

## **3G9W** – HSPA 7.2 Mbps Wi-Fi Router User Guide



Download from Www.Somanuals.com. All Manuals Search And Download.



# Thank you for purchasing NetComm's HSPA Wi-Fi Router

## Preface

The purpose of this manual is to provide you detailed information on the installation, operation and application of your HSPA 7.2Mbps Wi-Fi Router.

## Important Notice and Safety Precaution

- Before servicing or disassembling this equipment, always disconnect all power or telephone lines from the device.
- 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 20 cm from human body.
- The operation of this device may affect medical electronic devices, such as hearing aids and peacemakers.

# Table of Contents

1 – Introduction	
1.1 Features	
1.2 Package Contents	
1.3 LED Indicators	
1.4 Rear Panel	9
2 Quick Setup	11
2 – QUICK SELUP	
3 – Web user Interface	13
3.1 Default Settings	
3.2 Transmission Control Protocol/Internet Protocol (TCP/IP) Settings	14
3.3 Login Procedure	15
3.4 Web User Interface Homepage	
1 - 36 Settings	10
1 1 3G Service Satur	10
	20
1.2 PIN Configuration	
4.2 1 PIN Code Protection	
4.2.2 PIN Code Change	
5 – Wireless	
5.1 Setup	
5.2 Security	
5.3 Configuration	
5.4 Media Access Control (MAC) Filter	
5.5 Wireless Bridge	
5.6 Station into	
6 - Management	
6.1 Device Settings	
6.1.1 Configuration Backup	
6.1.2 Update Settings	
6.1.3 Restore Default	
6.1.4 Update Firmware	



6.2	Access Control	
	6.2.1 Services	
	6.2.2 IP Addresses	40
	6.2.3 Passwords	40
6.3	Simple Network Time Protocol (SNTP)	41
6.4	Save and Reboot	42
7 – Advance	ed setup	
7.1	Local-Area Network (LAN)	45
7.2	Network Address Translation (NAT)	46
	7.2.1 Port Forwarding	46
	7.2.2 Port Triggering	48
	7.2.3 Demilitarized Zone (DMZ) Host	49
7.3	Security	50
	7.3.1 IP Filtering	50
	7.3.2 Parental Control	52
7.4	Routing	53
	7.4.1 Default Gateway	53
	7.4.2 Static Route	54
	7.4.3 Dynamic Route	55
7.5	Domain Name System (DNS)	56
	7.5.1 Domain Name System (DNS) Server	56
	7.5.2 Dynamic Domain Name System (DNS)	57
8 – Status .		59
8.1	Diagnostics	60
8.2	System Log	61
8.3	3G Status	63
8.4	Statistics	66
	8.4.1 LAN Statistics	66
	8.4.2 3G Statistics	67
8.5	Route	68
8.6	Address Resolution Protocol (ARP)	69
8.7	Dynamic Host Configuration Protocol (DHCP)	69
Appendix A	: Command Line Interface (CLI) Commands Via Telnet	71

Introduction



# Introduction



With the increasing popularity of the 3G standard worldwide, this HSPA 7.2Mbps Wi-Fi Router provides you with triple-band coverage through expanding cellular networks throughout the world.

By following the simple step-by-step instructions found on the Connection Manager USB key, you can share your connection with multiple wireless and wired devices using the 3G network.

Integrating a Sierra Wireless HSPA module, this Router downloads turbo speeds of up to 7.2Mbps.

This Router also provides state-of-the-art security features such as Wi-Fi Protected Access (WPA) data encryption, Firewall and Virtual Private Networks (VPN) pass through.

## 1.1 Features

- This HSPA 7.2Mbps Wi-Fi Router allows you to share your 3G connection with multiple wireless or wired devices
- Provides you with worldwide coverage through triple-band HSUPA/HSDPA/UMTS (850 / 1900 / 2100 MHz), quad-band EDGE/GSM (850 / 900 / 1800 / 1900 MHz)
- Embedded multi-mode HSUPA/HSDPA/UMTS/EDGE/GPRS/GSM module
- Integrated 802.11g/54Mbps AP (backward compatible with 802.11b)
- Wi-Fi Protected Access (WPA)/ Wi-Fi 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 Universal Plug and Play (UPnP) and Internet Group Management Protocol (IGMP) snooping
- 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

## 1.2 Package Contents

Your package contains the following:

- 3G9W HSPA 7.2Mbps Wi-Fi Router
- Printed Quick Start Guide
- User Guide On CD
- Ethernet Cable
- 2 x 3G Antenna
- 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.

**HELEONING 3G9W** HSPA 7.2Mbps Wi-Fi Router  $\bullet_{\mathcal{P}^{OH^{O}}} \bullet_{\mathcal{I}^{H^{O}}} \bullet_{\mathcal{I}^{H^{O}}} \bullet_{\mathcal{I}^{H^{O}}} \bullet_{\mathcal{I}^{OH^{O}}} \bullet_{\mathcal{I}^{O}} \bullet_{\mathcal{I}^{O}} \bullet_{\mathcal{I}^{OH^{O}}} \bullet_{\mathcal{I}^{OH^{O$ 

LED	Color	Mode	Description		
POWER	Green	On	Power on		
		Off	Power off		
LAN 1~4 Green On			wered device connected to the associated port (includes devices with wake-on- N capability where a slight voltage is supplied to an Ethernet connection)		
		Off	No activity, modem powered off, no cable or no powered device connected to the associated port		
		Blink	LAN activity present (traffic in either direction)		
Wi-Fi	Fi Green On		The wireless module is ready.		
		Off	The wireless module is not installed.		
		Blink	Data being transmitted or received over Wi-Fi.		
Internet	Green	Blink	Internet connection established.		
		Off	No connection to the internet or router powered off		
3G	Green	On	Internet connection established.		
	Blink		Connecting with UMTS cellular station		
		Off	No connection with UMTS cellular station, no activity or router powered off.		
2G	Green	On	Internet connection established.		
		Blink	Connecting to an EDGE, GPRS or GSM cellular station		
		Off	No connection with EDGE, GPRS or GSM cellular station, no activity or router powered off.		
Low	Green	On	Low signal strength		
		Off	No activity, router powered off or on other signal strength		
Med	Green	On	Medium signal strength		
		Off	No activity, router powered off or on other signal strength		
High	Green	On	High signal strength		
		Off	No activity, router powered off or on other signal strength		

NOTE: The six LEDs on the right side of the front panel display (Internet, 36, 26, Low, Med, High) will cycle on and off if PIN code protection is activated. In this case, you should consult section 4.2.1 PIN Code Protection (page 21) for further instructions.

#### Download from Www.Somanuals.com. All Manuals Search And Download.

## 1.4 Rear Panel

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



- (7) Four RJ-45 Ethernet LAN ports
- (8) 2dBi wireless Antenna (fixed)

## Quick Setup

Download from Www.Somanuals.com. All Manuals Search And Download.

# **Quick Setup**

#### 21 Setup Procedure

These steps explain how to quickly setup your router:

- 1: Attach the two 3G antennas provided to the ports marked Main and AUX on the back of the router. The antennas should be screwed in a clockwise direction.
- 2: Insert your SIM card (until you hear a click) into the USIM slot at the back of the Router.
- 3: Connect the yellow networking cable to one of the yellow ports found at the back of the Router.
- 4: Connect the other end of the yellow networking cable to the port on your computer.
- 5: Connect the power adapter to the Power socket on the back of the Router.
- 6: Plug the power adapter into the wall socket and press the power button into the ON position (in).
- Configure the router through the Web User Interface (WUI). 7:

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

8: Save the router configuration and reboot (see section 6.4).



## Web User Interface

Download from Www.Somanuals.com. All Manuals Search And Download.

# 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 5.0 or later).

## 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
- WAN IP address: none
- 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 DefaultSettings screen.



## 3.2 TCP/IP Settings DHCP Mode

When your Router powers up, the Dynamic Host Configuration Protocol DHCP server (on the device) will start automatically. To set your PC for DHCP mode, check the Internet Protocol properties of your Local Area Connection. You can set your PC to DHCP mode by selecting Obtain an IP address automatically in the dialog box shown below.

You can this capa for the a	get IP settings as bility. Otherwise,	signed autor	natically if	our ne	twork :	upports
	the obtaine to the	tings.	raan joor i	heewori	c admin	istrator
	an an IP address	i automatica	ly.			
- D Uge	the following P	address:				
P add	hess:					
Spre	e mesk:					
Defai	k gaberray:					
	tain DNS server a	ódress autor	natically			
OUse	the following DN	S server add	resses:			
Pola	red DfG perver (					
Altern	ata DNS server:					

### STATIC IP Mode

To configure your Router manually, your PC must have a static IP address within the Router's subnet. The following steps show how to configure your PC IP address using subnet 192.168.1.x. The following assumes you are running Windows XP.

- 1: From the Network Connections window, open Local Area Connection (You may also access this screen by double-clicking the Local Area Connection icon on your taskbar). Click the Properties button.
- Select Internet Protocol (TCP/IP) and click the Properties button. The screen should now display as below. Change the IP address to the domain of 192.168.1.x (1<x<254) with subnet mask of 255.255.255.0. Set the default router and DNS server to the router's IP address.
- NOTE: The IP address of the router is 192.168.1.1 (default), so the PC must be set with a different IP. In the case below, the PC's IP address is set as 192.168.1.2

ieneral	
You can get IP settings assigner this capability. Otherwise, you n for the appropriate IP settings.	automatically if your network supports seed to ask your network administrator
O gotain an IP address autor	matically
Uge the following IP addres	ss:
IP address:	292.168.1.2
Sybnet mask:	255.255.255.0
Default gateway:	192.168.1.1
Ogtain DNS server address	automatically
Use the following DNS service	er addresses:
Breferred DNS server:	292.168.1.1
Albernate DNS server:	
	Adgenced

3: Click OK to submit the 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 for the Router in the Web address field. In this case http://192.168.1.1.
- NOTE: For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access, use the WAN IP address shown on the WUI Homepage screen and login with remote username and password.
- A dialog box will appear, as illutstrated below. Enter the default username and password, as defined in section 3.1 Default Settings.

Click OK to continue.

