NETCOMM GATEWAY™ SERIES

Dual ADSL2+ / 3G Gateway

3G29WN2

USER GUIDE

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 3G29WN2

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 3G29WN2.

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 3G29WN2, please confirm that you comply with the minimum system requirements below.

ADSL Requirement:

- An activated ADSL broadband connection to an ISP (Internet Service Provider)
- ADSL In-Line Splitter/Filter (Please refer to "Do I need a micro filter?" for more information)

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

3G Requirement:

- An activated 3G SIM Card

PC Requirement:

- A Web Browser such as Internet Explorer, Netscape Navigator, Mozilla Firefox, Opera, Safari etc.
- Computer with Windows, Macintosh, or Linux-based operating systems with a working Ethernet adapter with TCP/IP Protocol installed.
- Wireless Computer System Requirements:
  - Computer with a working 802.11b, 802.11g or 802.11n wireless adapter.

Do I need a micro filter?

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

Notation

The following symbols are utilised in this user manual:

- 

The following note requires attention

- 

The following note provides a warning

- 

The following note provides relevant information

Product Introduction

Product Overview

- Dual Internet connectivity between ADSL and 3G interfaces.
- Connect with ADSL2+ at up at 24Mbps speeds.
- Connect with 3G at up to 21Mbps speeds.
- Automatic failover from ADSL to 3G to ensure you are always online.
- The ability to share your internet with high speed Wireless N.
- Multiple wired connections possible with four Ethernet ports.
- USB port for print and storage serving functionality.

Speeds are dependent on network coverage. See your 3G provider coverage maps for more details. The total number of WiFi 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 3G29WN2 package consists of:

- NetComm Gateway Series ADSL2+/ 3G Router.
- Phone cable (RJ-11).
- Power Adapter.
- Quick Start Guide
- Ethernet Cable (RJ-45)
- Wireless Security Card
- Warranty Card
- 1 x Detachable WiFi antenna
- 2 x Detachable 3G antennas

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 NetComm 3G29WN2 Dual ADSL2+/ 3G Wireless N Gateway is designed for business and home users that rely on a constant and reliable high speed Internet connection. By integrating an ADSL2+ and HSPA+ (3G) modem into one device, users will have the flexibility to decide how they connect to the internet. Featuring automatic failover, the router will automatically connect to 3G should the ADSL connection fail, providing users with a constant and reliable connection to the internet. This flexibility is a necessity for any business or personal user who engages in internet critical activities.

Both connection methods with allow you to share the internet among multiple users with a built-in wireless access point offering speeds of up to 300Mbps and four Ethernet ports for wired connection.

The USB port can be used to connect and share a printer or a storage device making it a true office in a box solution.

Physical Dimensions and Indicators

LED Indicators

The 3G29WN2 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.

Figure 1: 3G29WN2 LED Indicator Icons

LED	ICON	COLOUR	MODE	FUNCTION
Power		Blue	On	The router is powered on.
			Off	The router is not powered on.
LAN 1-4	1 – 4	Blue	On	An Ethernet link is established.
			Off	There is no Ethernet link established.
			Blinking	Data is transmitting/receiving over the Ethernet connection.
WiFi		Blue	On	Local WiFi access to the Router is enabled and working.
			Off	The Wireless Module is not installed or not enabled.
			Blinking	Data is transmitting/receiving over the WiFi interface.
ADSL		Blue	On	The ADSL link is established
			Blinking slowly	There is no ADSL link established.
			Blinking	The ADSL line is training for a broadband signal.
Internet		Blue	On	A link to the Internet is established.
			Off	Modem is in bridged mode or an ADSL connection is not present.
			Blinking	Data is transmitting/receiving over the Internet.
		Lavender	On	The Internet connection has auto failed over from ADSL to 3G.
3G Mode	2G/3G	Blue	On	The 3G connection is active.
			Off	There is no available 3G connection.
		Lavender	On	The 2G connection is active.
3G Signal		Blue	On	The 3G signal strength is strong.
		Lavender	On	The 3G signal strength is medium.
		Red	On	The 3G signal strength is weak.
			Blinking	The SIM card is not installed or not detected.
USB		Blue	On	A USB device is plugged into the USB port.
			Off	There is no USB device plugged into the USB port.

Table 1: 3G29WN2 LED Indicator and Icon Functions

3G29WN2 Default Settings

The following tables list the default settings for the 3G29WN2.

LAN (MANAGEMENT)	
Static IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1

Table 2: 3G29WN2 Default Settings – LAN

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

Table 3: 3G29WN2 Default Settings – Wireless

3G29WN2 WEB INTERFACE ACCESS	
Username:	admin
Password:	admin

Table 4: 3G29WN2 Default Settings - Web Interface Access

Restore Factory Default Settings

Restoring factory defaults will reset the 3G29WN2 to its factory default configuration. Occasions may present themselves where you need to restore the factory defaults on your 3G29WN2 such as:

- You have lost your username and password and are unable to login to your 3G29WN2's web configuration page.
- You have purchased your 3G29WN2 from someone else and need to reconfigure the device to work with your ISP.
- You are asked to perform a factory reset by NetComm Support staff.

In order to restore your 3G29WN2 to its factory default settings, please follow these steps:

- Ensure that your 3G29WN2 is powered on (for at least 10 seconds);
- Use a paper clip or a pencil tip to depress the reset button for ten seconds and release. At this point, the reset is in progress. Do not power off the unit;
- When the indicator lights return to steady blue, reset is complete. The default settings are now restored. The entire process takes about 45 seconds to complete;
- Once you have reset your 3G29WN2 to its default settings you will be able to access the device's configuration web interface using http://192.168.1.1 with username 'admin' and password 'admin';

Integrated Interfaces

The following integrated interfaces are available on the 3G29WN2:

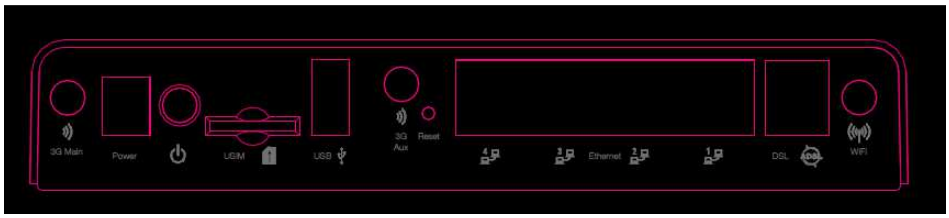

Figure 2: 3G29WN2 Rear Panel

REAR PANEL	DESCRIPTION
3G Main / 3G Aux	3G antennas for connecting to a 3G service broadcast from a 3G base station.
Power	Connect the supplied power adapter to this connector to power up the router.
On /Off (Icon)	Push to turn the 3G29WN2 on and off
USIM	USIM card slot. Insert your SIM card here.
USB	Connect your USB printer or storage device here.
Reset	Reset button. Depress for 10 seconds using a paperclip, toothpick or similar thin object to return the 3G29WN2 to factory default settings.
LAN x 4	4 x 10/100 Ethernet switch to connect wired devices.
DSL	Telephone jack (RJ-11) to connect to your telephone wall socket (ADSL Line).
WiFi	WiFi antenna for distributing the local wireless signal.

Table 5: 3G29WN2 Rear Panel - Interface Descriptions

Safety and Product Care

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

- To avoid fire or shock hazard do not use or install this product near water. For example, do not install 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 the power cord to lie freely. There should be no obstructions in the path of the cord and no heavy items should be placed onto it. In addition, do not walk on, step on or mistreat the cord.
- To safeguard the equipment against overheating, make sure that all ventilation openings in the unit housing that offer exposure to air are unobstructed.

WARNING
Disconnect the power line from the device before servicing.

Transport and Handling

When transporting the 3G29WN2, 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 3G29WN2

Placement of your 3G29WN2

Just like your mobile phone, the location of the 3G29WN2 will affect its signal strength to a 3G Mobile Base Station (Cell Tower). The data speed achievable is relative to the 3G signal strength, which is affected by many environmental factors. Please keep in mind that the 3G29WN2 will need adequate signal strength in order to provide Internet connectivity whilst choosing a location to place your 3G29WN2 router.

Similar the 3G connection signal strength, the wireless connection signal strength between your 3G29WN2 and your WiFi devices will be stronger the closer your connected devices are to your 3G29WN2. Your wireless connection and performance will degrade as the distance between your 3G29WN2 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 3G29WN2 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 WiFi Devices and your 3G29WN2, please try the following steps:

- In multi-storey homes, place the 3G29WN2 on a floor that is as close to the centre of the home as possible. This may mean placing the 3G29WN2 on an upper floor.
- Try not to place the 3G29WN2 near a cordless telephone that operates at the same radio frequency as the 3G29WN2 (2.4GHz).

Avoid obstacles and interference

Avoid placing your 3G29WN2 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 3G29WN2).

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 3G29WN2 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 3G29WN2.
- 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 3G29WN2 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 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 any other detected networks as possible.

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

Hardware installation

1. Connect the power adapter to the Power socket on the back of the 3G29WN2.
2. Plug the power adapter into the wall socket and switch on the power.
3. Wait approximately 60 seconds for the NetComm 3G29WN2 to power up.

Connecting via an Ethernet cable

1. Connect the supplied RJ-11 cable to the DSL port on the back of your device to the phone port that supplies your ADSL service.
2. And/or, insert a compatible 3G SIM card into the USIM slot on the back of the device.
3. Connect the supplied RJ-45 Ethernet cable from one of the Ethernet ports on the back of the device to your computer.
4. Connect the supplied detachable antennas to the WiFi and 3G connectors on the back of the router. (Attach antennas in a clockwise direction.)
5. Connect the supplied power adapter to your router and press the on/off button to power the router on.

Connecting wirelessly

Multiple wireless devices, including laptops, desktops and PDA's can be connected to your router by following these two basic steps.

1. Using your wireless device, scan for 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

Quick Setup

Please follow the steps below to configure your 3G29WN2 Wireless router via the web based configuration wizard.

Open your web browser (e.g. Internet Explorer/Firefox/Safari) and type http://192.168.1.1/ into the address bar at the top of the window.

A login screen should appear. Type “admin”(without quotations) into both the username and password fields. Then click the Ok button. This will take you directly to the Quick Setup page.

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

Figure 3: Basic - Quick Setup - Step 1

Connecting with ADSL

1. Select the ADSL only box and click Next;
2. Enter the User ID/Password on this screen as supplied by your Internet Service Provider (ISP).

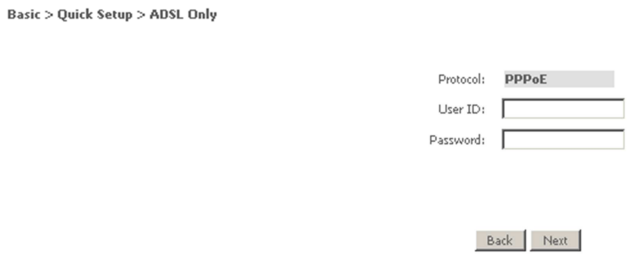

Figure 4: Basic - Quick Setup - ADSL only

3. Click on **Next** to use these settings,
4. You will then be asked to enter additional setup details. These additional steps are explained below.

Connecting with 3G

1. Select the 3G only box and click the Next button.
2. Type the APN in the APN field. This needs to be supplied by your 3G Internet Service Provider (ISP).
3. Select the Authentication Method as directed by your 3G ISP. Alternatively set this field to NONE if Authentication is not required.

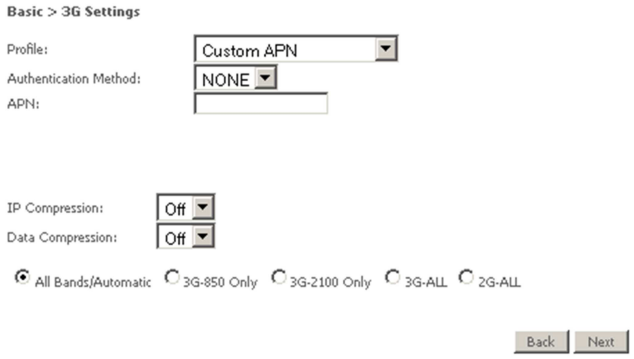

Figure 5: Quick Setup - 3G Only

4. If required enter the username and password supplied to you by your 3G ISP.

NOTE: Not all 3G users will have a username/password. Only enter this information if you have been supplied one by your 3G ISP.

5. Click on the Next button to save these settings and continue the setup.
6. You will then be asked to enter additional setup details. These additional steps are explained below

Configuring 3G backup

1. Select the "ADSL with 3G backup" option and click the Next button.
2. Follow the instructions listed above for both ADSL and 3G to set up both connections.
3. Check the "Enable 3G Backup" box and enter your desired backup settings.

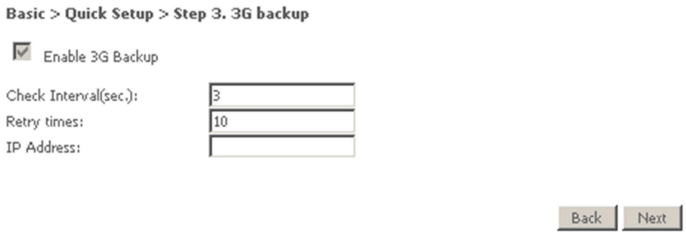

Figure 6: Quick Setup - 3G Backup

4. Click on the Next button to use save settings and continue the setup.
5. You will then be asked to enter additional setup details. These additional steps are explained below.

Wireless Set Up

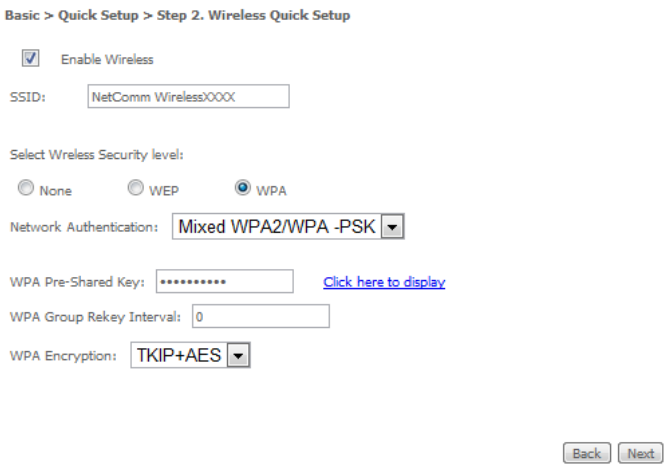

Figure 7: Quick Setup – Wireless

1. The default settings will appear on the wireless quick setup page.
2. You have the option to enable or disable the wireless signal using the Enable Wireless checkbox.
3. The wireless SSID (network name) can be customised here. If you change the SSID, be sure to remember the new network name or write it down so you know which network to connect to.
4. Select the level of wireless security and the network authentication type you require and change the wireless password.
5. Once you have completed entering your wireless settings click the Next button.

USB Storage

Figure 8: Quick Setup - USB Storage

1. If a USB device is plugged into the USB port, it will be auto detected and you will have the choice to Enable USB storage.
2. If you enable USB storage you will be shown the Netbios and Directory name. These fields can be changed for your preference.
3. Click the Next button once you are happy with the settings.
4. To access the storage device open a web browser and type \\Netbios\Directory\. The default access path for the USB storage is \\3G29WN2\USB-Storage\

USB Print Server

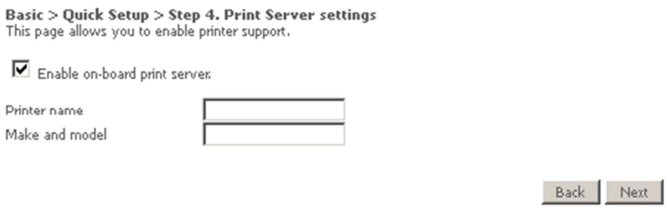

Figure 9: Quick Setup - Printer Server

1. If a USB printer is plugged into the USB port, it will be auto detected and you will have the choice to Enable the on-board print server.
2. If you enable the device to work as a print server you will be asked to enter the printer name and make and model. Both fields can be named anything you like. The names will be used to identify the printer later.
3. Click the Next button once you are happy with the settings.
4. To complete the network printer setup, please read Appendix A of the User Manual.

Passwords

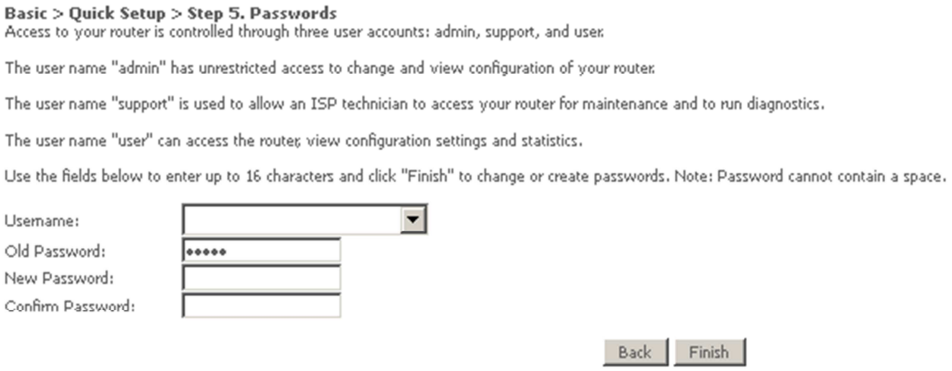

Figure 10: Quick Setup – Passwords

1. On this page you can change the router passwords for the different levels of users.
2. The default password for all users is the same as the corresponding username.
3. Once you have completed setting the passwords click the Finish button.
4. You will be taken back to the home page where you can view your connection status.

Advanced Configuration – Web User Interface

What can you do from here?

By logging into the web user interface, you are able to configure your 3G29WN2 with a wide array of basic and advanced settings. From setting wireless security, to backing up your routers settings, uploading new firmware and setting parental controls, the web user interface is a handy tool for personalizing your device to maximize its potential. Read on for a more advanced description on all elements of the web user interface.

Logging into the user interface

To login to the web interface, follow the steps below:

NOTE: The default settings can be found in Default Settings.

1. Open a web browser and enter the default IP address for the Router in the web address field at the top of the window. In this case the default IP address is http://192.168.1.1

NOTE: For local administration (i.e. LAN access), the PC running the browser must be attached using either an Ethernet or wireless connection to the router. For remote access, use the WAN IP address shown on the WUI Homepage screen and login with remote username and password.

