NETCOMM GATEWAYY™ SERIES

Dual ADSL2+/3G Gateway

User Guide

Preface

This manual provides information related to the installation, operation, and application of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be broken or malfunctioning, please contact technical support for immediate service by email at technicalsupport@netcomm.com.au

For product update, new product release, manual revision, or software upgrades, please visit our website at www.netcomm.com.au

Important Safety Instructions

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

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

⚠ WARNING

- Disconnect the power line from the device before servicing.

Copyright

NOTE:This document is subject to change without notice.

Save Our Environment

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

The cardboard box, the plastic contained in the packaging, and the parts that make up this router 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.

Table of Contents

Introduction

Introduction

Your Dual ADSL2+ / 3G Gateway

Congratulations on your purchase of a NetComm 3G29WN – Dual ADSL2+ / 3G Gateway. This product is a high-performance ADSL2+ Modem Router combined with a HSPA+ module that provides high-speed wireless N networking and Internet connectivity for your home, office or public space.

The NetComm 3G29WN gives you the option to plug directly into an ADSL service or connect with 3G by inserting a 3G SIM card to deliver Internet. The choice is yours. Both methods will allow you to share your Internet connection amongst multiple users with either the 4 LAN ports for wired connections or via high-speed Wireless N.

The 3G29WN also allows for a HSPA+/3G Mobile Broadband connection (provided by a SIM card) to act as a backup Internet connection to your fixed line service, providing automatic Internet failover to 3G in the event that the ADSL service fails. Should you have access to both connection methods, the 3G29WN will ensure you are “always on” which is vital to some individuals and business that perform Internet based critical operations.

The USB port is able to be used for the purpose of printing and a mass storage server. By simply plugging in a USB printer or a USB hard drive to the router, the functionality of these products will be able to be shared with everyone connected to the 3G29WN.

The 3G29WN features the latest standards of wireless security enabled by default on each router. An advanced firewall and VPN pass-through functionality allows for maximum security and caters for the encrypted Point-to-Point communications from connected computers through the 3G29WN to a VPN Server.

The Port Forwarding and UPnP functionality provided by the 3G29WN make it easier for today’s Internet users to setup and configure the various network Port Forwarding Rules needed by Internet applications such as On-Line Gaming, Peer-To-Peer file sharing and Instant Messaging services.

Package contents

Your 3G29WN contains the following items:

- 3G29WN – Dual ADSL2+ / 3G Gateway
- 12VDC, 1.5A Power Supply
- RJ-11 ADSL Line connection cable
- RJ-45 Ethernet cable
- 2 x Removable 3G Antennas
- 1 x Removable WiFi Antenna
- User Guide (on CD)
- Printed Quick Start Guide

Key features

- Fully featured ADSL2+ Modem Router
- Embedded multimode HSUPA/HSDPA/HSPA+/UMTS module
- Dual-band HSPA+/UMTS (850 / 2100 Mhz)
- Supports auto Internet failover from ADSL to 3G
- Wireless N access point – high speed wireless up to 300Mbps
- 2 Transmit and 2 Receive WiFi antennas
- 4 LAN ports for multiple wired connections
- 1 x USB host Port
- Web browser based interface for configuration and management: OS independent and easy to use
- Full wireless security - WEP, WPA, WPA2
- MAC address and IP filtering
- Static route functions
- DNS Proxy
- Web-based management
- Supports VPN Pass-through
- NAT/PAT
- Configuration backup and restoration
- DHCP Server/Relay/Client

Placement of your Dual ADSL2+ / 3G Gateway

When Connecting With 3G

Just like your mobile phone, the location of the 3G29WN will affect its signal strength to a 3G Mobile Base Station (Cell Tower). The data speed achievable is relative to this signal strength, which is affected by many environmental factors. Please keep in mind that the 3G29WN will need adequate signal strength in order to provide Internet connectivity whilst choosing a location to place your Router.

Similarly to the 3G connection, the wireless connection between the Router and your WiFi devices will be stronger the closer your connected devices are to your Router. Your wireless connection and performance will degrade as the distance between your Router and connected devices increases. This may or may not be 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 Router in order to see if distance is the problem. If difficulties persist even at close range, please contact NetComm Technical Support.

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.

Router placement

- Place your Router as close as possible to the centre of your wireless network devices to achieve the best wireless network coverage for all your "wireless clients" (i.e., computers with built in or USB Wireless Adapters, Laptops with Built-in Wireless, Wireless PDA / iPhone, etc)
- Ensure that your Router's antennas are parallel to each other, and are positioned vertically (toward the ceiling). If your Router itself is positioned vertically, point the antennas in an upward direction as much as possible.
- In multi-storey homes, place the Router on a floor that is as close to the centre of the home as possible. This may mean placing the Router on an upper floor.
- Try not to place the Router near a cordless telephone that operates at the same radio frequency as the 3G29WN (2.4GHz).

Avoid obstacles and interference

- Avoid placing your Router 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 these are not blocking the signal's path (between your devices and Router).

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 Router 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 Wi-Fi Router.
- 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 Router to channel 11. See your phones user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 5GHz cordless phone.

Choose the “quietest” channel for your wireless network

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with your wireless network.

Use the Site Survey capabilities found in the Wireless Utility to locate any other wireless networks that are available and switch your Router and computers to a channel as far away from other networks as possible.

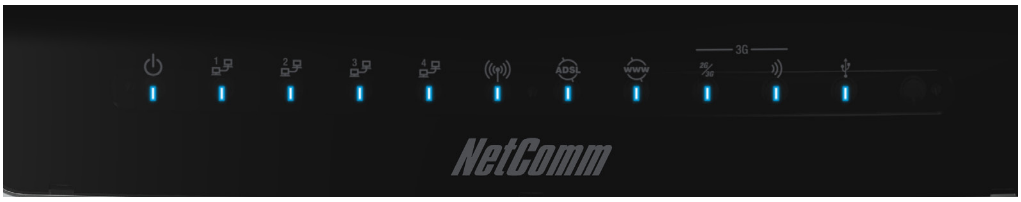
- Experiment with more than one of the available channels in order to find the clearest connection and avoid interference from neighbouring cordless phones or other wireless devices.
- For assistance with placing NetComm wireless networking products, use the detailed Site Survey and wireless channel information included with your wireless network card. See your network card’s user guide for more information.

These guidelines should allow you to cover the maximum possible area with your Router. Should you need to cover an even wider area, you should consider looking at building a hybrid network by combining your wireless network with a Powerline Network. See the NetComm website for more details on Powerline products.

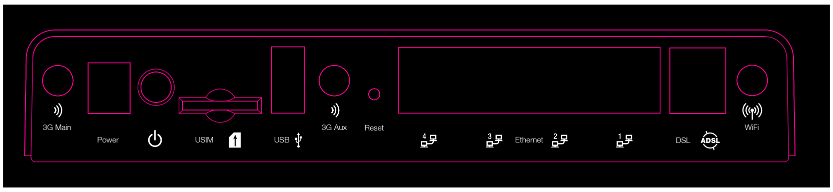
Product Layout

Getting to know your 3G29WN

It is recommended that you take a moment to acquaint yourself with the indicator lights, ports and default settings of the 3G29WN prior to commencing with installation.



LED	ICON	COLOUR	MODE	FUNCTION
Power	⏻	Blue	On	The router is powered on
			Off	The router is not powered
LAN 1-4	1🖧	Blue	On	Ethernet link is established
			Off	There is no Ethernet link established
			Blinking	Data transmitting/receiving over Ethernet
Wi-Fi	((ψ))	Blue	On	Local Wi-Fi access to the Router is enabled and working
			Off	Wireless Module is not installed / enabled
			Blinking	Data transmitting/receiving over Wi-Fi
ADSL	ADSL	Blue	On	The ADSL link is established
			Blinking slowly	The is no ADSL link established
			Blinking	The ADSL line is training or traffic is passing through
Internet	www	Blue	On	A link to the Internet is established
			Off	Modem is in bridged mode or ADSL connection is not present
			Blinking	Data transmitting/receiving over the Internet
		Lavender	On	The Internet connection has auto failed over from ADSL to 3G
3G Mode	2G/3G	Blue	On	3G connection is active
			Off	No available 3G connection
		Lavender	On	2G connection is active
3G Signal	)))	Blue	On	3G signal strong
		Lavender	On	3G signal medium
		Red	On	3G signal weak
			Blinking	SIM card not installed
USB	ψ	Blue	On	A USB device is plugged into the USB port
			Off	There is no USB device plugged into the USB port



PORT NAME	FUNCTION
3G Main / 3G Aux	3G antennas for connecting to 3G base station
Power	Connect the supplied power adapter
On/Off (icon)	Push to turn the 3G29WN on and off
USIM	USIM card slot. Insert your SIM card here
USB	Connect your USB printer or storage device
Reset	Reset button. Depress for 10 seconds to return your 3G29WN 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)
Wi-Fi	Wi-Fi antenna for distributing wireless Internet signal

Minimum system requirements

Different aspects of the 3G29WN have different requirements, so let's look at them in turn. We'll start with your computer, which ought to match the following requirements if you are to enjoy the benefits of a high-speed ADSL connection and use of 3G and wireless networking.

PC Requirements:

- Any computer running Windows 98/2000/Me/XP/Vista/7 or Macintosh OSX
- Ethernet or Wireless Network card
- CD-ROM drive
- Web browser e.g.
  - Internet Explorer 5.1 (or better)
  - Netscape Navigator
  - Mozilla FireFox 1.0.4 (or better)
  - Safari

ADSL Requirement:

- 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

Wireless Computer/Device Requirements

- Computer/device 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 Microfilter can be purchased from NetComm or your Service Provider, if required.

Default settings

LAN (Management)

- Static IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

WAN (Internet)

- WAN mode: DHCP

Wireless

- SSID: NetComm Wireless
- Channel: Auto
- Security: WPA-PSK
- WEP Key: a1b2c3d4e5

Interface Access

- Username: admin
- Password: admin

Restore Factory Default Settings

Restoring factory defaults will reset the 3G29WN to its factory default configuration. Occasions may present themselves where you need to restore the factory defaults on your 3G29WN such as:

- You have lost your username and password and are unable to login to your 3G29WN's web configuration page;
- You have purchased your 3G29WN 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 3G29WN to its factory default settings, please follow these steps:

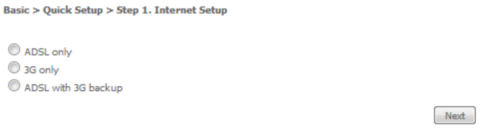
- Ensure that your 3G29WN is powered on (for at least 10 seconds);
- Use a paper clip or a pencil tip to depress the reset button for ten seconds and release. At this point, the reset is in progress. Do not power off the unit;
- When the indicator lights return to steady blue, reset is complete. The default settings are now restored. The entire process takes about 45 seconds to complete;
- Once you have reset your 3G29WN 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';

Connecting the Dual ADSL2+ / 3G Gateway

- Connect the supplied RJ-11 cable to the DSL port on the back of your router to the phone port that supplies your ADSL service.
- And/or, insert your SIM card (until you hear a click) into the USIM slot on the rear of the Router.
- Connect the supplied RJ-45 Ethernet cable from one of the LAN ports on the back of the router to your computer.
- Attach the two 3G antennas provided to the ports marked Main and AUX on the back of the router. The antennas should be screwed in a clockwise direction.
- Screw the supplied detachable Wi-Fi antenna to the Wi-Fi connector on the back of the router.
- Connect the supplied power adapter to your router and press the on/off button to power the router on.

Quick Setup

- Open a web browser (Internet Explorer, Firefox, Safari) and type 192.168.1.1 into the address bar at the top of the window.
- At the login screen type admin into both the username and password fields. Then click submit. This will take you directly to the Quick Setup page

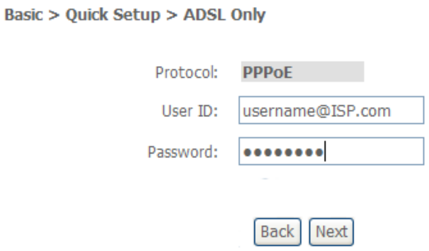


Basic > Quick Setup > Step 1. Internet Setup

○ ADSL only
○ 3G only
○ ADSL with 3G backup

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 ISP



Basic > Quick Setup > ADSL Only

Protocol: PPPoE

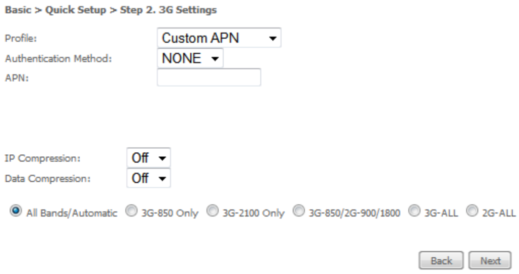
User ID: username@ISP.com

Password: ••••••••

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 Next
2. Type the APN in the APN field. This is supplied by your 3G ISP
3. Authentication Method should be provided by your Internet service provider; or just leave it to NONE if not required.



Basic > Quick Setup > Step 2. 3G Settings

Profile: Custom APN
Authentication Method: NONE
APN:

IP Compression: Off
Data Compression: Off

● All Bands/Automatic ○ 3G-850 Only ○ 3G-2100 Only ○ 3G-850/2G-900/1800 ○ 3G-ALL ○ 2G-ALL

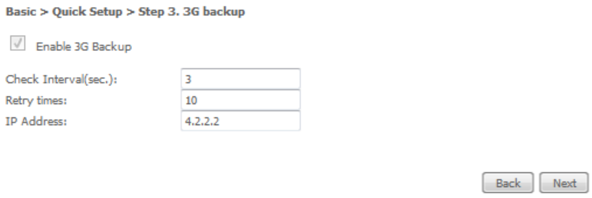
4. Enter the username/password supplied by your 3G ISP.