Connect to 192.1	58.1.1
R	GP4
The server 192.1 password. Warning: This ser password be sent without a secure	68.1.1 at N3G9 requires a username and ver is requesting that your username and in an insecure manner (basic authentication connection).
User name:	🖸 admin 👻
Password:	••••
	Remember my password
	OK Cancel

NOTE: The login password can be changed later (see 7.3.3 Passwords)

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

NetCom	3	<b>169W –</b> HSPA 7.2	Mbps Wi-Fi Rout	er		
Basic		3G Settings	Wreless	Management	Advanced	Status
Basic > Home						
Hardware Ve	ersion:	96358G-123				
Software Ve	rsion:	N3G9W-N101-5306N	CM-T03_R01			
Bootloader (	(CFE) Version	n: 1.0.37-6.0				
Wireless Dri	ver Versione	3.131.35.4.cpe2.0				
Device Info f	or 3G					
Network:	Teistra					
Link:	Connect	ted				
Mode:	HSDPA/	HSUPA				
Signal Stren	gthe T					
SIM Infec	SIM inte	erted				
This informat	ion reflects	the current status o	f your connection.			
LAN IP Addr	ess:	192.160.1.1				
WAN IP Add	ress:	10.220.6.191				
Default Gate	way:	10.64.64.64				
Primary DNS	Serveri	139,130.4.4				
Secondary D	NS Servert	203.50.2.71				
Date/Time:		Thu Aug 7 10:18:07 20	08			



## 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.



Fields	Description
Software version	The software version of the device.
Bootloader version	The bootloader version of the device.
Wireless driver version	The wireless driver version of the wireless module.
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 LAN interface.
WAN IP Address	Shows the IP address for WAN interface.
Default Gateway	Shows the IP address of the default gateway 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

The following table provides further details.

## 3G Settings

Download from Www.Somanuals.com. All Manuals Search And Download.

# **3G Settings**

This menu includes 3G service Setup and PIN Configuration.

Net G	n.com.au	<b>3G9W</b> – HSPA 7.2 N	lbps Wi-Fi Router				
Basic		3G Settings	Wireless	Management	Advanced	Status	
Basic >	Home	Setup PIN Configuration					

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

## 4.1 3G Service Setup

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

Het Gomm <sup>®</sup>	<b>3G9W</b> – HSPA 7	.2 Mbps Wi-Fi Rout	er			
Basic	3G Settings	Wireless	Management	Advanced	Status	
3G Settings > Setup						
Profile:	Custom APN	~				
APN:						
Username:						
Password:						
<ul> <li>All Bands/Automatic</li> </ul>	: 🔘 3G-850 Only 🔘 3G-8	350/2G-900/1800 🔘 3G-4	ALL O2G-ALL			
Save						



## 4.1.1 Profile Setup

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 gateway, then do so now.
- 2. Type the APN in the APN field. If you have not received a username and password, leave these fields empty.

<b>HetComm</b> ® www.netcomm.com.au	<b>3G9W</b> – HSPA 7	.2 Mbps Wi-Fi Rout	er		
Basic	3G Settings	Wireless	Management	Advanced	Status
3G Settings > Setup					
Profile:	Custom APN	~			
APN:					
Username:					
Password:					
<ul> <li>All Bands/Automatic</li> <li>Save</li> </ul>	🔿 3G-850 Only 🔘 3G-	850/2G-900/1800 🔿 3G-A	NL OZG-ALL		

- 3. Click the Save button to save the new settings and reboot the Gateway. .
- 4. After reboot, the Device Info for 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 Gateway should also be blinking.

et <i>Comm</i>	9# 3G	9 <b>W</b> - HSPA 7.2	Mbps Wi-Fi Rout	ler		
Basic	3	G Settings	Wreless	Managament	Advanced	Status
Basic > Home						
Hardware Version	ć.	963586-123				
Software Version:		N3G9W-N101-5306N	CM-T03_R01			
Dootloader (CFE) V	Version:	1.0.37-6.8				
Wireless Driver Ve	ersione	3.131.35.4.cpe2.0				
Network: 1 Link: 0 Mode: 1 Signal Strength: 0	Telstra Connecte HSDPA/HC					
51M Info: S	51M insert	led				
This information re	flects th	ne current status ol	your connection.			
LAN IP Address:	1	92.168.1.1				
WAN IP Address:	10	0.220.6.191				
Default Gateway:	10	0.64.64.64				
Primary DNS Serve	er: 1	39.130.4,4				
Secondary DNS Se	erver: 2	03.50.2.71				
Date/Time:	17	hu Aug 7 10:18:07 200	38			

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 in an on/off pattern moving from left to right this indicates that your SIM is PIN Locked, please lee PIN Lock Off on page 21 for instruction on how to fix this

## 4.2 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 Provider for assistance.

### 4.2.1 PIN Code Protection

PIN code protection prevents the use of a SIM card by unauthorized persons. To use the 3G internet 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.

NetGomm	<b>3G9W</b> – HSPA 7.2 M	bps Wi-Fi Router			
Desis	20 Cottings	Wireless	Management	0 chunced	Chatture
3G Settings > PIN (	Setup Confli PIN Configuration	WIEIESS	Management	Auvanceu	Status
PIN Code Change					
Old PIN Code: New PIN Code: Confirm PIN Code:					
O PIN code protectio	n				
PIN lock: PIN Code: Confirm PIN Code: Remember PIN code:	Off V				
O MEP Unlock Code:					
MEP lock: Lock Code:	Off 💌				
			Apply		

## **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 and click **Save/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**, enter the PIN Code and click **Save/Apply**.

Net Gomm www.netcomm.com.au	« 3g9w – HSPA 7.2 i	Mbps Wi-Fi Router			
Basic	3G Settings	Wireless	Management	Advanced	Status
3G Settings > PIN C	onfiguration				
OPIN Code Change					
Old PIN Code:					
New PIN Code:					
Confirm PIN Code:					
• PIN code protection					
PIN lock:	On 🛩				
PIN Code:					
Confirm PIN Code:	••••				
Remember PIN code:	No 💌				
O MEP Unlock Code:					
MEP lock:	Off 🔽				
Lock Code:					
			Apply		

After you do so, the following dialog box should appear.



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

NOTE: If the dialog box fails to appear, check your PIN code before trying again. Keep in mind you only have 3 attempts before your SIM card is locked. Contact your 3G provider if you require assistance.

#### 4.2.2 **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 and click Save/Apply.

asic .	3G Settings	Wireless	Management	Advanced	Status
G Settings > PIN	Configuration	•	•	·	•
PIN Code Change					
ld PIN Code:	•••				
ew PIN Code:					
onfirm PIN Code:					
PIN code protecti	DN				
IN lock:	Off 🗸				
IN Code:					
onfirm PIN Code:					
emember PIN code	No 🚩				
MEP Unlock Code:					
EP lock:	Off 👻				
ock Code:					

NOTE: elpful reminder.



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



## Wireless

# 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.

Basic	3G Settings	Wreless	Management	Advanced	Status			
li an		Setup						
Wireless 2	> Setup							
This page allows you to configure basic features of the w			n enable or disable the wireless LAN interface, hide the network from active scans, set the wi					
Cick "Apply	" to configure the basic vireless options.	MAC Filter	orenetics.					
		wrees bridge						
SSID: BSSID:	le Access Point wireless 00:1A:28:60:68:FA	]						
Country:	AUSTRALIA		~					
En En	able Wireless Guest Network							
	in the second se							

Option	Description
Enable Wireless	A checkbox that enables (default) or disables the wireless LAN interface. When selected, the Web UI 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 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	<ul> <li>A drop-down menu that permits worldwide and specific national settings. Each country listed below enforces specific regulations limiting channel range:</li> <li>USA = worldwide</li> <li>Australia/Japan = 1-14</li> <li>Jordan = 10-13</li> <li>Israel = 1-13</li> </ul>
Wireless Guest Network	The Guest SSID (Virtual Access Point) can be enabled by selecting the Enable Wireless Guest Network checkbox. Rename the Wireless Guest Network as you wish. NOTE: Remote wireless hosts cannot scan Guest SSIDs.

## 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 authenticate or encrypt your service on the Wired Equivalent Privacy (WEP) algorithm, which provides protection against unauthorized access such as eavesdropping.

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.

NetGomm	<sup>8</sup> <b>3G9W</b> – HSPA 7.	2 Mbps Wi-Fi Router				
Basic	3G Settings	Wireless	Management	Advanced	Status	
Wireless > Security						
This page allows you to key is required to auth Click "Apply" to configu	o configure security features enticate to this wireless net re the wireless security opti	of the wireless LAN interfact work and specify the encrypt ons.	e. You can sets the network ion strength.	<authentication method,="" sele<="" td=""><td>ecting data encryption, specify w</td><td>whether a network</td></authentication>	ecting data encryption, specify w	whether a network
Select SSID:	wireless	*				
Network Authentication	802.1X	~				
RADIUS Server IP Add	ress: 0.0.0.0					
RADIUS Port:	1812					
RADIUS Key:						
WEP Encryption:	Enabled	*				
Encryption Strength:	64-bit 🔽					
Current Network Key:	2 🛩					
Network Key 1:	a1b2c3d4e	5				
Network Key 2:						
Network Key 3:			1			
Network Key 4:			Ī			
	Enter 13 ASC Enter 5 ASCI	II characters or 26 hexadec ( characters or 10 hexadecin	mal digits for 128-bit encryp nal digits for 64-bit encryptic	ition keys in keys		
			Save/Apply			

Click **Save/Apply** to configure the wireless security options.



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 as illustrated below. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled.						
	Seed. 3380 Weekers V						
	WRA Group Paternal						
	ичнико ант НГ И АОУНИ И АОЛУ ИТТ 1012 8 800 / 10 4						
	WPA (horyston: TK/P r WPP Encyston: Disabled ref						
	Sawy/Apply						
	Window Security The text allow works where we will be used on 10 percentage. You are not an another allowed and an another text and an an another text and an another						
	rem page anno yozh o orrigare souzh y mature or the weeks suff rannan. You can seo be rehverk authentiation nethod, selectrojdata worsplan, gody whether anteknok Java vagaval to astronica to toni weeks encorriganti and gody the morsplannisteugh. Cidi 192/F to ordrage the weeks souzh gotana.						
	Select SID: www.less  WPA PSK						
	WRA Pre-Shared Days WRA Grap Salar Densal 0						
	WRA Evoyation TKP V WEP Exorption Cristified (in						
	Sam(Acply						
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 any one time.						
Enoruntion	This drap, down list hav will diaplay when WED Ensuration is applied						
Strength	This drop-down his box will display when WEP Encryption is enabled.						
-	This means that keys with a creater number of bits have a creater 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. FYI: Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.						

