NETCOMM LIBERTY™ SERIES

3G/4G Wireless N150 Router m2

3GM2WN

USER GUIDE

Copyright

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

Save Our Environment

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

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

Please be responsible and protect our environment.

This manual covers the following products:

NetComm 3GM2WN

DOCUMENT VERSION	DATE
1.0 - Initial document release	14/12/2011

Table of Contents

Overview

Introduction

This manual provides information related to the installation, operation, and utilisation of the 3GM2WN.

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 3GM2WN, please confirm that you comply with the minimum system requirements below.

- An activated ADSL, activated 3G/4G, 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, Netscape Navigator, 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 utilised in this user manual:

- ⚠

The following note requires attention

- ⚡

The following note provides a warning

- ℹ

The following note provides relevant information

Product Introduction

Product Overview

- Stylish and compact 3G/4G Router with internal antenna
- Creates an instant Wireless hotspot to share the internet connection of a 3G/4G USB modem or DSL/Cable modem
- Supports Wireless N standard with data speeds up to 150Mbps[1]
- USB 2.0 host port supports 3G/4G modems
- Ensure connectivity and business continuity with auto internet failover from WAN port to 3G/4G modem

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

Package Contents

The 3GM2WN package consists of:

- NetComm 3G/4G Wireless N150 Router m2 – 3GM2WN
- Power Adapter
- Quick Start Guide
- Ethernet Cable (RJ-45)
- Wireless Security Card
- Warranty Card

If any of these items are missing or damaged, please contact NetComm Support immediately by visiting the NetComm Support website at: http://www.netcomm.com.au/contact-us/technical-support

Product Features

The pocket-sized 3GM2WN is packed with the latest connection, sharing and security features for reliable broadband access without boundaries. Ideal for travel, the device offers flexible 3G/4G or ADSL2+ broadband Internet connection options.

Sharing the connection is easy. Create an instant and portable WiFi zone for multiple devices such as laptops, PCs, gaming consoles, tablets and smart phones from public areas using a 3G/4G USB modem; or connect to an in-room ADSL2+ service via the Ethernet port.

Where a power outlet is not available the device can be powered from a laptop or desktop USB port; and a host of advanced security features offer maximum wireless protection.

Physical Dimensions and Indicators

LED Indicators

The 3GM2WN has been designed to be placed on a desktop. All of the cables exit from the rear for better organization. The LED indicator display is visible on the front of the router to provide you with information about network activity and device status. See below for an explanation of each of the indication lights.

FRONT PANEL	ICON	COLOUR	ACTIVITY	DEFINITION
POWER	⏻	Green	Blinking Slowing	Router is powered on
			Blinking Quickly	Device is in WPS mode
		None	Off	Router is powered off
WWW	www	Red	Solid	Power on with connection configuration problem
		Green	Solid	Connected to internet successfully
		None	N/A	Power off

Physical Dimensions

The following page lists the physical dimensions of the 3GM2WN.

3GM2WN	
Length	85.5 mm
Width	56 mm
Height	17.5 mm
Weight	52 grams

3GM2WN Default Settings

The following tables list the default settings for the 3GM2WN.

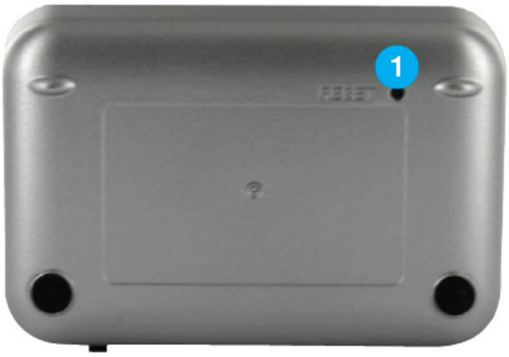
LAN (MANAGEMENT)	
Static IP Address:	192.168.20.1
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.20.1

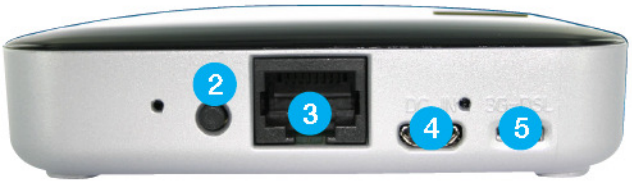
WIRELESS (WI-FI)	
SSID:	(Refer to the included Wireless Security Card)
Security:	WPA2-PSK
Security Key:	(Refer to the included Wireless Security Card)

3GM2WN WEB INTERFACE ACCESS	
Username:	admin
Password:	admin

Integrated Interfaces

The following integrated interfaces are available on the 3GM2WN:





REAR PANEL		DESCRIPTION
1	Reset button	By using a paper clip, hold this button down for more than 10 seconds to reset to factory defaults.
2	WPS	Hold this button for 3 seconds and release to enable the WPS push-button connect function.
3	Ethernet port	RJ-45 LAN port for wired Ethernet clients (computers, laptops, etc)
4	DC IN	Power connector, connects to a DC 5V 1.5A Power Adapter
5	3G-DSL switch	RJ-45 switchable WAN/LAN port Switch to 3G for LAN connection or to DSL for WAN connection

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 3GM2WN, 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 3GM2WN

Placement of your 3GM2WN

The wireless connection between your 3GM2WN and your Wi-Fi devices will be stronger the closer your connected devices are to your 3GM2WN. Your wireless connection and performance will degrade as the distance between your 3GM2WN 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 3GM2WN in order to see if distance is the problem.

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

If you experience difficulties connecting wirelessly between your Wi-Fi Devices and your 3GM2WN, please try the following steps:

- In multi-storey homes, place the 3GM2WN on a floor that is as close to the centre of the home as possible. This may mean placing the 3GM2WN on an upper floor.
- Try not to place the 3GM2WN near a cordless telephone that operates at the same radio frequency as the 3GM2WN (2.4GHz).

Avoid obstacles and interference

Avoid placing your 3GM2WN 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 3GM2WN).

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 3GM2WN 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 3GM2WN.
- 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 3GM2WN 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. If you are using a 3G connection, attach your USB 3G dongle to the USB port on top of the 3GM2WN.
2. Connect the power adapter to the power socket on the back of the NetComm 3GM2WN.
3. Plug the power adapter into the wall socket and switch on the power.
4. Wait approximately 60 seconds for the NetComm 3GM2WN to power up.

Connecting via a cable

1. Connect the yellow Ethernet cable provided to Ethernet port on the back of the NetComm 3GM2WN.
2. Connect the other end of the Ethernet cable to your computer or to another Ethernet-enabled device like a gaming console, a TV or a home cinema system.
3. Slide the “3G-DSL” switch to the “3G” side.
4. Wait approximately 30 seconds for the connection to establish.

Connecting wirelessly

You can connect multiple wireless devices, including laptops, desktops and PDA’s to your router by following these two basic steps.

1. Using your wireless device, scan the wireless networks in your area and select the wireless network name listed on the included Wireless Security Card and then click connect.

Please note: If you changed the wireless network name during set-up, select the wireless network displaying the new name you entered.

2. Enter the wireless security key listed on the included Wireless Security Card.

Please note: If you changed the wireless security password during set-up, enter the new password you entered.

3. To ensure wireless security, we recommend that you change the default settings through the web based user interface.

Web Based Configuration Interface

First-time Setup Wizard

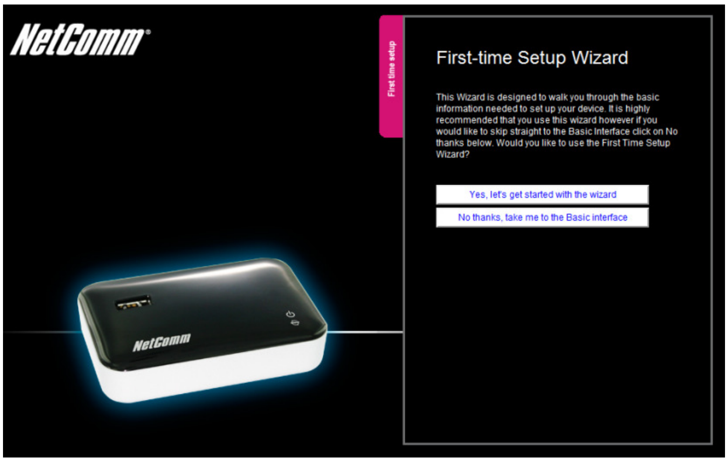
Please follow the steps below to configure your 3GM2WN Wireless router via the web based configuration wizard.

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**" (without quotes) in the username and password field. Then click on Login.

Please note: admin is the default username and password for the unit.

1. Click on “Yes, let’s get started with the wizard”.

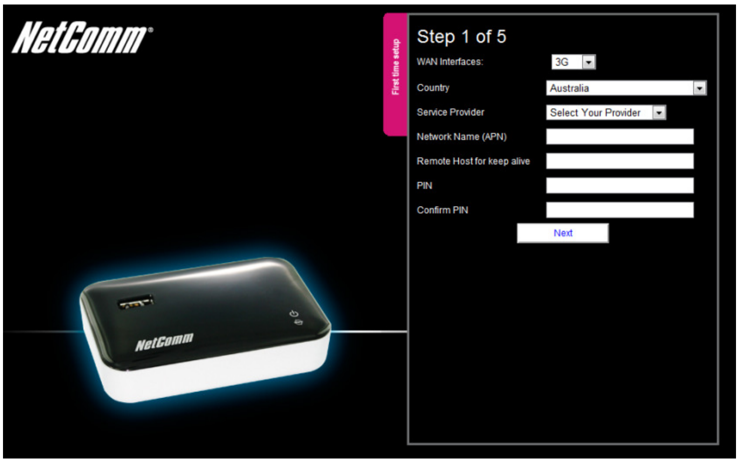


First-time Setup Wizard

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?

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

This page enables you to enter the information needed to setup your Internet connection.



Step 1 of 5

WAN Interfaces: 3G

Country: Australia

Service Provider: Select Your Provider

Network Name (APN):

Remote Host for keep alive:

PIN:

Confirm PIN:

2. Select your chosen connection. You can select from
   - 3G
   - WAN

3G

Please note: If you are utilising a 3G connection, please ensure the “3G-DSL” switch is set to “3G”.

You can manually enter the appropriate 3G/4G provider APN or alternatively select your country and 3G/4G provider from the dropdown box (If required, you can then also enter your username and password).

After entering the required details, click “Next”.

WAN

Please note: If you are utilising an Ethernet WAN connection, please ensure the “3G-DSL” switch is set to “DSL”.

Select the appropriate Ethernet WAN connection type for your network.

You can select from the following types:-

- Dynamic IP Address (DHCP)
- Static IP Address (Static IP)
- PPP over Ethernet (PPPoE)
- PPTP
- L2TP

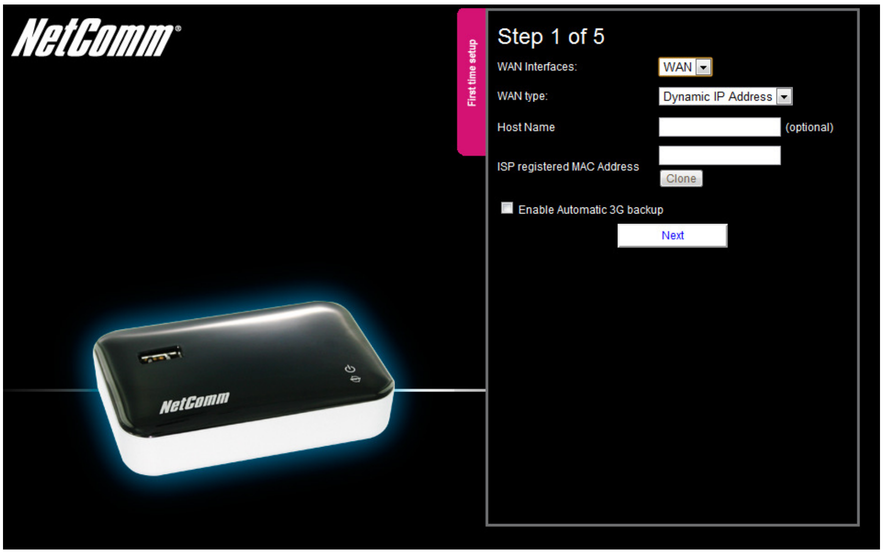
Enter the connection details as supplied by your Internet Service Provider.

(If you are unsure of the details, please contact your Internet Service Provider for more information.)

After entering the required details, click “Next”.

3. From the WAN type pull down menu, select the type of Internet connection you would like to utilise. You can select from:
    - Dynamic IP Address
    - Static IP Address
    - PPP over Ethernet
    - PPTP
    - L2TP

Dynamic IP Address


Step 1 of 5

WAN Interfaces: WAN

WAN type: Dynamic IP Address

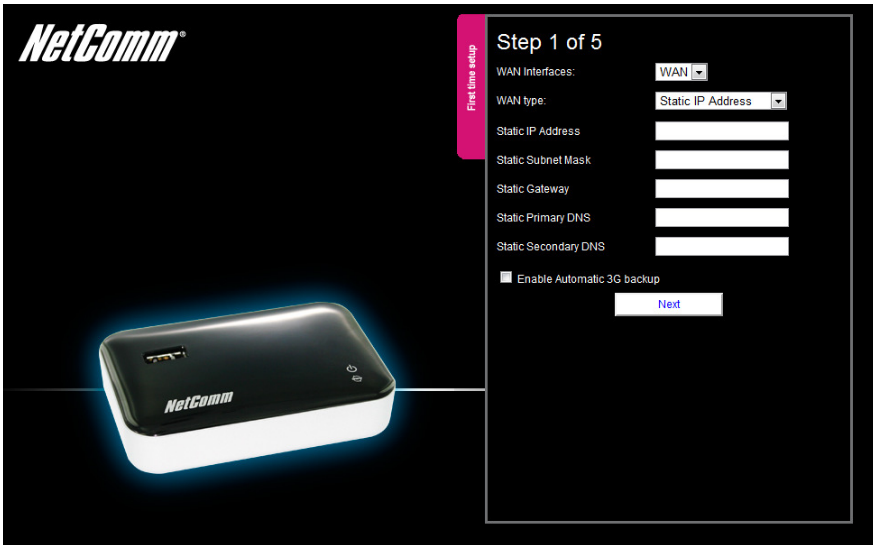
Host Name (optional)

ISP registered MAC Address

☐ Enable Automatic 3G backup

1. Enter the Host Name (if required).
2. Enter the ISP registered MAC Address (if required).
3. Click “Next”.

Static IP Address


Step 1 of 5

WAN Interfaces: WAN

WAN type: Static IP Address

Static IP Address

Static Subnet Mask

Static Gateway

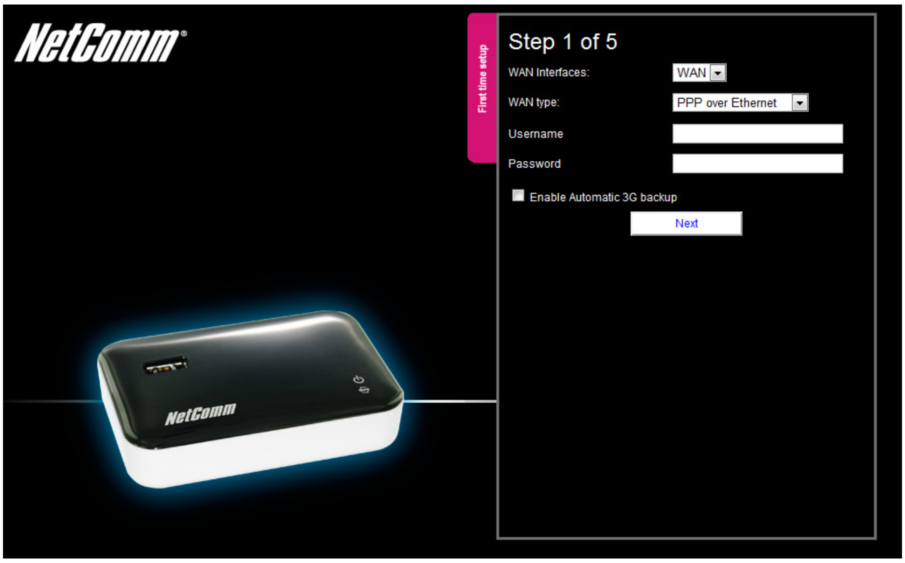
Static Primary DNS

Static Secondary DNS

☐ Enable Automatic 3G backup

1. Enter the Static IP Address for your connection.
2. Enter the Subnet Mask for your connection.
3. Enter the Static Gateway for your connection.
4. Enter the Static Primary DNS for your connection.
5. Enter the Static Secondary DNS for your connection (if available).
6. Click “Next”.

PPP over Ethernet



Step 1 of 5

WAN Interfaces: WAN

WAN type: PPP over Ethernet

Username

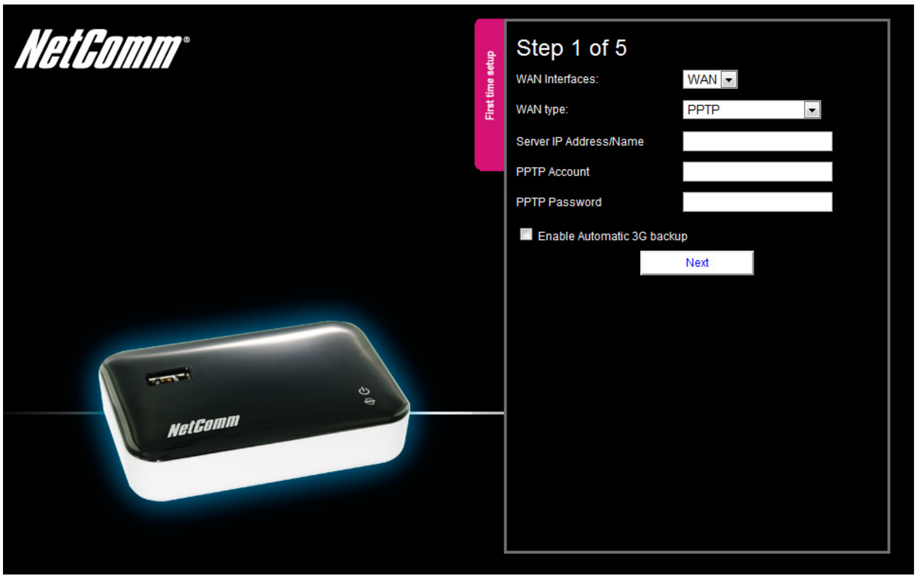
Password

□ Enable Automatic 3G backup

Next

1. Enter the Username required for your PPPoE connection.
2. Enter the Password required for your PPPoE connection.
3. Click “Next”.