2. A dialog box will appear, as illustrated below. Enter the default username and password, as defined in the Default Settings section.
    - User Name – admin.
    - Password – admin.
3. Click OK to continue.

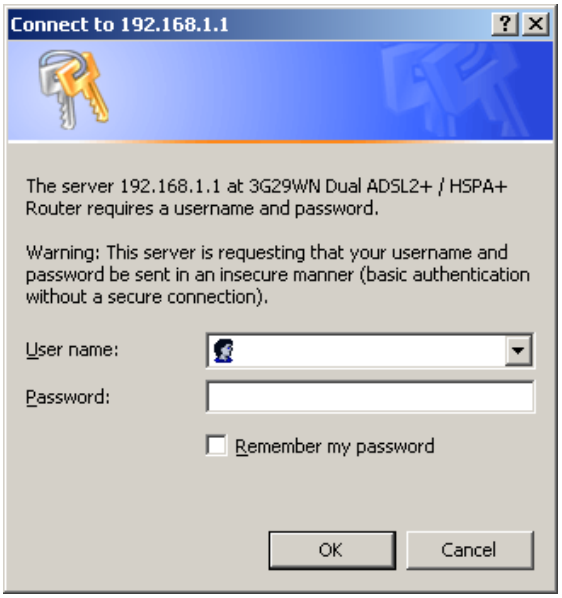

Figure 11: 3G29WN2 Login

NOTE: The login password can be changed later (see Access Control > Passwords).

Basic

Quick Setup

After you log into the web user interface, you will be taken directly to the Quick Setup page. See the instructions listed above in "Quick Setup" for instructions to configure your device for use.

Home

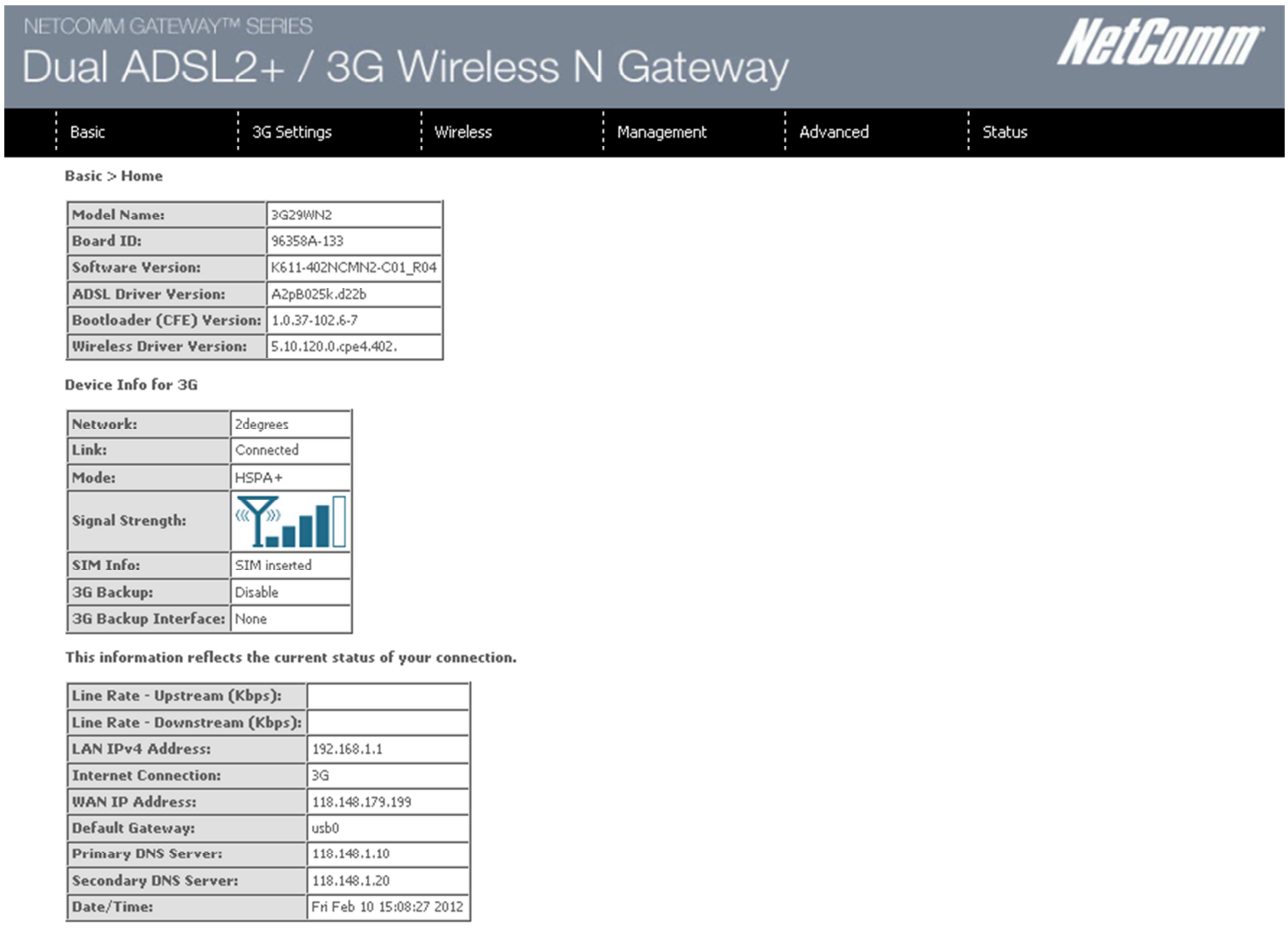

Figure 12: Basic – Home

The web user interface (WUI) is divided into two window panels, the main menu (on the top) and the display screen (on the bottom). The main menu has the following options: Basic, 3G Settings, Wireless, Management, Advanced and Status.
Selecting one of these options will open a submenu with more options. Basic is discussed below while subsequent chapters introduce the other main menu selections.
NOTE: The menu options available within the web user interface are based upon the device configuration and user privileges (i.e. local or remote).

The following table provides further details for each field:

FIELD	DESCRIPTION
Model Name	The model number of the device.
Board ID	A unique number assigned to the Printed Circuit Board (PCB) of the router.
Software Version	The current firmware version installed on the router.
ADSL Driver Version	The current ADSL driver version installed on the router.
Bootloader (CFE) Version	The current bootloader installed on the router.
Device Info for 3G	
Network	The name of the 3G network currently detected and in use by the router.
Link	The status of the 3G connection.
Mode	The radio access technique currently used to enable internet access. Possible modes include HSUPA, HSDPA, UMTS, EDGE, GPRS or Disconnected.
Signal Strength	The current 3G signal strength the router is receiving from your 3G service provider.
SIM Info	An indication of the SIM card status, whether it is activated and ready for use.
3G Backup	The current status of the WAN failover settings – either enabled or disabled. If enabled the HSPA+ 3G connection is set to activate if the ADSL connection becomes disconnected.
3G Backup Interface	This field indicates the WAN interface that is to be backed up.
Connection Status	
Line Rate - Upstream	The upstream line rate of the ADSL connection in Kbps (e.g. 256 Kbps).
Line Rate - Downstream	The downstream line rate of the ADSL connection in Kbps (e.g. 1500 Kbps).
LAN IPv4 Address	The IP Address to access the 3G29WN2 from the local LAN network.
Internet Connection	The current internet connection type – ADSL or 3G.
WAN IP Address	The WAN IP address to access the router from a remote WAN network.
Default Gateway	The gateway address of the 3G29WN2.
Primary DNS Server	The primary DNS address that the current internet connection of the 3G29WN2 is using.
Secondary DNS Server	The secondary DNS address that the current internet connection of the 3G29WN2 is using
Date/Time	The date and time currently set on the router.

Table 6: Basic - Home Field Descriptions

3G Settings

This menu includes Setup, PIN Configuration and 3G Backup Config options.

Setup

This page allows you to select your 3G service settings according to predefined or custom profiles. Setup instructions are provided in the following sections for your assistance.

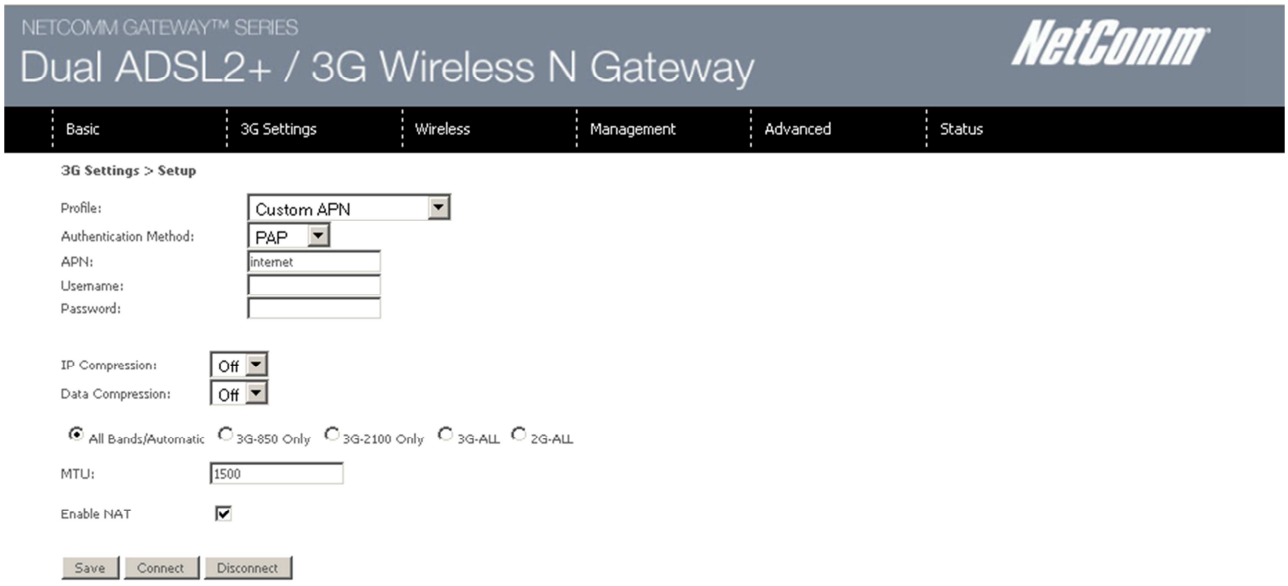

Figure 13: 3G Settings – Setup

Your 3G Service Provider will provide the information required to complete the first time setup instructions below. This includes profile, username and password. Only complete those steps for which you have information and skip the others.

1. If your SIM card is not inserted into the router, then do so now.
2. The Authentication Method should be provided to you by your 3G service provider. Set this field to NONE if not required.
3. Type the APN your 3G service provider has given you in the APN field. If you were not assigned a username and password, leave these fields empty.
4. Select IP compression and Data compression to be “On” or “Off”. By default these fields are set to “Off”.
5. Enter the MTU rate. If you are unsure or have no preference, leave it as the default value 1500.
6. Enable or disable NAT (Network Address Translation) – By default this is option is enabled.
7. Click the Save button to save the new settings.
8. Press the Connect button to reboot the router and to connect to the Internet. After rebooting, the Device Info for 3G network box in the GUI Basic screen should indicate an active 3G connection.

PIN Configuration

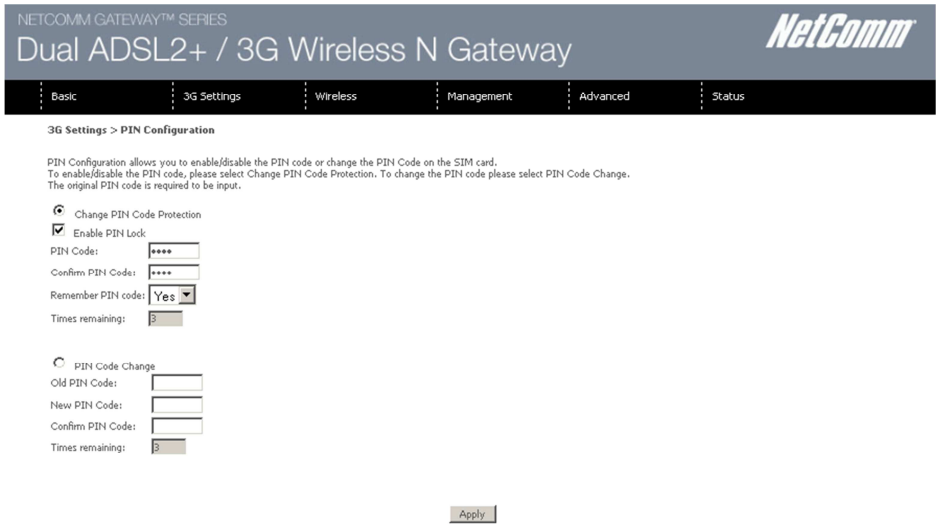

Figure 14: 3G Settings - PIN Configuration

On the 3G Settings > PIN Configuration page PIN Code Protection for using a SIM card with the 3G29WN2 can be enabled or disabled. An existing PIN code can also be changed on this page.

FIELD	DESCRIPTION
Change PIN Code Protection	Select this option to make any changes to the PIN code protection of the SIM card of the 3G29WN2.
Enable PIN Lock	Use this option to enable or disable the PIN lock on the 3G29WN2's SIM card..
PIN Code	Enter the current or new PIN Code.
Confirm PIN Code	Re-enter to confirm the current or new PIN Code.
Remember PIN Code	Select whether the PIN field should be automatically populated or not .
Times remaining	Enter the number of attempts to enter the PIN that can be made before a user is denied access.
PIN Code Change	Select this option to change an existing PIN code.
Old PIN Code	Enter the current PIN code.
New PIN Code	Enter the new PIN code that you wish to update to.
Confirm PIN Code	Re-enter and confirm the new PIN code that you wish to update to.
Times remaining	Enter the number of attempts to enter the PIN that can be made before a user is denied access.

Table 7: 3G Settings - PIN Configuration Settings

3G Backup Configuration

On this page you are able to configure your 3G29WN2 to use the 3G connection as a backup internet connection to the ADSL service. If both connection options are made available, should the ADSL connection fail for any reason the 3G configuration will automatically initiate an Internet connection to ensure the 3G29WN2 remains connected to the Internet. Once the ADSL connection has been re-established the 3G connection will failover to the ADSL connection.

Figure 15: 3G Backup Configuration

FIELD	DESCRIPTION
Enable 3G Backup	Select this option to enable the 3G connection as a backup for the ADSL connection.
Check Interval	The time in seconds that the 3G29WN2 will check the status of the current internet connection.
Retry Times	The number of ping attempts the router will make before failover in the event the internet connection drops out.
IP Address	The Public IP address to be used for checking the current Internet connection by ICMP (ping) request.
Selected WAN Interface	The WAN interface to be used as a 3G backup.

Table 8: 3G Backup Configuration Settings

Click the Save/Apply button to save any changes to the settings.

Wireless

Settings

The Wireless submenu provides access to Wireless Local Area Network (WLAN) configuration settings including:

- Wireless network name (SSID)
- Channel restrictions (based on country)
- Security
- Access point or bridging behaviour
- Station information

This screen allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as the SSID) and restrict the channel set based on country requirements. The Wireless Guest Network function adds extra networking security when connecting to remote hosts.

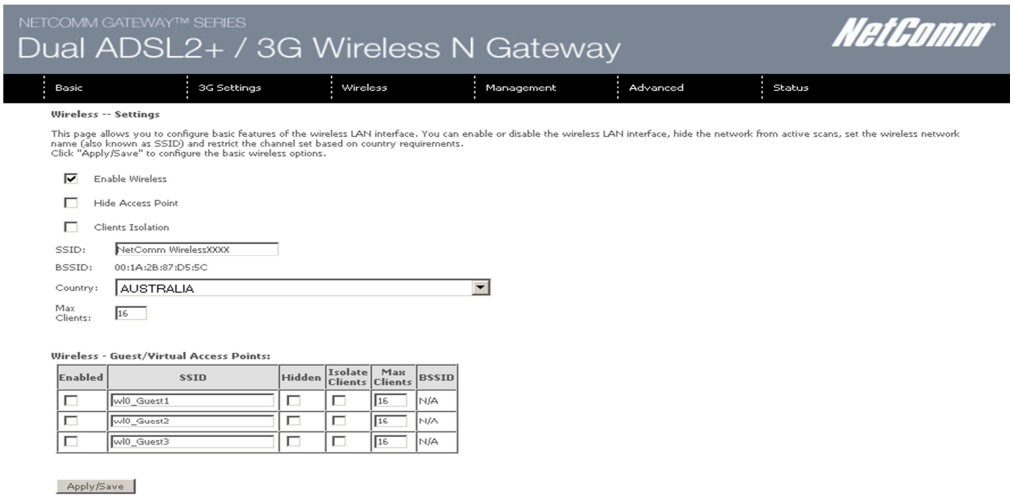

Figure 16: Wireless - Settings

FIELD	DESCRIPTION
Enable Wireless	A checkbox that enables (default) or disables the wireless LAN interface.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows, open Network Connections from the start Menu and select View Available Network Connections. If the access point is hidden, it will not be listed there. To connect a wireless client to a hidden access point, the user must add the access point SSID manually to its wireless configuration.
Clients Isolation	This field stops clients PC from detecting one another in My Network Places or Network Neighbourhood and prevents one wireless client communicating with another wireless client.
SSID [1-32 characters]	SSID (Service Set Identifier) sets the wireless network name. All wireless devices attempting to connect with the router must be configured with the correct SSID to access the WLAN. If the SSID does not match, the wireless device will not be granted network access.
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Each country listed enforces specific regulations limiting channel range. For Australia and New Zealand channels are limited to numbers 1-13.
Max Clients	The maximum number of wireless clients that can be connected to the 3G29WN2 at any one time.
Wireless Guest Network	The Guest SSID (Virtual Access Point) can be enabled by selecting the Enable Wireless Guest Network checkbox. Rename the Wireless Guest Network as you wish.