## 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.

Netcomm.com.au	3G9W -	- HSPA 7.2 M	lbps Wi-Fi Roi	uter			
Basic	3G Sett	ings	Wireless		Management	Advanced	Status
Wireless > Configura	tion		Setup				
This page allows you to speed, set the fragment set whether short or low Click "Apply" to configure	This page allows you to configure advanced features of i speed, set the fragmentation threshold, set the RTS thre set whether short or long preambles are used. Click "Apply" to configure the advanced wireless options.		Configuration MAC Filter Wireless Bridge	a	u can select a particular channel on which to operate, force the transmission rate to a parti al for clients in power-save mode, set the beacon interval for the access point, set XPress n		
AP Isolation:	Γ	Off 🛩	Station Info				
Band:		2.4GHz 🔽					
Channel:		Auto 🔽		Current	: 1		
Auto Channel Timer(min)	)	0					
54g™ Rate:	Ì	Auto 🔽					
Multicast Rate:		Auto 🔽					
Basic Rate:		Default		~			
Fragmentation Threshold	d:	2346					
RTS Threshold:	į.	2347					
DTIM Interval:	Ì	1					
Beacon Interval:	Ì	100					
XPress™ Technology:	Ĺ	Disabled 🔽					
54g™ Mode:		54g Auto	*				
54g™ Protection:		Auto 🔽					
Preamble Type:		long 🔽					
Transmit Power:		100% 🗸					
					Save/ánnly		



Option	Description
AP Isolation	Select On or Off. By enabling this feature, wireless clients associated with the Access Point can be linked.
Band	The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network. The two standards apply to the 2.4 GHz frequency band. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Allows selection of a specific channel (1-14) or Auto mode.
Auto Channel Timer (min)	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 discrete values between 1 to 54 Mbps.
Multicast Rate	Setting for multicast packet transmission rate. (1-54 Mbps)
Basic Rate	Sets basic transmission rate.
Fragmentation Threshold	A threshold (in bytes) determines whether packets will be fragmented and at what size. Packets that exceed the fragmentation threshold of an 802.11 WLAN will be split into smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value however are not fragmented. Values between 256 and 2346 can be entered but should remain at a default setting of 2346. Setting the Fragmentation Threshold too low may reput in ager parformance.
RTS Threshold	Request To Send (RTS) specifies the packet size that exceeds the specified RTS threshold, which then triggers the RTS/CTS mechanism. Smaller packets are sent without using RTS/CTS. The default setting of 2347 (max length) will disables the RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions in is milliseconds. The default is 100 ms and the acceptable range is $1 - 65535$ . The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon.
Xpress™ Technology	Broadcom's Xpress <sup>™</sup> Technology is compliant with draft specifications of two planned wireless industry standards. It has been designed to improve wireless network efficiency. Default is disabled.

Option	Description
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 802.11b 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 shown below.

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

Wet GOMMe <sup>®</sup>	<b>3G9W</b> – HSPA 7.2 M	bps Wi-Fi Router				
Basic	3G Settings	Wireless	Management	Advanced	Status	
		Setup				
Wireless > MAC Filter		Security				
		Configuration		0.0		
		MAC Filter	Uisabled U Allow	U Deny		
		Wireless Bridge				
		Station Info	Address Remove			
		A	dd Remove			

Option	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 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.

NET GOMM <sup>®</sup> www.netcomm.com.eu	<b>3G9W</b> – HSPA 7.2	Mbps Wi-Fi Router				
Basic	3G Settings	Wireless	Management	Advanced	Status	
Wireless MAC Filter Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.						
MAC AUURSS:			Save/Apply			

## 5.5 Wireless Bridge

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

Click Save/Apply to implement new configuration settings.

Hetcomm.com.au	3 <b>g9w</b> – HSPA 7.2 i	Mbps Wi-Fi Router				
Basic	3G Settings	Wireless	Management	Advanced	Status	
Wireless > Bridge This page allows you to functionality. Selecting / Disabled in Bridge Restri-	configure wireless bridge featu cess Point enables access poi ct which disables wireless brid Demote Differe will be work	Setup Security are Configuration MAC Filter	e. You can select Wire functionality will still be ge will be granted acces	less Bridge (also known as V available and wireless stati is, Selecting Enabled or Enal	Vireless Distribution System) to ions will be able to associate to bled(Scan) enables wireless br	o disables acess point o the AP. Select ridge restriction. Only
Click "Refresh" to updat Click "Save/Apply" to co	e the remote bridges will be grand of the remote bridges. Wait for figure the wireless bridge opt	fe Station Info				
AP Mode: Bridge Restrict:	Disable	ed 💙				

Refresh Save/Apply
--------------------

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



## 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.

<b>NETCOMM</b> * <b>3G9W</b> – HSPA 7.2 Mbps Wi-Fi Router							
Basic	3G Settings	Wireless	Management	Advanced	Status		
Setup     Setup       WireLess > Station Info     Security       This page shows authenticated wireless stations and the Configuration     MAC Fiker       BSSID     Associated     Authorized       Vireless Bridge     Station Info							
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 ad hoc networks, the BSSID is generated randomly.						
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



# Management

The Management menu has the following maintenance functions and processes:

- 6.1 Device Settings
- 6.2 Access Control
- 6.3 Simple Network Time Protocol (SNTP)
- 6.4 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 a backup file to save to your PC.

Net Gom	<b>3G9W</b> – HSPA 7.2	2 Mbps Wi-Fi Router			
Basic	3G Settings	Wireless	Management	Advanced	Status
Management > Device Settings > Backup Backup Gateway configurations. You may save your Gateway configurations to a file.			Device Settings	Backup	
			SNTP	Update	
			Access Control	Restore default	
			Save/Reboot	Update Firmwave	
		E	Backup Settings		
#### 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.

Wetcomm.com.au	<b>3G9W</b> – HSPA 7.2 M	lbps Wi-Fi Router			
Basic	3G Settings	Wireless	Management	Advanced	Status
			Device Settings	Backup	
Management > Device	e Settings > Update		SNTP	Update	
Update Gateway settings	. You may update your Gatew-	ay settings using your saved f	Access Control	Restore default	
Settings File Name:	Browse		Save/Reboot	Update Firmwave	
			Jpdate Settings		

#### 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.

Het Gomme www.netcomm.com.au	<b>3G9W</b> - HSPA 7.	2 Mbps Wi-Fi Router			
Basic	3G Settings	Wireless	Management	Advanced	Status
			Device Settings	Backup	
Management >	Device Settings > Restore	Default	SNTP	Update	
Restore Gateway	settings to the factory defaults.		Access Control	Restore default	
			Save/Reboot	Update Firmwave	
			Restore Default Settings		

#### 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).

#### **Gateway Restore**

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

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

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 this screens steps, you can update your Routers firmware. Manual device upgrades from a locally stored file can also be performed using the following screen.

RECOMM <sup>®</sup> netcomm.com.au	<b>3G9W</b> – HSPA 7	.2 Mbps Wi-Fi Router			
Basic	3G Settings	Wireless	Management	Advanced	Status
Manager and a Devia	- C-10		Device Settings	Backup	
management > Devic	e seccings > Update i	Irmware	SNTP	Update	
Step 1: Obtain an update	ed software image file fro	om your ISP.	Access Control	Restore default	
Step 2: Enter the path to	the image file location in	the box below or click the "Browse	Save/Reboot	Update Firmwave	
Step 3: Click the "Update	Software" button once	to upload the new image file.			
NOTE: The update proces and your Gateway will reb	is for the Gateway takes boot. Please DO NOT clos	about 2 minutes to complete, and a the Browser and reload/or chang	for the 3G modem takes abou le the webpage during the up	t 10 minutes, date process.	
Software File Name:	Br	owse			
			Jpdate Software		

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

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 Access Control

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

- Services
- IP Addresses
- Passwords

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

WetGomm.com.au	<b>3G9W</b> – HSPA 7.	2 Mbps Wi-Fi Router			
Basic	3G Settings	Wireless	Management	Advanced	Status
			Device Settings		
Management > Acces	ss Control > Services		SNTP		
A Service Control List ("S	CL") enables or disables s	ervices from being used.	Access Control	Services	
The following ports are no management or mode in a	ot recommended for HTTP come particular case (21	remote management in case cor	nfli Save/Reboot	IP Addresses	
management purpose in s	some paracalar case (21)	erer, ee, eeee, 23, 2323, 09, 0	<i>303, 101, 10110)</i>	Passwords	

#### 6.2.1 Services

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

Wet Comm.com.au	<b>3G9W</b> – HSPA 7.2 M	bps Wi-Fi Route				
Basic	3G Settings	Wireless	Man	agement .	Advanced	Status
Management > Acces A Service Control List ("Sú The following ports are no management purpose in s	s Control > Services IL") enables or disables service It recommended for HTTP remo ome particular case (21, 2121,	is from being used, ite management in cas , 22, 2222, 23, 2323, 1	e conflict with 59, 6969, 161	them for other 16116)		
		Services	LAN	WAN		
		FTP	💌 Enable	Enable		
		HTTP	🗹 Enable	Enable 80 p	ort	
		ICMP	Enable	Enable		
		SSH	🗹 Enable	Enable		
		TELNET	🗹 Enable	Enable		
		TETP	🗹 Enable	🔲 Enable		
			Sav	e/Apply		



#### 6.2.2 IP Address

The IP Address option limits local access by IP address. When the Access Control Mode is enabled, only the IP addresses listed here can access the device. Before enabling Access Control Mode, add IP addresses with the Add button.



On this screen, enter the IP address of a local PC which you wish to allow permission. Click Save/Apply to continue.