PPTP



Step 1 of 5

WAN Interfaces: WAN

WAN type: PPTP

Server IP Address/Name

PPTP Account

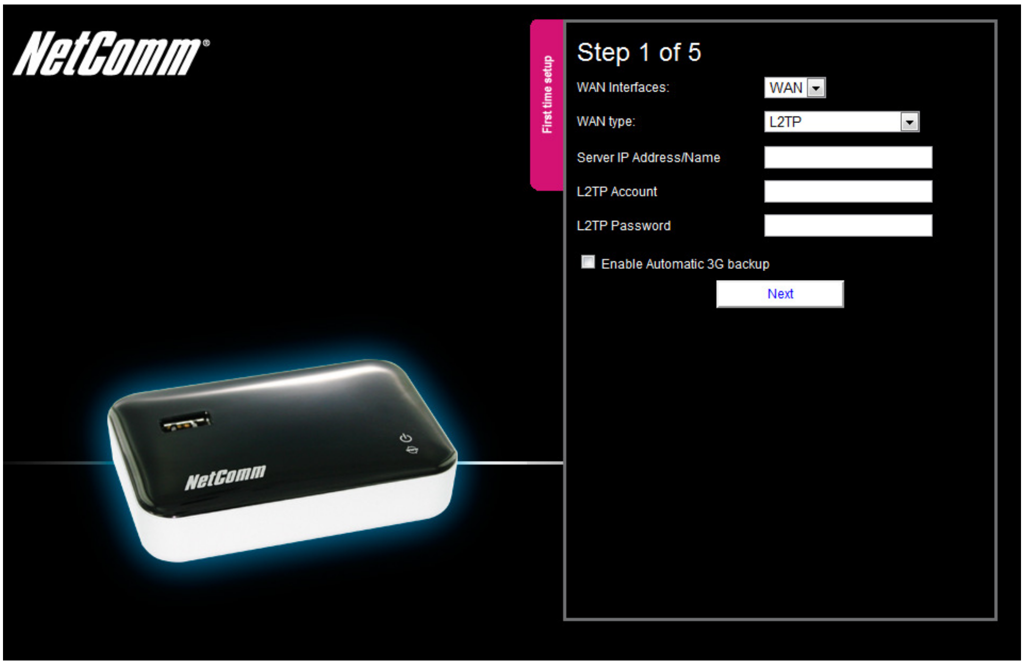
PPTP Password

□ Enable Automatic 3G backup

Next

1. Enter the Sever IP Address/Name for your PPTP connection. (optional)
2. Enter the Username required for your PPTP connection.
3. Enter the Password required for your PPTP connection.
4. Click “Next”.

L2TP



Step 1 of 5

WAN Interfaces: WAN

WAN type: L2TP

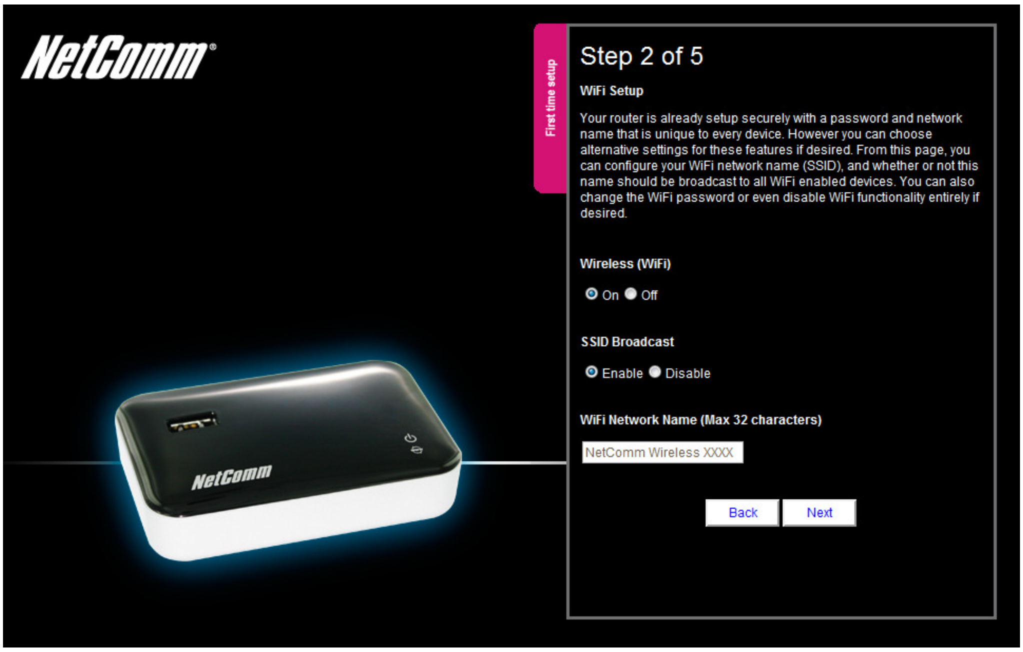
Server IP Address/Name

L2TP Account

L2TP Password

□ Enable Automatic 3G backup

1. Enter the Sever IP Address/Name for your PPTP connection. (optional)
2. Enter the Username required for your L2TP connection.
3. Enter the Password required for your L2TP connection.
4. Click “Next”.



Step 2 of 5

WiFi Setup

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 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 (WiFi)

● On ○ Off

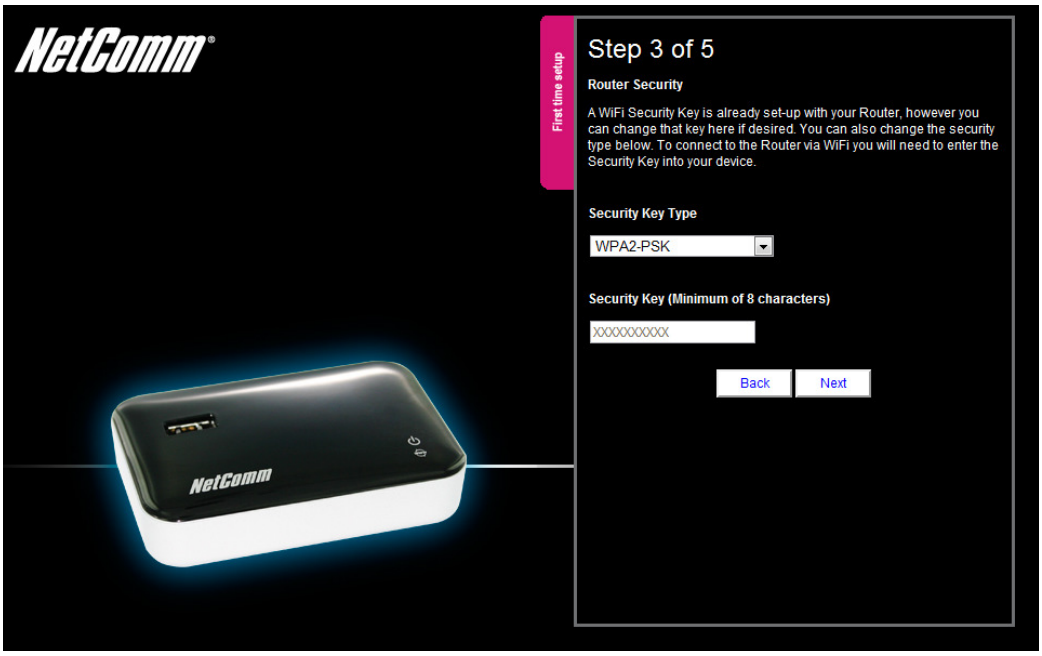
SSID Broadcast

● Enable ○ Disable

WiFi Network Name (Max 32 characters)

NetComm Wireless XXXX

3. If you want to change the 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 3 of 5

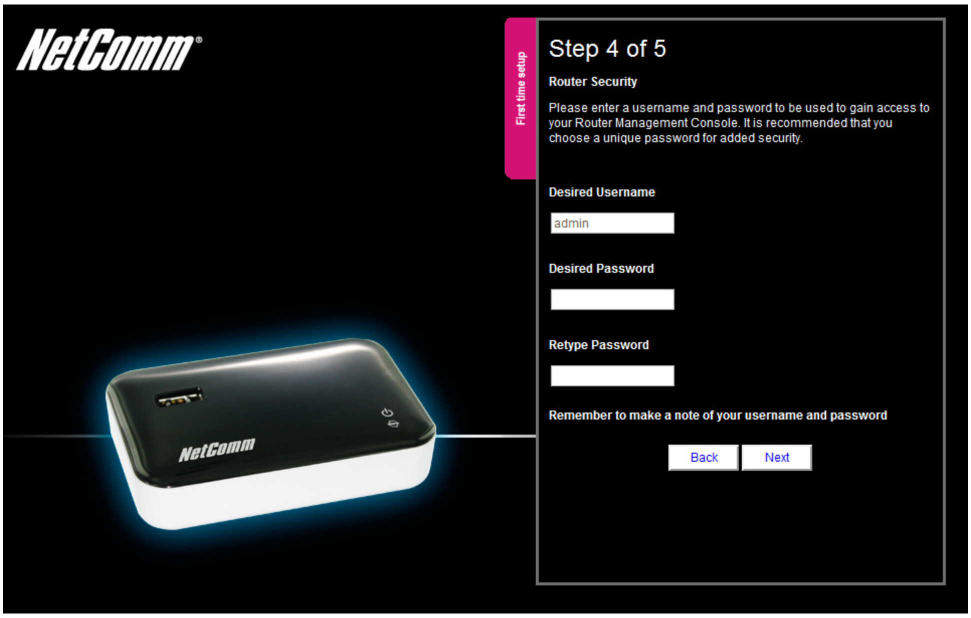
Router Security

A WiFi 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): XXXXXXXXXX

4. If you want to change the Wireless network security settings, you can do so on this page. You can change the type of Wireless network security in use or the Wireless Security key. Change the settings as needed and click “Next”.
(If you wish to use the default settings, click “Next”)



Step 4 of 5

Router Security

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

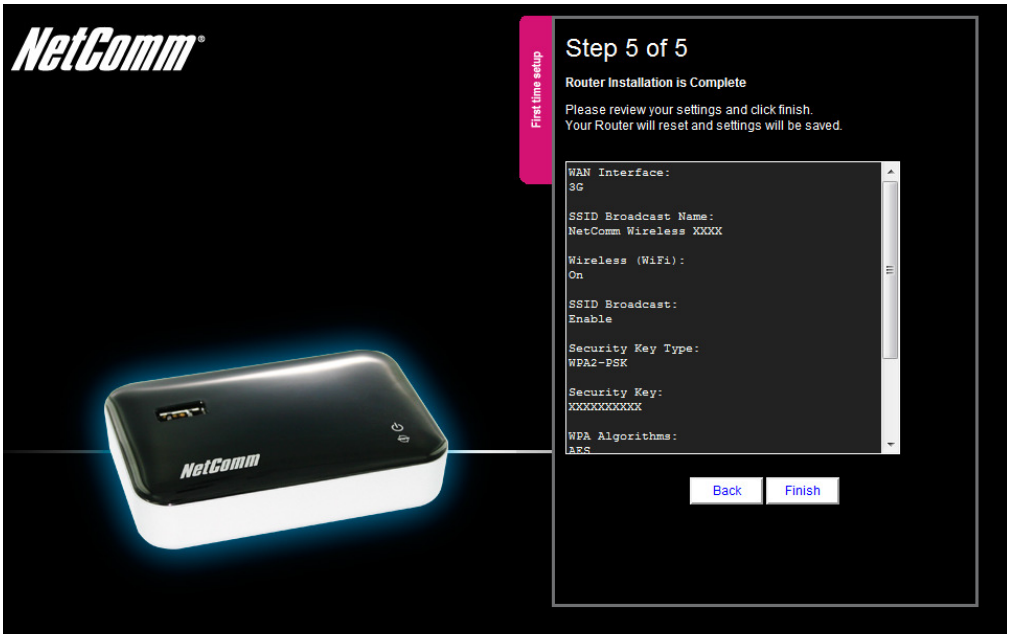
Desired Password

Retype Password

Remember to make a note of your username and password

5. If you want to change the system username or password, enter the new username to use or the current system password into the "Old Password" 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”)



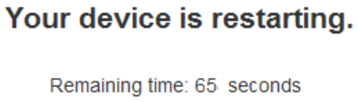
Step 5 of 5

Router Installation is Complete

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

```
WAN Interface:
3G

SSID Broadcast Name:
NetComm Wireless XXXX

Wireless (WiFi):
On

SSID Broadcast:
Enable

Security Key Type:
WPA2-PSK

Security Key:
XXXXXXXXXX

WPA Algorithms:
AES
```

6. 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.



Your device is restarting.

Remaining time: 65 seconds

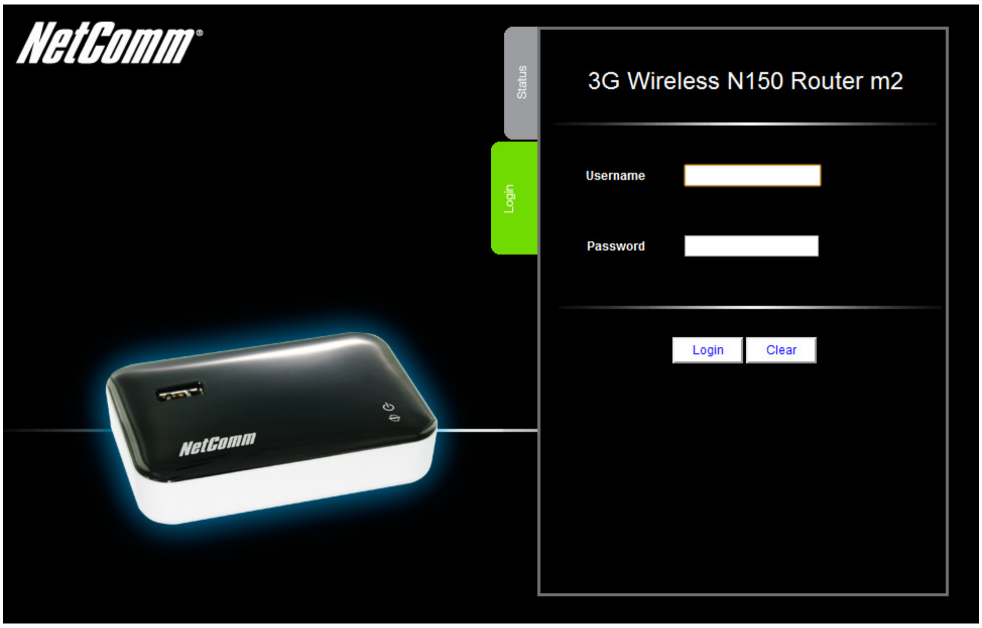
7. The router will then apply your configured settings and restart.

System is ready

8. Once completed, your router is configured and should be connected to the Internet.

Simple View

Login to the Web Based Configuration Interface to verify you are connected to the Internet. You can also change your settings from the other tabs available.



3G Wireless N150 Router m2

Username

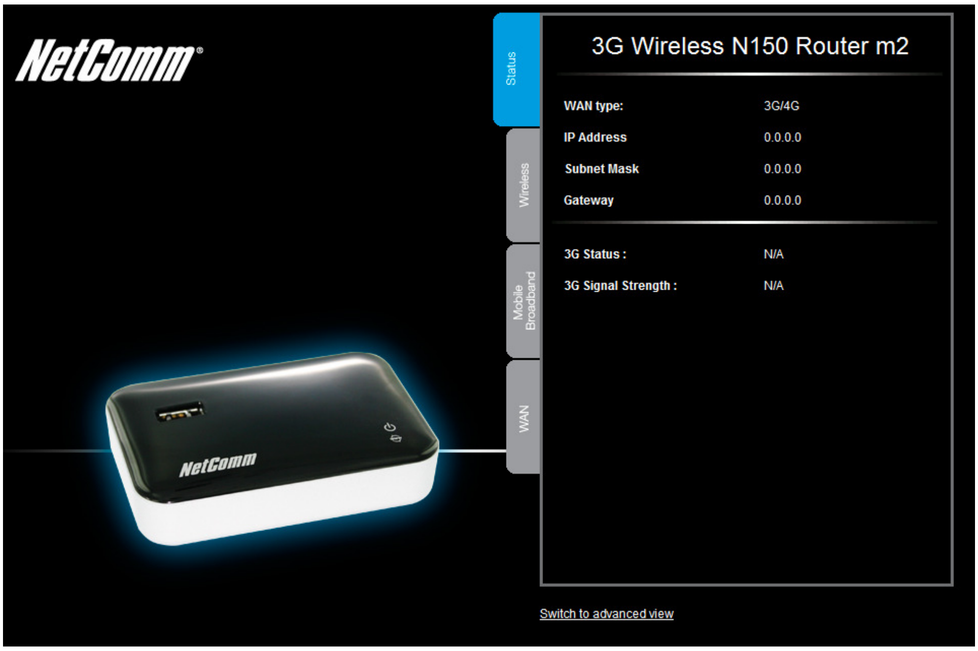
Password

At the login screen, type "**admin**" (without quotes) in the Username and Password field. Then click on Login.

Please note: admin is the default username and password for the unit.

