N600 Dual Band WiFi Gigabit Modem Router

NB16DG

USER GUIDE

Copyright

⚠ 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 NB16DG

DOCUMENT VERSION	DATE
1.0 - Initial document release	May 2013

Table 1 - Document Revision History

Table of Contents

Overview

Introduction

This manual provides information related to the installation, operation, and use of the NB16DG.

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 NB16DG, please confirm that you comply with the minimum system requirements below.

- An activated ADSL or configured 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.

Notation

The following symbols are used in this manual:

⚠	Indicates a note requiring attention.
⚡	Indicates a note providing a warning.
ℹ	Indicates a note providing useful information.

Product Introduction

Product Overview

- Powerful dual-band wireless router with support for ADSL.
- Creates instant Wireless hotspots to share the Internet connection of a DSL/Cable connection.
- Supports Wireless N standard with data speeds up to 600Mbps.
- One Gigabit WAN port for alternate wired Internet connection (NBN/Cable/Satellite via Ethernet).
- Four Gigabit LAN ports to connect wired devices like PCs or gaming consoles.
- Ensures connectivity and business continuity with auto Internet failover from ADSL to Ethernet WAN.
- 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.
- Download assistant.

Speeds are dependent on network coverage. 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 NB16DG package consists of:

- N600 Dual Band WiFi Gigabit Modem Router.
- Quick Start Guide.
- Power Supply Unit.
- Ethernet Cable (RJ-45).
- 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 NB16DG integrates an ADSL modem, dual-band wireless LAN and a full Gigabit Ethernet interface into one unit. Connection to the Internet is achieved through the ADSL modem, or via a connection to the NB16DG's WAN port, providing you with the flexibility to choose how you access the Internet.

The NB16DG's automatic failover ensures you are always connected by activating the Ethernet connection should the ADSL connection drop out.

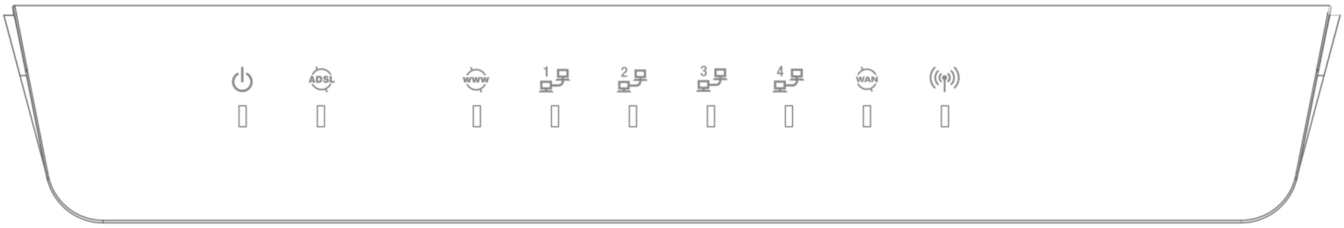
Users are able to share a single Internet connection via both a wired and wireless connection to the NB16DG. With two built-in antennas providing a 2 transmit, 2 receive (2T2R) 802.11n concurrent dual band wireless access point, this router provides wireless speeds of up to 600Mbps. On top of this, the NB16DG has four gigabit LAN ports for high-speed wired connections to multiple devices.

The NB16DG 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 NB16DG 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 NB16DG 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 NB16DG is powered off
		Blue	The NB16DG is powered on and operating normally
		Blue Flashing	The NB16DG is starting up
ADSL	ADSL	Off	No ADSL configuration present
		Blue	The NB16DG is connected to the Internet via an xDSL service
		Blue Flashing	The NB16DG is attempting to connect to the xDSL service
WWW	www	Off	No Internet configuration present
		Red	The NB16DG is connected via a 3G service
		Flashing Red	Data is being sent or received via the 3G service
		Blue	The NB16DG is connected via an xDSL service
		Flashing Blue	Data is being sent or received via the xDSL service
		Purple	The NB16DG is connected via an Ethernet WAN service
		Flashing Purple	Data is being sent or received via the Ethernet WAN service
LAN 1-4	1 – 4	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
WAN	WAN	Off	No device is connected to the Ethernet WAN port
		Blue	A device is connected to the Ethernet WAN port
WiFi	((ı))	Off	WiFi is disabled on the NB16DG
		Blue	WiFi is enabled on the NB16DG
		Flashing Blue	The NB16DG is waiting for a WPS PBC connection

Physical Dimensions

The following page lists the physical dimensions of the NB16DG.

NB16DG DIMENSIONS	
Length	215 mm
Width	145 mm
Height	37 mm
Weight	386 grams

NB16DG Default Settings

The following tables list the default settings for the NB16DG.

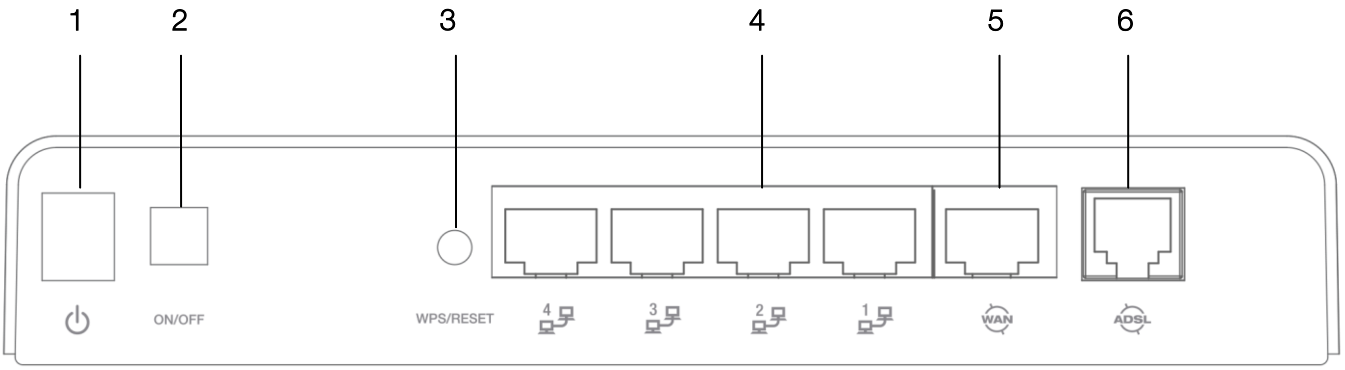
LAN (MANAGEMENT)	
Static IP Address	192.168.20.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.1

WIRELESS (WIFI)	
SSID	(Refer to the included Wireless Security Card)
Security	WPA-SPK/WPA2-PSK (mixed mode)
Security Key	(Refer to the included Wireless Security Card)

NB16DG WEB INTERFACE ACCESS	
Username	admin
Password	admin

Interfaces

The following interfaces are available on the NB16DG:



NUMBER	INTERFACE	DESCRIPTION
1	Power Jack	Connection point for the included power adapter. Connect the power supply here.
2	Power button	Turns the NB16DG on or off.
3	WPS/RESET button	Activate the WiFi WPS (2.4GHz) function by press/hold the WPS/RESET button for 3 seconds. Activate the WiFi WPS (5GHz) function by press/hold the WPS/RESET button for 5 seconds. Activate the RESET function by press/hold the WPS/RESET button for 15 seconds.
4	LAN 1-4	Gigabit Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.
5	WAN	Gigabit WAN port for connection to a WAN network.
6	ADSL	Use the provided RJ-11 cable to connect the router to the telephone line operating your xDSL 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 NB16DG, 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 NB16DG

Placement of your NB16DG

The wireless connection between your NB16DG and your WiFi devices will be stronger the closer your connected devices are to your NB16DG. Your wireless connection and performance will degrade as the distance between your NB16DG 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 NB16DG in order to see if distance is the problem.

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 WiFi Devices and your NB16DG, please try the following steps:

- In multi-storey homes, place the NB16DG on a floor that is as close to the centre of the home as possible. This may mean placing the NB16DG on an upper floor.
- Try not to place the NB16DG near a cordless telephone that operates at the same radio frequency as the NB16DG (2.4GHz).

Avoid obstacles and interference

Avoid placing your NB16DG 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 NB16DG).

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 NB16DG 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 NB16DG.
- 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 NB16DG 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 NB16DG.
2. Plug the power adapter into the wall socket and switch on the power.
3. Wait approximately 60 seconds for the NB16DG 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 NB16DG.
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 NB16DG.

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 NB16DG.

Note: Refer to the included Wireless Security Card for the default SSID and wireless security key of your NB16DG

3. When prompted for your wireless security settings, enter the Wireless security key configured on the NB16DG.
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 NB16DG.

Web Based Configuration Interface

First-time Setup Wizard

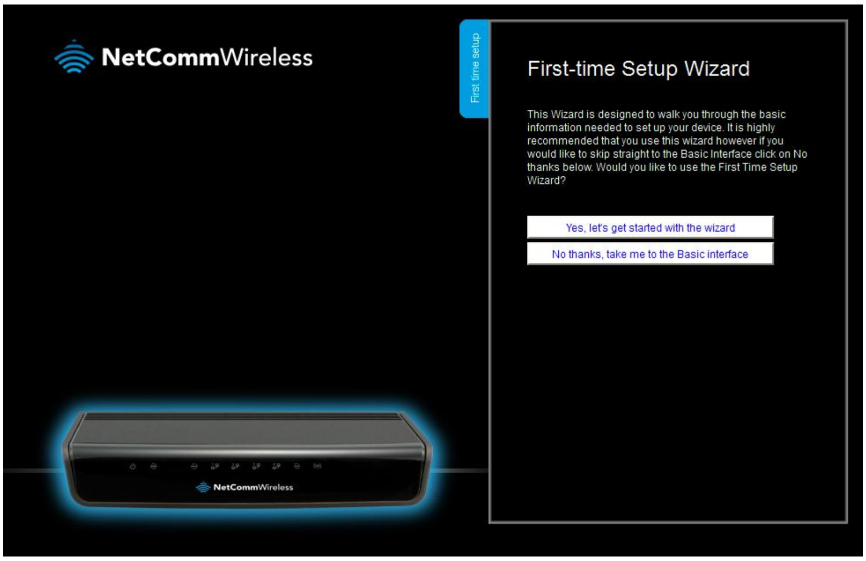
Please follow the steps below to configure your NB16DG Wireless router via the web based configuration wizard.

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**.

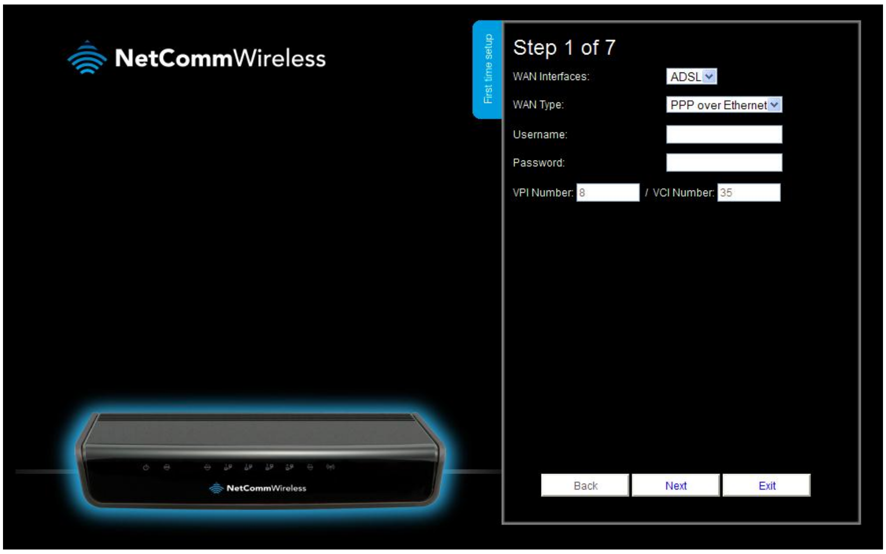


NetCommWireless
First time setup
Yes, let's get started with the wizard
No thanks, take me to the Basic interface

First-time Setup Wizard

This Wizard is designed to walk you through the basic information needed to set up your device. It is highly recommended that you use this wizard however if you would like to skip straight to the Basic Interface click on No thanks below. Would you like to use the First Time Setup Wizard?

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



Step 1 of 7

WAN Interfaces: ADSL

WAN Type: PPP over Ethernet

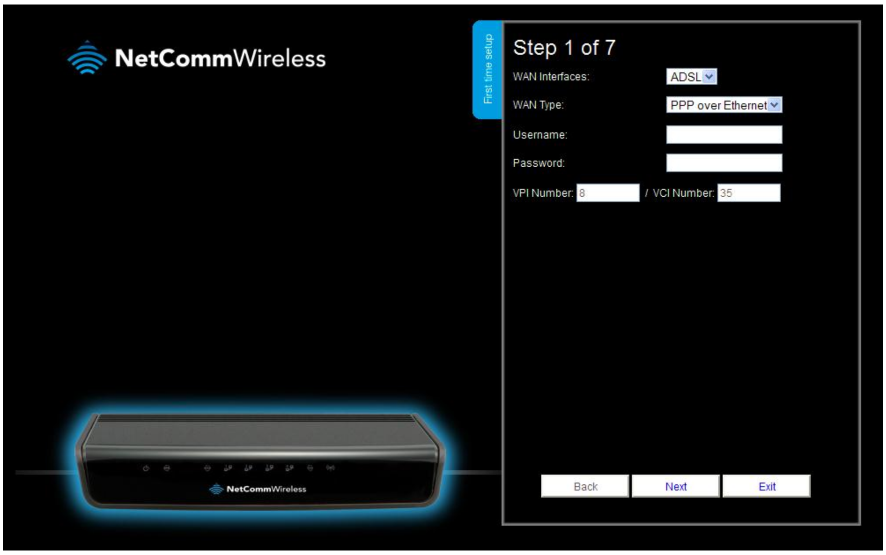
Username:

Password:

VPI Number: 8 / VCI Number: 35

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



Step 1 of 7

WAN Interfaces: ADSL

WAN Type: PPP over Ethernet

Username:

Password:

VPI Number: 8 / VCI Number: 35

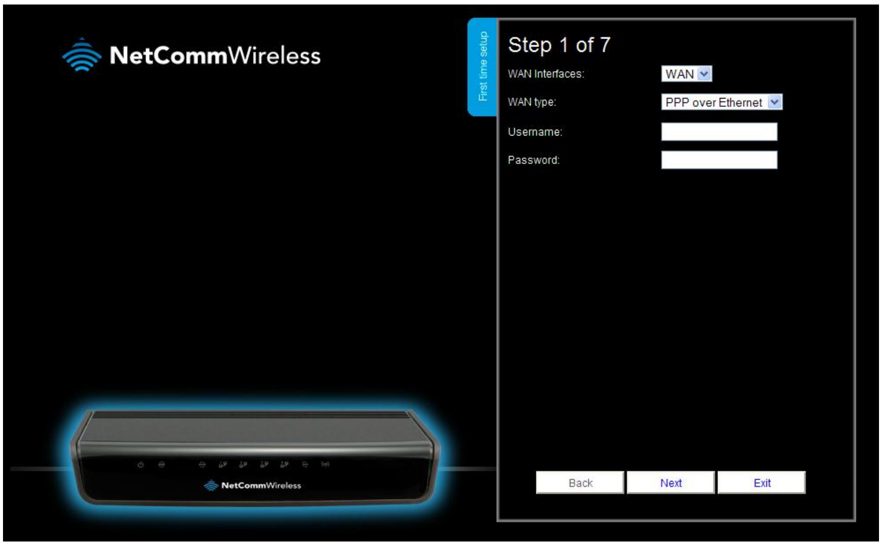
a. Select the type of ADSL connection. You can select from:
   - PPP over ATM (or PPPoA)
   - PPP over Ethernet (or PPPoE)

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.

WAN



Step 1 of 7

WAN Interfaces: WAN

WAN type: PPP over Ethernet

Username:

Password:

Select the type of WAN connection:

Dynamic IP Address

a. Enter the Host Name (Optional)
b. 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

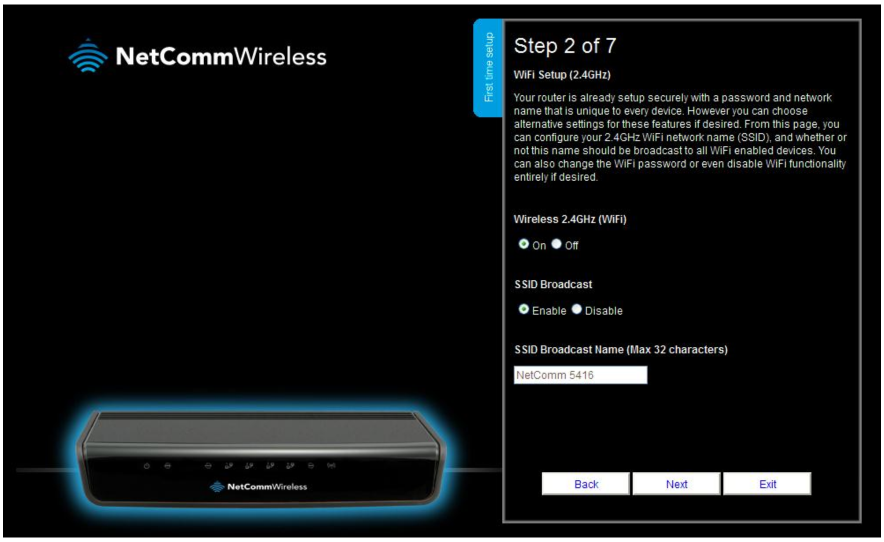
a. Enter the Server IP Address/Name

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**)



Step 2 of 7

WiFi Setup (2.4GHz)

Your router is already setup securely with a password and network name that is unique to every device. However you can choose alternative settings for these features if desired. From this page, you can configure your 2.4GHz WiFi network name (SSID), and whether or not this name should be broadcast to all WiFi enabled devices. You can also change the WiFi password or even disable WiFi functionality entirely if desired.

Wireless 2.4GHz (WiFi)

● On ○ Off

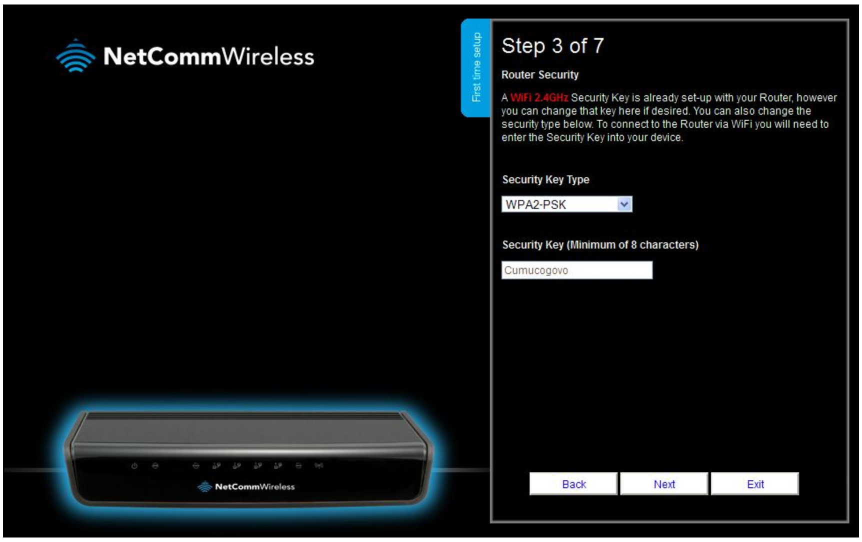
SSID Broadcast

● Enable ○ Disable

SSID Broadcast Name (Max 32 characters)

NetComm 5416

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.



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

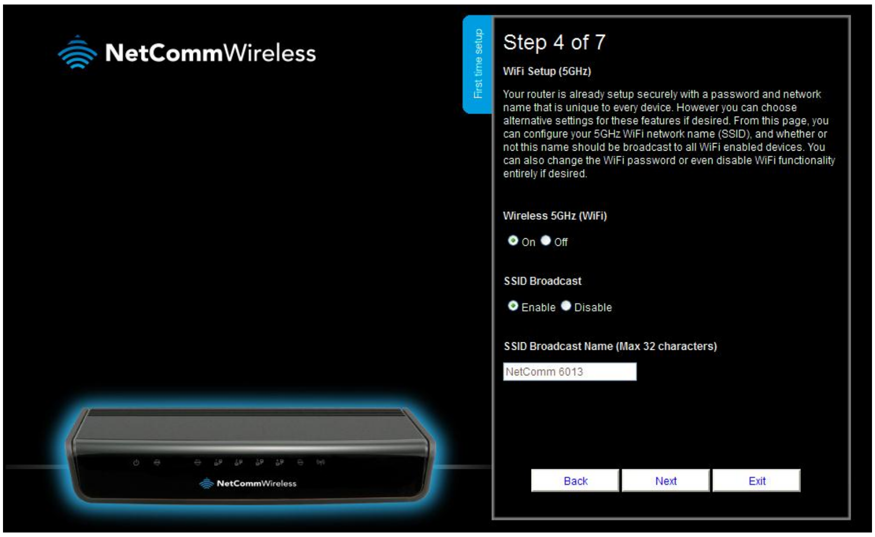
WPA2-PSK

Security Key (Minimum of 8 characters)

Cumucogovo

5. 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**)



Step 4 of 7

WiFi Setup (5GHz)

Your router is already setup securely with a password and network name that is unique to every device. However you can choose alternative settings for these features if desired. From this page, you can configure your 5GHz WiFi network name (SSID), and whether or not this name should be broadcast to all WiFi enabled devices. You can also change the WiFi password or even disable WiFi functionality entirely if desired.