Table 9: Wireless - Settings

Security

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

Figure 17: Wireless - Security Settings

FIELD	DESCRIPTION
Select SSID	Pre- configured to the default SSID of the NetComm Wireless settings. This field can be changed in the Wireless > Settings section.
Network Authentication	The type of wireless security you prefer to use can be set using this field. NOTE: The wireless security types available are listed in the order of level of security from least (top) to most (bottom).
WEP Encryption	The option to enable or disable your wireless security encryption.
WPA-PSK / WPA2-PSK	A newer type of wireless security that gives a more secure network when compared to WEP. The security key needs to be more than 8 characters and less than 63 characters and it can be any combination of letters and numbers.
WPA/WPA2	WPA (WiFi Protected Access) is suitable for enterprise applications. It must be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management.
Encryption Strength	The strength/length of your wireless security key. 64 bit is the default setting.
Current Network Key	The current network key that is active. You have the choice of setting up to 4 different wireless security keys
Network Key 1	The value of network key 1. The default value is a1b2c3d4e5.
Network Key 2	The value of network key 2.
Network Key 3	The value of network key 3.
Network Key 4	The value of network key 4.

Table 10: Wireless - Security Settings

Advanced

This screen allows you to control the following advanced features of the Wireless Local Area Network (WLAN) interface:

- Select the wireless channel which you wish the router to operate from.
- Force the transmission rate to a particular speed.
- Set the fragmentation threshold. This can be used to improve throughput in noisy or congested situations.
- Set the RTS threshold. RTS stands for “Request to Send”. This parameter controls what size data packet the low level RF protocol issues to an RTS packet. The default is 2346.
- Set the wake-up interval for wireless clients using power-save mode.
- Set the beacon interval for the access point.
- Set Xpress mode.

Please see the Table below for an explanation of the advanced wireless settings.

Click the Apply/Save button to set any changes to the advanced wireless configuration.

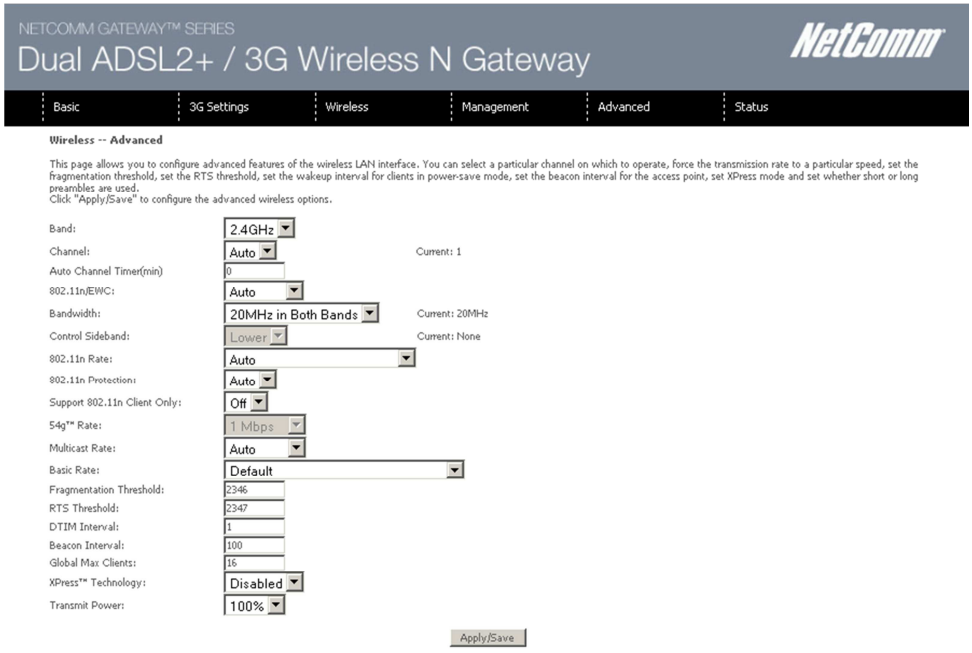

Figure 18: Wireless - Advanced Settings

FIELD	DESCRIPTION
Band	The frequency of the wireless network. 2.4GHz is standard.
Channel	Allows selection of a specific channel (1-13) or Auto mode.
Auto Channel Timer	The Auto Channel sets the length of time it takes to scan a channel in minutes.
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC).
Bandwidth	Drop-down menu specifies the following bandwidth: 20MHz in 2.4G Band and 40 MHz in 5G Band, 20MHz in both bands and 40MHz in both bands.
802.11n Rate	Drop-down menu specifies the following fixed rates. The maximum rate for bandwidth, 20MHz, is 130Mbps and the maximum bandwidth, 40MHz, is 270Mbps.
802.11n Protection	Turn off for maximized throughput. Turn on for greater security.
Support 802.11n Client Only	The option to provide wireless Internet access only to clients who are operating at 802.11n speeds.
54g Rate	In Auto (default) mode, your Router uses the maximum data rate and lowers the data rate dependent on the signal strength. The appropriate setting is dependent on signal strength. Other rates are discrete values between 1 to 54 Mbps.

Multicast rate	Setting for multicast packet transmission rate. (1-54 Mbps).
Basic Rate	Sets basic transmission rate.
Fragmentation Threshold	A threshold (in bytes) determines whether packets will be fragmented and at what size. Packets that exceed the fragmentation threshold of an 802.11 WLAN will be split into smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value however are not fragmented. Values between 256 and 2346 can be entered but should remain at a default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request To Send (RTS) specifies the packet size that exceeds the specified RTS threshold, which then triggers the RTS/CTS mechanism. Smaller packets are sent without using RTS/CTS. The default setting of 2347 (max length) will disables the RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is 1.
Beacon Interval	The amount of time between beacon transmissions in is milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon.
Global Max Clients	Here you have the option of setting the limit of the number of clients who can connect to your wireless network.
Xpress Technology	Broadcom's Xpress™ Technology is compliant with draft specifications of two planned wireless industry standards. It has been designed to improve wireless network efficiency. The default value is disabled.
Transmit Power	The option of decreasing the transmitting power of your wireless signal

Table 11: Wireless - Advanced Settings

MAC Filter

This screen appears when Media Access Control (MAC) Filter is selected. This option allows access to be restricted based upon the unique 48-bit MAC address.
To add a MAC Address filter, click the **Add** button shown below.
To delete a filter, select it from the table below and click the **Remove** button.

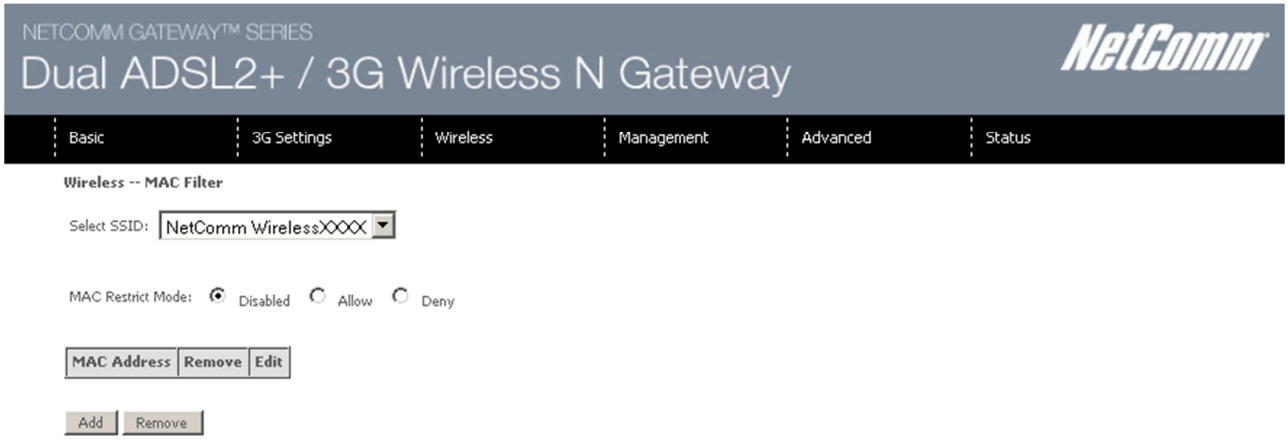

Figure 19: Wireless - MAC Filter

FIELD	DESCRIPTION
MAC Restrict Mode	Disabled – Disables MAC filtering Allow – Permits access for the specified MAC addresses. NOTE: Add a wireless device's MAC address before clicking the Allow radio button or else you will need to connect to the Router's web user interface using the supplied yellow Ethernet cable and add the wireless device's MAC address. Deny – Rejects access for the specified MAC addresses
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. The Add button prompts an entry field that requires you type in a MAC address in a two-character, 6-byte convention: xx:xx:xx:xx:xx:xx where xx are hexadecimal numbers. A maximum of 60 MAC addresses can be added.

Table 12: Wireless - MAC Filter Settings

Enter the MAC address on the screen below and click **Apply/Save**.

Figure 20: Wireless – MAC Filter - Add MAC Address

Wireless Bridge

The following screen appears when selecting Wireless Bridge, and gives a detailed explanation of how to configure wireless bridge features for the wireless LAN interface.

Click **Apply/Save** to implement new configuration settings.

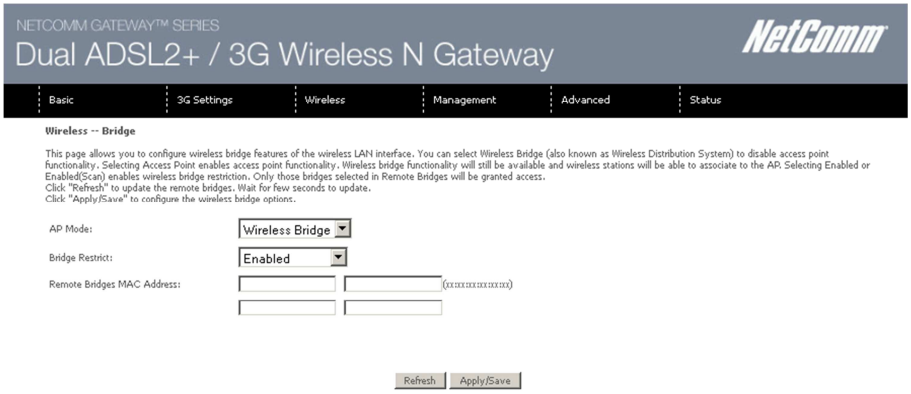

Figure 21: Wireless - Wireless Bridge

FIELD	DESCRIPTION
AP Mode	Selecting Wireless Bridge (Wireless Distribution System) disables Access Point (AP) functionality while selecting Access Point enables AP functionality. In Access Point mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting Disabled in Bridge Restrict disables the Wireless Bridge restriction, which means that any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) turns the wireless bridge restriction on. Only those bridges selected in Remote Bridges will be granted access. Click Refresh to update the station list when Bridge Restrict is enabled.

Table 13: Wireless - Wireless Bridge Settings

Station info

The following screen appears when you select Station Info, and shows authenticated wireless stations and their status. Click the Refresh button to update the list of stations in the WLAN.

Figure 22: Wireless - Station Info

FIELD	DESCRIPTION
MAC	The MAC address of any connected wireless client.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.
SSID	The SSID(Service Set Identifier) of your wireless network.
Interface	The wireless interface being used to connect to the network.

Table 14: Wireless - Station Info Fields

Management

Device Settings

The Device Settings screens allow you to backup, retrieve and restore the default settings of your Router. It also provides a function for you to update your Routers firmware.

Backup

The following screen appears when Backup is selected. Click the Backup Settings button to save the current configuration settings. You will be prompted for the location to save the backup file to on your PC.

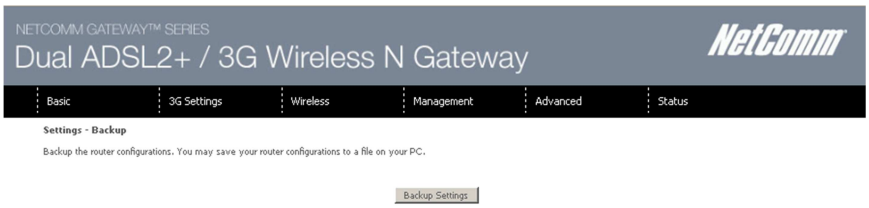

Figure 23: Management - Device Settings – Backup

Update

The following screen appears when selecting Update from the Device Settings submenu. By clicking on the Browse button, you can locate a previously saved filename as the configuration backup file. Click on the Update settings button to upload the selected file.

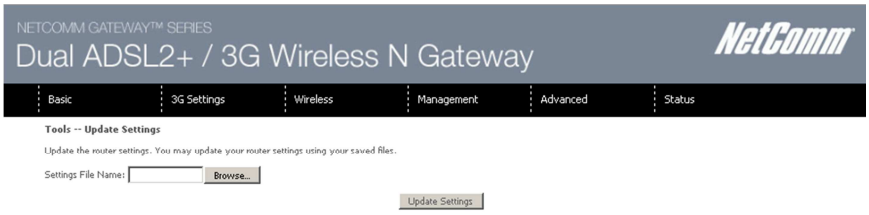

Figure 24: Management - Device Settings – Update

Restore Default

The following screen appears when selecting Restore Default from the Device Settings submenu. By clicking on the Restore Default Settings button, you can restore your Routers default firmware settings. To restore system settings, reboot your Router.

Figure 25: Management - Device Settings - Restore Default Settings

NOTE: The Restore Default function has the same effect as the reset button. The device board hardware and the boot loader support the reset to default button. If the reset button is continuously pushed for more than 5 seconds (and not more than 12 seconds), the boot loader will erase the configuration settings saved on flash memory.

Update Firmware

The following screen appears when selecting Update Firmware. By following this screens steps, you can update your Routers firmware. Manual device upgrades from a locally stored file can also be performed using the following screen.

1. Obtain an updated software image file
2. Enter the path and filename of the firmware image file in the Software File Name field or click the Browse button to locate the image file.
3. Click the Update Software button once to upload and install the file.

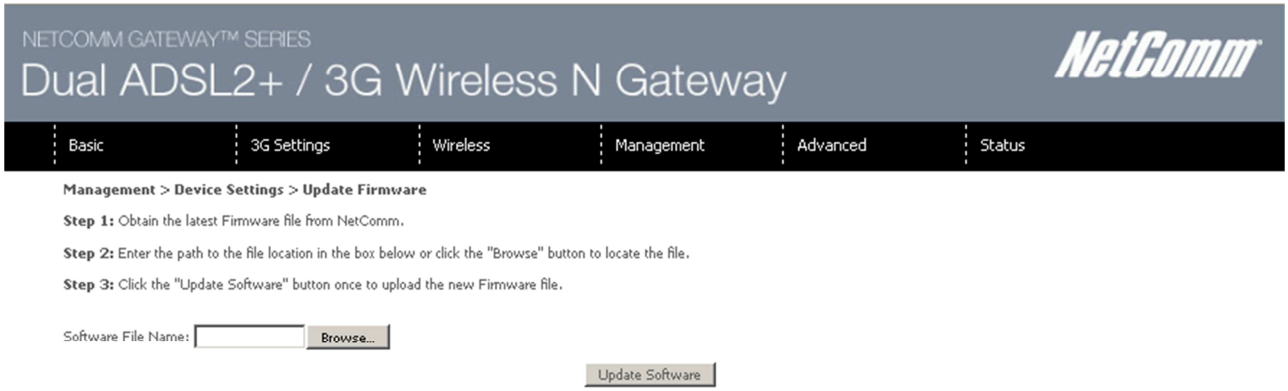

Figure 26: Management - Device Settings - Update Firmware

SNMP

The Simple Network Management Protocol (SNMP) allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this, the administrator typically runs an SNMP management station program such as MIB browser on a local host to obtain information from the SNMP agent, in this case the 3G29WN2 (if SNMP is enabled). An SNMP 'community' performs the function of authenticating SNMP traffic. A 'community name' acts as a password that is typically shared among SNMP agents and managers.

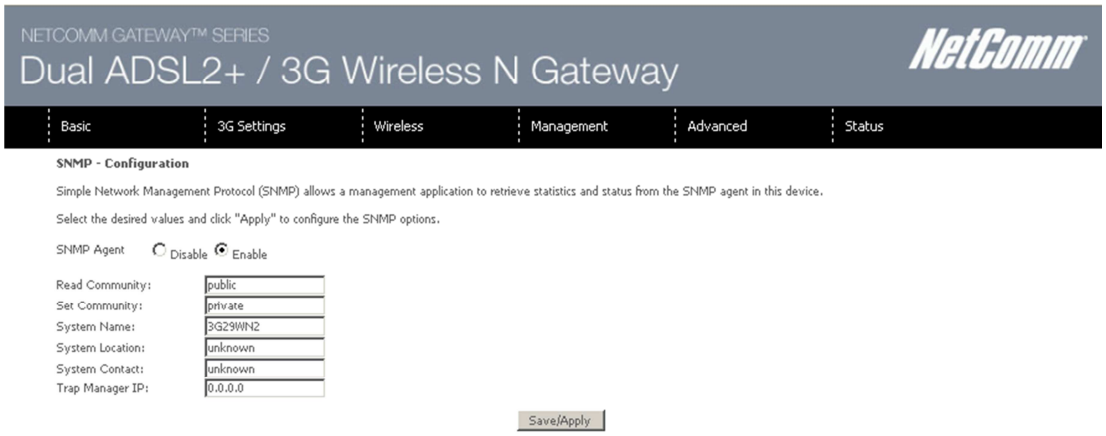

Figure 27: Management - SNMP

OPTIONS	DESCRIPTION
Read Community	Read device Settings.
Set Community	Read and change device settings.
System Name	Default system name is 3G29WN2.
System Location	User defined value.
System Contact	User defined value.
Trip Manager IP	The IP address of the administrator machine.

Table 15: Management - SNMP Settings

TR-069 Client

TR-069 enables provisioning, auto-configuration or diagnostics to be automatically performed on your router if supported by your Internet Service Provider (ISP).

