NETCOMM LIBERTY™ SERIES

3G WiFi Router

NetComm

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:

The purpose of this manual is to provide you with detailed information on the installation, operation and application of your 3G WiFi Router.

Important Notice and Safety Precaution

Before servicing or disassembling this equipment, always disconnect all power or telephone lines from the device.

- 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.
- Use an appropriate power supply, preferably the supplied power adapter, with an output of DC 12V 1.5A
- Do not operate the device near flammable gas or fumes. Turn off the device when you are near a petrol station, fuel depot or chemical plant/depot. Operation of such equipment in potentially explosive atmospheres can represent a safety hazard.
- The device and antenna shall be used only with a minimum of 20cm from human body.

The operation of this device may affect medical electronic devices, such as hearing aids and peacemakers

WARNING

- Disconnect the power line from the device before servicing.

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

With the increasing popularity of the 3G/UMTS standard worldwide, this 3G WiFi Router provides you with 3G/UMTS tri-band coverage through expanding cellular networks throughout the world.

Integrating a Sierra Wireless HSPA module, this router is capable of data downloads at high speeds of up to 7.2Mbps.

To protect your data from unwanted access this router also provides security features such as WiFi Protected Access (WPA) data encryption, a Firewall and Virtual Private Networks (VPN) pass through.

1.1 Features

- This 3G WiFi Router allows you to share your 3G connection with multiple wireless or wired devices.
- Global 3G/UMTS coverage through tri-band HSUPA/HSDPA/UMTS (850/1900/2100MHz), quad-band EDGE/GSM (850/900/1800/1900 MHz)
- Embedded multi-mode HSUPA/HSDPA/UMTS/EDGE/GPRS/GSM module
- Four Ethernet LAN 10/100 Mbps connections
- Integrated Wireless IEEE 802.11g/54Mbps access point (backward compatible with IEEE 802.11b)
- WiFi Protected Access (WPA) / WiFi Protected Access 2 (WPA2) and 802.1x wireless encryption
- Static route / Routing Information Protocol (RIP)/RIP v2 routing functions
- Media Access Control (MAC) address and IP filtering
- Network Address Translation (NAT) / Port Address Translation (PAT)
- Supports Virtual Private Network (VPN) Pass-Through
- Dynamic Host Configuration Protocol (DHCP) Server/Relay/Client
- Domain Name System (DNS) Proxy and Dynamic Domain Name System (DDNS)
- Web-based Management
- Command Line Interface (CLI) command interface via Telnet
- Configuration backup and restoration
- Remote configuration
- Router and 3G module firmware upgrade
- Supports Simple Network Management Protocol (SNMP)

1.2 Package Contents

Your package contains the following:

- 3G19W-AU - 3G WiFi Router
- Printed Quick Start Guide
- Ethernet Cable
- Wireless Security Card
- 2 x 3G Antennas (Removable)
- 1 x WiFi Antenna (Removable)
- Power Supply

1.3 LED Indicators

The front panel LED indicators are shown in this illustration and followed by detailed explanations in the table below.

NOTE: The six LEDs on the front panel display (Internet, 3G, 2G, Low, Med and High) will cycle on and off if PIN code protection is activated. In this case, you should consult section 4.3.1 PIN Code Protection for further instructions.

LED	COLOUR	MODE	DESCRIPTION
Power	Blue	On	Power On
		Off	Power Off
LAN 1-4	Blue	On	Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to an Ethernet connection)
		Off	No activity, router powered off, no cable or no powered device connected to the associated port.
		Flashing	LAN activity present (traffic in either direction)
WiFi	Blue	On	The wireless module is ready
		Off	The wireless module is not installed
		Flashing	WiFi activity present (traffic in either direction)
Internet	Blue	On	Internet connection established
		Off	No connection to the internet or router powered off
		Flashing	Data being transmitted through the internet connection
3G	Blue	On	Internet connection established
		Off	No connection with UMTS cellular station, no activity or router is powered off
		Flashing	Connecting with UMTS
2G	Blue	On	Internet connection established
		Off	No connection with EDGE, GPRS or GSM cellular station, no activity or router is powered off
		Flashing	Connecting to an EDGE, GPRS or GSM cellular station
Low	Blue	On	Low signal strength
		Off	No activity, router is powered off or higher signal strength found
Medium	Blue	On	Medium signal strength
		Off	No activity, router is powered off or a higher signal strength found
High	Blue	On	High signal strength
		Off	No activity, router is powered off, or a lower signal strength found

1.4 Rear Panel

The rear panel contains the ports for data and power connections.

- Main 3G Antenna (removable, SMA connection)
- Power jack for DC power input (12VDC / 1.5A)
- Power button
- USIM card slot
- Aux 3G Antenna
- WiFi Antenna
- Reset button
- 4 RJ-45 Ethernet Ports

Quick Setup

2. Quick Setup

2.1 Setup Procedure

These steps explain how to quickly setup your 3G Router:

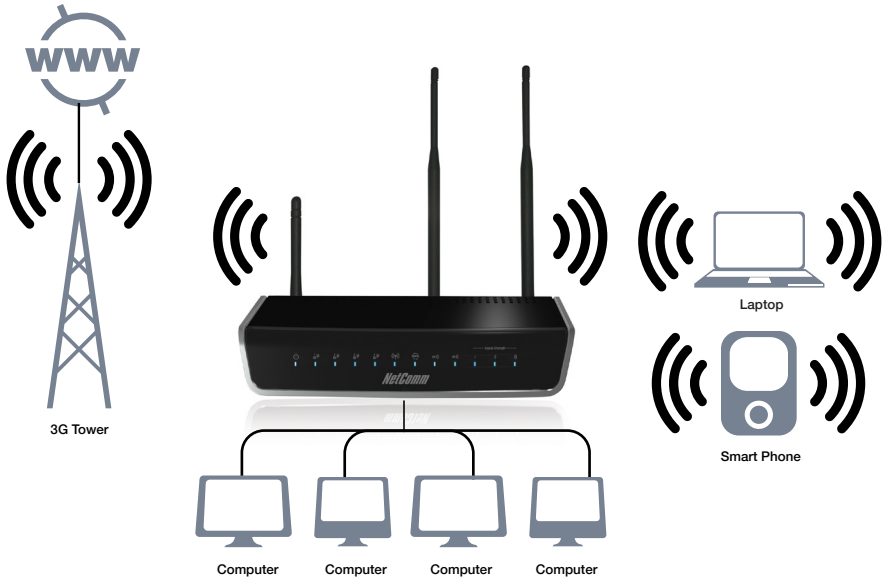
1. Attach the 3G antennas provided to the ports marked Main and Aux on the back of the router. The antennas should be screwed on in a clockwise direction.
2. Attach the WiFi antenna provided to the port marked WiFi on the back of the router.

The antennas should be screwed on in a clockwise direction.

3. Insert your SIM card (until you hear a click) into the USIM slot at the back of the Router.
4. Connect the yellow networking cable to one of the LAN ports found at the back of the Router.
5. Connect the other end of the yellow networking cable to the port on your computer.
6. Connect the power adapter to the Power socket on the back of the Router.
7. Plug the power adapter into the wall socket and push the power button into the ON position (in).
8. Configure the router through the Web User Interface (WUI).

NOTE: Chapters 3 through 8 explain how to setup and use the WUI

9. Save the router configuration and reboot (see section 6.5 Save and Reboot).



Web User Interface

3. Web User Interface

This section describes how to access the device via the web user interface using a web browser such as Microsoft Internet Explorer (version 6.0 or later), Firefox or Safari.

3.1 Default Settings

The following are the default settings for the device.

- Local (LAN) access (username: admin, password: admin)
- Remote (WAN) access (username: support, password: support)
- User access (username: user, password: user)
- LAN IP address: 192.168.1.1
- Remote WAN access: disabled
- NAT and firewall: enabled
- Dynamic Host Configuration Protocol (DHCP) server on LAN interface: enabled

Technical Note:

During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Default Settings screen.

3.2 TCP/IP Settings

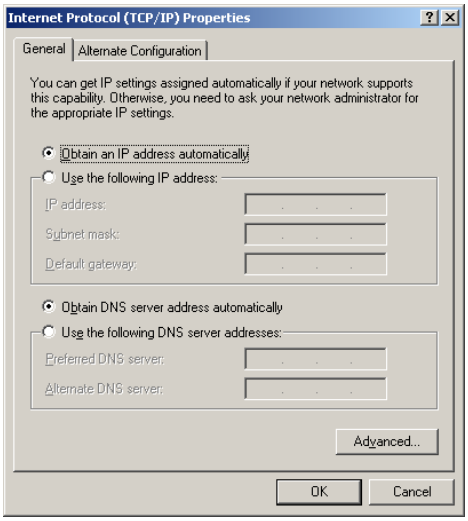
Your computer should automatically obtain an IP Address and join the network. This is because the Dynamic Host Configuration Protocol (DHCP) server will start automatically when your Router powers up.