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 Next to use these settings
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 box and click Next
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



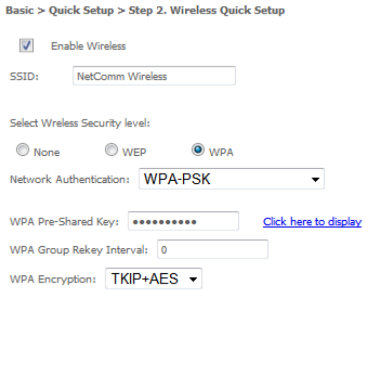
Basic > Quick Setup – Step 3. 3G backup

☑ Enable 3G Backup

Check Interval(sec.): 3
Retry times: 10
IP Address: 4.2.2.2

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

Wireless Set Up



Basic > Quick Setup > Step 2. Wireless Quick Setup

☑ Enable Wireless

SSID: NetComm Wireless

Select Wireless Security level:

○ None ○ WEP ● WPA

Network Authentication: WPA-PSK

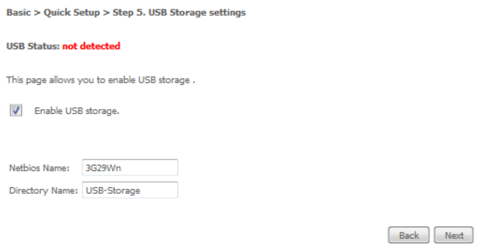
WPA Pre-Shared Key: •••••••••• Click here to display

WPA Group Rekey Interval: 0

WPA Encryption: TKIP+AES

1. The default settings already appear on the wireless quick setup page.
2. You can enable/disable the wireless signal.
3. You can change your wireless SSID. If you do, be sure to remember the new name or write it down so you know which network to connect to.
4. You can also select the level of wireless security and change the wireless password.
5. Once you have completed entering your wireless settings click Next.

USB Storage



Basic > Quick Setup > Step 5. USB Storage settings

USB Status: not detected

This page allows you to enable USB storage .

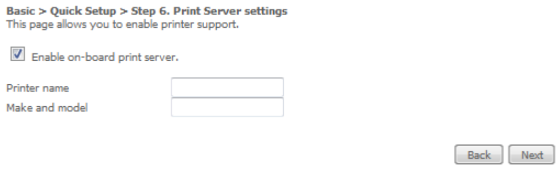
☑ Enable USB storage.

Netbios Name: 3G29Wn

Directory Name: 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, you can change these to anything you want.
3. Click Next once you are happy with the settings.
4. To access the storage device open a web browser and type \\Netbios\Directory\ . So using the defaults \\3G29WN\USB-Storage\

USB Print Server



Basic > Quick Setup > Step 6. Print Server settings
This page allows you to enable printer support.

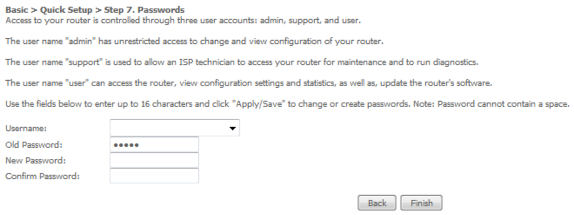
☑ Enable on-board print server.

Printer name

Make and model

1. If a USB printer is plugged into the USB port, it will be auto detected and you will have the choice to Enable 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 Next once you are happy with the settings.
4. To complete setting up your network printer, please read Appendix A of the User Manual.

Passwords



Basic > Quick Setup > Step 7. Passwords
Access to your router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your router.

The user name "support" is used to allow an ISP technician to access your router for maintenance and to run diagnostics.

The user name "user" can access the router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

Username:

Old Password: •••••

New Password:

Confirm Password:

1. On this page you can change the 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 Finish.
4. You will be taken back to the home page where you can view your connection status.

Troubleshooting

Cannot establish a wireless connection

1. Make sure the wireless switch on your laptop is in the on position
2. Ensure your device and wireless adapter are using the same wireless security settings
3. Make sure you are trying to connect to the correct SSID with the correct security key

Cannot establish an ADSL connection

1. Ensure you have entered the correct username and password as supplied by your ISP. If you cannot find them please contact your ISP to ensure you have the correct details.

Cannot establish a 3G Connection

1. Ensure you inserted your 3G SIM Card to the SIM slot properly
2. Ensure you are using an activated 3G SIM Card
3. Ensure you have entered the correct 3G Profile (ISP name and pre/post paid) and that the APN is the same as supplied by your 3G ISP

Cannot access the Web UI

1. 1.If you have changed your username/password and forgotten them you will need to reset your router to the factory default settings and use the default settings admin/admin

How to reset your router to the factory default settings

1. With a paperclip, sharp pencil or similar object press the reset button on the back panel of the device and hold for approximately 10 seconds.

Advanced Configuration

Advanced Configuration – Web User Interface

What can you do from here?

By logging into the web user interface, you are able to configure your 3G29WN 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:

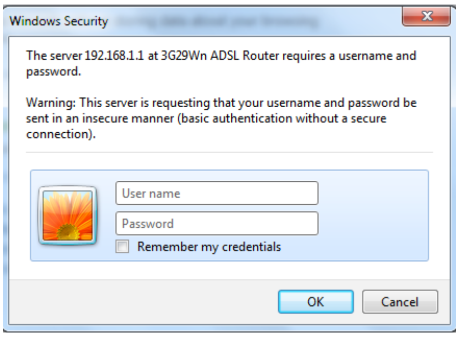
NOTE: The default settings can be found in Default Settings.

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 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 section Default Settings.

Click OK to continue.



Windows Security

The server 192.168.1.1 at 3G29Wn ADSL Router requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

- User Name – admin
- Password – admin

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

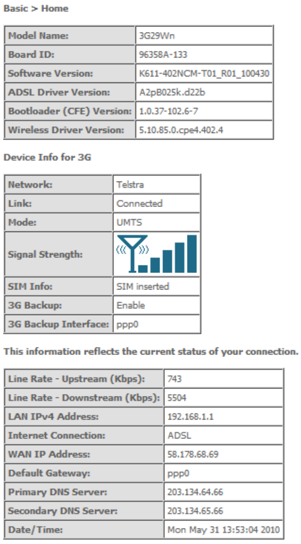
Basic

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 instruction on how to configure your device for use.

Basic - Home



Basic > Home

Model Name:	3G29Wn
Board ID:	96358A-133
Software Version:	K611-402NCM-T01_R01_100430
ADSL Driver Version:	A2pB025k.d22b
Bootloader (CFE) Version:	1.0.37-102.6-7
Wireless Driver Version:	5.10.85.0.cpe4.402.4

Device Info for 3G

Network:	Telstra
Link:	Connected
Mode:	UMTS
Signal Strength:	
SIM Info:	SIM inserted
3G Backup:	Enable
3G Backup Interface:	ppp0

This information reflects the current status of your connection.

Line Rate - Upstream (Kbps):	743
Line Rate - Downstream (Kbps):	5504
LAN IPv4 Address:	192.168.1.1
Internet Connection:	ADSL
WAN IP Address:	58.178.68.69
Default Gateway:	ppp0
Primary DNS Server:	203.134.64.66
Secondary DNS Server:	203.134.65.66
Date/Time:	Mon May 31 13:53:04 2010

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

FIELD	DESCRIPTION
Model Name	Model number of your device
Board ID	The unique number of the board inside your device
Software Version	The current version of software loaded on your device
ADSL Driver Version	The current ADSL driver version loaded on your device
Bootloader (CFE) Version	The version of the bootloader
Wireless Driver Version	The current version of wireless driver being used by your device
DEVICE INFO FOR 3G	
Network	The name of your 3G network
Link	The status of your 3G connection
Mode	The radio access technique currently used to enable internet access. It can be HSUPA, HSDPA, UMTS, EDGE, GPRS or Disconnected.
Signal Strength	The level of signal that your router is receiving from your 3G service provider
SIM Info	Indicates whether or not your SIM card is activated and ready for use
3G Backup	Indicates whether you have set the Dual ADSL2+ / 3G Gateway to act as failover for your ADSL connection
3G Backup Interface	Indicates the WAN interface that is to be back up
CONNECTION STATUS	
Line Rate - Upstream	The ADSL upstream line rate in Kbps (e.g. 256 Kbps)
Line Rate - Downstream	The ADSL downstream line rate in Kbps (e.g. 1500 Kbps)
LAN IPv4 Address	The IP address to access the 3G29WN on the LAN side
Internet Connection	Indicates the Internet Connection type, it can be either “ADSL” or “3G”.
WAN IP Address	The IP address to access the 3G29WN on the WAN side
Default Gateway	The default gateway that your 3G29WN communicates with
Primary DNS Server	The primary DNS server IP address
Secondary DNS Server	The secondary DNS server IP address
Date/Time	The date and time of your Router

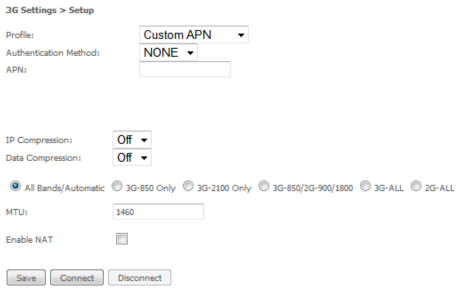
3G Settings

3G Settings

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

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.



3G Settings > Setup

Profile: Custom APN

Authentication Method: NONE

APN:

IP Compression: Off

Data Compression: Off

● All Bands/Automatic ○ 3G-850 Only ○ 3G-2100 Only ○ 3G-850/2G-900/1800 ○ 3G-ALL ○ 2G-ALL

MTU: 1460

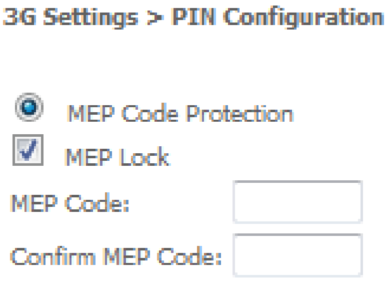
Enable NAT □

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. Authentication Method should be provided by your Internet service provider; or just leave it to AUTO if not required. Type the APN provded in the APN field. If you did not receive a username and password, leave these fields empty.
3. Select IP compression and Data compression to be On or Off. By default they are set to Off.
4. Enter the MTU rate. If you are unsure or have no preference, leave it as the default value
5. Enable or disable NAT – By default this is disabled
6. Click the Save button to save the new settings.
7. Press the Connect button to reboot the router and to connect to Internet. After reboot, the Device Info for 3G network box in the WUI Basic screen should indicate an active connection.

PIN Configuration

On this page you are able to unlock your Router with the appropriate MEP code to work with other 3G providers.



3G Settings > PIN Configuration

● MEP Code Protection

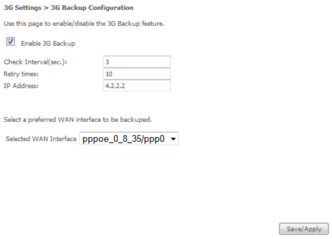
☑ MEP Lock

MEP Code:

Confirm MEP Code:

3G Backup Configuration

On this page you are able to configure your 3G29WN to use 3G as a backup to ADSL. Therefore if you have both connection options available, should your ADSL connection fail, for whatever reason, then your 3G will automatically kick in to ensure you remain connected to the Internet



3G Settings > 3G Backup Configuration

Use this page to enable/disable the 3G Backup feature.

☑ Enable 3G Backup

Check Interval(sec.): 3
Retry times: 10
IP Address: 4.2.2.2

Select a preferred WAN interface to be backuped.

Selected WAN Interface pppoe_0_8_35/ppp0 ▾

OPTION	DESCRIPTION
Enable 3G backup	Check this box to enable your 3G29WN to work with 3G backup
Check Interval	The time in seconds that your 3G29WN will check continuously for your ADSL signal
Retry times	How many times the router will retry the pinging.
IP address	The Public IP address that you would like to use for checking the ADSL Internet connection by Pinging
Selected WAN Interface	The WAN interface that you would like to backup with 3G

Wireless

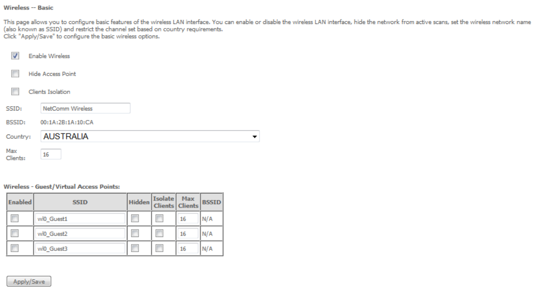
Wireless

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.



Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.
Click "Apply/Save" to configure the basic wireless options.

☑ Enable Wireless

□ Hide Access Point

□ Clients Isolation

SSID: NetComm Wireless

BSSID: 00:1A:2B:1A:10:CA

Country: AUSTRALIA

Max Clients: 16

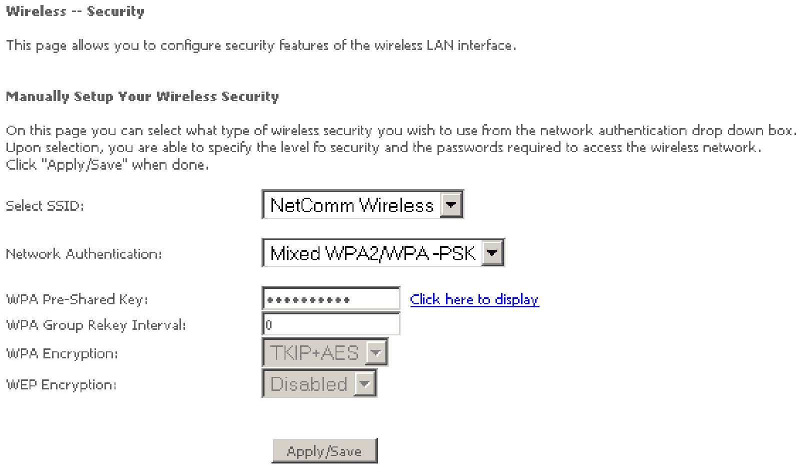
Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Max Clients	BSSID
□	wl0_Guest1	□	□	16	N/A
□	wl0_Guest2	□	□	16	N/A
□	wl0_Guest3	□	□	16	N/A

OPTION	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 client to a hidden access point, the station must add the access point manually to its wireless configuration.
Clients Isolation	1. Prevents clients PC from seeing one another in My Network Places or Network Neighborhood. 2. Prevents one wireless client communicating with another wireless client.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
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 below enforces specific regulations limiting channel range: • Australia = 1-13
Max Clients	The maximum number of Wireless clients which can connect to your wireless network.
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. NOTE: Remote wireless hosts cannot scan Guest SSIDs.

Security

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.



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.

Manually Setup Your Wireless Security

On this page you can select what type of wireless security you wish to use from the network authentication drop down box.
Upon selection, you are able to specify the level fo security and the passwords required to access the wireless network.
Click "Apply/Save" when done.