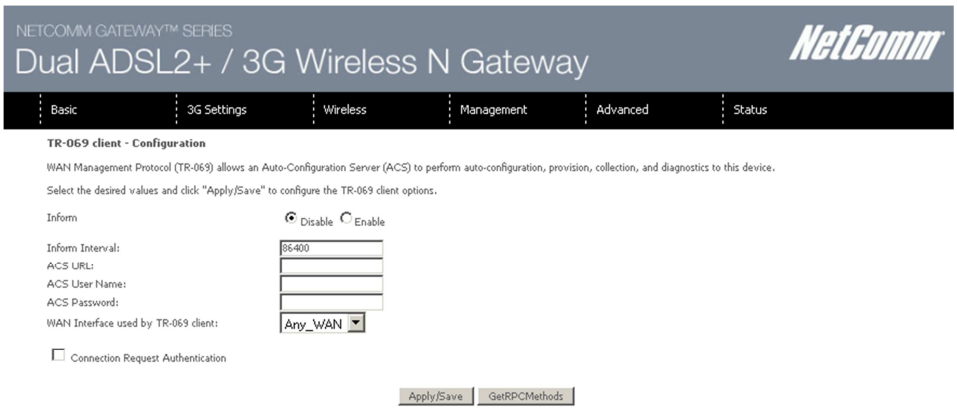

Figure 28: Management - TR-069 Client

FIELD	DESCRIPTION
Inform	Set to enable to activate TR-069 client settings.
Inform interval	Time in seconds that data is sent to the Auto-Configuration Server (ACS).
ACS URL	The address where the ACS server is located.
ACS User Name	The user name to access the ACS server.
ACS Password	The password to access the ACS server.
WAN Interface used by TR-069 Client	The connection used to send and receive data to the ACS server.

Table 16: Management - TR-069 Settings

SNTP

This interface allows you to configure the time settings of the 3G29WN2.

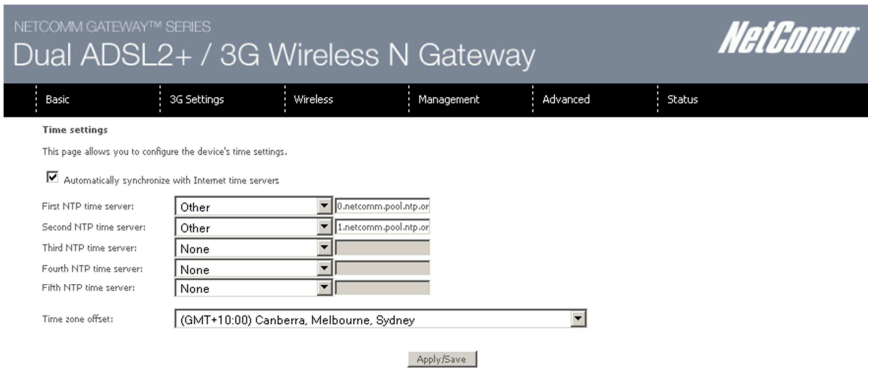

Figure 29: Management - SNTP

FIELD	DESCRIPTION
First NTP Time Server	Select the required internet time server.
Second NTP Time Server	Select a second time server if required.
Time Zone Offset	Set the local time zone.

Table 17: Management - SNTP Settings

NOTE: SNTP must be activated to use Parental Control.

Access Control

The Access Control option found in the Management drop down menu configures access related parameters in the following three areas:

- Services
- Passwords

Access Control is used to control local and remote management settings for your Router.

Services

The Service Control List (SCL) allows you to enable or disable your Local Area Network (LAN) or Wide Area Network (WAN) services by ticking the checkbox as illustrated below. The following access services are available: FTP, HTTP, ICMP, SNMP, SSH, TELNET, and TFTP. Click the Apply/Save button after making any changes to continue.

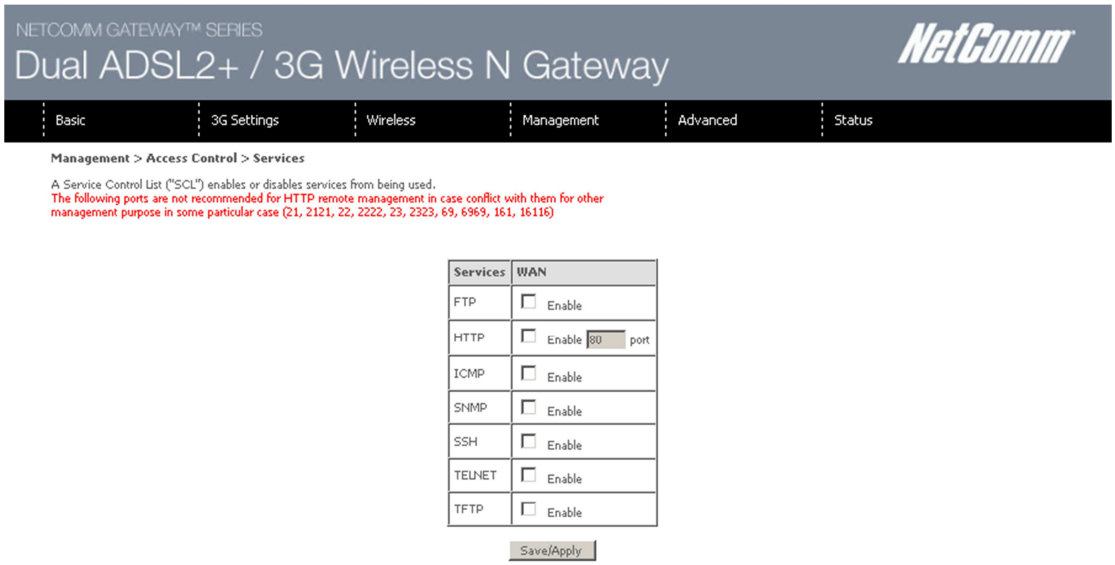

Figure 30: Management - Access Control - Services

Passwords

The Passwords option configures your account access password for your Router. Access to the device is limited to the following three user accounts:

- admin is to be used for local unrestricted access control
- support is to be used for remote maintenance of the device
- user is to be used to view information and update device firmware

Use the fields illustrated in the screen below to change or create your password. Passwords must be 16 characters or less with no spaces. Click the Apply/Save button after making any changes to continue.

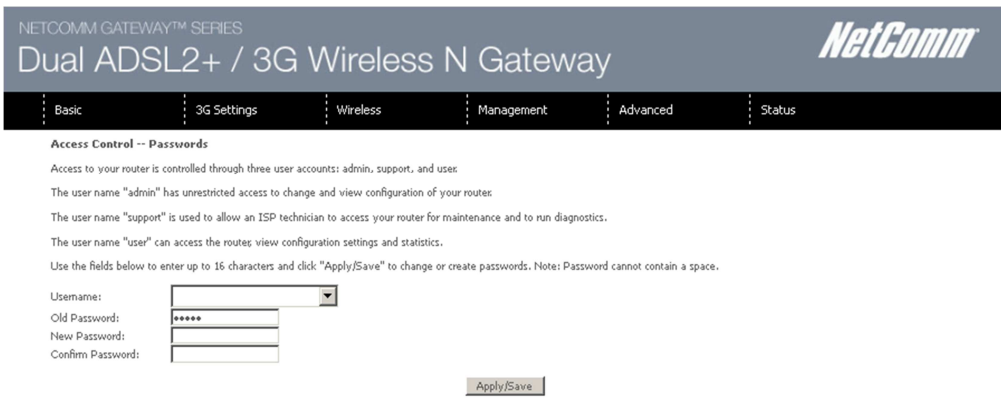

Figure 31: Management - Access Control - Passwords

Save/Reboot

This option saves the current configuration settings and reboots the 3G29WN2 router.

NOTE 1: It may be necessary to reconfigure your TCP/IP settings to adjust for the new configuration. For example, if you disable the Dynamic Host Configuration Protocol (DHCP) server you will need to apply Static IP settings.

NOTE 2: If you lose all access to your web user interface, simply press the reset button on the rear panel for 5-7 seconds to restore default settings.

Advanced

ATM Interface

The ATM interface page shows the settings of all available DSL ATM interfaces.

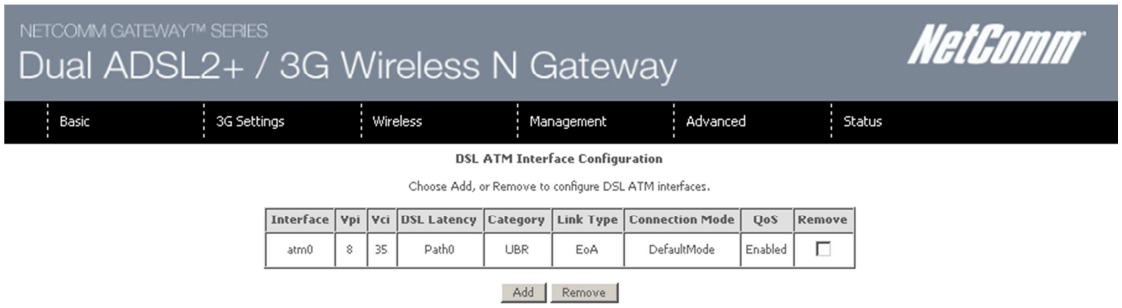

Figure 32: Advanced - ATM Interfaces

FIELD	DESCRIPTION
Interface	This field shows the interface name.
VPI	This field shows the VPI value. For most Australia connections the VPI is 8, for most new Zealand connections the VPI is 0.
VCI	This field shows the VCI value. For most Australia connections the VCI is 35, for most new Zealand connections the VCI is 100.
DSL Latency	The value of the DSL Latency.
Category	This field shows the ATM service classes.
Link Type	This field shows the type of link in use.
Connection Mode	This field shows the selected mode of connection.
QoS	This field shows the status of the Quality of Service (QoS) function.
Remove	Select this field to remove the ATM configuration.

Table 18:Advanced - ATM Interface Settings

WAN Service

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

A new PVC can be added or an existing entry can be edited.

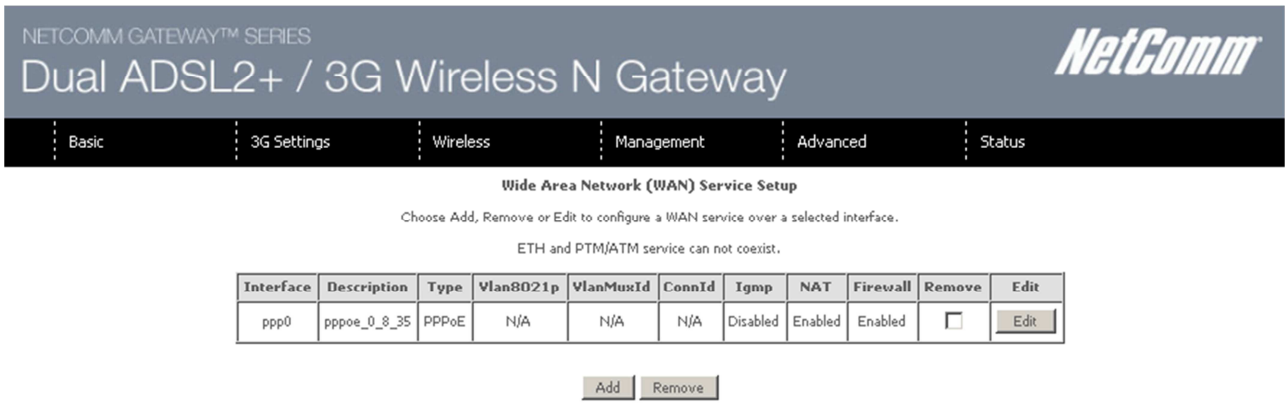

Figure 33: Advanced - WAN Service

FIELD	DESCRIPTION
Interface	This field shows the interface name that the PVC uses.
Description	A descriptive name assigned to the PVC.
Type	This field shows what type of connection the PVC is.
VLAN802.1p	The VLAN tag of the PVC (if applicable).
VLANMuxID	The MUX Server ID of the selected PVC.
ConnID	The VLAN Connection ID of the selected PVC.
IGMP	This field indicates whether IGMP multicast traffic is enabled or disabled for the selected PVC.
NAT	This field indicates whether Network Address Translation (NAT) is enabled or disabled.
Firewall	This field indicates whether the inbuilt firewall is enabled or disabled for the selected PVC.

Table 19: Advanced - WAN Service Settings

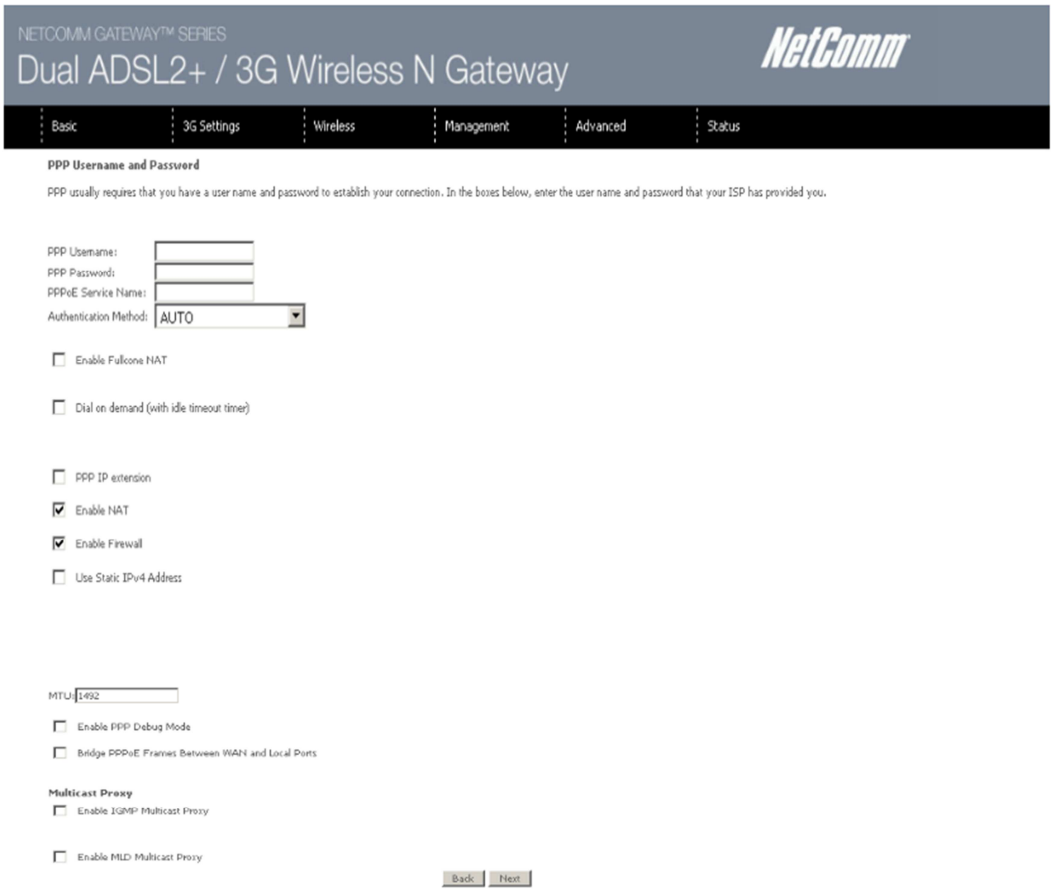

Figure 34: Advanced - WAN Service Settings

FIELD	DESCRIPTION
PPP Username	Enter your broadband username as supplied by your Internet Service Provider (ISP) into this field.
PPP Password	Enter your broadband password as supplied by your Internet Service Provider (ISP) into this field.
PPPoE Service Name	A name to identify the PPP connection should be entered into this field.
Authentication Method	The type of authentication the connection uses. If you are unsure which option to use select the AUTO option.
Enable Fullcone NAT	Enable 1 to 1 mapping of an IP address and port to an internal host.
Dial On demand	Initiate an internet connection when data traffic bound for the internet passes through the router.
PPP IP Extension	Enable PPP IP Extension for this connection (if supported by your ISP).
Enable NAT	Enable Network Address Translation (NAT) for this connection.
Enable Firewall	Enable the inbuilt firewall for this connection.
Use Static IP V4 Address	Use a Static IP Address (as supplied by your ISP) for this connection.
MTU	Set the MTU (Maximum Transmit Unit) size. A PPPoE connection requires an MTU of 1492.
Enable PPP Debug Mode	Enable extended PPP logging for this connection.
Bridge PPP Connections between WAN and Local ports	Use this field if you need to configure your PPPoE connection from a LAN connected host instead of the router.
Enable IGMP Multicast Proxy	Use this option to enable IGMP Multicast support on the connection.
Enable MLD Multicast proxy	Enable IPV6 IGMP Multicast support on the connection.

Table 20: Advanced - WAN Service Settings

LAN

This screen allows you to configure the Local Area Network (LAN) interface on your Router.

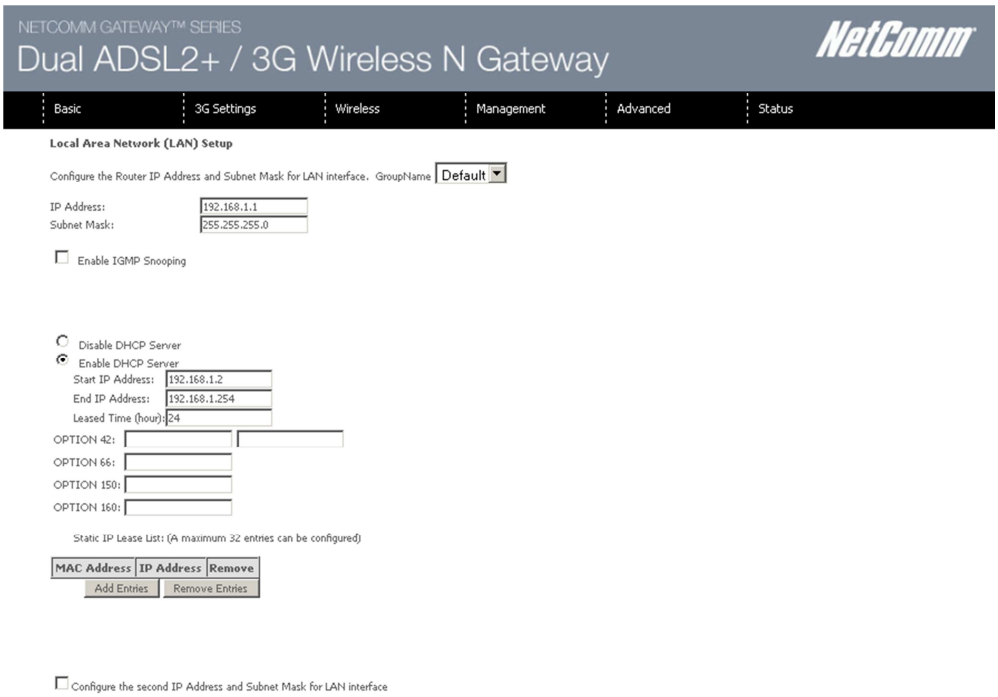

Figure 35: Advanced - LAN

See the field descriptions below for more details.

