

**Table Of Content**

1. Introduction .....	3
Your 3G8WV – HSPA Wi-Fi Router with Voice .....	3
1.1 Package Contents .....	3
1.2 Key Features .....	4
2. Placement of your 3G8WV .....	4
2.1 Router Placement .....	5
2.2 Avoid obstacles and interference .....	5
2.3 Cordless Phones .....	5
2.4 Choose the “Quietest” Channel for your Wireless Network .....	6
3. Product Layout .....	6
3.1 Connecting and Configuring your Router .....	6
3.2 Network and System Requirements .....	7
3.3 Connecting your 3G8WV .....	8
Step1 – Insert SIM card .....	8
Step2 – Connect a computer .....	8
Step3 – Plug in the power .....	8
4. Advanced Features .....	8
4.1 Login Procedure .....	9
4.2 Status .....	9
4.3 Internet Settings .....	10
4.3.1 3G Internet Settings .....	10
4.3.2 WAN .....	13
4.3.3 LAN .....	18
4.3.4 Advanced Routing .....	19

4.3.	5 DHCP Client .....	20
5.0	Wireless Setting .....	20
5.1	Basic .....	20
5.2	Advanced.....	21
5.3	Security .....	23
5.4	WPS .....	28
5.5	Station List.....	30
6.0	Firewall.....	30
6.1	Mac/IP/Port Filtering .....	30
6.2	Port Forwarding .....	32
6.3	DMZ.....	33
6.4	System Security .....	34
6.5	Content Filtering .....	35
7.0	Administration .....	36
7.1	Management.....	36
7.2	Upload Firmware .....	38
7.3	Setting Manager.....	38
7.4	Statistics .....	39
7.5	System Log .....	40
8.0	Legal & Regulatory Information.....	41
8.1	Customer Information .....	41
8.2	Federal Communication Commission Interference Statement .....	41

## 1. Introduction

### Your 3G8WV – HSPA Wi-Fi Router with Voice



The NetComm 3G8WV integrates a Wireless LAN, HSPA module and voice gateway into one stylish unit. Insert an active HSPA SIM card into the slot on the rear panel and get instant access to a 3G Internet connection.

The NetComm 3G8WV incorporates a WLAN 802.11b/g/n access point, two Ethernet 10/100Mbps ports and two phone ports for voice calls. It features the latest security options such as WPA2 data encryption, SPI Firewall and VPN pass through.

This feature packed device enables you to quickly and simply create a secure Wi-Fi network and provide Internet access using a 3G network. Share your 3G connection with multiple wireless and wired devices, without the hassle of a fixed line Internet connection. Featuring a voice port means you can now stay connected using the Internet and telephone. If you need a flexible Internet connection for your business, this is the perfect solution for you.

#### 1.1 Package Contents

1. 3G8WV – HSPA Wi-Fi Router with Voice
2. 12VDC~1.5A Power Adapter
3. RJ45 LAN Cable
4. Quick Install Guide

## 5. CD(User's Manual)

**1.2 Key Features**

1. Tri-band UMTS / Quad-band GSM/EDGE
2. 7.2Mbps down / 5.76Mbps up
3. 2 x Voice port (circuit-switched)
4. 2 x 10/100 Ethernet ports (Configurable as WAN or LAN)
5. 802.11n/300Mbps wireless1
6. WAN port for alternate Internet connection (ADSL/Cable/Satellite)
7. Supports auto Internet failover to 3G
8. 2 Transmit and 2 Receive Internal Wi-Fi antennas
9. Wi-Fi Protected Setup (WPS) for an easy and secure wireless connection
10. Browser based interface for configuration and management: OS independent and easy to use
11. Full wireless security - WEP, WPA, WPA2

**2. Placement of your 3G8WV**

Just like your mobile phone, a 3G Router's location will affect its signal strength to the 3G Mobile Base Station (Cell Tower). The data speed achievable from a 3G Router is relative to this signal strength, which is affected by many environmental factors. Please keep in mind that the 3G Router will need adequate signal strength in order to provide Internet connectivity whilst choosing a location to place your 3G8WV.

Similarly to the 3G Router, the wireless connection between the Router and your Wi-Fi devices will be stronger the closer your connected devices are to your Router. Your wireless connection and performance will degrade as the distance between your Router and connected devices increases. This may or may not be directly noticeable, and is greatly affected by the individual installation environment.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between three to five meters from the Router in order to see if distance is the problem. If difficulties persist even at close range, please contact NetComm Technical Support.

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

## 2.1 Router Placement

Place your Router as close as possible to the centre of your wireless network devices. To achieve the best wireless network coverage for your “wireless clients” (i.e., computers with built in or USB Wireless Adapters, Laptops with Built-in Wireless, Wireless PDA / iPhone, etc):

- Ensure that your Router’s antennas are parallel to each other, and are positioned vertically (toward the ceiling). If your Router itself is positioned vertically, point the antennas in an upward direction as much as possible.
- In multi-storey homes, place the Router on a floor that is as close to the centre of the home as possible. This may mean placing the Router on an upper floor.
- Try not to place the Router near a cordless telephone that operates at the same radio frequency as the 3G8WV (2.4GHz).

## 2.2 Avoid obstacles and interference

Avoid placing your Router near devices that may emit radio “noise,” such as microwave ovens. Dense objects that can inhibit wireless communication include:

- Refrigerators
- Washers and/or dryers
- Metal cabinets
- Large aquariums
- Metallic-based, UV-tinted windows

If your wireless signal seems weak in some spots, make sure that objects such as these are not blocking the signal’s path (between your devices and Router).

## 2.3 Cordless Phones

If the performance of your wireless network is impaired after considering the above issues, and you have a cordless phone:

- Try moving cordless phones away from your Router and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4GHz band (check manufacturer’s information). If this fixes the problem, your phone may be interfering with the Wi-Fi Router.

- If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your Router to channel 11. See your phones user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 5GHz cordless phone.