Wireless 5GHz (WiFi)

● On ○ Off

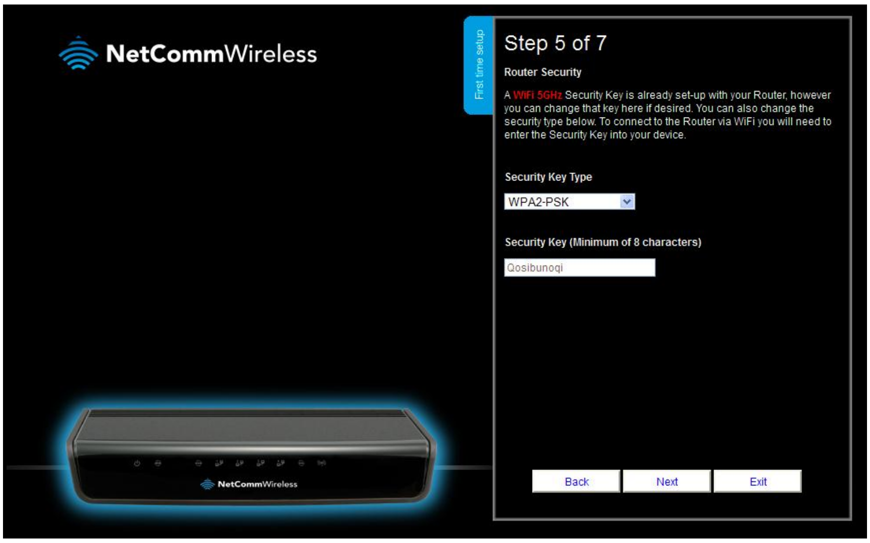
SSID Broadcast

● Enable ○ Disable

SSID Broadcast Name (Max 32 characters)

NetComm 6013

6. 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.



Step 5 of 7

Router Security

A WiFi 5GHz 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.

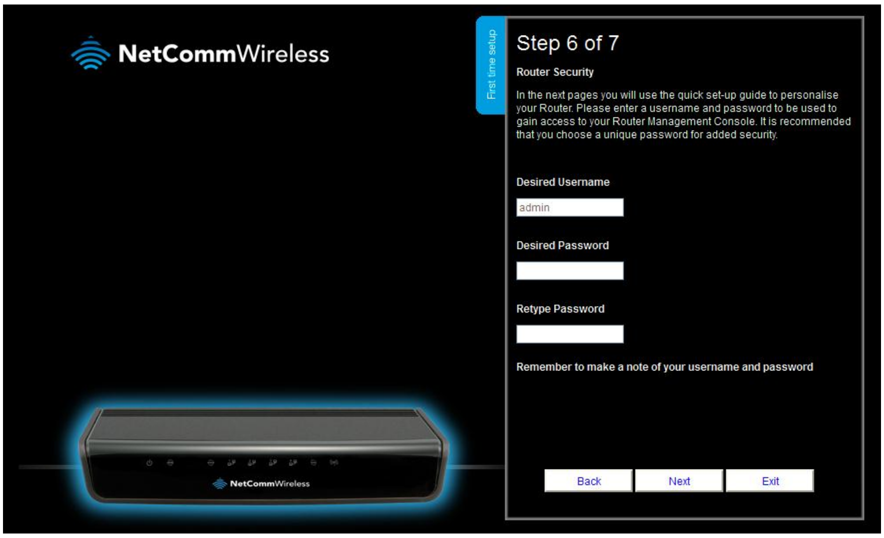
Security Key Type

WPA2-PSK

Security Key (Minimum of 8 characters)

Qosibunoqi

7. 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**).



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

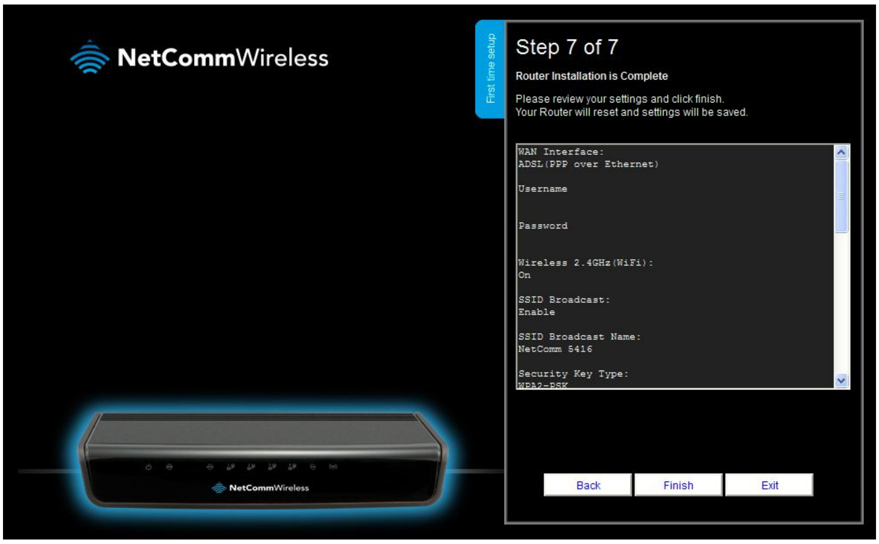
admin

Desired Password

Retype Password

Remember to make a note of your username and password

8. 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.



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:
ADSL(PPP over Ethernet)