FIELD	DESCRIPTION
IP Address	The IP address of the LAN interface.
Subnet Mask	Enter the subnet mask for the LAN interface.
Enable IGMP Snooping	Enable by ticking the box. Standard Mode: In standard mode multicast traffic will broadcast to all bridge ports when no client subscribes to a multicast group. Blocking Mode: In blocking mode, the multicast data traffic will be blocked. When there are no client subscriptions to a multicast group, it will not broadcast to the bridge ports.
Enable LAN Side Firewall	The option to enable a firewall on the LAN side.
Disable DHCP Server	This option disables the DHCP server and should only be selected when using a Static IP address.
Enable DHCP Server	On selecting this field enter the start IP address and the end IP address as well as the lease time. With the DHCP server enabled the router automatically assigns the IP address, subnet mask , default gateway and DNS server addresses to all DHCP clients connecting to the router.
Enable DHCP Server Relay	Select this option to relay DHCP requests from a subnet with no DHCP server on it to a DHCP server on a different subnet. By default this option is disabled. To enable DHCP relay , first disable NAT and then press the Save button.
Configure the Second IP Address and Subnet Mask for LAN interface	Use this option to configure a second IP address for a second LAN interface. Enter the IP address and subnet mask of the secondary LAN connection.

Table 21: Advanced - LAN Settings

You can set a static DHCP address for a particular host by clicking the Add entries button and then entering the appropriate MAC and IP address for the nominated host. This effectively reserves an IP address for a particular LAN client.

NAT

Port Forwarding

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

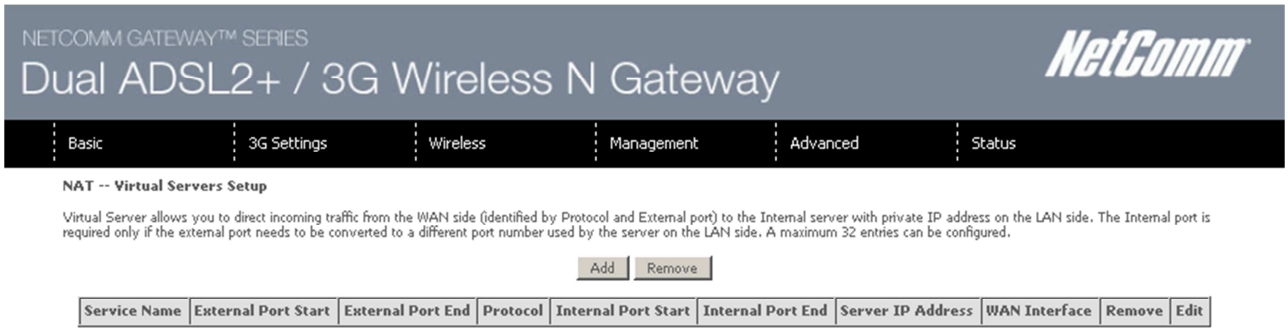

Figure 36: Advanced - NAT - Virtual Server

To add a Virtual Server, click the Add button. The following screen will display.

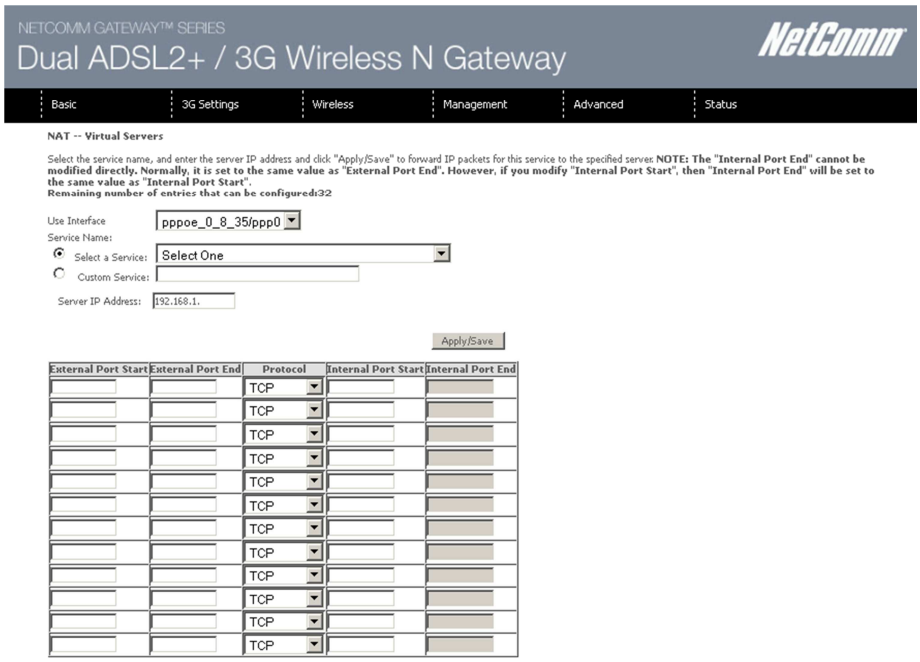

Figure 37: Advanced - NAT - Add Virtual Server

FIELD	DESCRIPTION
Select a Service or custom Server	Select a pre-configured port forwarding rule or choose custom server to create your own port forwarding rule.
Server IP Address	Enter the IP address of the local server.
External Port Start	Enter the starting external port number (when custom server is selected). When a service is connected this field will be completed automatically.
External Port End	Enter the ending external port number (when custom server is selected). When a service is connected this field will be completed automatically.
Protocol	Options include TCP, UDP or TCP/UDP.
Internal Port Start	Enter the starting internal port number (when custom server is selected). When a service is connected this field will be completed automatically.

Internal Port End	Enter the ending internal port number (when custom server is selected). When a service is connected this field will be completed automatically.

Table 22: Advanced - NAT - Add Virtual Server Settings

Port Triggering

Some applications require specific ports in the Router's firewall to be open for access by remote parties. Port Triggering opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'.

The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

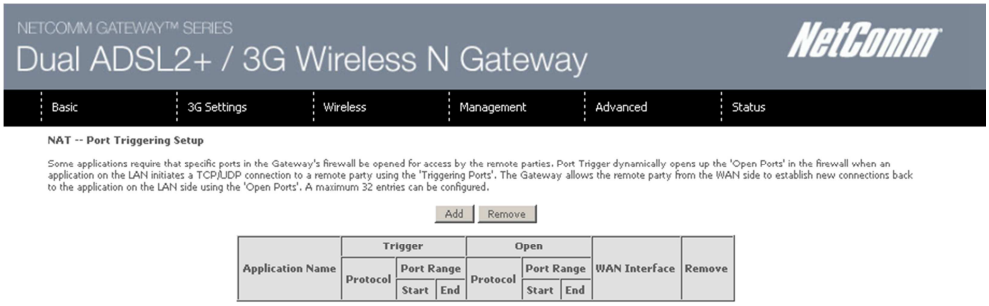

Figure 38: Advanced - NAT - Port Triggering

To add a Trigger Port, press the Add button. The following screen will be displayed.

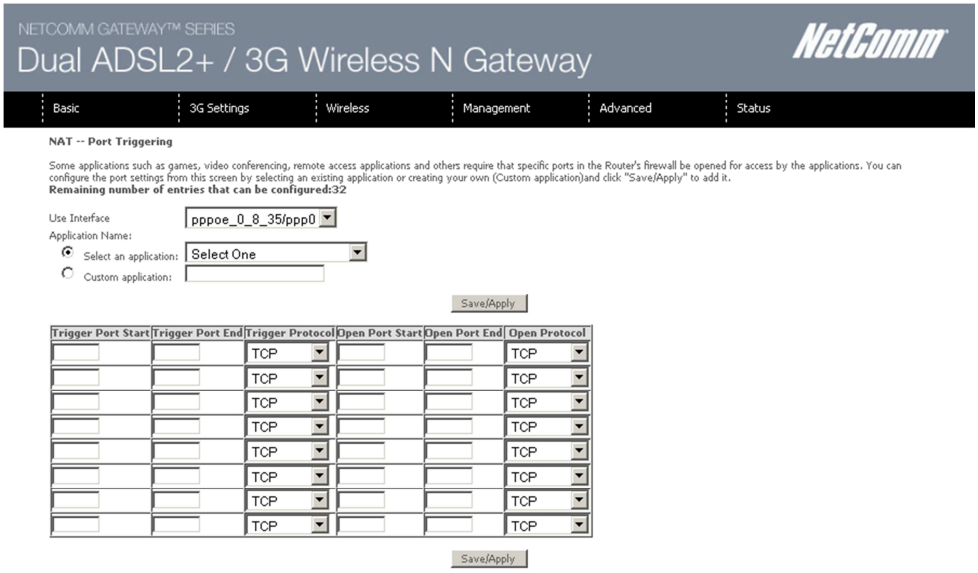

Figure 39: Advanced - NAT - Add Port Trigger

FIELD	DESCRIPTION
Select an Application or Custom Application	A user can select a pre-configured application from the list or select the Custom Application option to create custom application settings.
Trigger Port Start	Enter the starting trigger port number (when you select Custom Application). When an application is selected the port range values are automatically entered.
Trigger Port End	Enter the ending trigger port number (when you select Custom Application). When an application is selected the port range values are automatically entered.
Trigger Protocol	Options include TCP, UDP or TCP/UDP.
Open Port Start	Enter the starting open port number (when you select Custom Application). When an application is selected the port range values are automatically entered.

Open Port End	Enter the ending open port number (when you select Custom Application). When an application is selected the port range values are automatically entered.
Open Protocol	Options include TCP, UDP or TCP/UDP.

Table 23: Advanced - NAT - Add Port Trigger Settings

DMZ Host

The 3G29WN2 will forward IP packets from the Wide Area Network (WAN) that does not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click Apply to activate the DMZ host. To deactivate the DMZ Host function clear the IP address field and press the Save/Apply button.

Figure 40: Advanced - NAT - DMZ Host

Security

IP Filtering

The IP Filtering function sets filter rules that limit incoming and outgoing IP traffic. Multiple filter rules can be set with at least one limiting condition. All conditions must be fulfilled for individual IP packets to pass through the filter.

Outgoing IP Filter

The default setting for Outgoing traffic is ACCEPTED. Under this condition, all outgoing IP packets that match the filter rules will be BLOCKED.

Figure 41: Advanced - Security - Outgoing IP Filter

To add an outgoing IP filtering rule, click the Add button. The following screen will be displayed.

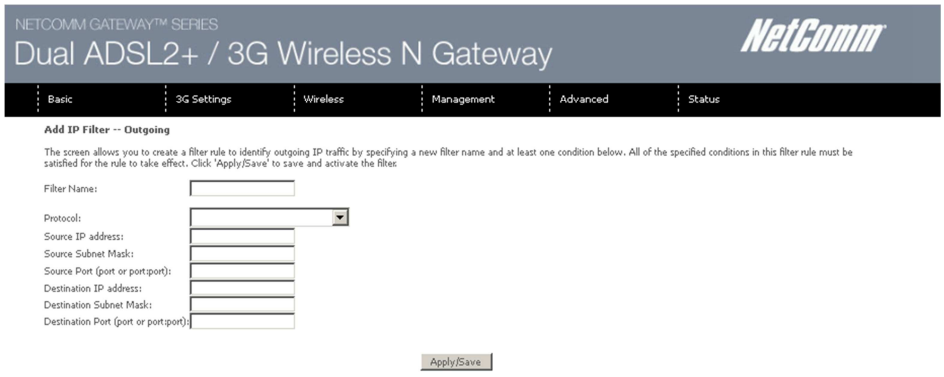

Figure 42: Advanced - Security - Add Outgoing IP Filter

FIELD	DESCRIPTION
Filter Name	The filter rule descriptive name.
Protocol	Options include TCP, UDP, TCP/UDP or ICMP Source IP Address.
Source IP Address	Enter the local source IP address from where the data originates.
Source Subnet Mask	Enter the local source subnet mask.
Source Port (port or port:port)	Enter the source port number or port range for the filter rule.
Destination IP Address	Enter the destination IP address.
Destination Subnet Mask	Enter the destination subnet mask..
Destination Port (port or port:port)	Enter the destination port number or port range for the filter rule.

Table 24: Advanced - Security - Add Outgoing IP Filter Settings

Incoming IP Filter

The default setting for all Incoming traffic is BLOCKED. Under this condition only those incoming IP packets that match the filter rules will be ACCEPTED.

Figure 43: Advanced - Security - Incoming IP Filter

To add an incoming IP filtering rule, click the Add button. The following screen will display.

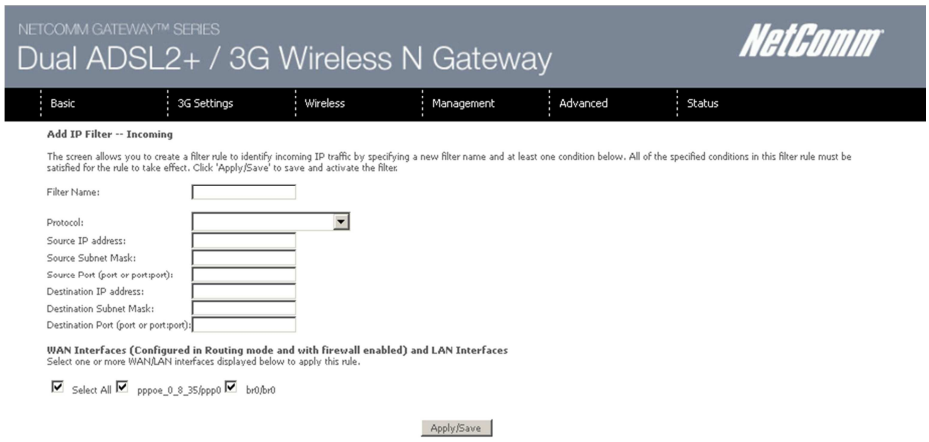

Figure 44: Advanced - Security - Add Incoming IP Filter

Please refer to the Outgoing IP Filter table for field descriptions.
Click Apply/Save to save and activate the filter.

Parental Control

The Parental Control feature allows you to take advanced measures to ensure the computers connected to the LAN are used only when and how you decide.

Time Restriction

This Parental Control function allows you to restrict access from a Local Area Network (LAN) connected device to an outside network through the router on selected days and at certain times. Make sure to activate the Internet Time server synchronization as described in the SNTP section, so that the scheduled times match your local time.

Figure 45: Advanced - Parental Control - Time Restriction

To add a time restriction rule press the Add button. The following screen will appear.

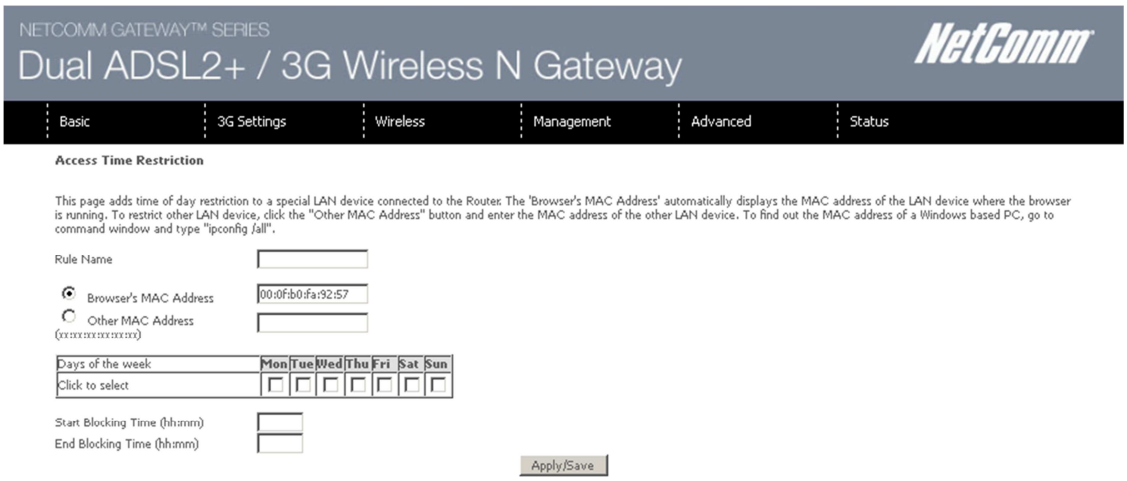

Figure 46: Advanced - Parental Control - Add Time Restriction

See the instructions below. Press the Apply/Save button to save a time restriction rule.

FIELD	DESCRIPTION
Rule Name	A user defined name for the time restriction rule.
Browser's MAC Address	The MAC address of the network card of the computer running the browser.
Other MAC Address	The MAC address of a second LAN device or network card.
Days of the Week	The days of the week for which the rules apply.
Start Blocking Time	The time of day when the restriction starts.
End blocking time	The time of day when the restriction ends.

Table 25: Advanced - Parental Control - Add Time Restriction Settings

URL Filter

With the URL filter, you are able to add certain websites or URLs to a safe or blocked list. This will provide you added security to ensure any website you deem unsuitable will not be able to be seen by anyone who is accessing the Internet via the 3G29WN2.

Select the 'To block' or 'To allow' option and then click Add to enter the URL you wish to add to the URL Filter list.

Figure 47: Advanced - Parental Control - URL Filter

Once you have chosen to add a URL to the list you will be prompted to enter the address. Simply type it in and select the Apply/Save button.

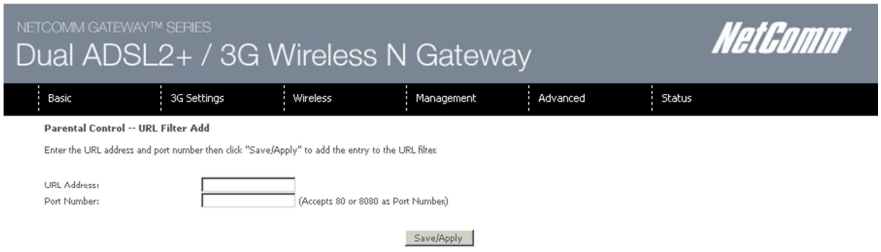

Figure 48: Advanced - Parental Control - Add URL Filter

Quality of Service

Quality of Service offers a defined level of performance in a data communications system - for example the ability to guarantee that video traffic is given priority over other network traffic to ensure that video streaming is not disrupted by other network requirements. This means that should you be streaming video and someone else in the house starts downloading a large file, the download won't disrupt the flow of video data.