### 2.4 Choose the “Quietest” Channel for your Wireless Network

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

Use the Site Survey capabilities found in the Wireless Utility of your wireless adapter to locate any other wireless networks that are available (see your wireless adapter’s user manual), and switch your Router and computers to a channel as far away from other networks as possible.

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

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

## 3. Product Layout

### 3.1 Connecting and Configuring your Router

The Router has been designed to be placed on a desktop. All of the cables exit from the rear of the Router for better organization. The display is easily visible on the FRONT of the Router to provide you with information about network activity and status. See below for explanation of each of the features.

Front Panel	Description
Wireless	Lights up when WLAN is enabled. Blinks on traffic
WAN	Lights up when the router is connected via WAN
LAN	Lights up when specific LAN connection is established. Blinks on LAN PORT traffic
3G	Lights up when the router is connected via 3G

Phone 1	Lights up when the handset connected to Phone 1 is on hook
Phone 2	Lights up when the handset connected to Phone 2 is on hook
Power	Lights up and flashing when powered ON

Rear Ports	
SIM Slot	Insert your SIM card here
3G Antenna	Screw in the 3G Antenna here
WAN	WAN Ethernet port for Fixed Line (ADSL/Cable/Satellite) connection
LAN	LAN Port for wired Ethernet clients (Computers, Laptops, etc)
Phone 2	Phone Port for Handset
Phone 1	Phone Port for Handset
Reset	Hold this button down for 10 seconds to reset to factory defaults.
Power	Power connector, connects to DC 12V 1.25A Power Adapter

### 3.2 Network and System Requirements

Before continuing with the installation of your 3G8WV, please confirm that you comply with the minimum system requirements below.

- Compatible 3G SIM card(850MHz/1900MHz/2100MHz) with Active SIM/Data Service if you want to use 3G Broadband service.

Note: Subject to terms and conditions from your 3G Mobile Broadband Service Provider.

- Computer with Windows, Macintosh, or Linux-based operating systems with a working Ethernet adapter with TCP/IP Protocol installed.
- A Web Browser such as Internet Explorer, Netscape Navigator, Mozilla Firefox, Opera, Safari etc.

#### Wireless Computer System Requirements

- Computer with a working 802.11b, 802.11g or 802.11n wireless adapter.

### 3.3 Connecting your 3G8WV

#### Step1 – Insert SIM card

Insert SIM card into the SIM Slot.

#### Step2 – Connect a computer

Connect one end of the Ethernet cable into a LAN Port on the back panel of the 3G8WV, and the other end into an available Ethernet port on the network adapter in the computer you will use to configure the unit.

#### Step3 – Plug in the power

Connect the power adapter to the port on the back panel of your 3G Router. Then plug the other end of the power adapter into a wall outlet or power strip.

#### Default Settings

##### LAN (Management)

- Static IP Address: 192.168.20.1
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.20.1

##### WAN (Internet)

- WAN mode: DHCP

##### Wireless

- SSID: NetComm Wireless
- Channel: 11
- Security: WEP, 64bit
- WEP Key: a1b2c3d4e5

##### Modem Access

- Username: admin
- Password: admin

## 4. Advanced Features

This section explains other features that you may want to enable depending on your application. Some features can add extra stability and error recovery. Other features are available to assist with integrating the 3G8WV with your application.



## 4.1 Login Procedure

1. Open your web browser (e.g. Internet Explorer/Firefox/Safari) and navigate to <http://192.168.20.1/>
2. Click Login and type "admin" (without quotes) in the Username and Password fields. Then click on Submit.

The screenshot shows the login interface for the NetComm 3G8WV router. At the top, there is a blue banner with the NetComm logo and the text '3G8WV - 3G 2-Port 11n Wi-Fi Router'. Below this is a green navigation bar with three buttons: 'Status', 'Login', and 'Log'. The main content area is titled 'Login' and contains a form with two input fields: 'User Name:' and 'Password:'. The 'User Name' field contains the text 'admin' and the 'Password' field contains five dots. Below the input fields are two buttons: 'Submit' and 'Clear'.

Note: admin is the default username and password for the unit.




## 4.2 Status

The status page provides system related information. It is shown on login to the 3G8WV, and can also be accessed by selecting Status from the top menu.

By default, the status page will show System Info, Local Network, WWAN, Connection Status and Ethernet Status.

To view either WAN, PPPoE or PPTP individually, click on their relevant buttons. To view them all, click on the All Status button.

[All Status](#)   [WAN](#)   [PPPoE](#)   [PPTP](#)

System Info			
Firmware Version	1.0.16.6 (Jan 13 2010)		
System Up Time	00 : 56 : 21		
Operation Mode	Gateway Mode		
Local Network			
Local IP Address	192.168.20.1		
Local Netmask	255.255.255.0		
MAC Address	00:60:64:25:E9:DE		
WWAN (WAN/3G)			
Operation Mode	AlwaysOn		
Interface	Status	Local	Remote
3G	up	10.250.19.124	10.64.64.65
Connection Status			
Module Name	HSPA USB MODEM		
Provider	Telstra Mobile		
APN	telstra.internet		
Service Type	UMTS		
Coverage	N/A		
IMEI	352347039084974		
Frequency	N/A		
Signal Strength (dBm)	-67 dBm (strong)		
SIM Status	SIM OK		
Ethernet Port Status			
 Full			
1		WAN	

## 4.3 Internet Settings

### 4.3.1 3G Internet Settings

This page allows you to setup your WWAN (Wireless Wide Area Network) connection. Enter the relevant settings as provided by your 3G provider.

Note For 3G WAN connection: The 3G connection fields may not be necessary for your connection. The information on this page will only be used when your service provider requires you to enter a User Name and Password to connect to the 3G network.


3G8WV - 3G 2-Port 11n Wi-Fi Router

Status
▶ Internet Settings
▶ Wireless Settings
▶ Firewall
▶ Administration

Internet Settings > 3G Internet Settings

### WWAN (3G) Settings

This page allows you to setup your WWAN (Wireless Wide Area Network) connection. Enter the relevant settings as provided by your 3G provider.

