NETCOMM WIRELESS M2M SERIES

HSPA+ M2M WiFi Router

NTC-40WV

USER GUIDE

Copyright

⚠ **Please note:** This document is subject to change without notice.

Save Our Environment

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

The cardboard box, the plastic contained in the packaging, and the parts that make up this device can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

This manual covers the following products:

NetComm NTC-40WV

DOCUMENT VERSION	DATE
1.0- Initial document release	05/12/2011

Table 1 - Document Revision History

Table of Contents

Overview

Introduction

This document provides you all the information you need to set up, configure and use the NTC-40WV router. .

Target Users

This document is intended for system integrators or experienced hardware installers who understand telecommunications terminology and concepts.

Prerequisites

Before continuing with the installation of your NTC-40WV, please confirm that you comply with the minimum system requirements below.

- An activated 3G SIM card.
- Device with a working Ethernet or wireless (802.11b/g/n) network adapter.
- A Web Browser such as Internet Explorer, Netscape Navigator, Mozilla Firefox, Opera, Safari etc.

Telephony Requirements

- Standard analogue PSTN or cordless PSTN phone handset (DECT) with an RJ-11 port.

  (ISDN phone handsets are not supported)
- RJ-11 cable

Notation

The following symbols are utilised in this installation manual:

- ⚠

The following note requires attention

- ⚡

The following note provides a warning

- ℹ

The following note provides relevant information

Product Introduction

Product Overview

- Industrial-grade fixed wireless gateway with extended temperature tolerance and wall mount option.
- Designed for rugged deployments in remote environments and industrial applications.
- Ideal for providing primary and backup wireless connectivity over 3G UMTS networks.
- Embedded high-performance Sierra Wireless 3G cellular modem supporting HSPA+/EDGE/GPRS.
- Wireless LAN 802.11n access point with 2x2 MIMO antenna technology.
- Powerful processor for optimal performance on advanced 3G UMTS networks.
- Ethernet 10/100 connectivity for universal deployment.
- Analogue telephone connectivity (CS Voice) for complete landline replacement.
- Supports SNMP with cellular specific MIB.
- Flexible DC power input and to suit diverse installation environments.
- Built-in VPN clients for a secure connection over a public cellular network.
- GPS support for remote asset tracking.
- Embedded NetComm Linux OS and Software Development Kit (SDK).
- Remote diagnostics, configuration and firmware upgrade capabilities.
- Supports PPPoE, RIP, VRRP. DDNS, MAC /NET address filtering, Open VPN, DHCP/DHCP relay.
- Management and configuration via web user interface, SNMP or SMS.

Package Contents

The NTC-40WV series package consists of:

- NetComm Wireless NTC-40WV - HSPA+ M2M WiFi Router
- 1 x Power supply (8-28VDC)
- 1 x Quick Start Guide
- 2 x 3G Antennas (SMA connector)
- 2 x WiFi Antennas (SMA connector)
- 1 x RJ-45 Ethernet Cable

If any of these items are missing or damaged, please contact NetComm Support immediately by visiting the NetComm Support website at: http://www.netcomm.com.au/contact-us/technical-support

Product Features

The NTC-40WV is a robust 3G (HSPA+) router is designed to provide real-time M2M data connectivity even in harsh environments, and allows you to build wide area networks utilising the superior speeds supported by 3G UMTS networks.

The router integrates a powerful Sierra module (MC8704) and delivers download speeds of up to 21Mbps which is then transmitted via Ethernet to a WiFi router inside the property.

Utilising a NetComm M2M router allows customers to significantly reduce the cost for the deployment and operation of new products and services in remote locations. Using mobile data networks, wireless Machine-to-Machine (M2M) communication enables the secure collection and analysis of data from remote unmanned locations.

The NTC-40WV provides the user a point-to-point or point-to-multi-point communications link in a single, compact and resilient unit. As a fully featured cellular router, it supports a large number of communication interfaces and protocols to meet the demands of today's telemetry and WAN applications.

The integrated telephone adapter connects standard analogue phone handsets to the NTC-40WV. It allows for phone calls to be made over the 3G UMTS network from inside the premise for a full landline replacement.

The device's powerful processor delivers optimal performance and it's embedded NetComm Linux OS and Software Development Kit (SDK) offers the end user the capability to install custom firmware to the on-board flash memory via the programming interface. Built in VPN clients also ensure a secure connection over a public mobile network.