Username


Password


Wireless 2.4GHz(WiFi):
On

SSID Broadcast:
Enable

SSID Broadcast Name:
NetComm 5416

Security Key Type:
WPA2-PSK
```

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.

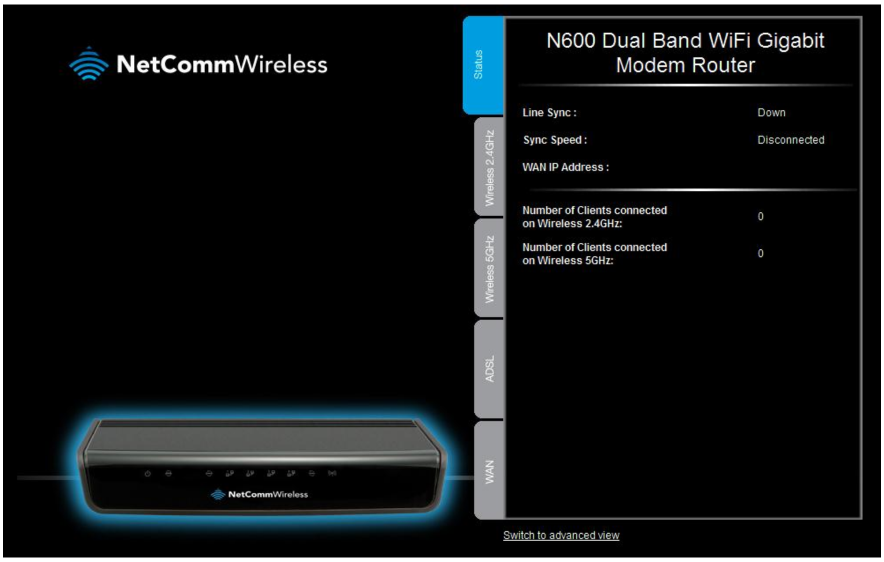
Basic View

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
- Number of clients connected on Wireless 2.4GHz
- Number of clients connected on Wireless 5GHz



N600 Dual Band WiFi Gigabit Modem Router

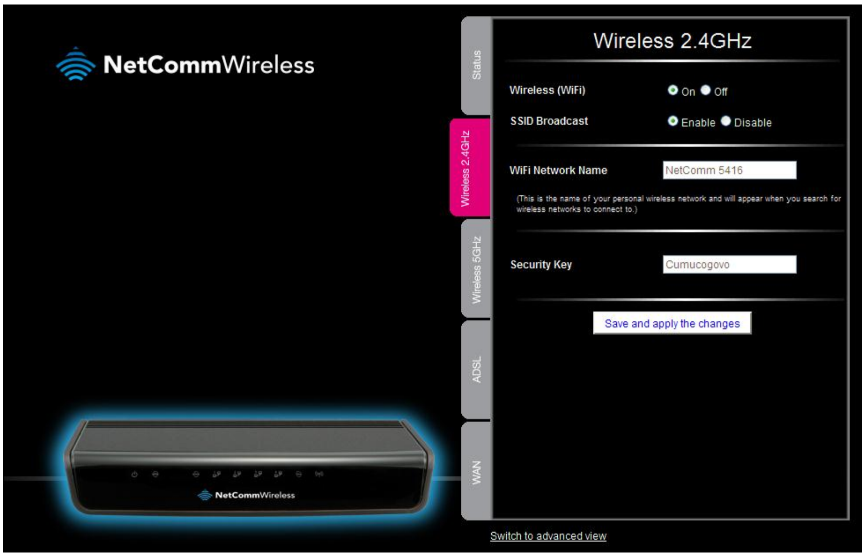
Line Sync :	Down
Sync Speed :	Disconnected
WAN IP Address :	
Number of Clients connected on Wireless 2.4GHz:	0
Number of Clients connected on Wireless 5GHz:	0

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 2.4GHz

Wireless (WiFi) ● On ○ Off

SSID Broadcast ● Enable ○ Disable

WiFi Network Name: NetComm 5416

(This is the name of your personal wireless network and will appear when you search for wireless networks to connect to.)

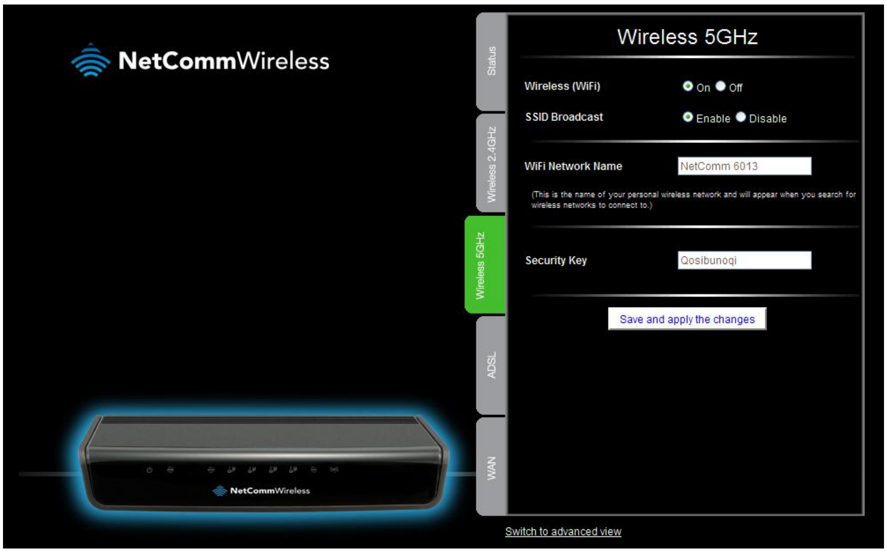
Security Key: Cumucogovo

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.



Wireless 5GHz

Wireless (WiFi) ● On ○ Off

SSID Broadcast ● Enable ○ Disable

WiFi Network Name: NetComm 6013

(This is the name of your personal wireless network and will appear when you search for wireless networks to connect to.)

Security Key: Qosibunoqi

ADSL

The following configuration options are available on the ADSL tab:

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

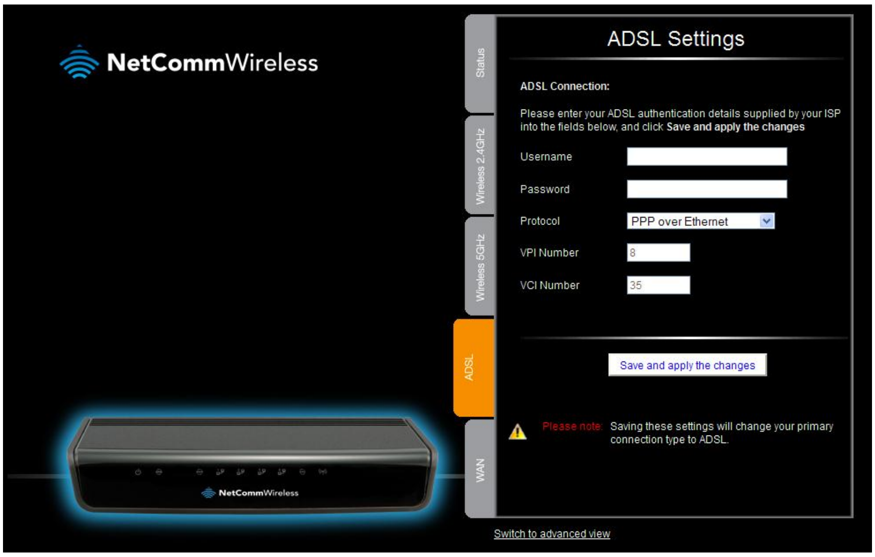
To configure your xDSL connection, enter the username and password as supplied by your xDSL service Provider.

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

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

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

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



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: 8

VCI Number: 35

Please note: Saving these settings will change your primary connection type to ADSL.

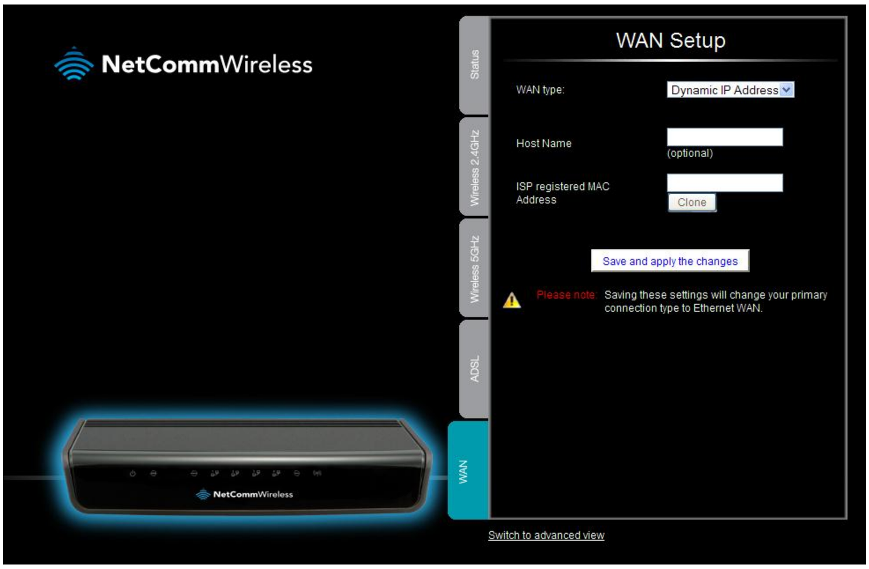
Note: Saving any configuration changes on this page will make the xDSL connection the primary method of connecting to the Internet and disable the WAN connection.

WAN

The WAN tab provides configuration options for your WAN connection. The available WAN types are:

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

Select the correct WAN type and enter the appropriate information in the fields provided. When you have finished, click **Save and apply the changes** to make them active.



WAN Setup

WAN type: Dynamic IP Address

Host Name (optional)

ISP registered MAC Address Clone

Save and apply the changes

Please note: Saving these settings will change your primary connection type to Ethernet WAN.

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

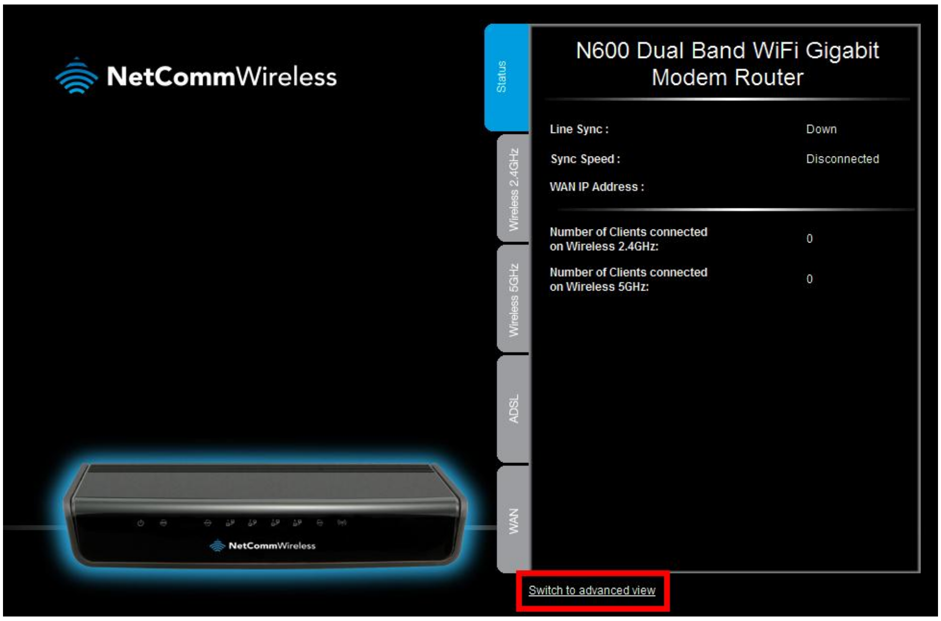
Advanced Configuration

To access the advanced configuration options of your NB16DG, 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.

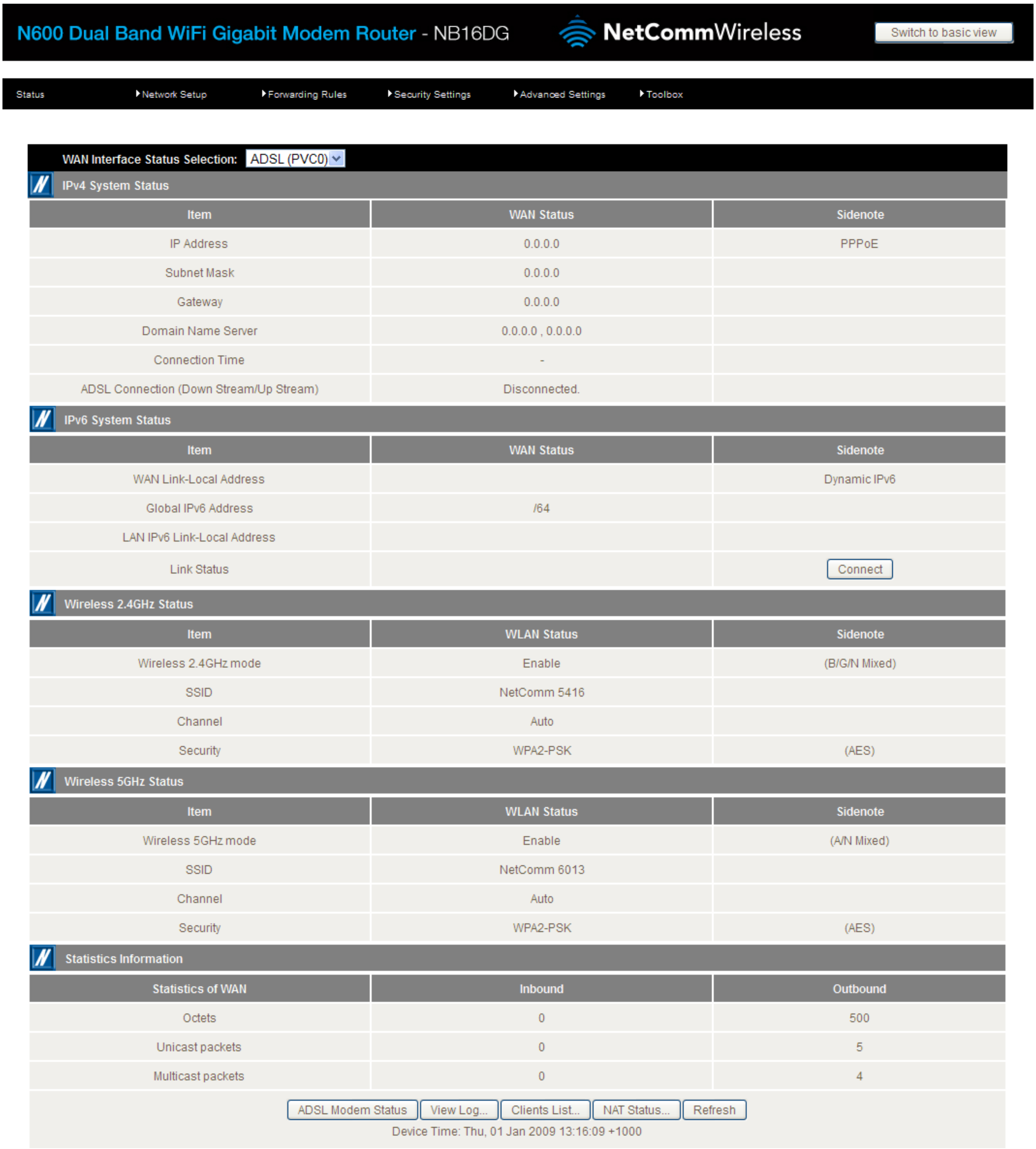


N600 Dual Band WiFi Gigabit Modem Router

Line Sync :	Down
Sync Speed :	Disconnected
WAN IP Address :	
Number of Clients connected on Wireless 2.4GHz:	0
Number of Clients connected on Wireless 5GHz:	0

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

Status



WAN Interface Status Selection: ADSL (PVC0)

IPv4 System Status

Item	WAN Status	Sidenote
IP Address	0.0.0.0	PPPoE
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0 , 0.0.0.0	
Connection Time	-	
ADSL Connection (Down Stream/Up Stream)	Disconnected.	

IPv6 System Status

Item	WAN Status	Sidenote
WAN Link-Local Address		Dynamic IPv6
Global IPv6 Address	/64	
LAN IPv6 Link-Local Address		
Link Status		Connect

Wireless 2.4GHz Status

Item	WLAN Status	Sidenote
Wireless 2.4GHz mode	Enable	(B/G/N Mixed)
SSID	NetComm 5416	
Channel	Auto	
Security	WPA2-PSK	(AES)

Wireless 5GHz Status

Item	WLAN Status	Sidenote
Wireless 5GHz mode	Enable	(A/N Mixed)
SSID	NetComm 6013	
Channel	Auto	
Security	WPA2-PSK	(AES)

Statistics Information

Statistics of WAN	Inbound	Outbound
Octets	0	500
Unicast packets	0	5
Multicast packets	0	4

Device Time: Thu, 01 Jan 2009 13:16:09 +1000

ITEM	DESCRIPTION
IPv4 System Status	
IP Address	The IP Address assigned to the router.
Subnet Mask	The Subnet Mask of the router.
Gateway	The router's gateway.
Domain Name Server	The IP addresses of the primary and secondary Domain Name Servers.
Connection Time	The length of time the router has been connected on the selected connection type.
ADSL Connection (Down Stream/Up Stream)	The ADSL downstream and upstream synchronization speeds.
IPv6 System Status	
WAN Link-Local Address	The link-local address assigned to the router on the WAN side. The router will process packets destined to link-local addresses but will not forward them to other links.
Global IPv6 Address	The publicly routable and reachable IPv6 internet address.
LAN IPv6 Link-Local Address	The link-local address assigned to the router on the LAN side. The router will process packets destined to link-local addresses but will not forward them to other links.
Link Status	The current status of the IPv6 link.
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 encryption in use on the router for the 2.4GHz wireless network.
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 encryption in use on the router for the 5GHz wireless network.
Statistics Information	
Octets	The number of data packets 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.

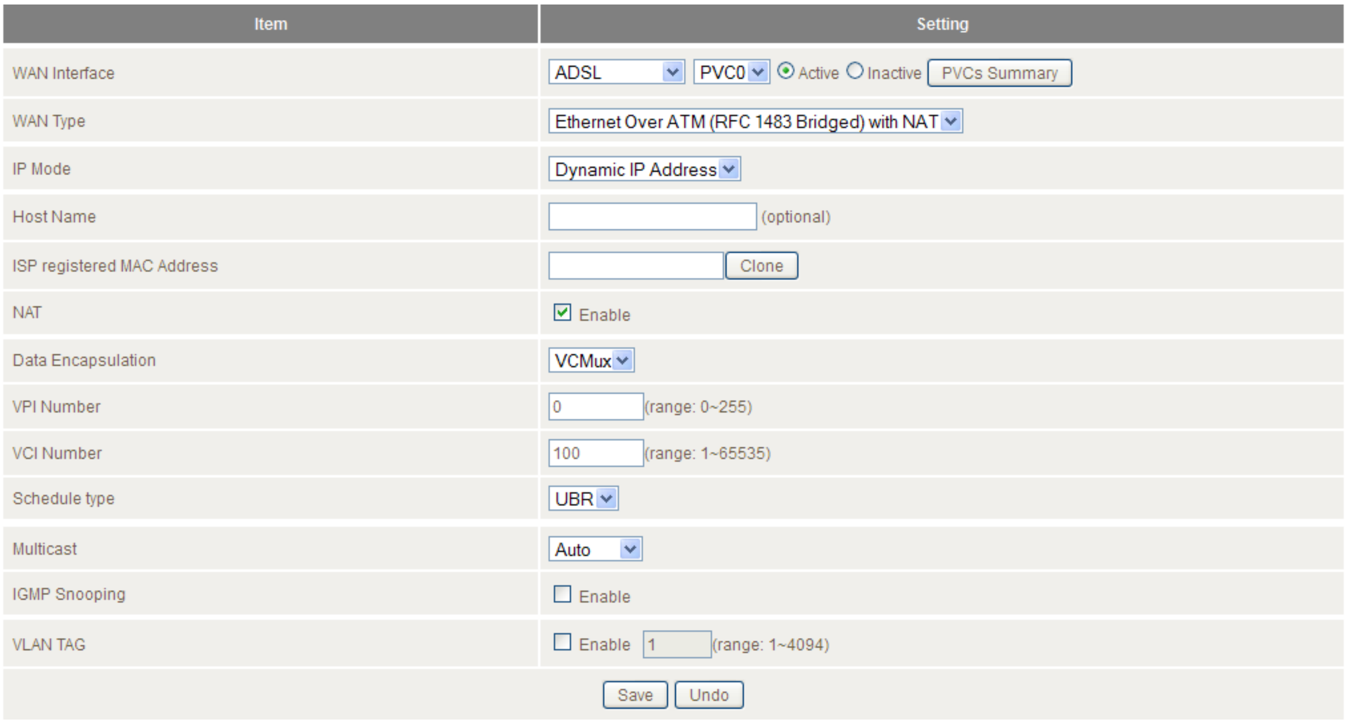
Network Setup

Network Setup

This page allows you to configure the ADSL and Ethernet WAN (Wide Area Network) connection settings on the NB16DG.

ADSL

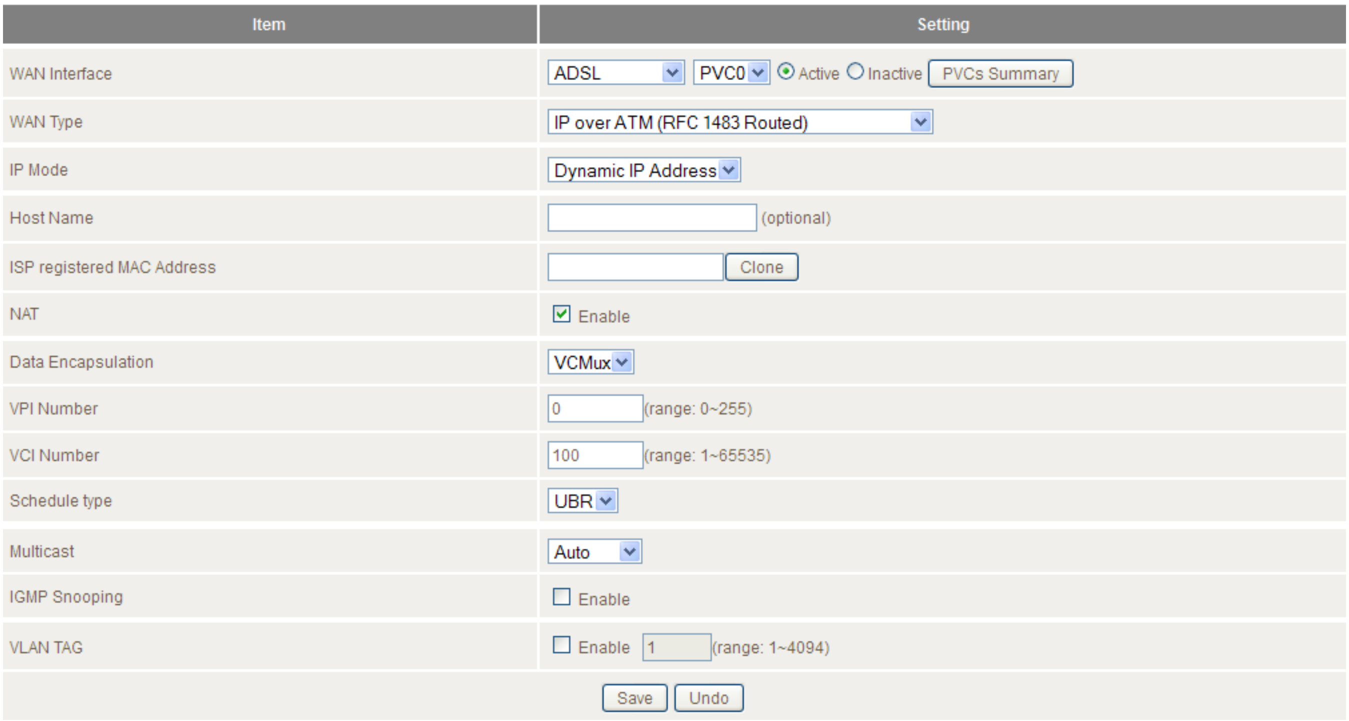
Ethernet over ATM (RFC1483 bridged) with NAT



Item	Setting
WAN Interface	ADSL ▾ PVC0 ▾ ● Active ○ Inactive PVCs Summary
WAN Type	Ethernet Over ATM (RFC 1483 Bridged) with NAT ▾
IP Mode	Dynamic IP Address ▾
Host Name	(optional)
ISP registered MAC Address	Clone
NAT	☑ Enable
Data Encapsulation	VCMux ▾
VPI Number	0 (range: 0~255)
VCI Number	100 (range: 1~65535)
Schedule type	UBR ▾
Multicast	Auto ▾
IGMP Snooping	□ Enable
VLAN TAG	□ Enable 1 (range: 1~4094)
	Save 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 *(Refer to your ISP for more information)*.