Select SSID: NetComm Wireless

Network Authentication: Mixed WPA2/WPA -PSK

WPA Pre-Shared Key: •••••••••• Click here to display

WPA Group Rekey Interval: 0

WPA Encryption: TKIP+AES

WEP Encryption: Disabled

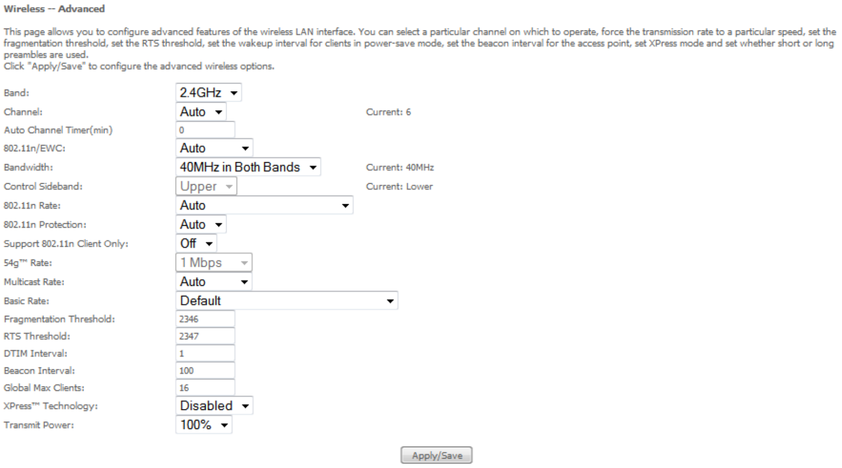
OPTIONS	Description
Select SSID	Pre configured to the default of NetComm Wireless. Can be changed in the Wireless > Settings section
Network Authentication	Here, you can select the type of wireless security you desire. NOTE: The wireless security types are listed in order of level of security from least (top) to most (bottom)
WEP Encryption	The option to enable or disable your wireless security encryption
WPA-PSK / WPA2-PSK	A new 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	WPA (Wi-Fi 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 default
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. 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

Advanced

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

- Select the channel which you wish to operate from
- Force the transmission rate to a particular speed
- Set the fragmentation threshold
- Set the RTS threshold
- Set the wake-up interval for clients in power-save mode
- Set the beacon interval for the access point
- Set Xpress mode
- Program short or long preambles

Click Apply/Save to set the advanced wireless configuration.



Wireless -- Advanced

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

Band:	2.4GHz	
Channel:	Auto	Current: 6
Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	40MHz in Both Bands	Current: 40MHz
Control Sideband:	Upper	Current: Lower
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
54g™ Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	16	
XPress™ Technology:	Disabled	
Transmit Power:	100%	

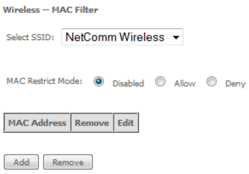
OPTIONS	Description
Band	The frequency of the wireless network. 2.4GHz is standard.
Channel	Allows selection of a specific channel (1-14) or Auto mode.
Auto Channel Timer	The Auto Channel times the length it takes to scan in minutes.
802.11n/EWC	An equipment interoperability standard setting based on 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
Control Sideband	This is available for 40MHz. Drop-down menu allows selecting upper sideband or lower sideband
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.
Fragment 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 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. Default is disabled
Transmit Power	The option of decreasing the transmitting power of your wireless signal
Transmit Power	The option of decreasing the transmitting power of your wireless signal

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.



Wireless -- MAC Filter

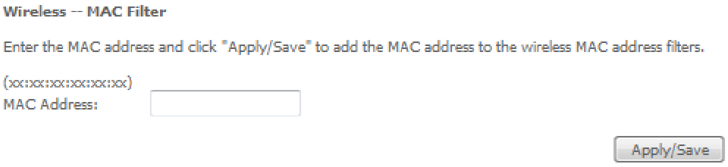
Select SSID: NetComm Wireless

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove	Edit

OPTIONS	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.

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



Wireless -- MAC Filter

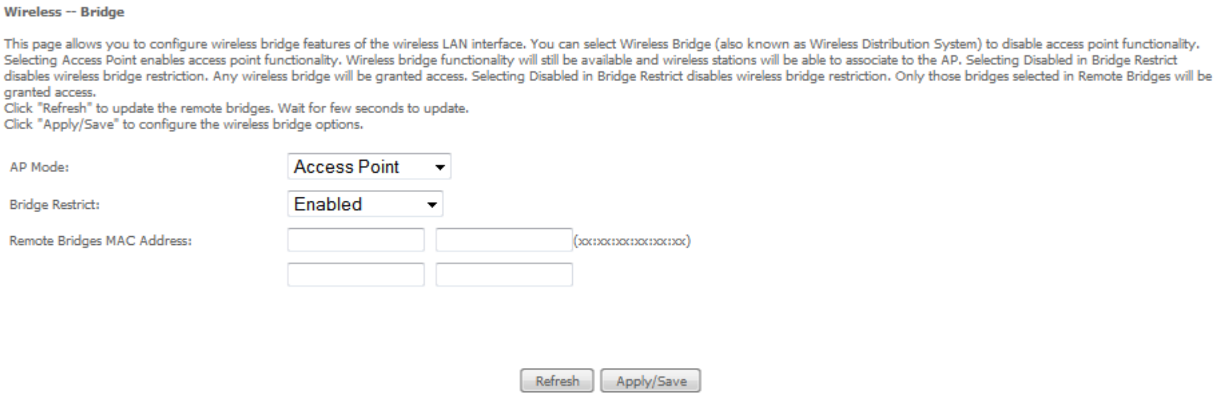
Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

(xx:xx:xx:xx:xx:xx)
MAC Address:

Wireless Bridge

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

Click Apply/Save to implement new configuration settings.



Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Selecting Disabled in Bridge Restrict disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Disabled in Bridge Restrict disables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Apply/Save" to configure the wireless bridge options.

AP Mode: Access Point

Bridge Restrict: Enabled

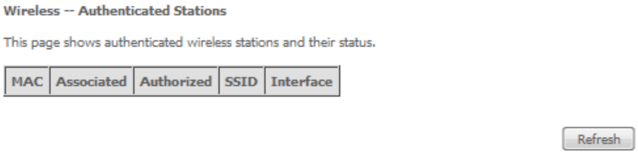
Remote Bridges MAC Address: (xx:xx:xx:xx:xx:xx)

OPTIONS	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.

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.



Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface

OPTIONS	Description
MAC	The MAC address of any connected 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 of your wireless network
Interface	The wireless interface being used to connect

Management

Management

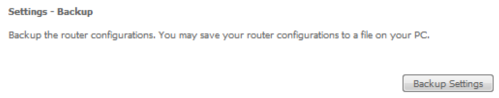
Device Settings

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.

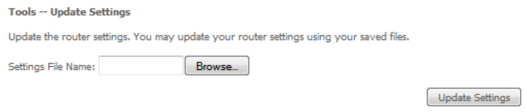


Settings - Backup

Backup the router configurations. You may save your router configurations to a file on your PC.

Update

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



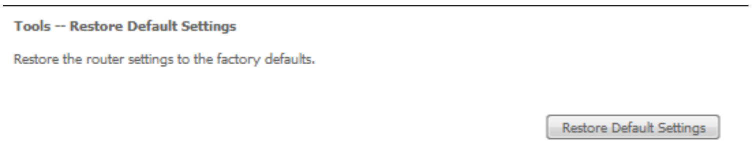
Tools -- Update Settings

Update the router settings. You may update your router settings using your saved files.

Settings File Name:

Restore Default

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

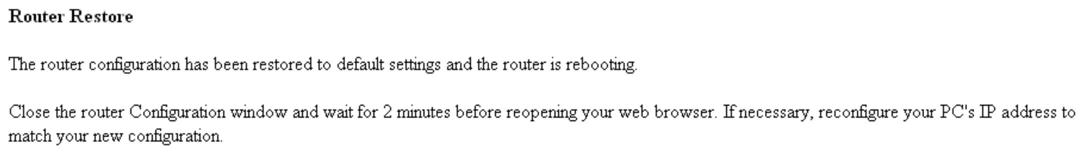


Tools -- Restore Default Settings

Restore the router settings to the factory defaults.

NOTE: The default settings can be found in section 3.1 Default Settings.

Once you have selected the Restore Default Settings button, the following screen will appear. Close the window and wait 2 minutes before reopening your browser. If required, reconfigure your PCs IP address to match your new configuration (see section 3.2 TCP/IP Settings for details).



Router Restore

The router configuration has been restored to default settings and the router is rebooting.

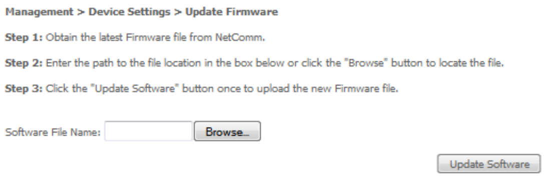
Close the router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

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.



Management > Device Settings > Update Firmware

Step 1: Obtain the latest Firmware file from NetComm.

Step 2: Enter the path to the file location in the box below or click the "Browse" button to locate the file.

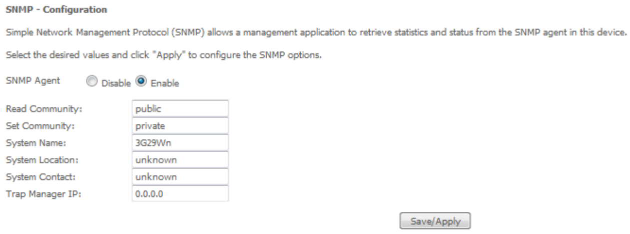
Step 3: Click the "Update Software" button once to upload the new Firmware file.

Software File Name:

NOTE: The update process will take about 2 minutes to complete. The Router will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the Software Version at the top of the Basic screen (WUI homepage) with the firmware version installed, to confirm the installation was successful.

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 3G29WN (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.



SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

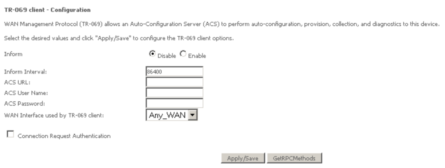
Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent ○ Disable ● Enable

Read Community: public
Set Community: private
System Name: 3G29Wn
System Location: unknown
System Contact: unknown
Trap Manager IP: 0.0.0.0

OPTIONS	Description
Read Community	Read device settings
Set Community	Read and change device settings
System Name	Default = 3G29WN
System Location	User defined value
System Contact	User defined value
Trap Manager IP	IP address of admin machine

TR-069 Client



TR-069 client - Configuration

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

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform	● Disable ○ Enable
Inform Interval:	86400
ACS URL:	
ACS User Name:	
ACS Password:	
WAN Interface used by TR-069 client:	Any_WAN

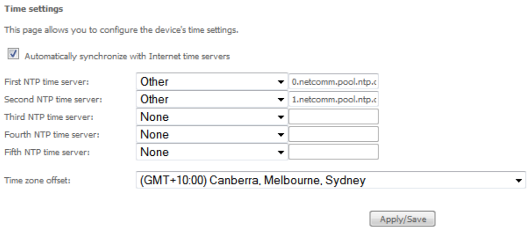
□ Connection Request Authentication

TR-069 enables provisioning, auto-configuration or diagnostics to be automatically performed on your router.*

* - If supported by your Internet Service Provider (ISP)

SNTP

This screen allows you to configure the time settings of your Router.



Time settings

This page allows you to configure the device's time settings.

☑ Automatically synchronize with Internet time servers

First NTP time server:	Other	0.netcomm.pool.ntp.c
Second NTP time server:	Other	1.netcomm.pool.ntp.c
Third NTP time server:	None	
Fourth NTP time server:	None	
Fifth NTP time server:	None	
Time zone offset:	(GMT+10:00) Canberra, Melbourne, Sydney	

OPTIONS	Description
First NTP timeserver:	Select the required server.
Second NTP timeserver:	Select second timeserver, if required.
Time zone offset:	Select the local time zone.

NOTE: SNTP must be activated to use Parental Control .

Access Control

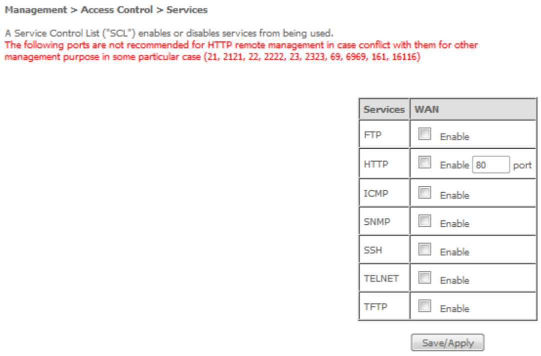
The Access Control option found in the Management drop down menu configures access related parameters in the following three areas:

- Services
- Passwords
- Save/Reboot

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 Apply/Save to continue.



Management > Access Control > Services

A Service Control List ("SCL") enables or disables services from being used.
The following ports are not recommended for HTTP remote management in case conflict with them for other management purpose in some particular case (21, 2121, 22, 2222, 23, 2323, 69, 6969, 161, 16116)

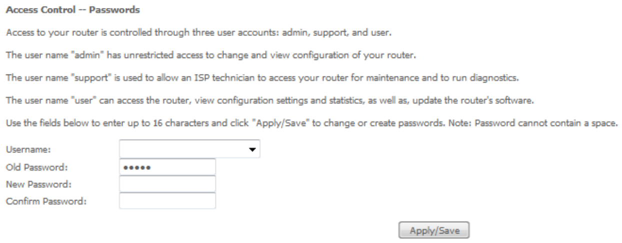
Services	WAN
FTP	□ Enable
HTTP	□ Enable 80 port
ICMP	□ Enable
SNMP	□ Enable
SSH	□ Enable
TELNET	□ Enable
TFTP	□ Enable

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 Apply/Save to continue.



Access Control -- Passwords

Access to your router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your router.

The user name "support" is used to allow an ISP technician to access your router for maintenance and to run diagnostics.

The user name "user" can access the router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

Username:

Old Password: •••••

New Password:

Confirm Password:

8.5.3 Save/Reboot

This function saves the current configuration settings and reboots your Router.

Click the button below to reboot the 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.