The computer should already be configured to use DHCP, but if you are required to configure this, please see the instructions below.

Windows XP:

DHCP Mode:

1. Click on the Start button and go to Settings (or control panel).
2. Double left click on the “Network Connections” control panel item.
3. Right click on the “Local Area Connection” and select “Properties”.
4. Left click on the “Internet Protocol (TCP/IP)” item and then click “Properties”.
5. Make sure “Obtain IP Address automatically” and “Obtain DNS server address automatically” are selected.



6. Click OK and then OK again to save these settings.

The IP Address will be automatically assigned from the Router.

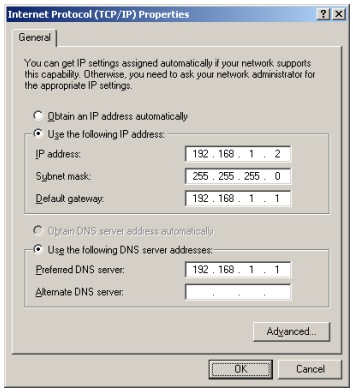
STATIC Mode:

If you do not wish to use automatic assignment of IP Addresses and want to configure your network settings manually, your computer must have a static IP address within the Router's subnet.

The following steps show how to configure your computer's IP address within the default subnet of 192.168.1.x:

NOTE: The default IP address of the router is 192.168.1.1, so the computer must be set with a different IP to the router. In the case below, the computer's IP address is set as 192.168.1.2

1. Click on the Start button and go to Settings, then select the control panel (or proceed directly to the control panel).
2. Double left click on the "Network Connections" control panel item.
3. Right click on the "Local Area Connection" and select "Properties".
4. Left click on the "Internet Protocol (TCP/IP)" item and then click "Properties".
5. Choose an IP address between 192.168.1.2 — 192.168.1.254 and enter this IP address into the IP Address field.
6. Enter a Subnet mask of 255.255.255.0 and the IP address of the Router (the default IP is 192.168.1.1) into the Default gateway fields.
7. Enter the IP address of the Router (the default IP is 192.168.1.1) into the Primary DNS field.

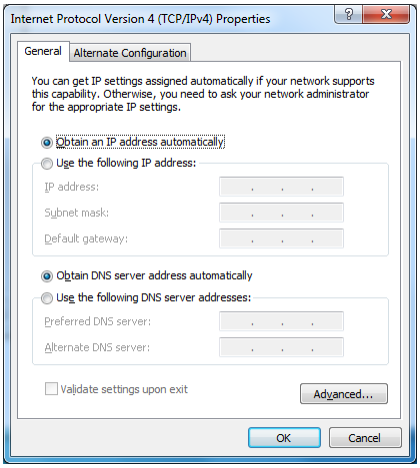


8. Click OK and then OK again to save these settings.

Windows Vista/7:

DHCP Mode:

1. Click on the Start button and go to the control panel.
2. Click on "Network and Internet" and then click on "Network and Sharing Centre".(For Windows Vista)
3. Left click on "Manage Network Connections" from the menu on the left hand side of the window.(For Windows 7)
4. Left click on "Change adapter settings" from the menu on the left hand side of the window.
5. Right click on the "Local Area Connection" item and left click on "Properties".
6. Left click on "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties".
7. Make sure "Obtain IP Address automatically" and "Obtain DNS server address automatically" are selected.



7. Click OK and then OK again to save these settings.

The IP Address will be automatically assigned from the Router.

STATIC Mode:

If you do not wish to use automatic assignment of IP Addresses and want to configure your network settings manually, your computer must have a static IP address within the Router's subnet.

The following steps show how to configure your computer's IP address within the default subnet of 192.168.1.x:

NOTE: The default IP address of the router is 192.168.1.1, so the computer must be set with a different IP to the router. In the case below, the computer's IP address is set as 192.168.1.2

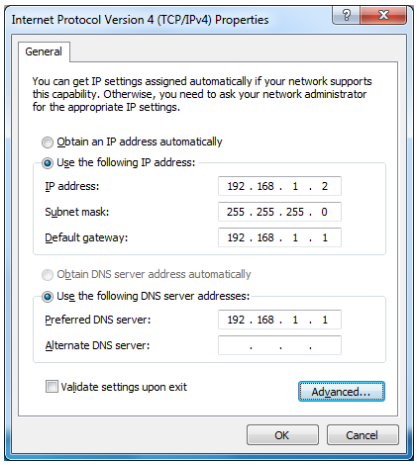
1. Click on the Start button and go to the control panel.
2. Click on "Network and Internet" and then click on "Network and Sharing Centre".

(For Windows Vista)

3. Left click on "Manage Network Connections" from the menu on the left hand side of the window.

(For Windows 7)

3. Left click on "Change adapter settings" from the menu on the left hand side of the window.
4. Right click on the "Local Area Connection" item and left click on "Properties".
5. Left click on "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties".
6. Choose an IP address between 192.168.1.2 — 192.168.1.254 and enter this IP address into the IP Address field.
7. Enter a Subnet mask of 255.255.255.0 and the IP address of the Router (the default IP is 192.168.1.1) into the Default gateway fields.
8. Enter the IP address of the Router (the default IP is 192.168.1.1) into the Primary DNS field.



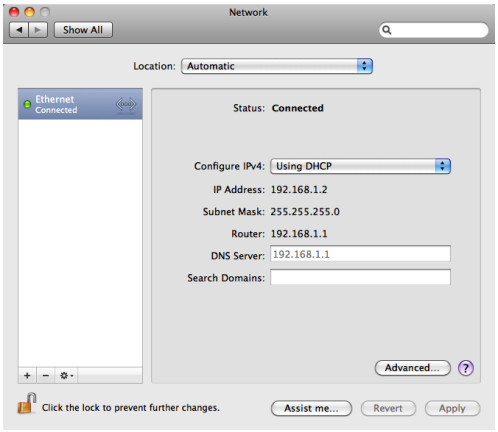
9. Click OK and then OK again to save these settings.

MAC OSX 10.4

DHCP Mode:

To set your computer for DHCP mode, perform the following steps:

1. Click on the Apple menu and select "System Properties".
2. In the System Preferences window, click on the Network icon and select the Ethernet connection.
3. Select "Using DHCP" from the Configure drop down list.



4. Click Apply to save these changes.

The IP Address will be automatically assigned from the Router.

STATIC Mode:

If you do not wish to use automatic assignment of IP Addresses and want to configure your network settings manually, your computer must have a static IP address within the Router's subnet.

The following steps show how to configure your computer's IP address within the default subnet of 192.168.1.x:

NOTE: The default IP address of the router is 192.168.1.1, so the computer must be set with a different IP to the router. In the case below, the computer's IP address is set as 192.168.1.2

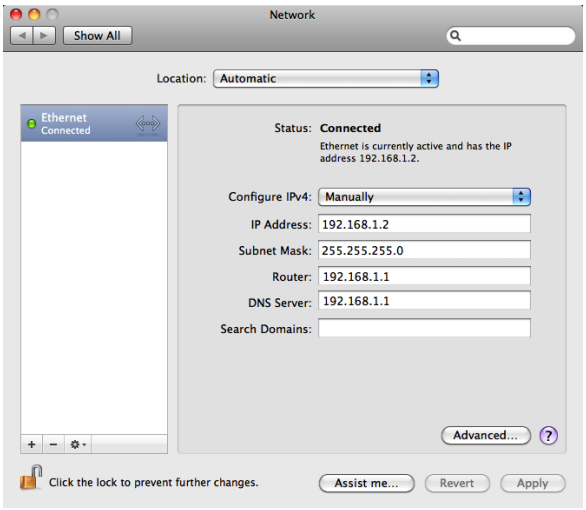
1. Click on the Apple menu and select System Preferences.
2. In the System Preferences window, click the Network icon and select the Ethernet connection.

(For Windows Vista)

3. From the Configure drop down list, you can set your computer to Static IP mode by selecting to use the "Manually" option.