The following information is available on the Status tab:

- WAN Type
- IP address
- Subnet Mask
- 3G Status
- 3G Signal Strength

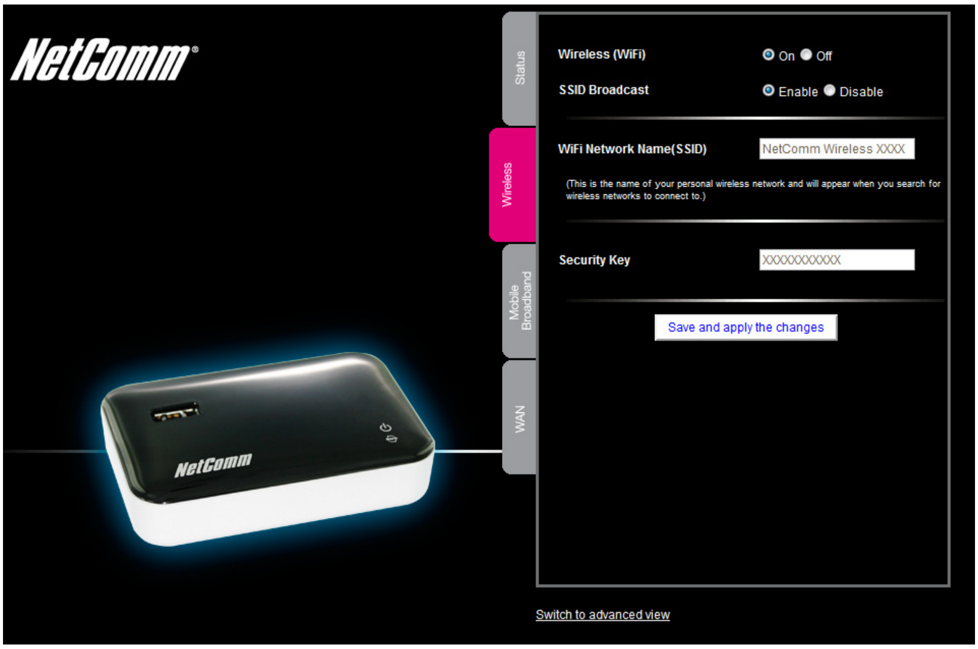


3G Wireless N150 Router m2

WAN type:	3G/4G
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
3G Status :	N/A
3G Signal Strength :	N/A

The following configuration options are available on the Wireless tab:

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



Wireless (WiFi) ◉ On ○ Off

SSID Broadcast ◉ Enable ○ Disable

WiFi Network Name(SSID) NetComm Wireless XXXX

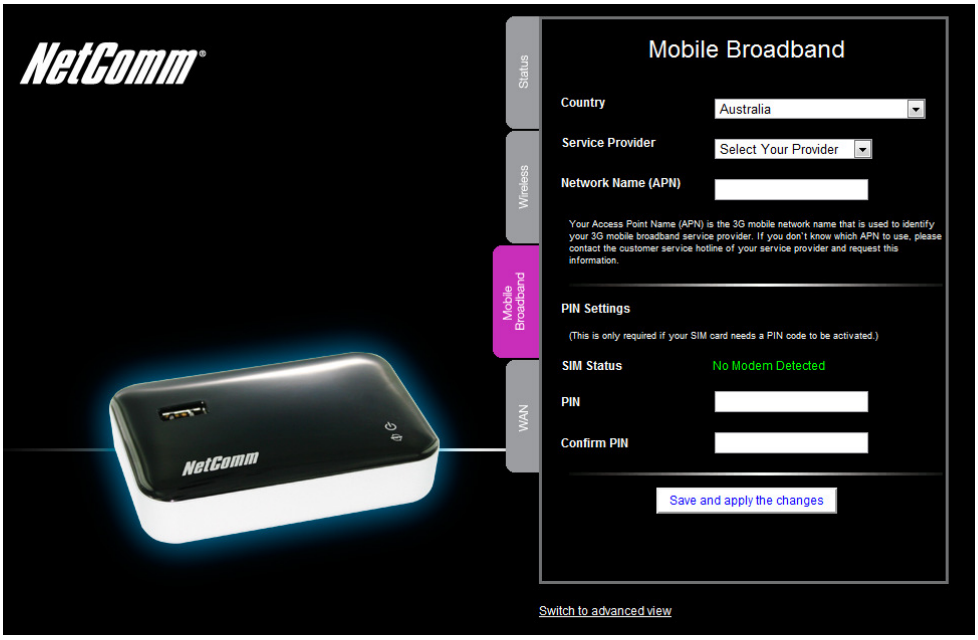
(This is the name of your personal wireless network and will appear when you search for wireless networks to connect to.)

Security Key XXXXXXXXXXX

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

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

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



Mobile Broadband

Country Australia

Service Provider Select Your Provider

Network Name (APN)

Your Access Point Name (APN) is the 3G mobile network name that is used to identify your 3G mobile broadband service provider. If you don't know which APN to use, please contact the customer service hotline of your service provider and request this information.

PIN Settings

(This is only required if your SIM card needs a PIN code to be activated.)

SIM Status No Modem Detected

PIN

Confirm PIN

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

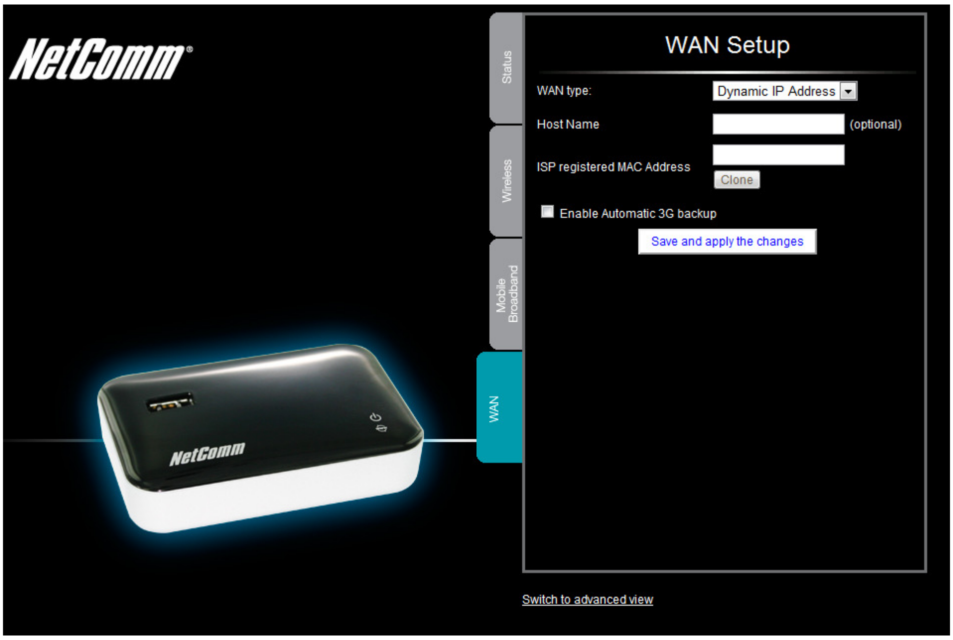
The SIM Status will show if a PIN is required to use your SIM. If it is, enter the SIM PIN into the ‚PIN' and ‚Confirm PIN' fields.

If you make any changes to the 3G/4G configuration, Click the ‚Save and apply the changes' button to make these changes active.

Please note: Saving any configuration changes will make the Mobile Broadband connection the primary method for connecting to the Internet.

The following configuration options are available on the WAN tab:

- WAN type
- Host Name
- ISP registered MAC Address



WAN Setup

WAN type: Dynamic IP Address

Host Name (optional)

ISP registered MAC Address

□ Enable Automatic 3G backup

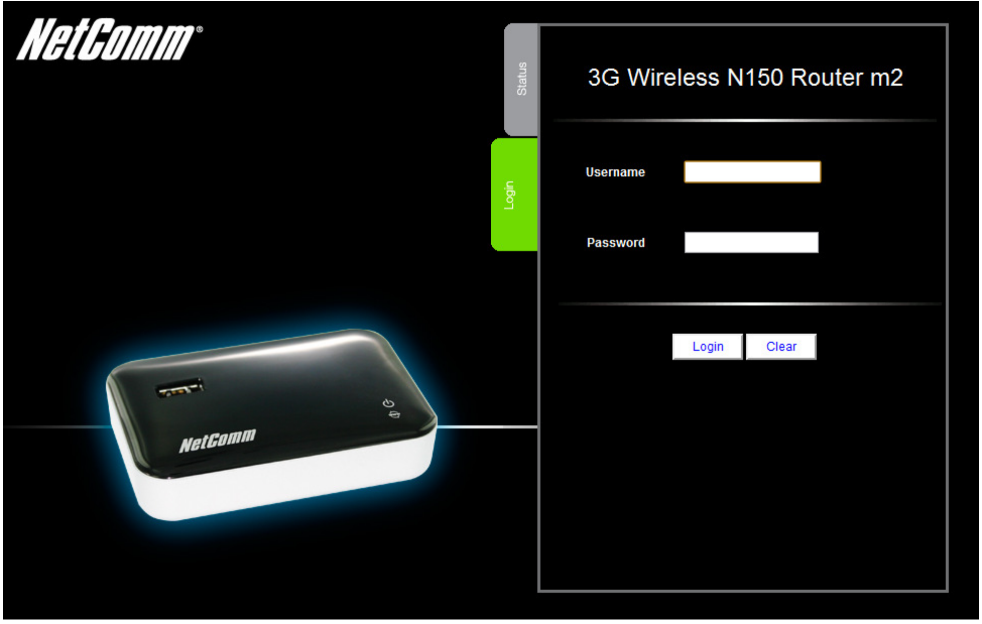
Enter the connection details as supplied by your Internet Service Provider.
(If you are unsure of the details, please contact your Internet Service Provider for more information.)

If you make any changes to the WAN configuration, Click the, Save and apply the changes' button to make these changes active.

Advanced Configuration

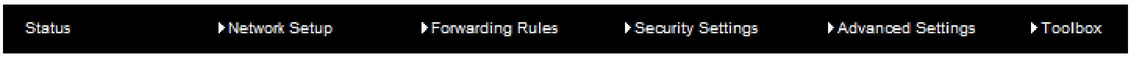
To access the advanced configuration options of your 3GM2WN, you need to login to the web configuration and change to Advanced view.

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.



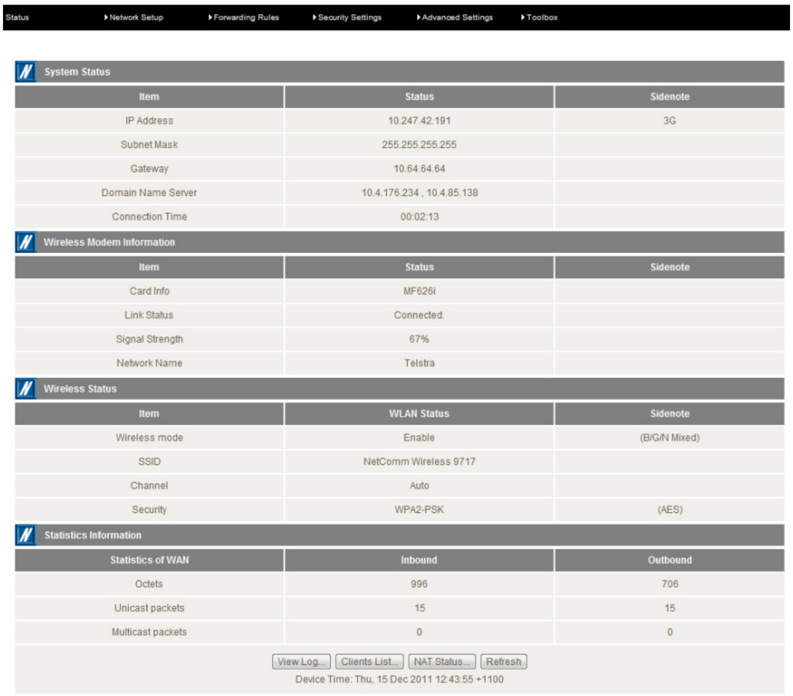
At the login screen, type "**admin**" (without quotes) in the Username and Password field. Then click on Login.

Please note: admin is the default username and password for the unit.



Click on any of the top menu items to access the respective function configuration pages.

Status



System Status

Item	Status	Sidenote
IP Address	10.247.42.191	3G
Subnet Mask	255.255.255.255	
Gateway	10.64.64.64	
Domain Name Server	10.4.176.234 , 10.4.85.138	
Connection Time	00:02:13	

Wireless Modem Information

Item	Status	Sidenote
Card Info	MF626i	
Link Status	Connected.	
Signal Strength	67%	
Network Name	Telstra	

Wireless Status

Item	WLAN Status	Sidenote
Wireless mode	Enable	(B/G/N Mixed)
SSID	NetComm Wireless 9717	
Channel	Auto	
Security	WPA2-PSK	(AES)

Statistics Information

Statistics of WAN	Inbound	Outbound
Octets	996	706
Unicast packets	15	15
Multicast packets	0	0

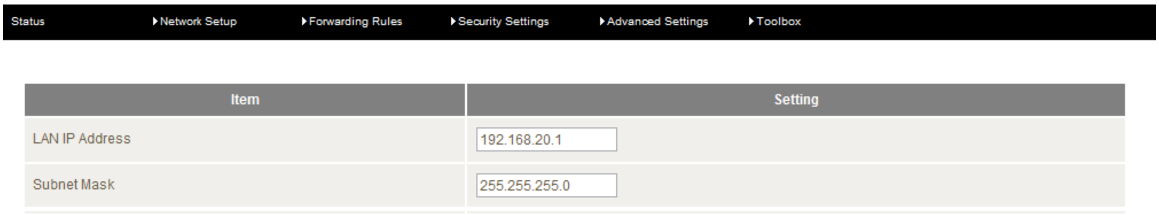
Device Time: Thu, 15 Dec 2011 12:43:55 +1100

ITEM	DESCRIPTION
IP Address	The current WAN IP address of the router
Subnet Mask	The current subnet mask in use by the router
Gateway	The gateway in use by the router to access the internet
Domain Name Server	The Domain name server converts
Connection Time	The time the current connection to the internet has been active
WAN Link-Local Address	The current WAN IPv6 address
Global IPv6 Address	The current IPv6 subnet mask in use
LAN IPv6 Link-Local Address	The current LAN IPv6 address of the 3GM2WN
Link Status	The current IPv6 WAN connection status
Card Info	The name of the 3G USB modem connected to the 3GM2WN
Link Status	The current status of your connection to a 3G Broadband service
Signal Strength	The current available 3G signal strength
Network Name	The name of the 3G network you are connecting to
Wireless mode	The current status of the wireless network (enabled or disabled)
SSID	The current wireless network name is use by the router
Channel	The current wireless channel in use on your wireless network
Security	The currently selected wireless security in use on your wireless network
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 change the LAN (Local Area Network) and WAN (Wide Area Network) connection settings as well as the automatic failover function on the 3GM2WN.



Item	Setting
LAN IP Address	192.168.20.1
Subnet Mask	255.255.255.0

OPTION	DEFINITION
LAN IP Address	The local IP address of the 3G2WN. *(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.

WAN Interface Types

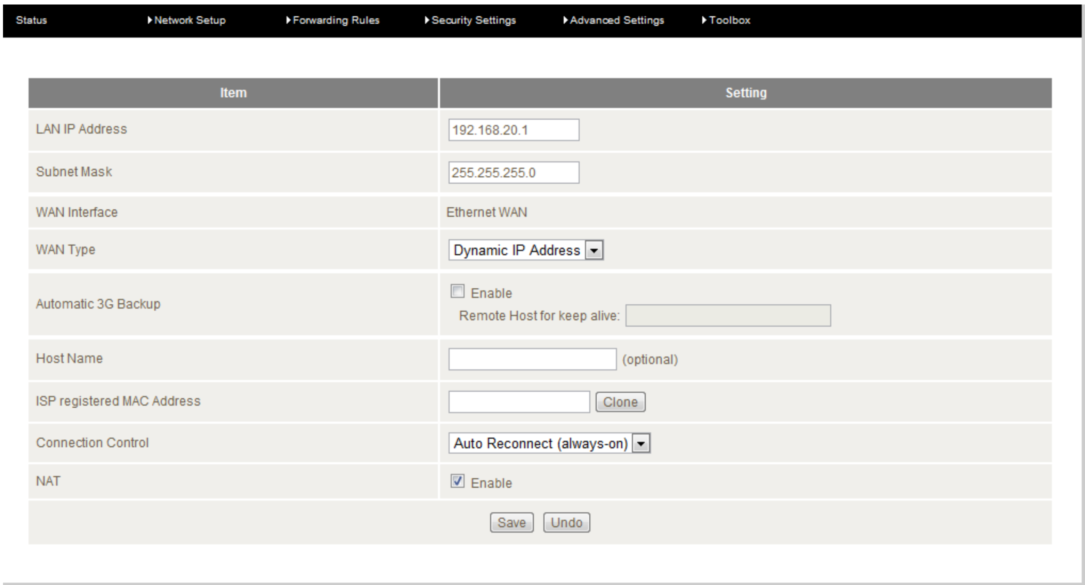
Ethernet WAN (xDSL/Cable/Satellite)

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

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

Please note: If you are utilising an Ethernet WAN connection, please ensure the "3G-DSL" switch is set to "DSL".

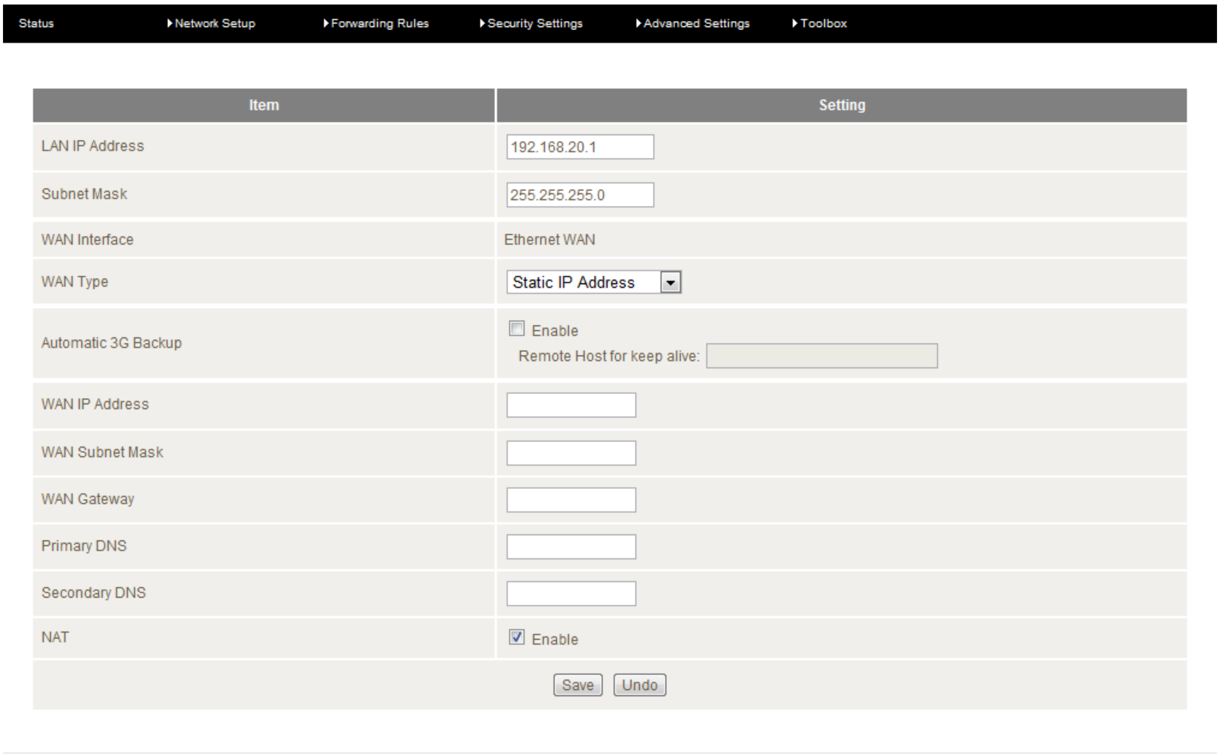
Dynamic IP



Item	Setting
LAN IP Address	192.168.20.1
Subnet Mask	255.255.255.0
WAN Interface	Ethernet WAN
WAN Type	Dynamic IP Address
Automatic 3G Backup	□ Enable Remote Host for keep alive:
Host Name	(optional)
ISP registered MAC Address	Clone
Connection Control	Auto Reconnect (always-on)
NAT	☑ Enable

OPTION	DEFINITION
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/4G modem *(Optional - Refer to your ISP for more information).*
Connection Control	There are 3 modes to select from: ▪ **Connect-on-demand:** The 3GM2WN will connect to the internet when a client sends outgoing packets. ▪ **Auto Reconnect (Always-on):** The 3GM2WN will automatically reconnect to the internet until the connection is manually disconnected. ▪ **Manually:** The 3GM2WN will not connect to the internet until someone clicks the connect button in the Status-page.
NAT	This option enables or disables "Network Address Translation" for this connection type.