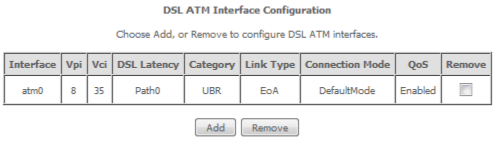
NOTE 2: If you lose all access to your web user interface, simply press the reset button on the rear panel for 5-7 seconds to restore default settings.

Advanced

Advanced

ATM interface

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



DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

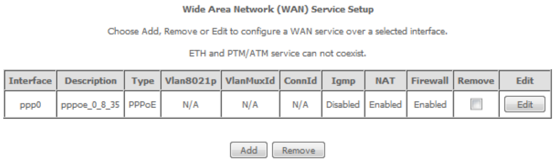
Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
atm0	8	35	Path0	UBR	EoA	DefaultMode	Enabled	□

OPTIONS	Description
Interface	Shows the Interface Name
Vpi	Shows the value of Vpi
Vci	Shows the value of Vci
DSL Latency	The value of the DSL latency
Category	Shows the ATM service classes
Link Type	Shows the type of the Link
Connection Mode	Shows the selected mode of connection
QoS	Shows the status of the QoS function
Remove	Select to remove ATM interface configuration

WAN service

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

You can then add a new PVC or edit an existing entry.



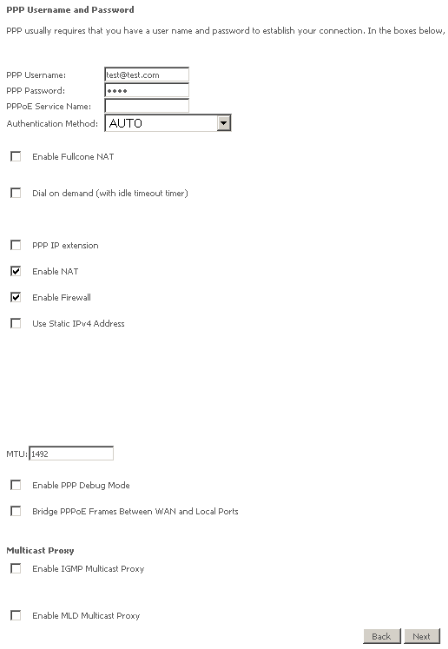
Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

ETH and PTM/ATM service can not coexist.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove	Edit
ppp0	pppoe_0_8_35	PPPoE	N/A	N/A	N/A	Disabled	Enabled	Enabled	□	Edit

OPTIONS	Description
Interface	The interface the configured PVC uses.
Description	The name given to the selected PVC
Type	The type of connection the selected PVC utilizes
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	Shows whether IGMP multicast traffic is enabled or disabled for the selected PVC..
NAT	Shows whether Network Address Translation is enabled or disabled for the selected PVC.
Firewall	Shows whether the inbuilt firewall is enabled or disabled for the selected PVC.



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided you.

PPP Username: test@test.com
PPP Password: ••••
PPPoE Service Name:
Authentication Method: AUTO

□ Enable Fullcone NAT

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

☑ Enable NAT

☑ Enable Firewall

□ Use Static IPv4 Address

MTU: 1492

□ Enable PPP Debug Mode

□ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

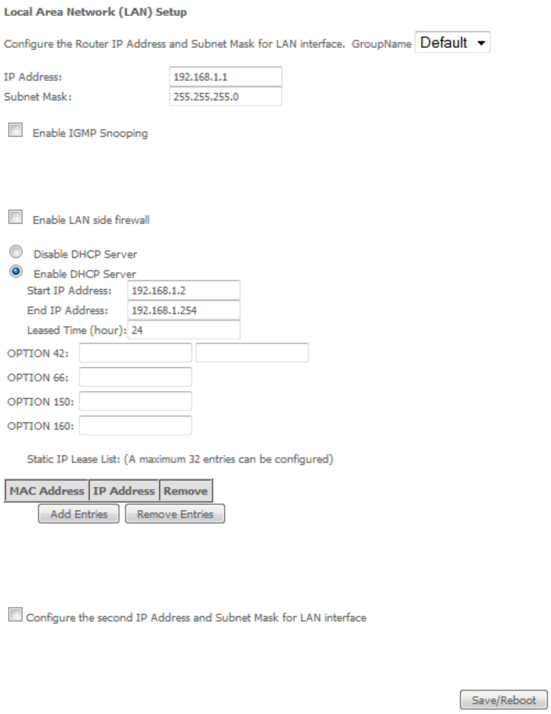
□ Enable IGMP Multicast Proxy

□ Enable MLD Multicast Proxy

OPTIONS	Description
PPP Username	The username supplied by your ISP
PPP Password	The password supplied by your ISP
PPPoE Service Name	A name you enter to identify the connection
Authentication Method	This is the type of authentication used for your connection. This would usually be left set to Auto.
Enable Fullcone NAT	Enable a 1 to 1 mapping of an IP address and port to an internal host.
Dial on Demand	Initiate an internet connection when traffic bound for the internet passes through the router.
PPP IP extension	Enable PPP IP extension for the connection. (if supported by your ISP)
Enable NAT	Enable Network Address Translation for the connection.
Enable Firewall	Enable the built-in firewall for the connection.
Use static IPv4 address	Use a static IP address (as supplied by your ISP) for the connection.
MTU	Set the MTU (Maximum Transmit Unit) size. This should be left at 1492 for a PPPoE connection.
Enable PPP debug mode	Enable extended PPP logging for the connection.
Bridge PPPoE Frames between WAN and Local ports	You use this to configure your PPPoE connection from a LAN connected host instead of the Router.
Enable IGMP Multicast Proxy	You can use this to enable IGMP multicast support on the connection.
Enable MLD Multicast Proxy	Enable IPv6 multicast support on the conneciton.

LAN

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



Local Area Network (LAN) Setup

Configure the Router IP Address and Subnet Mask for LAN interface. GroupName Default

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

□ Enable IGMP Snooping

□ Enable LAN side firewall

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Leased Time (hour): 24
OPTION 42:
OPTION 66:
OPTION 150:
OPTION 160:

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove

□ Configure the second IP Address and Subnet Mask for LAN interface

See the field descriptions below for more details.

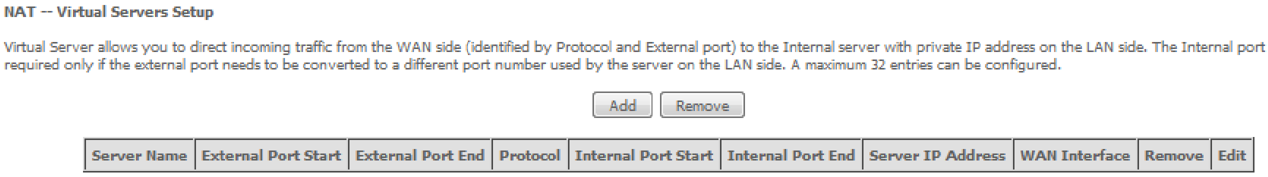
OPTIONS	Description
IP Address	Enter the IP address for the LAN interface
Subnet Mask	Enter the subnet mask for the LAN interface
Enable IGMP Snooping	Enable by ticking the box Standard Mode: In standard mode, multicast traffic will broadcast to all bridge ports when no client subscribes to a multicast 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	Check box to enable Firewall on LAN
Disable DHCP Server	Disables the DHCP server. Only to be done if Static IP address is set up
Enable DHCP Server	Select Enable DHCP server and enter your starting and ending IP addresses and the lease time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every DHCP client on your LAN
Enable DHCP Server Relay	To relay DHCP requests from the subnet with no DHCP server on it to a DHCP server on other subnets. DHCP Server Relay is disabled by default. To enable DHCP relay, please disable NAT first, and then press save button.
Configure the second IP Address and Subnet Mask for LAN Interface	Configure a second IP address by ticking the checkbox shown below and enter the following information: Enter the secondary IP address for the LAN interface. Enter the secondary subnet mask for the LAN interface.

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.

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.

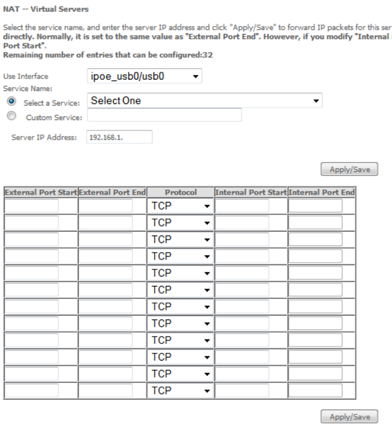


NAT -- Virtual Servers Setup

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

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove	Edit

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



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".**

Remaining number of entries that can be configured:32

Use Interface: ipoe_usb0/usb0

Service Name:

● Select a Service: Select One

○ Custom Service:

Server IP Address: 192.168.1.

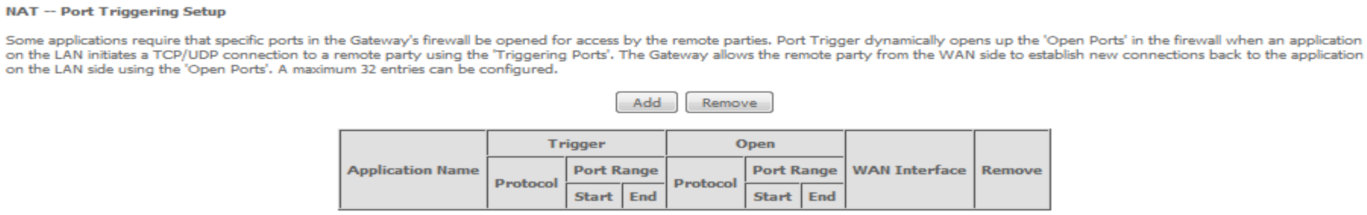
External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

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

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.

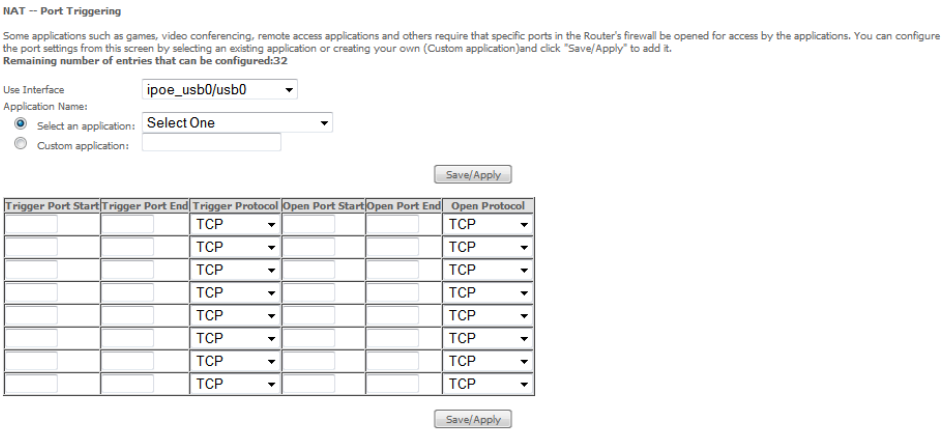


NAT -- Port Triggering Setup

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

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		

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



NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application)and click "Save/Apply" to add it.
Remaining number of entries that can be configured:32

Use Interface: ipoe_usb0/usb0
Application Name:
● Select an application: Select One
○ Custom application:

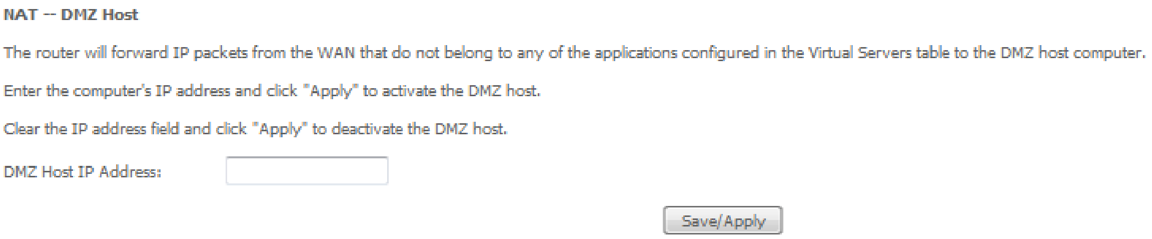
Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

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

DMZ Host

Your Router will forward IP packets from the Wireless Area Network (WAN) that do 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. Clear the IP address field and click Apply to deactivate the DMZ host.



NAT -- DMZ Host

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

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

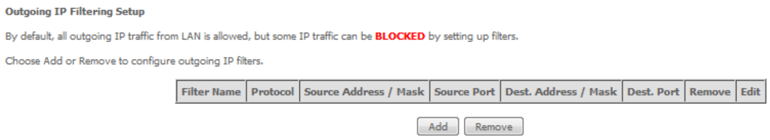
Security

IP Filtering

The IP Filtering screen 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.



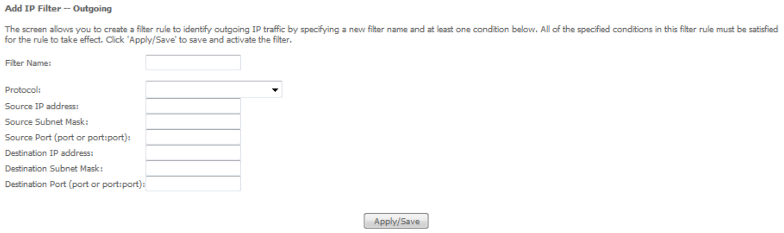
Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove	Edit

To add a filtering rule, click the Add button. The following screen will display.



Add IP Filter -- Outgoing

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

Filter Name:

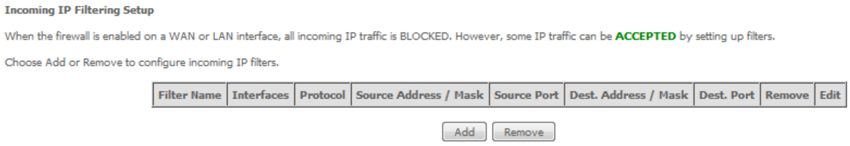
Protocol:
Source IP address:
Source Subnet Mask:
Source Port (port or port:port):
Destination IP address:
Destination Subnet Mask:
Destination Port (port or port:port):

FILTER NAME	THE FILTER RULE LABEL
Protocol	TCP, TCP/UDP, UDP or ICMP Source IP address
Source IP address	Enter source IP address Source Subnet Mask
Source Subnet Mask	Enter source subnet mask
Source Port (port or port:port)	Enter source port number or port range
Destination IP address	Enter destination IP address
Destination Subnet Mask	Destination Subnet Mask
Destination port (port or port:port)	Enter destination port number or range

Click Apply/Save to save and activate the filter.