(For Windows 7)

3. Choose an IP address between 192.168.1.2 — 192.168.1.254 and enter this IP address into the field marked IP Address, and enter a Subnet Mask of 255.255.255.0
4. Set the Router and DNS Server field to 192.168.1.1 (The Router's default IP address).



5. Click Apply to save these settings.

3.3 Login Procedure

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

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

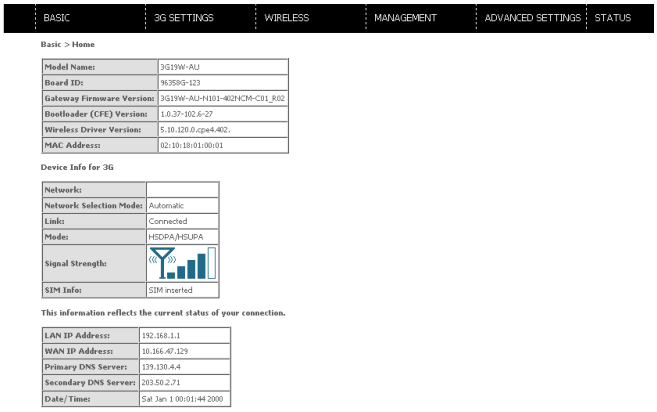
1. Open a web browser and enter the default IP address (http://192.168.1.1) for the Router in the Web address field at the top of the web browser window.

NOTE: For local administration (i.e. LAN access), the PC running the browser must be attached via Ethernet though not necessarily directly to the device. 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 3.1 Default Settings.
3. Click OK to continue.

NOTE: The login password can be changed later (see 6.4.2 Passwords)

4. After successfully logging in for the first time, you will reach this screen.



3.4 Web User Interface Homepage

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)

BASIC / HOME

The Basic / Home screen is the WUI homepage and the first selection on the main menu. It provides information regarding the firmware, 3G, and IP configuration of the device.

The following table provides further details:

FIELD	DESCRIPTION
Model Name	The model name of the Router.
Board ID	The identification number of the main board.
Gateway Firmware version	The firmware version on the device.
Bootloader (CFE) version	The bootloader version of the device.
Wireless driver version	The wireless driver version of the wireless module.
MAC Address	The MAC address of the Router.
Network	The name of or other reference to the mobile network operator.
Link	Shows the connection status of the current 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 mobile network (UMTS or GSM) signal quality available at the device location. This signal quality affects the performance of the unit. If two or more bars are green, the connection is usually acceptable.
SIM info	Shows the SIM card status on the device.
LAN IP Address	Shows the IP address for the LAN interface.
WAN IP Address	Shows the IP address for the WAN interface.
Primary DNS Server	Shows the IP address of the primary DNS server.
Secondary DNS Server	Shows the IP address of the secondary DNS server.
Date/Time	The time according to the device's internal clock

3G Settings

4. 3G Settings

Select your 3G Mobile Broadband service settings according to predefined or custom profiles. Setup instructions are provided in the following sections for your assistance.

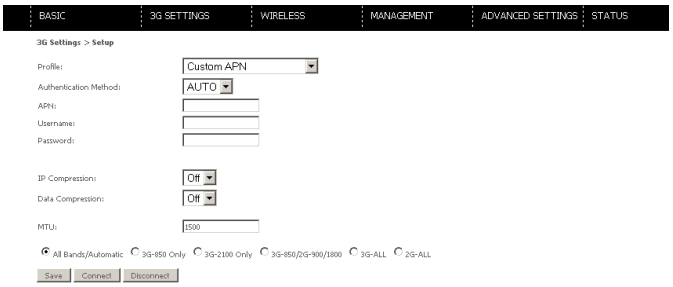
This menu includes 3G Mobile Broadband service Setup, Network Selection and PIN Configuration.

4.1 Setup

NOTE: Sections 8.3 and 8.4.2 also provide information about the 3G Mobile Broadband service.

Your 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. Type the APN in the APN field. Authentication Method should be provided by your Internet service provider; or just leave it set to AUTO if not required. If you have not received a username and password, leave these fields empty.



Select IP compression and Data compression to be ON or OFF. By default they are set to off.

3. Click the Save button to save the new settings.
4. Press the Connect button to reboot the router and to connect to Internet. After reboot, the Device Info for

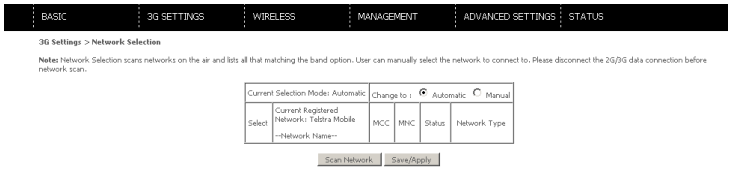
The 3G network box in the WUI Basic screen should indicate an active connection, as shown below. The 3G and Internet LEDs on the front panel of the Router should also be blinking.

If the LEDs are off, then either your profile settings are incorrect, the SIM card is not working or the service network is unavailable. In either case, contact Technical Support for further instructions.

NOTE: If the LEDs light up in an on/off pattern moving from left to right this indicates that your SIM is PIN Locked; please see the 4.3.1 PIN Lock Off section for instructions on how to fix this.

4.2 Network Selection

This screen allows for automatically or manually selecting the 3G Mobile Broadband service to use.



Auto - To automatically connect to the appropriate available 3G service.

Manual - To manually select which 3G service to attempt to connect to.

You can click “Scan Network” to scan for available 3G services around you and select your chosen 3G service.

Click Save/Apply to save any changes you have made.

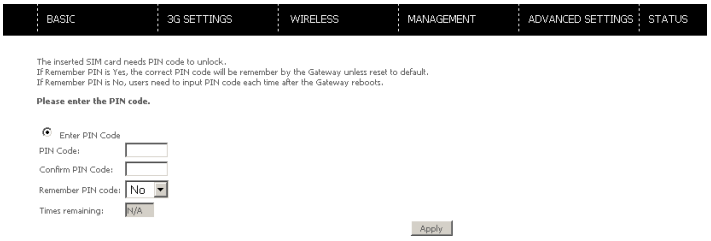
4.3 PIN Configuration

This screen allows for changes to the 3G SIM card PIN code protection settings.

NOTE: If you have entered the incorrect PIN 3 times, your SIM card will be locked for your security. Please call your 3G service provider for assistance.

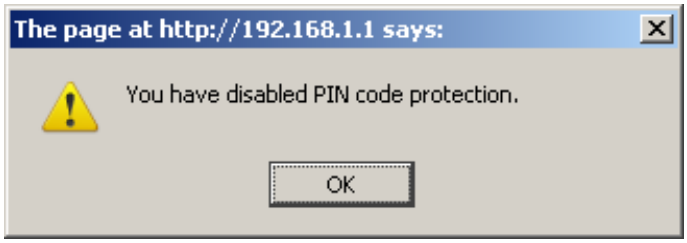
4.3.1 PIN Code Protection

PIN code protection prevents the use of a SIM card by unauthorized persons. To use the 3G Mobile Broadband service with this router however, the PIN code protection must be disabled. If the SIM card inserted into the router is locked with a PIN code, the web user interface will display the following screen after login.



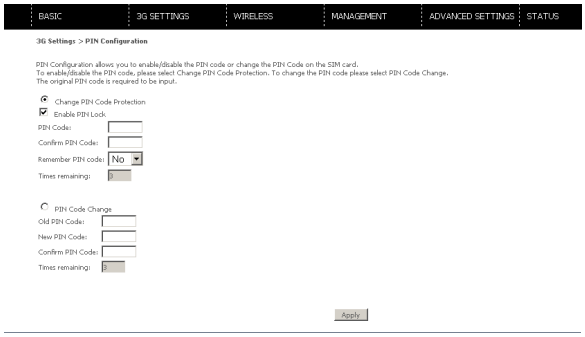
PIN Lock Off

If you wish to connect to the Internet using a PIN locked SIM card, you must first turn PIN code protection Off. Select PIN lock Off, enter the PIN Code twice. Please keep in mind you only have 3 attempts before your SIM card is locked. The remaining attempts’ number shows how many attempts left. Contact your service provider if you require assistance. You can set Remember PIN Code to ON so you don’t need to input the PIN code every time when the router turns on. Afterwards, click Apply. The following dialog box should now appear.



PIN Lock On

After you are finished using your SIM card for Internet service, you may wish to lock it again. In this case, first go to the 3G Settings - PIN Configuration screen, as shown below. Select PIN lock ON and enter the PIN code twice. You can set Remember PIN code to Yes so you don't need to input the PIN code every time when the router turns on.