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.
Data Encapsulation	Select the Data Encapsulation required by your ISP *(Refer to your ISP for more information)*.
VPI Number	Enter the VPI provided by your ISP *(This will usually be 8 for Australia or 0 for New Zealand)*
VCI Number	Enter the VCI provided by your ISP *(This will usually be 35 for Australia or 100 for New Zealand)*
Schedule Type	Select the data schedule type required by your ISP (Refer to your ISP for more information).
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.

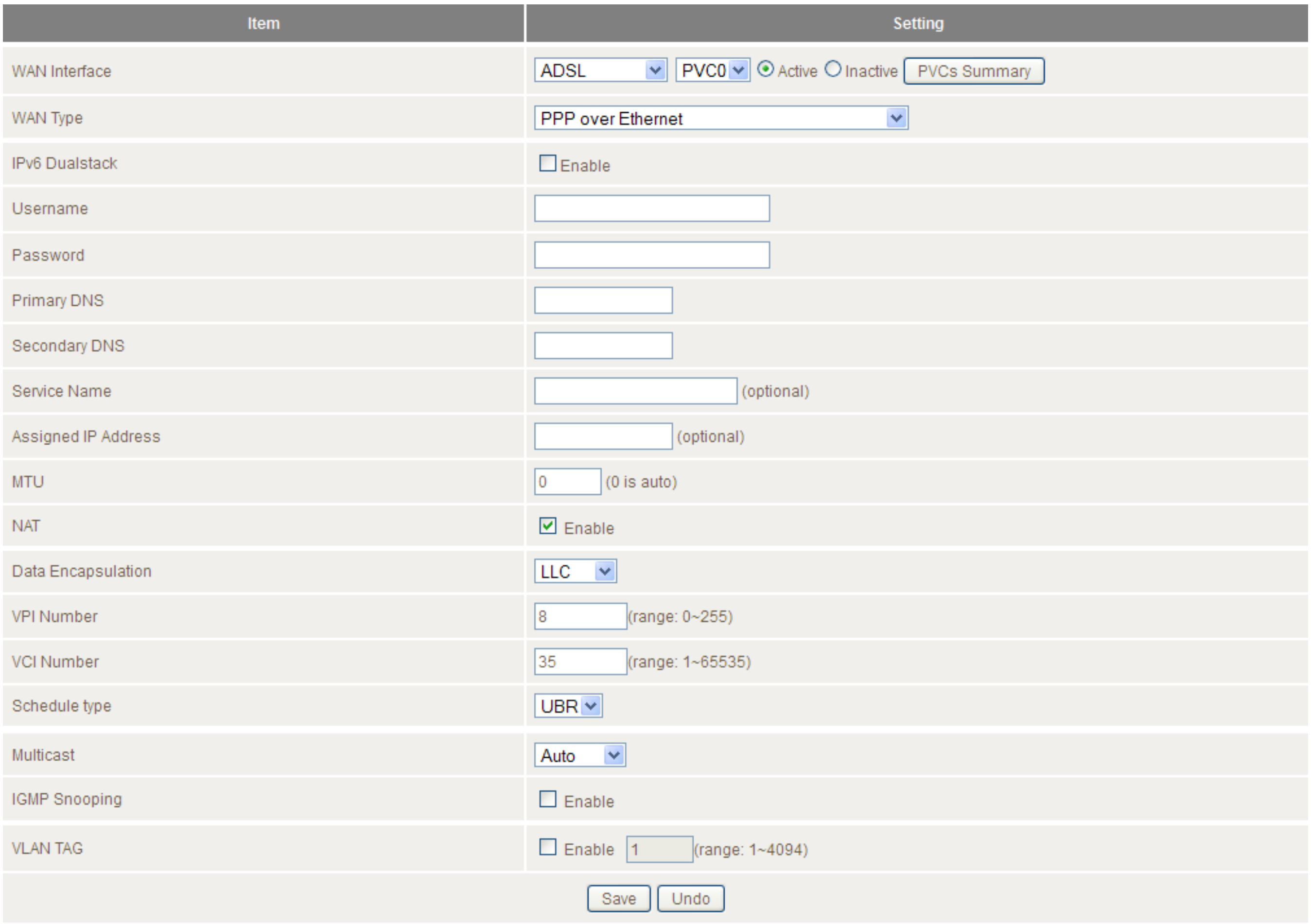
IP over ATM (RFC1483 routed)



Item	Setting
WAN Interface	ADSL PVC0 ● Active ○ Inactive PVCs Summary
WAN Type	IP over ATM (RFC 1483 Routed)
IP Mode	Dynamic IP Address
Host Name	(optional)
ISP registered MAC Address	Clone
NAT	☑ Enable
Data Encapsulation	VCMux
VPI Number	0 (range: 0~255)
VCI Number	100 (range: 1~65535)
Schedule type	UBR
Multicast	Auto
IGMP Snooping	□ Enable
VLAN TAG	□ Enable 1 (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 *(Refer to your ISP for more information)*.
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.
Data Encapsulation	Select the Data Encapsulation required by your ISP *(Refer to your ISP for more information)*.
VPI Number	Enter the VPI provided by your ISP *(This will usually be 8 for Australia or 0 for New Zealand)*
VCI Number	Enter the VCI provided by your ISP *(This will usually be 35 for Australia or 100 for New Zealand)*
Schedule Type	Select the data schedule type required by your ISP (Refer to your ISP for more information).
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.

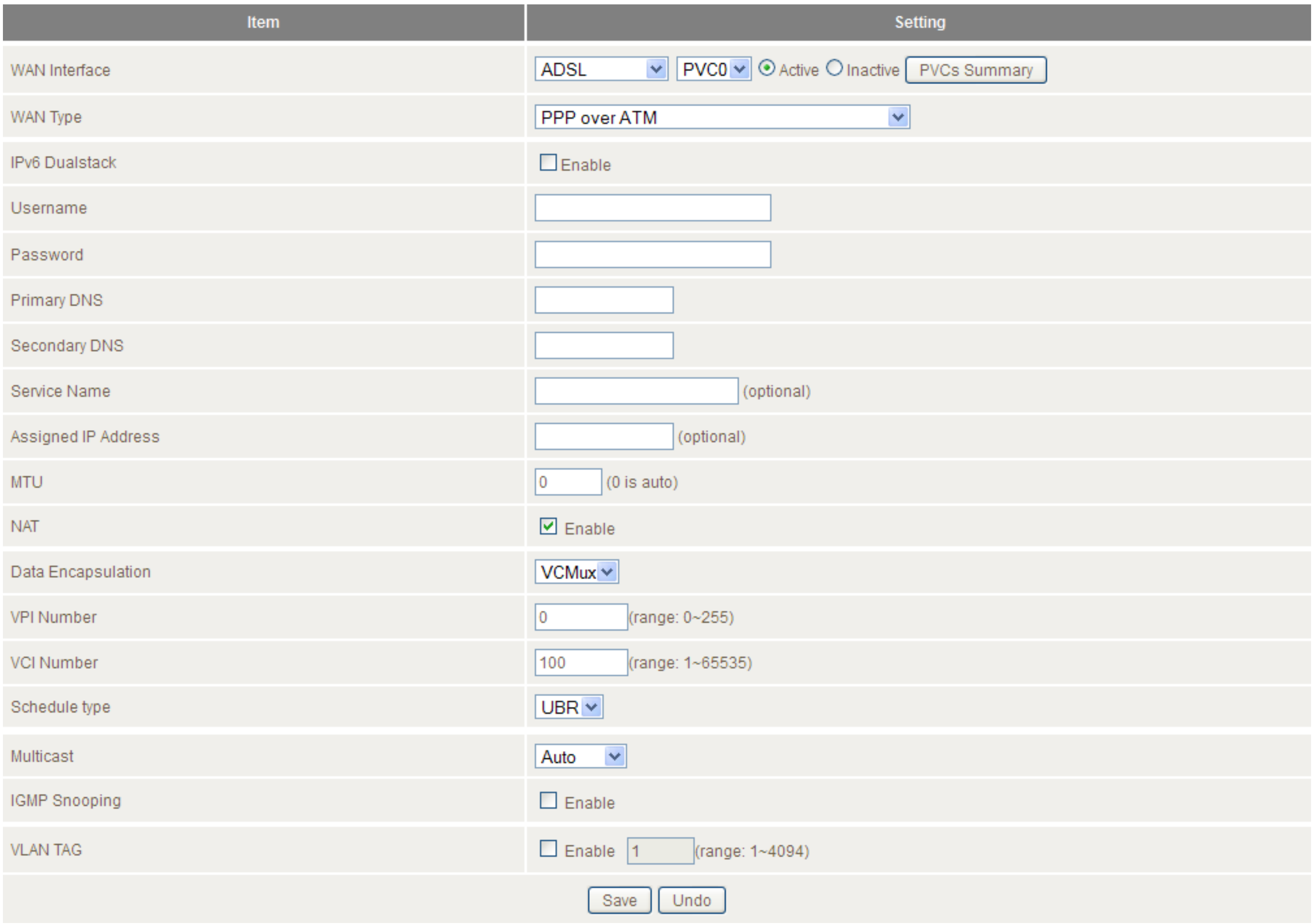
PPP over Ethernet



Item	Setting
WAN Interface	ADSL PVC0 ● Active ○ Inactive [PVCs Summary]
WAN Type	PPP over Ethernet
IPv6 Dualstack	□ Enable
Username	
Password	
Primary DNS	
Secondary DNS	
Service Name	(optional)
Assigned IP Address	(optional)
MTU	0 (0 is auto)
NAT	☑ Enable
Data Encapsulation	LLC
VPI Number	8 (range: 0~255)
VCI Number	35 (range: 1~65535)
Schedule type	UBR
Multicast	Auto
IGMP Snooping	□ Enable
VLAN TAG	□ Enable 1 (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.
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. *(For security, this field appears blank. If you don't want to change the password, leave it empty)*
Primary DNS	This feature allows you to manually assign a Primary DNS Server *(Optional - Refer to your ISP for more information)*.
Secondary DNS	This feature allows you to manually assign a Secondary DNS Server *(Optional - Refer to your ISP for more information)*.
Service Name	Enter the service name if your ISP requires it *(Optional - Refer to your ISP for more information)*.
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 *(Refer to your ISP for more information)*.
VPI Number	Enter the VPI provided by your ISP *(This will usually be 8 for Australia or 0 for New Zealand)*
VCI Number	Enter the VCI provided by your ISP *(This will usually be 35 for Australia or 100 for New Zealand)*
Schedule Type	Select the data schedule type required by your ISP (Refer to your ISP for more information).
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.

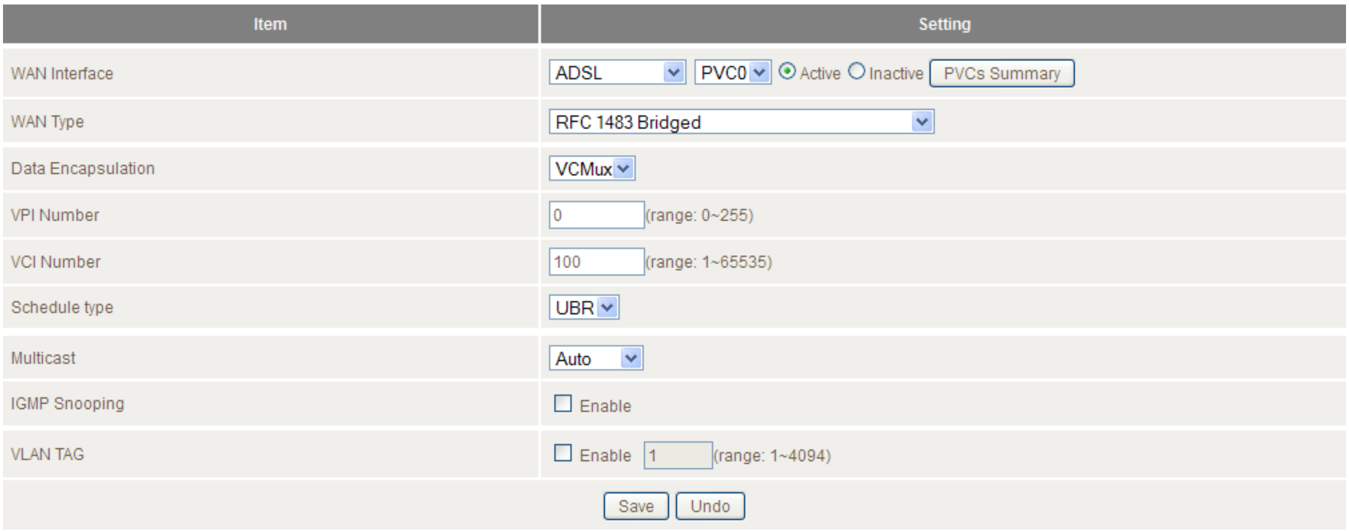
PPP over ATM



Item	Setting
WAN Interface	ADSL ▾ PVC0 ▾ ● Active ○ Inactive [PVCs Summary]
WAN Type	PPP over ATM ▾
IPv6 Dualstack	□ Enable
Username	
Password	
Primary DNS	
Secondary DNS	
Service Name	(optional)
Assigned IP Address	(optional)
MTU	0 (0 is auto)
NAT	☑ Enable
Data Encapsulation	VCMux ▾
VPI Number	0 (range: 0~255)
VCI Number	100 (range: 1~65535)
Schedule type	UBR ▾
Multicast	Auto ▾
IGMP Snooping	□ Enable
VLAN TAG	□ Enable 1 (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.
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. *(For security, this field appears blank. If you don't want to change the password, leave it empty)*
Primary DNS	This feature allows you to manually assign a Primary DNS Server *(Optional - Refer to your ISP for more information)*.
Secondary DNS	This feature allows you to manually assign a Secondary DNS Server *(Optional - Refer to your ISP for more information)*.
Service Name	Enter the service name if your ISP requires it *(Optional - Refer to your ISP for more information)*.
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 *(Refer to your ISP for more information)*.
VPI Number	Enter the VPI provided by your ISP *(This will usually be 8 for Australia or 0 for New Zealand)*
VCI Number	Enter the VCI provided by your ISP *(This will usually be 35 for Australia or 100 for New Zealand)*
Schedule Type	Select the data schedule type required by your ISP (Refer to your ISP for more information).
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



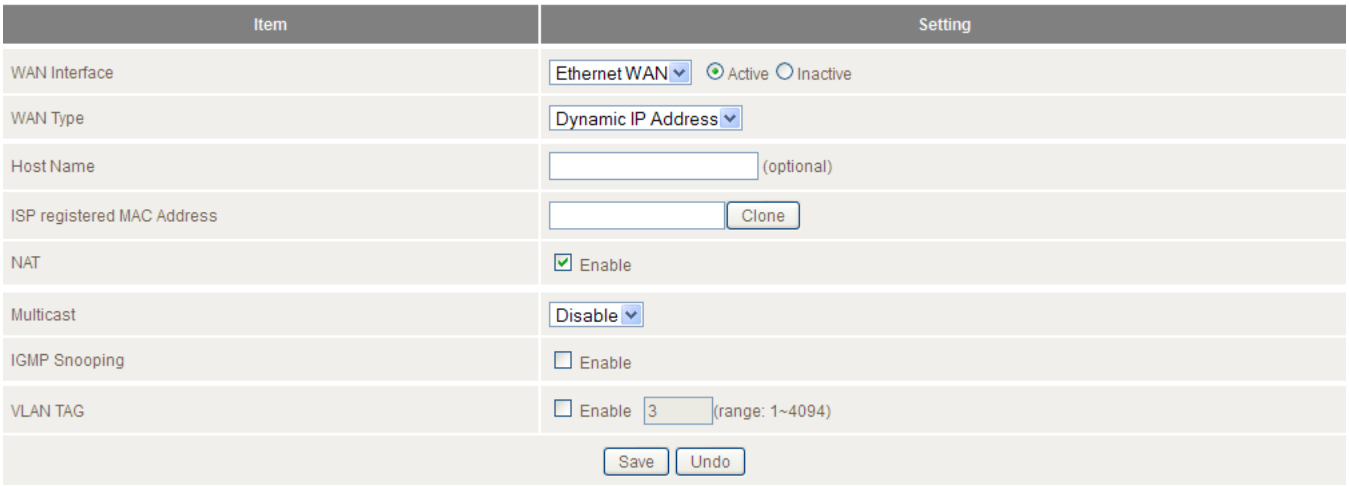
Item	Setting
WAN Interface	ADSL PVC0 ● Active ○ Inactive PVCs Summary
WAN Type	RFC 1483 Bridged
Data Encapsulation	VCMux
VPI Number	0 (range: 0~255)
VCI Number	100 (range: 1~65535)
Schedule type	UBR
Multicast	Auto
IGMP Snooping	□ Enable
VLAN TAG	□ Enable 1 (range: 1~4094)

Ethernet WAN

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

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

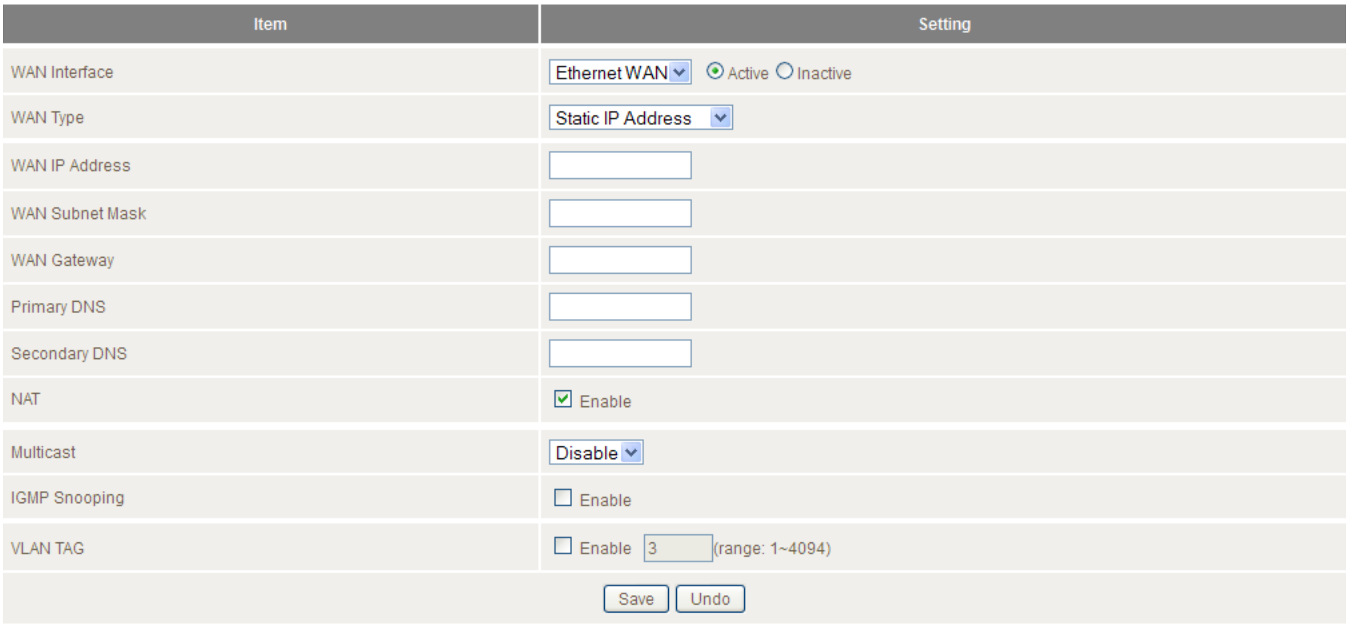
Dynamic IP Address



Item	Setting
WAN Interface	Ethernet WAN ● Active ○ Inactive
WAN Type	Dynamic IP Address
Host Name	(optional)
ISP registered MAC Address	Clone
NAT	☑ Enable
Multicast	Disable
IGMP Snooping	□ Enable
VLAN TAG	□ Enable 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.
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.

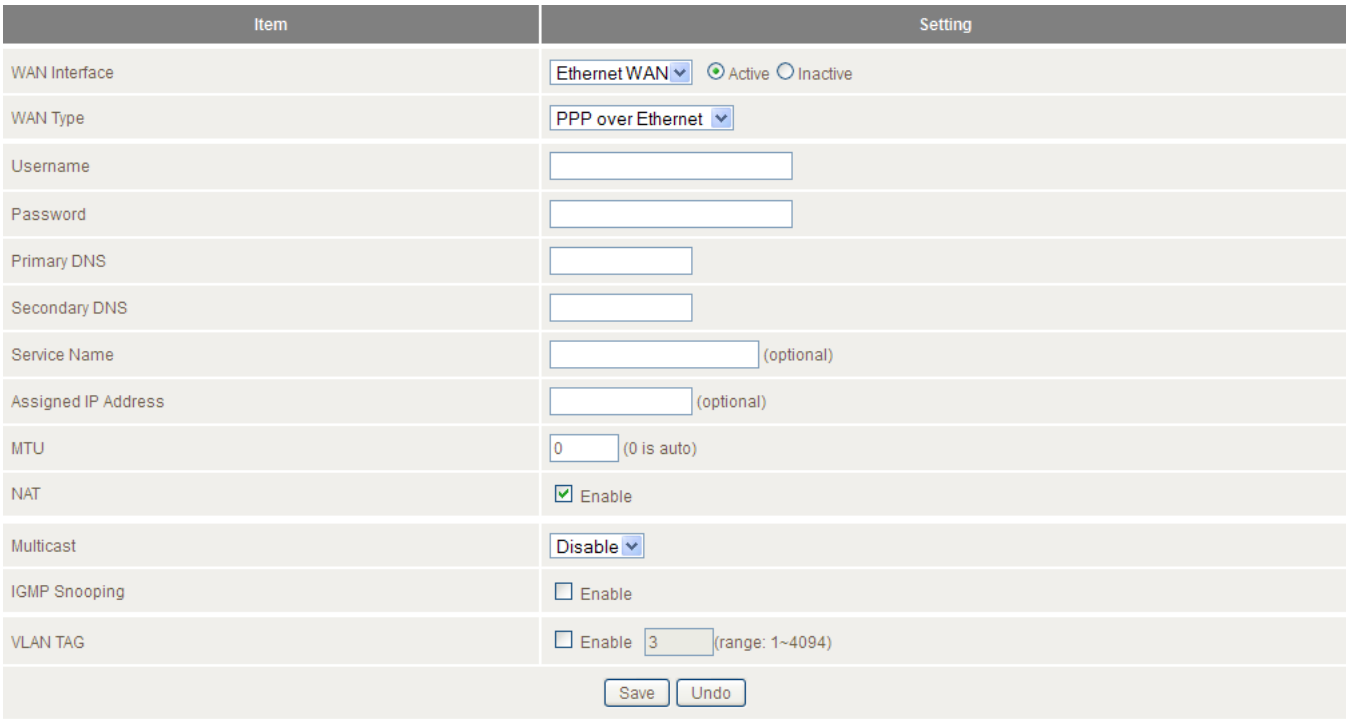
Static IP Address



Item	Setting
WAN Interface	Ethernet WAN ▾ ● Active ○ Inactive
WAN Type	Static IP Address ▾
WAN IP Address	
WAN Subnet Mask	
WAN Gateway	
Primary DNS	
Secondary DNS	
NAT	☑ Enable
Multicast	Disable ▾
IGMP Snooping	□ Enable
VLAN TAG	□ Enable 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 *(Optional - Refer to your ISP for more information)*.
Secondary DNS	This feature allows you to manually assign a Secondary DNS Server *(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.

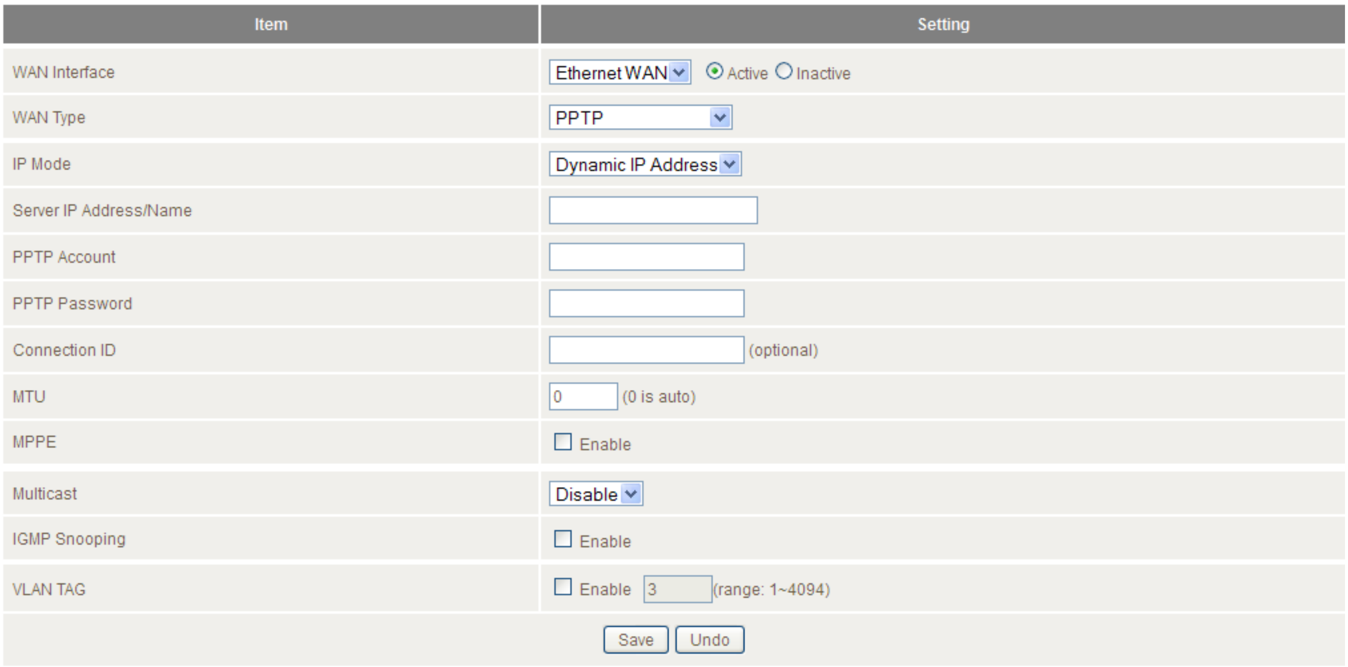
PPP over Ethernet



Item	Setting
WAN Interface	Ethernet WAN ● Active ○ Inactive
WAN Type	PPP over Ethernet
Username	
Password	
Primary DNS	
Secondary DNS	