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.



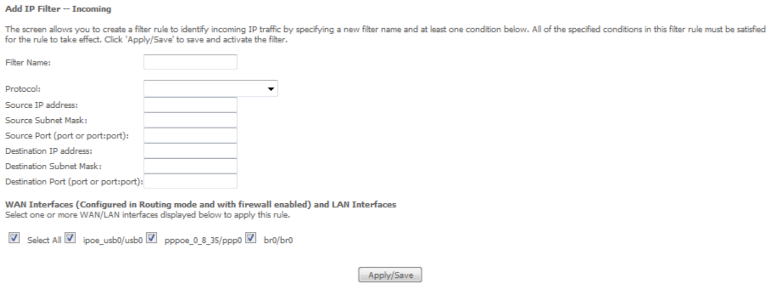
Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove	Edit

To add a filtering rule, click the Add button. The following screen will display.



Add IP Filter -- Incoming

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

Filter Name:

Protocol:
Source IP address:
Source Subnet Mask:
Source Port (port or port:port):
Destination IP address:
Destination Subnet Mask:
Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
Select one or more WAN/LAN interfaces displayed below to apply this rule.

☑ Select All ☑ ipoe_usb0/usb0 ☑ pppoe_0_8_35/ppp0 ☑ br0/br0

Please refer to the Outgoing IP Filter table for field descriptions.

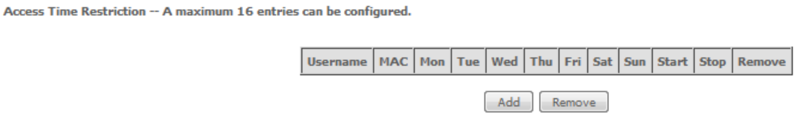
Click Apply/Save to save and activate the filter.

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

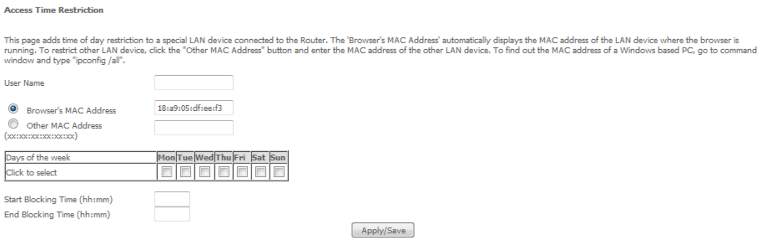
This Parental Control allows you to restrict access from a Local Area Network (LAN) connected device to an outside network through the Router on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section 6.3 SNTP, so that the scheduled times match your local time.



Access Time Restriction -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove

Click Add to display the following screen.



Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

● Browser's MAC Address 18:a9:05:df:ee:f3

○ Other MAC Address
(xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	□	□	□	□	□	□	□

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

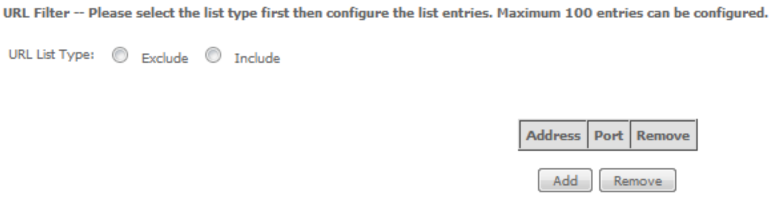
See instructions below and click Apply/Save to apply the settings.

OPTIONS	Description
User Name	A user-defined label for this restriction
Browser's MAC Address	MAC address of the PC running the browser
Other MAC Address	MAC address of another LAN device
Days of the week	The days the restrictions apply
Start Blocking Time	The time the restrictions start
End Blocking Time	The time the restrictions end

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 3G29WN.

Simply check To block or To allow and then click Add to enter the URL you wish added to a list

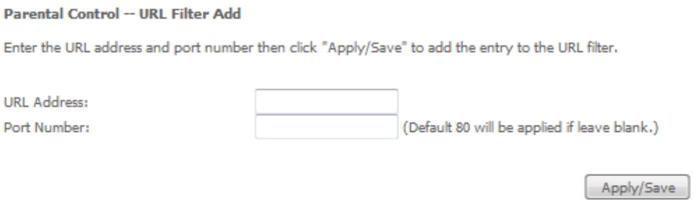


URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: ○ Exclude ○ Include

Address	Port	Remove

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 Apply/Save.



Parental Control -- URL Filter Add

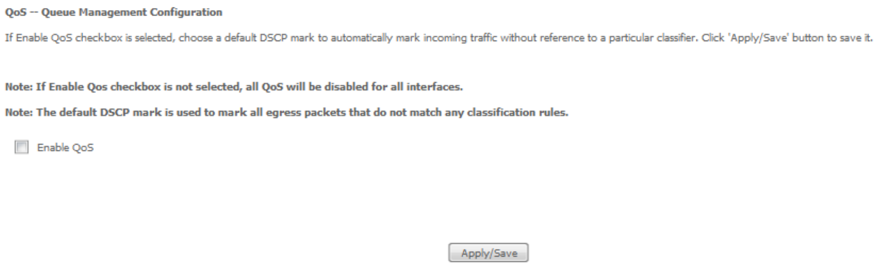
Enter the URL address and port number then click "Apply/Save" to add the entry to the URL filter.

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

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 big file, the download won't disrupt the flow of video data.



QoS -- Queue Management Configuration

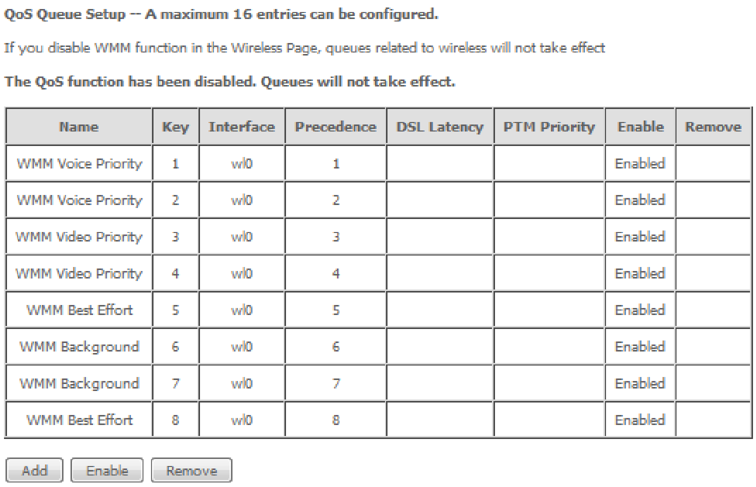
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

□ Enable QoS

Queue Setup



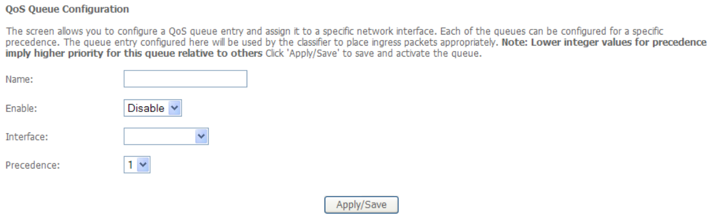
QoS Queue Setup -- A maximum 16 entries can be configured.

If you disable WMM function in the Wireless Page, queues related to wireless will not take effect

The QoS function has been disabled. Queues will not take effect.

Name	Key	Interface	Precedence	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	1			Enabled	
WMM Voice Priority	2	wl0	2			Enabled	
WMM Video Priority	3	wl0	3			Enabled	
WMM Video Priority	4	wl0	4			Enabled	
WMM Best Effort	5	wl0	5			Enabled	
WMM Background	6	wl0	6			Enabled	
WMM Background	7	wl0	7			Enabled	
WMM Best Effort	8	wl0	8			Enabled	

Click Add to display the following screen



QoS Queue Configuration

The 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: Lower integer values for precedence imply higher priority for this queue relative to others** Click 'Apply/Save' to save and activate the queue.

Name:

Enable: Disable

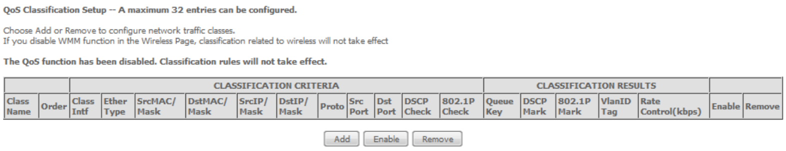
Interface:

Precedence: 1

This 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



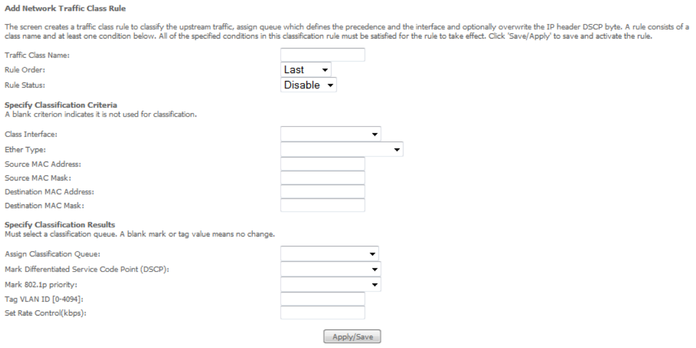
QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.
If you disable WMM function in the Wireless Page, classification related to wireless will not take effect

The QoS function has been disabled. Classification rules will not take effect.

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS						
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ Mask	DstIP/ Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Control(kbps)	Enable	Remove

Click Add to configure network traffic classes.



Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

Traffic Class Name:
Rule Order: Last
Rule Status: Disable

Specify Classification Criteria
A blank criterion indicates it is not used for classification.

Class Interface:
Ether Type:
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:

Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:
Mark Differentiated Service Code Point (DSCP):
Mark 802.1p priority:
Tag VLAN ID [0-4094]:
Set Rate Control(kbps):

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

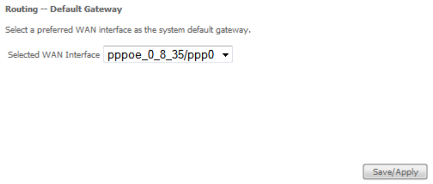
Click Save/Apply to save and activate the rule.

Routing

Default Gateway, Static Route, Policy Routing and Dynamic Route settings can be found in the Routing link.

Default gateway

Select your preferred WAN interface from the drop down box.



Routing -- Default Gateway

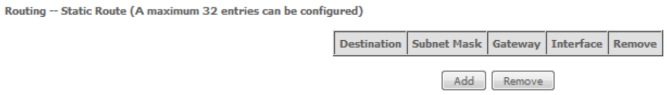
Select a preferred WAN interface as the system default gateway.

Selected WAN Interface pppoe_0_8_35/ppp0

Static route

The Static Route screen displays the configured static routes.

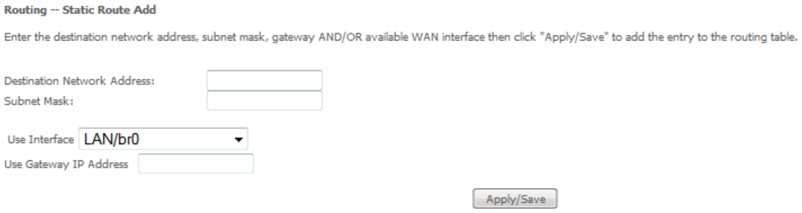
Click the Add or Remove buttons to change settings.



Routing -- Static Route (A maximum 32 entries can be configured)

Destination	Subnet Mask	Gateway	Interface	Remove

Click the Add button to display the following screen.



Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

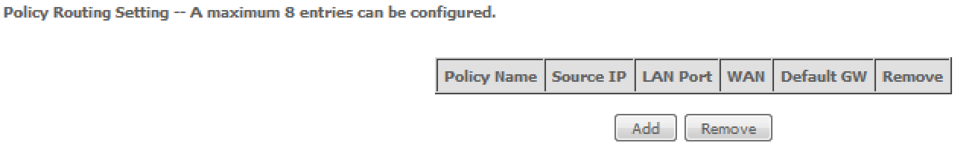
Destination Network Address:
Subnet Mask:

Use Interface LAN/br0
Use Gateway IP Address

Enter 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

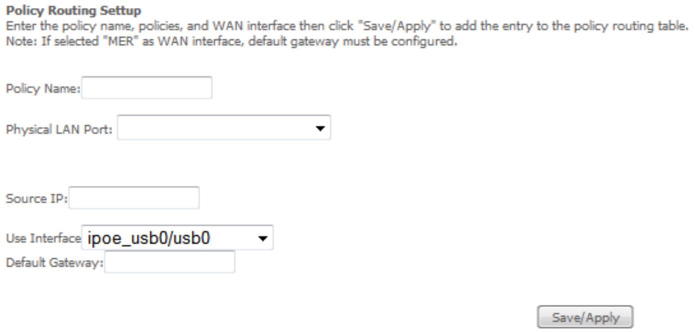
Allows you to add policy rules to certain situations



Policy Routing Setting -- A maximum 8 entries can be configured.

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove

Click Add to display the following screen



Policy Routing Settup

Enter the policy name, policies, and WAN interface then click "Save/Apply" to add the entry to the policy routing table.

Note: If selected "MER" as WAN interface, default gateway must be configured.

Policy Name:

Physical LAN Port:

Source IP:

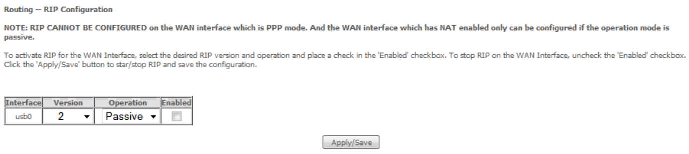
Use Interface: ipoe_usb0/usb0

Default Gateway:

Dynamic Route

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, followed by placing a check in the Enabled checkbox for that interface. Click Apply/Save to save the configuration and to start or stop dynamic routing.



Routing -- RIP Configuration

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which is PPP mode. And the WAN interface which has NAT enabled only can be configured if the operation mode is passive.