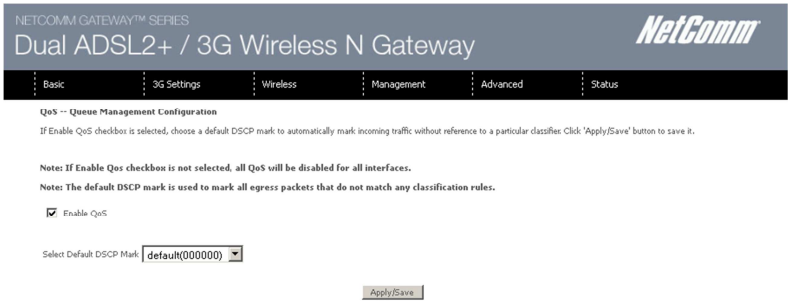

Figure 49: Advanced - QoS - QoS Management Configuration

To enable QoS select the Enable QoS checkbox and set the Default DSCP (Differentiated Services Code Point) Mark. Then press the Apply/Save button.

Queue Setup

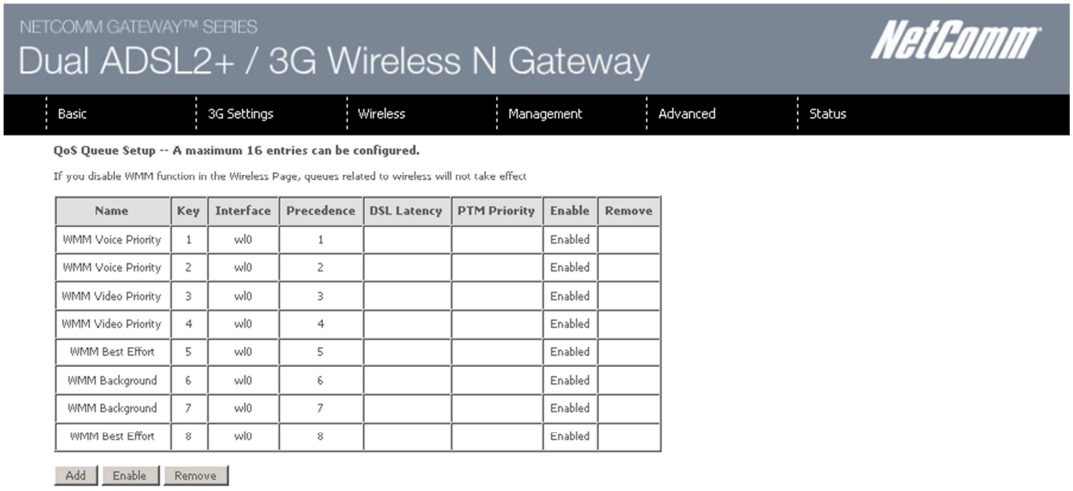

Figure 50: Advanced -QoS - Queue Setup

Click Add to display the following screen.

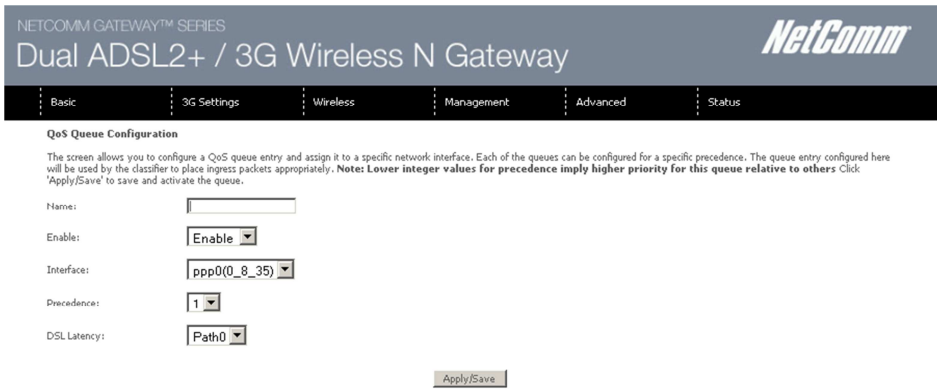

Figure 51: Advanced - QoS - Add Queue Configuration

The above screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately.
NOTE: Precedence level 1 relates to higher priority while precedence level 3 relates to lower priority.

QoS Classification

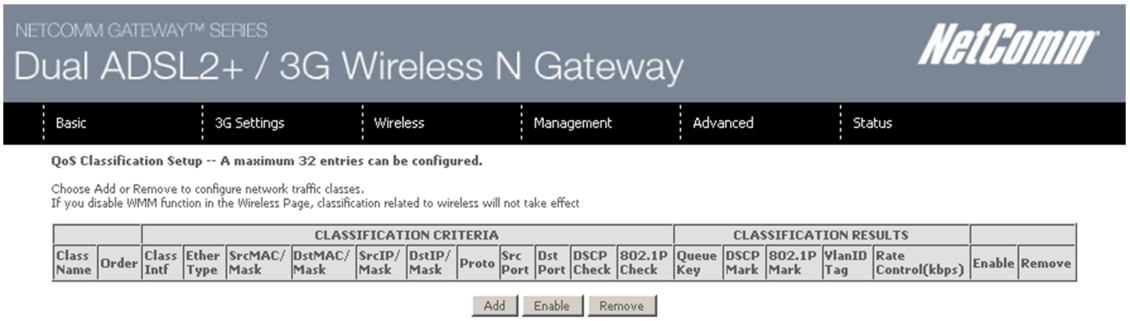

Figure 52: Advanced - QoS - Classification Setup

Click the Add button to configure network traffic classes.

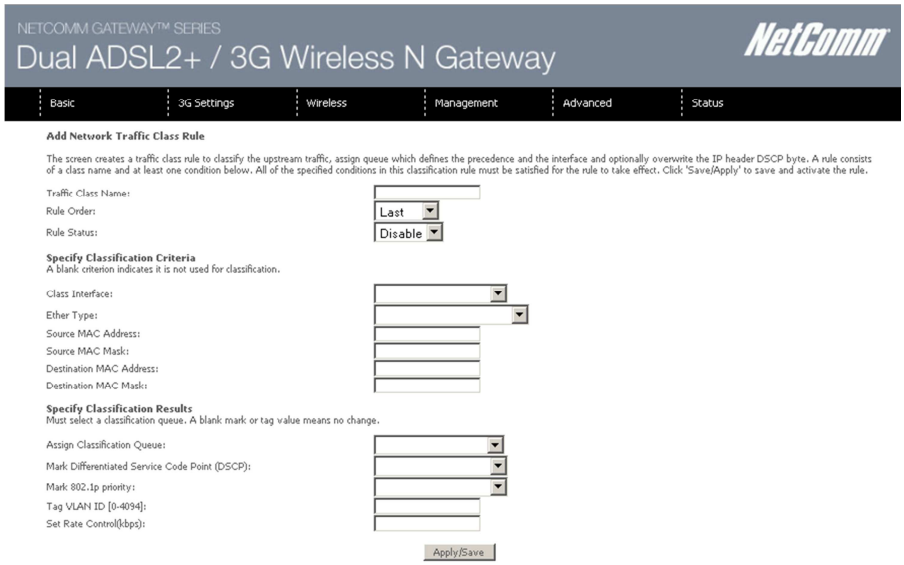

Figure 53: Advanced - QoS - Add Network Traffic Rule

The above screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS (type of service) byte. A rule consists of a class name and at least one condition. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

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

Routing

The Default Gateway, Static Route, Policy Routing and Dynamic Route settings can be found in the Routing option of the Advanced menu.

Default Gateway

Select your preferred WAN interface from the drop down box.

Figure 54: Advanced - Routing - Default Gateway

Static Route

The Static Route screen displays the configured static routes. Click the Add or Remove buttons to change settings.

Figure 55: Advanced - Routing - Static Route

Click the Add button to display the following screen.

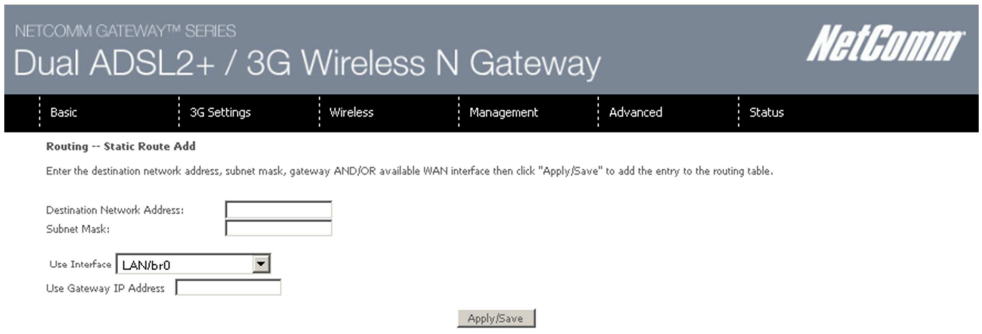

Figure 56: Advanced - Routing - Add Static Route

Enter the Destination Network Address, Subnet Mask, Gateway IP Address and/or WAN Interface. Then click Apply/Save to add the entry to the routing table.

Policy Routing

This function allows you to add policy rules to certain situations.

Figure 57: Advanced - Routing - Policy Routing

Click Add to display the following screen.

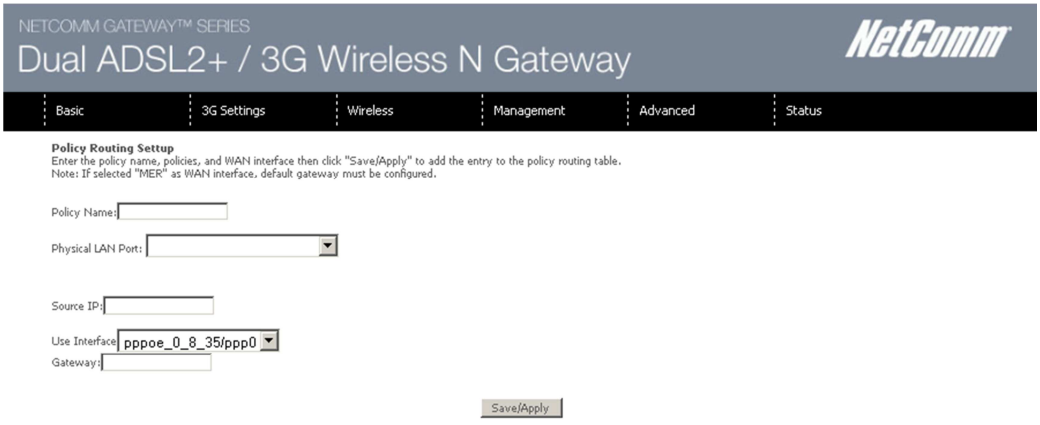

Figure 58: Advanced - Routing - Add Policy Route

Enter a, select the LAN port to be used, enter the source IP address

FIELD	DESCRIPTION
Policy Name	A user defined name for the policy route.
Physical LAN Port	The LAN port to be used for the policy.
Source IP	The IP address of the LAN device involved with the policy.
Use Interface	Select the Interface that the policy will employ.
Gateway	Enter the gateway address.

Dynamic Routing

To activate this option, select the Enabled radio button for Global RIP Mode.
To configure an individual interface, select the desired RIP version and operation, and enter a check in the Enabled checkbox for that interface. Click Apply/Save to save the configuration and to start or stop dynamic routing.

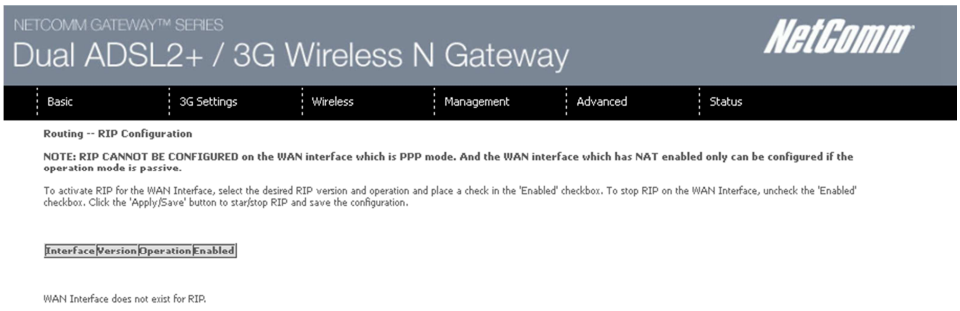

Figure 59: Advanced - Routing - Dynamic Routing

DNS

DNS Server

This page allows the user to enable automatic DNS settings detected from the Internet Service Provider or specify their own DNS server address manually.

Figure 60: Advanced - DNS - DNS Server

Dynamic DNS

The Dynamic DNS service allows a dynamic IP address to be aliased to a static hostname in any of a selection of domains, allowing the router to be more easily accessed from various locations on the internet.

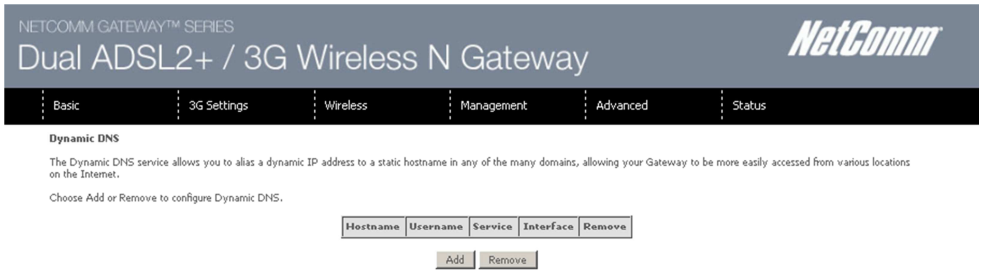

Figure 61: Advanced - DNS - Dynamic DNS

Note: The Add/Remove buttons will be displayed only if the router has been assigned an IP address from the remote server.
To add a dynamic DNS service, click the Add button and the following screen will display.

Figure 62: Advanced - DNS - Add Dynamic DNS

FIELD	DESCRIPTION
D-DNS Provider	Select the dynamic DNS provider from the list.
Host Name	The name of the dynamic DNS provider.
Interface	Select the interface from the list.
Username	Enter the Dynamic DNS account username.
Password	Enter the Dynamic DNS account password.

Table 26: Advanced - DNS - Add Dynamic DNS Settings

DSL

This page allows the user to modify the DSL modulation settings on the unit. By changing the settings, the user can specify which DSL modulation that the modem will use.

Figure 63: Advanced - DSL Settings

For advanced DSL options press the Advanced Settings button.

Figure 64: Advanced - DSL - Advanced Settings

The DSL advanced settings relate to test mode settings. The default selection is 'Normal'.

ADSL Tone Settings

For ADSL Tone Settings select the 'Tone Selection' button on the DSL Advanced Settings page.

The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125kHz apart. With each tone carrying separate data, the technique operates as if 256 separate routers were running in parallel. The tone range is from 0 to 31 for upstream traffic and from 32 to 255 for downstream traffic. Do not change these settings unless you are directed by your Internet Service Provider.

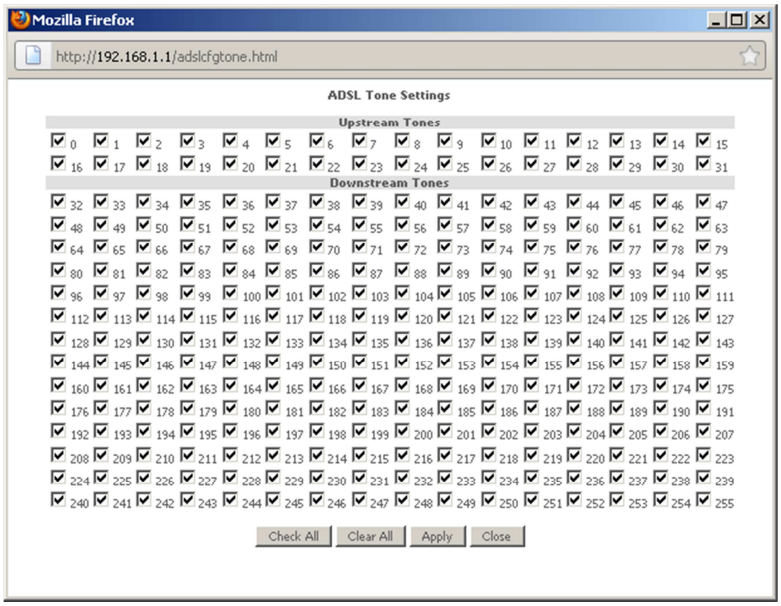

Figure 65: Advanced - DSL - Advanced settings - Tone Selection

UPnP

Universal Plug and Play (UPnP) is a set of networking protocols that can allow networked devices, such as computers, printers, WiFi access points and mobile phones to automatically detect each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

Figure 66: Advanced – UpnP

DNS Proxy

To enable DNS Proxy settings, tick the corresponding checkbox and then enter host and Domain name, as in the example shown below. Click Apply/Save to continue.

Figure 67: Advanced - DNS Proxy

The Host Name and Domain name are combined to form a unique label that is mapped to the router IP address. This can be used to access the user interface of the router with a local name rather than by using the router IP address.

USB Storage

This page allows you to enable or disable the USB port of the 3G29WN2 so it can be used as a mass storage server.

Please see Appendix B for more details on setting up your router to work with Storage Server functionality.

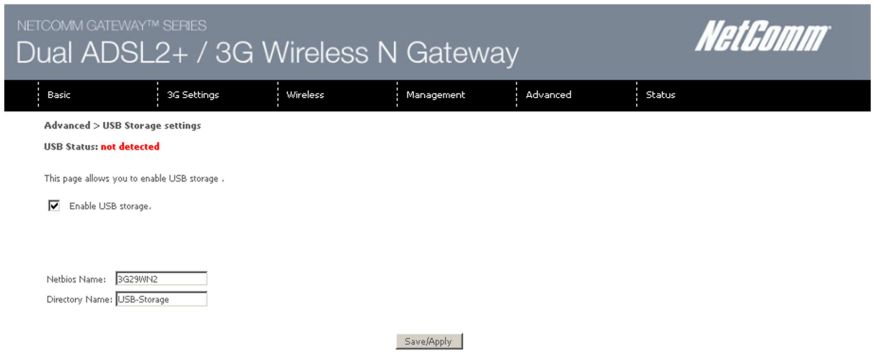

Figure 68: Advanced - USB Storage

Print Server

This page allows you to enable or disable the USB port of the 3G29WN2 to be used as a print server.