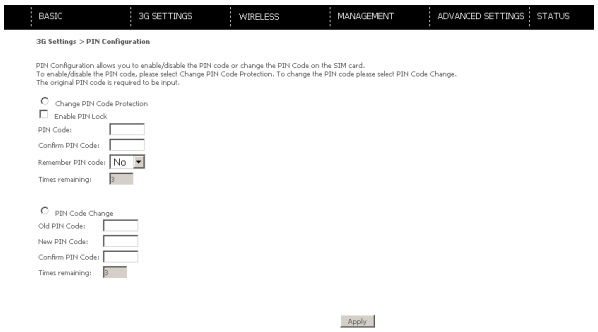
You can now return your SIM card to your cellular phone or other mobile device.

4.3.2 PIN Code Change

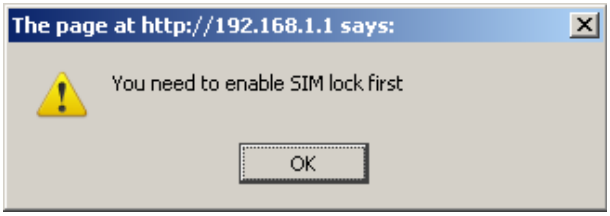
If you wish to change your PIN code for greater security, enable the PIN Code protection. Go to the previous section and follow the procedure listed under PIN Lock On.

After locking the SIM card, select PIN Code Change and enter your Old and New PIN codes in the fields provided. Keep in mind you only have 3 attempts before your SIM card is locked. The remaining attempts' number shows how many attempts are left. Contact your 3G Carrier if you require assistance.

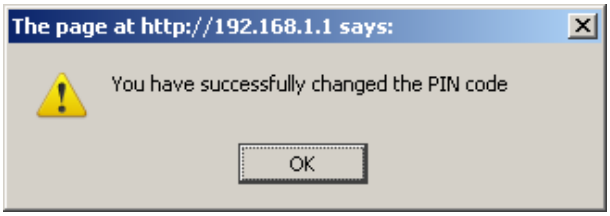
Click Apply to activate the change.



NOTE: If you forget to change the PIN Code without first turning on PIN lock protection, you will see this dialog box as a helpful reminder.



If your PIN Code change request was successful the following dialog box will display.



Wireless

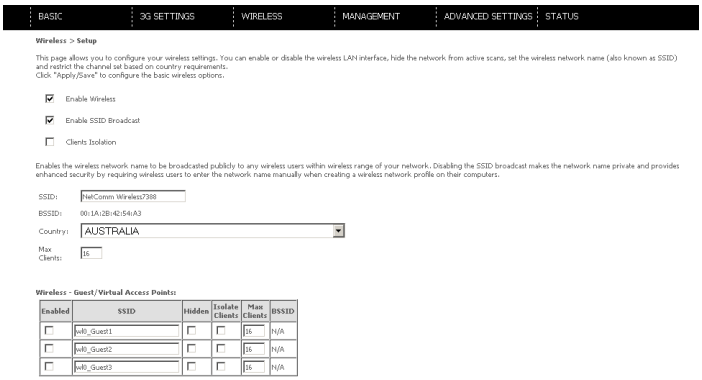
5.Wireless

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

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

5.1 Setup

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 SSID) and restrict the channel set based on country requirements. The Wireless Guest Network function adds extra networking security when connecting to remote hosts.



OPTION	DESCRIPTION
Enable Wireless	A checkbox that enables (default) or disables the wireless LAN interface. When selected, the WebUI displays Hide Access point, SSID, BSSID and Country settings.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, 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.
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 48 bit 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 adhoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings.
Wireless Guest	The Guest SSID (Virtual Access Point) can be enabled by selecting the Enable Wireless Guest Network checkbox
	You can rename, hide or limit the number of users of the Wireless Guest Network as needed.
Clients Isolation	Prevent wireless clients from communicating with each other

NOTE: Wireless hosts cannot scan Guest SSIDs.

5.2 Security

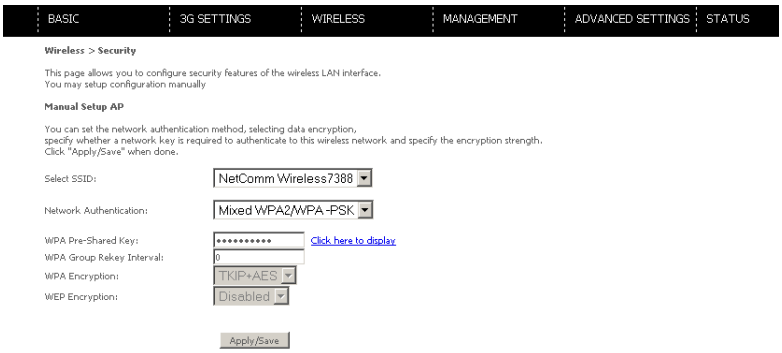
This Router includes a number of security options that provides you with a secure connection to a 3G network. State-of-the art security includes:

- WEP / WPA / WPA2 data encryption
- SPI Firewall
- VPN Pass-Through
- MAC address IP filtering
- Authentication protocols — PAP / CHAP

You can also authenticate or encrypt your service using the WEP algorithm, which provides protection against unauthorized access such as eavesdropping.

By default, WPA-PSK security is specified for the Network authentication type in use.

The following screen appears when Security is selected. The Security page allows you to configure security features of your Router's wireless LAN interface. You can set the network authentication method, select data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.



Click Save/Apply to configure the wireless security options.

OPTION	DESCRIPTION
Select SSID	Your Service Set Identifier (SSID), sets your Wireless Network Name. You can connect multiple devices including Laptops, Desktop PCs and PDAs to your Wireless Router. To get additional devices connected, scan for a network, and locate the SSID shown on your Wireless Security Card. If the SSID does not match, access is denied.
Network Authentication	This option is used for authentication to the wireless network. Each authentication type has its own settings. (For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled)
WEP Encryption	This option indicates whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Whilst four network keys can be defined, only one can be used at anyone time. Use the network key found in the drop-down list.
Encryption Strength	This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack.
	Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers.

NOTE: Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

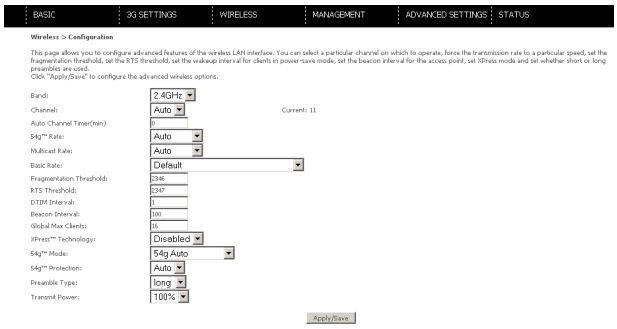
Click Apply/Save to save any changes you have made to your Wireless security.

Please note: You will need to reconfigure and reconnect any wirelessly connected devices after changing the security on your wireless network.

5.3 Configuration

The following screen appears when you select Configuration. 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 Save/Apply to set the advanced wireless configuration.

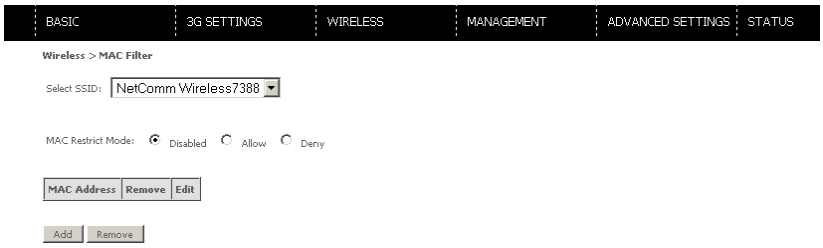
OPTION	DESCRIPTION
Band	The new amendment allows IEEE802.11g units of all types to fallback to speeds of 11Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network.
Channel	Allows selection of a specific channel (1 - 1 1) or Automode.
Auto Channel Timer (mins)	The Auto Channel times the length it takes to scan in minutes.
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 discreet values between 1 to 54 Mbps.
Multicast Rate	Setting for multicast packet transmission rate. (1-54Mbps)
Basic Rate	Sets basic transmission rate.
Fragmentation Threshold	A threshold (in bytes) determines whether packets will be fragmented and at what size. Packets that exceed the fragmentation threshold of an 802.11 WLAN will be split into smaller units suitable for the network. Packets smaller than the specified fragmentation threshold value are not fragmented. Values between 256 and 2346 can be entered but this 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 (maxlength) will disable 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. A PC 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 is in milliseconds. The default is 100 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.
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.
54g Mode	Select Auto mode for greatest compatibility. Select Performance mode for the fastest performance among 54g certified equipment. Select LRS mode if you are experiencing difficulty with legacy 802.1 1b equipment. If this does not work, you may also try 802.11b only mode.
54g Protection	In Auto mode, the router will use RTS/CTS to improve 802.11g performance in mixed 802.11g / 802.11b networks. Turning protection Off will maximize 802.11g throughput under most conditions.
Preamble Type	Short preamble is intended for applications where maximum throughput is desired but it does not work with legacy equipment. Long preamble works with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999
Transmit Power	Set the power output (by percentage) as desired.