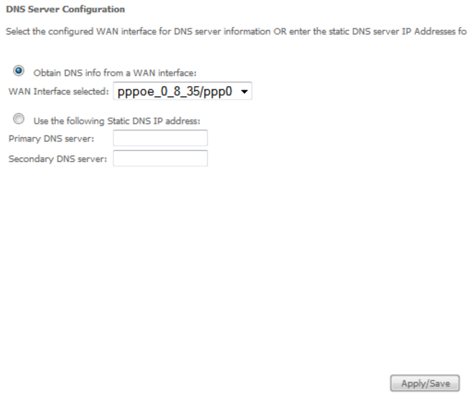
To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
usb0	2	Passive	□

DNS

9.9.1 DNS server

This page allows user to enable automatic DNS from the ISP or specify their own DNS server address manually.



DNS Server Configuration

Select the configured WAN interface for DNS server information OR enter the static DNS server IP Addresses for single PVC with IPoA, static IPoE protocol.

● Obtain DNS info from a WAN interface:

WAN Interface selected: pppoe_0_8_35/ppp0

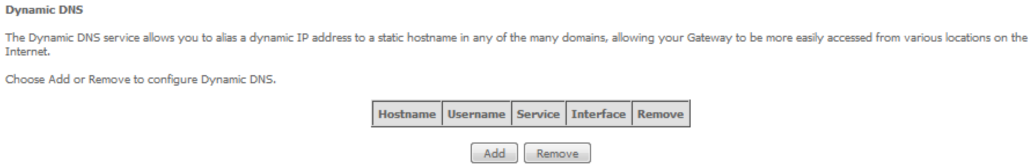
○ Use the following Static DNS IP address:

Primary DNS server:

Secondary 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.



Dynamic DNS

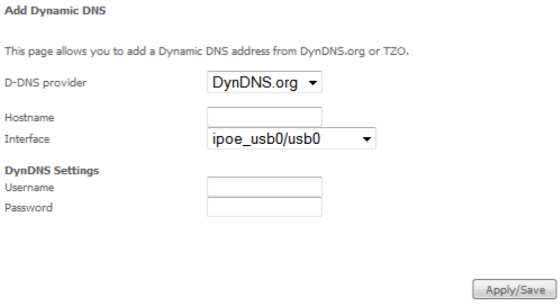
The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Gateway to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

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 this screen will display.



Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider: DynDNS.org

Hostname:

Interface: ipoe_usb0/usb0

DynDNS Settings

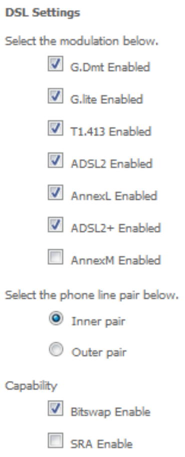
Username:

Password:

NAME	DESCRIPTION
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name for the dynamic DNS server
Interface	Select the interface from the list
Username	Enter the username for the dynamic DNS server
Password	Enter the password for the dynamic DNS server

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.



DSL Settings

Select the modulation below.

☑ G.Dmt Enabled

☑ G.lite Enabled

☑ T1.413 Enabled

☑ ADSL2 Enabled

☑ AnnexL Enabled

☑ ADSL2+ Enabled

□ AnnexM Enabled

Select the phone line pair below.

● Inner pair

○ Outer pair

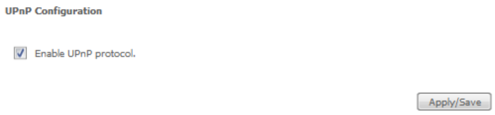
Capability

☑ Bitswap Enable

□ SRA Enable

UPnP

Simply check or uncheck the box and press Apply/Save to enable or disable the UPnP protocol

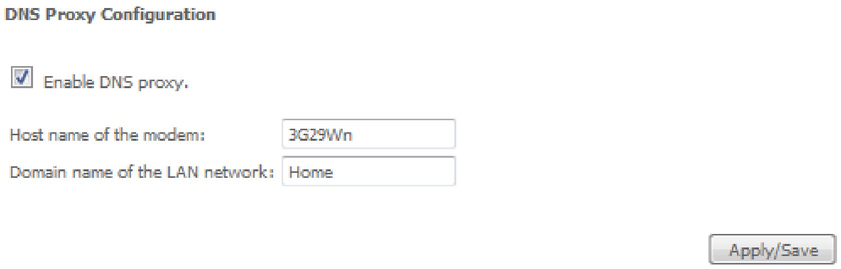


UPnP Configuration

☑ Enable UPnP protocol.

DNS proxy

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



DNS Proxy Configuration

☑ Enable DNS proxy.

Host name of the modem: 3G29Wn

Domain name of the LAN network: Home

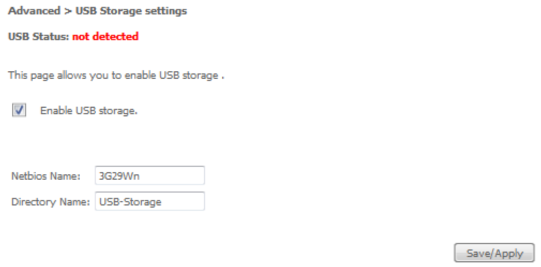
The Host Name and Domain name are combined to form a unique label that is mapped to the router IP address. This can be used to access the WebUI with a local name rather than by using the router IP address.

Status

USB Storage

This page allows you to enable/disable the USB port of the 3G29Wn to 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.



Advanced > USB Storage settings

USB Status: not detected

This page allows you to enable USB storage .

☑ Enable USB storage.

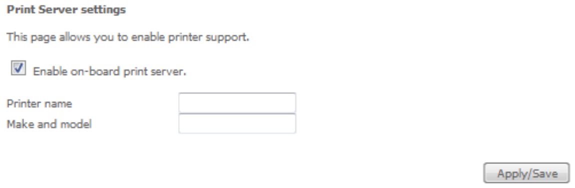
Netbios Name: 3G29Wn

Directory Name: USB-Storage

Print Server

This page allows you to enable/disable the USB port of the 3G29Wn 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



Print Server settings

This page allows you to enable printer support.

☑ Enable on-board print server.

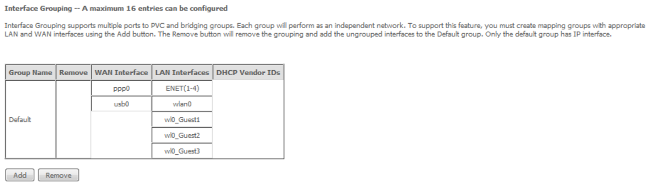
Printer name

Make and model

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.

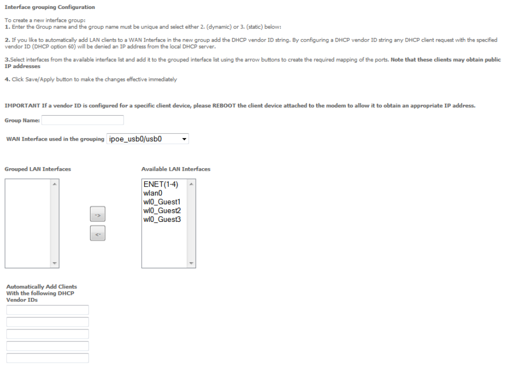


Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0	ENET(1-4)	
		usb0	wlan0	
			wl0_Guest1	
			wl0_Guest2	
			wl0_Guest3	

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:



Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:

2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

3.Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**

4. Click Save/Apply button to make the changes effective immediately

IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

WAN Interface used in the grouping ipoe_usb0/usb0

Grouped LAN Interfaces

Available LAN Interfaces

ENET(1-4)
wlan0
wl0_Guest1
wl0_Guest2
wl0_Guest3

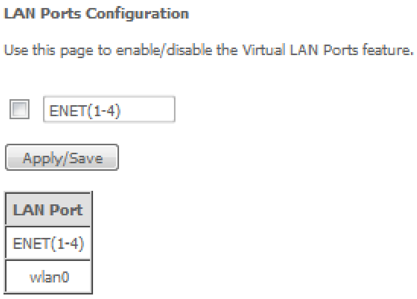
Automatically Add Clients With the following DHCP Vendor IDs

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/disable the Virtual LAN Ports feature



LAN Ports Configuration

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

□ ENET(1-4)

LAN Port
ENET(1-4)
wlan0

Status

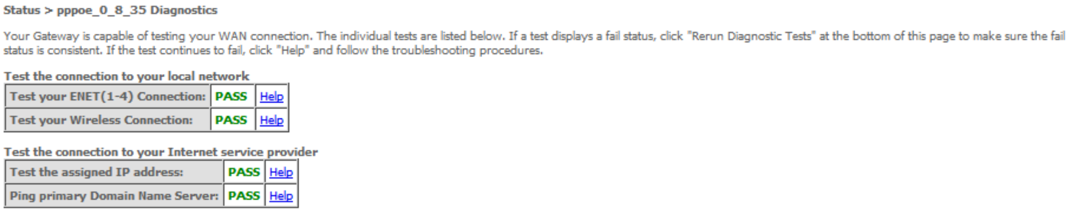
The Status menu has the following submenus:

- 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, follow the troubleshooting procedures in the Help screen.
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.



Status > pppoe_0_8_35 Diagnostics

Your Gateway is capable of testing your WAN connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your ENET(1-4) Connection:	PASS	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your Internet service provider

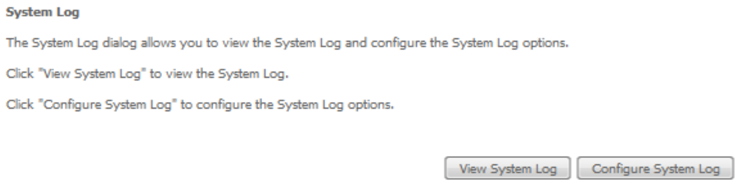
Test the assigned IP address:	PASS	Help
Ping primary Domain Name Server:	PASS	Help

OPTIONS	Description
ENET Connection	Pass: Indicates that the Ethernet interface from your computer is connected to the LAN port of this Router.
	Fail: Indicates that the Router does not detect the Ethernet interface on your computer.
Test your Wireless Connection	Pass: Indicates that the wireless card is ON.
	Down: Indicates that the wireless card is OFF.
Test the assigned IP Address	Pass: Indicates that the modem has received a valid IP (Internet Protocol) address from the PPP server.
	Fail: Indicates that the modem does not have a valid IP address from the PPP server.
Ping Primary Domain Name Server	Pass: Indicates that the Router can communicate with the primary Domain Name Server (DNS).
	Fail: Indicates that the Router was unable to communicate with the primary Domain Name Server (DNS). It may not have an effect on your Internet connectivity. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.

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.



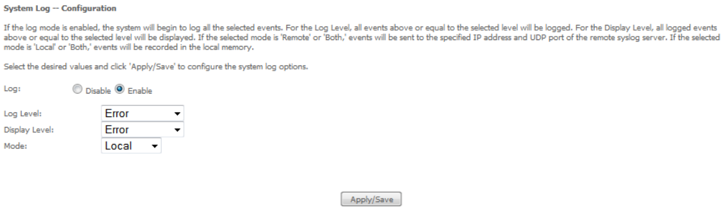
System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

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



System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: ○ Disable ● Enable

Log Level: Error

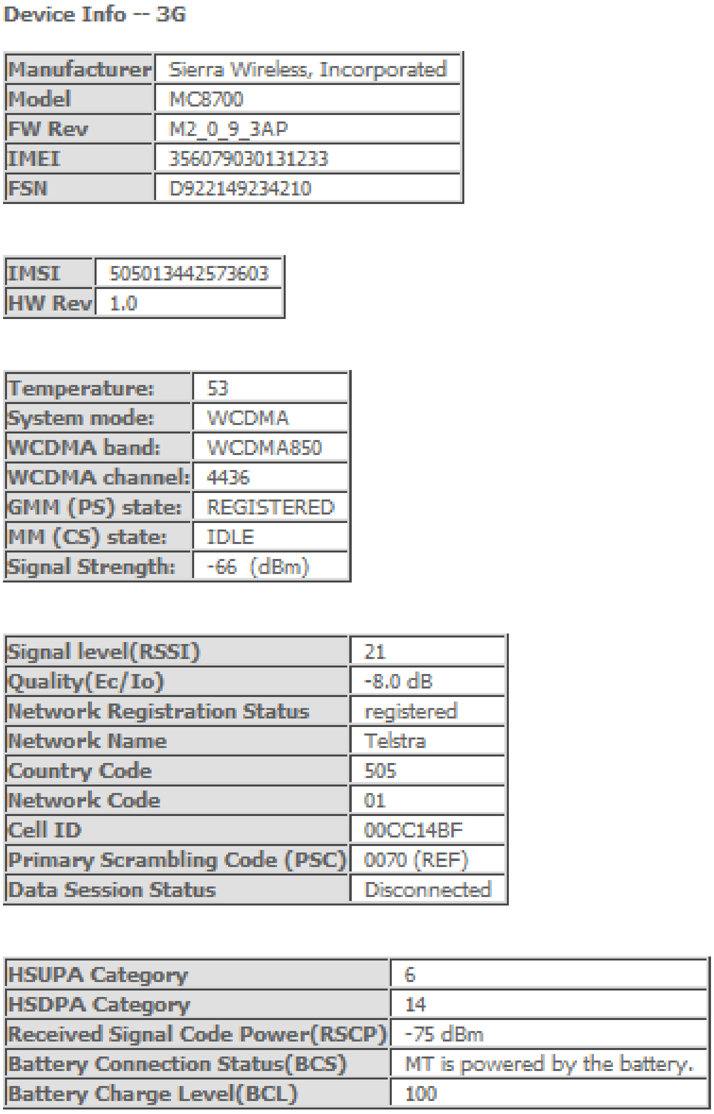
Display Level: Error

Mode: Local

OPTIONS	Description
Log	Indicates whether the system is currently recording events. You can enable or disable event logging. By default, it is disabled.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the Router's SDRAM. When the log buffer is full, the newest event will wrap up to the top of the log buffer and overwrite the oldest 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 level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display	Allows you to select the logged events and displays on the View System Log window for events of this level and above to the highest Emergency level.
Level	Allows you to select the logged events and displays on the View System Log window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, be sent to a remote syslog server, or to both simultaneously. If remote mode is selected, the view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the WEB UI will prompt the you to enter the Server IP address and Server UDP port.