The unit will default to 'Auto APN Select Mode' if the APN field is blank. You may need to check the APN that is displayed on the Status page while the unit is connecting. If the default APN does not match your SIM account, then you will need to type in the correct APN manually or choose one from the drop down list below.

Auto-APN	<input type="text" value="Enable"/>
Interface Metric	<input type="text" value="20"/>
Operation Mode	<input type="text" value="Always On"/>
Always On Mode: Redial Period <input type="text" value="20"/> seconds	

### PIN Settings

SIM Status	SIM OK
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>

Internet Settings > 3G Internet Settings

**WWAN (3G) Settings**

This page allows you to setup your WWAN (Wireless Wide Area Network) connection. Enter the relevant settings as provided by your 3G provider.

The unit will default to 'Auto APN Select Mode' if the APN field is blank. You may need to check the APN that is displayed on the Status page while the unit is connecting. If the default APN does not match your SIM account, then you will need to type in the correct APN manually or choose one from the drop down list below.

Auto-APN	<input type="text" value="Disable"/>		
APN	<input type="text"/>	<input type="text" value="Australia"/>	<a href="#">Choose an APN here</a>
Dial	<input type="text" value="*99#"/> (default *99#)		
Authentication Type	<input type="text" value="CHAP"/>		
User Name	<input type="text"/>		
Password	<input type="text"/>		
Verify Password	<input type="text"/>		
Interface Metric	<input type="text" value="20"/>		
Operation Mode	<input type="text" value="Always On"/>		
	Always On Mode: Redial Period <input type="text" value="20"/> seconds		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

**PIN Settings**

SIM Status	SIM OK
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Name	Description
Auto-APN	Default is "enabled", 3G8WV will fill up the APN automatically by detecting your SIM card.
User Name	Enter your 3G Username
Password	Enter your 3G Password
Operation Mode	There are 3 Options as following:
'Always On'	Keeps the Internet connection alive, does not disconnect
'OFF'	Does not connect to the Internet

'Automatic 3G Backup'	The Automatic 3G Backup feature of the 3G8WV is designed to provide a backup 3G Internet connection in case your primary connection should fail. To use this feature, you will need both an Ethernet WAN connection (from an xDSL modem/ISDN/Satellite etc) and a 3G WAN connection.
PIN	Enter the Pin Code for your SIM card

Note: For current APN's of various providers, consult the Setting Up Your Router section of this user manual.

### 4.3.2 WAN

Select the WAN connection type suitable for your environment and configure parameters according to the selected connection type.

#### STATIC (fixed IP)

If your WAN connection uses a static IP address, please select Static IP Address and fill in the required information in the fields provided.

[Internet Settings > WAN](#)

**Wide Area Network (WAN) Settings**

This page allows you to setup your WAN Connection. First select the WAN connection type (Static, DHCP, PPPoE, PPTP), then enter the relevant settings as provided by your ISP.

WAN Connection Type:	STATIC (fixed IP) ▼
<b>Static Mode</b>	
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>
Primary DNS Server	139.130.4.4
Secondary DNS Server	203.50.2.71
MTU	1500
<b>MAC Clone</b>	
Enabled	Disable ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
<b>WAN Failover Backup</b>	
Automatic 3G Backup	Disable ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Name	Description
<b>IP Address:</b>	Type in the IP address assigned by your Internet Service Provider
<b>Subnet Mask:</b>	Type in the Subnet mask assigned by your Internet Service Provider
<b>Default Gateway:</b>	Type in the WAN Gateway assigned by your Internet Service Provider
<b>Primary/ Secondary DNS:</b>	Type in the DNS address assigned by your Internet Service Provider
<b>MAC Clone:</b>	Please input the MAC address of your computer here if your service provider only permits computers with a certain MAC address to access the Internet. If you are using the computer which used to connect to the Internet via a cable modem, you can simply press the 'Default' button to fill the MAC address field with the MAC address of your computer.

Click Apply to save the settings.

### DHCP (Auto config)

This connection will get the IP address from the Internet service provider. Choose this connection if you are connecting the router to a Cable Modem service. Leave everything as default unless instructed by your Internet Service Provider.

Internet Settings > WAN

**Wide Area Network (WAN) Settings**

This page allows you to setup your WAN Connection. First select the WAN connection type (Static, DHCP, PPPoE, PPTP), then enter the relevant settings as provided by your ISP.

WAN Connection Type: DHCP (Auto config) ▼

DHCP Mode

Hostname (optional)

MAC Clone

Enabled Disable ▼

Apply
Cancel

**WAN Failover Backup**

Automatic 3G Backup Disable ▼

Apply
Cancel

Name	Description
Host Name	Please input the host name of your computer. This is optional, and only required if your service provider asks you to do so.
Mac Clone	Please input the MAC address of your computer here if your service provider only permits computers with a certain MAC address to access the Internet. If you are using the computer which used to connect to Internet via a cable modem, you can simply press the 'Default'

	button to fill the MAC address field with the MAC address of your computer.
--	---

Click Apply to save the settings.

**PPPoE (ADSL)**

Most ADSL services use the PPP over Ethernet protocol. Use this if you connect your 3G Router to a bridged ADSL modem.

[Internet Settings > WAN](#)

**Wide Area Network (WAN) Settings**

This page allows you to setup your WAN Connection. First select the WAN connection type (Static, DHCP, PPPoE, PPTP), then enter the relevant settings as provided by your ISP.

WAN Connection Type: PPPoE

**PPPoE Mode**

User Name: pppoe\_user

Password: ●●●●●●●●

Verify Password: ●●●●●●●●

Operation Mode: Keep Alive

Keep Alive Mode: Redial Period 60 seconds

On demand Mode: Idle Time 5 minutes

**MAC Clone**

Enabled: Disable

Apply
Cancel

Name	Description
<b>Username/Password</b>	Type in your PPPoE account username and password.
<b>Operation Mode;</b> There are 3 options:	
<b>'Keep Alive'</b>	Keeps the Internet connection alive, does not disconnect.
<b>'On Demand'</b>	Only connects to the Internet when there's a connect attempt
<b>'Manual'</b>	Only connects to the Internet when the 'Connect' button on this page is pressed, and disconnects when the 'Disconnect' button is pressed.
<b>MAC Clone</b>	Please input the MAC address of your computer here if your service provider only permits computers with a certain MAC address to access the Internet. If you are using the computer which used to connect to the Internet via cable modem, you can simply press the 'Default' button to fill the MAC address field with the MAC address of your computer.