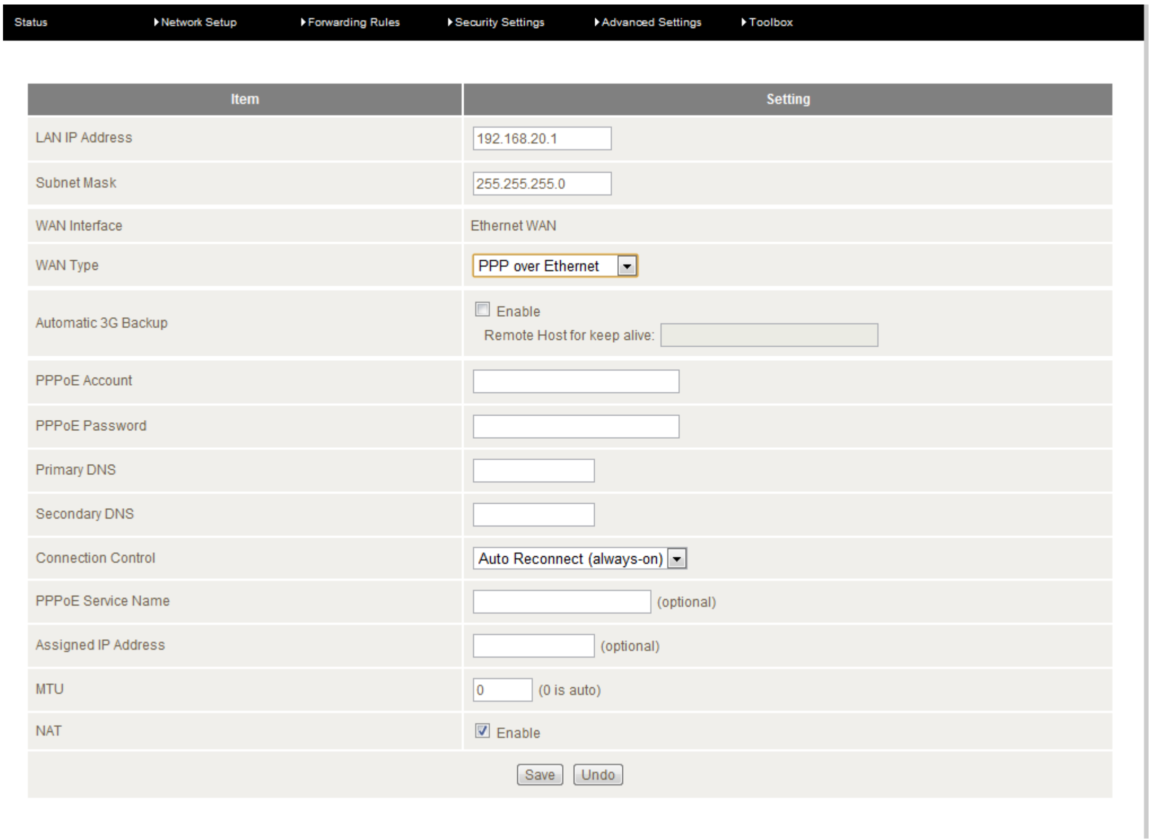
Static IP



Item	Setting
LAN IP Address	192.168.20.1
Subnet Mask	255.255.255.0
WAN Interface	Ethernet WAN
WAN Type	Static IP Address
Automatic 3G Backup	□ Enable Remote Host for keep alive:
WAN IP Address	
WAN Subnet Mask	
WAN Gateway	
Primary DNS	
Secondary DNS	
NAT	☑ Enable

OPTION	DEFINITION
WAN IP Address	Enter the WAN IP address used for your connection.
WAN Subnet Mask	Enter the WAN Subnet mask used for your connection.
WAN Gateway	Enter the WAN Gateway address used for your connection.
Primary DNS	Ente r the Primary DNS used for your connection.
Secondary DNS	Enter the Secondary DNS (if available) used for your connection.
NAT	This option enables or disables "Network Address Translation" for this connection type.

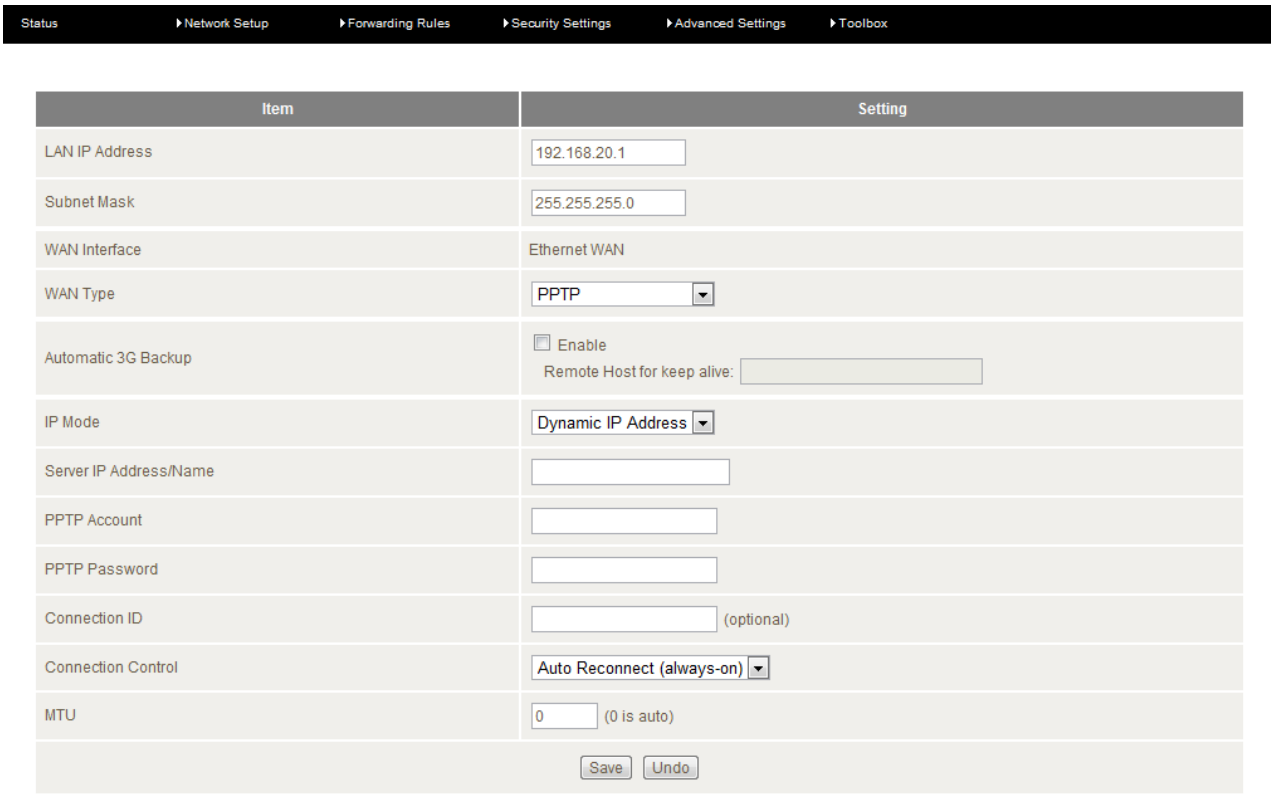
PPP over Ethernet



Item	Setting
LAN IP Address	192.168.20.1
Subnet Mask	255.255.255.0
WAN Interface	Ethernet WAN
WAN Type	PPP over Ethernet
Automatic 3G Backup	□ Enable Remote Host for keep alive:
PPPoE Account	
PPPoE Password	
Primary DNS	
Secondary DNS	
Connection Control	Auto Reconnect (always-on)
PPPoE Service Name	(optional)
Assigned IP Address	(optional)
MTU	0 (0 is auto)
NAT	☑ Enable

OPTION	DEFINITION
PPPoE Account	The account name given to you by your ISP.
PPPoE 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).*
Connection Control	There are 3 modes to select from: ▪ **Connect-on-demand:** The 3GM2WN will connect to the internet when a client sends outgoing packets. ▪ **Auto Reconnect (Always-on):** The 3GM2WN will automatically reconnect to the internet until the connection is manually disconnected. ▪ **Manually:** The 3GM2WN will not connect to the internet until someone clicks the connect button in the Status-page.
PPPoE 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

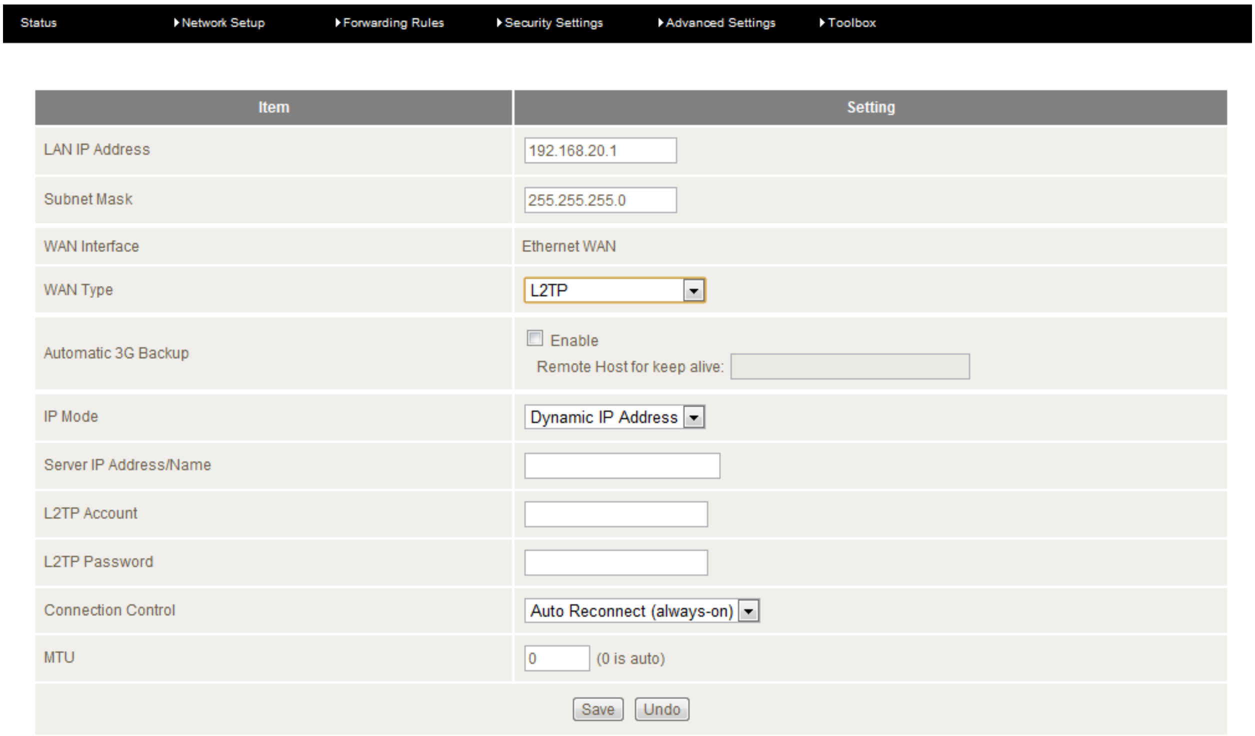
PPTP



Item	Setting
LAN IP Address	192.168.20.1
Subnet Mask	255.255.255.0
WAN Interface	Ethernet WAN
WAN Type	PPTP
Automatic 3G Backup	□ Enable Remote Host for keep alive:
IP Mode	Dynamic IP Address
Server IP Address/Name	
PPTP Account	
PPTP Password	
Connection ID	(optional)
Connection Control	Auto Reconnect (always-on)
MTU	0 (0 is auto)

OPTION	DEFINITION
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.
Connection Control	There are 3 modes to select from: ▪ **Connect-on-demand:** The 3GM2WN will connect to the internet when a client sends outgoing packets. ▪ **Auto Reconnect (Always-on):** The 3GM2WN will automatically reconnect to the internet until the connection is manually disconnected. ▪ **Manually:** The 3GM2WN will not connect to the internet until someone clicks the connect button in the Status-page.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.

L2TP



Item	Setting
LAN IP Address	192.168.20.1
Subnet Mask	255.255.255.0
WAN Interface	Ethernet WAN
WAN Type	L2TP
Automatic 3G Backup	□ Enable Remote Host for keep alive:
IP Mode	Dynamic IP Address
Server IP Address/Name	
L2TP Account	
L2TP Password	
Connection Control	Auto Reconnect (always-on)
MTU	0 (0 is auto)

OPTION	DEFINITION
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 L2TP 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.
Connection Control	There are 3 modes to select from: ▪ **Connect-on-demand:** The 3GM2WN will connect to the internet when a client sends outgoing packets. ▪ **Auto Reconnect (Always-on):** The 3GM2WN will automatically reconnect to the internet until the connection is manually disconnected. ▪ **Manually:** The 3GM2WN will not connect to the internet until someone clicks the connect button in the Status-page.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.

Wireless WAN Interface Types

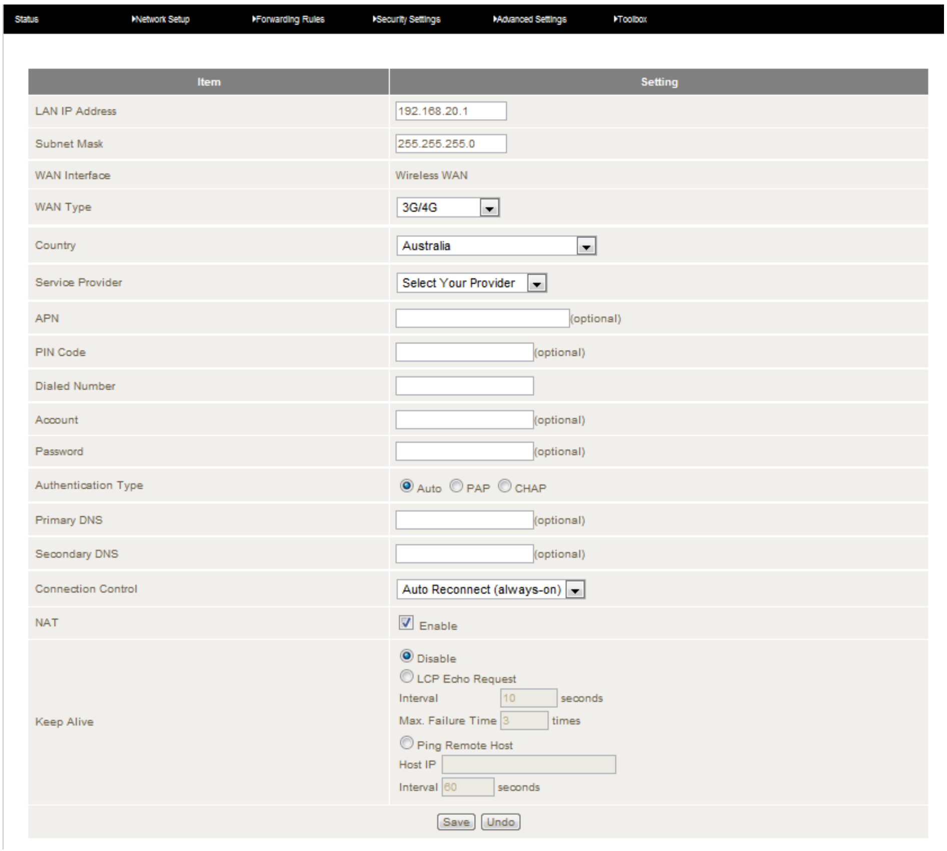
Ethernet WAN (3G/4G / WiFi Hotspot)

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

- 3G/4G
- WiFi Hotspot

Please note: If you are utilising an Ethernet WAN connection, please ensure the “3G-DSL” switch is set to “3G”.