NetGomm	3G9W – HSPA	.2 Mbps WI-Fi Rout	er			
Dasic	3G Settings	wireless	Management	Advanced	Status	
Access Control Enter the IP address of t	he management station	permitted to access the loc	al management services, and clic	k SavejApply."		
IP Address:			Save/Apply			

#### 6.2.3 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.

et Comm	<b>7" 309W -</b> HSPA 7	2 Mbps Wi-Fi Route			
Basic	3G Settings	Wireless	Management	Advanced	Status
Management > /	Access Control > Password	ls.	Device Settings		
Access to your Gab	way is controlled through thre	e user accounts: admin, eu	eport, ar Access Control	Services.	
the user name "adr	nin" has unrestricted access to	change and view configura	tion of your generative	IP Addresses	
The user name "sup	port" is used to allow an ISP to	chnician to access your Gal	teway for maintenance and to n	in diagnostics.	
The user name "Use	r" can access the Gateway, vi	ew configuration settings ar	nd statistics, as well as, update (	the Gateway's software.	
the fields below	to enter up to 16 characters	and click "Apply" to change	or create passwords. Note: Pas	sword cannot contain a spi	sca.
Jsername:		~			
Old Password:					
Yew Password:					

### 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.

НЕ	ticomm.com.au 3	<b>G9W</b> – HSPA 7.2 M	bps Wi-Fi Router			
E	Basic	3G Settings	Wireless	Management	Advanced	Status
~	4anagement > SNTP			Device Settings SNTP		
т	his page allows you to the m	nodem's time configuration.		Access Control		
[	Automatically synchroniz	e with Internet time server	s	Save/Reboot		
F	First NTP time server: Second NTP time server:	Other Other	<ul> <li>✓ au.pool.ntp.org</li> <li>✓ ntp0.cs.mu.OZ</li> </ul>	9 AU		
Т	ime zone offset:	(GMT+10:00) Canb	erra, Melbourne, Sydney	/	*	
			(	Save/Apply		

The following options should now appear (see screenshot below):

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.

NetGOMM <sup>®</sup> ww.netcomm.com.au	3G9W – HSPA 7	7.2 Mbps Wi-Fi Rout	er			
Basic	3G Settings	Wireless	Management	Advanced	Status	
Management > SNTP						
This page allows you to the	modem's time configu	ration.				
Automatically synchron	nize with Internet time	servers				
First NTP time server:	Other	🖌 au.poo	l.ntp.org			
Second NTP time server:	Other	rtp0.cs	.mu.OZ.AU			
Time zone offset:	(GMT+10:00)	Canberra, Melbourne,	Sydney	*		
			Save/Apply			

NOTE: SNTP must be activated to use Parental Control (section 7.3.2).



## 6.4 Save and Reboot

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

WWW.netcomm.com.au	<b>3G9W</b> - HSPA 7.2 M	bps Wi-Fi Router			
Basic	3G Settings	Wireless	Management	Advanced	Status
			Device Settings		
Management > Save/I	Reboot		SNTP		
		Click the button belo	Save/Reboot	Gateway.	
			Save/Reboot		

- NOTE1: 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.
- NOTE2: If you lose all access to your web user interface, simply press the reset button on the rear panel for 5-7 seconds to restore default settings.

Advanced Setup



# Advanced Setup

This chapter explains advanced setup for your Router:



### 7.1 Local Area Network (LAN)

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

Basic	3G Settings	Wreless	Management	Advanced	Status
Advanced > Local 4	krea Network (LAN) Setu				
Configure the Gatewar reboots the Gatewar	y IP Address and Subnet Mar to nake the new configuratio	i.for LAN interface. Sav	e button only saves the LAN co	rfiguration data Save/Re	boot button saves the LAN configuration
IP Address:	10.0.0.138	_			
Subret Mask:	255.255.255.0				
Diskupp					
Enable NAT					
Enable 1999 Sto  Standard Mode  Blocking Mode	oping				
O Deable DHCP See	week.				
C Enable DHCP Ser	ver				
Bart 2º Addresso	10.0.0.129				
End IP Address:	10.0.0.254				
Leased Time (hour	0:24				
	Stranger and	1	and the sector offending 12 and	the second se	-formed
Static 2 <sup>th</sup> Lease Lie	t; Rease click on Seve,Reboo			contraction and the statement of the statement of	

Configure the second IP Address and Subset Mask for UAN interfac

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 Internet Group	Enable by ticking the box				
Management Protocol (IGMP) Snooping	Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.				
	<b>Blocking Mode</b> : In blocking mode, the multicast data traffic will be blocked. When there are no client subscriptions to a multicast group, it will not flood to the bridge ports.				
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 IP, default gateway and DNS server addresses to every DHCP client on your LAN				

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.

Configure the second IP Address and Subnet Mask for LAN interface
 P Address:
 Subnet Mask:

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)

Net Gon	∭ <sup>®</sup> 3	<b>g9w</b> – HSPA 7.2 i	Mbps Wi-Fi Rout	er						
Basic		3G Settings	Wireless		Management	Advanced	Sta	tus		
						LAN				_
Advanced 3	> NAT > Port F	orwarding				NAT	Port	Forward	ling	
Virtual Server	allows you to di	rect incoming traffic fron	n WAN side (identified	by Protocol	and External port) to the	Ir Security	Port	Triggerin	ng	Internal port
is required on	ly if the externa	I port needs to be conve	rted to a different por	t number us	ed by the server on the	-A Routing	DMZ	host		
	Add Remove ONS									
_										
	Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Ad	dress I	Remove	Edit

#### 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.

Net Gon	алана <sup>в</sup> алана з	<b>g9W</b> - HSPA 7.2	Mbps Wi-Fi Rout	er							
Basic		3G Settings	Wireless		Management	Advanced		Status			
Advanced 3	NAT > Port F	orwarding				LAN					
Virtual Server	allows you to di	ivert incoming traffic from	m WAN side (identified )	by Protocol	and External nort) to the	Tr Security		Port Porwar Port Trigger	ang ina	) Internal n	ort
is required on	ly if the externa	port needs to be conve	erted to a different por	t number us	ed by the server on the	LA Routing	1	OMZ host		, incontarp	
				Add	d Remove	DNS					
[	Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP	Address	Remove	Edit	

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

				_				
NetComm	3 <b>G9W</b> – HSI	PA 7.2 Mb	os Wi-Fi Rout	er				
www.netcomm.com.au								
Basic	3G Settings		Wireless		Management	Advanced		Status
NAT Virtual Servers								
Select the service name, an be changed. It is the sar Remaining number of er	d enter the servi me as "Extern- ntries that can	er IP address al Port End" be configur	and click "Save/Ap normally and w red:32	ply" to forw ill be the s	ard IP packets fo same as the "Ir	r this service to the spe I <b>ternal Port Start"</b> o	ecified server. NO or "External Por	TE: The "Internal Port End" cannol t End" if either one is modified.
Server Name:								
Select a Service: Se	elect One			*				
Custom Server:								
Server IP Address: 192	2.168.1.							
				F	Save /Annly			
					oave/whhile			
External Port Start Exte	ernal Port End	Protocol	Internal Por	t Start Int	ernal Port End			
		TOP						
		TOP	×					
		TOP	×					
		TOP	×					
			×					
		TOP	×					
		TCP						
Options	Descrip	tion						
Select a Service	User sho	ould sele	ect the serv	vice fro	m the list.			
Or	Or							
						6 U		
custom Server	Create a	a custom	ier server a	and ent	er a name	tor the serve	r	
Server IP Address	Enter th	e IP add	ress for the	e serve	r.			
External Port Start	Enter th	e startin	g external	port nu	mber (whe	en you select	Custom Se	rver). When a service
	is select	ed the p	ort ranges	are au	tomatically	/ configured.		
External Port End	Enter the selected	e ending I the por	) external p t ranges ar	ort nur e autoi	mber (whei matically c	n you select C onfigured.	Custom Ser	ver). When a service is
Protocol	User car	n select '	from: TCP,	TCP/U	OP or UDP.			
Internal Port Start	Enter the selected	e interna I the por	al port stari t ranges ar	ing nur e autor	mber (whe matically c	n you select ( onfigured	Custom Ser	rver). When a service is

**Internal Port End** Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.



#### 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.

М	<b>etGOMM</b> ®	<b>3G9W</b> – HSPA 7.2	Mbps Wi-Fi	Router									
	Basic	3G Settings	Wireless		M	lanage	ement		Adva	nced		Status	
	Advanced > NAT > Port Triggering Setun								LAN			David Damanulla a	
		· · · · · · · · · · · · · · · · · · ·							NAT			Port norwarding	
	Some applications require	that specific ports in the Ga	steway's firewal	l be opened	for acces	ss by ti ving Do	he remote p vtc' The Col	arties.	becurity		Port Iriggering	rewall when an	
	back to the application on	the LAN side using the 'Op	en Ports'. A max	imum 32 en	tries can	be con	figured.	ceway a	Routin	9		DMZ host	Connections
					_	_	-		DNS				
					Add	Re	move						
			Application Trigger Open			pen		Remove					
			Name	Protocol Port Range Protocol Port			Port R	ange					
					Start	End		Start	End				

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

Basic     3G Settings     Wreless     Mangement     Adanced     State	Net Gomme	<b>7° зару</b> – н	SPA 7.2 Mbps	: Wi-Fi Router					
Std - Pot Trigger Pot       Select Ope       Se	Basic	3G Setting	s V	/ireless	Manage	ment	Advanced	Status	
Bree applications that as gares, video conferencing, renote access applications and others require that specific ports in the sciencesy's freewall be opened for access by the applications and others require that specific ports in the sciencesy's freewall be opened for access by the applications and others require that specific ports in the sciencesy's freewall be opened for access by the applications and others require that specific ports in the sciencesy's freewall be opened for access by the applications and others require that specific ports in the sciencesy's freewall be opened for access by the applications and others require that specific ports in the sciencesy's freewall be opened for access by the applications are drawn application and access and access the applications are drawn application applications and others require that specific ports in the sciences's freewall be opened for access by the applications are drawn application a	NAT Port Trigg	jering							
Application Name: else an application: Custom application: Trigger Port End Trigger Protocol/Dpen Port Start Dpen Port End Open Protocol TCP V TCP V TCP V TCP V TCP V TCP V	Some applications s You can configure I Remaining numl	such as games, video o the port settings from t oer of entries that o	onferencing, remol his screen by selec <b>an be configure</b>	e access applicatio ting an existing ap <b>1:32</b>	ns and others re plication or creat	quire that speci ng your own (C	fic ports in the Gateway Sustom application)and c	's firewall be opened for access lick "Save/Apply" to add it.	by the applications
Image: Coston application:	Application Name: Select an ap	plication: Select Or	18	~					
Trigger Port Start Trigger Port End Trigger Protocol Dpen Port Start Dpen Port End       Dpen Port Start Trigger Port End Trigger Protocol Dpen Port Start Dpen Port End         TCP       TCP       TCP         TCP       TCP       TCP <td>Custom appl</td> <th>ication:</th> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Custom appl	ication:							
Trigger Port Start Trigger Port Start Dpen Port					Save/A	pply			
Image: Constraint of the constraint	Trigger Port Sta	rt Trigger Port End 1	Frigger Protocol	Open Port Start	Open Port End	Open Protoc	lo		
Image: Constraint of the constraint			TCP			TCP	*		
TCP       TCP       TCP			TCP 🔽			TCP	~		
TCP       TCP       TCP         Save/Apply       Save/Apply			TCP 🔽			TCP	~		
Image: Constraint of the constr			TCP 🔽			TCP	*		
TCP     TCP       TCP     TCP       TCP     TCP       TCP     TCP       TCP     TCP       TCP     TCP       Save/Apply			TCP 🔽			TCP	*		
TCP     TCP       TCP     TCP       TCP     TCP       TCP     TCP       Save/Apply			TCP 🗸			TCP	*		
TCP     TCP       Save/Apply			TCP V			TCP	*		
Save/Apply			TCP 🗸			TCP	~		
Save/Apply									
					Save/	Apply			

Options	Description
Select an Application	User should select the application from the list.
or	or
Custom Application	User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Port End	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.