Please see Appendix A for more details on setting up your router to work with Print Server functionality.

Figure 69: Advanced - Print Server

Interface Grouping

Interface grouping supports multiple ports to PVC and bridge groups. Each group performs as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WA N interfaces using the Add button.

The Remove button removes mapping groups, returning the ungrouped interfaces to the default group. Only the default group has an IP interface.

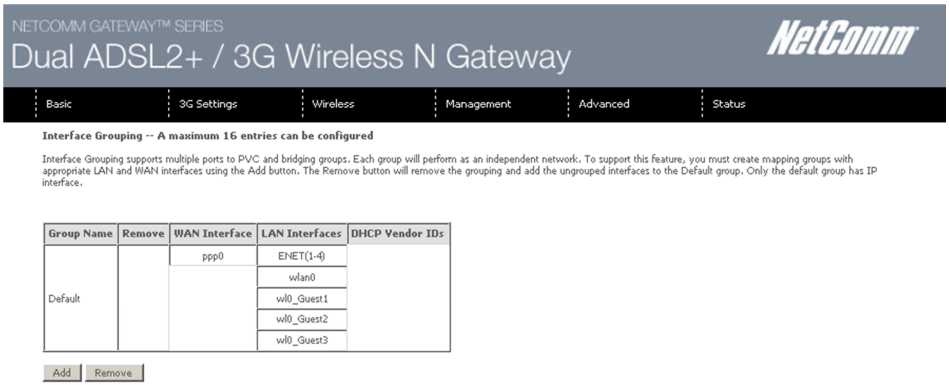

Figure 70: Advanced - Interface Grouping

To add an Interface Group, click the Add button. The following screen will appear. It lists the available and grouped interfaces. Follow the instructions shown below:

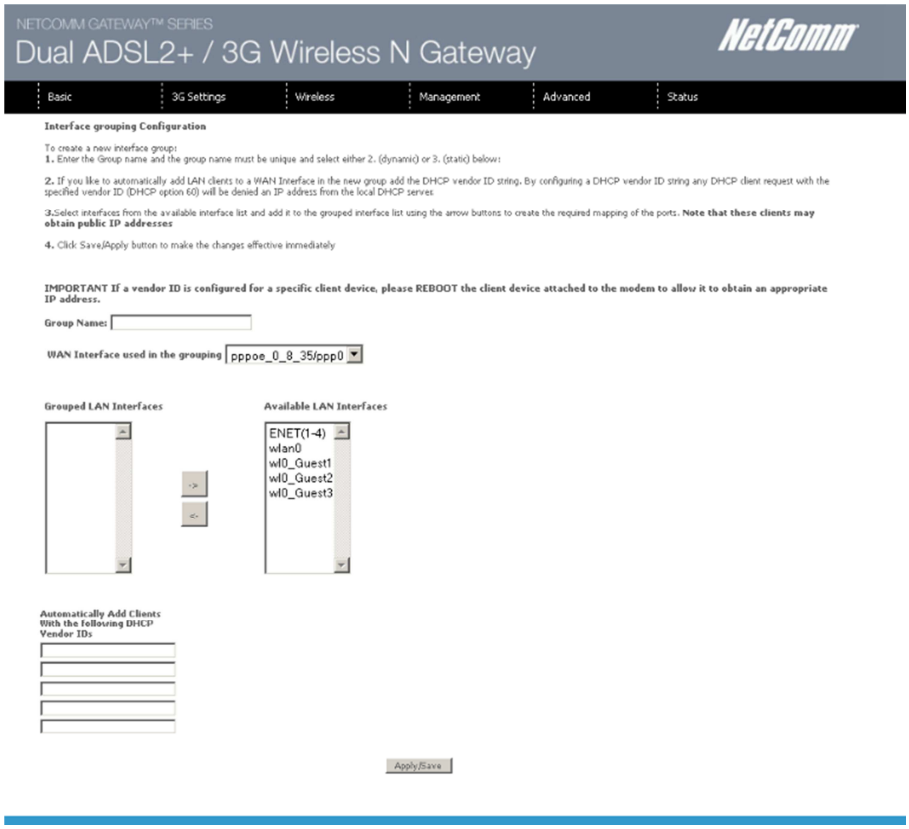

Figure 71: Advanced - Add Interface Grouping

Automatically Add Clients with the following DHCP Vendor IDs

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

LAN Ports

Use this page to enable or disable the Virtual LAN Ports feature.

Figure 72: Advanced - LAN Ports

Status

The Status menu has the following submenus:

- Diagnostics
- System Log
- 3G network
- Statistics
- Route
- ARP
- DHCP

Diagnostics

The Diagnostics menu provides feedback on the connection status of the device. The individual tests are listed below. If a test displays a fail status:

1. Click on the Help link and follow the troubleshooting procedures in the Help screen that appears.
2. Now click Re-run Diagnostic Tests at the bottom of the screen to re-test and confirm the error
3. If the test continues to fail, contact Technical Support.

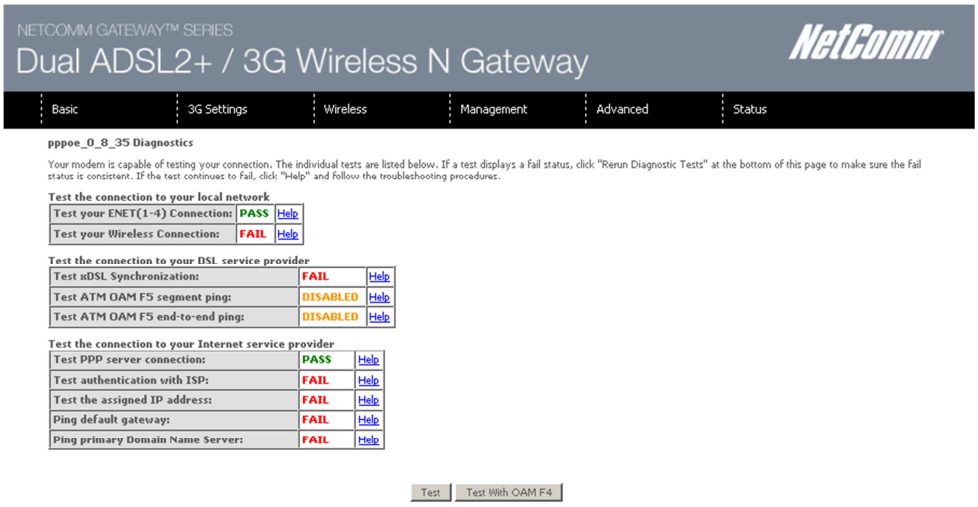

Figure 73: Status - Diagnostics

FIELD	DESCRIPTION
ENET Connection	Pass: Indicates the Ethernet connection to your computer is connected to the LAN port of the router. Fail: Indicates that the router does not detect the Ethernet interface of your computer.
Test your Wireless Connection	Pass: Indicates that the wireless card is switched ON. Fail: Indicates that the wireless card is switched OFF.
Test the Assigned IP Address	Pass: Indicates that the modem has received a valid IP address from the PPP server. Fail: Indicates that the modem has not received a valid IP address from the PPP server.
Ping Primary Domain Name Server	Pass: Indicates that the router can communicate with the DNS server. Fail: Indicates that the router was unable to communicate with the primary Domain Name Server (DNS). This may not have an effect on your internet connection. Therefore if this test fails but you are still able to connect to the internet there is no need to troubleshoot this issue.

Table 27: Status - Diagnostics Fields

System Log

This function allows you to view system events and configure related options. Follow the steps below to enable and view the System Log.

1. Click Configure System Log to continue.

Figure 74: Status - System Log

2. Select the system log options (see table below) and click Apply/Save.

Figure 75: Status - Configure System Log

FIELD	DESCRIPTION
Log	Indicates whether the system is currently recording events. System logging can be disabled or enabled. By default system logging is disabled.
Log Level	Allows you to configure the event level and filter out unwanted events below this level. The events range from the highest level "Emergency" down to the lowest "Debugging" level and are stored in the router's SDRAM memory. When the log buffer is full the newest event will wrap up to the top of the log buffer and overwrite the lowest event. By default the log level is "Debugging" which is the lowest critical level. The log levels are defined as follows: Emergency is the most serious event level whereas debugging is the least important. For instance if the log level is set to debugging, all the events from the lowest debugging to the highest Emergency level will be recorded. If the log level is set to Error level only error level logs will be able to be viewed.
Display	Allows you to select the log events and displays in the View System Log window. For events from debugging level and above to the highest Emergency level.
Level	Allows you to select the logged events and display in the View system Log window, per log level.
Mode	Allows you to specify whether events should be stored in local memory, be sent to a remote system log server or both simultaneously. If remote mode is selected the view system log windows will not be able to display events saved to the remote system log server. When either Remote mode or both mode are selected you will be prompted for the system log server IP address and UDP port.

3G Network

Select this option for detailed status information on your router's 3G connection.

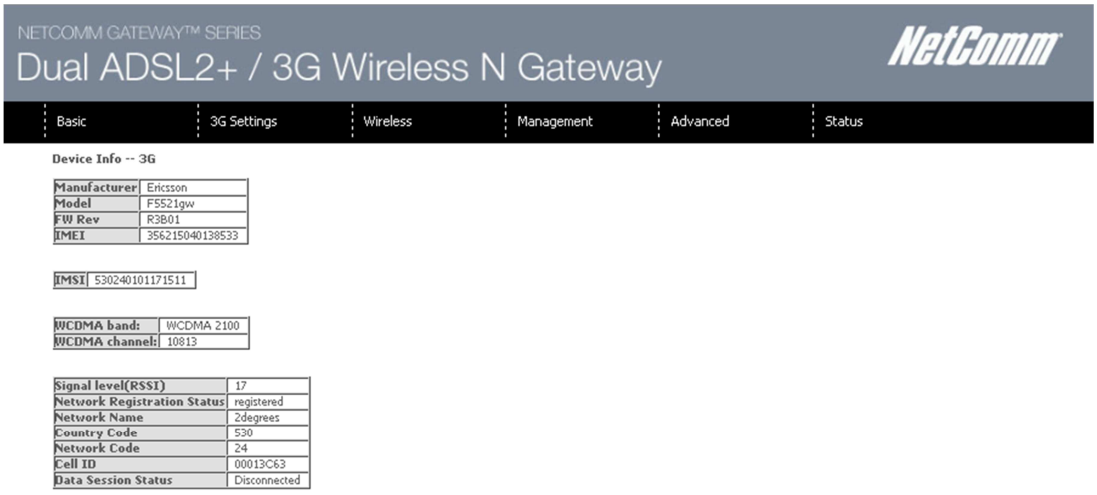

Figure 76: Status - 3G Network

STATUS	DESCRIPTION
Manufacturer	The manufacturer of the embedded 3G module.
Model	The model name of the embedded 3g module.
FW Rev	The firmware version of the 3G module.
IMEI	The IMEI (International mobile Equipment Identity) is a 15 digit number that is used to identify a mobile device on a network.
IMSI	The IMSI (International Mobile Subscriber Identity) is a unique 15 digit number that is used to identify an individual user on a UMTS or GSM network.
WCDMA Band	A 3G radio frequency which supports tri-band UMTS/HSDPA/HSUPA frequencies (850/1900/2100MHz), IMT2000 is 2100MHz. WCDMA800 is 850 MHz, WCDMA1900 is 1900 MHz.
WCDMA Channel	The 3G channel.
Signal Level(RSSI)	3G Radio Signal Strength Index.
Network Registration Status	This filed should display as registered with a valid unlocked SIM card.
Network Name	The 3G Internet Service Provider.
Country and Network Code	Each country and network has a unique code.
Cell ID	The network information for the serving cell ID.
Data Session Status	This field displays whether the 3G module is connected or disconnected to the 3g network.

Figure 77: Status - 3G Network Settings

Statistics

These screens provide detailed information for:

- Local Area Network (LAN), Wide Area Network (WAN), ATM and ADSL
- 3G Interfaces

NOTE: These statistics page refresh every 15 seconds.

LAN

This screen displays statistics for the Ethernet and Wireless LAN interfaces.

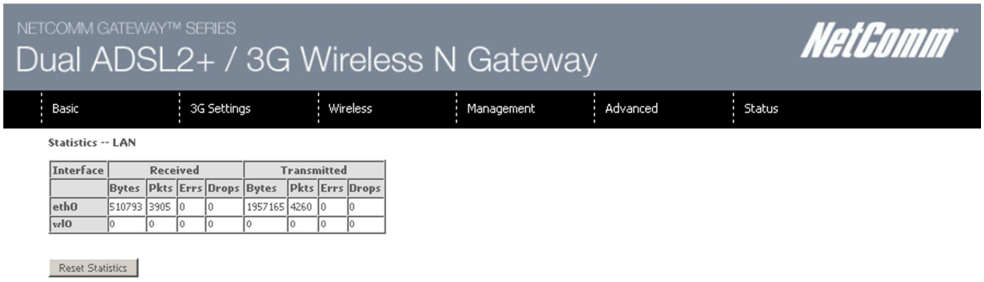

Figure 78: Status - Statistics - LAN

INTERFACE	DESCRIPTION	
Received/Transmitted	Bytes	Rx/Tx (receive/transmit) packets in bytes.
	Pkts	Rx/Tx (receive/transmit) packets.
	Errs	Rx/Tx (receive/transmit) packets with errors.
	Drops	Rx/Tx (receive/transmit) packets with drops.

Table 28: Status - Statistics - LAN Fields

3G Network

This page displays the inbound and outbound statistics of the 3G network.

Figure 79: Status - Statistics - 3G

WAN

This screen displays statistics for the Ethernet and Wireless LAN interfaces.

Figure 80: Status - Statistics - WAN

INTERFACE	DESCRIPTION	
Received/Transmitted	Bytes	Rx/Tx (receive/transmit) packets in bytes.
	Pkts	Rx/Tx (receive/transmit) packets.
	Errs	Rx/Tx (receive/transmit) packets with errors.
	Drops	Rx/Tx (receive/transmit) packets with drops.

Table 29: Status - Statistics – WAN Fields

ATM

The ATM statistics page shows the details of the ATM interface.

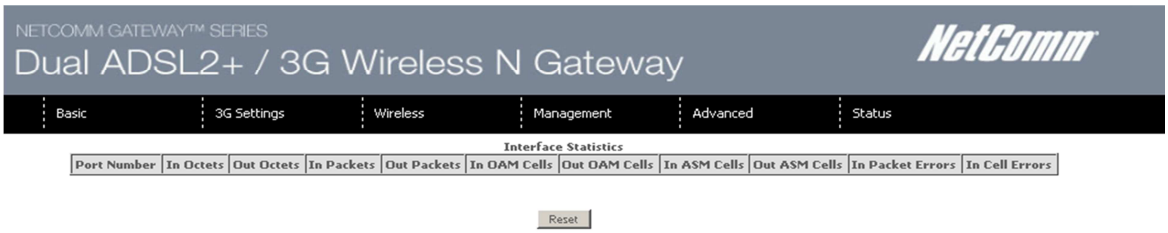

Figure 81: Status - Statistics – ATM

FIELD	DESCRIPTION
In Octets	The number of data packets in octets received over the ATM interface.
Out Octets	The number of data packets in octets transmitted over the ATM interface.
In Errors	The number of data packets dropped due to uncorrectable HEC errors.
In Unknown	The number of cells discarded during cell header validation, including cells with unrecognisable VPI/VCI values and cells with invalid cell header patterns. If cells with undefined PTI values are discarded they are also counted here.
In HEC Errors	The number of cells received with an ATM Cell Header HEX Error
In Invalid VPI VCI Errors	The number of cells with an unregistered VCC address.
In Port not Enable Errors	The number of cells received on a port that has not been enabled.
In PTI Errors	The number of cells received with an ATM Header Payload Type Indicator (PTI) error.
In Idle Cells	The number of idle cells received.
In Circuit Type Errors	The number of cells received with an illegal circuit type.
In OAM RM CRC Errors	The number of OAM and RM cells received with CRC errors.
In GFC Errors	The number of cells received with non-zero GFC.

Table 30: Status - Statistics - ATM Fields

ADSL

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

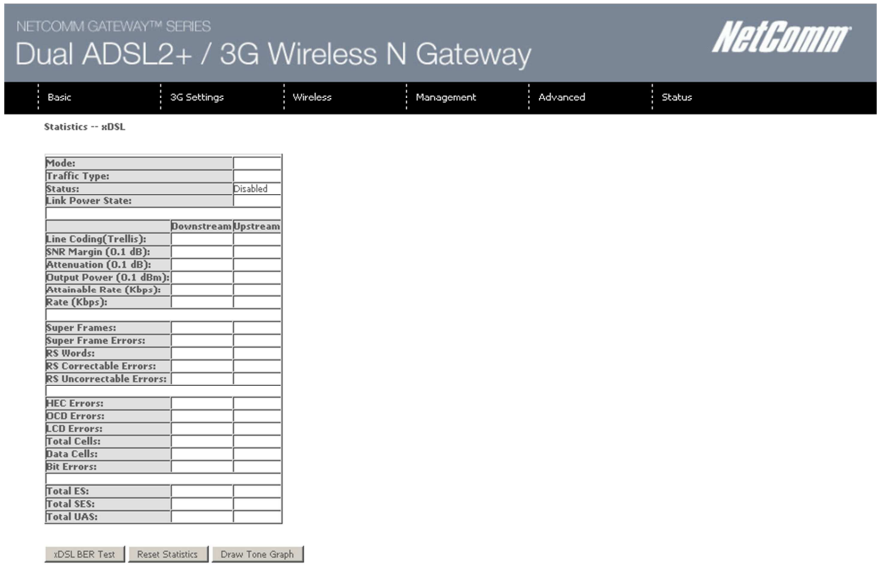

Figure 82: Status - Statistics – ADSL

Route

Select Route to display the paths the Router has found.