Service Name	(optional)
Assigned IP Address	(optional)
MTU	0 (0 is auto)
NAT	☑ Enable
Multicast	Disable
IGMP Snooping	□ Enable
VLAN TAG	□ Enable 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 *(Optional - Refer to your ISP for more information)*.
Secondary DNS	This feature allows you to manually assign a Secondary DNS Server *(Optional - Refer to your ISP for more information)*.
Service Name	Enter the service name if your ISP requires it *(Optional - Refer to your ISP for more information)*.
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.

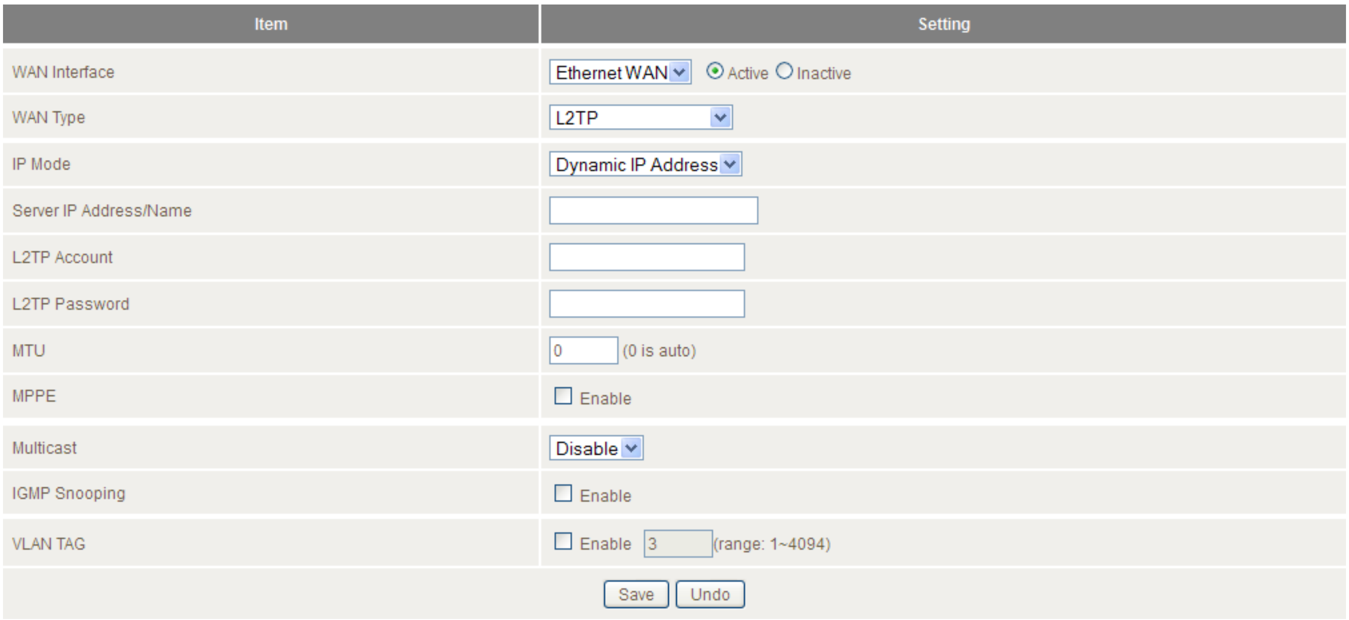
PPTP



Item	Setting
WAN Interface	Ethernet WAN ▾ ● Active ○ Inactive
WAN Type	PPTP ▾
IP Mode	Dynamic IP Address ▾
Server IP Address/Name	
PPTP Account	
PPTP Password	
Connection ID	(optional)
MTU	0 (0 is auto)
MPPE	□ Enable
Multicast	Disable ▾
IGMP Snooping	□ Enable
VLAN TAG	□ Enable 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 *(Refer to your PPTP administrator for more information)*.
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



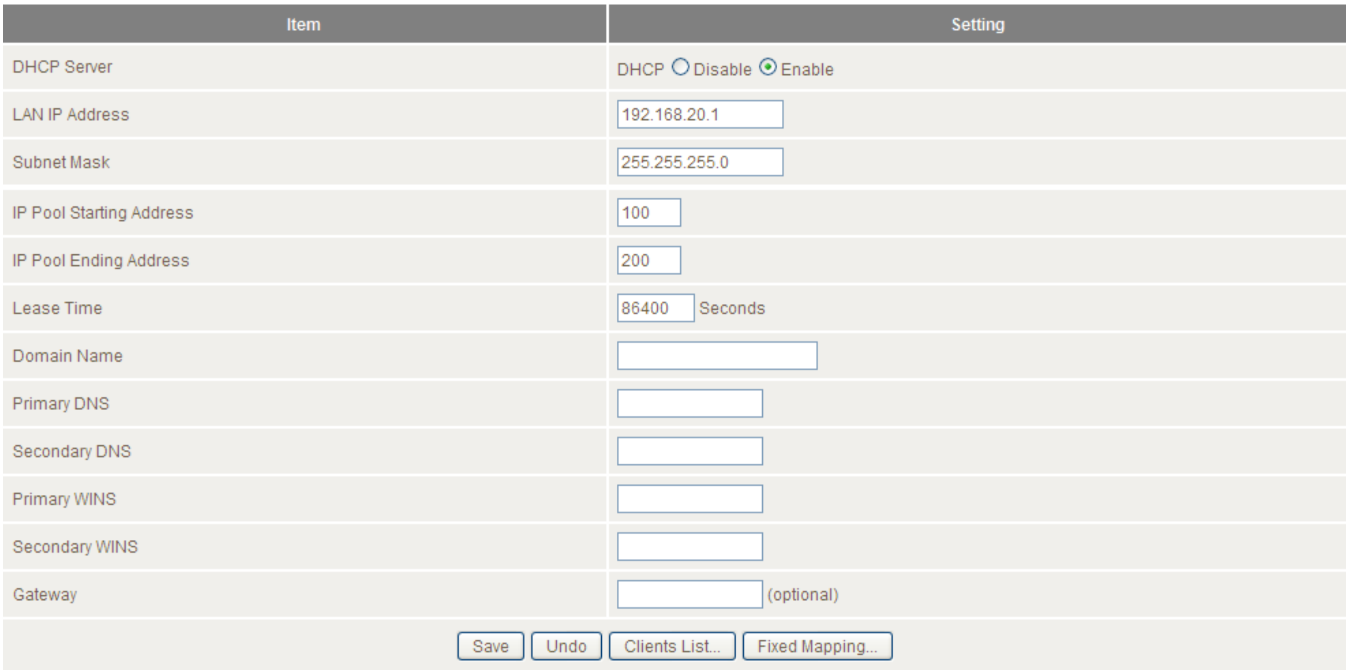
Item	Setting
WAN Interface	Ethernet WAN ● Active ○ Inactive
WAN Type	L2TP
IP Mode	Dynamic IP Address
Server IP Address/Name	
L2TP Account	
L2TP Password	
MTU	0 (0 is auto)
MPPE	□ Enable
Multicast	Disable
IGMP Snooping	□ Enable
VLAN TAG	□ Enable 3 (range: 1~4094)

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 *(Refer to your PPTP administrator for more information)*.
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 CLAN 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 NB16DG. The DHCP Server enables computers or devices connecting to the NB16DG 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 ○ Disable ● Enable
LAN IP Address	192.168.20.1
Subnet Mask	255.255.255.0
IP Pool Starting Address	100
IP Pool Ending Address	200
Lease Time	86400 Seconds
Domain Name	
Primary DNS	
Secondary DNS	
Primary WINS	
Secondary WINS	
Gateway	(optional)

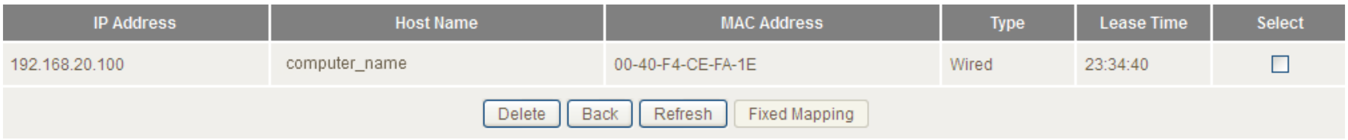
OPTION	DEFINITION
DHCP Server	Enable or disable the DHCP server.
LAN IP Address	The local IP address of the NB16DG. *(The computers on your network must use this IP address as their Default Gateway. You can change it if necessary.)*
Subnet Mask	Enter the subnet mask for use on the local network. This 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.

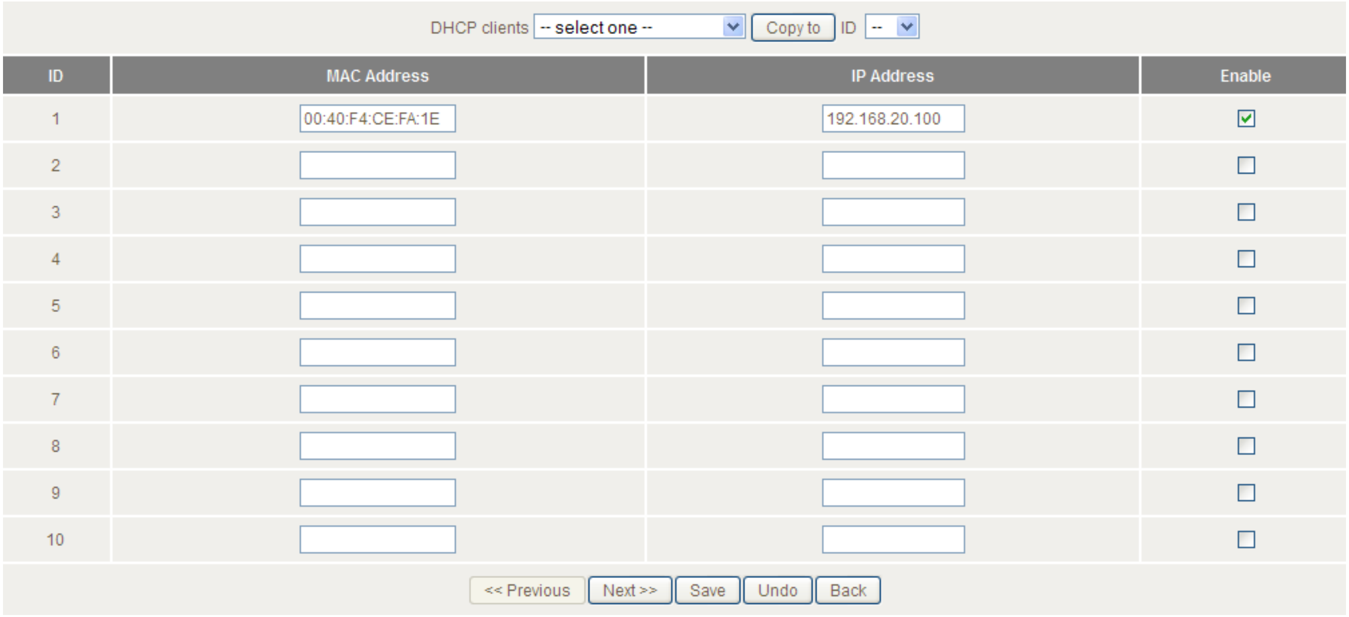


IP Address	Host Name	MAC Address	Type	Lease Time	Select
192.168.20.100	computer_name	00-40-F4-CE-FA-1E	Wired	23:34:40	□

If you wish to set a permanent IP address for a particular DHCP client (or device), select the appropriate DHCP client by clicking in the "Select" box. This will ensure the clients current IP address is always assigned to it.

DHCP Fixed Mapping

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



DHCP clients -- select one -- Copy to ID --

ID	MAC Address	IP Address	Enable
1	00:40:F4:CE:FA:1E	192.168.20.100	☑
2			□
3			□
4			□
5			□
6			□
7			□
8			□
9			□
10			□

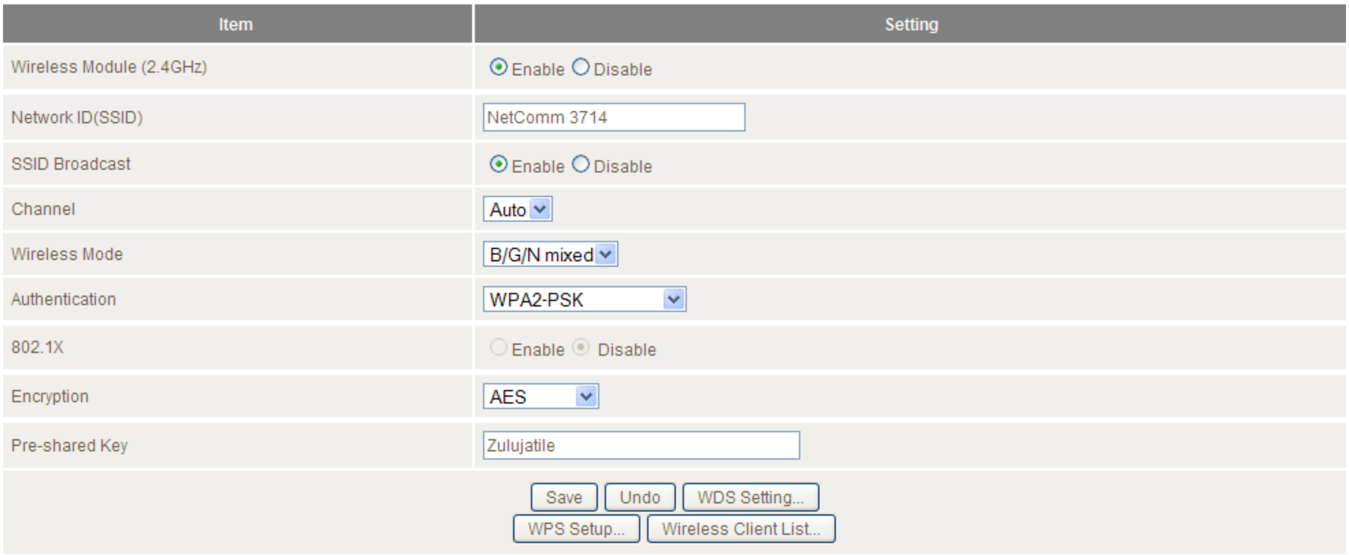
The DHCP Server will reserve a specific IP for a device based on that device’s unique MAC address.

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.

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)	● Enable ○ Disable
Network ID(SSID)	NetComm 3714
SSID Broadcast	● Enable ○ Disable
Channel	Auto
Wireless Mode	B/G/N mixed
Authentication	WPA2-PSK
802.1X	○ Enable ● Disable
Encryption	AES
Pre-shared Key	Zulujatile

OPTION	DEFINITION
Wireless Module (2.4GHz)	Select to enable or disable the 2.4GHz Wireless network function of the NB16DG.
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. *(Please refer to the included Wireless Security Card insert for your default SSID)*
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. *(The factory default setting is B/G/N mixed)*
Authentication	
Authentication	You may select from the following authentication types to secure your wireless network: ▪ Open ▪ Shared ▪ Auto ▪ WPA ▪ WPA-PSK ▪ WPA2 ▪ WPA2-PSK ▪ WPA/WPA2 ▪ WPA-PSK/WPA2-PSK. 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. Please enter the key in the “Preshare Key”. The key needs to be more than 8 characters and less than 63 characters. It can be any combination of letters and numbers. (Please refer to the included Wireless Security Card insert for your default WPA-PSK2 key)
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

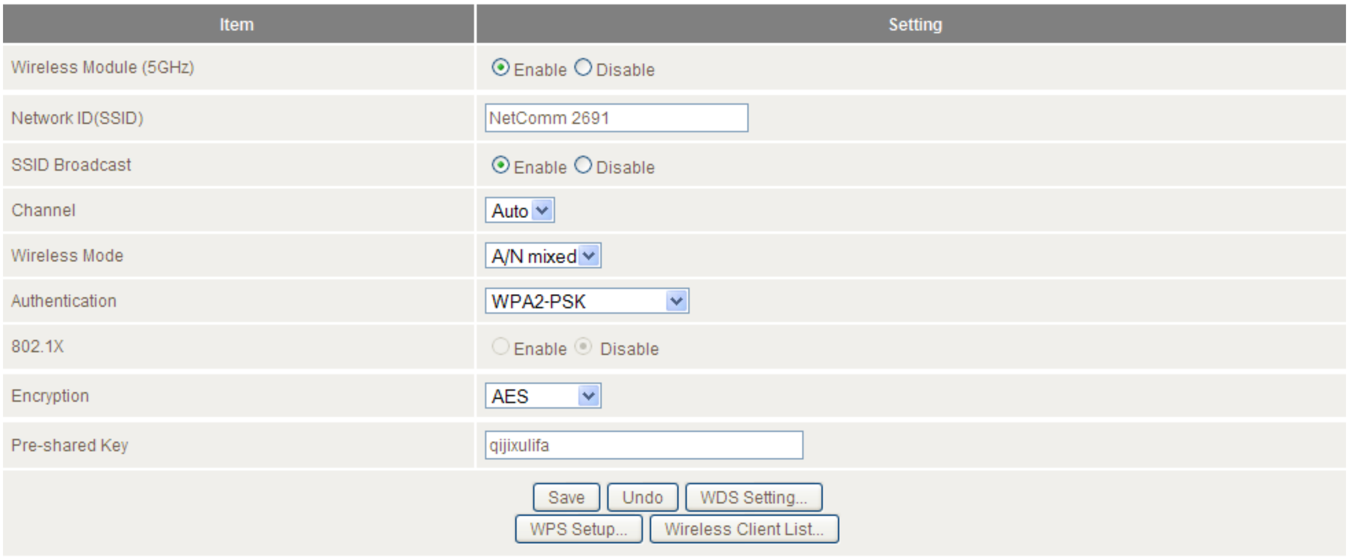
After configuring wireless security, you also need to configure your wireless adapter to use the same security settings before you can connect wirelessly. Not all wireless adapters support WPA-PSK/WPA2-PSK/WPA/WPA2 security. Please refer to your wireless adapter user guide for more information.

It is strongly recommended that you set up wireless security such as WPA-PSK (when the wireless client supports WPA) 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.

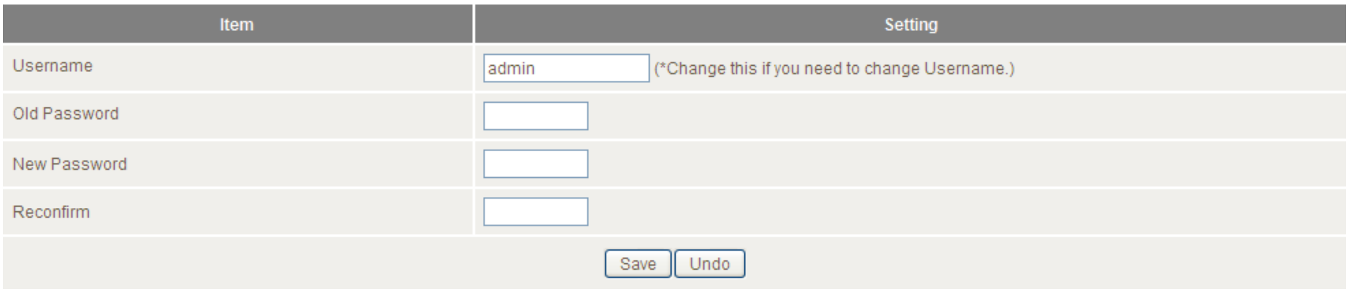


Item	Setting
Wireless Module (5GHz)	● Enable ○ Disable
Network ID(SSID)	NetComm 2691
SSID Broadcast	● Enable ○ Disable
Channel	Auto
Wireless Mode	A/N mixed
Authentication	WPA2-PSK
802.1X	○ Enable ● Disable
Encryption	AES
Pre-shared Key	qijixulifa

OPTION	DEFINITION
Wireless Module (5GHz)	Select to enable or disable the 5GHz Wireless network function of the NB16DG.
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. *(Please refer to the included Wireless Security Card insert for your default SSID)*
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. *(The factory default setting is A/N Mixed)*
Authentication	You may select from the following authentication types to secure your wireless network: ▪ Open ▪ Shared ▪ Auto ▪ WPA ▪ WPA-PSK ▪ WPA2 ▪ WPA2-PSK ▪ WPA/WPA2 ▪ WPA-PSK/WPA2-PSK. 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. Please enter the key in the “Preshare Key”. The key needs to be more than 8 characters and less than 63 characters. It can be any combination of letters and numbers. (Please refer to the included Wireless Security Card insert for your default WPA-PSK2 key)
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.

Change Password

This page allows you to change the NB16DG web configuration password.



Item	Setting
Username	admin (*Change this if you need to change Username.)