Click Apply to save the settings.

**PPTP**

Internet Settings > WAN

**Wide Area Network (WAN) Settings**

This page allows you to setup your WAN Connection. First select the WAN connection type (Static, DHCP, PPPoE, PPTP), then enter the relevant settings as provided by your ISP.

WAN Connection Type: PPTP ▼

**PPTP Mode**

Server IP:

User Name:

Password:

Address Mode: Static ▼

IP Address:

Subnet Mask:

Default Gateway:

Operation Mode: Keep Alive ▼

Keep Alive Mode: Redial Period  seconds

On demand Mode: Idle Time  minutes

**MAC Clone**

Enabled: Disable ▼

Name	Description
Server IP	Type in the server IP address assigned by your Internet Service Provider.
User Name/Password	Type in the username and password assigned by your provider.
Address Mode	Select Dynamic if your service uses a DHCP server, or select Static and type in the IP address, Subnet Mask and Default Gateway assigned by your Internet Service Provider.
<b>Operation Mode</b>	
'Keep Alive'	Keeps the Internet connection alive, does not disconnect.
'On Demand'	Only connects to Internet when there's a connect attempt
'Manual'	Only connects to the Internet when the 'Connect' button on this page is pressed, and disconnects when the 'Disconnect' button is pressed.
Mac Clone	Please input the MAC address of your computer here if your service provider only permits computers with a certain MAC address to access the Internet. If you are using



	the computer which used to connect to the Internet via a cable modem, you can simply press the 'Default' button to fill the MAC address field with the MAC address of your computer.
--	--

Click Apply to save the settings.

**WAN Failover Backup**

The WAN Failover Backup feature of the 3G8WV is designed to provide a backup 3G Internet connection in case your primary connection should fail. To use this feature, you will need both an Ethernet WAN connection (from an xDSL modem/ISDN/Satellite etc) and a 3G WAN connection.

To set up WAN failover on your 3G Router, first tick "Enable automatic 3G backup", then fill in the fields that appear.

WAN Failover Backup	
Automatic 3G Backup	<input type="checkbox"/> Enable
Internet Host	<input type="text" value="www.netcomm.com.au"/>
APN	<input type="text"/>
Dial	<input type="text" value="*99#"/>
Authentication Type	<input type="checkbox"/> CHAP
User Name	<input type="text"/>
Password	<input type="password"/>
Verify Password	<input type="password"/>
Interface Metric	<input type="text" value="20"/>
Always On Mode: Redial Period	<input type="text" value="60"/> Seconds
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Name	Description
<b>Internet Host:</b>	Enter an Internet address here to check the Internet connection
<b>APN:</b>	Enter the APN for your 3G
<b>User Name:</b>	Enter your 3G username
<b>Password:</b>	Enter your 3G password

Click Apply to save the settings.

**4.3.3 LAN**

Local Area Network (LAN) Settings	
This page allows you to configure the LAN IP address, subnet mask and DHCP settings of your 3G Router.	
<b>LAN Setup</b>	
IP Address	<input type="text" value="192.168.20.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
LAN 2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
LAN2 IP Address	<input type="text"/>
LAN2 Subnet Mask	<input type="text"/>
MAC Address	00:60:64:25:E9:DE
DHCP Type	Server <input type="button" value="v"/>
Start IP Address	<input type="text" value="192.168.20.100"/>
End IP Address	<input type="text" value="192.168.20.254"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Primary DNS Server	<input type="text" value="192.168.20.1"/>
Secondary DNS Server	<input type="text" value="192.168.20.1"/>
Default Gateway	<input type="text" value="192.168.20.1"/>
Lease Time	<input type="text" value="86400"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
802.1d Spanning Tree	Disable <input type="button" value="v"/>
LLTD	Disable <input type="button" value="v"/>
IGMP Proxy	Disable <input type="button" value="v"/>
UPnP	Enable <input type="button" value="v"/>

Name	Description
<b>IP Address:</b>	The local IP address of this device.
<b>Subnet Mask:</b>	The subnet mask of the local IP address
<b>LAN 2:</b>	Used to configure a secondary LAN IP Address
<b>MAC Address:</b>	The LAN MAC address of your 3G Router
<b>DHCP Type:</b>	Please leave this set to 'Enable' unless you have another DHCP server on the same network.
<b>Primary DNS/Secondary DNS:</b>	(Optional) This feature allows you to manually assign DNS Servers
<b>Lease Time:</b>	DHCP lease times of the DHCP clients of your 3G Router.

Click Apply to save the settings.

#### 4.3.4 Advanced Routing

This page allows you to configure static and dynamic routing rules for your 3G Router.

Internet Settings > Advanced Routing

**Advanced Routing Settings**

This page allows you to configure static and dynamic routing rules for your 3G Router.

**Add a routing rule**

Destination	<input type="text"/>
Range	Host <input type="button" value="v"/>
Gateway	<input type="text"/>
Interface	LAN <input type="button" value="v"/> <input type="text"/>
Comment	<input type="text"/>

**Current Routing table in the system:**

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	10.64.64.65	255.255.255.255	0.0.0.0	5	0	0	0	ppp1(ppp1)	
2	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)	
3	192.168.20.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)	
4	239.0.0.0	255.0.0.0	0.0.0.0	1	0	0	0	LAN(br0)	
5	0.0.0.0	0.0.0.0	0.0.0.0	1	0	0	0	ppp1(ppp1)	

**Dynamic Routing Settings**

**Dynamic Routing Protocol**

RIP	Disable <input type="button" value="v"/>
-----	--

### Advanced Routing – Static

Static Routing allows computers that are connected to your 3G Router to communicate with computers on another LAN segment which are connected to it via another router. To set a rule, you need to specify the following:

- Destination
- Subnet mask
- Gateway
- Interface

### Advanced Routing – Dynamic

Dynamic Routing uses the RIP protocol to allow the 3G Router to adapt to changes in the network. RIP enables the device to determine the best route for each packet based on the “hop count” or number of hops between Source and Destination. To enable Dynamic Routing, select Enable from the drop box and click Apply.