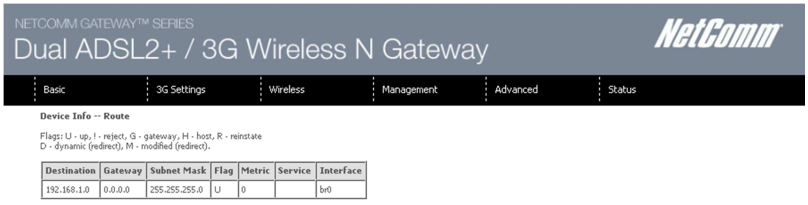

Figure 83: Status - Route

ARP

Click ARP to display the ARP information.

This option can be used to determine which IP address / MAC address is assigned to a particular host. This can be useful when setting up URL filtering, Time of Day filtering or Static DHCP addressing.

Figure 84: Status - ARP

DHCP

Click DHCP to display the DHCP information.

Figure 85: Status - DHCP

You can use this to determine when a specific DHCP lease will expire, or to assist you with setting up Static DHCP addressing.

PING

Figure 86: Status - PING

You can use this to verify your internet connection is active or to test whether a website is currently available or not.
For example: www.google.com

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 3G29WN2 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 any 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.

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 3G29WN2 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 3G29WN2 and the power source are both turned on and device is receiving sufficient power.
3	Turn the 3G29WN2 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 3G29WN2. 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 3G29WN2'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 3G29WN2 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 3G29WN2 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 3G29WN2 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 3G29WN2.

MODEL	3G29WN2
CPU	BCM5325
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	12V DC – 1.5A
Dimensions & Weight	215 mm (W) x 37 mm (H) x 145 mm (D)
Regulatory Compliance	C-Tick

Electrical Specifications

It is recommended that the 3G29WN2 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 3G29WN2 housing enables it to operate over a wide variety of temperatures from 0˚C - 40˚C (operating temperature).

Appendix A: Print Server

These steps explain the procedure for enabling the Print Server.

1. Enable Print Server from the Advanced menu in the Web User Interface of the router.
2. Select Enable on-board print server checkbox and enter the printer name and make and model.

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

3. Press the Apply/Save button to save the new settings.

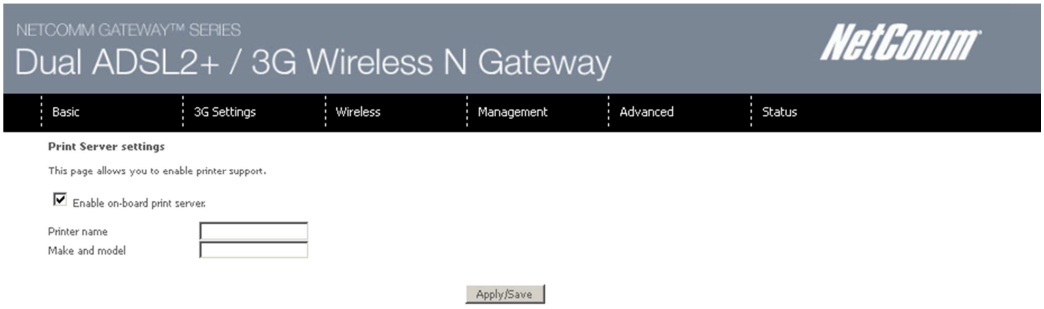

Figure 87: Advanced - Print Server Settings

For Windows Vista/7

These steps explain the procedure for enabling the Printer Server.

1. Enable Print Server from Web User Interface.

Select Enable on-board print server checkbox and enter the printer name and make and model.

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

Figure 88: Advanced - Print Server Settings

2. Go to the control panel, and select 'Printers' if you are using Windows Vista or select "Devices and Printers" if you are using Windows 7.
3. Once in the 'Printers' page, click the 'Add a printer' button as shown below.

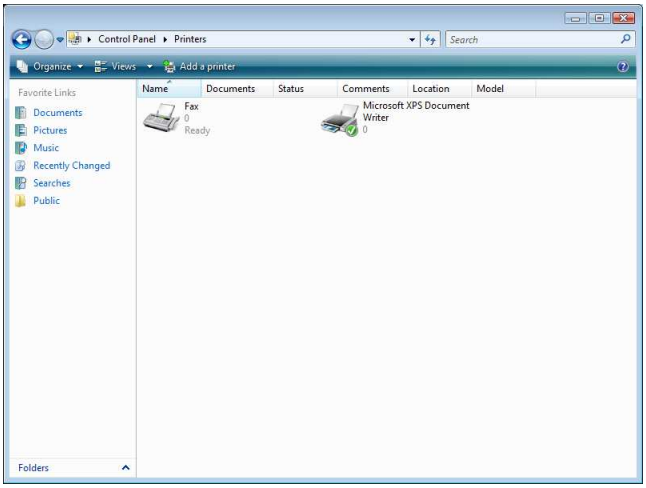

Figure 89: Windows 7 - Control Panel – Printers

4. Select the 'Add a network, wireless or bluetooth printer' option.

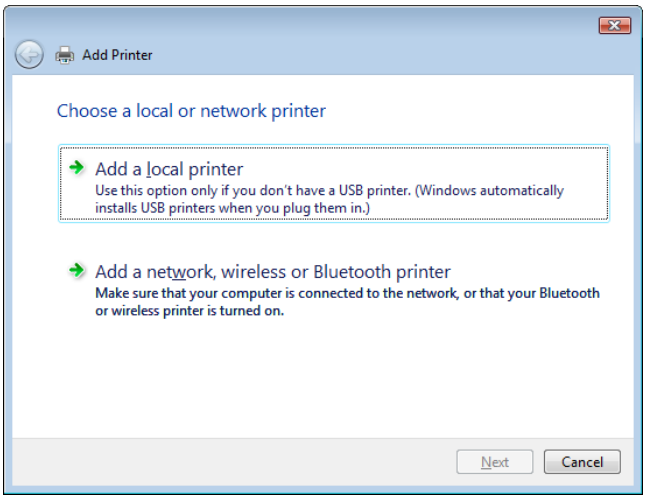

Figure 90: Windows 7 - Add Printer

5. Click on the radio-button labelled **'Select a shared printer by name'**, and type

   "http://192.168.1.1:631/printers/Printer_Name" in the box below. Ensure the printer name is the name you entered in step 1 Click 'Next'.

NOTE: The PrinterName must be the same as the printer name entered into the Printer section of Dual-3G29WN2.

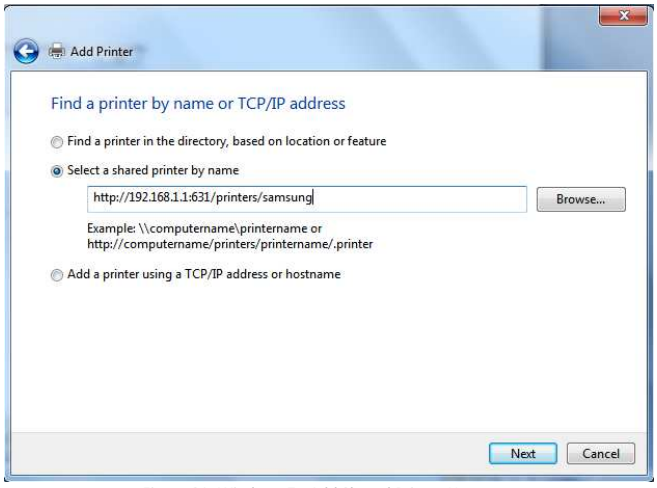

Figure 91: Windows 7 - Add Shared Printer Name

6. Next, select the driver that came with your printer. Browse through the list to select your printer driver, or click 'Have Disk' if you have your printer driver installation media.

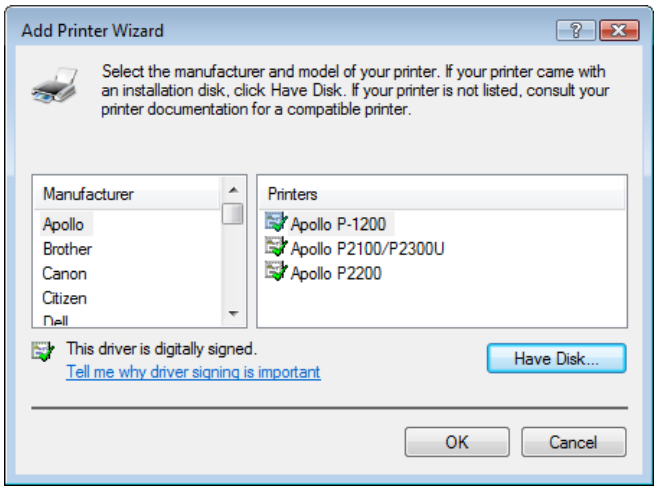

Figure 92: Add Printer Drivers

7. Choose whether you want this printer to be the default printer, and then click 'Next'.

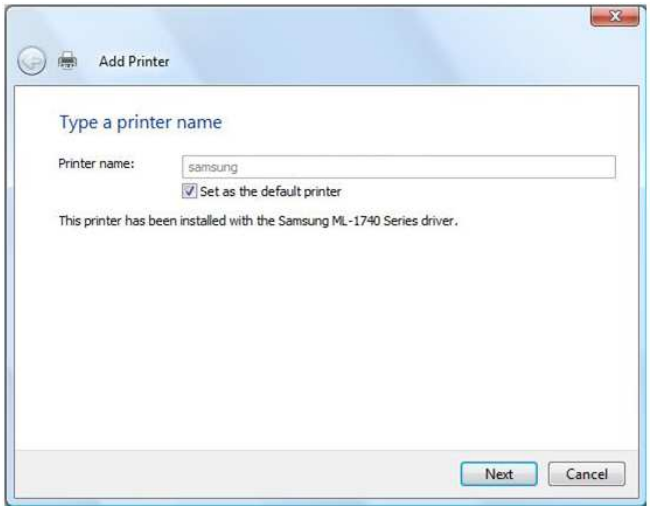

Figure 93: Add Printer Name

8. Click 'Finish'. Your device is now configured and ready for use.

For MAC OSX

These steps explain the procedure for enabling the Printer Server and setting up a printer for the Mac OSX operating system.

1. Enable Print Server from Web User Interface.

Select Enable on-board print server checkbox and enter the printer name and make and model.
NOTE: The Printer name can be any text string up to 40 characters. The Make and model can be any text string up to 128 characters.

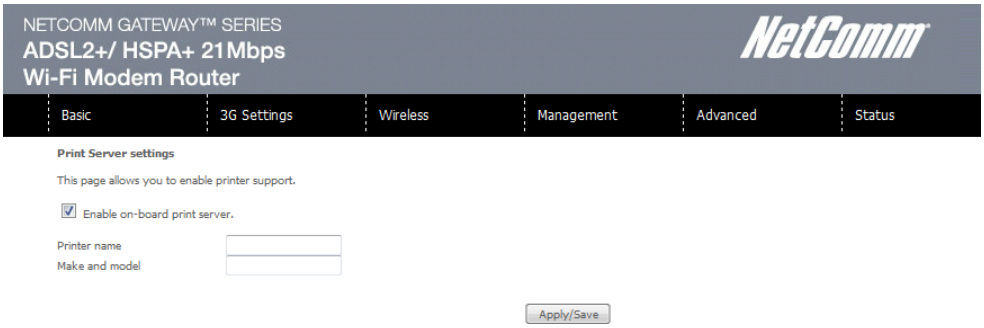

Figure 94: Enable Print Server

2. To set up your printer, check the Apple menu and select the "System Preferences" option. In the System Preferences menu click on the "Print & Fax" option.

Figure 95: System Preferences

3. With your Printer driver installed, please add your printer from the Print &Fax menu.

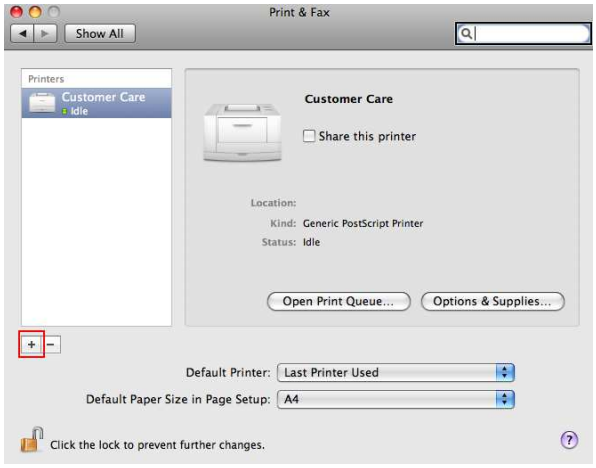

Figure 96: Print & Fax Menu

4. Mouse over to the Protocol drop down list and select Internet Printing Protocol – IPP.

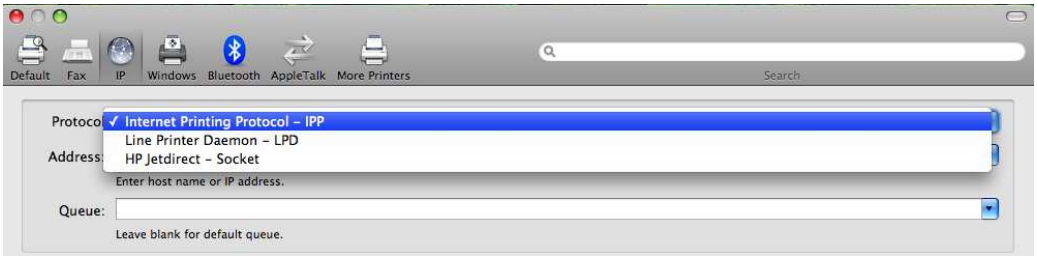

Figure 97: Internet Printing Protocol

5. Input the Address field with "192.168.1.1:631" and the Queue with "/printers/PrinterName"

Figure 98: Add Printer Path

NOTE: The Printer Name must be the same as the printer name entered into the Printer section of Dual-3G29WN2.

6. From the "Print Using" drop down list and select your corresponding printer driver.

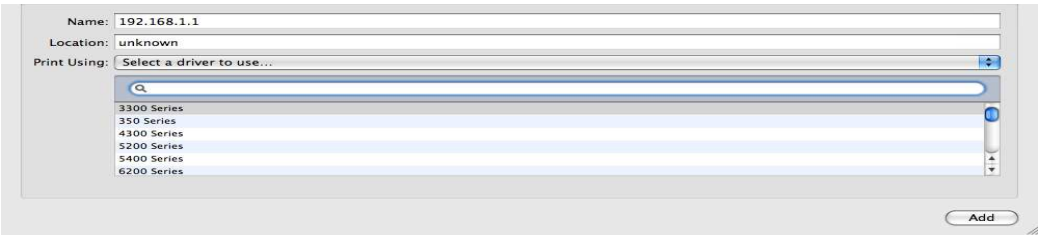

Figure 99: Add Printer Driver

7. Click Add and check the printer status.

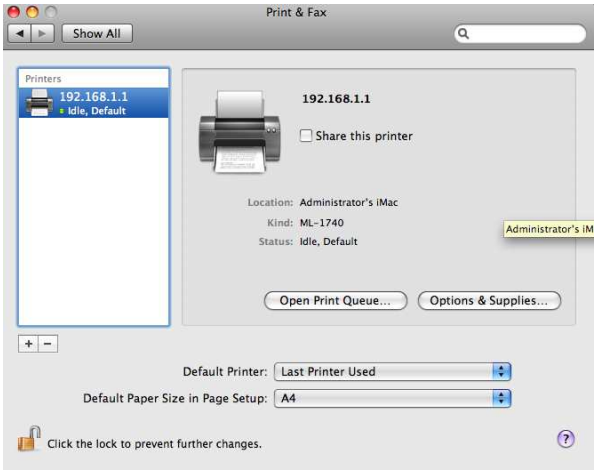

Figure 100: Check Printer Status

Appendix B: Samba Server

For Windows Vista/7

1. Open a web-browser (such as internet Explorer, Firefox or Safari).

2. Type in the address \\ “NetbiosName”\ “DirectoryName” \ (eg \\ntc-cpe\ntc-cpe).

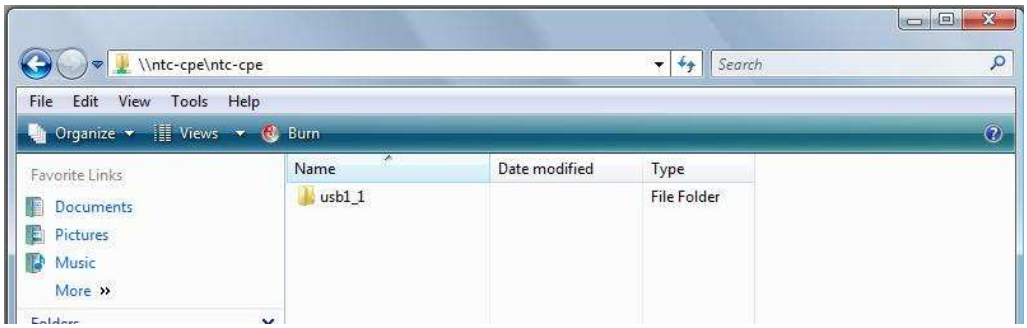

Figure 101: Access USB Drive

Note: There are no username and password required to access the USB drive, the user will be able to read/write the folder/files in the USB drive.

For MAC OSX

1. Click the finder icon in the Dock.
2. Choose **Connect to Server** from the **Go** menu.
3. In the address field of the Connect to Server dialog, type in the URL Smb:// “NetbiosName”/“DirectioryName” (eg smb://ntc-cpe/ntc-cpe) .

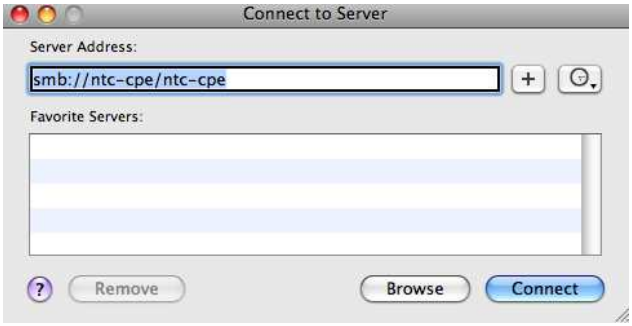

Figure 102: USB Drive Access with Mac

4. Select the Connect button to connect your USB driver.

Legal & Regulatory Information

Intellectual Property Rights

All intellectual property rights (including copyright and trade mark rights) subsisting in, relating to or arising out this Manual are owned by and vest in NetComm Wireless 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.

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.

Consumer Protection Laws

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

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

Product Warranty

All NetComm 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.

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