Old Password	
New Password	
Reconfirm	

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**.

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:

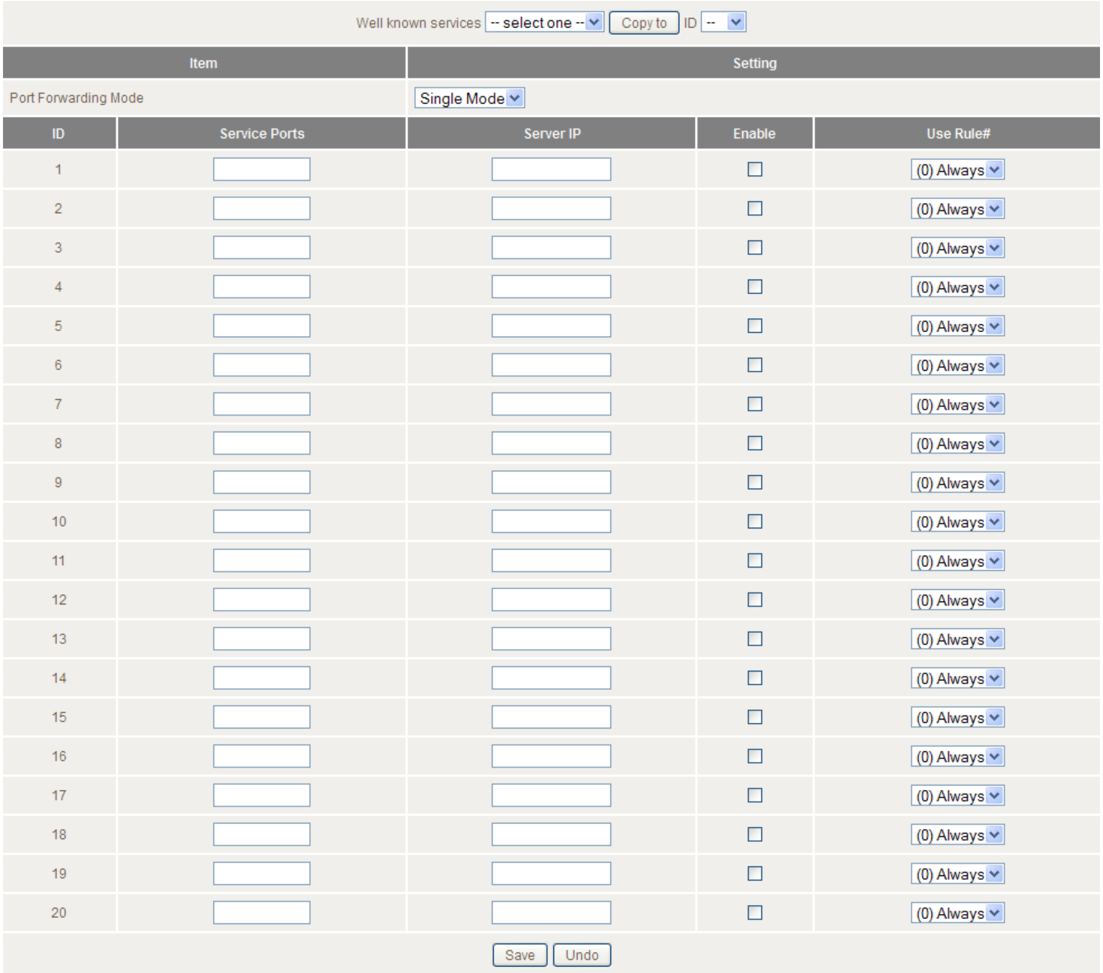
- Port Forwarding
- Port Triggering
- DMZ Host

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 --] Copy to ID [--]

Item	Setting
Port Forwarding Mode	Single Mode

ID	Service Ports	Server IP	Enable	Use Rule#
1			□	(0) Always
2			□	(0) Always
3			□	(0) Always
4			□	(0) Always
5			□	(0) Always
6			□	(0) Always
7			□	(0) Always
8			□	(0) Always
9			□	(0) Always
10			□	(0) Always
11			□	(0) Always
12			□	(0) Always
13			□	(0) Always
14			□	(0) Always
15			□	(0) Always
16			□	(0) Always
17			□	(0) Always
18			□	(0) Always
19			□	(0) Always
20			□	(0) Always

Save Undo

For example, if you have an FTP server (the default port is 21) at 192.168.1.10, a Web server (the default port is 80) at 192.168.20.40, and a VPN server (the default port is 1723) at 192.168.20.60, then you would need to specify the following virtual server mappings:

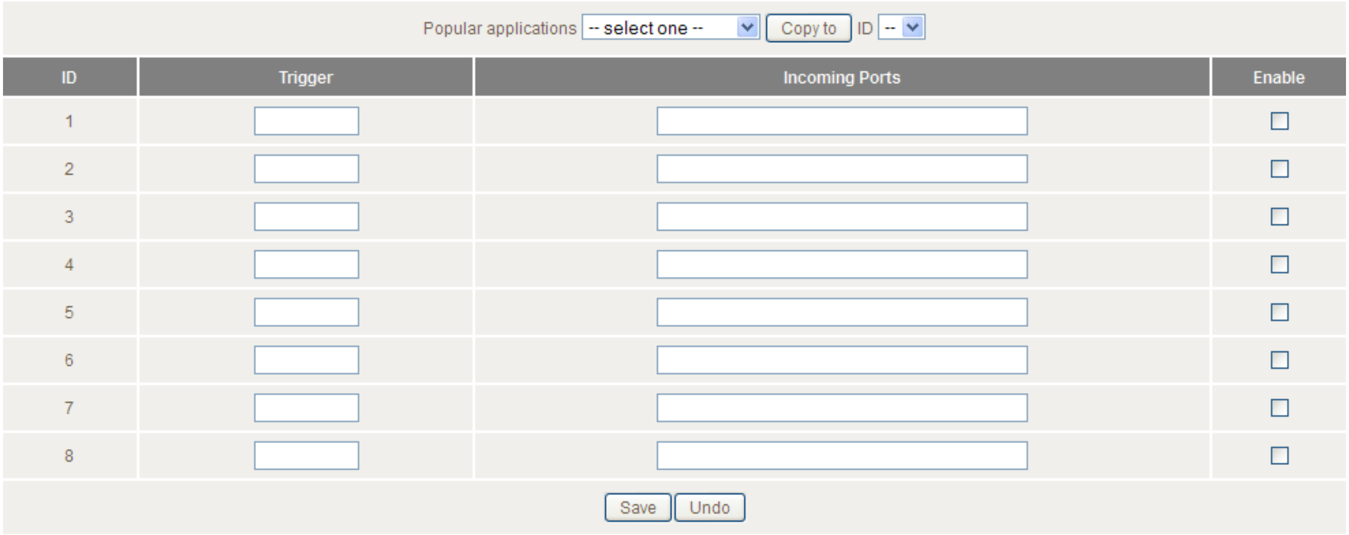
Note: At any given time, only one IP address can be bound to a particular Service Port.

SERVICE PORT	SERVER IP	ENABLE	USE RULE#
21	12.168.1.10	✓	(0) Always
80	192.168.20.40	✓	(0) Always
1723	192.168.20.60	✓	(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 NB16DG.



ID	Trigger	Incoming Ports	Enable
1			□
2			□
3			□
4			□
5			□
6			□
7			□
8			□

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

Note: If this fails to make the application work, try to configure that computer as the DMZ host instead.

(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.
Enable	Select to enable or disable the configured special application entry.

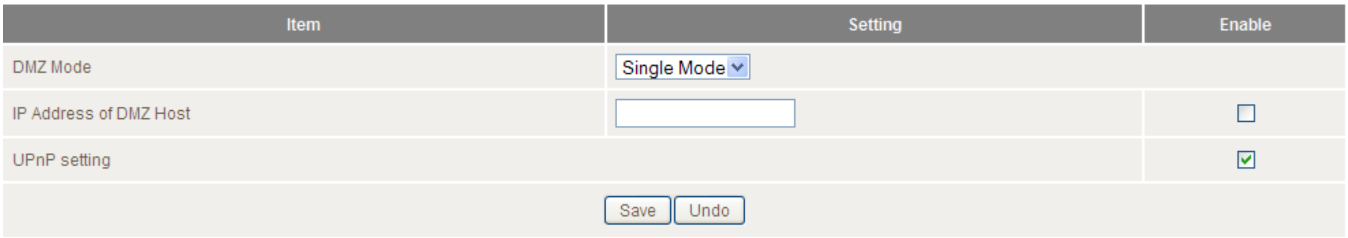
The NB16DG also provides predefined settings for some popular applications.

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.



Item	Setting	Enable
DMZ Mode	Single Mode	
IP Address of DMZ Host		□
UPnP setting		☑

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.

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 also supports UPnP. If the DMZ host operating system supports this function enable it to automatically configure the required network settings.

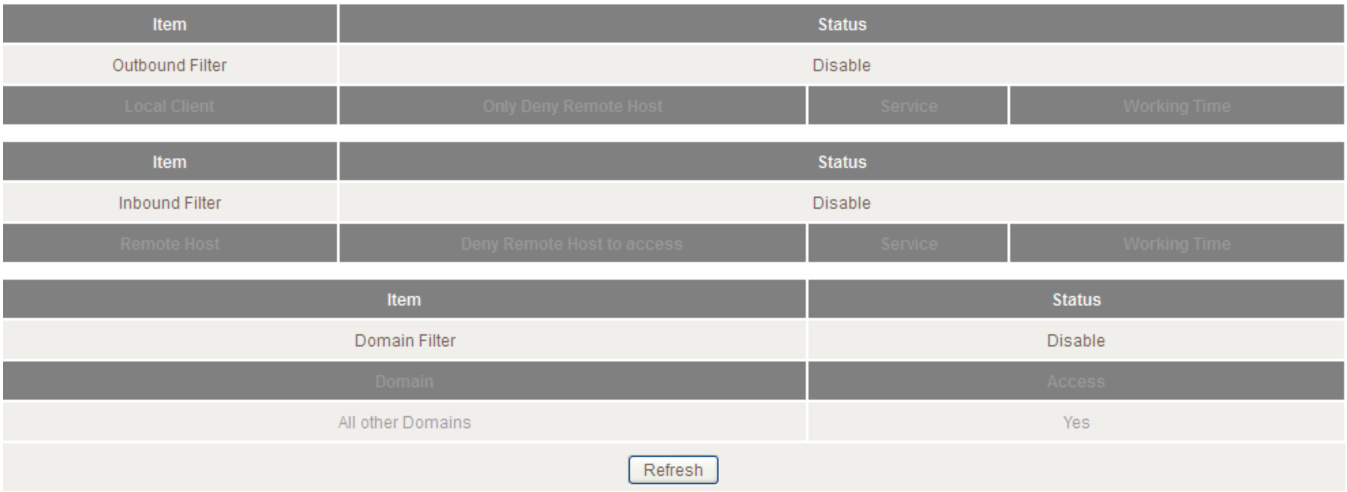
Click **Save** to save the settings or **Undo** to cancel.

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

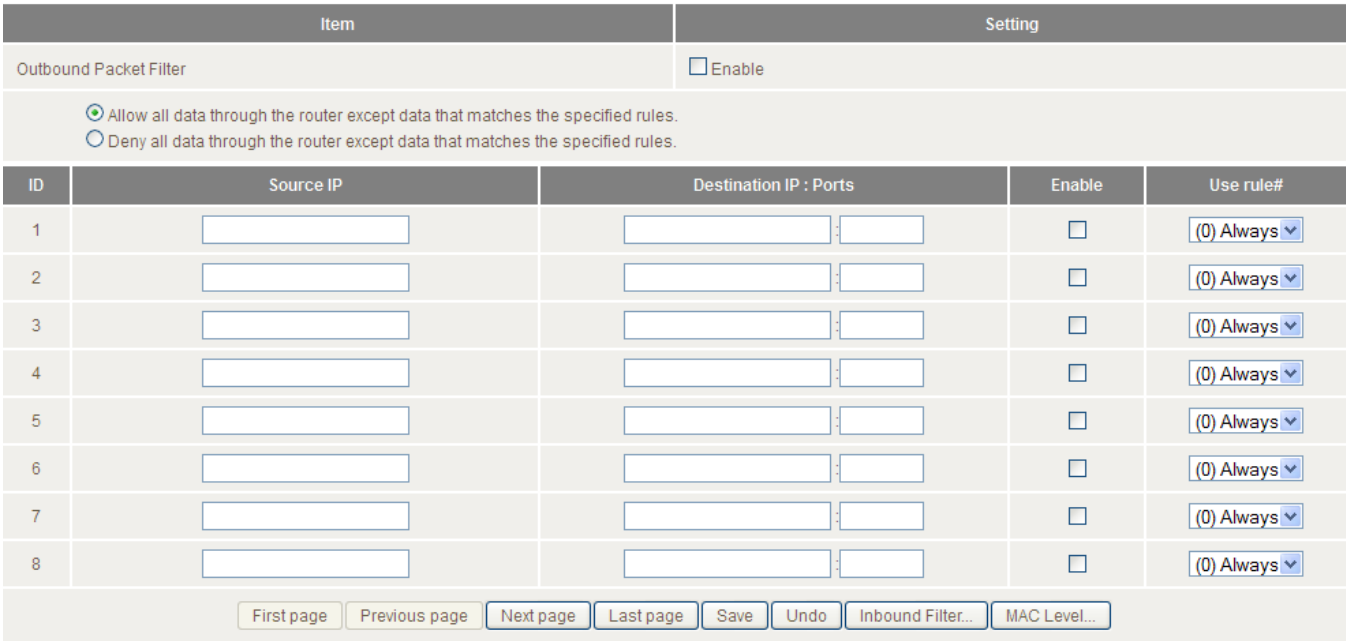
Packet Filters

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 Virtual Server or DMZ host only.

Note: 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	□ Enable

● Allow all data through the router except data that matches the specified rules.
○ Deny all data through the router except data that matches the specified rules.

ID	Source IP	Destination IP : Ports	Enable	Use rule#
1		:	□	(0) Always
2		:	□	(0) Always
3		:	□	(0) Always
4		:	□	(0) Always
5		:	□	(0) Always
6		:	□	(0) Always
7		:	□	(0) Always
8		:	□	(0) Always

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.

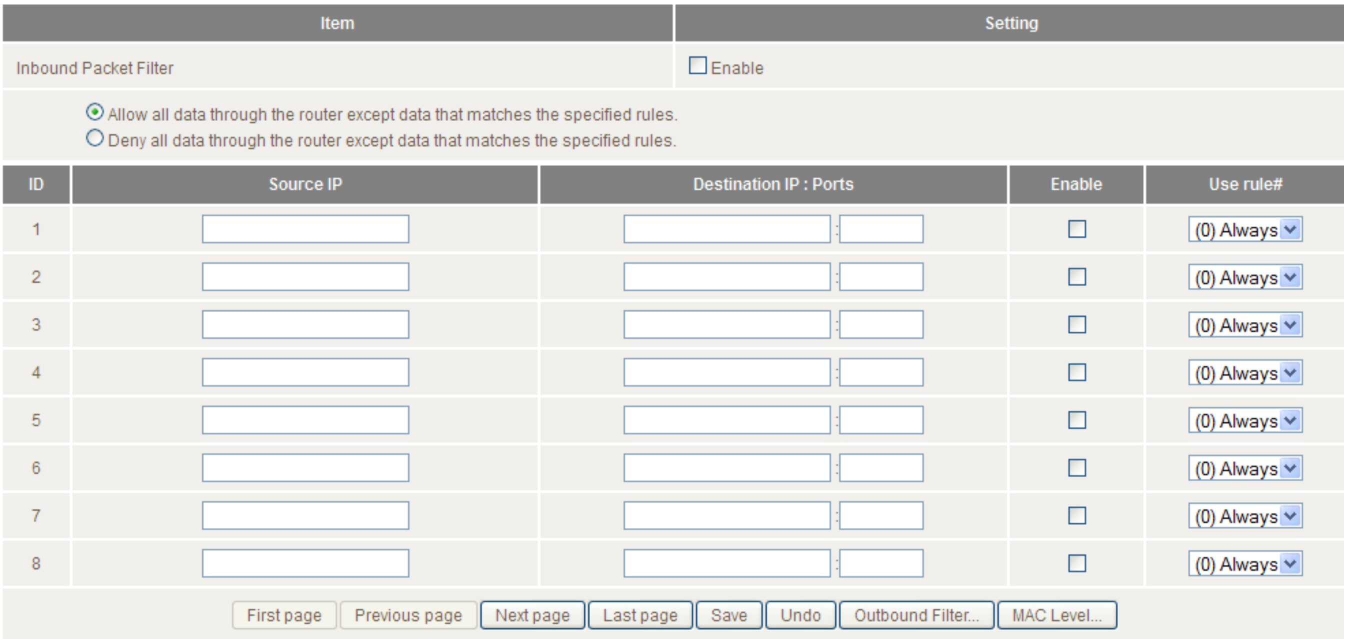
The Packet Filter also works with Scheduling Rules, and gives you more flexibility on Access control.

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	□ Enable

● Allow all data through the router except data that matches the specified rules.
○ Deny all data through the router except data that matches the specified rules.

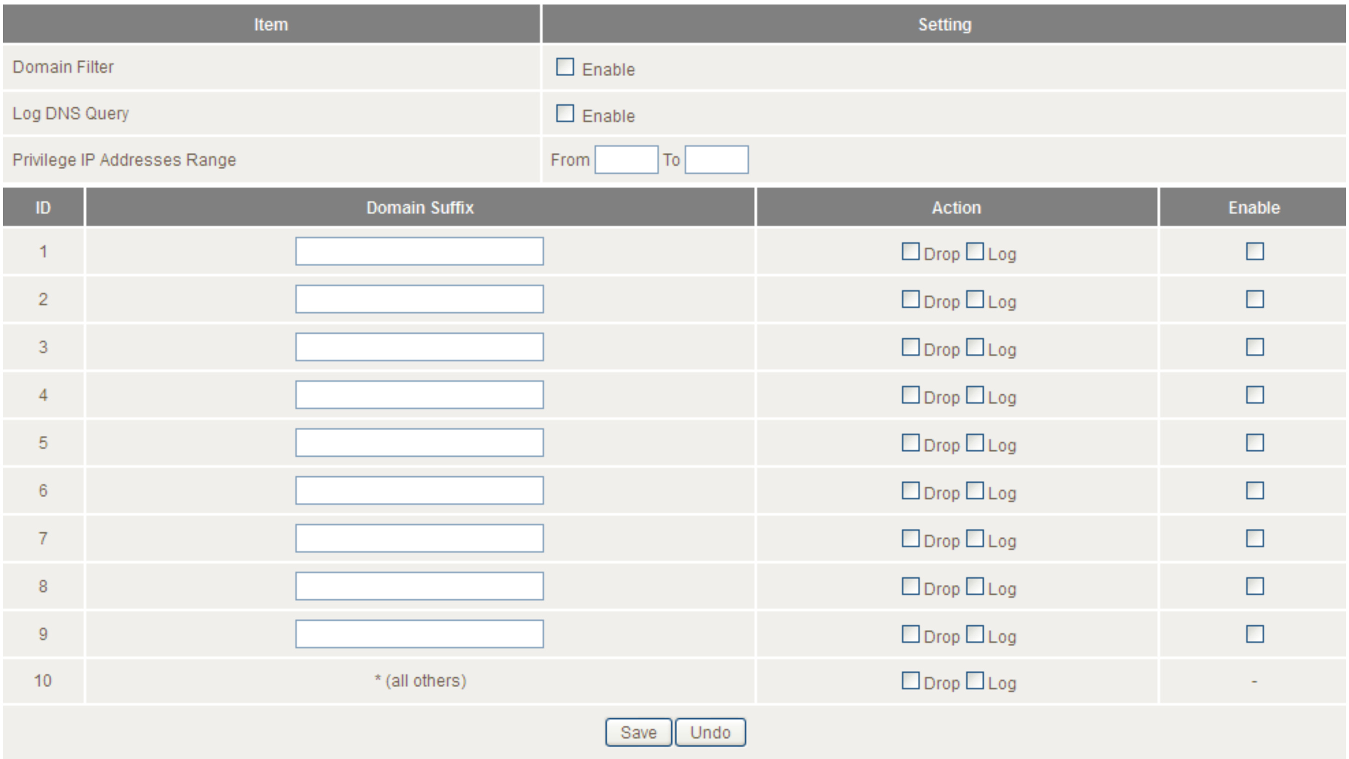
ID	Source IP	Destination IP : Ports	Enable	Use rule#
1		:	□	(0) Always
2		:	□	(0) Always
3		:	□	(0) Always
4		:	□	(0) Always
5		:	□	(0) Always
6		:	□	(0) Always
7		:	□	(0) Always
8		:	□	(0) Always

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	□ Enable
Log DNS Query	□ Enable
Privilege IP Addresses Range	From ▭ To ▭

ID	Domain Suffix	Action	Enable
1	▭	□ Drop □ Log	□
2	▭	□ Drop □ Log	□
3	▭	□ Drop □ Log	□
4	▭	□ Drop □ Log	□
5	▭	□ Drop □ Log	□
6	▭	□ Drop □ Log	□
7	▭	□ Drop □ Log	□
8	▭	□ Drop □ Log	□
9	▭	□ Drop □ Log	□
10	* (all others)	□ Drop □ 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

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

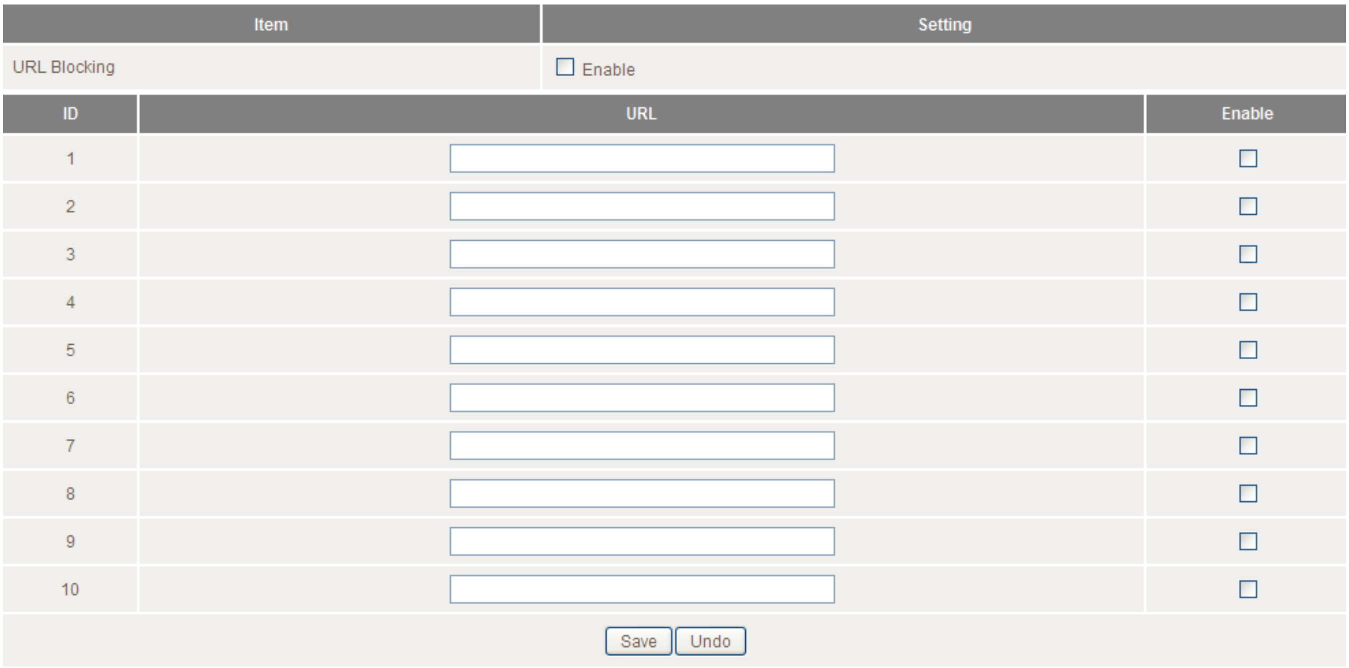
OPTION	DEFINITION
Domain Suffix	Please type the suffix of the URL that needs to be restricted. For example, ".com", "xxx. com".
Action	The router action that you want when someone is accessing a URL that matches the specified domain suffix. Select Drop to block the access and/or select Log to log this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

ID	URL	Enable
1		□
2		□
3		□
4		□
5		□
6		□
7		□
8		□
9		□
10		□

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

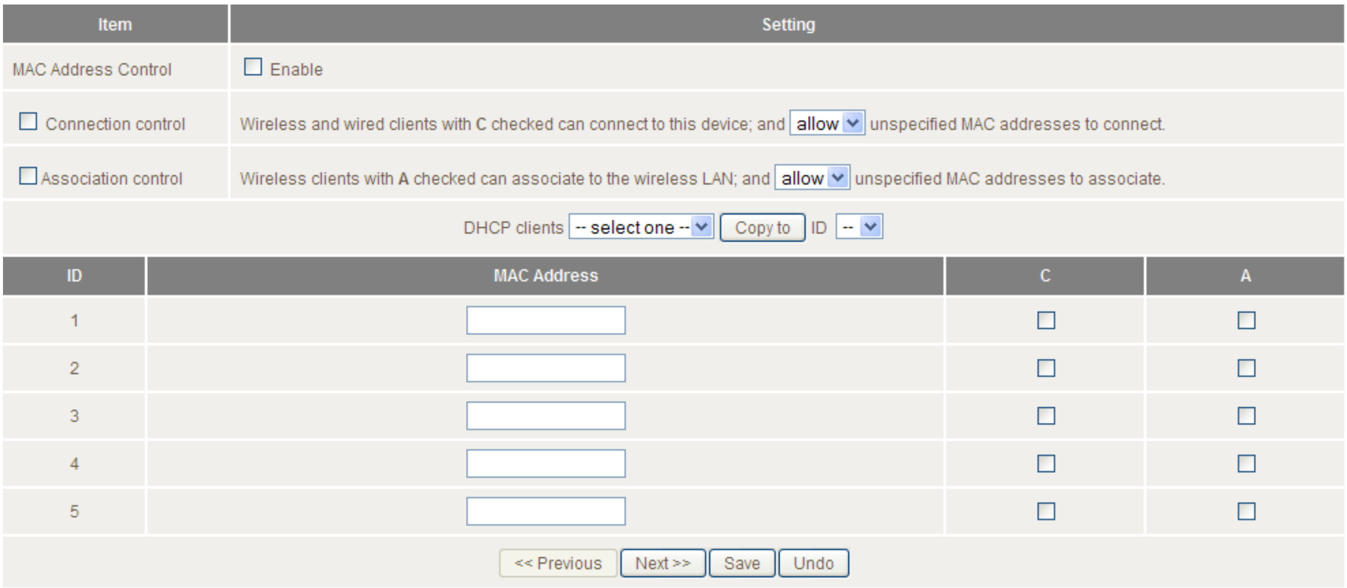
OPTION	DEFINITION
URL	If any part of the Website's URL matches the pre-defined word then the connection will be blocked. For example, you can use pre-defined word "sex" to block all websites if their URLs contain the pre-defined word "sex".
Enable	Tick to enable the rule.

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

MAC Control

MAC Control allows you to assign different access rights for different users and to assign a specific IP address to a specific MAC address.

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



Item	Setting
MAC Address Control	□ Enable
□ Connection control	Wireless and wired clients with **C** checked can connect to this device; and allow unspecified MAC addresses to connect.
□ Association control	Wireless clients with **A** checked can associate to the wireless LAN; and allow unspecified MAC addresses to associate.

DHCP clients -- select one -- [Copy to] ID --

ID	MAC Address	C	A
1		□	□
2		□	□
3		□	□
4		□	□
5		□	□

Two types of MAC Control are available:

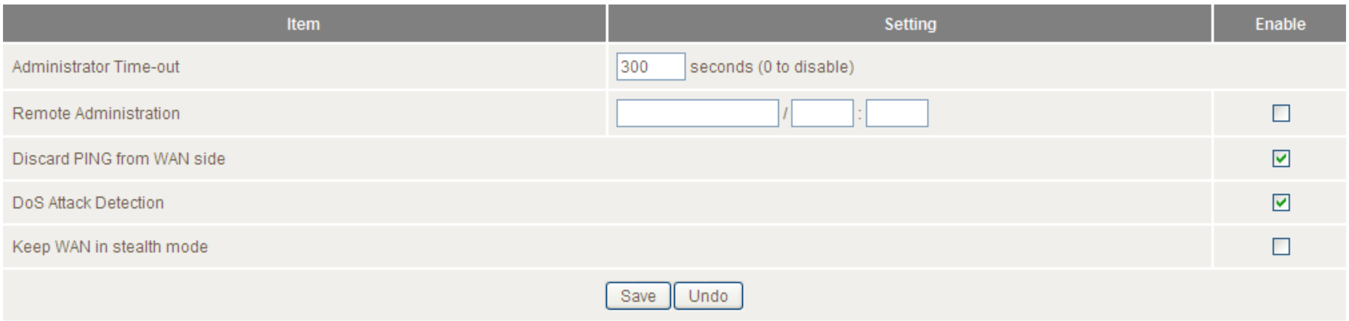
OPTION	DEFINITION
Connection control (C column)	Use this to control which clients (wired and wireless) can connect to the unit. If a client is denied access to connect to this device, it means the client cannot access the Internet either. Choose to allow or deny clients with MAC addresses that are not 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. 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

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	300 seconds (0 to disable)	
Remote Administration	/ :	□
Discard PING from WAN side		☑