3G/4G



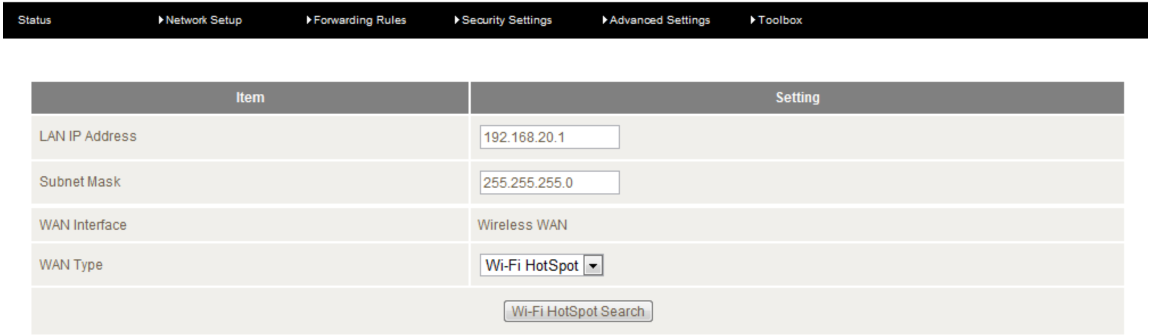
Item	Setting
LAN IP Address	192.168.20.1
Subnet Mask	255.255.255.0
WAN Interface	Wireless WAN
WAN Type	3G/4G
Country	Australia
Service Provider	Select Your Provider
APN	(optional)
PIN Code	(optional)
Dialed Number	
Account	(optional)
Password	(optional)
Authentication Type	● Auto ○ PAP ○ CHAP
Primary DNS	(optional)
Secondary DNS	(optional)
Connection Control	Auto Reconnect (always-on)
NAT	☑ Enable
Keep Alive	● Disable ○ LCP Echo Request Interval 10 seconds Max. Failure Time 3 times ○ Ping Remote Host Host IP Interval 60 seconds

OPTION	DEFINITION
Country	Select your country from the list. This will shorten the APN list to those in your selected country.
Service Provider	Select your 3G service provider from the list. This will then enable you to select the correct APN for the 3G service in use.
APN	Enter the APN for your 3G service. This should be automatically filled in after selecting your country and 3G provider name. If the wrong APN is shown, enter the correct APN for your 3G service
PIN Code	Enter the Pin Code for your SIM card (if required). Dial Number This number is required to connect to your 3G service. (Unless advised otherwise by NetComm Technical Support, this setting should not be changed)
Username	The username provided by your 3G service provider to enable access to your 3G service.
Password	The password provided by your 3G service provider to enable access to your 3G service.
Authentication Type	Choose the appropriate authentication type for your 3G service.
Primary DNS	Manually assign a Primary DNS Server.
Secondary DNS	Manually assign a Secondary DNS Server.
Connection Control	There are 3 modes to select from: ▪ **Connect-on-demand:** The 3GM2WN will connect to the internet when a client sends outgoing packets. ▪ **Auto Reconnect (Always-on):** The 3GM2WN will automatically reconnect to the internet until the connection is manually disconnected. ▪ **Manually:** The 3GM2WN will not connect to the internet until someone clicks the connect button in the Status-page.
Keep Alive	There are three keep alive options to select from: ▪ **Disable:** Disable the keep alive function. ▪ **LCP Echo Request:** The 3GM2WN will automatically verify the connection is active. Set the interval and Max. number of failures to determine when the connection is up or down. ▪ **Ping Remote Host:** The 3GM2WN will ping the chosen host IP to verify the connection is active. Set the host IP address and the interval between ping tests.

WiFi Hotspot

This WAN type allows you to share one WiFi hotspot account with your friends or colleagues. Local clients connect to this router via a WiFi connection, and surf the Internet by connecting to a remote WiFi hotspot. Follow the few steps below to connect to a remote WiFi Hotspot.

⚠ If choosing WiFi HotSpot WAN type, the wireless channel of the Wireless network will be set to the same channel as used on the remote WiFi HotSpot.



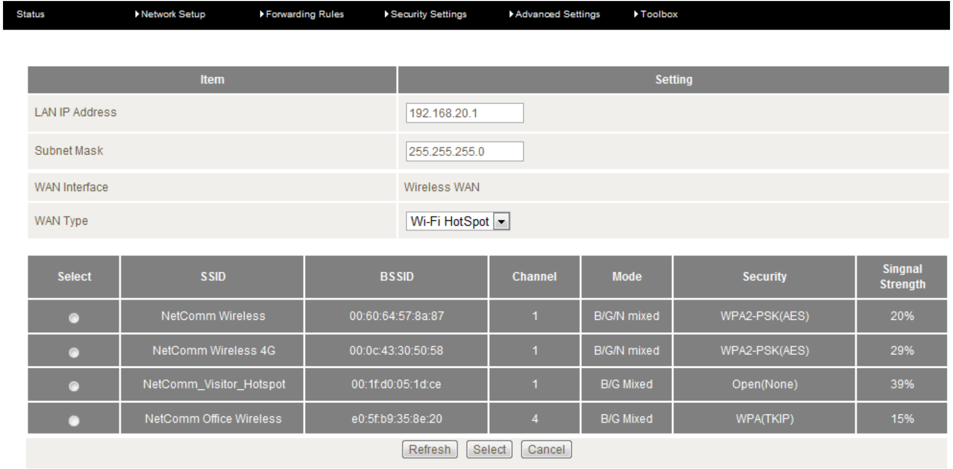
Item	Setting
LAN IP Address	192.168.20.1
Subnet Mask	255.255.255.0
WAN Interface	Wireless WAN
WAN Type	Wi-Fi HotSpot

Step 1:

Click “WiFi HotSpot Search” button to search for any available WiFi hotspots or WiFi APs (Access Points) nearby.

Step 2:

After searching, a list of the all available WiFi APs around you will be shown. Select the appropriate Wireless network and click the “Select” button to start the connection or press “Refresh” button to search again.

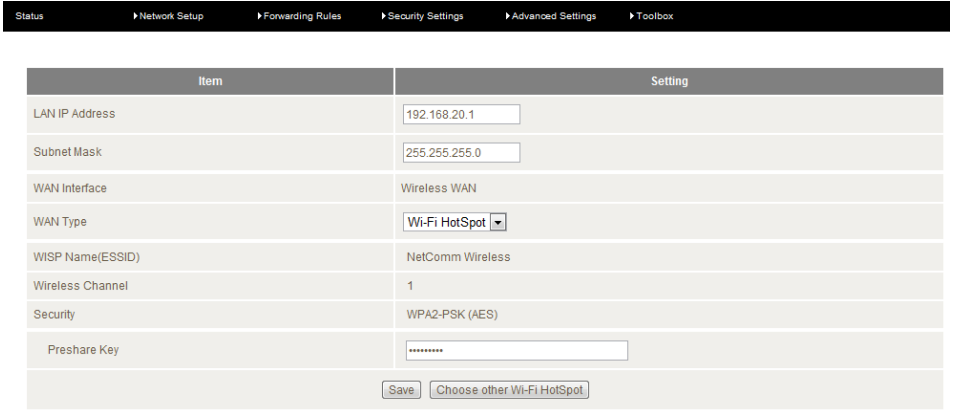


Item	Setting
LAN IP Address	192.168.20.1
Subnet Mask	255.255.255.0
WAN Interface	Wireless WAN
WAN Type	Wi-Fi HotSpot

Select	SSID	BSSID	Channel	Mode	Security	Singnal Strength
○	NetComm Wireless	00:60:64:57:8a:87	1	B/G/N mixed	WPA2-PSK(AES)	20%
○	NetComm Wireless 4G	00:0c:43:30:50:58	1	B/G/N mixed	WPA2-PSK(AES)	29%
○	NetComm_Visitor_Hotspot	00:1f:d0:05:1d:ce	1	B/G Mixed	Open(None)	39%
○	NetComm Office Wireless	e0:5f:b9:35:8e:20	4	B/G Mixed	WPA(TKIP)	15%

Step 3:

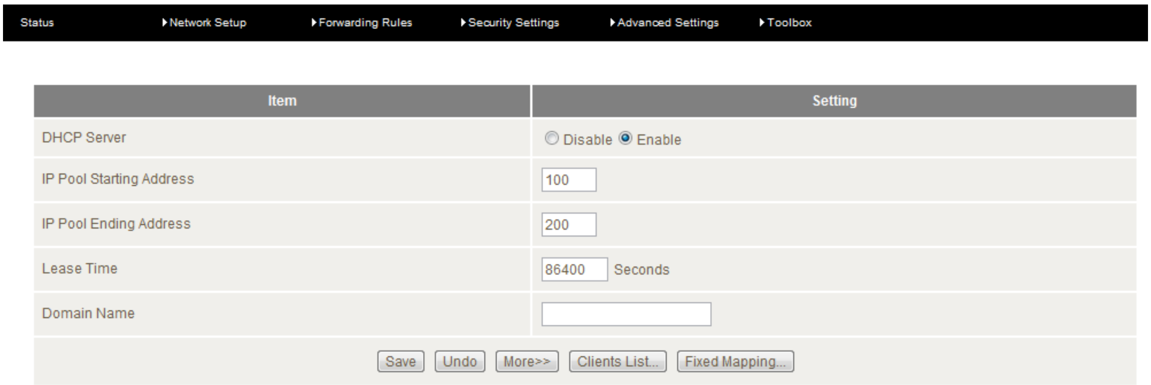
If required, you can enter the Wireless security for the remote wireless network. Click the “Save” button to save your selected settings. The Device will reboot so that the new setting can take effect.



Item	Setting
LAN IP Address	192.168.20.1
Subnet Mask	255.255.255.0
WAN Interface	Wireless WAN
WAN Type	Wi-Fi HotSpot
WISP Name(ESSID)	NetComm Wireless
Wireless Channel	1
Security	WPA2-PSK (AES)
Preshare Key	•••••••••

DHCP Server

This Page allows you to change the Dynamic Host Configuration Protocol (DHCP) server settings on the 3GM2WN. The DHCP Server enables computers or devices connecting to the 3GM2WN to automatically obtain their network configuration settings. By default, the DHCP server is enabled.



Item	Setting
DHCP Server	○ Disable ● Enable
IP Pool Starting Address	100
IP Pool Ending Address	200
Lease Time	86400 Seconds
Domain Name	

OPTION	DEFINITION
DHCP Server	Enable or disable the DHCP server.
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

Click "Save" to save these settings or “Undo” to cancel.

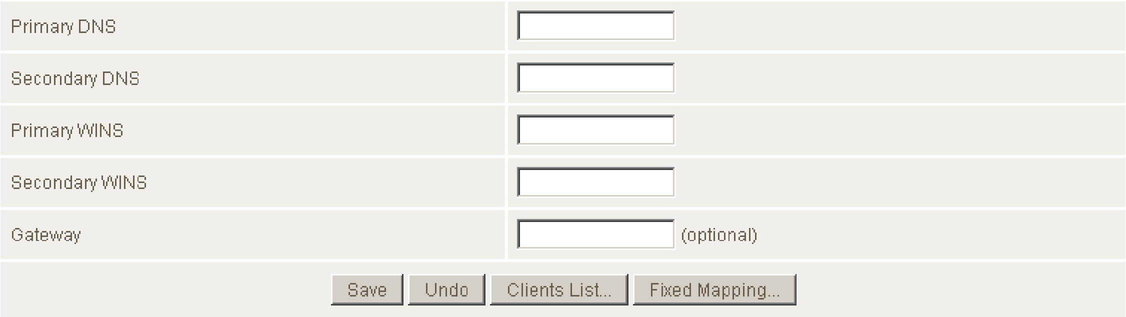
You can also check the DHCP client list by clicking the “Client List” button.

Please note: See the section “DHCP Client List” below for more information

The “Fixed Mapping…” button allows you to map a specific IP address to a specific MAC address.

Please note: See the section “DHCP Fixed Mapping” below for more information

Click the "More…" button for the following extended options:

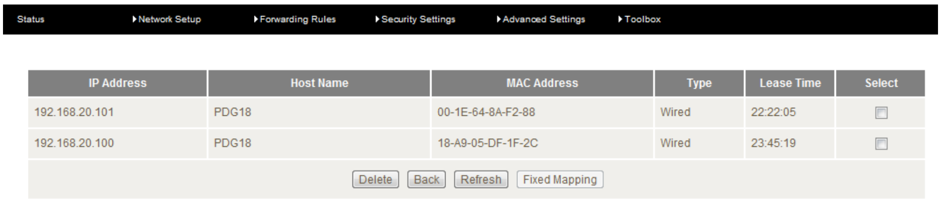


Primary DNS	
Secondary DNS	
Primary WINS	
Secondary WINS	
Gateway	(optional)

OPTION	DEFINITION
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

DHCP Client List

This is the list of currently connected devices utilising DHCP.

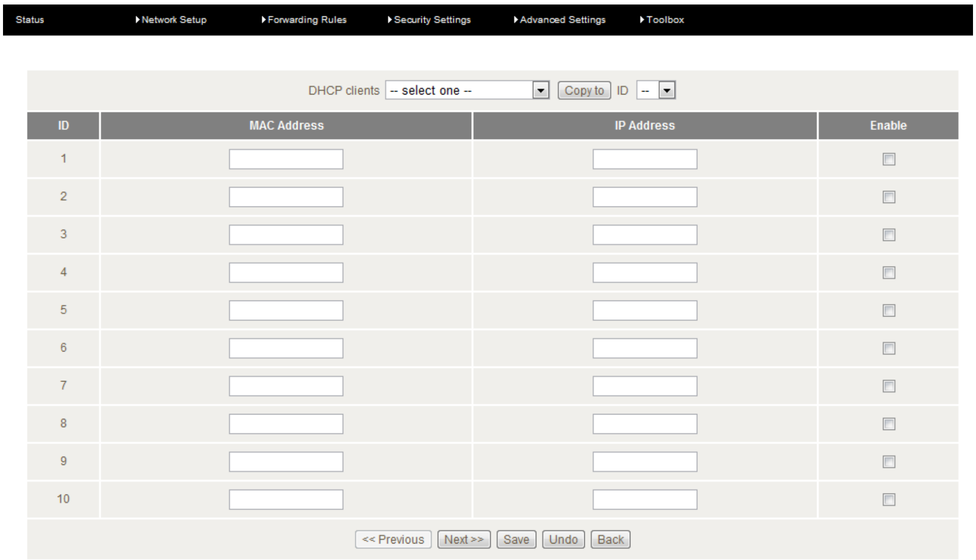


IP Address	Host Name	MAC Address	Type	Lease Time	Select
192.168.20.101	PDG18	00-1E-64-8A-F2-88	Wired	22:22:05	□
192.168.20.100	PDG18	18-A9-05-DF-1F-2C	Wired	23:45:19	□

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			□
2			□
3			□
4			□
5			□
6			□
7			□
8			□
9			□
10			□

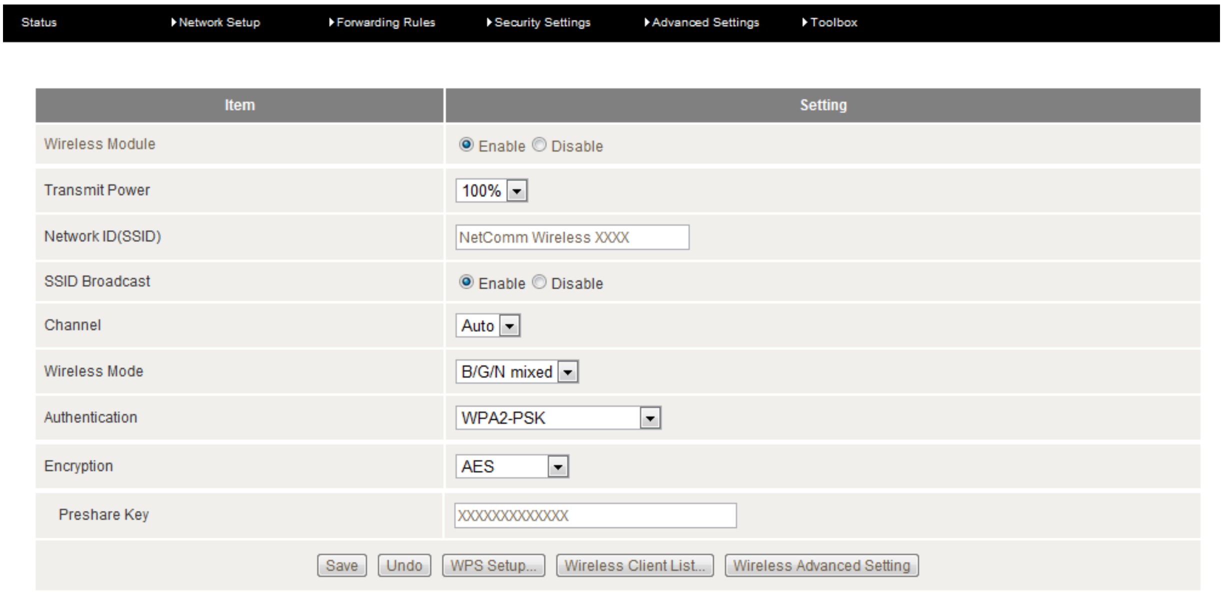
The DHCP Server will reserve a specific IP for a device based on that devices unique MAC address.

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.

Click on the "Enable" checkbox to activate the DHCP fixed mapping entry.

Wireless

The Wireless LAN settings page allows you to configure the wireless network features of the router.



Item	Setting
Wireless Module	● Enable ○ Disable
Transmit Power	100%
Network ID(SSID)	NetComm Wireless XXXX
SSID Broadcast	● Enable ○ Disable
Channel	Auto
Wireless Mode	B/G/N mixed
Authentication	WPA2-PSK
Encryption	AES
Preshare Key	XXXXXXXXXXXXX

OPTION	DEFINITION
Wireless Module	Select to enable or disable the Wireless network function of the 3GM2WN.
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	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)

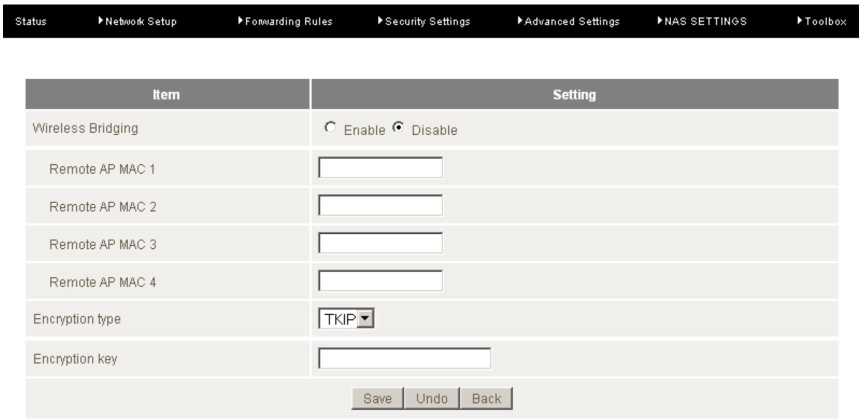
Please Note: The configuration for WPA-PSK and WPA2-PSK is identical

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 to 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.

WDS (Wireless Bridging)

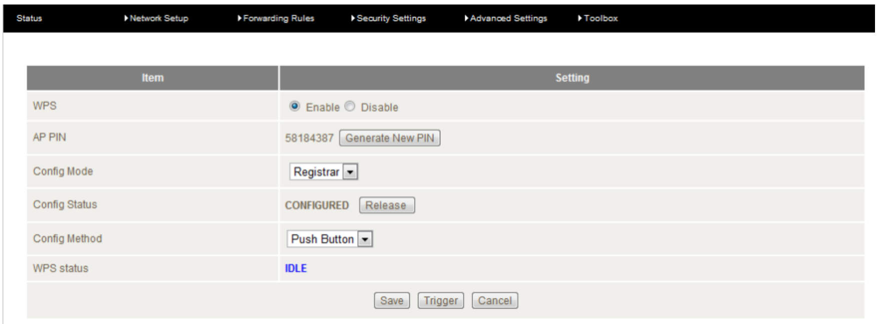


Item	Setting
Wireless Bridging	○ Enable ● Disable
Remote AP MAC 1	
Remote AP MAC 2	
Remote AP MAC 3	
Remote AP MAC 4	
Encryption type	TKIP
Encryption key	

Wireless Distribution System (WDS) allows you to connect to other wireless access points (Remote APs), and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.