<b>etGOMM</b> ®	3G9W - HSPA 7	7.2 Mbps Wi-Fi Rout				
Basic	3G Settings	Wireless	Management	Advanced	Status	
				LAN		_
Advanced > NAT > DM	Z Host			NAT	Port Forwarding	
The Gateway will forward	IP packets from the WA	N that do not belong to an	vy of the applications configured in the '	Security	Port Triggering	
Enter the computer's IP ac	dress and click "Apply"	to activate the DM7 bost		Routing	DMZ host	
chief die compaters in ac	aress and cick. Apply	to activate the DH2 host.		DNS		
Clear the IP address field a	and click "Apply" to dea	ctivate the DMZ host.				
DMZ Host IP Address:						
			Save/Apply			



## 7.3 Security

Your Router can be secured with IP Filtering or Parental Control functions.



#### 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**.

NetCo	3G9W -	HSPA 7.2 Mb	os Wi-Fi Router					
Basic	3G Setti	ngs	Wireless	Management		Advanced	Status	
Advances	d > Security > 1P Filterin	g > Outgoing IP	Filtering Setup			LAU NAT		
By default,	all outgoing IP traffic from L	AN is allowed, but	some IP traffic can be BLOCK	LD by setting up	filters.	Security	SP Filtering	Outgoing
Choose Ad	d or Remove to configure ou	tacina IP filters.				Routing	Parental Control	Shoothing
						DRS		
	Filter	Name Protocol	Source Address / Mask	Source Port	Dest. Adu	dress / Mask Dest. Port	Remove	
			Ad	d Remove	]			

Basic	3G Settings	Wheless	Management	Advanced	Status
Add IP Filter Dutgoing					
The screen allows you to cre must be satisfied for the rule	sate a filter rule to ider s to take effect. Click 1	tify outgoing IP traffic by SavelApply' to save and a	specifying a new filter name and thyste the filter.	d at least one condition bei	ow. All of the specified conditions in this fil
Filter Name:					
Protocol:		~			
Source IP address:					
Source Subnet Mask:					
	rt):				
Source Port (port or port:po					
Source Port (port or port:po Destination IP address:					
Source Port (port or port:po Destination IP address: Destination Subnet Mask:					

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

Options	Description
Filter Name	The filter rule label
Protocol	TCP, TCP/UDP, UDP or ICMP
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 address	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**.

NetComm <sup>*</sup>	3G9W – HSPA 7	.2 Mbps Wi-Fi Rou	ter		
Basic	3G Settings	Wreless	Management	Advanced	Status
Advanced > Security by default, all incoming to	r > DP Filtering > Inco P traffic from the WAN is	ning IP Filtering Setup blocked when the firewal	is enabled. However, some IP tr	affic can be ACCEPTED by s	etting up filters.
Choose Add or Remove	to configure incoming (P)	Rers.			
	Filter Name VPI/V	CI Protocol Source J	Address / Mask Source Port	Dest. Address / Mask	Dest. Port Remove
			Add Remove		

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

Dasic	3G Cettings	Wrelcis	Management	Advanced	Statud
Add IP Filter - 1	Incoming				ter for the
The ocrash allows	you to greate a filter rule to id	and Py incoming IP traffic by	specifying a new litter name an	d at least one condition bei	on. All of the specified conditions in t
nuit be ratafied !	or the rule to take effect. Gid	Save(Appl/ to save and a	sively the filter.		
filter tanier					
la ses Waddane	_				
varie tubiet Ha	-				
Source Part (port -	or pot ports				
Instruction IP add	Sent:				
Destination Submit	e Maski				
	cont or port-port)				
relation void (1					
restration voit ()	After Revending Bandling and				
WAN Interfaces Select at least one	(Configured in Routing In or multiple Will/Interfaces de	ode and with farewall end played below to apply this r	de.		

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

Click Save/Apply to save and activate the filter.

Download from Www.Somanuals.com. All Manuals Search And Download.



#### 7.3.2 Parental Control

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

Wet Gomm.com.au	<b>3G9W</b> – HSPA 7	7.2 Mbps Wi-Fi Route	r		
Basic	3G Settings	Wireless	Management	Advanced	Status
Advanced > Security	> Time of Day Restri				
Advanced > Security	> Time of Day Result	cuons A maximum or	to encles can be conligated.		
					IP Filtering
	Enable	Username MAC Mon	Tue Wed Thu Fri Sat Sun	Routing	Parental Control
			1 1 1 1 1 1 1 1 1 1	DNS	
			Add Remove		

Click Add to display the following screen.

NetGom.	∭ <sup>®</sup> 3G9W	– HSPA 7.2 Mbps Wi-	Fi Router			
Basic	3G Se	ttings Wirele:	is Managa	ement Adva	anced S	Status
Time of Day Re	estriction					
This page adds ti browser is runnin based PC, go to (	me of day restrictio g. To restrict other command window ar	n to a special LAN device conn LAN device, click the "Other M nd type "ipconfig /all".	ected to the Gateway. The 'B AC Address'' button and ente	rowser's MAC Address' au r the MAC address of the	comatically displays the M other LAN device. To find	IAC address of the LAN device where the I out the MAC address of a Windows
User Name						
<ul> <li>Browser's M</li> </ul>	IAC Address	00:1D:0F:BE:AC:D7				
O Other MAC (xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Address :xx)					
Days of the wee Click to select	k	Mon Tue Wed Thu Fri Sa	t Sun			
Start Blocking Tim	ie (hh:mm)					
End Blocking Time	e (hh:mm)					
			Save/A	.oply		

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

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

#### 7.4 Routing

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

<b>ALCONT</b> ®	<b>3G9W</b> – HSPA 7.2	Mbps Wi-Fi Router			
Basic	3G Settings	Wireless	Management	Advanced	Status
Advanced > Routing >	Default Gateway		LAN		
If Enable Automatic Assign selected, enter the static	ned Default Gateway check default Gateway AND/OR a	will accept the first received def oply' button to save it.	Security Routing	n WAN connection. If the checkbox is not Default Gateway	
NOTE: If changing the Aut	comatic Assigned Default G	ateway from unselected to sele	ected, You must reboot the Gate	DN5	Static Route Dynamic Route
Enable Automatic As	ssigned Default Gateway				

#### 7.4.1 Default Gateway

NOTE:

If the **Enable Automatic Assigned Default Gateway** checkbox is selected, this device will accept a default Gateway assignment. If the checkbox is not selected, a field will appear allowing you to enter the static default gateway and/or WAN interface, then click **Save/Apply**.

Save/Apply

Net Comm.com.	3G9W – HSPA 7	.2 Mbps Wi-Fi Rout	er			
Basic	3G Settings	Wireless	Management	Advanced	Status	
Advanced > R	outing > Default Gateway					
If Enable Automa selected, enter t	atic Assigned Default Gateway ch the static default Gateway AND/C	eckbox is selected, this Gal R a WAN interface. Click 'S	teway will accept the first receiv save/Apply' button to save it.	ed default Gateway assignm	ent from WAN connection. If th	e checkbox is not
NOTE: If changin	ng the Automatic Assigned Default	t Gateway from unselected	l to selected, You must reboot t	he Gateway to get the autor	natic assigned default Gateway.	
	cultaric Assigned Deradic dateina	7				
			Save/Apply			
After enabling	the Automatic Assign	ned Default Gatev	way, you must re-bo	ot the Router to a	ctivate the assigned	default Gatev



#### 7.4.2 Static Route

The Static Route screen displays the configured static routes.

Click the Add or Remove buttons to change settings.

HetGomm.com.au	<b>3G9W</b> – HSPA 7.	.2 Mbps Wi-Fi Rout	er			
Basic	3G Settings	Wireless	Management	Advanced	Status	
Advanced > Ro	outing > Static Route					
		Destination S	ubnet Mask Gateway In	terface Remove		
			Add Remove			

Click the Add button to display the following screen.

unn	etcomm.com.au 31	<b>g9w</b> - HSPA 7.2 N	Abps Wi-Fi Route	r			
	Basic	3G Settings	Wireless	Management	Advanced	Status	
	Routing Static Route	e <b>Add</b> work address, subnet i	mask, Gateway AND	/OR available WAN interface	then click "Save/Appl	y" to add the entry to the	routing table.
	Destination Network Addre Subnet Mask:	ess:					
	Use Gateway IP Addr Use Interface	ppp0/ppp0 🗸					
				Save/Apply			

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

#### 7.4.3 Dynamic Route

To activate this option, select the Enabled radio button for Global RIP Mode.

To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the Enabled checkbox for that interface. Click Save/Apply to save the configuration and to start or stop dynamic routing.

	<b>etGD</b>	MM om.au	7¢	<b>3G9W</b> – HS	SPA 7.2 N	1bps Wi-Fi Ro	uter				
	Basic			3G Settings		Wireless		Management	Advanced	Status	
	Advanced > Routing > Dynamic Route							LAN			
									NAT		
	To activate R	RIP for th	ne dev	ice, select the 'I	nableď rad	o button for Globa	RIP Mode.	To configure an individual inte	Security	version and operation, fol	lowed by placing
	a check in th	e 'Enable	d' che	ckbox for the in	terface. Clic	k the 'Save/Apply'	button to sa	we the configuration, and to	Routing	Default Gateway	
	Global RIP	Mode	• D	isabled 🔘 En	abled				DNS	Static Route	
			-							Dynamic Route	
	Interface	Versi	n	Operation	Enabled						
	br0	2	~	Active 🔽							
	ppp0	2	*	Passive 🔽							
							(	Save/Apply			



#### 7.5 Domain Name Servers (DNS) 7.5.1 DNS Server Configuration

If the Enable Automatic Assigned DNS checkbox is selected, this device will accept the first received DNS assignment from the Wireless 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.

et Gomm <sup>®</sup>	<b>3G9W</b> – HSPA 7.2 I	Mbps Wi-Fi Router			
Basic	3G Settings	Wireless	Management	Advanced	Status
Advanced > DNS > DNS	Server Configuration			LAN NAT	
If 'Enable Automatic Assign checkbox is not selected, e	ed DNS' checkbox is select inter the primary and option	e first received DNS assignmen Idresses. Click 'Save' button to	Security Routing	the connection establishment. If the You must reboot the Gateway to make the	
new configuration effective	в.			DNS	DNS Server
Enable Automatic Ass	signed DNS				Dynamic DNS
			Save		

NOTE: Click the Save button to save the new configuration. To make the new configuration effective, reboot your Router.