#### 4.3.5 DHCP Client

This page allows you to view the current DHCP client of your 3G Router.

## 5.0 Wireless Setting

### 5.1 Basic

This page allows you to define the basic wireless settings for this device such as the SSID and channel.

[Wireless Settings > Basic](#)

Basic Wireless Settings	
This page allows you to define the basic wireless settings for this device such as the SSID and channel.	
<b>Wireless Network</b>	
Radio On/Off	<input checked="" type="radio"/> On <input type="radio"/> Off
Network Mode	11b/g/n mixed mode ▼
Network Name(SSID)	NetComm Wireless
Frequency (Channel)	2437MHz (Channel 6) ▼
<b>Wireless Distribution System(WDS)</b>	
WDS Mode	Disable ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Radio On/Off: On by default. Changing this option to Off will turn off the wireless feature on the unit and you will not be able to connect to your 3G Router wirelessly.
- Network Mode: You can select which wireless standards are able to connect to your wireless network:
  - 11b/g mixed mode: Both 802.11b and 802.11g wireless devices are in your network.
  - 11b only: Select this if all of your wireless clients are 802.11b.
  - 11g only: Select this if all of your wireless clients are 802.11g.
  - 11a only: Select this if all of your wireless clients are 802.11a.
  - 11a/n mixed mode: Both 802.11a and 802.11n wireless devices are in your network.
  - 11b/g/n mixed mode: Select this if 802.11b and 802.11g and 802.11n wireless devices are in your network.
- Network Name (SSID): The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless device so that you can easily connect from your wireless clients. This field is case sensitive and can be up to 32 characters. You should change the default SSID for added security.
- Frequency (Channel): This setting configures the frequency that the Wireless Radio uses for wireless connectivity. Select one channel that you wish to use from the drop down list.
- WDS Mode: WDS (Wireless Distribution System), is a system that enables the wireless interconnection of access points, and allows a wireless network to be expanded using multiple access points without a wired backbone to link them. Each WDS Access Point needs to be set with the same channel and encryption type.

Click Apply to save the settings.

## 5.2 Advanced

This page allows you to modify the advanced wireless settings for your 3G Router. These settings should not be changed unless you are aware of what effect they will have.

Wireless Settings > Advanced

Advanced Wireless Settings	
This page allows you to modify the advanced wireless settings for your 3G Router. These settings should not be changed unless you are aware of what effect they will have.	
<b>Advanced Wireless</b>	
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Country Code	AU (Australia)
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	00:60:64:29:44:B1
Multiple SSID1	<input type="text"/>
Multiple SSID2	<input type="text"/>
Multiple SSID3	<input type="text"/>
Multiple SSID4	<input type="text"/>
Multiple SSID5	<input type="text"/>
Multiple SSID6	<input type="text"/>
Multiple SSID7	<input type="text"/>
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>Wi-Fi Multimedia</b>	
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DLS Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Parameters	<a href="#">WMM Configuration</a>
<b>Multicast-to-Unicast Converter</b>	
Multicast-to-Unicast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Other</b>	
HT TxStream	2
HT RxStream	2
<b>HT Physical Mode</b>	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> Long <input checked="" type="radio"/> Auto
MCS	Auto
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2412MHz (Channel 1)
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- **Beacon Interval:** Interval of time the wireless router broadcasts a beacon, used to synchronize the wireless network.

- **Data Beacon Rate (DTIM):** Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages
- **Fragment Threshold:** This specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
- **RTS Threshold:** When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
- **AP Isolation:** This feature allows you to isolate clients on your wireless network. To enable communication between the wireless clients connected to your 3G Router, select Disabled. To cut the communication between the wireless clients, please choose Enabled.
- **TX Power:** This determines the output power of the antenna
- **WMM Capable:** WMM (Wi-Fi MultiMedia) if enabled supports QoS for experiencing better audio, video and voice in applications
- **WMM Parameters:** Click on the WMM Configuration button to configure the WMM parameters
- **Broadcast Network Name (SSID):** Select 'Disabled' to hide the SSID of your 3G Router. If disabled, other people will not be able scan and detect this product's SSID.

Click Apply to save the settings.

### 5.3 Security

This page allows you to configure the wireless security for your 3G Router. Setting up sufficient wireless security can prevent unauthorised access to your wireless network.

Wireless Settings > Security

Wireless Security Settings			
This page allows you to configure the wireless security for your 3G Router. Setting up sufficient wireless security can prevent unauthorised access to your wireless network.			
<b>Select SSID</b>			
SSID choice	NetComm Wireless ▾		
<b>"NetComm Wireless"</b>			
Security Mode	WEPAUTO ▾		
<b>Wire Equivalence Protection (WEP)</b>			
Default Key	Key 1 ▾		
WEP Keys	WEP Key 1 :	a1b2c3d4e5	Hex ▾
	WEP Key 2 :		Hex ▾
	WEP Key 3 :		Hex ▾
	WEP Key 4 :		Hex ▾
<b>Access Policy</b>			
Policy	Disable ▾		
Add a MAC address to the allow/block list:			
Apply		Cancel	

- SSID Choice: Select the SSID on which to configure the security settings
- Security Mode: Select the security mode for the wireless network. See below for more information
- Access Policy: This feature allows MAC Address Control, which prevents unauthorized clients from accessing your wireless network. Select whether to allow/block users on the policy list, and add their MAC addresses to the list on the format XX:XX:XX:XX:XX:XX

Click Apply to save the settings.