5.4 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 as shown below.

To delete a filter, select it from the table below and click the Remove button.



FEATURE	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.

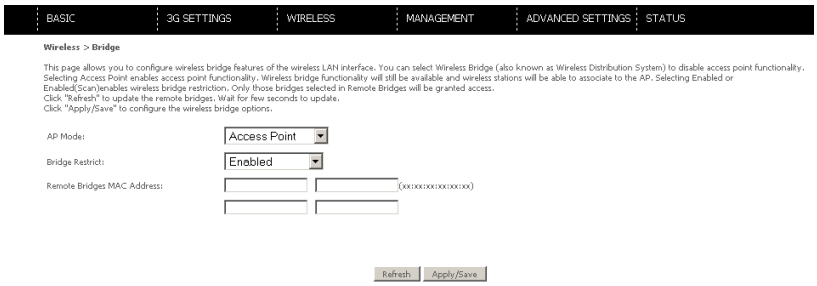
Enter the MAC address on the screen below and click Save/Apply.

5.5 Wireless Bridge

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

A wireless bridge is utilised to extend your WiFi network coverage and enable distant computers to access network resources.

Click Save/Apply to implement new configuration settings.



FEATURE	DESCRIPTION
AP Mode	Selecting Wireless Bridge (or Wireless Distribution System) disables Access Point (AP) functionality. Selecting AP enables Access Point mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting Enabled or Enabled (Scan) allows wireless bridge restriction. Only those bridges selected in "Remote Bridges" will be granted access. Enabled (Scan) scans the detected wireless networks and allows you to select one to connect to. Click Refresh to update the station list when Enabled (Scan) is selected.

5.6 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.

FEATURE	DESCRIPTION
MAC	This shows the unique 48-bit MAC address of wireless clients
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.

Management

6. Management

The Management menu has the following maintenance functions and processes:

- 6.1 Device Settings
- 6.2 Simple Network Management Protocol (SNMP)
- 6.3 Simple Network Time Protocol (SNTP)
- 6.4 Access Control
- 6.5 Save and Reboot

6.1 Device Settings

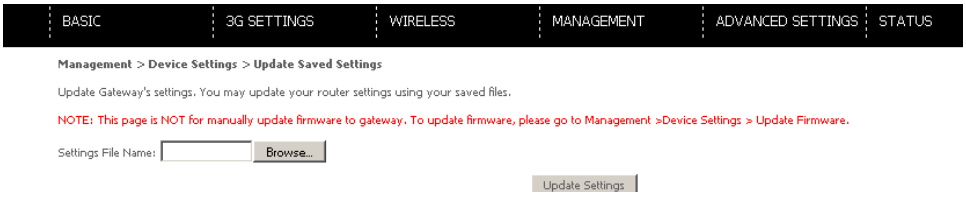
The Device Settings screens allow you to backup, retrieve and restore the default settings of your Router. It also provides a function for you to update your Routers firmware.

6.1.1 Backup Settings

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

6.1.2 Update Settings

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.



6.1.3 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

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).

After a successful reboot, the browser will return to the Device Info screen. If the browser does not refresh to the default screen, close and restart the browser.

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.

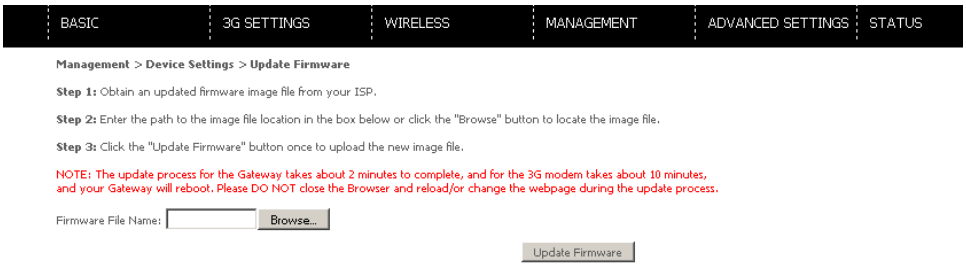
6.1.4 Update Firmware

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

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 Firmware button once to upload and install the file.

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.



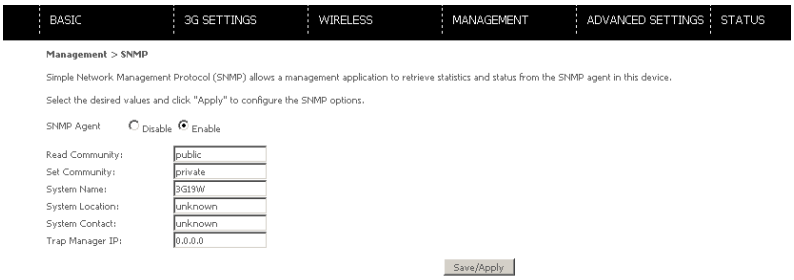
6.2 Configure SNMP agent

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 3G19W-AU (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.

By default, SNMP agent is enabled on the router.

Setting up SNMP agent

1. Open a web browser (IE/Firefox/Safari), type in LAN address of the router (http://192.168.1.1 by default) to log into the web interface.
2. The login username and password by default is admin/admin.
3. Go to Management> SNMP.
4. Enable SNMP agent and set up all options according to your requirements.

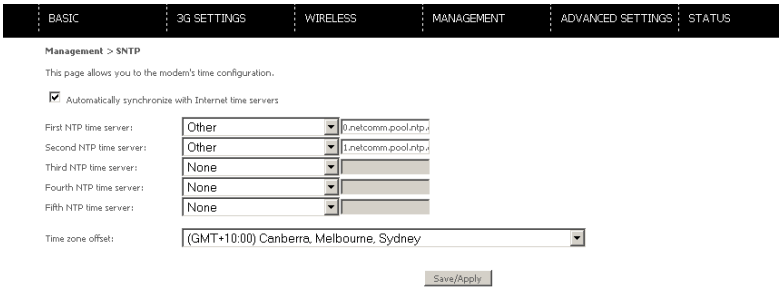


5. Press Save/Apply to activate the settings.

6.3 Simple Network Time Protocol (SNTP)

This screen allows you to configure the time settings of your Router. To automatically synchronize with Internet timeservers, tick the box as illustrated below.

The following options should now appear:



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

Configure these options and then click Save/Apply to activate.

NOTE: SNTP must be activated to use Parental Control (see section 7.4).

6.4 Access Control

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

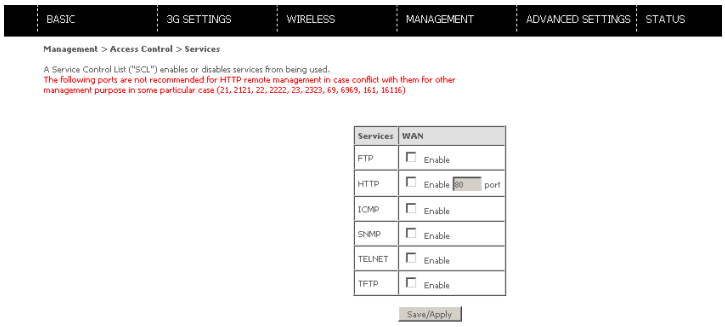
- Services
- Passwords

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

6.4.1 Services

The Service Control List (SCL) allows you to enable or disable your Wide Area Network (WAN) services by ticking the checkbox as illustrated below. The following access services are available: FTP, HTTP, ICMP, SNMP, TELNET, and TFTP.

Enable or disable these options are per your requirements.