#### 7.5.2 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.

Het Gomme www.netcomm.com.au	° <b>3G9W</b> – HSPA 7	7.2 Mbps Wi-Fi Rout	er			
Basic	3G Settings	Wireless	Management	Advanced	Status	
Advanced > DNS	> Dynamic DNS					
The Dynamic DNS s accessed from vario	ervice allows you to alia: us locations on the Inte	s a dynamic IP address t rnet.	to a static hostname in any o	of the many domains, all	owing your Gateway to be more ea	sily
Choose Add or Rem	ove to configure Dynan	nic DNS.				
		Hostname	Username Service Inte	rface Remove		
			Add Remove			

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

<b>HetGomm</b> ®	<b>3G9W</b> – HSPA 7	.2 Mbps Wi-Fi Route	er			
Basic	3G Settings	Wireless	Management	Advanced	Status	
Add dynamic DDNS						
This page allows you t	to add a Dynamic DNS	address from DynDNS.	org or TZO.			
D-DNS provider	DynDNS	.org 🚩				
Hostname Interface	ppp0/pp	p0 🗸				
DynDNS Settings Username Password						

Save/Apply

Options	Descriptions
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

# Status

The Status menu has the following submenus:

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

<b>et.GOMM</b> ® netcomm.com.au	<b>3G9W</b> – HSPA 7.	2 Mbps \	Vi-Fi Rout	er				
Basic	3G Settings	Wir	eless	Management	Advanced		Status	
ol							Diagnostics	
Status > pppU Diagr	nostics						System log	
Your Gateway is canab	le of testing your WA	N connect	ion. The ind	ividual tacts are listed hele	w. If a text displays a	fail status in	3G network	ts" at the
bottom of this page to	make sure the fail st	atus is con	sistent. If th	e test continues to fail, cli	ck "Help" and follow t	the troubles	Statistics	
							Route	
Test the connection	to your local netwo	ork						
Test your ENET(1-4)	) Connection:	PASS	Help				DHCP	
Test your Wireless C	Connection:	PASS	Help					



#### 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 in the Help screen.

etcomm.com.au	<b>3G9W</b> – HS	PA 7.2 M	Mbps Wi-I	Fi Router			
Basic	3G Settings		Wireles	is Manageme	nt Advanced	Status	
Status > ppp0 Diagno	stics						
Your Gateway is capable make sure the fail status	of testing your WA is consistent. If th	N connect e test cont	ion. The indivi inues to fail,	vidual tests are listed below. If a t click "Help" and follow the trouble	est displays a fail status, di shooting procedures.	ck "Rerun Diagnostic Tests" at the bottom of t	his page to
Test the connection t	o your local net	work		_			
Toet your ENET(1-4)	C		DACC Hel				
reservour ENET(1=4)	Connection:		FR35 100	E			

Test	Description
ENET Connection	<b>Pass</b> : 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.
Wireless connection	Pass: Indicates that the wireless card is ON.
	Down: Indicates that the wireless card is OFF.
Ping Default Gateway	<b>Pass</b> : Indicates that the Router can communicate with the first entry point to the network. It is usually the IP address of the ISP's local Gateway.
	Fail: Indicates that the Router was unable to communicate with the first entry point on the network, and it may not have an effect on your Internet connectivity. If this test fails and you can access the Internet, there is no need to troubleshoot this issue.
Ping Primary Domain Name Server	<b>Pass</b> : 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.

WWW.netcomm.com.au	3G9W – HSPA 7	<b>3G9W</b> – HSPA 7.2 Mbps Wi-Fi Router								
Basic	3G Settings	Wireless	Management	Advanced	Status					
Etatur > Euctors Lo					Diagnostics					
Status > System Lu	9				System log					
The System Log dialog	allows you to view the Sys	tem Log and configure the	System Log options.		3G network					
Click "View System Log"	to view the System Log.				Statistics					
chille - Course anton	· · · · · · · · · · · · · · · · · · ·	hans I am an Rama			Route					
Click "Configure System	Click "Configure System Log" to configure the System Log options.									
					DHCP					
		View Syst	tem Log Configure	System Log						

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

// 	etcomm.com.au	<b>3G9W</b> – HSPA 7.2	Mbps Wi-Fi Router				
	Basic	3G Settings	Wireless	Management	Advanced	Status	
	System Log Conf	iguration					
	If the log mode is ena the Display Level, all lo specified IP address ar	bled, the system will be ogged events above or e nd UDP port of the remo	gin to log all the selected equal to the selected leve ote syslog server. If the s	d events. For the Log Lev el will be displayed. If the selected mode is 'Local' or	el, all events above or e selected mode is 'Remo ' 'Both,' events will be r	equal to the selected level will l ote' or 'Both,' events will be se ecorded in the local memory.	oe logged. For nt to the
	Select the desired val	ues and click 'Save/Apply	y' to configure the system	m log options.			
	Log: 💿 Disa	ible 🔿 Enable					
	Log Level:	Debugging 🔽					
	Display Level:	Error 🗸					
	Mode:	Local 🛩					

-		-
	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 system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the WEB UI will prompt the you to enter the Server IP address and Server UDP port.

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

System Log

Date/Time	Facility	Severity	Message
Jan 1 00:00:12	kern	crit	kernel: eth0 Link UP.

Refresh Close

# 8.3 3G Status

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

ofEn	mm	7°			
etcomm.c	com.au	3G9W	- HS	SPA 7.2 Mbp	s WI-FI Rou
Basic		3G Se	ttings	1	Vireless
tatus > :	BG				
Manufac	turer: S	ierra Wireless, 1	nc.		
Model:	M	IC8780			
FW Rev:	F	1_0_0_19AP	_		
IMEI:	3	5421901068518	6		
F5N:	D	330458623410			
	-				
IMSI:	5050134	141486175			
HW REV:		1.0			
*		10			
Tempera	ture:	b3 WCDM0			
WEDMA	noue:	IMT2000			
GSM ban	d:	Unknown			
WCDMA (	hannel:	10563			
GSM cha	nnel:	65535			
GMM (PS	) state:	Requesting sr	/c NOF	RMAL SERVICE	
MM (C5)	state:	IDLE NORMAL	SERVI	CE	
Signal St	rength:	-80 (dBm) [Mi	ddle]		
Signal lev	el(RSSI	):	13		
Quality(E	c/Io)		-4.5	i dB	
Network	Name	ition status	regi 3Te	stered, roaming	
Country (	Tode		505	1501 0	
Network	Code		06		
Cell ID			530	.c	
Primary Scrambling Code (PSC) 368		(REF)			
Data Ses	sion Sta	tus	Con	nected	
HSUPA Ca	ategory:			5	
HSDPA Ca	ategory:			8	1
Received	Signal (	ode Power(R	SCP):	-86	dBm
Battery (	onnecti	on Status(BC	5):	MT is powered	by the battery.
Battery (	harge L	evel(BCL):		10	U

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



Status	Description									
Manufacturer	The manufac	The manufacturer of the embedded 3G module.								
Model	The model na	The model name of the embedded 3G module.								
FW Rev.	The firmware	version of the	3G module.							
IMEI	The IMEI (Inte identify a mol	The IMEI (International Mobile Equipment Identity) is a 15 digit number that is used to dentify a mobile device on a network.								
FSN	Factory Seria	I Number of the	e 3G module.							
IMSI	The IMSI (Inte identify an ine	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	e version of the	3G module.							
Temperature	The temperat	ure of the 3G r	module in degre	es Celsius.						
System Mode	WCDMA/Euro	pe								
	CDMA 2000	/ America								
WCDMA band	The 3G radio (850/1900/2 is 1900 MHz	The 3G radio frequency band which supports tri-band UTMS/HSDPA/HSUPA frequencies (850/1900/2100 MHz), IMT2000 is 2100 MHz, WCDMA800 is 850 MHz, WCDMA1900 is 1900 MHz.								
GSM band	The 2G radio frequency band which supports Quad-band GSM/GRPS frequencies, including GSM850, GSM900, DCS1800, PCS1900 with each number representing the respective frequency in MHz.									
WCDMA channel	The 3G chan	nel.								
GSM channel	The 2G chan	nel.								
GSM (PS) state	Packet Switc	ning state								
MM (CS) state	Circuit Switch	ning state								
Signal Strength	The 3G/2G se	ervice signal st	rength in dBm.							
	Signal level in dBm	-109 ~ -103	-101 ~ -93	-91 ~ -87	-85 ~ -79	-77 ~ -52				
	5 Signal									
	Dars									
	LED	Low		Medium		High				

Download from Www.Somanuals.com. All Manuals Search And Download.