Enter the MAC address of the other wireless access points taking part in the WDS network and then click “Save”.

WPS Setup



Item	Setting
WPS	● Enable ○ Disable
AP PIN	58184387 Generate New PIN
Config Mode	Registrar
Config Status	CONFIGURED Release
Config Method	Push Button
WPS status	IDLE

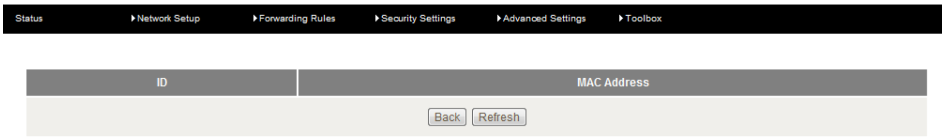
Wi-Fi Protected Setup (WPS) offers safe and easy way to connect wirelessly.

Simply push the WPS button on the router and then press the WPS on your wireless device within 2 minutes and the WLAN connection should be completed automatically.

OPTION	DEFINITION
AP PIN	The current PIN used to connect. ▪ Click “Generate New PIN” to force the router to create a new PIN.
Config Mode	Set the router to be either the Registrar or Enrollee.
Config Status	You can discard the current WPS configuration by clicking “Release”.
Config Method	Set the WPS configuration method to either Push Button or PIN code.

Please note: These settings should not need to be changed.

Wireless Client List

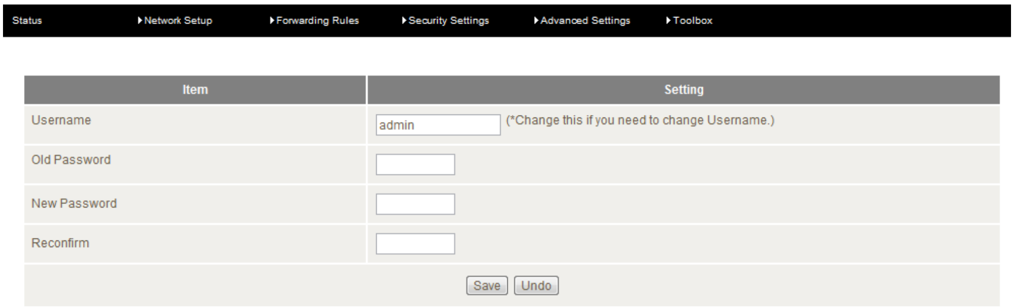


ID	MAC Address

The list of currently connected wireless devices is shown here.

Change Password

This page allows you to change the 3GM2WN web configuration password.



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

Please type in the old password or username *(the factory default username and password is admin)* and then type in the new password. Type the same 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:

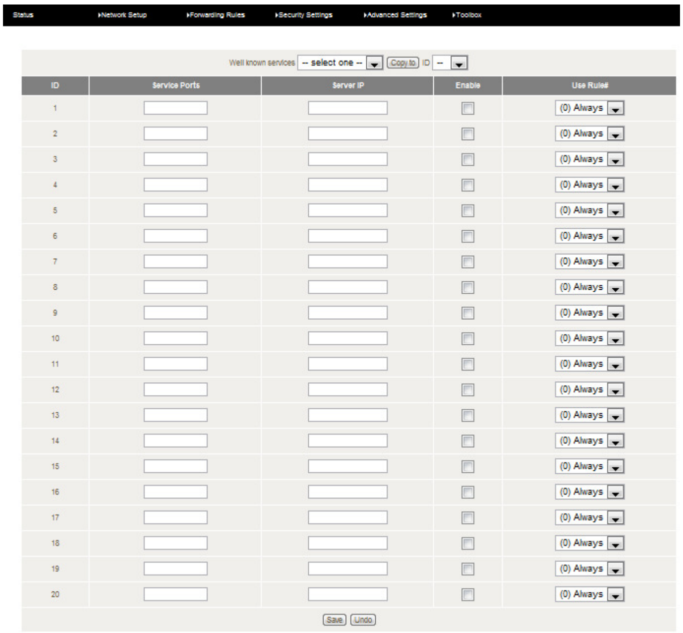
- Port Forwarding (available in the Virtual Server page)
- Port Triggering (available in the Special AP page)
- DMZ Host (available in the Miscellaneous page)

Virtual Server

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.

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

Please 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 --

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

For example, if you have an FTP server (the default port is 21) at 192.168.20.10, 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:

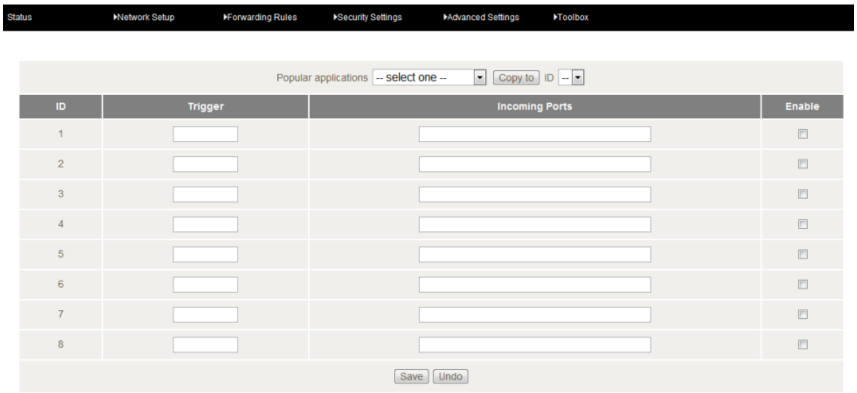
Please note: At any given time, only one IP address can bind to a particular Service Port.

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.

Special AP

Some applications like On-line 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 3GM2WN.



Popular applications -- select one -- ID --

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

The Special Applications feature allows some of these applications to work with this router.

Please Note: If this fails to make the application work, try to set up 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.

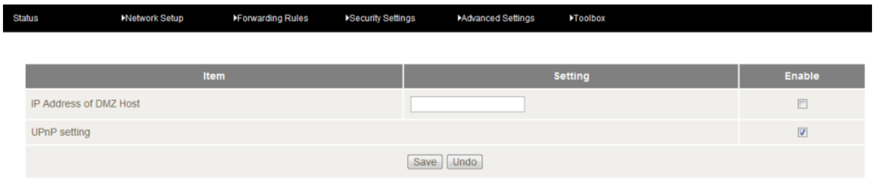
The 3GM2WN also provides predefined settings for some popular applications.

To use the predefined settings, select your application from the Popular application pull down ist, 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
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 click on "**Enable**".

Please Note: This feature should be used only when necessary.

OPTION	DEFINITION
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.

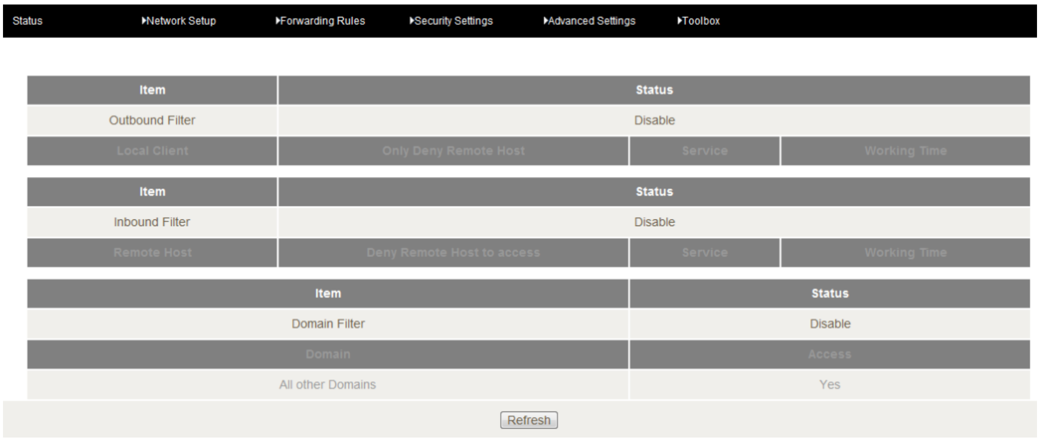
Click "Save" to save the settings or "Undo" to cancel.

Security Settings

The Security Setting page allows you to configure the security management on the router such as Packet filters and MAC Control. Click on any of the menu items on the left to access the respective setting page.

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

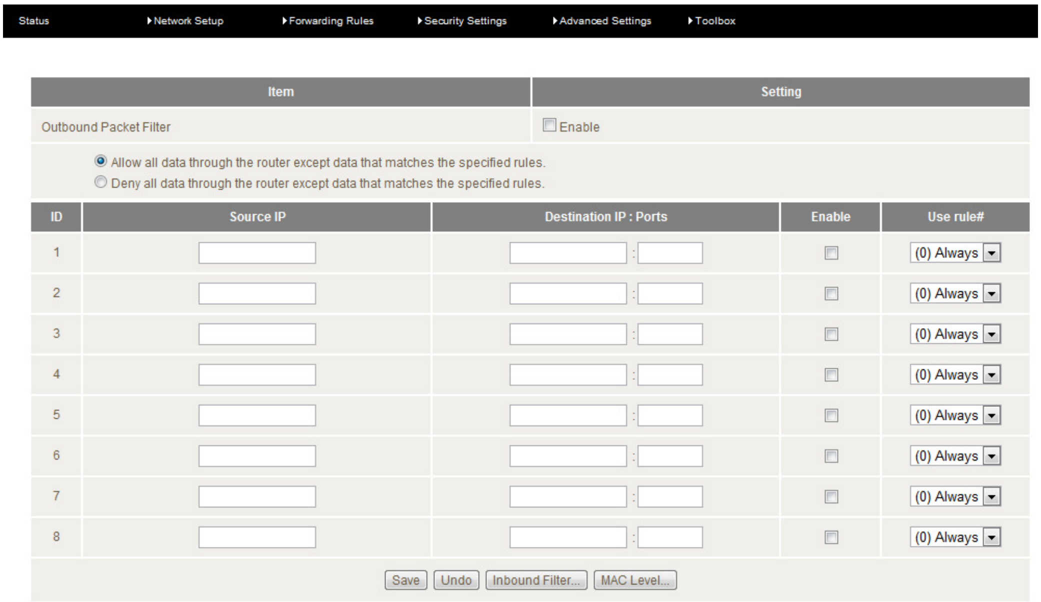
Packet Filters

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.

Please 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 (192.168.20.1) or a range of IP addresses (192.168.20.100-192.168.20.200). 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.

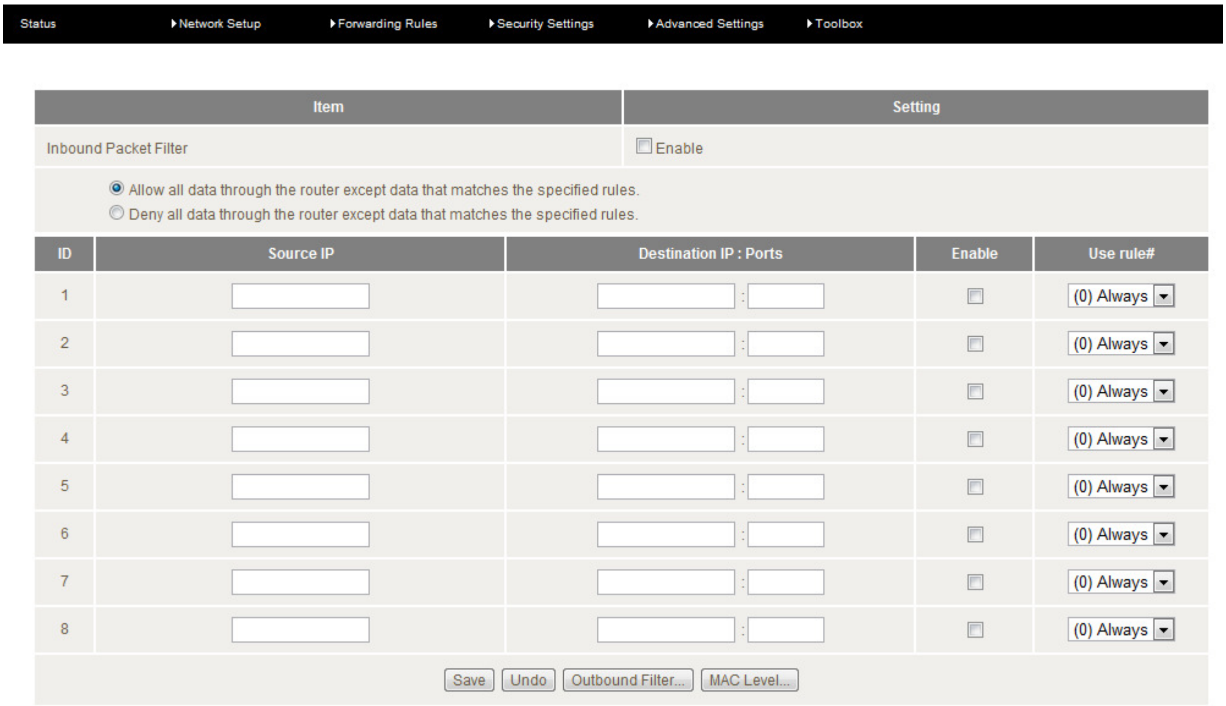
The Packet Filter also works with Scheduling Rules, and gives you more flexibility on Access control.

Please 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.

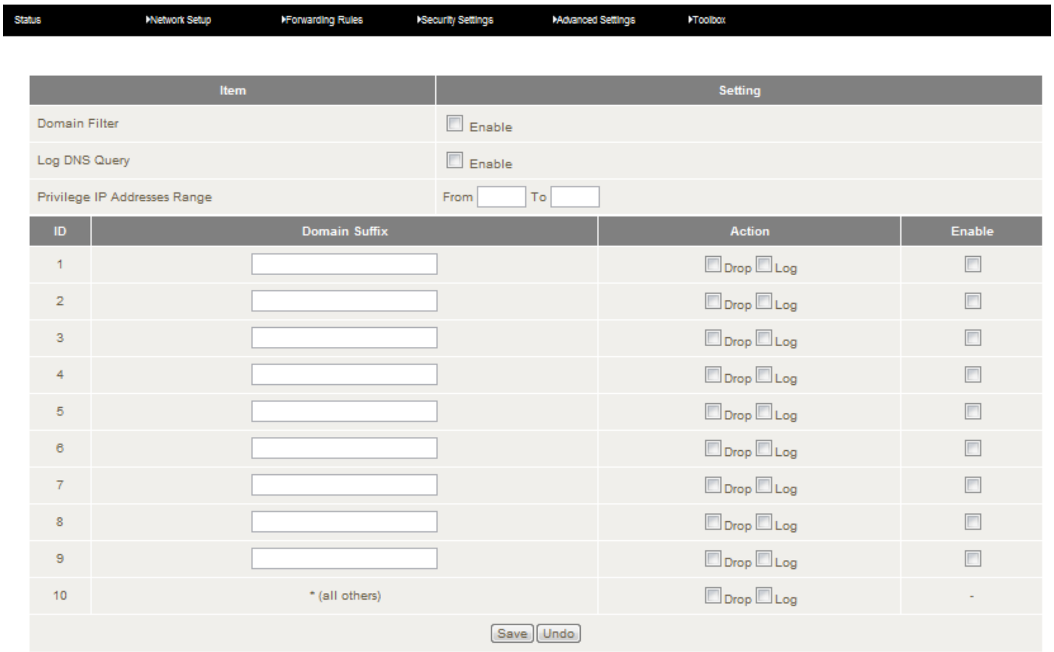
ID	Source IP	Destination IP : Ports	Enable	Use rule#
1		:	□	(0) Always
2		:	□	(0) Always
3		:	□	(0) Always
4		:	□	(0) Always
5		:	□	(0) Always
6		:	□	(0) Always
7		:	□	(0) Always
8		:	□	(0) Always

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, tick 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:

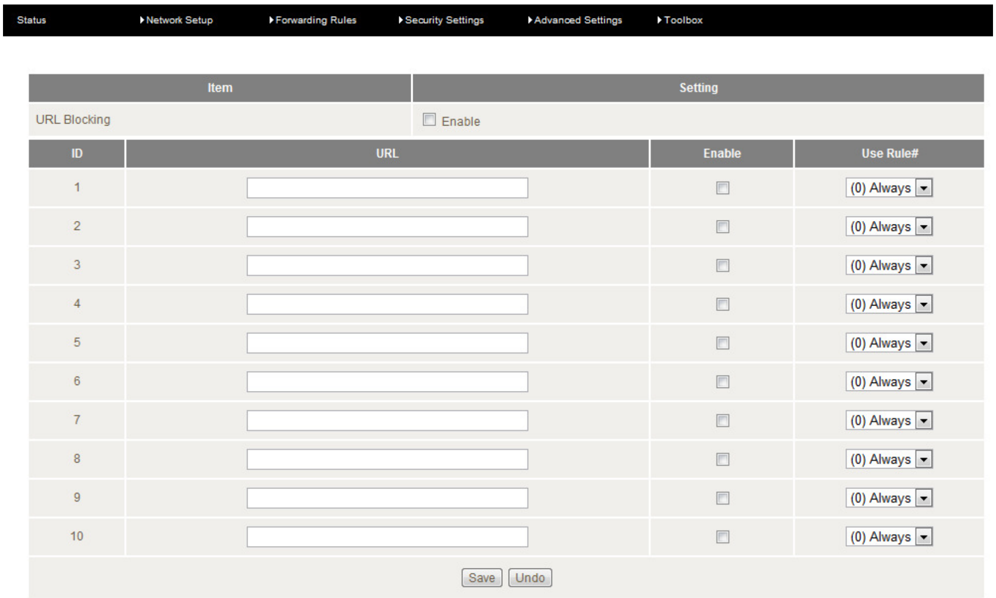
OPTION	DEFINITION
Domain Suffix	Please type the suffix of the URL that needs to be restricted. For example, ".com", "xxx. com".
Action	The router action that you want when someone is accessing a URL that matches the specified domain suffix. Select Drop to block the access and/or select Log to log this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

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

URL Blocking

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

To enable URL Blocking, tick the “Enable” tick box at the top of the page.