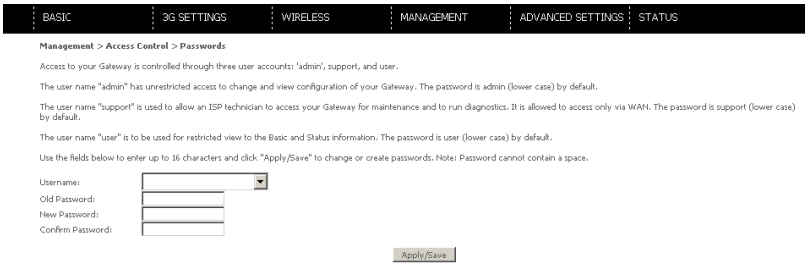
Click Save/Apply to continue.

6.4.2 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 Save/Apply to continue.

6.5 Save and Reboot

This function saves the current configuration settings and reboots your 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 on your connected devices.

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 the default settings.

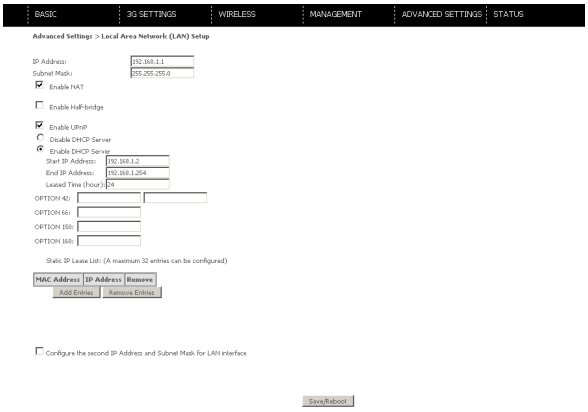
Advanced Setup

7. Advanced Setup

This chapter explains the advanced setup options for your Router:

7.1 Local Area Network (LAN)

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



See the field descriptions below for more details.

OPTION	DESCRIPTION
IP Address	Enter the IP address for the LAN interface
Subnet Mask	Enter the subnet mask for the LAN interface
Enable UPnP	Tick the box to enable Universal Plug and Play
Enable Half-Bridge	The Router can be setup as a half-transparent bridge to cope with some special applications such as VPN pass-through. By default half-bridge is off..
Dynamic Host Configuration Protocol (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 the IP address, default gateway and DNS server addresses to every DHCP client on your LAN.
Option 42, 66, 150, 160	These options are used for special DHCP setup.
Static IP Lease List	To specify the IP address assigned through DHCP according to the MAC address of the hosts connected to the router.

Configure a second IP address by ticking the checkbox shown below and enter the following information:

IP Address:	Enter the secondary IP address for the LAN interface.
Subnet Mask:	Enter the secondary subnet mask for the LAN interface.

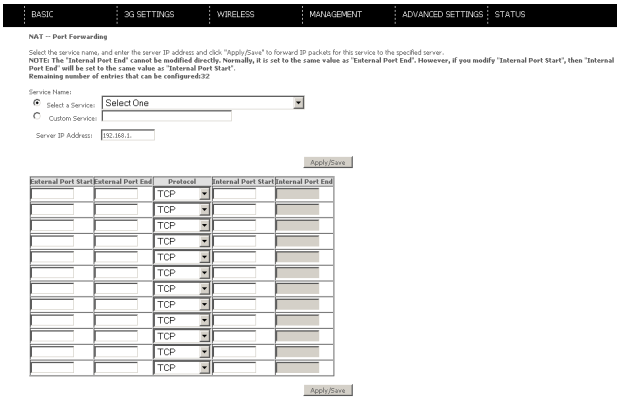
NOTE: The Save button saves new settings to allow continued configuration, while the Save/Reboot button not only saves new settings but also reboots the device to apply the new configuration (i.e. all new settings).

7.2 Network Address Translation (NAT)

7.2.1 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.

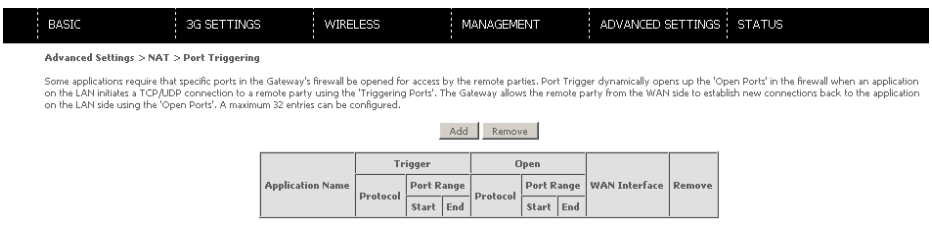
To add a Virtual Server, click the Add button. The following screen will display.



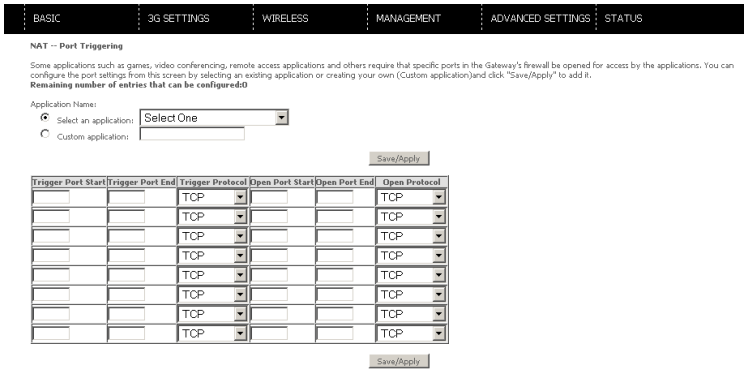
OPTION	DESCRIPTION
Select a Service	Select a predefined service to port forward. Or
Custom Server	Create a custom server and enter a name for it.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a predefined 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 predefined 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 predefined 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 predefined service is selected the port ranges are automatically configured.

7.2.2 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.



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

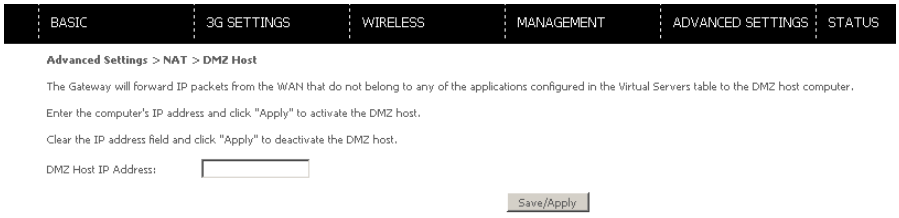


OPTION	DESCRIPTION
Select an Application	Select a predefined service to port trigger on.
	Or
Custom Application	Create a custom server and enter a name for it.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected , the port ranges are automatically configured.
Trigger Port End	Enter 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.

7.2.3 Demilitarized (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.



7.3 Security

Your Router can be secured with incoming or outgoing IP Filtering. This allows you to control whether data can enter or leave via the router.

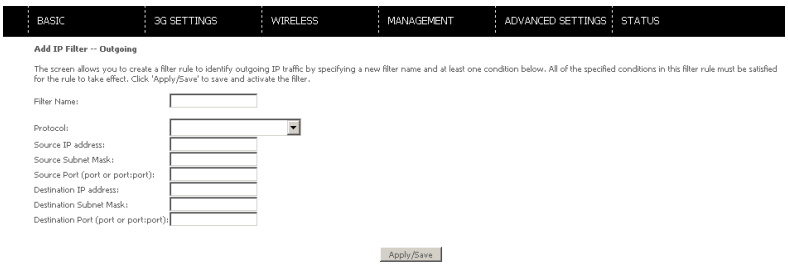
7.3.1 IP Filtering

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 when individual IP packets pass 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.

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



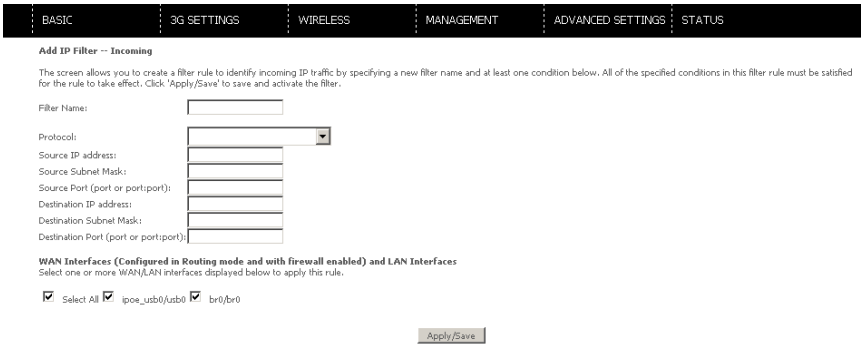
OPTION	DESCRIPTION
Filter Name	The Filter rule label.
Protocol	TCP, TCP/UDP, UDP or ICMP traffic.
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source Subnet mask.
Source Port (port or port:port)	Enter source port number or port range.
Destination IP adress	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number or range.