### Security Mode

You may choose from the following wireless security options: Disabled, Open, Shared, WEPAUTO, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK-WPA2-PSK, WPA1-WPA2 or 802.1x.

- WEP: WEP (Wired Equivalent Privacy) is enabled by default to help prevent against unwanted wireless users accessing your 3G Router. The default 64 bit Hexadecimal WEP key is: a1b2c3d4e5



Wireless Settings > Security

Wireless Security Settings	
This page allows you to configure the wireless security for your 3G Router. Setting up sufficient wireless security can prevent unauthorised access to your wireless network.	
<b>Select SSID</b>	
SSID choice	NetComm Wireless ▾
<b>"NetComm Wireless"</b>	
Security Mode	WEPAUTO ▾
<b>Wire Equivalence Protection (WEP)</b>	
Default Key	Key 1 ▾
WEP Keys	WEP Key 1 : <input type="text" value="a1b2c3d4e5"/> <input type="text" value="Hex"/> ▾
	WEP Key 2 : <input type="text"/> <input type="text" value="Hex"/> ▾
	WEP Key 3 : <input type="text"/> <input type="text" value="Hex"/> ▾
	WEP Key 4 : <input type="text"/> <input type="text" value="Hex"/> ▾
<b>Access Policy</b>	
Policy	Disable ▾
Add a MAC address to the allow/block list:	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- WPA/WPA2: WPA (Wi-Fi Protected Access) authentication is suitable for enterprises. It must be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. It can provide stronger encryption and authentication solution than non WPA modes.

Wireless Settings > Security

Wireless Security Settings	
This page allows you to configure the wireless security for your 3G Router. Setting up sufficient wireless security can prevent unauthorised access to your wireless network.	
<b>Select SSID</b>	
SSID choice	NetComm Wireless ▼
<b>"NetComm Wireless"</b>	
Security Mode	WPA ▼
<b>WPA</b>	
WPA Algorithms	<input checked="" type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIPAES
Key Renewal Interval	3600 seconds
<b>Radius Server</b>	
IP Address	<input type="text"/>
Port	1812
Shared Secret	<input type="text"/>
Session Timeout	0
Idle Timeout	<input type="text"/>
<b>Access Policy</b>	
Policy	Disable ▼
Add a MAC address to the allow/block list:	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- WPA-PSK/WPA2-PSK: A newer type of security is WPA-PSK (TKIP) and WPA2-PSK (AES). This type of security gives a more secure network compare to WEP. Use TKIP Encryption Type for WPA-PSK and AES for WPA2-PSK. After that, please enter the key in the Passphrase field. The key needs to be more than 8 characters and less than 63 characters and it can be any combination of letters and numbers. Please note that the configuration for WPA-PSK and WPA2-PSK is identical.

Wireless Settings > Security

Wireless Security Settings	
This page allows you to configure the wireless security for your 3G Router. Setting up sufficient wireless security can prevent unauthorised access to your wireless network.	
<b>Select SSID</b>	
SSID choice	NetComm Wireless ▾
<b>"NetComm Wireless"</b>	
Security Mode	WPA-PSK ▾
<b>WPA</b>	
WPA Algorithms	<input checked="" type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIPAES
Pass Phrase	1234567890
Key Renewal Interval	3600 seconds
<b>Access Policy</b>	
Policy	Disable ▾
Add a MAC address to the allow/block list:	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- 802.1x: In order to use 802.1X security, you need to have a RADIUS server on your network that will act as the authentication server. Please type in the details for your RADIUS server in the fields required.

Wireless Settings > Security

Wireless Security Settings	
This page allows you to configure the wireless security for your 3G Router. Setting up sufficient wireless security can prevent unauthorised access to your wireless network.	
<b>Select SSID</b>	
SSID choice	NetComm Wireless ▼
<b>"NetComm Wireless"</b>	
Security Mode	802.1X ▼
<b>802.1x WEP</b>	
WEP	<input type="radio"/> Disable <input type="radio"/> Enable
<b>Radius Server</b>	
IP Address	<input type="text"/>
Port	1812
Shared Secret	<input type="text"/>
Session Timeout	0
Idle Timeout	<input type="text"/>
<b>Access Policy</b>	
Policy	Disable ▼
Add a MAC address to the allow/block list:	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Note: After configuring wireless security, you also need to configure your wireless adapter to use the same security settings before you can connect wirelessly. Not all wireless adapters support WPA-PSK/WPA2-PSK/WPA/WPA2 security; please refer to your wireless adapter user guide for more details. It is strongly recommended to set up a simple wireless security such as WEP 64bit or WPA (when the wireless client supports WPA) in order to secure your network.

### 5.4 WPS

WPS is the simplest way to establish a connection between wireless clients and your 3G Router. This method removes the need to manually select the encryption mode and fill in the passphrase. You only need to press a button on both wireless client and wireless router, and the WPS will do the rest for you. The wireless router supports two types of WPS:

- WPS via Push Button – you have to push a specific button on the wireless client or in your wireless client utility to start the WPS mode, and switch the wireless router to WPS mode. You can simply push the WPS button of the wireless router, or click the ‘Start to Process’ button in the web configuration interface.
- WPS via PIN code – you have to know the PIN code of the wireless client and switch it to WPS mode, then input the wireless client PIN to the wireless router web interface.

Wireless Settings > WPS

**WPS**

page allows you to configure WPS (Wi-Fi Protected Setup) for your 3G Router. WPS provides a simple method to establish a secure wireless connection between wireless clients and your 3G Router. Once WPS is enabled, you will only need to press a button (Push Button Mode), or enter a PIN (PIN Mode) on both the wireless client and your 3G Router to enable a secure connection between the two.