Status	Descriptior	Description					
Signal Level (RSSI)	3G Radio Si	gnal Strength	Index				
	Value	2 ~ 5	6 ~ 10	11 ~ 13	14 ~ 17	18 ~ 31	99
	Signal level in dBm	-109 ~ -103	-101 ~ -93	-91 ~ -87	-85 ~ -79	-77 ~ -52	unknown
	5 Signal bars						
	LED	Low		Medium		High	
Quality (Ec/lo)	The total en strongest ce	ergy per chip ells.	per power dei	nsity (Ec/lo)	value of the	active set's	three
Network Registration Status	Should disp	lay as register	ed with a valio	d unlocked S	SIM card.		
Network Name	The 3G inte	rnet Service P	rovider.				
Country & Network Codes	Each countr	y and network	t has a unique	code.			
Cell ID	The network	c information f	or the "servin	g" cell ID.			
Primary Scrambling Code (PSC)	The PSC of	The PSC of the reference WCDMA cell					
Data Session Status	Connected of	or Disconnecte	ed				
HSUPA/HSDPA Categories	The HSUPA/ higher num	HSDPA catego pers generally	ories correspo indicating fas	nd to differe ter rates	ent data trar	nsmission ra	tes with
Received Signal Code Power (RSCP)	The RSCP o	f the active se	t's three stror	igest cells			
Battery Connection Status (BCS)	BCS of the I	VT (Mobile Ter	rmination)				
Battery Charge Level (BCL)	BCL of the N	MT (Mobile Ter	mination)				



# 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.

etcomm.co	m.au	76	3G9'	<b>W</b> – H	ISPA 7.2	2 Mbj	ps Wi-Fi F	uter			
Basic			3G	Setting	15		Wireless	Management	Advanced	Status	
		:							•	Diagnostics	
Status > S	tatistics	5 > LA	N			:				Diagnostics System log	
Status > S	tatistics	; >LA Recei	N		T	ransm	iitted	:	•	Diagnostics System log 3G network	
Status > 5 Interface	Bytes	5 > LA Recei Pkts	N ived Errs	Drops	Ti Bytes	ransm	itted	i	·	Diagnostics System log 3G network Statistics	LAN
Status > 5 Interface Ethernet	Bytes 302626	s > LA Recei Pkts 2687	N ived Errs 0	Drops 0	Ti Bytes 1861019	Pkts	itted Errs Drops	i		Diagnostics System log 9G network Statistics Route	LAN 3G ne
Status > S Interface Ethernet Wireless	Bytes 0	s > LA Recei Pkts 2687 0	N ived Errs 0	Drops 0	Ti Bytes 1861019 80311	Pkts 2925 420	iitted Errs Drops 0 0 51 0		·	Diagnostics System log OG network Statistics Route ARP	LAN 3G ne

#### 8.4.1 LAN Statistics

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

<b>etGomm.co</b>	m.au	e	3G9	<b>W</b> – H	ISPA 7.2	2 Mb	ps W	i-Fi Ro				
Basic			36	Setting	ĸ		Wirel	ess	Management	Advanced	Status	
			50	oottang								
Status > Sl	tatistics	> LA	N			:						
Status > Sl Interface	tatistics	>LA	N		Tr	ransn	nitted					
Status > 50	atistics I Bytes	> LA Recei Pkts	N ved Errs	Drops	Tr Bytes	ransn Pkts	hitted Errs	Drops	;	·	·	
Status > Si Interface Ethernet	Bytes 311419	>LA Recei Pkts 2762	N ved Errs 0	Drops 0	Tr Bytes 1909778	Pkts	Errs	Drops 0				

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

#### 8.4.2 3G Statistics

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

Net Gomman	'® 3G9	W – HSPA	A 7.2 Mbps Wi-Fi Router				
Basic	3G	Settings	Wireless	Management	Advanced	Status	
				•	•	Diagnostics	
Status > Statistics	; > 3G					System log	
Statistics of WAN	Inbound	Outbound	1			3G network	
Octects	10107	2339				Statistics	LAN
Octects	10107	2339				Statistics Route	LAN 3G networ
Octects Packets Drops	10107 113	2339 41				Statistics Route ARP	LAN 3G networ

Service	Shows the service type					
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.

<b>etGom</b>	30 au	<b>39W</b> - HSPA 7	.2 Mt	ops Wi-	Fi Route	er			
Basic		3G Settings		Wirele	55	Ma	nagement	Advanced	Status
	•					•		•	Diagnostics
Status > Rou	te								System log
Flags: U - up, !	- reject, G - ga	teway, H - host, R ·	- reinst	ate					3G network
D - dynamic (rei	direct), M - moo	dified (redirect).							Statistics
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface			Route
10 64 64 64	0.0.0.0	DEE DEE DEE DEE	110	0	0000	0000			ARP
10.04.04.04	0.0.0.0	200.200.200.200	on	0	pppo	pppo			
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0			

Field	Description
Destination	Destination network or destination host
Gateway	Next hop IP address
Subnet Mask	Subnet Mask of Destination
Flag	U: route is up
	!: reject route
	G: use gateway
	H: target is a host
	R: reinstate route for dynamic 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 WAN connection
Interface	Shows connection interfaces

#### ARP 8.6

Click ARP to display the ARP information.

<b>etGUII</b> netcomm.con	n.au	<b>3G9W</b> – HSPA	7.2 Mbps	Wi-Fi Router				
Basic		3G Settings	w	reless	Management	Adva	nced	Status
			•		•			Diagnostics
Status > ARI	Р							System log
TD address	Flage	HW Address	Device					3G network
100.440.4.0	riug <i>s</i>	1117 Huur C33	Lo					Statistics
192.168.1.2	Complete	UU:1D:UF:BE:AC:D7	DrU					Route
								ARP

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.

etcomm.com	nav sg9w	- HSPA 7.	2 Mbps Wi-F	i Router		
Basic	3G Se	ttings	Wireless	Management	Advanced	Status
					•	Diagnostics
Status > DH	CP Leases					System log
Hostname	M&F &ddress	IP Address	Expires In			3G network
mostinanite	The mode case	AT THOM COD	copies an			Statistics
		100 110 1 0				
test	00:1D:0F:BE:AC:D7	192.168.1.2	Expired			Route
test	00:1D:0F:8E:AC:D7	192.168.1.2	Expired			Route

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

Download from Www.Somanuals.com. All Manuals Search And Download.

# CLI commands Via Telnet

Download from Www.Somanuals.com. All Manuals Search And Download.

# CLI commands via Telnet

### Show all CLI commands

Description: List all available CLI commands that the 3G router supports.

Synopsis: help | ?

Example:

> help ? help logout reboot atm ddns dumpcfg ping sntp sysinfo tftp wlan sierra QOS version build



# End the telnet session

Description: End the telnet session

Synopsis: logout

Example:

> logout

#### Reset/reboot device Description: To reboot the router.

Synopsis: reboot

#### Example:

> reboot

# Radio Signal Strength

# Description: Display the 3G radio signal strength.

Synopsis: sierra show --signal

#### Example:

> sierra show --signal

signal: 23

Note: Signal value is explain in the table below

Value	2 ~ 5	6 ~ 10	11 ~ 13	14 ~ 17	18 ~ 31	99
Signal level in dBm	-109 ~ -103	-101 ~ -93	-91 ~ -87	-85 ~ -79	-77 ~ -52	unknown
5 Signal bars						
LED	Low		Medium		High	
# Radio Band Description: Display the 3G band

Synopsis: sierra show --band

#### Example:

> sierra show --band band: IMT2000

Note: IMT2000 is band 2100 and WCDMA800 is band 850

# Connection status

# Description: Display the 3G network connection status

Synopsis: sierra show -link

sierra show --gstatus

#### Examples:

> sierra show --link link: Connected

> sierra showgstatus	
Current Time: 450	Temperature: 45
Bootup Time: 1	Mode: ONLINE
System mode: WCDMA	PS state: Attached
WCDMA band: WCDMA800	GSM band: Unknown
WCDMA channel: 4436	GSM channel: 65535
GMM (PS) state:REGISTERED	NORMAL SERVICE
MM (CS) state: IDLE	NORMAL SERVICE

WCDMA L1 State:L1M\_FACH RX level (dBm):-90 RRC State: CELL\_FACH



# IMSI & IMEI read Description: Display the IMSI and IMEI value

Synopsis: sierra show --imsi sierra show --imei

#### Example:

> sierra show --imsi imsi: 466974800524867

> sierra show --imei

IMEI: 354219010024303

# Wireless LAN mode set and read

# Description: Allows user to configure the Wireless LAN interfaces on the 3G router.

This command can be use to configure basic feature, security feature, wireless bridge feature and MAC filter features of the wireless LAN interface.

Synopsis:

> wlan wlan command usage : wlan config [option] wlan security [option] wlan macfilter [option] wlan wds [option] wlan info [option] wlan –help

Each option will be explained separately below.

Note:

The settings changed from these commands take effect immediately and will be updated on the web page

1. Please enable the wireless BEFORE changing other wireless settings.

2. The wlan command will save the configuration into flash memory and the new settings will be saved.

Since the settings changed from wlan command take effect immediately, it is not recommended to modify the wireless settings through the Web UI at the same time.

# Configure basic Wireless LAN features

Description: Configure basic wireless LAN features such as 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.

Synopsis:

wlan config [--enable <0|1>] [--hide <0|1>]

[--ssid <ssidStr>] [--country <countryStr>]

[--isolate <0|1>]

[--channel <channelVal>] [--rate <rateVal>]

[--mrate <rateVal>]

[--rts <rtsThreshold>] [--frag <fragThreshold>]

[--dtim <dtimInterval>] [--beacon <beaconInterval>]

[--xpress <onloff>] [--gmode <autolperformancellrsl802.11b>]

[--gprotect <offlauto>] [--preamble <longlshort>]

# Options:

--enable <0|1>

#### Description: Enable or disable wireless LAN interface.

Valid value: 0 or 1

0 - disabled the wireless LAN interface.

1 - enabled the wireless LAN interface.

Default value: 1

--hide <0|1>

#### Description: Hide wireless LAN network name (SSID).

Valid value: 0 or 1 0 - not hide wireless LAN SSID.

1 – hide wireless LAN SSID

Default value: 0

--ssid <ssidStr>

#### Description: Set Wireless LAN network name (SSID).

Valid value: 32 characters string

--country <countryStr>

## Description: Set Wireless LAN Country, only accept abbreviation.

Valid value: 2 or 3 characters string (AUSTRALIA is abbreviated to AU).



#### --isolate <0|1>

# Description: Set wireless devices isolation. When enabled, wireless devices connected to the router will not be able to communicate to each other

Valid value: 0 or 1

0 - not isolate wireless devices.