Designed with remote installation in mind the NTC-40WV series supports multi-level system monitoring giving the user peace of mind the device will keep the lines of communication up and open.

In the event of system corruption, a built-in recovery mode provides the facility to re-install the system software to the router and resume normal operations quickly.

Physical Dimensions and Indicators

LED Indicators

The NTC-40WV uses 5 LEDs to display the current system and connection status.

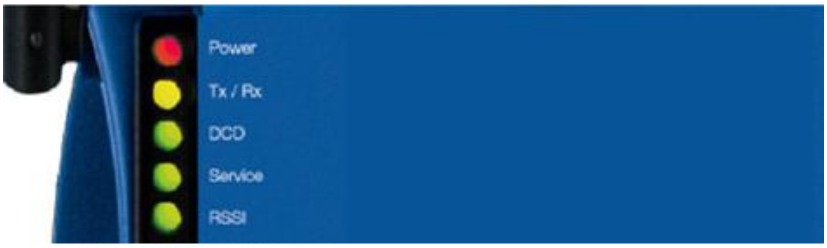


Figure 1 - NTC-40WV LED Indicators

LED	DISPLAY	DESCRIPTION
POWER (red)	Solid ON	The red Power LED indicates correct power is applied to the DC power input jack.
Tx Rx (amber)	Solid ON	The amber LED will light upon data being sent to or received from the cellular network.
DCD (green)	Solid ON	The green Carrier Detect LED illuminates to indicate a Data connection.
Service Type (green)	The green LED will illuminate when cellular network coverage is detected.	
	Solid On	3G: indicates UMTS/HSPA available coverage.
	Blinking	EDGE: indicates EDGE available coverage.
	Off	2G: indicates GSM/GPRS available coverage only.
RSSI (green)	This green LED indicates the received signal strength. There are three possible states that the RSSI LED can operate in, based upon signal level.	
	Solid ON	HIGH - Indicates the RSSI level is -77dBm (high), or greater.
	Flashing once per second	MEDIUM - Indicates the RSSI level is -91dBm and –78dBm (medium).
	Off	LOW - Indicates the RSSI level is less than -92dBm (low).

Table 2 - LED Indicators

Physical Dimensions

The following page lists the physical dimensions of the NTC-40WV, as well as the physical dimensions of the antennas and the included mounting bracket which can be used to attach the NTC-40WV to a pole or to provide a wall / ceiling mount.

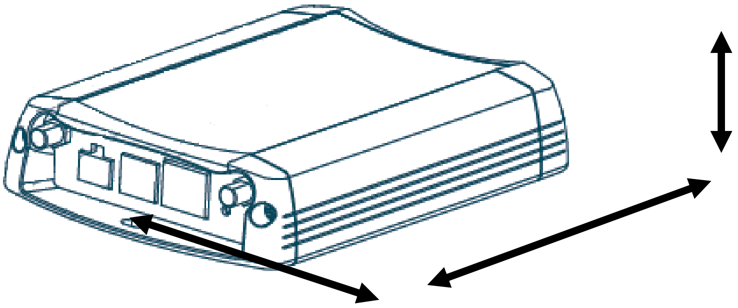


Figure 2 – NTC-40WV Dimensions

NTC-40WV (WITHOUT ANTENNAS ATTACHED)	
Length	155 mm
Depth	104 mm
Height	30 mm
Weight	300 g

Table 3 - Device Dimensions

Integrated Interfaces

The following integrated interfaces are available on the NTC-40WV:

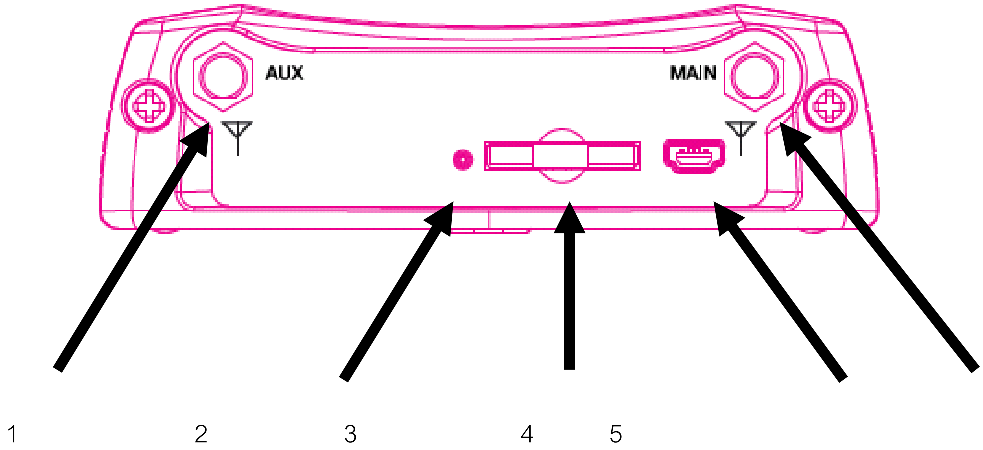


Figure 3 - Bottom Mounted Integrated Interfaces

ITEM	INTERFACE	FUNCTION
1	Diversity Receive 3G Antenna	Connect one of the 3G antennas here
2	SIM Card Reader Tray Eject button	Push in with a paper clip to eject the SIM card reader tray.
3	SIM Card Reader Tray	Insert the SIM Card reader tray with a SIM inserted here.
4	Mini USB 2.0 Console Port	Connect a Mini USB cable to access the NTC-40WV console here. The current firmware version does not implement this port but it may be included in a future firmware release.
5	Main 3G Antenna	Connect one of the 3G antennas here.

Table 4 - Bottom Mounted Integrated Interfaces

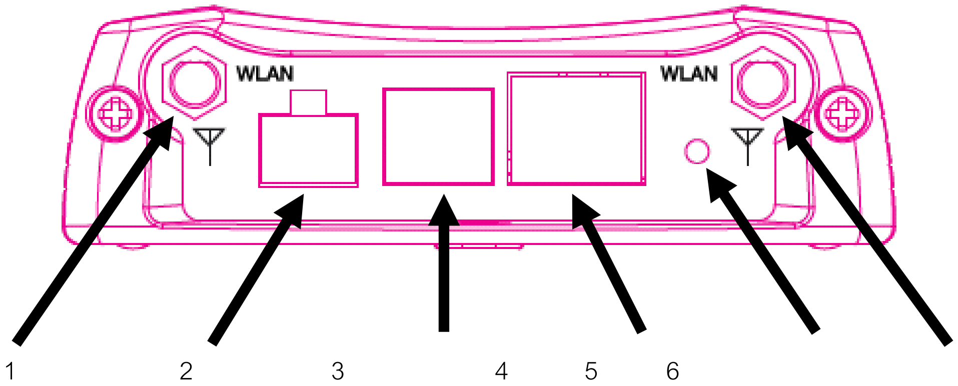


Figure 4 - Top Mounted Integrated Interfaces

ITEM	INTERFACE	FUNCTION
1	WiFi Antenna Port	Connect one of the WiFi antennas here
2	Captive Power Terminal	Connect the supplied power cable here.
3	RJ-11 Telephone Cable Port	Connect a PSTN telephone here in order to make calls via the 3G connection.
4	RJ-45 Ethernet Port	Connect an Ethernet cable here.
5	Reset button	To reboot the router push and hold the reset button for one second to reboot the NTC-40WV. To boot the router into system recovery mode hold the reset button for approximately 10 seconds until the LEDs on the front of the router start to flash in an ON / OFF sequence and then release it.

6	WiFi Antenna Port	Connect one of the WiFi antennas here.

Table 5 - Top Mounted Integrated Interfaces

NTC-40WV Default Settings

The following tables list the default settings for the NTC-40WV.

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

Table 6 - LAN Management Default Settings

WIRELESS (WIFI)	
SSID:	NetComm Wireless XXXX where XXXX are a set of 4 random digits.
Security:	WPA2-PSK
Security Key:	Check your Wireless Security Card or the device label on the bottom of the NTC-40WV for your default SSID and Security key.

Table 7 – WiFi Default Settings

For security purposes, it is recommended to change the Default SSID and Wireless Security Key.

NTC-40WV WEB INTERFACE ACCESS	
Username:	admin /root
Password:	admin

Table 8 - Web Interface Default Settings

NTC-40WV TELNET ACCESS	
Username:	root
Password:	bovine

Table 9 - Telnet Access

Logging into the router with the username of root gives extended System options such as the ability to reboot the router, upgrade the firmware and install extra packages.