Item	Setting
URL Blocking	□ Enable

ID	URL	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

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

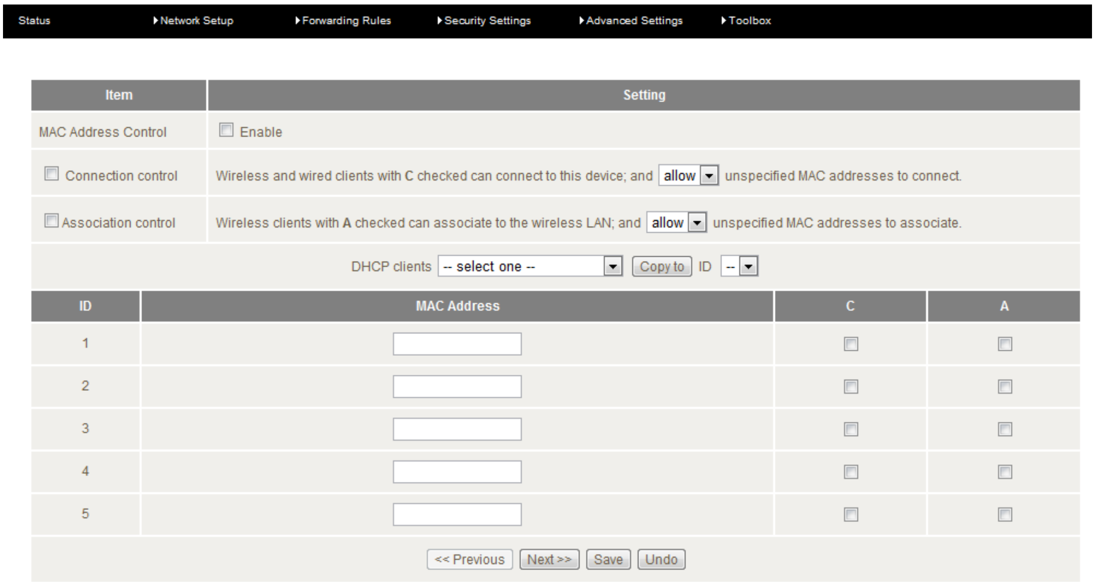
OPTION	DEFINITION
URL	If any part of the Website’s URL matches the pre-defined word then the connection will be blocked. For example, you can use pre-defined word "sex" to block all websites if their URLs contain the pre-defined word "sex".
Enable	Tick to enable the rule.

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, tick the “Enable” tick box 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		□	□

<< Previous Next >> Save Undo

Two types of MAC Control are available:

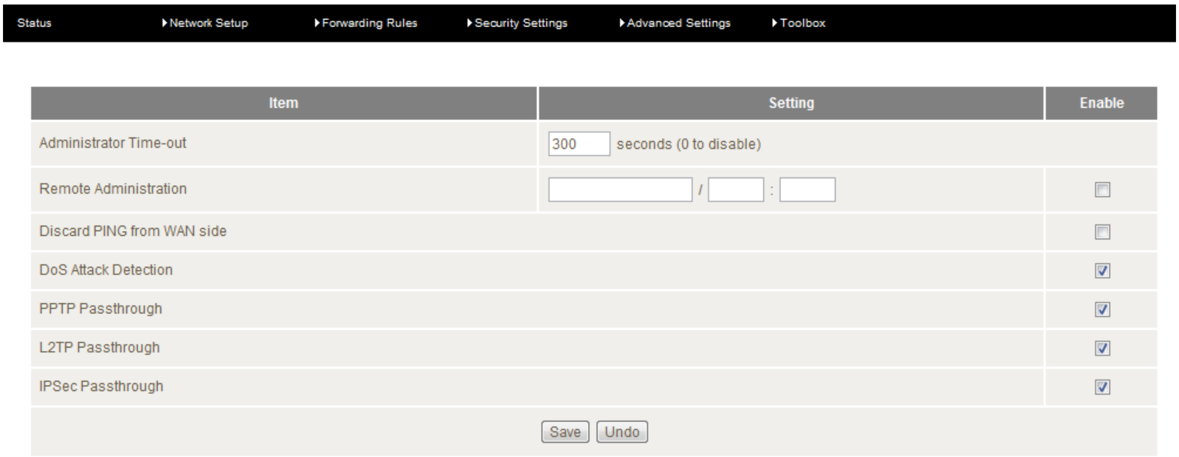
OPTION	DEFINITION
Connection control (C column)	Use this to control which clients (wired and wireless) can connect to the unit. If a client is denied access to connect to this device, it means the client cannot access the Internet either. Choose to allow or deny clients with MAC addresses that are not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

Please 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 miscellaneous 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		☑
PPTP Passthrough		☑
L2TP Passthrough		☑
IPSec Passthrough		☑

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.
PPTP Passthrough	When this feature is enabled, the router will allow PPTP traffic to passthrough
L2TP Passthrough	When this feature is enabled, the router will allow L2TP traffic to passthrough
IPSec Passthrough	When this feature is enabled, the router will allow IPSec traffic to passthrough

Please 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

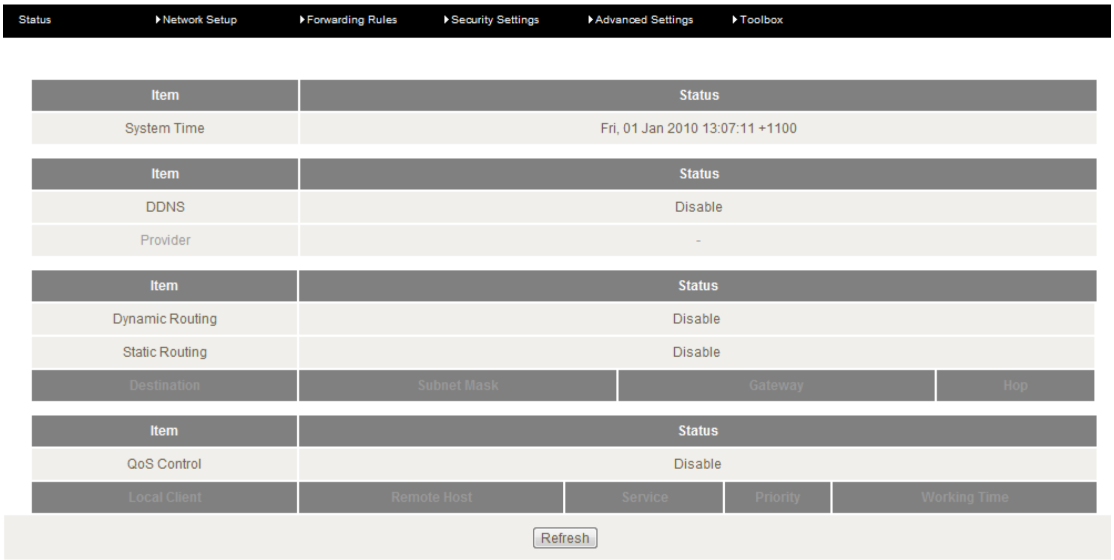
Click "Save" to save the settings or "Undo" to cancel.

Advanced Settings

The Advanced Setting page allows you to configure the advanced settings on the router such as the System log, Dynamic DNS and SNMP options. Click on any of the menu items on the left to configure the access the respective setting page.

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	Fri, 01 Jan 2010 13:07:11 +1100

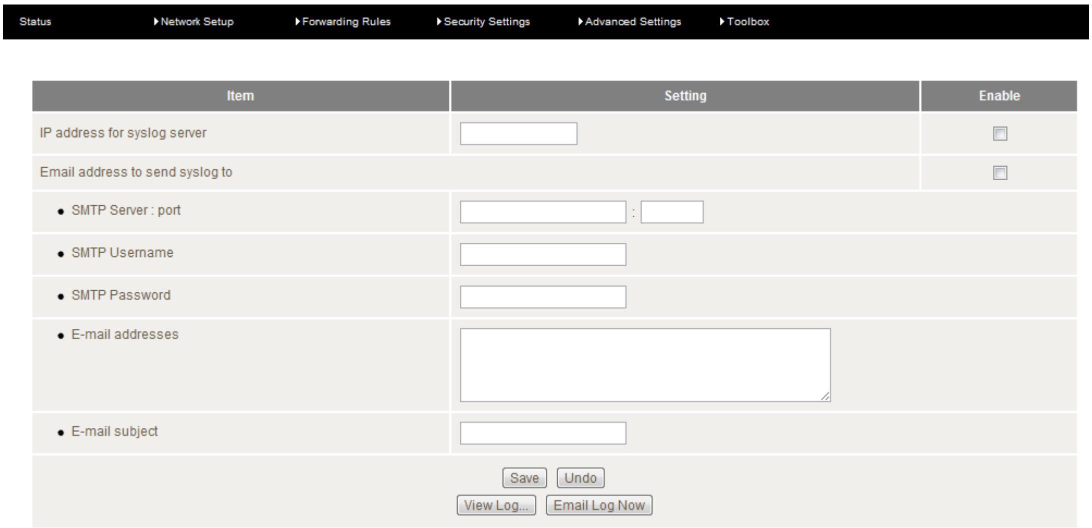
Item	Status
DDNS	Disable
Provider	-

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		

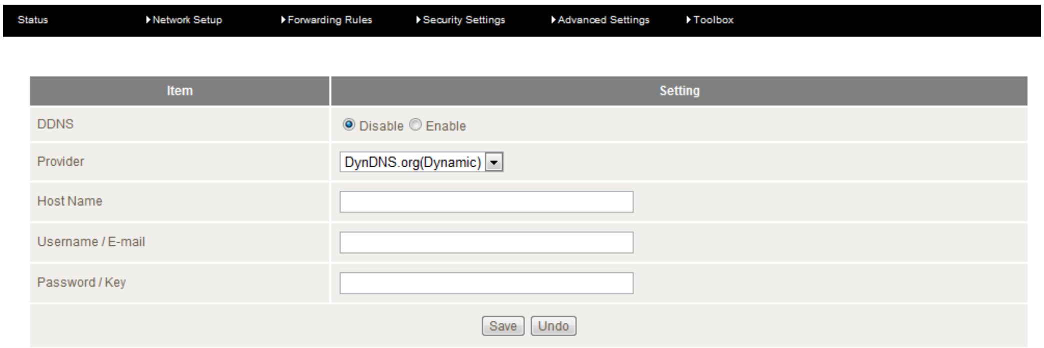
OPTION	DEFINITION
IP Address for remote System Logs (syslog)	The IP address of the syslog server where the system log data will be sent. Click the "Enable" checkbox to enable this function.
Email address to send syslog to	Click the “Enable” checkbox to enable this function.
SMTP Server : port	Enter the 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 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:

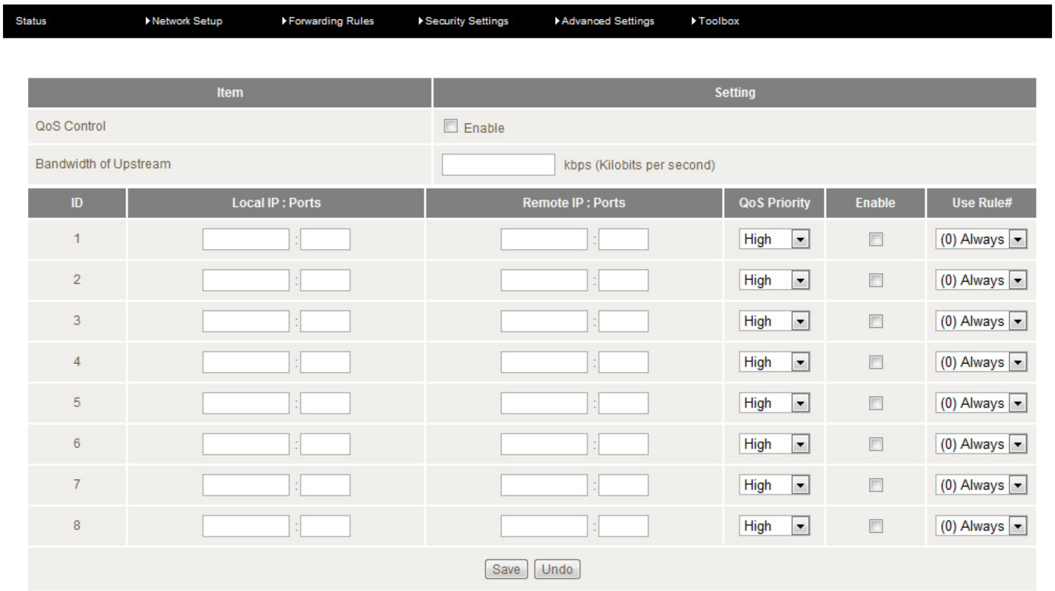
- Host Name
- Username/Email
- Password/Key

To enable the Dynamic DNS feature on the unit, click the “Enable” check box, 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.



Status ▸Network Setup ▸Forwarding Rules ▸Security Settings ▸Advanced Settings ▸Toolbox

Item	Setting
QoS Control	□ Enable
Bandwidth of Upstream	kbps (Kilobits per second)

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1	:	:	High	□	(0) Always
2	:	:	High	□	(0) Always
3	:	:	High	□	(0) Always
4	:	:	High	□	(0) Always
5	:	:	High	□	(0) Always
6	:	:	High	□	(0) Always
7	:	:	High	□	(0) Always
8	:	:	High	□	(0) Always

Save Undo

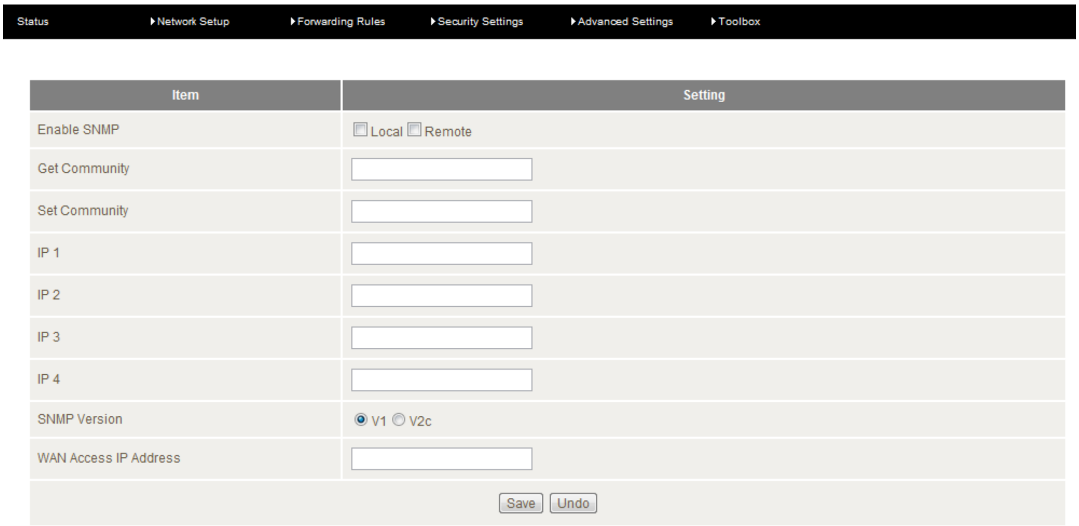
OPTION	DEFINITION
QoS Control:	This item enables QoS function or not.
Bandwidth of Upstream	Set the limit on the upstream speed.
Local IP: Ports	Define the Local IP address and port to apply QoS to.
Remote IP: Ports	Define the Remote IP address and port to apply QoS to.
QoS Priority	This defines the priority level of the current Policy Configuration. Packets associated with this policy will be services based upon the priority level set. For critical applications High or Normal levels are recommended. For non-critical applications select a Low level.
User Rule#:	The QoS rules can work in conjunction with Scheduling Rules.

Please 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.

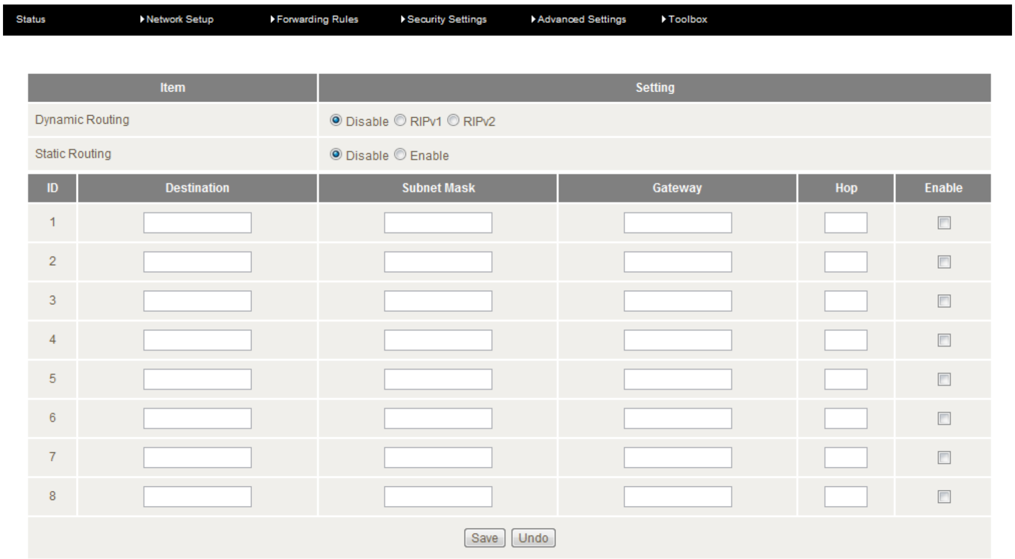
Please note: If "Remote" access is enabled, the default setting of 0.0.0.0 means any IP obtain SNMP protocol Information.

Click on "Save" to store your setting or "Undo" 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 3GM2WN.



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.

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

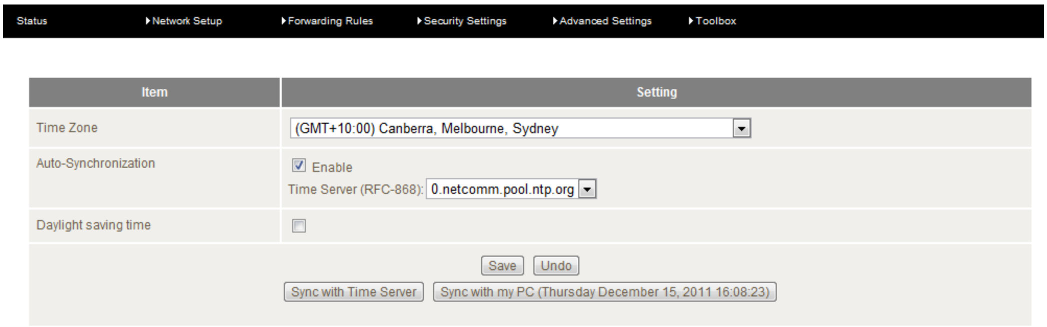
Static Routing:
For static routing, you can specify up to 8 routing rules.