Click Save/Apply 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.

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



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

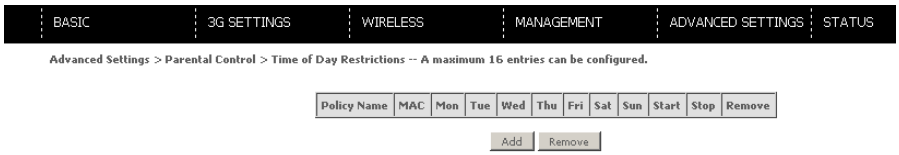
Click Save/Apply to save and activate the filter.

7.4 Parental Control

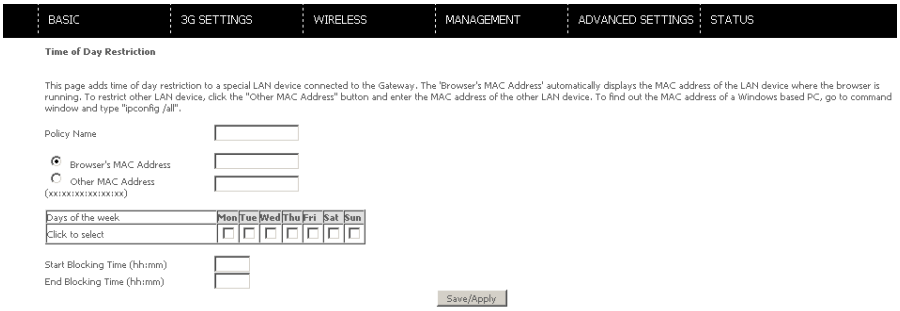
Parental Control allows you to restrict access from a Local Area Network (LAN) to an outside network through the Router on selected days and/or at certain times. Make sure to activate the Internet Time server synchronization (see section 6.3 SNTP), so that the scheduled times match your local time.

7.4.1 Time of Day Restrictions

This enables you to select a time of the day to impose or relax any network restrictions you have in place.



Click Add to display the following screen.



OPTION	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.

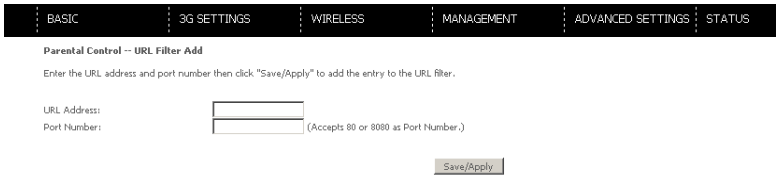
Click Save/Apply to save and activate the parental control entered.

7.4.2 URL Filter

This enables you to allow or prevent access to specific websites based on the address being entered to access it.

Select either “To Block” or “To Allow” depending on your current IP Filtering (see section 7.3 Security) as per the screenshot below.

You can then click “Add” to add a new URL filter.



You can then enter the URL and the port number as prompted on the page to enter a new URL filter and click “Save/Apply”.

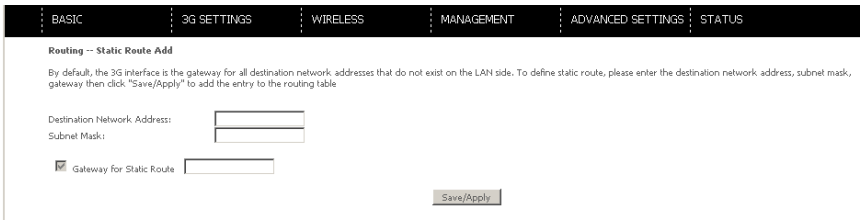
7.5 Routing

Static Route settings can be found in the Routing link as illustrated below.

7.5.1 Static Route

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

Click Add to display the following screen.

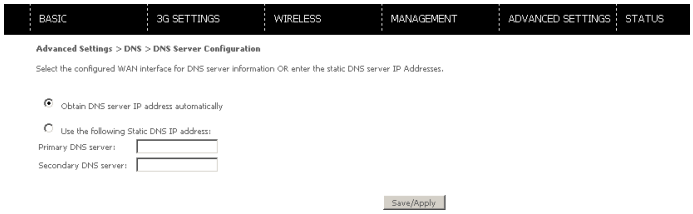


Enter the Destination Network Address, Subnet Mask, Gateway IP Address and/or WAN Interface.

Click Save/Apply to add the entry to the routing table.

7.6 Domain Name Servers (DNS)

If the Enable Automatic Assigned DNS checkbox is selected, this device will accept the first received DNS assignment from the Wide Area Network (WAN) interface during the connection process. If the checkbox is not selected, a field will appear allowing you to enter the primary and optional secondary DNS server IP addresses.



Click on Save to apply.

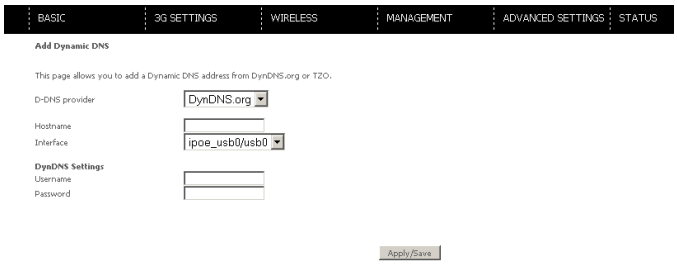
NOTE: To make the new configuration effective, reboot your Router.

7.6.1 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.

NOTE: The Add/Remove buttons will be displayed only if the router has been assigned an IP address from the remote server.

To add a dynamic DNS service, click the Add button and the following screen will display.



OPTION	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.

Status

8. Status

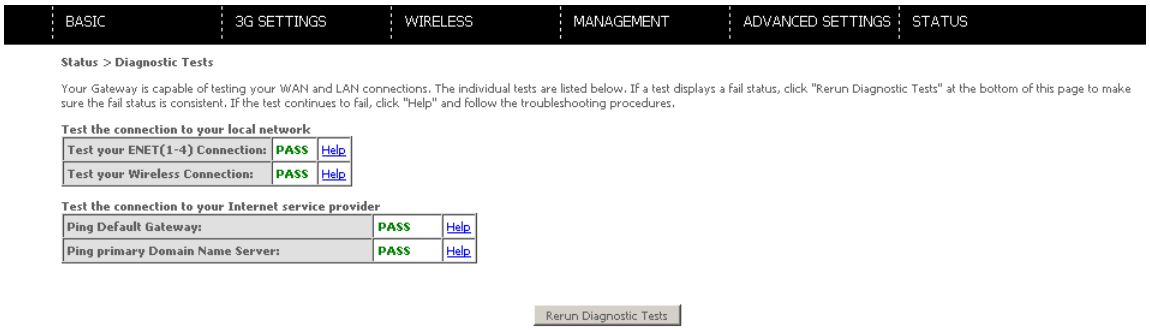
The Status menu has the following submenus:

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

8.1 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
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, follow the troubleshooting procedures on the Help screen.

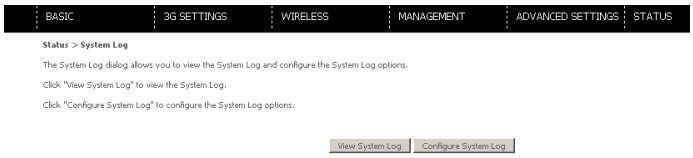


OPTION	DESCRIPTION
Test your ENET (1-4) Connection	Pass: Indicates that the Ethernet interface from your computer is connected to the LAN port of this Router.
	Fail: Indicates that the Router does not detect the Ethernet interface on your computer.
Test your Wireless connection	Pass: Indicates that the wireless card is ON.
	Down: Indicates that the wireless card is OFF.
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.

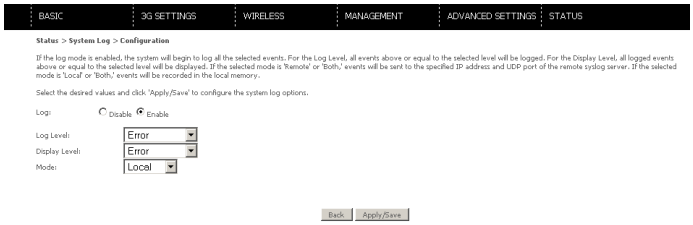
8.2 System Log

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.