**WPS Config**

WPS:

**WPS Summary**

WPS Current Status:	Idle
WPS Configured:	Yes
WPS SSID:	NetComm Wireless
WPS Auth Mode:	Open
WPS Encryp Type:	None
WPS Default Key Index:	1
WPS Key(ASCII)	
AP PIN:	20633806

**WPS Progress**

WPS mode:  PIN  PBC

PIN:

**WPS Status**

WPS: Idle

- **WPS:** Use the dropbox to either enable or disable the WPS function.
- **WPS Current Status:** If the wireless security (encryption) function of this wireless router is properly set, you will see a 'Success' message here. Otherwise, you will see 'Idle'.
- **WPS SSID:** This is the network broadcast name (SSID) of the router.
- **WPS Auth Mode:** It shows the active authentication mode for the wireless connection.
- **WPS PIN:** This is the WPS PIN code of the wireless router. You may need this information when connecting to other WPS-enabled wireless devices.
- **WPS Mode:** Select either PIN or PBC.

## 5.5 Station List

The Station List shows the wireless clients currently associated with your 3G Router.

[Wireless Settings > Station List](#)

Station List							
This page allows you to view a list of the wireless clients that are currently associated with your 3G Router.							
Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
00:1F:5B:6A:B3:91	1	1	0	7	20M	0	0

## 6.0 Firewall

### 6.1 Mac/IP/Port Filtering

This page allows you to setup MAC, IP and port filtering rules to protect your network from malicious activity. The filtering rules can be used to either allow or block certain users and/or ports from accessing the Internet.

Firewall > MAC/IP/Port Filtering

**MAC/IP/Port Filtering Settings**

This page allows you to setup MAC, IP and port filtering rules to protect your network from malicious activity. The filtering rules can be used to either allow or block certain users and/or ports from accessing the Internet.

**Basic Settings**

MAC/IP/Port Filtering Disable ▾

Default Policy – The packet that don't match with any rules would be: Dropped. ▾

**MAC/IP/Port Filter Settings**

MAC address

Dest IP Address

Source IP Address

Protocol None ▾

Dest Port Range  -

Source Port Range  -

Action Accept ▾

Comment

(The maximum rule count is 32.)

**Current MAC/IP/Port filtering rules in system:**

No.	MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
Others would be dropped									-

**Basic Settings**

- MAC/IP/Port Filtering: Select Enable to enable MAC/IP/Port Filtering
- Default Policy: Select whether packets that do not match any rules are accepted or dropped

**MAC/IP/Port Filtering Settings**

- MAC Address: MAC address of a local computer
- Dest IP Address: Destination IP Address for the filter rule
- Source IP Address: Source IP Address for the filter rule
- Protocol: Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default "TCP&UDP" setting
- Dest Port Range: Destination Port Range of the filter rule
- Source Port Range: Source Port Range of the filter rule
- Action: Either accept or drop the packet that matches the rule
- Comment: Add a comment to identify the rule (optional)

Click Apply to save the settings.

**6.2 Port Forwarding**

This page allows you to configure port forwarding rules to allow remote users to access services such as Web or FTP on your local computers. This allows you to redirect a particular port number (from the Internet/WAN port) to a particular LAN IP address.



Firewall > Port Forwarding

**Port Forwarding Settings**

This page allows you to configure port forwarding rules to allow remote users to access services such as Web or FTP on your local computers. This allows you to redirect a particular port number (from the Internet/WAN port) to a particular LAN IP address.

**Virtual Server Settings**

Virtual Server Settings	<input type="button" value="Disable"/> ▾
IP Address	<input style="width: 90%;" type="text"/>
Port Range	<input style="width: 45%;" type="text"/> - <input style="width: 45%;" type="text"/>
Protocol	<input type="button" value="TCP&amp;UDP"/> ▾
Comment	<input style="width: 90%;" type="text"/>

(The maximum rule count is 32.)

**Current Virtual Servers in system:**

No.	IP Address	Port Range	Protocol	Comment
<input type="button" value="Delete Selected"/> <input type="button" value="Reset"/>				

- Virtual Server Settings: Enable/Disable port forwarding
- IP Address: The LAN IP address that the public port number packet will be sent to
- Port Range: The public port numbers to be sent to the specific LAN IP address
- Protocol: Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it as the default “TCP&UDP” setting
- Comment: Add a comment to identify the rule (optional)

Click Apply to save the settings.

### 6.3 DMZ

If you have a client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open up the firewall restrictions to allow unrestricted two-way Internet access by defining a DMZ Host.

The DMZ function allows you to re-direct all packets going to your WAN port IP address, to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

Firewall > DMZ

DMZ Settings	
This page allows you to nominate a computer on your network that can be accessed from the Internet regardless of any port forwarding or firewall settings.	
DMZ Settings	Disable ▾
DMZ IP Address	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

- DMZ Settings: Enable/disable DMZ.
- DMZ IP Address: Fill-in the IP address of a particular host in your LAN Network that will receive all the packets originally going to the WAN port/Public IP address of your 3G Router.

Click Apply to save the above configurations.

## 6.4 System Security

This page allows you to improve the security of your 3G Router through the SPI firewall and remote access settings.

Firewall > System Security

System Security Settings	
page allows you to improve the security of your 3G Router through the SPI firewall and remote access settings.	
<b>Remote management</b>	
Remote management (via WAN)	Deny ▾
<b>Ping form WAN Filter</b>	
Ping form WAN Filter	Disable ▾
<b>Stateful Packet Inspection (SPI)</b>	
SPI Firewall	Disable ▾
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

- Remote Management (via WAN): Enable/Disable remote management on the WAN interface.
- Deny ping from WAN interface: Select Enable to deny ICMP packets received on the WAN interface. Otherwise, select Disable to allow ICMP packets received on the WAN interface.

- SPI Firewall: Enable/Disable the SPI (Stateful Packet Inspection) firewall to improve the security of your 3G Router.

Click Apply to save the settings.