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

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

System Time

This page allows you to change the System time setting on the 3GM2WN.



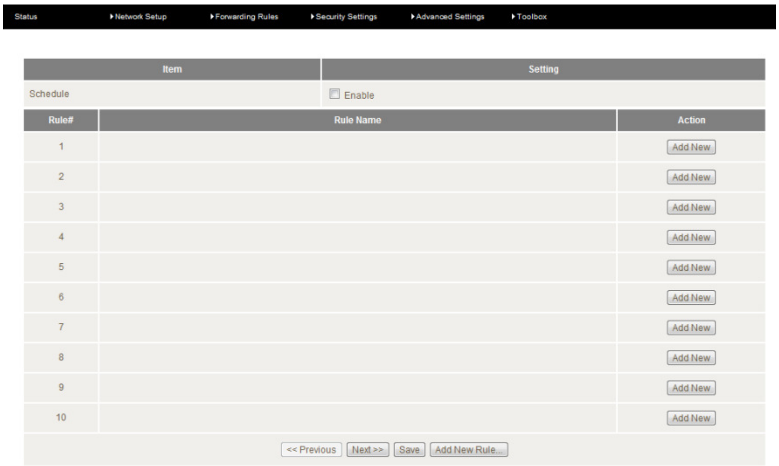
Item	Setting
Time Zone	(GMT+10:00) Canberra, Melbourne, Sydney
Auto-Synchronization	☑ Enable Time Server (RFC-868): 0.netcomm.pool.ntp.org
Daylight saving time	□

OPTION	DEFINITION
Time Zone	Select the time zone where this device is located.
Auto-Synchronization	Select the "Enable" checkbox to enable this function.
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

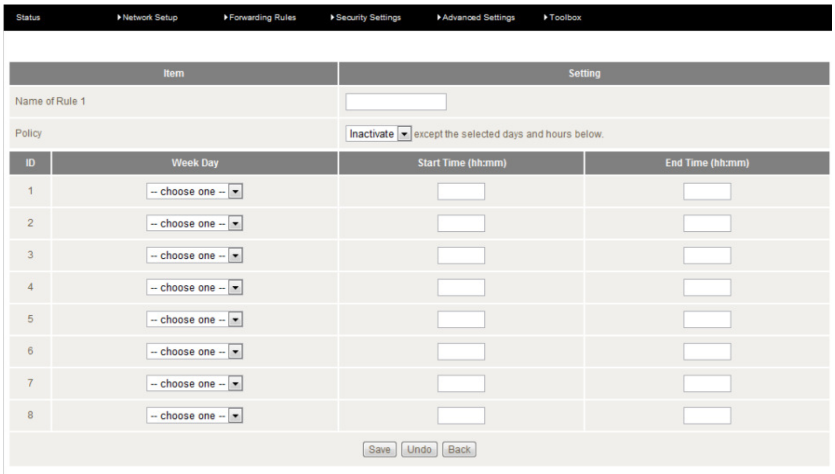
You can use scheduling to enable or disable a service at a specific time or on a specific day.



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 "New Add" button.



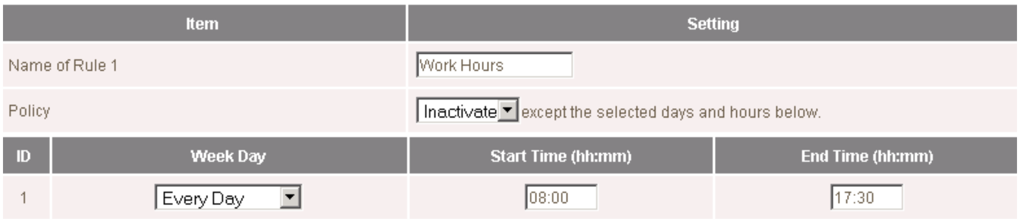
Item	Setting
Name of Rule 1	
Policy	Inactivate ▾ except the selected days and hours below.

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 "Save"

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

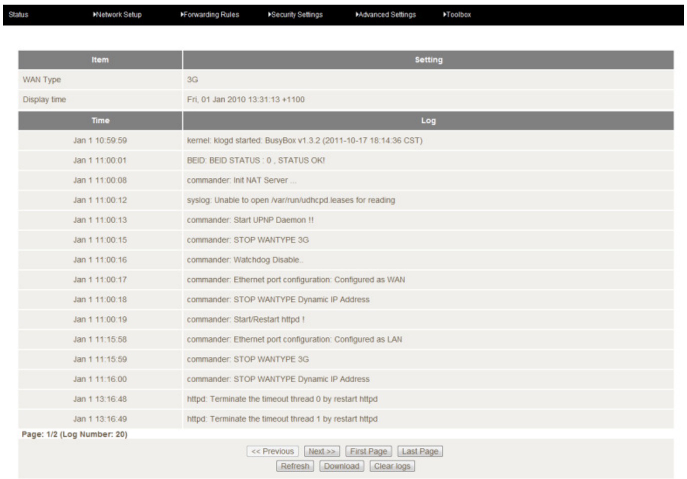
This example would prevent any access to the IP address 66.102.11.104 from any device connected to the router, 7 days a week, only between the hours of 08:00 and 17:30.

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

Toolbox

System Info

From this page you can view the current System log entries for the router.



Item	Setting
WAN Type	3G
Display time	Fri, 01 Jan 2010 13:31:13 +1100

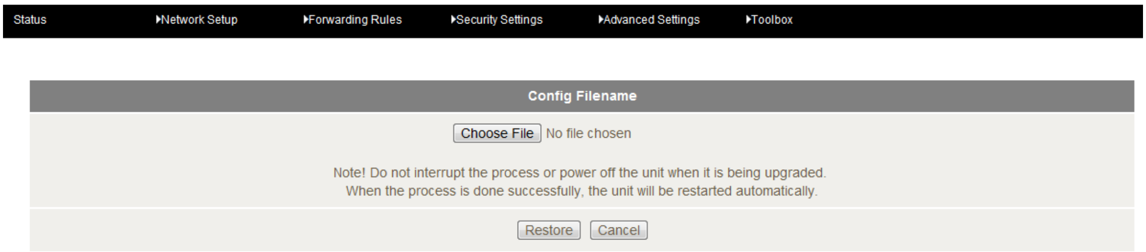
Time	Log
Jan 1 10:59:59	kernel: klogd started: BusyBox v1.3.2 (2011-10-17 18:14:36 CST)
Jan 1 11:00:01	BEID: BEID STATUS : 0 , STATUS OK!
Jan 1 11:00:08	commander: Init NAT Server ...
Jan 1 11:00:12	syslog: Unable to open /var/run/udhcpd.leases for reading
Jan 1 11:00:13	commander: Start UPNP Daemon !!
Jan 1 11:00:15	commander: STOP WANTYPE 3G
Jan 1 11:00:16	commander: Watchdog Disable..
Jan 1 11:00:17	commander: Ethernet port configuration: Configured as WAN
Jan 1 11:00:18	commander: STOP WANTYPE Dynamic IP Address
Jan 1 11:00:19	commander: Start/Restart httpd !
Jan 1 11:15:58	commander: Ethernet port configuration: Configured as LAN
Jan 1 11:15:59	commander: STOP WANTYPE 3G
Jan 1 11:16:00	commander: STOP WANTYPE Dynamic IP Address
Jan 1 13:16:48	httpd: Terminate the timeout thread 0 by restart httpd
Jan 1 13:16:49	httpd: Terminate the timeout thread 1 by restart httpd

Page: 1/2 (Log Number: 20)

You can also select to save a copy of the syslog data to your computer by clicking the "Download" button or clear the current syslog data by clicking the "Clear Logs" button.

Restore Settings

This page enables you to restore a previously saved backup of the 3GM2WN’s configuration.



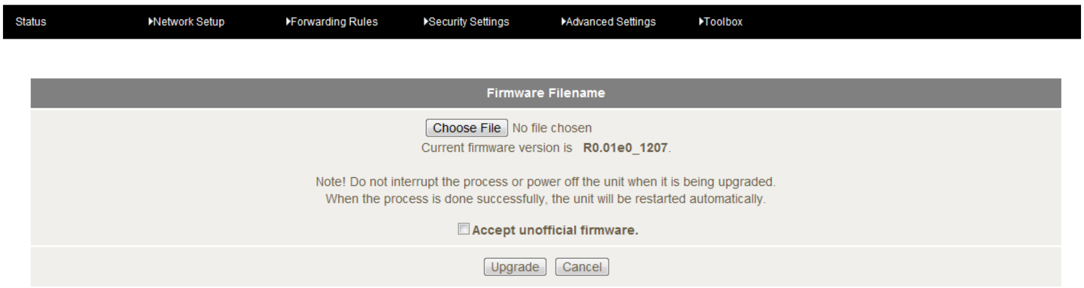
No file chosen

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.

Click the "Browse" button and navigate to the location you previously saved the configuration file.
Click the "Restore" button once you have selected the appropriate .bin file to use.

Firmware Upgrade

This page enables you to update the firmware on the 3GM2WN.



No file chosen
Current firmware version is **R0.01e0_1207**.

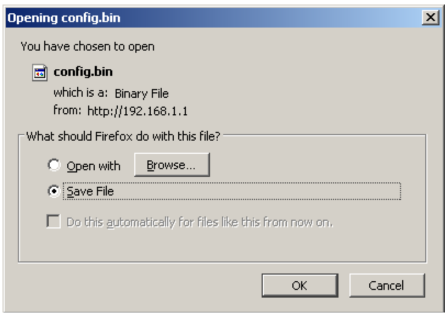
Note! Do not interrupt the process or power off the unit when it is being upgraded.
When the process is done successfully, the unit will be restarted automatically.

□ **Accept unofficial firmware.**

Click the "Browse" button and navigate to the location you saved the firmware update file.
You can then upgrade the routers firmware by clicking the "Upgrade" button.

Backup Settings

You can backup your current settings by clicking the "Backup Setting" button then and save it as a bin file.



Opening config.bin

You have chosen to open

config.bin

which is a: Binary File

from: http://192.168.1.1

What should Firefox do with this file?

○ Open with Browse...

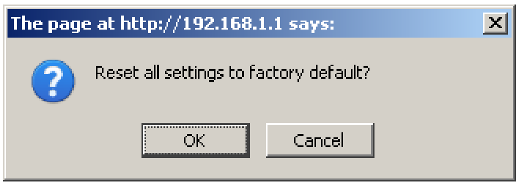
● Save File

□ Do this automatically for files like this from now on.

When you want to restore these settings, click the "Restore Setting" link and use the bin file you saved.

Reset to Default

You can reset your 3GM2WN to the factory default settings by clicking on this link.



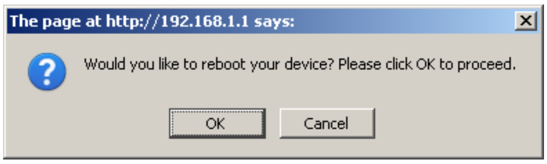
The page at http://192.168.1.1 says:

Reset all settings to factory default?

After clicking "OK", the router will reset and start up with the default settings loaded.

Reboot

You can reboot your router by clicking on the "Reboot" link. This can be useful to ensure restore settings are loaded.



The page at http://192.168.1.1 says:

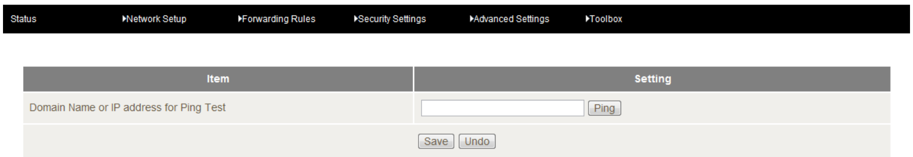
Would you like to reboot your device? Please click OK to proceed.

Startup Wizard

Click this link to re-run the First time Setup Wizard. You can use this to easily reconfigure your 3GM2WN.

Miscellaneous

Wake-on-LAN enables the router to start-up a computer or device (if the computer supports it) when a WOL packet is detected on the network going to the client MAC you have entered.



Item	Setting
Domain Name or IP address for Ping Test	Ping

You can also control the brightness of the LEDs on the router manually or via a scheduled time (Please refer to the scheduling section for instructions on setting up scheduled times).

OPTION	DEFINITION
Domain Name or IP address for Ping Test	Enter the domain name or IP address you would like to attempt to ping.

Logout

Click this link to logout of the 3GM2WN's Web based User Interface.

Additional Product Information

Establishing a wireless connection

Windows XP (Service Pack 2)

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 3GM2WN 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.

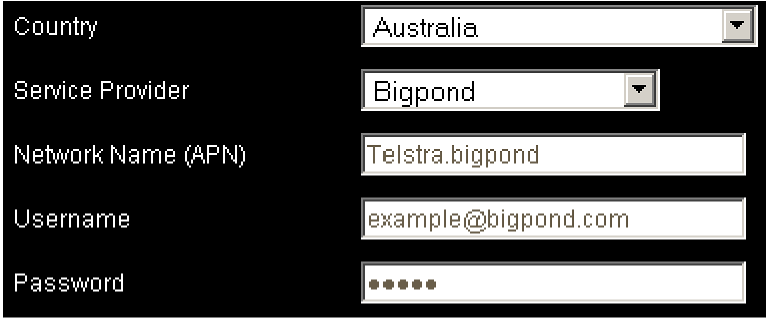
Please note: For other operating system (Windows 98SE, Windows ME, Windows 2000 etc) or if you use a wireless adaptor utility to configure your wireless connection, please consult the wireless adapter documentation for additional information.

Establishing a Bipgond connection

The following steps will enable you to utilise the 3GM2WN2 on your Bigpond Mobile Broadband service.

First time Setup:

1. Simply follow the steps as per the Quick Start Guide supplied with the 3GM2WN2. In the First time setup Wizard, check the following settings.
   - Ensure the Country selection is set to "Australia".
   - Select "Bigpond" from the Service Provider pull down menu.
   - Enter the Username and Password as supplied by Bigpond.

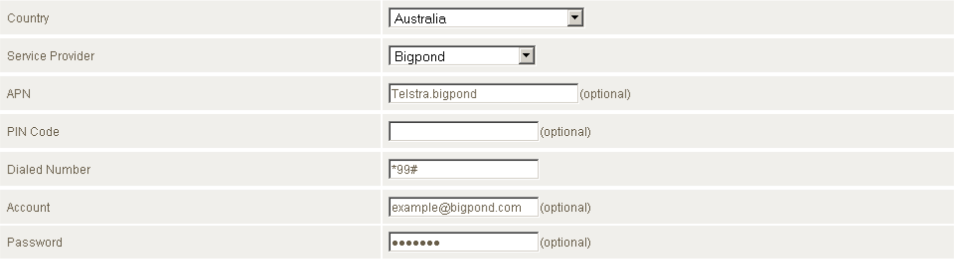


Country	Australia
Service Provider	Bigpond
Network Name (APN)	Telstra.bigpond
Username	example@bigpond.com
Password	●●●●●

Adjusting a saved configuration:

If the 3GM2WN2 has previously been configured, you can change the configuration in order to be used with a Bigpond Mobile Broadband service by performing the following steps:

1. Login to the Web Based Management Console by opening your web browser (e.g. Internet Explorer/Firefox/Safari) and navigate to the address http://192.168.20.1.
2. Enter "admin" (without the quotes) into the Username and Password fields and click "Login".
3. Click on the "Switch to advanced view" link at the bottom of the page.
4. Click on the "Network Setup" menu at the top of the page and then "Network Setup" item underneath.
5. Ensure the Country selection is set to "Australia".
6. Select "Bigpond" from the Service Provider pull down menu.
7. Enter the Username and Password as supplied by Bigpond.



Country	Australia
Service Provider	Bigpond
APN	Telstra.bigpond (optional)
PIN Code	(optional)
Dialed Number	*99#
Account	example@bigpond.com (optional)
Password	••••••• (optional)

8. Click the "Save" button at the bottom of the page to store the new configuration settings and connect to the Bigpond Mobile Broadband service.

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 3GM2WN 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 3GM2WN and the power source are both turned on and device is receiving sufficient power.
3	Turn the 3GM2WN 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 3GM2WN. 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 3GM2WN'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.

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 3GM2WN 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 3GM2WN from the WLAN or ping any computer on the WLAN.

STEP	CORRECT ACTION
1	If you are using a static IP address for the WLAN connection, make sure that the IP address and the subnet mask of the 3GM2WN 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 3GM2WN.

MODEL	3GM2WN
CPU	RT5350
Wireless LAN	IEEE 802.11n. Backwards compatible with IEEE 802.11b/g
Ethernet WAN/LAN port	1 x WAN/LAN port (10/100Mbps)
Connectivity	1 x USB 2.0, 1 x 10/100Mbps WAN/LAN, WLAN
LED Indicators	Power, WWW
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	5V DC - 1A
Dimensions & Weight	85.5 mm (L) x 56 mm (W) x 17.5 mm (H) 53 grams
Regulatory Compliance	C-Tick

Electrical Specifications

It is recommended that the 3GM2WN be powered by the supplied 12V DC, 1.5A power supply. A replacement power supply is available from the NetComm Online shop.

Environmental Specifications / Tolerances

The 3GM2WN housing enables it to operate over a wide variety of temperatures from 0˚C - 40˚C (operating temperature).

Legal & Regulatory Information

1. 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 Limited (ACN 002490486) (**NetComm**) (or its licensors). This Manual does not transfer any right, title or interest in NetComm's (or its licensors') intellectual property rights to you.

You are permitted to use this Manual for the sole purpose of using the NetComm 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.

NetComm is a trademark of NetComm. All other trademarks are acknowledged to be the property of their respective owners.

2. 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 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:
   - Change the direction or relocate the receiving antenna.
   - Increase the separation between this equipment and the receiver.
   - Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
   - Consult an experienced radio/TV technician for help.
3. The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

3. 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.

4. Product Warranty

All NetComm 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 within 30 days of the original purchase by registering online via the NetComm web site at www.netcomm.com.au. 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 Section 3 above).

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Section 3 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 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 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;

1. 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);
2. the fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
3. 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;
4. 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; or
5. the serial number has been defaced or altered in any way or if the serial number plate has been removed.

5. 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 Section 3 above), NetComm accepts no liability or responsibility, for consequences arising from the use of this product. NetComm 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'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's liability for any breach of that guarantee, condition or warranty is limited to: (i) in the case of a supply of goods, NetComm 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 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 is unable to limit its liability as set out above, NetComm 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
P: +61(0)2 9424 2070   F: +61(0)2 9424 2010
E: sales@netcomm.com.au
W: www.netcomm.com.au