3G Network

Select this option for detailed status information on your Routers 3G connection.



Device Info -- 3G

Manufacturer	Sierra Wireless, Incorporated
Model	MC8700
FW Rev	M2_0_9_3AP
IMEI	356079030131233
FSN	D922149234210

IMSI	505013442573603
HW Rev	1.0

Temperature:	53
System mode:	WCDMA
WCDMA band:	WCDMA850
WCDMA channel:	4436
GMM (PS) state:	REGISTERED
MM (CS) state:	IDLE
Signal Strength:	-66 (dBm)

Signal level(RSSI)	21
Quality(Ec/Io)	-8.0 dB
Network Registration Status	registered
Network Name	Telstra
Country Code	505
Network Code	01
Cell ID	00CC14BF
Primary Scrambling Code (PSC)	0070 (REF)
Data Session Status	Disconnected

HSUPA Category	6
HSDPA Category	14
Received Signal Code Power(RSCP)	-75 dBm
Battery Connection Status(BCS)	MT is powered by the battery.
Battery Charge Level(BCL)	100

Consult the table on the next page for detailed field descriptions.

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.
FSN	Factory Serial Number of the 3G module.
IMSI	The IMSI (International Mobile Subscriber Identity) is a unique 15-digit number used to identify an individual user on a GSM or UMTS network.
HW Rev.	The hardware version of the 3G module.
Temperature	The temperature of the 3G module in degrees Celsius.
System Mode	WCDMA/Europe
CDMA 2000 / America	
WCDMA band	The 3G radio frequency band which supports tri-band UTMS/HSDPA/HSUPA frequencies (850/1900/2100 MHz), IMT2000 is 2100 MHz, WCDMA800 is 850 MHz, WCDMA1900 is 1900 MHz.
GSM band	The 2G radio frequency band which supports Quad-band GSM/GRPS frequencies, including GSM850, GSM900, DCS1800, PCS1900 with each number representing the respective frequency in MHz.
WCDMA channel	The 3G channel.
GSM channel	The 2G channel.
GSM (PS) state	Packet Switching state
MM (CS) state	Circuit Switching state
Signal Strength	The 3G/2G service signal strength in dBm.

OPTIONS	Description
Signal Level (RSSI)	3G Radio Signal Strength Index
Quality (Ec/Io)	The total energy per chip per power density (Ec/Io) value of the active set's three strongest cells.
Network Registration Status	Should display as registered with a valid unlocked SIM card.
Network Name	The 3G internet Service Provider.
Country & Network Codes	Each country and network has a unique code.
Cell ID	The network information for the "serving" cell ID.
Primary Scrambling Code (PSC)	The PSC of the reference WCDMA cell
Data Session Status	Connected or Disconnected
HSUPA/HSDPA Categories	The HSUPA/HSDPA categories correspond to different data transmission rates with higher numbers generally indicating faster rates
Received Signal Code Power (RSCP)	The RSCP of the active set's three strongest cells
Battery Connection Status (BCS)	BCS of the MT (Mobile Termination)
Battery Charge Level (BCL)	BCL of the MT (Mobile Termination)

Statistics

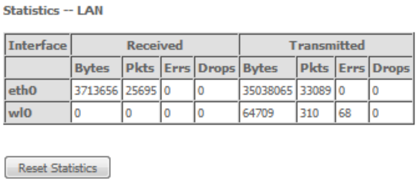
These screens provide detailed information for:

- 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



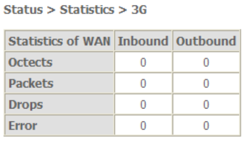
Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	3713656	25695	0	0	35038065	33089	0	0
wl0	0	0	0	0	64709	310	68	0

INTERFACE	SHOWS CONNECTION INTERFACES	
Received/Transmitted	Bytes	Rx/TX (receive/transmit) packet in bytes
	Pkts	Rx/TX (receive/transmit) packets
	Errs	Rx/TX (receive/transmit) packets with errors
	Drops	Rx/TX (receive/transmit) packets dropped

3G Network

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

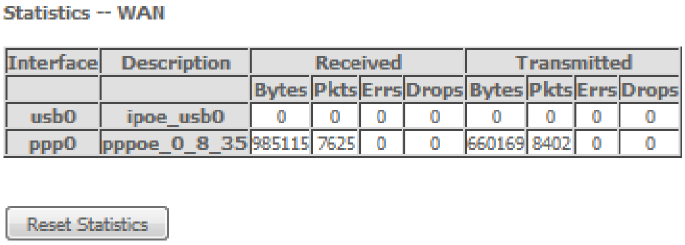


Status > Statistics > 3G

Statistics of WAN	Inbound	Outbound
Octects	0	0
Packets	0	0
Drops	0	0
Error	0	0

WAN

This screen displays statistics for the Ethernet and Wireless LAN interfaces

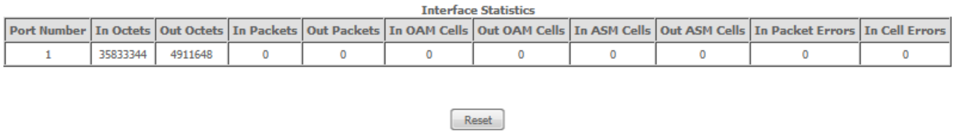


Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
usb0	ipoe_usb0	0	0	0	0	0	0	0	0
ppp0	pppoe_0_8_35	985115	7625	0	0	660169	8402	0	0

INTERFACE	SHOWS CONNECTION INTERFACES	
Received/Transmitted	Bytes	Rx/TX (receive/transmit) packet in bytes
	Pkts	Rx/TX (receive/transmit) packets
	Errs	Rx/TX (receive/transmit) packets with errors
	Drops	Rx/TX (receive/transmit) packets dropped

ATM



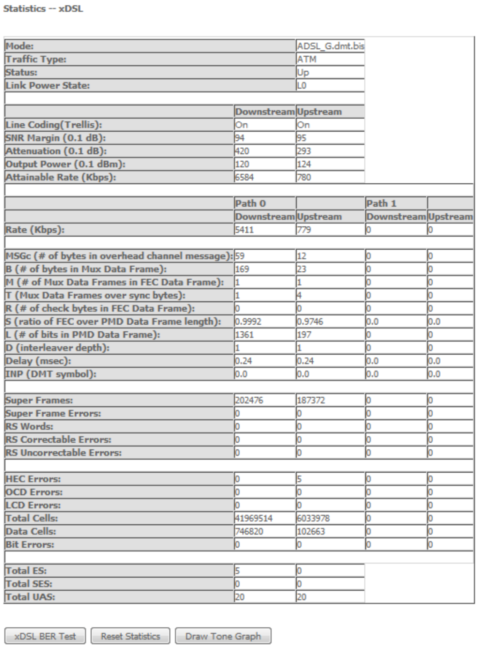
Interface Statistics

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
1	35833344	4911648	0	0	0	0	0	0	0	0

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

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.



Statistics -- xDSL

Mode:	ADSL_G.dmt.bis
Traffic Type:	ATM
Status:	Up
Link Power State:	L0

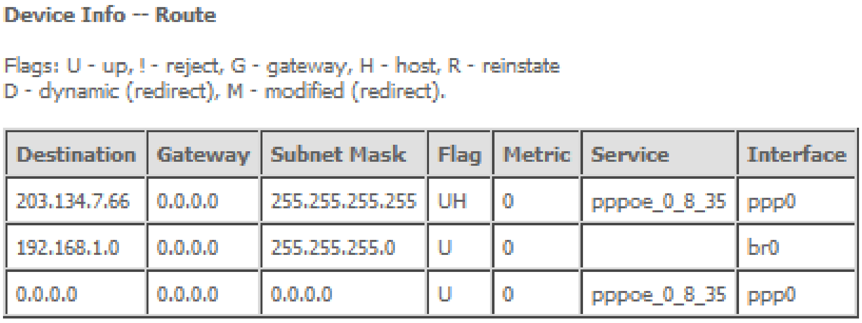
	Downstream	Upstream
Line Coding(Trellis):	On	On
SNR Margin (0.1 dB):	94	95
Attenuation (0.1 dB):	420	293
Output Power (0.1 dBm):	120	124
Attainable Rate (Kbps):	6584	780

	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	5411	779	0	0
MSGc (# of bytes in overhead channel message):	59	12	0	0
B (# of bytes in Mux Data Frame):	169	23	0	0
M (# of Mux Data Frames in FEC Data Frame):	1	1	0	0
T (Mux Data Frames over sync bytes):	1	4	0	0
R (# of check bytes in FEC Data Frame):	0	0	0	0
S (ratio of FEC over PMD Data Frame length):	0.9992	0.9746	0.0	0.0
L (# of bits in PMD Data Frame):	1361	197	0	0
D (interleaver depth):	1	1	0	0
Delay (msec):	0.24	0.24	0.0	0.0
INP (DMT symbol):	0.0	0.0	0.0	0.0
Super Frames:	202476	187372	0	0
Super Frame Errors:	0	0	0	0
RS Words:	0	0	0	0
RS Correctable Errors:	0	0	0	0
RS Uncorrectable Errors:	0	0	0	0
HEC Errors:	0	5	0	0
OCD Errors:	0	0	0	0
LCD Errors:	0	0	0	0
Total Cells:	41969514	6033978	0	0
Data Cells:	746820	102663	0	0
Bit Errors:	0	0	0	0

Total ES:	5	0
Total SES:	0	0
Total UAS:	20	20

Route

Select Route to display the paths the Router has found.



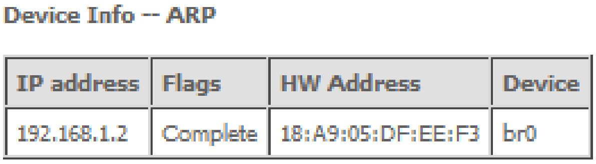
Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
203.134.7.66	0.0.0.0	255.255.255.255	UH	0	pppoe_0_8_35	ppp0
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	0.0.0.0	0.0.0.0	U	0	pppoe_0_8_35	ppp0

ARP

Click ARP to display the ARP information.



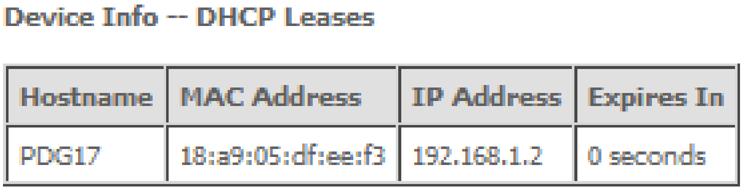
Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.2	Complete	18:A9:05:DF:EE:F3	br0

You can use this 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.

DHCP

Click DHCP to display the DHCP information.

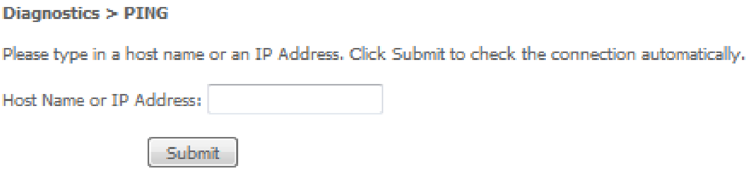


Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
PDG17	18:a9:05:df:ee:f3	192.168.1.2	0 seconds

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

Ping



Diagnostics > PING

Please type in a host name or an IP Address. Click Submit to check the connection automatically.

Host Name or IP Address:

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

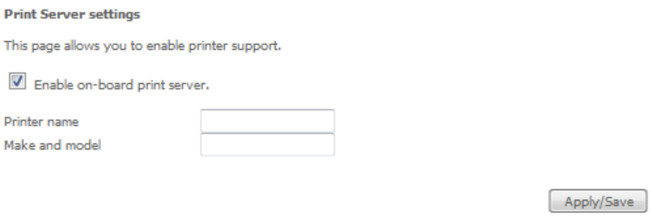
Appendix A: Print Server

These steps explain the procedure for enabling the Print Server.

1. Enable Print Server from the Advanced menu in the Web User Interface.

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

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



Print Server settings

This page allows you to enable printer support.

☑ Enable on-board print server.

Printer name

Make and model

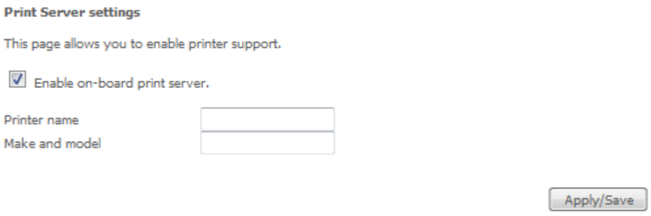
For Windows Vista/7

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 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.



Print Server settings

This page allows you to enable printer support.

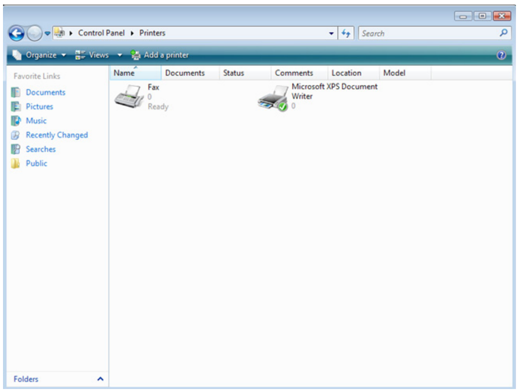
☑ Enable on-board print server.

Printer name

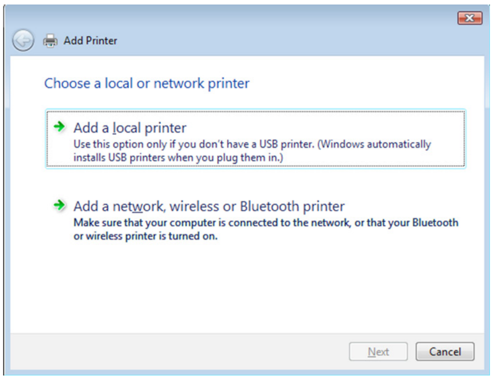
Make and model

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.

Once in the ‘Printers’ page, click the ‘Add a printer’ button as shown below.