Restore Factory Default Settings

Restoring factory defaults will reset the NTC-40WV to its factory default configuration. Occasions may present themselves where you need to restore the factory defaults on your NTC-40WV such as:

- You have lost your username and password and are unable to login to the web configuration page;
- You have purchased your NTC-40WV from someone else and need to reconfigure the device to work with your 3G service;
- You are asked to perform a factory reset by support staff.

In order to restore your NTC-40WV to its factory default settings, please follow these steps:

- Ensure that your NTC-40WV Router is powered on (for at least 10 seconds);
- Use a paper clip or a pencil tip to depress the reset button for ten seconds until the LEDs on the front of the router start to flash in an ON / OFF sequence and then release.
- At this point, refresh your browser and check that the banner now reads “NetComm NTC-40WV Cellular Router Recovery Console”.
- Select the Settings option from the menu before selecting the “Restore” button.
- When the Power light returns to a steady red, the reset is complete. The default settings are now restored. The entire process takes about 45 seconds to complete.

Once you have reset your NTC-40WV Router to its default settings you will be able to access the device’s configuration web interface using http://192.168.1.1 with username ‘admin’ or ‘root’ and password ‘admin’.

Implementation and Deployment Scenario

The robust and intelligent HSPA+ M2M WiFi Router NTC-40W is designed to provide real-time M2M data connectivity in a single device even in harsh environments.

Utilising a NetComm M2M router allows customers to significantly reduce the cost for the deployment and operation of new products and services in remote locations. Using mobile data networks, wireless Machine-to-Machine (M2M) communication enables the secure collection and analysis of data from remote unmanned locations.

The NTC-40W creates reliable point-to-point or point-to-multi-point wide area network (WAN) connections for a variety of mission critical applications such as primary broadband, video surveillance, retail, payments, in-vehicle wireless hotspot and business continuity.