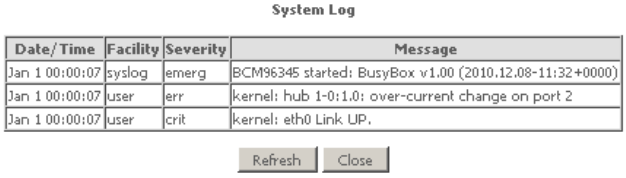


2. Select the system log options (see table below) and click Save/Apply.



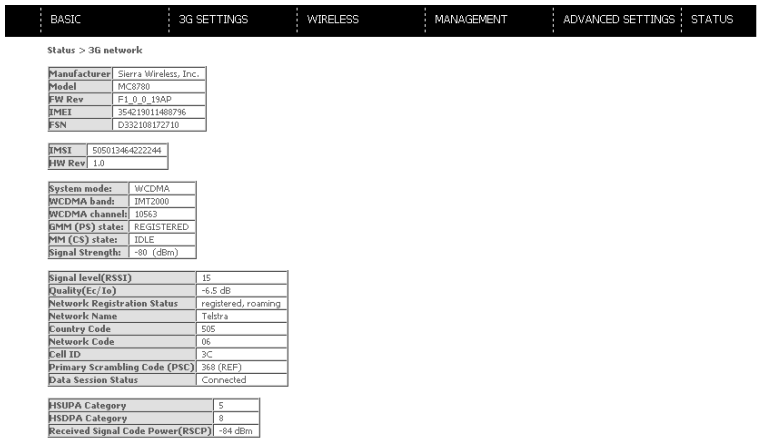
OPTION	DESCRIPTION
Log	Indicates whether the system is currently recording events. You can enable or disable event logging. By default, it is disabled.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "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 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 systemlog 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 you to enter the Server IP address and Server UDP port.

3. Click View System Log. The results are displayed as follows.



8.3 3G Network

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



Consult the table for detailed field descriptions.

OPTION	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.
System Mode	WCDMA/Europe CDMA 2000/America
WCDMA band	The 3G radio frequency band which supports tri-band UTMS/HSDPA/HSUPA frequencies (850/1900/2100MHz), IMT2000 is 2100MHz, WCDMA800 is 850MHz,WCDMA1900 is 1900 MHz.
WCDMA channel	The 3G channel.
GMM 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.
GMM (PS) state	Packet Switching state.
MM (CS) state	Circuit Switching state.
Signal Strength	The 3G/2G service signal strength in dBm.
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 Code	Each country has a unique code.
Network Code	Each 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 Category	The HSUPA categories correspond to different data transmission rates with higher numbers generally indicating faster rates.
HSDPA Category	The HSDPA categories correspond to different incoming data rates with higher numbers generally indicating faster rates.
Received Signal Code Power (RSCP)	The RSCP of the active set's three strongest cells.

8.4 Statistics

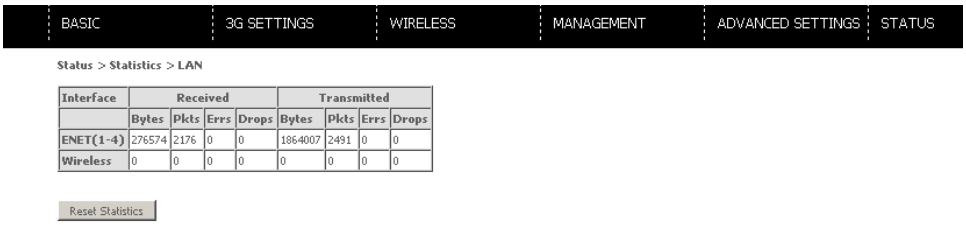
These screens provide detailed information for:

- Local Area Network (LAN) and Wireless Local Area Network (WLAN)
- 3G Interfaces

NOTE: These statistics page refresh every 15 seconds.

8.4.1 LAN Statistics

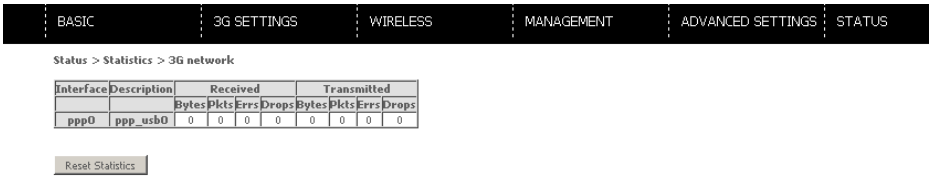
This screen displays statistics for the Ethernet and Wireless LAN interfaces.



INTERFACE	Shows connection interfaces	
Received/Transmitted	Bytes	Rx/TX (receive/transmit) packets in bytes
	Pkts	Rx/TX (receive/transmit) packets
	Errs	Rx/TX (receive/transmit) packets with errors
	Drops	Rx/TX (receive/transmit) packets dropped

8.4.2 3G Statistics

Click 3G network in the Statistics submenu to display the screen below.

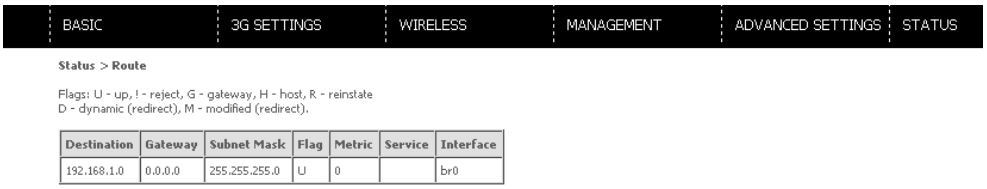


Inbound Octets	
Number of received octets over the interface.	
Packets	Number of received packets over the interface.
Drops	Received packets which are dropped.
Error	Received packets which are errors.

Outbound Octets	
Number of transmitted octets over the interface.	
Packets	Number of transmitted packets over the interface.
Drops	Transmitted packets which are dropped.
Error	Transmitted packets which are errors.

8.5 Route

Select Route to display the paths the Router has found or has had manually added.



DESTINATION	DESTINATION NETWORK OR DESTINATION HOST
Gateway	Next hop IP address
Subnet Mask	Subnet Mask of Destination
Flag	U : route is up
	I : reject route
	G : use gateway
	H : target is a host
	R : reinstate route ford ynamic routing
	D : dynamically installed by daemon or redirect
	M : modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not Used by recent kernels, but may be needed by routing daemons.
Service	Shows the name for the WAN connection
Interface	Shows connection interfaces

8.6 ARP

Click ARP to display the ARP information.

FIELD	DESCRIPTION
IP address	Shows IP address of host pc
Flags	Complete
	Incomplete
	Permanent
	Publish
HW Address	Shows the MAC address of host pc
Device	Shows the connection interface

8.7 Dynamic Host Configuration Protocol (DHCP)

Click DHCP to display the DHCP information.

FIELD	DESCRIPTION
Hostname	Shows the device/host/PC network name
MAC Address	Shows the Ethernet MAC address of the device/host/PC
IP address	Shows IP address of device/host/PC
Expires In	Shows how much time is left for each DHCP Lease

8.8 PING

The PING menu provides feedback of connection test to an IP address or a host name.

Input an IP address or a host name, e.g www.google.com and press Submit. The connection test result will be shown as below.

Appendix

Appendices

Legal & Regulatory Information

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 TSOO8 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.

Federal Communication Commission Interference Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This device complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

Operation is subject to the following two conditions:

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

IC Important Note

IC Radiation Exposure Statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter. The County Code Selection feature is disabled for products marketed in the US/Canada.

Operation is subject to the following two conditions:

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme a la norme NMB-003 du Canada.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.

This device has been designed to operate with an antenna having a maximum gain of 4 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

Operation is subject to the following two conditions:

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please refer to the GNU General Public License below to check the detailed terms of this license.

The following parts of this product are subject to the GNU GPL, and those software packages are copyright by their respective authors.

Linux-2.6.21 system kernel

busybox_1_00_rc2

bridge-utils 0.9.5

dhcpcd-1.3

ISC DHCP V2 P5

syslogd spread from busybox

wireless tools

ntpclient of NTP client implementation

GNU Wget

Availability of source code

Please visit our web site or contact us to obtain more information.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive

use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection
b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in
   full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by

public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,

INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

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.

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: 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.