3. Select ‘Add a network, wireless or bluetooth printer’.



Add Printer

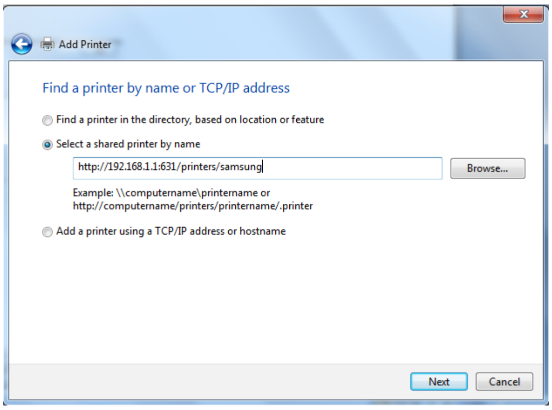
Choose a local or network printer

Add a local printer
Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)

Add a network, wireless or Bluetooth printer
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

4. Click on the radio-button labelled ‘Select a shared printer by name’, and type “http://192.168.1.1:631/printers/samsung” in the box below. Click ‘Next’.

NOTE: The PrinterName must be the same as the printer name entered into the Printer section of 3G29WN.



Find a printer by name or TCP/IP address

○ Find a printer in the directory, based on location or feature

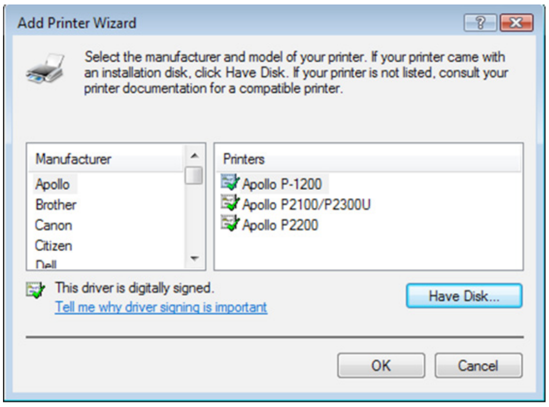
● Select a shared printer by name

http://192.168.1.1:631/printers/samsung

Example: \\computername\printername or
http://computername/printers/printername/.printer

○ Add a printer using a TCP/IP address or hostname

5. 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.

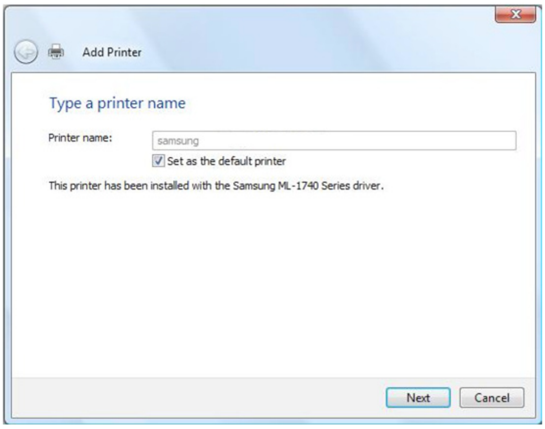


Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturer	Printers
Apollo	Apollo P-1200
Brother	Apollo P2100/P2300U
Canon	Apollo P2200
Citizen	
Dell	

This driver is digitally signed.
Tell me why driver signing is important

6. Choose whether you want this printer to be the default printer, and then click ‘Next’.



Type a printer name

Printer name: samsung

☑ Set as the default printer

This printer has been installed with the Samsung ML-1740 Series driver.

7. Click ‘Finish’. Your device is now configured and ready for use.

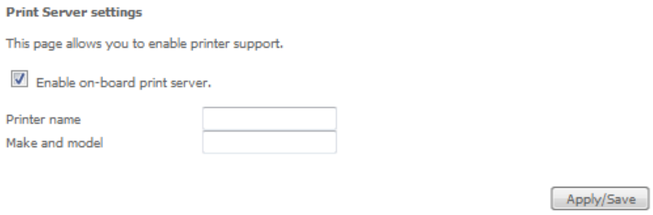
For MAC OSX

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

- Enable Print Server from Web User Interface.

Select Enable on-board print server checkbox and enter Printer name and Maker 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.



Print Server settings

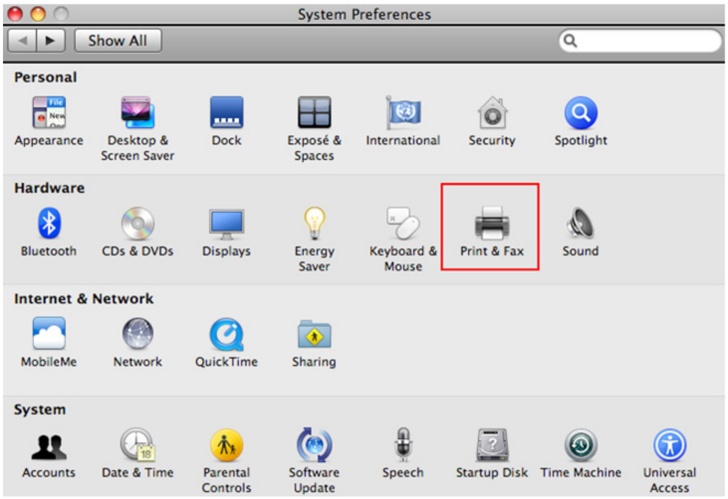
This page allows you to enable printer support.

☑ Enable on-board print server.

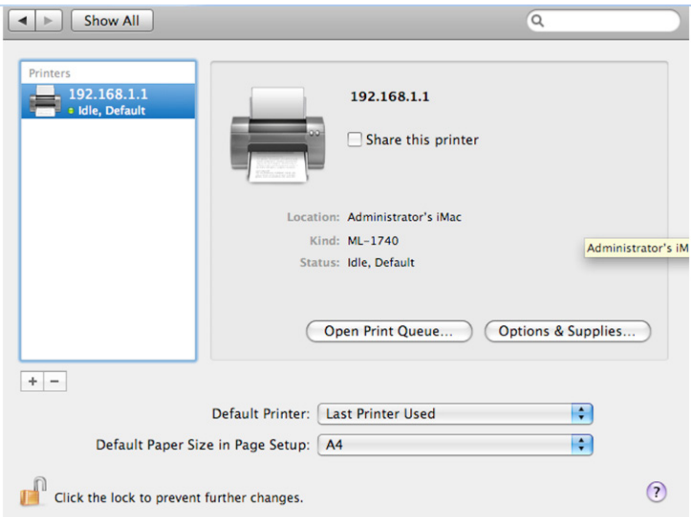
Printer name

Make and model

- To set up your printer, check the Apple menu, select System Preferences. In the System Preference menu click on the Print & Fax.



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



192.168.1.1
Idle, Default

192.168.1.1

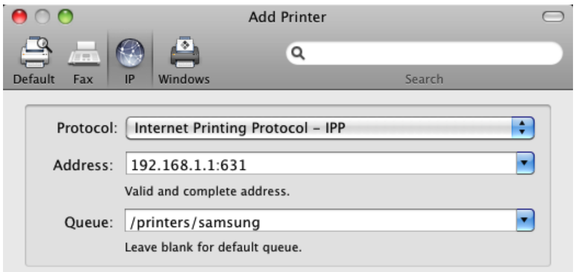
☐ Share this printer

Location: Administrator's iMac
Kind: ML-1740
Status: Idle, Default

Default Printer: Last Printer Used
Default Paper Size in Page Setup: A4

Click the lock to prevent further changes.

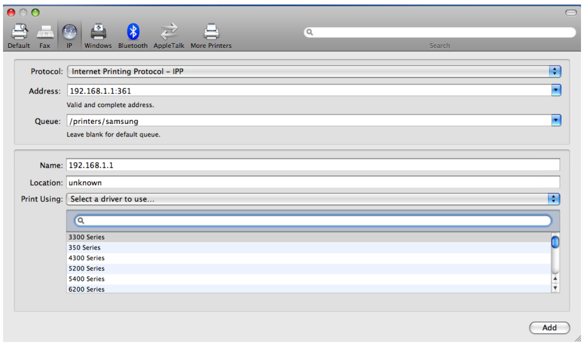
- Use the Protocol drop down list and select Internet Printing Protocol – IPP and enter "192.168.1.1:631" into the Address field and enter "/printers/PrinterName" into the Queue field.



Protocol: Internet Printing Protocol – IPP
Address: 192.168.1.1:631
Valid and complete address.
Queue: /printers/samsung
Leave blank for default queue.

NOTE: The PrinterName must be the same as the printer name entered into the Printer section of the 3G29WN.

- From the Print Using drop down list, select your corresponding printer driver.

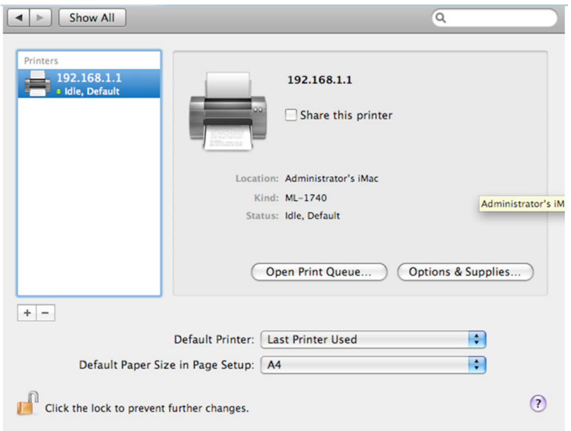


Protocol: Internet Printing Protocol – IPP
Address: 192.168.1.1:361
Valid and complete address.
Queue: /printers/samsung
Leave blank for default queue.

Name: 192.168.1.1
Location: unknown
Print Using: Select a driver to use...

3300 Series
350 Series
4300 Series
5200 Series
5400 Series
6200 Series

- Click Add and check the printer status.



192.168.1.1
Idle, Default

192.168.1.1

☐ Share this printer

Location: Administrator's iMac
Kind: ML-1740
Status: Idle, Default

Default Printer: Last Printer Used
Default Paper Size in Page Setup: A4

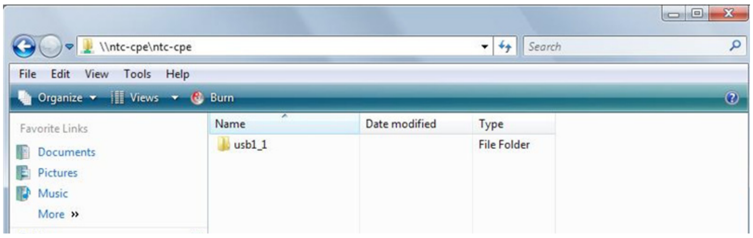
Click the lock to prevent further changes.

Appendix B: Samba Server

For Windows Vista/7

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

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



Name	Date modified	Type
usb1_1		File Folder

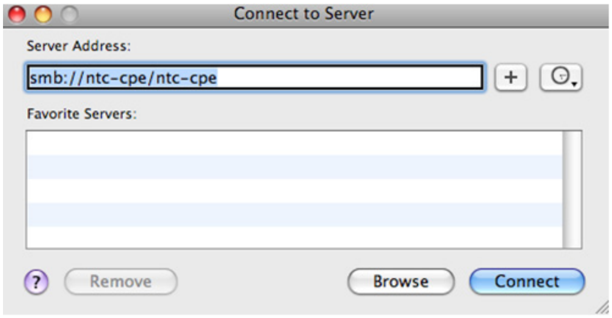
Note: There are no username and password required to access the USB drive, the user will be able to read/write the folder/files in the USB drive.

For MAC OSX

Click the finder icon in the Dock.

Choose Connect to Server from the Go menu.

In the address field of the Connect to Server dialog, type in the URL Smb:// “NetbiosName”/“DirectioryName”
(eg smb://ntc-cpe/ntc-cpe))



Server Address: smb://ntc-cpe/ntc-cpe

Select Connect to connect your USB driver.

Legal & Regulatory Information

NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product.

NetComm Limited reserves the right to change the specifications and operating details of this product without notice.

NetComm is a registered trademark of NetComm Limited.

All other trademarks are acknowledged the property of their respective owners.

Customer Information

ACA (Australian Communications Authority) requires you to be aware of the following information and warnings:

(1) This unit shall be connected to the Telecommunication Network through a line cord which meets the requirements of the ACA TS008 Standard.

(2) This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACA . These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:

- Change the direction or relocate the receiving antenna.
- Increase the separation between this equipment and the receiver.
- Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
- Consult an experienced radio/TV technician for help.

(3) The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

Product Warranty

The warranty is granted on the following conditions:

1. This warranty extends to the original purchaser (you) and is not transferable;
2. This warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. The customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting product to and from NetComm's nominated premises is your responsibility; and,
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.
6. The customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

GNU General Public License

This product includes software code that is subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). This code is subject to the copyrights of one or more authors and is distributed without any warranty. A copy of this software can be obtained by contacting NetComm Limited on +61 2 9424 2059.

The warranty is automatically voided if:

1. You, or someone else, use the product, or attempts to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitations of Warranty

The Trade Practices Act 1974 and corresponding State and Territory Fair Trading Acts or legalisation of another Government ("the relevant acts") in certain circumstances imply mandatory conditions and warranties which cannot be excluded. This warranty is in addition to and not in replacement for such conditions and warranties.

To the extent permitted by the Relevant Acts, in relation to your product and any other materials provided with the product ("the Goods") the liability of NetComm under the Relevant Acts is limited at the option of NetComm to:

- Replacement of the Goods; or
- Repair of the Goods; or
- Payment of the cost of replacing the Goods; or
- Payment of the cost of having the Goods repaired.

All NetComm ACN 002 490 486 products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option (refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at **www.netcomm.com.au**

NETCOMM LIMITED Head Office
PO Box 1200, Lane Cove NSW 2066 Australia
P: 02 9424 2070 **F:** 02 9424 2010
E: int.sales@netcomm.com.au
W: www.netcomm.com.au.

DYNALINK NZ 12c Tea Kea Place, Albany, Auckland,
New Zealand
P: 09 448 5548
F: 09 448 5549
E: sales@dynalink.co.nz
W: www.dynalink.co.nz

Product Warranty

NetComm products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option, via registering your product online at the NetComm website **www.netcomm.com**.au

Technical Support

If you have any technical difficulties with your product, please refer to the support section of our website.

www.netcomm.com.au/support

Note:NetComm Technical Support for this product only covers the basic installation and features outlined in the Quick Start Guide. For further information regarding the advanced features of this product, please refer to the configuring sections in the User Guide or contact a Network Specialist.