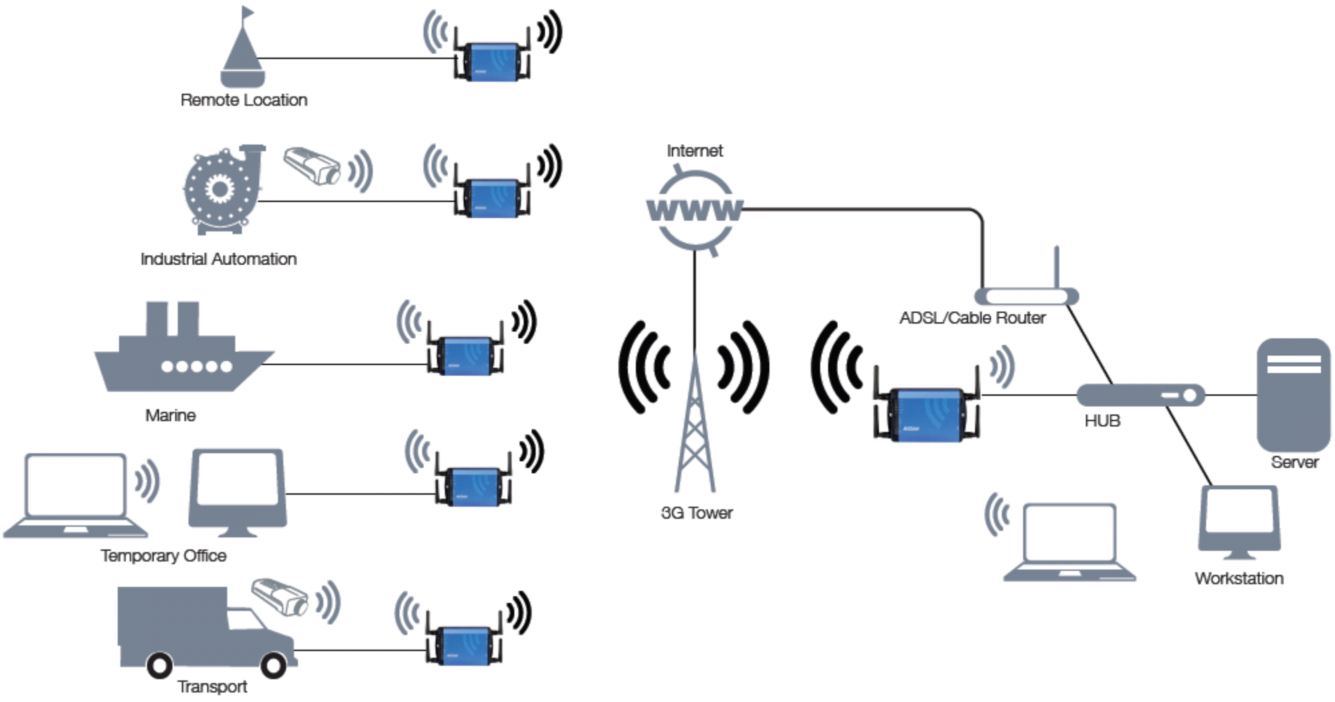


Figure 5 - Typical NTC-40WV Deployment

Installation and Configuration of the NTC-40WV

Connecting via an Ethernet cable

1. Connect the Ethernet cable provided to the port marked “Ethernet” on the side of the NTC-40WV.
2. Connect the other end of the yellow Ethernet cable to your computer.
3. Wait approximately 30 seconds for the connection to establish.

Connecting via wireless

1. Ensure WiFi is enabled on your device (computer/laptop/Smartphone).
2. Scan for wireless networks in your area and connect to the network name that matches the Wireless network name configured on the NTC-40WV.
3. When prompted for your wireless security settings, enter the Wireless security key configured on the NTC-40WV.
4. Wait approximately 30 seconds for the connection to establish.

Configuring the NTC-40WV

1. After connecting via Ethernet cable or wirelessly, open your Web browser, and enter http://192.168.1.1 into the address bar and press enter.
2. Follow the steps on the next pages to set up your NTC-40WV.

Web based User Interface

To log in to the management console and view the status and make changes to your NTC-40WV, please follow the steps below:

1. Open your web browser (e.g. Internet Explorer/Firefox/Safari) and navigate to http://192.168.1.1
2. Enter the username and password configured during the first time setup and click the “Submit” button. The default username and password is “admin” if the details haven’t been customized. Click the “Submit” button to continue.

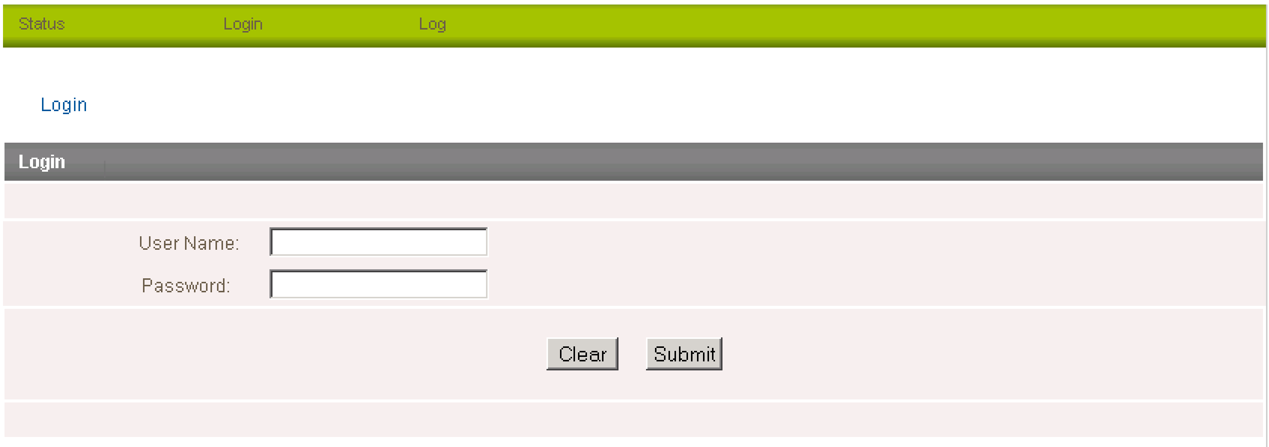
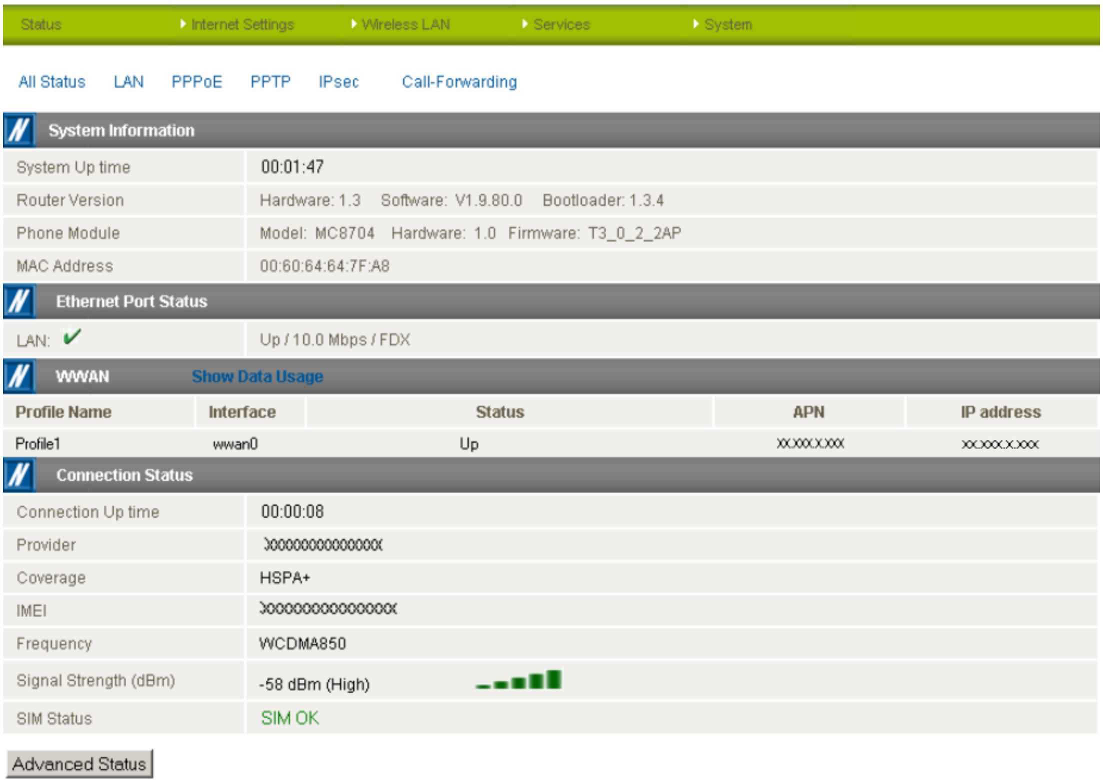