DoS Attack Detection		☑
Keep WAN in stealth mode		□

OPTION	DEFINITION
Administrator Time-out	The period of time with no activity in the web configuration page to logout automatically, set this to zero to disable this feature.
Remote Administrator Host/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.

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 80.

You can also change the web server port. When enabled, the router can detect the following (and more) DoS attack types:

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

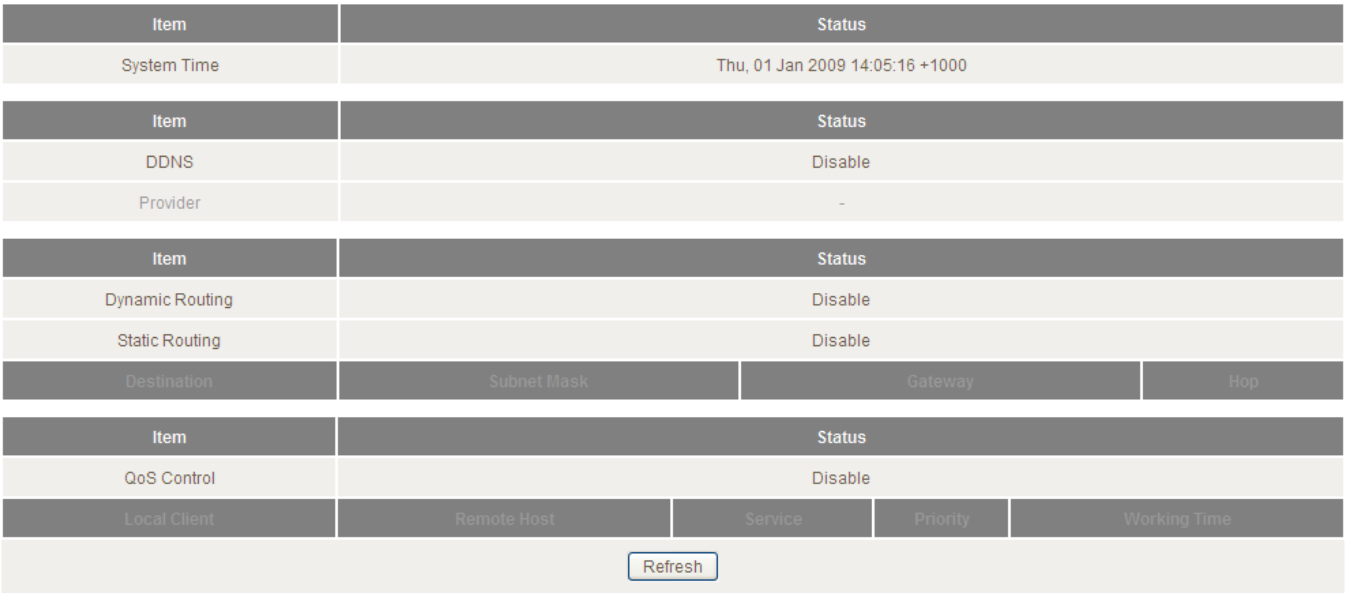
Click **Save** to save the settings or **Undo** to cancel.

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

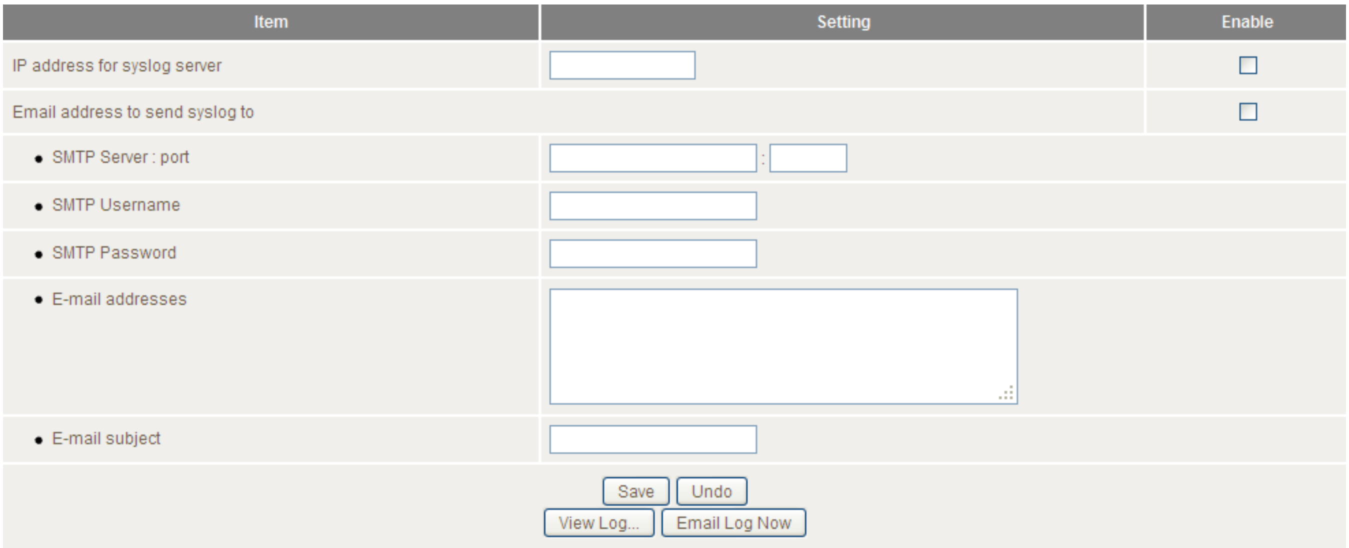
Destination	Subnet Mask	Gateway	Hop

Item	Status
QoS Control	Disable

Local Client	Remote Host	Service	Priority	Working Time

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		□
Email address to send syslog to		□
• SMTP Server : port	:	
• SMTP Username		
• SMTP Password		
• E-mail addresses		
• E-mail subject		

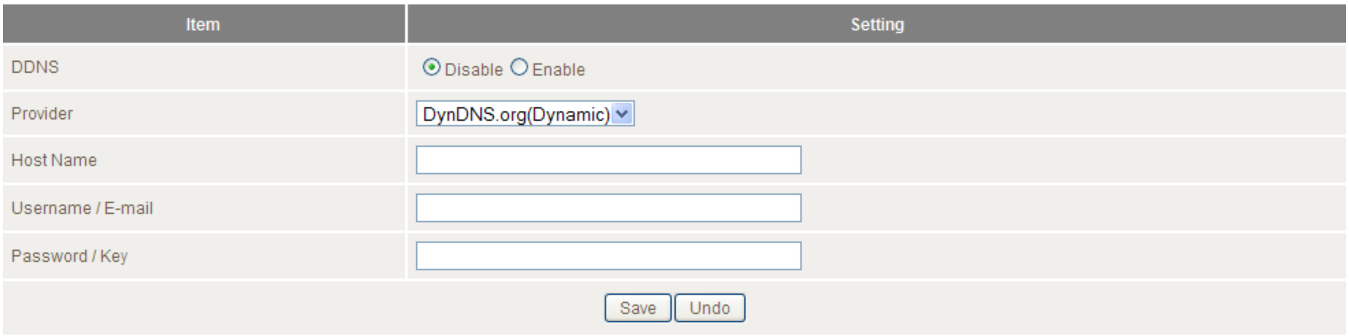
OPTION	DEFINITION
IP Address for remote System Logs (syslog)	The IP address of the syslog server where the system log data will be sent. Click the "Enable" checkbox to enable this function.
Email address to send syslog to	Click the “Enable” checkbox to enable this function.
SMTP Server : port	Enter the IP address or fully qualified domain name (FQDN) and port for the selected email server.
SMTP Username	The SMTP username required to send email *(if required)*.
SMTP Password	The SMTP password required to send email *(if required)*.
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	● Disable ○ Enable
Provider	DynDNS.org(Dynamic)
Host Name	
Username / E-mail	
Password / Key	

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

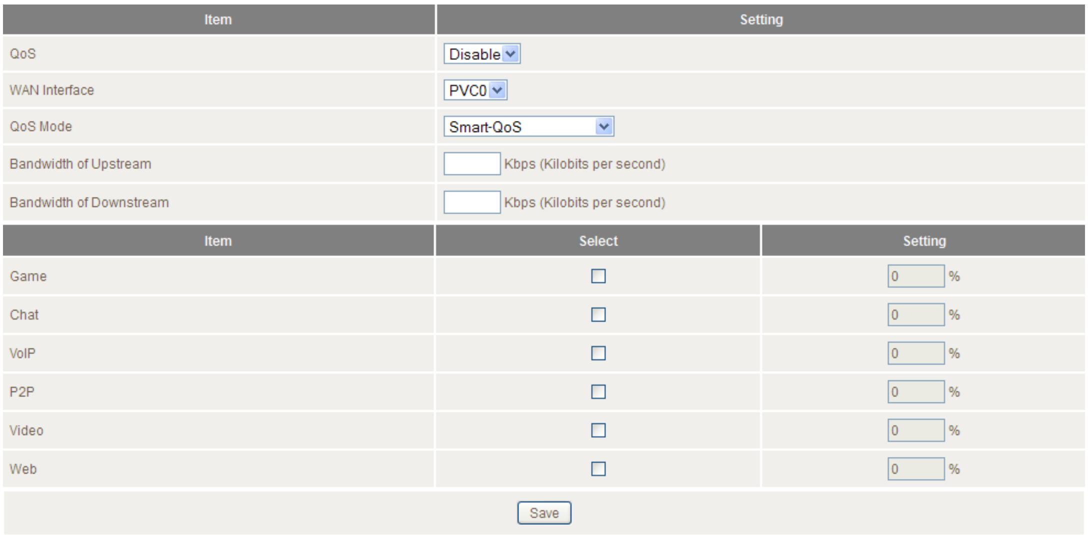
- Host Name
- Username/Email
- Password/Key

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.



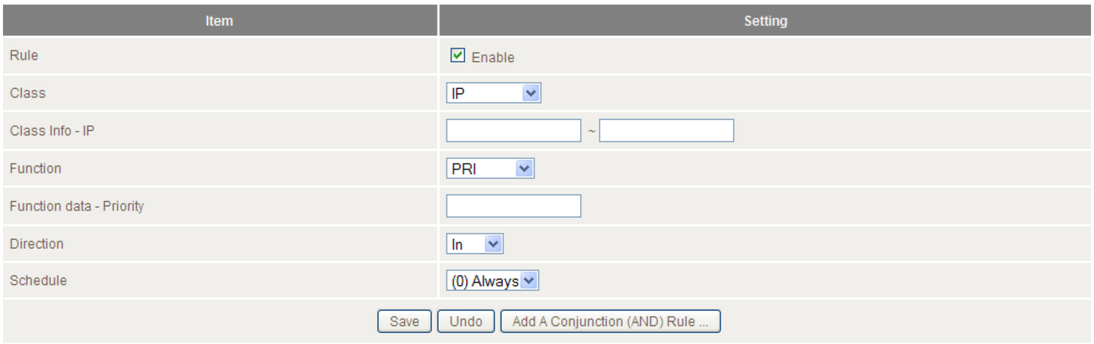
Item	Setting
QoS	Disable
WAN Interface	PVC0
QoS Mode	Smart-QoS
Bandwidth of Upstream	Kbps (Kilobits per second)
Bandwidth of Downstream	Kbps (Kilobits per second)

Item	Select	Setting
Game	□	0 %
Chat	□	0 %
VoIP	□	0 %
P2P	□	0 %
Video	□	0 %
Web	□	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 devide 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	☑ Enable
Class	IP
Class Info - IP	~
Function	PRI
Function data - Priority	
Direction	In
Schedule	(0) Always

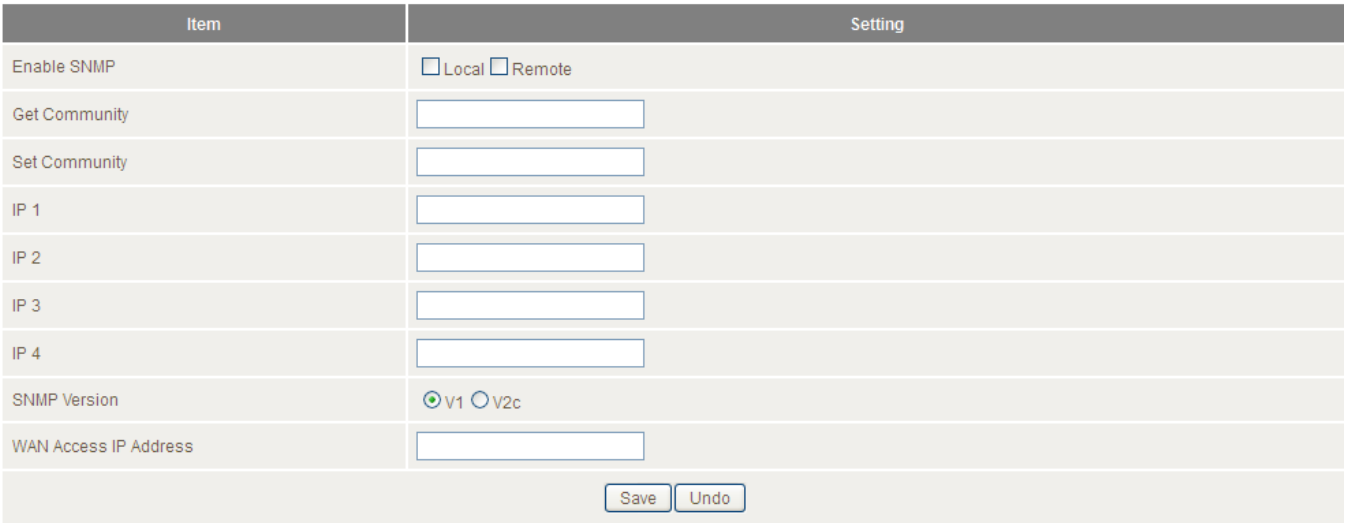
OPTION	DEFINITION
Rule	Select to enable or disable the QoS rule.
Class	Select the class of traffic you would like to prioritise.
Class Info	Enter the range of IP addresses of the class.
Function	Select the function of the rule. You can select from Priority, Max Rate, Session, Drop, Log or Alert.
Function 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	□ Local □ Remote
Get Community	
Set Community	
IP 1	
IP 2	
IP 3	
IP 4	
SNMP Version	● V1 ○ V2c
WAN Access IP Address	

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.

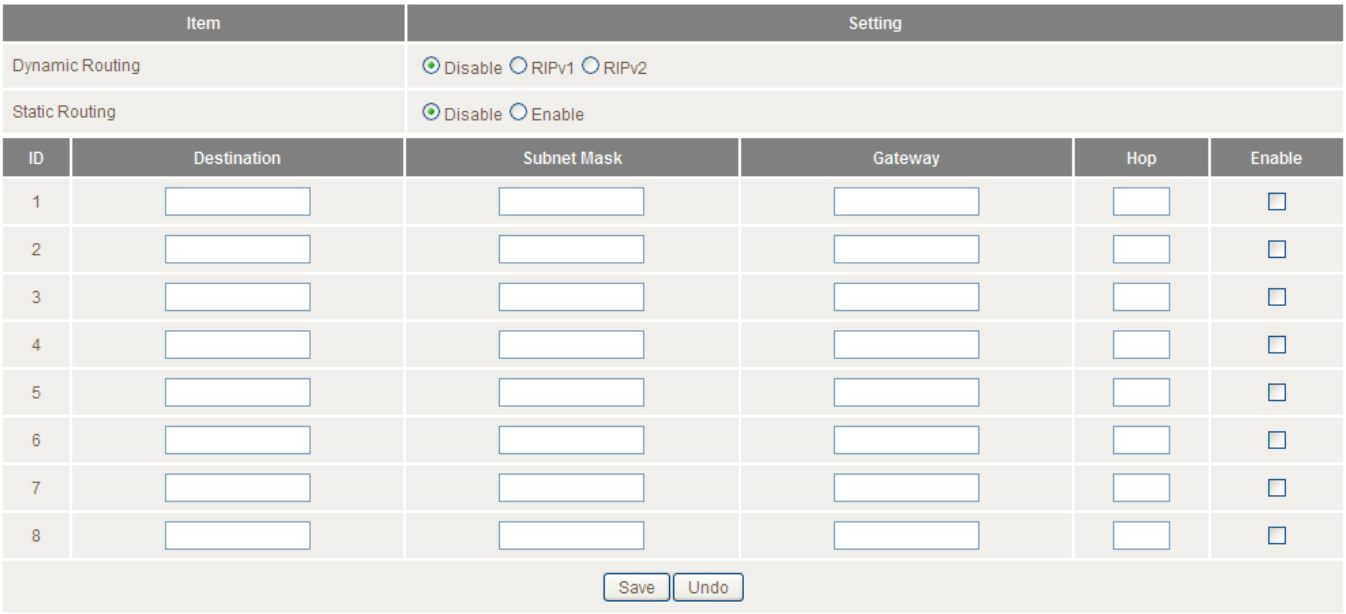
Note: If "Remote" access is enabled, the default setting of 0.0.0.0 means any IP obtain SNMP protocol Information.

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 NB16DG.



Item	Setting
Dynamic Routing	● Disable ○ RIPv1 ○ RIPv2
Static Routing	● Disable ○ Enable

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1					□
2					□
3					□
4					□
5					□
6					□
7					□
8					□

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:

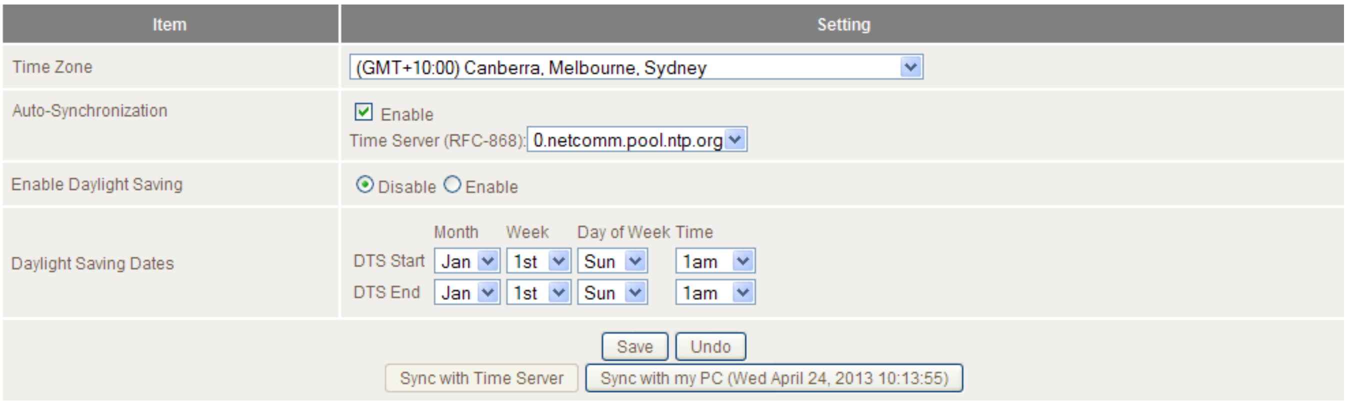
For static routing, you can specify up to 8 routing rules.

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 NB16DG.



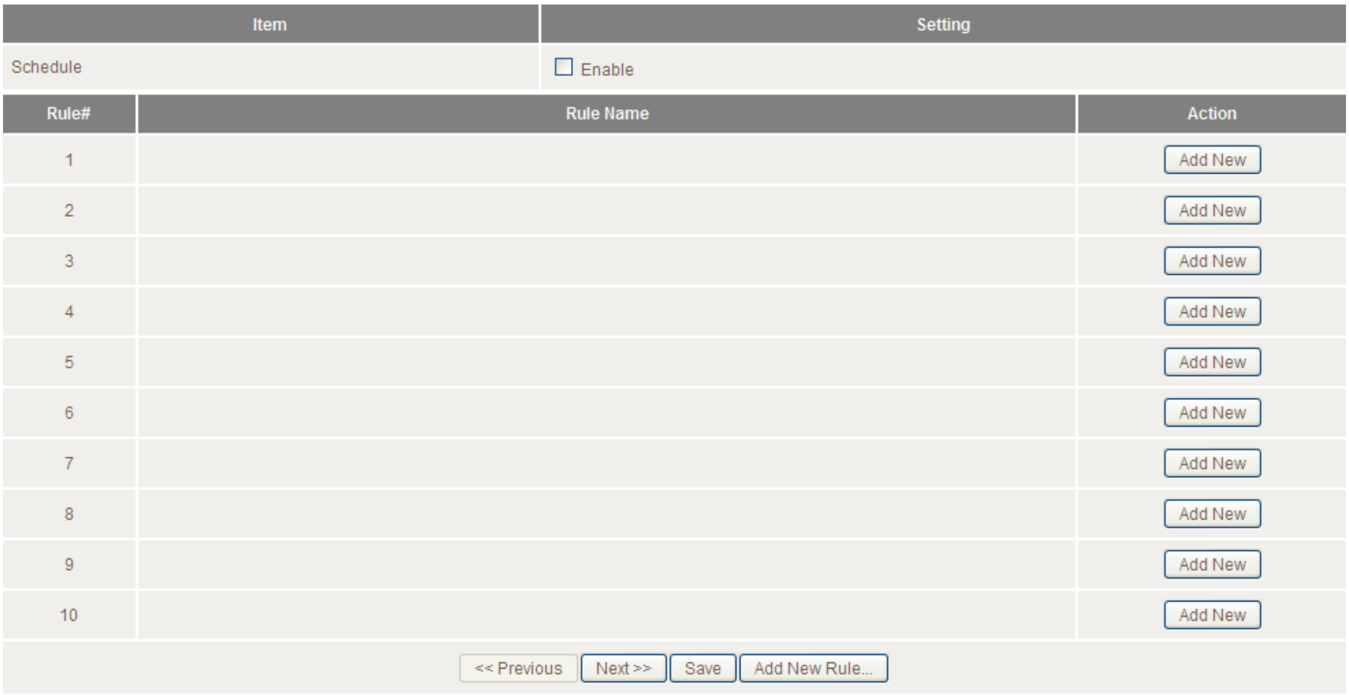
Item	Setting
Time Zone	(GMT+10:00) Canberra, Melbourne, Sydney
Auto-Synchronization	☑ Enable Time Server (RFC-868): 0.netcomm.pool.ntp.org
Enable Daylight Saving	● Disable ○ Enable
Daylight Saving Dates	Month / Week / Day of Week / Time DTS Start: Jan, 1st, Sun, 1am DTS End: Jan, 1st, Sun, 1am

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

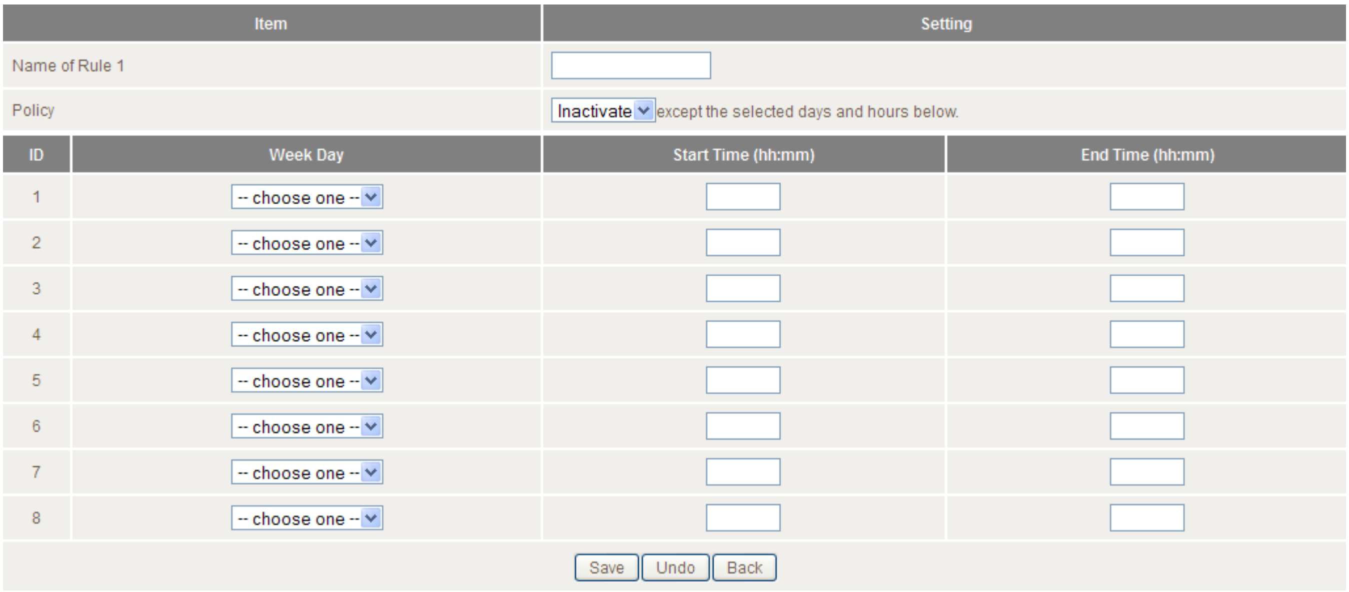
You can use scheduling to enable or disable a service at a specific time or on a specific day.



Item	Setting
Schedule	□ Enable

Rule#	Rule Name	Action
1		Add New
2		Add New
3		Add New
4		Add New
5		Add New
6		Add New
7		Add New
8		Add New
9		Add New
10		Add New

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



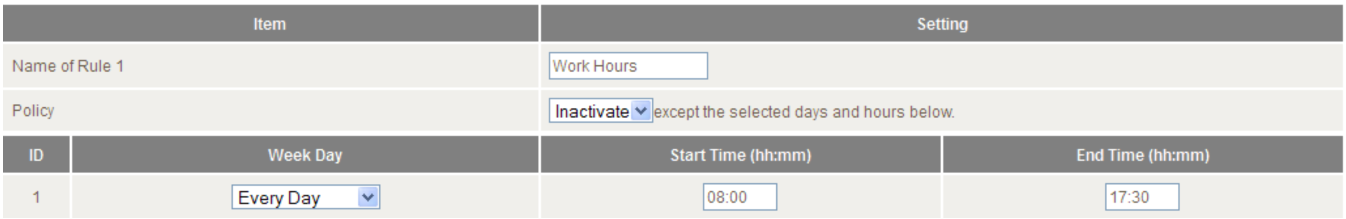
Item	Setting
Name of Rule 1	
Policy	Inactivate except the selected days and hours below.

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one --		
2	-- choose one --		
3	-- choose one --		
4	-- choose one --		
5	-- choose one --		
6	-- choose one --		
7	-- choose one --		
8	-- choose one --		

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	Work Hours
Policy	Inactivate except the selected days and hours below.

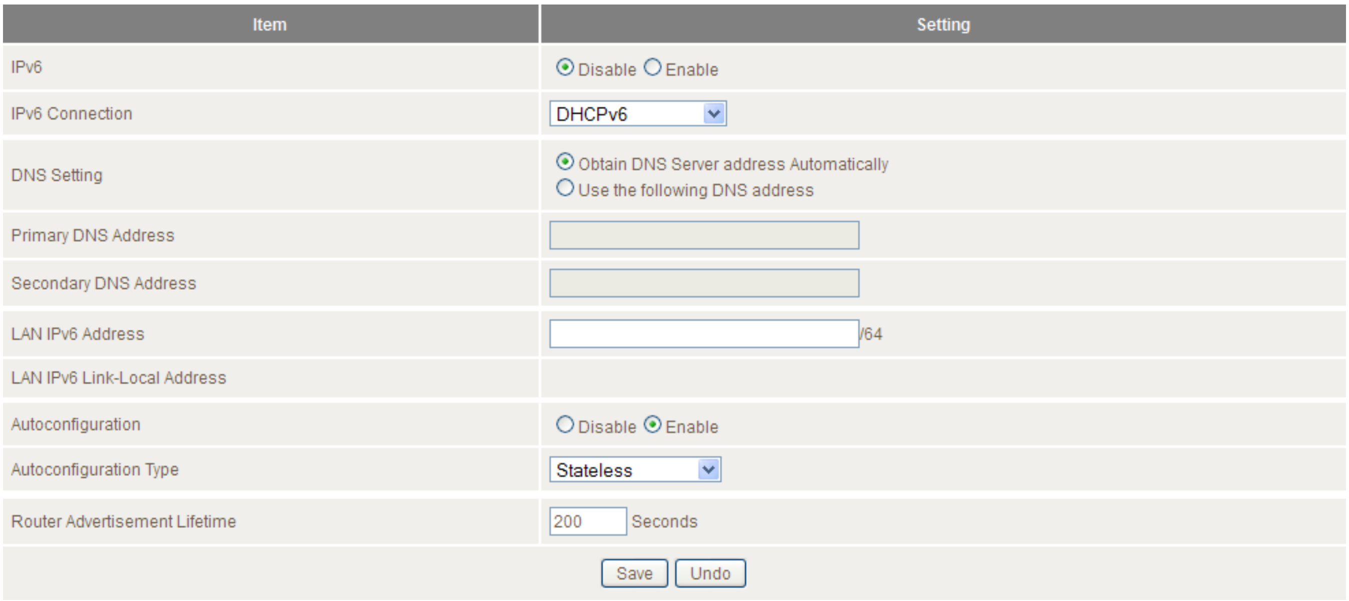
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	Every Day	08:00	17:30

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).

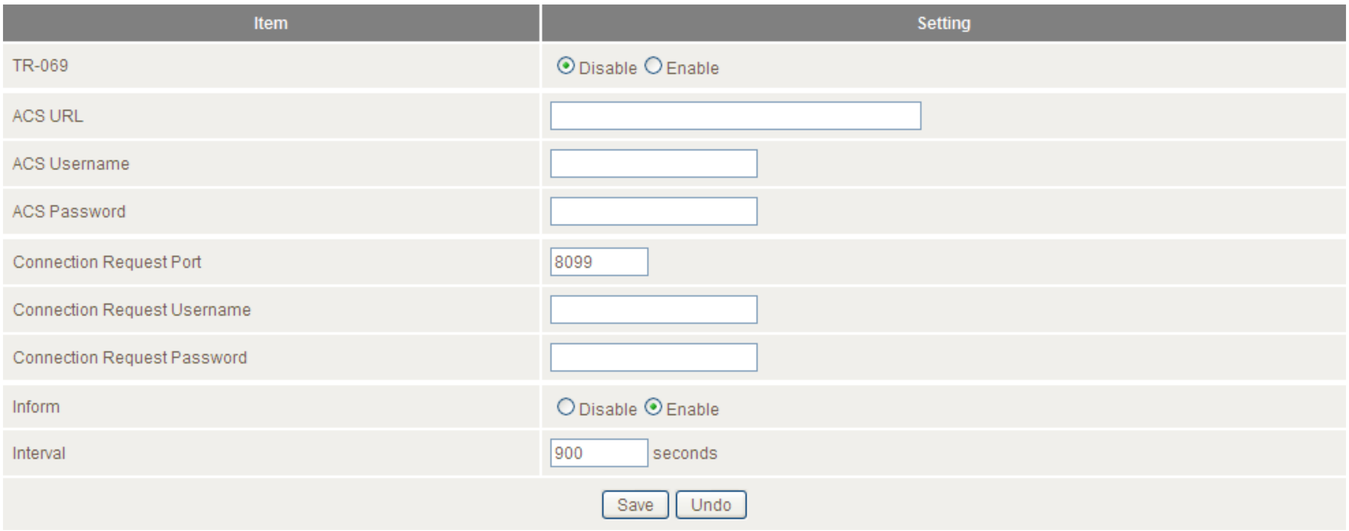


Item	Setting
IPv6	● Disable ○ Enable
IPv6 Connection	DHCPv6
DNS Setting	● Obtain DNS Server address Automatically ○ Use the following DNS address
Primary DNS Address	
Secondary DNS Address	
LAN IPv6 Address	/64
LAN IPv6 Link-Local Address	
Autoconfiguration	○ Disable ● Enable
Autoconfiguration Type	Stateless
Router Advertisement Lifetime	200 Seconds

OPTION	DEFINITION
IPv6	Select to enable or disable IPv6 functionality.
IPv6 Connection	Select the type of IPv6 connection to utilise for your service. You can select from: ▪ 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 specify.
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 service connection.
LAN IPv6 Link-Local Address	The current local LAN IPv6 address of the NB16DG.
Autoconfiguration	Select to enable or disable IPv6 auto configuration (if supported by your Internet Service Provider).
Autoconfiguration Type	Select the appropriate type of auto configuration mode as required by your Internet Service Provider for their IPv6 service.
Router Advertisement Lifetime	Enter the length of time between the router advertising its availability on the IPv6 connection.