## 6.5 Content Filtering

This page allows you to configure content, URL and host filters to restrict improper content access from LAN computers

[Firewall > Content Filtering](#)

Content Filter Settings	
This page allows you to configure content, URL and host filters to restrict improper content access from LAN computers.	
Webs Content Filter	
Filters:	<input type="checkbox"/> Proxy <input type="checkbox"/> Java <input type="checkbox"/> ActiveX
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	
URL Filter Settings	
Current Webs URL Filters:	
No	URL
<input type="button" value="Delete"/> <input type="button" value="Reset"/>	
Add a URL filter:	
URL:	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Reset"/>	
Host Filter Settings	
Current Website Host Filters:	
No	Host(Keyword)
<input type="button" value="Delete"/> <input type="button" value="Reset"/>	
Add a Host(keyword) Filter:	
Keyword	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

- Web Content Filter: Tick the boxes to enable Proxy, Java or ActiveX content filtering
- URL Filter: Block access to a website by entering its full URL address.
- Host Filter: Block access to block access to certain websites by entering a keyword

Click Apply to save the settings.

## **7.0 Administration**

### **7.1 Management**

This page allows you to configure administrator system settings including the administrator username and password, NTP settings, and DDNS settings.

Administration > Management

System Management	
This page allows you to configure administrator system settings including the administrator username and password, NTP settings, and DDNS settings.	
Language Settings	
Select Language	English ▾
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
Administrator Settings	
Account	admin
Password	••••
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
NTP Settings	
Current Time	Sat Jan 1 02:17:32 UTC 2000 <input type="button" value="Sync with host"/>
Time Zone:	(GMT-11:00) Midway Island, Samoa ▾
NTP Server	0.netcomm.pool.ntp.org <small>ex: time.nist.gov                      ntp0.broad.mit.edu                      time.stdtime.gov.tw</small>
NTP synchronization(hours)	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
Green AP	
Duration	Action
00 ▾ : 00 ▾ ~ 00 ▾ : 00 ▾	Disable ▾
00 ▾ : 00 ▾ ~ 00 ▾ : 00 ▾	Disable ▾
00 ▾ : 00 ▾ ~ 00 ▾ : 00 ▾	Disable ▾
00 ▾ : 00 ▾ ~ 00 ▾ : 00 ▾	Disable ▾
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
DDNS Settings	
Dynamic DNS Provider	None ▾
Account	<input type="text"/>
Password	<input type="text"/>
DDNS	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Select Language: Select a language for the web interface.
- Administrator Settings (account/password): Configure a new administrator username and password.

- **NTP Settings:** The NTP (Network Time Protocol) settings allow your router to synchronise its internal clock with the global Internet Time. These settings will affect functions such as System Log entries and Firewall settings.
- **DDNS:** DDNS (Dynamic Domain Name Service) allows you to map the static domain name to a dynamic IP address. To use this features, you must sign up for an account from a DDNS service provider. This router supports DynDNS, TZO and other common DDNS service providers.

Click Apply to save the settings.

## 7.2 Upload Firmware

This page allows you to upgrade the router’s firmware. To upgrade the firmware of your 3G Router, you need to download the firmware file to your local hard disk, and then click the Browse button to locate the firmware file on your computer.

Once you have selected the new firmware file, click Apply to start the upgrade process.

[Administration](#) > [Upload Firmware](#)

**Upload Firmware**

This page allows you to upgrade your 3G Routers firmware. Click on Browse to locate the firmware file to be used for the upgrade. **Please note that it takes approximately 3 minutes for the firmware to be upgraded. DO NOT turn off your 3G Router during the firmware upgrade process.**

**Update Firmware**

Location:

## 7.3 Setting Manager

This page allows you to import/export the system settings, reset your 3G Router to factory defaults, or reboot your 3G Router.

Administration > Settings Manager

**Settings Management**

This page allows you to import/export the system settings, or reset your 3G Router to factory defaults.

---

**Export Settings**

---

**Import Settings**

Settings file location:

---

**Load Factory Defaults**

---

**Reboot Router**

## 7.4 Statistics

This page allows you to view the LAN, WAN and wireless statistics of your 3G Router.

Administration > Statistics

Statistics	
This page allows you to view the LAN, WAN and wireless statistics of your 3G Router.	
<b>Memory</b>	
Memory total:	13112 kB
Memory left:	2064 kB
<b>WAN/LAN</b>	
WAN Rx packets:	0
WAN Rx bytes:	0
WAN Tx packets:	888
WAN Tx bytes:	521328
LAN Rx packets:	16573
LAN Rx bytes:	1299526
LAN Tx packets:	11772
LAN Tx bytes:	2262235
<b>All interfaces</b>	
Name	lo
Rx Packet	17
Rx Byte	2995

## 7.5 System Log

All important system events are logged. You can use this function to check the event log of your 3G Router.

[Administration > System Log](#)

**System Log**

**System Log**

```
Jan 1 02:00:20 (none) syslog.info syslogd started: BusyBox v1.12.1
Jan 1 02:00:20 (none) user.notice kernel: klogd started: BusyBox v1.12.1 (2009-02-25 12:42:22 EST)
Jan 1 02:00:23 (none) user.debug kernel: ra0: no IPv6 routers present
Jan 1 02:00:23 (none) user.debug kernel: eth2.2: no IPv6 routers present
Jan 1 02:00:24 (none) user.debug kernel: br0: no IPv6 routers present
Jan 1 02:00:29 (none) user.info kernel: br0: topology change detected, propagating
Jan 1 02:00:29 (none) user.info kernel: br0: port 2(eth2.1) entering forwarding state
Jan 1 02:00:29 (none) user.info kernel: br0: topology change detected, propagating
Jan 1 02:00:29 (none) user.info kernel: br0: port 1(ra0) entering forwarding state
Jan 1 02:10:46 (none) user.warn kernel: Rcv Wcid(1) AddBAReq
Jan 1 02:10:46 (none) user.warn kernel: Start Seq = 00000008
```



## 8.0 Legal & Regulatory Information

This manual is copyright. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the Copyright Act, no part may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Limited. NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product.

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

NetComm is a registered trademark of NetComm Limited.

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

### 8.1 Customer Information

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

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

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

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

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

### 8.2 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 radiated 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.

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

Cet appareil numérique de la classe B est conforme à 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 4.35 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.