3. Choose "Connect to the Internet" and click on "Next".
4. Select the wireless network listed on your included wireless security card and click Connect.
5. Enter the network key (refer to the included wireless security card for *the default wireless network key*).
6. Select the appropriate location. This will affect the firewall settings on the computer.
7. Click on both "Save this network" and "Start this connection automatically" and click "Next".

Windows 7

1. Open the Network and Sharing Center (Start > Control Panel > Network and Sharing center).
2. Click on "Change Adapter settings" on the left-hand side.
3. Right-click on "Wireless Network Connection" and select "Connect / Disconnect".
4. Select the wireless network listed on your included wireless security card and click Connect.
5. Enter the network key (refer to the included wireless security card for *the default wireless network key*).
6. You may then see a window that asks you to "Select a location for the 'wireless' network". Please select the "Home" location.
7. You may then see a window prompting you to setup a "HomeGroup". Click "Cancel" on this.
8. You can verify your wireless connection by clicking the "Wireless Signal" indicator in your system tray.
9. After clicking on this, you should see an entry matching the SSID of your NB16WW-02 with "Connected" next to it.

Windows 8/8.1

1. Open the Network and Sharing Center (Click on Start, Type "Network and Sharing Center")
2. Click on "Change adapter settings" on the left hand column.
3. Right-click on Wireless Network Adaptor and select "Connect / Disconnect".
4. Select the wireless network listed on your included wireless security card and click Connect.
5. Enter the network key (refer to the included wireless security card for *the default wireless network key*).
6. You can verify your wireless connection by clicking the "Wireless Signal" indicator in your system tray.
7. After clicking on this, you should see an entry matching the SSID of your NB16WW-02 with "Connected" under it.

Mac OSX 10.6

1. Click on the Airport icon on the top right menu.
2. Select the wireless network listed on your included wireless security card and click Connect.
3. On the new window, select "Show Password", type in the network key (refer to the included wireless security card for *the default wireless network key*) in the Password field and then click on OK.
4. To check the connection, click on the Airport icon and there should be a tick on the wireless network name.



Note: For other operating systems, or if you use a wireless adaptor utility to configure your wireless connection, please consult the wireless adapter documentation for instructions on establishing a wireless connection.

Troubleshooting

Using the indicator lights (LEDs) to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

Power LED

The Power LED does not light up.

STEP	CORRECTIVE ACTION
1	Make sure that the NB16WV-02 power adaptor is connected to the device and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the NB16WV-02 and the power source are both turned on and device is receiving sufficient power.
3	Turn the NB16WV-02 off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact technical support.

Technical Data

The following table lists the hardware specifications of the NB16WV-02.

MODEL	NB16WV-02
ADSL2+	ITU 992.1 (G.dmt) Annex A ITU 992.2 (G.lite) ITU 992.3 ADSL2 (G.dmt.bis, Annex J/L) ITU 992.5 ADSL2+ (Annex M)
Wireless WAN	1 x USB 2.0 port for external HSPA/LTE modem PPP (for WCDMA / HSPA)
Ethernet WAN	1 x Gigabit WAN port (10/100/1000 Mbps)
Connectivity	2 x USB 2.0, 4 x 10/100/1000 Mbps, 1 x RJ-11 ADSL, 1 x RJ-11 Telephone Handset, 1 x WLAN
LED Indicators	Power, ADSL, 3G, WWW, LAN 1-4, WAN, WIFI, VoIP
Operating Temperature	Operating temperature: 0°C - 40°C, Humidity: 10%-90% non-condensing Storage temperature: -10°C - 70°C, Humidity: 0%-95% non-condensing
Power Input	12V DC - 2.5A
Dimensions & Weight	215 mm (L) x 145 mm (W) x 37 mm (H) 403 grams
VoIP	PROTOCOL SIP 2.0 VOICE COMPRESSION G.711-Alaw voice compression G.711-Mulaw voice compression G.726-32 voice compression G.729AB voice compression G.168 116 ms tail line echo cancellation CALL FUNCTION Call forward Caller ID Dial plan Call waiting 3-way conference call Hot line
Regulatory Compliance	A-Tick

Electrical Specifications

It is recommended that the NB16WV-02 be powered by the supplied 12V DC, 2.5A power supply. A replacement power supply is available from the NetComm Wireless Online shop.

Environmental Specifications / Tolerances

The NB16WV-02 housing enables it to operate over a wide variety of temperatures from 0°C - 40°C (operating temperature).