TR-069

The TR-069 client allows the NB16DG 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.



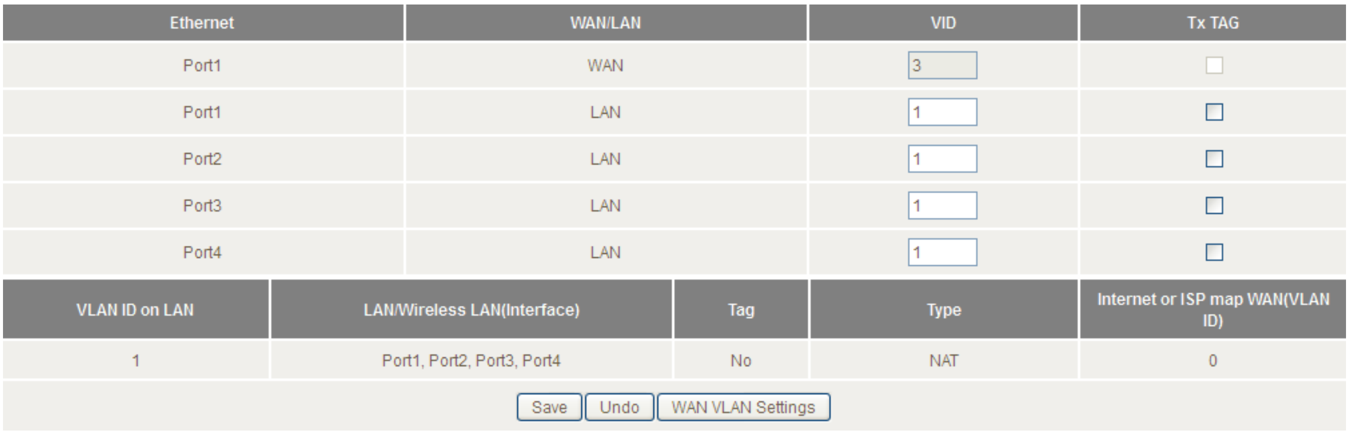
Item	Setting
TR-069	● Disable ○ Enable
ACS URL	
ACS Username	
ACS Password	
Connection Request Port	8099
Connection Request Username	
Connection Request Password	
Inform	○ Disable ● Enable
Interval	900 seconds

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 requests 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.

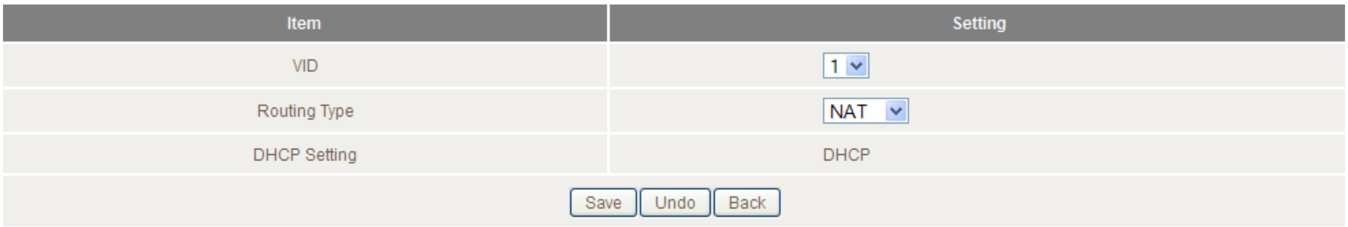


Ethernet	WAN/LAN	VID	Tx TAG
Port1	WAN	3	□
Port1	LAN	1	□
Port2	LAN	1	□
Port3	LAN	1	□
Port4	LAN	1	□

VLAN ID on LAN	LAN/Wireless LAN(Interface)	Tag	Type	Internet or ISP map WAN(VLAN ID)
1	Port1, Port2, Port3, Port4	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.

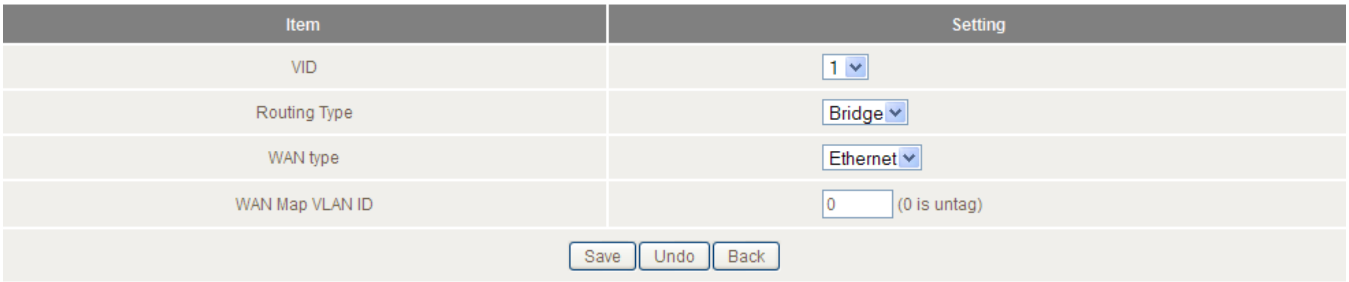
To adjust advanced WAN VLAN settings for a particular VID, click the **WAN VLAN Settings** button. The following window is displayed:



Item	Setting
VID	1
Routing Type	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	1
Routing Type	Bridge
WAN type	Ethernet
WAN Map VLAN ID	0 (0 is untag)

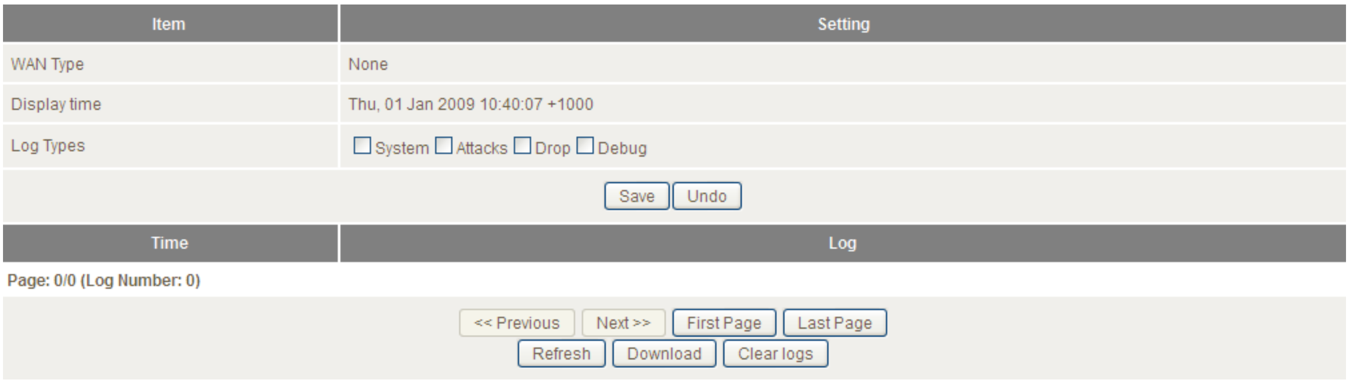
OPTION	DEFINITION
VID	Use the drop down list to select the VID you want to configure.
Routing Type	Use the drop down list to type of routing for the selected VID.
WAN type	Use the drop down list to select which WAN type the VLAN uses.
WAN Map VLAN ID	Enter the VLAN ID to tag packets on the WAN interface.

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.



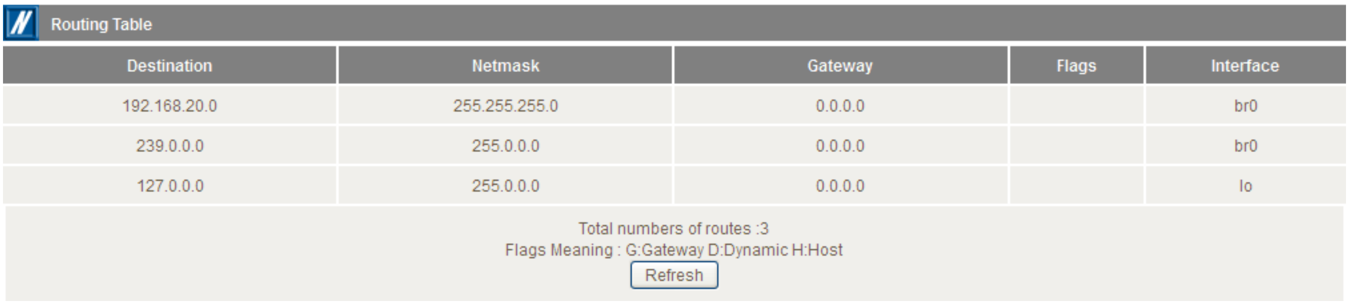
Item	Setting
WAN Type	None
Display time	Thu, 01 Jan 2009 10:40:07 +1000
Log Types	□ System □ Attacks □ Drop □ Debug

Time	Log

Page: 0/0 (Log Number: 0)

Routing Table

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



Routing Table

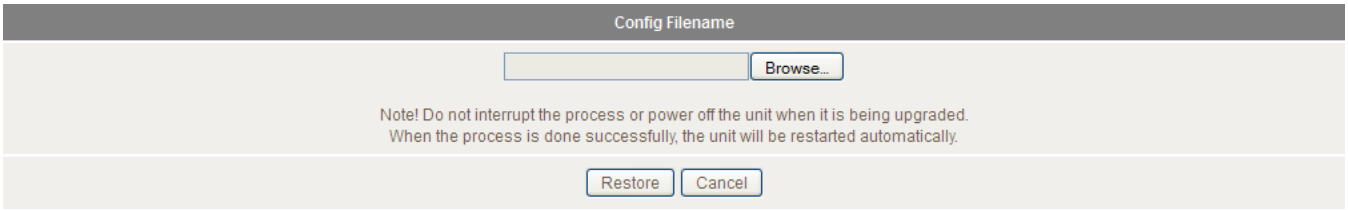
Destination	Netmask	Gateway	Flags	Interface
192.168.20.0	255.255.255.0	0.0.0.0		br0
239.0.0.0	255.0.0.0	0.0.0.0		br0
127.0.0.0	255.0.0.0	0.0.0.0		lo

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.



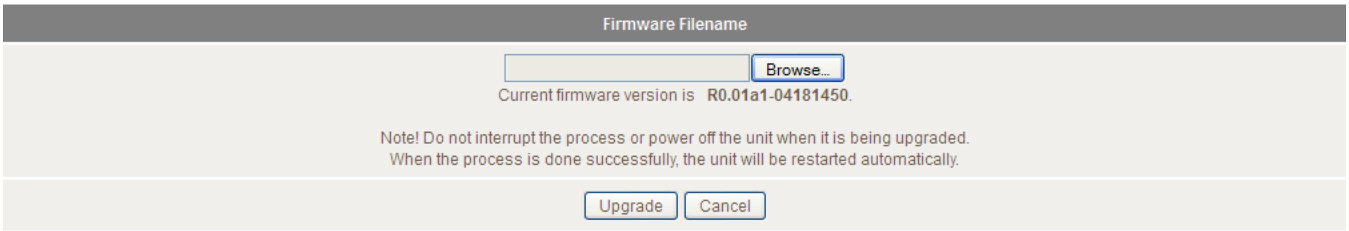
Config Filename

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

Current firmware version is **R0.01a1-04181450**.

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.

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

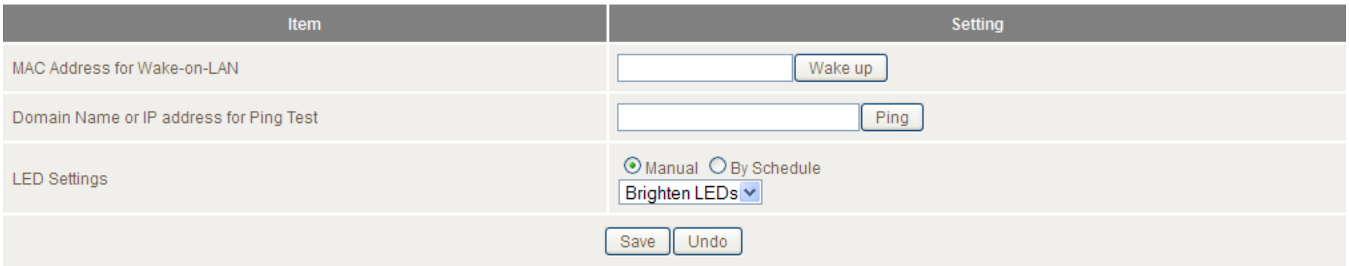
Click the Reboot menu item to restart the router.

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	Wake up
Domain Name or IP address for Ping Test	Ping
LED Settings	● Manual ○ By Schedule Brighten LEDs

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 NB16WV with "Connected" next to 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 NB16DG 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 NB16DG and the power source are both turned on and device is receiving sufficient power.
3	Turn the NB16DG off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact technical support.

Web Configuration

I cannot access the web configuration pages.

STEP	CORRECTIVE ACTION
1	Make sure you are using the correct IP address of the NB16DG. You can check the IP address of the device from the Network Setup configuration page.
2	Check that you have enabled remote administration access. If you have configured an inbound packet filter, ensure your computer's IP address matches it.
3	Your computer's and the NB16DG's IP addresses must be on the same subnet for LAN access. You can check the subnet in use by the router on the Network Setup page.
4	If you have changed the devices IP address, then enter the new one as the URL you enter into the address bar of your web browser.
5	If you are still not able to access the web configuration pages, reset the router to the factory default settings by pressing the reset button for ten seconds and then releasing it. When the Power LED begins to blink, the defaults have been restored and the NB16DG restarts. Navigate to 192.168.20.1 in your web browser and enter "admin" (without the quotes) as the username and password.

The web configuration does not display properly.

STEP	CORRECTIVE ACTION
1	Delete the temporary web files and log in again. In Internet Explorer, click Tools, Internet Options and then click the Delete Files ... button. When a Delete Files window displays, select Delete all offline content and click OK. (Steps may vary depending on the version of your Internet browser.)

Login Username and Password

I forgot my login username and/or password.

STEP	CORRECTIVE ACTION
1	Press the Reset button for ten seconds, and then release it. When the Power LED begins to blink, the defaults have been restored and the NB16DG restarts. You can now login with the factory default username and password "admin" (without the quotes)
2	It is highly recommended to change the default username and password. Make sure you store the username and password in a safe place.

WLAN Interface

I cannot access the NB16DG from the WLAN or ping any computer on the WLAN.

STEP	CORRECTIVE ACTION
1	Check the Wi-Fi LED on the front of the unit and verify the WLAN is enabled as per the LED Indicator section.
2	If you are using a static IP address for the WLAN connection, make sure that the IP address and the subnet mask of the NB16DG and your computer(s) are on the same subnet. You can check the routers configuration from the Network Setup page.

Technical Data

The following table lists the hardware specifications of the NB16DG.

MODEL	NB16DG
ADSL2+	ITU 992.1 (G.dmt) Annex A ITU 992.2 (G.lite) ITU 992.3 ADSL2 (G.dmt.bis) ITU 992.5 ADSL2+
Wireless WAN	PPP (for WCDMA / HSPA)
Ethernet WAN	1 x Gigabit WAN port (10/100/1000 Mbps)
Connectivity	4 x 10/100/1000 Mbps, 1 x RJ-11 ADSL, 1 x WLAN
LED Indicators	Power, ADSL, WWW, LAN 1-4, WAN, WiFi.
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 - 1.5A
Dimensions & Weight	215 mm (L) x 145 mm (W) x 37 mm (H) 386 grams
Regulatory Compliance	A-Tick

Electrical Specifications

It is recommended that the NB16DG be powered by the supplied 12V DC, 1.5A power supply. A replacement power supply is available from the NetComm Wireless Online shop.

Environmental Specifications / Tolerances

The NB16DG 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 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