1 – isolate wireless devices

Default value: 0

--channel <channelVal>

#### Description: Set the wireless LAN channel.

Valid value: 0~14 0 means auto select channel. Default value: 0

--rate <rateVal>

#### Description: Set the wireless LAN data rate.

Valid value: 0, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 (Mbps) 0 means auto Default value: 0

--mrate <rateVal>

#### Description: Set the wireless LAN Multicast rate.

Valid value: 0, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 (Mbps) 0 means auto Default value: 0

--rts <rtsThreshold>

#### Description: Set the wireless LAN RTS threshold.

Valid value: 0~2347 Default value: 2347 --frag <fragThreshold>

## Description: Set the wireless LAN fragment threshold.

Valid value: 256~2346 Default value: 2346

--dtim <dtimInterval>

#### Description: Set the wireless LAN DTIM interval.

Valid value: 1~255 Default value: 1

--beacon <beaconInterval>

#### Description: Set the wireless LAN beacon interval.

Valid value: 1~65535 Default value: 100

--xpress <onloff>

# Description: Enable or disable the xpress feature

Valid value: on / off Default value: off

--gmode <autolperformancellrsl802.11b>

#### Description: Set the wireless LAN G mode

Default value: auto

--gprotect <offlauto>

#### Description: Enable or disable the gprotect feature

Default value: auto

--preamble <longlshort>

#### Description: Set the wireless LAN preamble

Default value: long



# Example 1:

User wants to enable the wireless LAN, configure the wireless LAN network name (SSID) as "TestAP", configure wireless LAN channel to 5 and then hide the SSID:

wlan config --enable 1 wlan config --ssid "TestAP" wlan config --channel 5 --hide 1

Or merge the above commands

wlan config --enable 1 --ssid "TestAP" --channel 5 --hide 1

## Configure wireless LAN security

Description: Enable or disable and configure the wireless LAN security. This router supports different types of security such as: WEP, 802.1X, WPA and WPA2.

```
Synopsis:
```

```
wlan security open
    [--wep <enabled|disabled>] [--kevbit <64|128>]
             [--nkev1 <kevStr>] [--nkev2 <kevStr>]
    [--nkey3 <keyStr>] [--nkey4 <keyStr>]
    [--kevidx <1|2|3|4>]
wlan security shared (wep have to enable)
    [--wep <enabled|disabled>] [--keybit <64|128>]
    [--nkey1 <keyStr>] [--nkey2 <keyStr>]
    [--nkey3 <keyStr>] [--nkey4 <keyStr>]
    [--kevidx <1|2|3|4>]
wlan security radius (wep have to enable)
    [--rasip <serverlp>] [--raspt <portVal>] [--raskey <"raskeyStr">]
    [--wep <enabled|disabled>] [--kevbit <64|128>]
    [--nkey2 <keyStr>] [--nkey3 <keyStr>]
    [--kevidx <2|3>]
wlan security wpa / wpa2 / wpa2mix
    [--wlPreauth <0|1>] [--wlNetReauth <interval>]
    [--wpaenc <tkiplaes|tkip+aes>] [--rekey <interval>]
    [--rasip <serverlp>] [--raspt <portVal>] [--raskev <"raskevStr">]
    [--wep <enabledIdisabled>] [--keybit <64|128>]
    [--nkey2 <keyStr>] [--nkey3 <keyStr>]
    [--kevidx <2|3>]
wlan security psk / psk2 / psk2mix
    [--wpaenc <tkiplaesltkip+aes>] [--rekey <interval>]
    [--pskey <"pskeyStr">]
    [--wep <enabledIdisabled>] [--keybit <64|128>]
    [--nkev2 <kevStr>] [--nkev3 <kevStr>]
    [--keyidx <2|3>]
```



# Options:

--wep <enabledIdisabled>

Description: enable or disable WEP encryption

--keybit <64|128>

# Description: Set the WEP encryption strength

--nkey1 <keyStr>

--nkey2 <keyStr>

--nkey3 <keyStr>

--nkey4 <keyStr>

# Description: Set the WEP key.

 Note:
 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys

--keyidx <1|2|3|4>

# Description: Set the current WEP Key index.

--rasip <serverlp>

Description: Set the RADIUS server IP address.

--raspt <portVal>

# Description: Set the RADIUS server port.

Valid value: 1~65535 Default value: 1812

--raskey <raskeyStr>

# Description: Set the RADIUS Key.

Valid value: string of 79 characters.

--wpaenc <tkiplaesltkip+aes>

# Description: Set the WPA encryption

--rekey <interval>

#### Description: Set the Group Rekey Interval

Default value: 0

--pskey <"pskeyStr">

#### Description: Set the WPA Pre-Shared Key

Valid value: string of  $8 \sim 63$  characters.

#### Note: 1. wlPreauth can only be used with WPA2.

2. When using WPA-PSK or WPA2-PSK, WPA Pre-Shared Key (pskey) must be set first.

3. WEP MUST be enable when security is set to shared / 802.1X radius security mode.

4. WEP MUST be disable when security is set to WPA/WPA-PSK security mode

5. When setting keyidx to N for WEP key, ensure that the nkeyN field has a string value.

6. Always issue a complete security command. For example, once WEP is enabled, it will still be enabled even after changing the security mode, until the command "--wep disabled" is received by the router.

#### Example 2:

After setting up the wireless configuration in example 1, the user wants to configure the wireless LAN security.

#### Scenario 1:

WPA2 with Radius server IP address of 172.16.2.199

wlan security wpa2 --rasip 172.16.2.199 --wlPreauth 1

#### Scenario 2:

WPA-PSK with "123456789" as the passkey.

wlan security psk --pskey "123456789" --wpaenc aes --wep disabled

#### Scenario 3:

802.1X with Radius server IP of 172.16.2.199 and RADIUS key as "whatever"

wlan security radius --rasip 172.16.2.199 --raskey "whatever" --wep enabled



# Configure wireless LAN MAC filter

Description: Enable, disable and configure the wireless LAN MAC filter feature. This feature enables the router to allow or deny connection from wireless client based on the MAC address.

Synopsis:

wlan macfilter [--mode <disabledlallowldeny>]

[--add <MACaddress>]

[--remove <MACaddress>]

#### Options:

--mode <disabledlallowldeny>

#### Description: Disable and set the wireless LAN MAC filter mode.

Valid Value:

Disabled: disable wireless LAN MAC filter

Allow: only allow access to wireless client with the MAC address listed in the router Deny: allow all wireless client to connect unless the MAC address is listed in the router Default Value: disabled

--add <MACaddress>

### Description: add one MAC Address entry

--remove <MACaddress>

#### Description: remove one MAC Address entry

Note: The setting of the MAC filter takes effect immediately. When setting up this feature through the wireless interface, be careful of blocking the computer. Changing the mode will make the MAC address list be reserved. To see the list of MAC addresses, use the command "wlan info –macfilter".

#### Example 3:

After Example 2, the user want to allow only wireless client with MAC address of 00:11:22:33:44:55 to be able to connect to the router

wlan macfilter --mode allow --add 00:11:22:33:44:55

Following the command above, if the user wants to deny wireless client with MAC address of 00:11:22:33:44:55 to be able to connect to the AP.

wlan macfilter --mode deny

# Configure Wireless Bridge (Wireless Distribution System/WDS) Description: configure the wireless bridge

Synopsis:

wlan wds [--mode <aplwds>] [--restrict <enabledldisabled>] [--rmac1 <MACaddress>] [--rmac2 <MACaddress>] [--rmac3 <MACaddress>] [--rmac4 <MACaddress>]

#### **Options:**

--mode <aplwds>

#### Description: configure wireless AP mode.

Default value: ap

--restrict <enabledldisabled>

#### Description: enable or disable bridge restrict mode.

Default value: disabled

- --rmac1 <MACaddress>
- --rmac2 <MACaddress>
- --rmac3 <MACaddress>
- --rmac4 <MACaddress>

#### Description: set remote bridge MAC address

Note: The "--restrict" option have to be enable before setting any restrict MAC address (--rmac1~4) or the restrict MAC address setting will be ignored.

The behavior of WDS is similar to connecting two or more AP using a hub. However, please be aware of the IP assignment to prevent assigning two or more hosts / STAs to the same IP address. To avoid IP address conflict, only enable DHCP server in one router and disable the other router DHCP server.

WDS CLI (command line interface) does NOT support Enable(Scan) mode in Bridge Restrict while using WUI (Web UI) does. When Bridge Restrict set to Enable(Scan) mode in WUI, the CLI will show Bridge Restrict disabled.

#### Example 4:

After example 3, the user want to connect another AP which has DHCP disabled and the MAC address is 00:12:34:56:78:9a

wlan wds --mode wds --restrict enabled --rmac1 00:12:34:56:78:9a



# Show wireless LAN interface configurations

Description: show the current configuration of the wireless LAN interface

Synopsis:

wlan info [--config] [--security] [--macfilter] [--wds] [--station]

#### Options:

--config

Description: display the list of parameters from config option

#### Example:

> wlan info --config Wlan Config Info :

Basic :

wlan config enable = 1 wlan config hide = 0 wlan config ssid = Series7Wireless7890 wlan config bssid = 00:11:22:33:44:56 wlan config country = AU

Advance :

wlan config isolate = 0 wlan config band = b wlan config channel = 0 wlan config rate = 0 wlan config mrate = 0 wlan config brate = default wlan config trs = 2347 wlan config frag = 2346 wlan config dtim = 1 wlan config beacon = 100 wlan config press = off wlan config gmode = auto wlan config gprotect = auto wlan config preamble = long --security

# Description: display the list of parameters from security option

# Example:

> wlan info --security Wlan Security Info : wlan security auth mode = psk wlan security wpa = aes wlan security wpaGTKRekey = 0 wlan security wpaPresharedKey = 1234567890 wlan security Wepstate = disabled wlan security Wepstate = 128 wlan security WepKey2 = wlan security WepKey3 = wlan security WepCurrentKeyindex = 1

--macfilter

# Description: display the list of parameters from macfilter option Example:

> wlan info --macfilter
 Wlan macfilter Info :
 wlan macfilter mode = disabled
 wlan macfilter entry :

--wds

# Description: display the list of parameters from wds opiton

#### Example:

```
    > wlan info --wds
    Wlan wds Info :
    wlan wds mode = ap
    wlan wds restrict mode = disabled
```

#### --station

# Description: display the list of authenticated wireless stations and their status Example:

> --wlan info --station

--wlan info --station: not found



# **Contact Information**

If you have any technical difficulties with your product, please do not hesitate to contact NetComm's Customer Support Department. **Email: support@netcomm.com.au** 

#### www.netcomm.com.au

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.



NetComm Limited ABN 85 002 490 486 PO Box 1200, Lane Cove NSW 2066 Australia E – sales@netcomm.com.au W – www.netcomm.com.au

Download from Www.Somanuals.com. All Manuals Search And Download.

Free Manuals Download Website <u>http://myh66.com</u> <u>http://usermanuals.us</u> <u>http://www.somanuals.com</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.com</u> <u>http://www.404manual.com</u> <u>http://www.luxmanual.com</u> <u>http://aubethermostatmanual.com</u> Golf course search by state

http://golfingnear.com Email search by domain

http://emailbydomain.com Auto manuals search

http://auto.somanuals.com TV manuals search

http://tv.somanuals.com