Legal & Regulatory Information

Intellectual Property Rights

All intellectual property rights (including copyright and trade mark rights) subsisting in, relating to or arising out of this Manual are owned by and vest in NetComm Wireless (ACN 002490486) (NetComm Wireless Limited) (or its licensors). This Manual does not transfer any right, title or interest in NetComm Wireless Limited's (or its licensors') intellectual property rights to you.

You are permitted to use this Manual for the sole purpose of using the NetComm Wireless product to which it relates. Otherwise no part of this Manual may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Wireless Limited.

NetComm, NetComm Wireless and NetComm Wireless Limited are a trademark of NetComm Wireless Limited. All other trademarks are acknowledged to be the property of their respective owners.

Customer Information

The Australian Communications & Media Authority (ACMA) requires you to be aware of the following information and warnings:

1. This unit may be connected to the Telecommunication Network through a line cord which meets the requirements of the AS/CA S008-2011 Standard.
2. This equipment incorporates a radio transmitting device, in normal use a separation distance of 20cm will ensure radio frequency exposure levels complies with Australian and New Zealand standards.
3. This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACMA. 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:
 - i. Change the direction or relocate the receiving antenna.
 - ii. Increase the separation between this equipment and the receiver.
 - iii. Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
 - iv. Consult an experienced radio/TV technician for help.
4. 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 Wireless. Failure to do so may cause damage to this product, fire or result in personal injury.

Consumer Protection Laws

Australian and New Zealand consumer law in certain circumstances implies mandatory guarantees, conditions and warranties which cannot be excluded by NetComm and legislation of another country's Government may have a similar effect (together these are the Consumer Protection Laws). Any warranty or representation provided by NetComm is in addition to, and not in replacement of, your rights under such Consumer Protection Laws.

If you purchased our goods in Australia and you are a consumer, you are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure. If you purchased our goods in New Zealand and are a consumer you will also be entitled to similar statutory guarantees.

Product Warranty

All NetComm Wireless products have a standard one (1) year warranty from date of purchase, however, some products have an extended warranty option (refer to packaging and the warranty card) (each a Product Warranty). To be eligible for the extended warranty option you must supply the requested warranty information to NetComm Wireless Limited within 30 days of the original purchase date by registering online via the NetComm Wireless web site at www.netcommwireless.com. For all Product Warranty claims you will require proof of purchase. All Product Warranties are in addition to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Consumer Protection Laws Section above).

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see the [Consumer Protection Laws](#) Section above), the Product Warranty is granted on the following conditions:

1. the Product Warranty extends to the original purchaser (you / the customer) and is not transferable;
2. the Product 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;
5. NetComm Wireless Limited does not have any liability or responsibility under the Product 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; and
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 Wireless Limited recommends that you enable these features to enhance your security.

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Section 3 above), the Product Warranty is automatically voided if:

1. you, or someone else, use the product, or attempt to use it, other than as specified by NetComm Wireless Limited;
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 Wireless Limited; or
6. the serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitation of Liability

This clause does not apply to New Zealand consumers. Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see the [Consumer Protection Laws](#) Section above), NetComm Wireless Limited accepts no liability or responsibility, for consequences arising from the use of this product. NetComm Wireless Limited reserves the right to change the specifications and operating details of this product without notice.

If any law implies a guarantee, condition or warranty in respect of goods or services supplied, and NetComm Wireless's liability for breach of that condition or warranty may not be excluded but may be limited, then subject to your rights and remedies under any applicable Consumer Protection Laws which cannot be excluded, NetComm Wireless's liability for any breach of that guarantee, condition or warranty is limited to: (i) in the case of a supply of goods, NetComm Wireless Limited doing any one or more of the following: replacing the goods or supplying equivalent goods; repairing the goods; paying the cost of replacing the goods or of acquiring equivalent goods; or paying the cost of having the goods repaired; or (ii) in the case of a supply of services, NetComm Wireless Limited doing either or both of the following: supplying the services again; or paying the cost of having the services supplied again.

To the extent NetComm Wireless Limited is unable to limit its liability as set out above, NetComm Wireless Limited limits its liability to the extent such liability is lawfully able to be limited.

Contact

Address: NETCOMM WIRELESS LIMITED Head Office
PO Box 1200, Lane Cove NSW 2066 Australia
Phone: +61(0)2 9424 2070
Fax: +61(0)2 9424 2010
Email: sales@netcommwireless.com techsupport@netcommwireless.com