Figure 6 - Login prompt for the Web based User Interface

After logging in, the Status page should then be displayed.

Status

The status page provides system related information and is displayed when you login to the NTC-40WV management console. By default, the status page will show System Information, Ethernet Port Status, WWAN Status, IPSec Status and the 3G service connection details.



System Information	
System Up time	00:01:47
Router Version	Hardware: 1.3 Software: V1.9.80.0 Bootloader: 1.3.4
Phone Module	Model: MC8704 Hardware: 1.0 Firmware: T3_0_2_2AP
MAC Address	00:60:64:64:7F:A8

Ethernet Port Status	
LAN: ✓	Up / 10.0 Mbps / FDX

WWAN Show Data Usage

Profile Name	Interface	Status	APN	IP address
Profile1	wwan0	Up	XX.XXX.X.XXX	XX.XXX.X.XXX

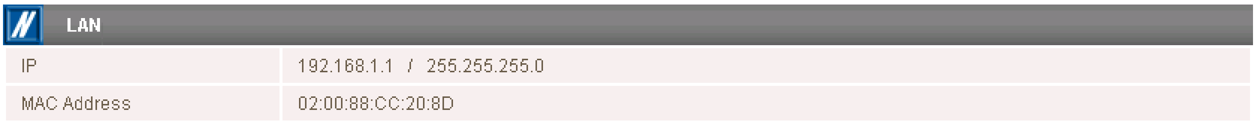
Connection Status	
Connection Up time	00:00:08
Provider	XXXXXXXXXXXXXXX
Coverage	HSPA+
IMEI	XXXXXXXXXXXXXXXX
Frequency	WCDMA850
Signal Strength (dBm)	-58 dBm (High)
SIM Status	SIM OK

Figure 7 - The Status Page

ITEM	DEFINITION
System Uptime	The current uptime of the router.
Router Version	The firmware version running on the router.
Phone Module	The type of phone module and the firmware version of the module.
Serial Number	The serial number (MAC Address) of the router.
Ethernet Port Status	The current speed and status of the Ethernet port.
WWAN	The current connection profile, Interface, status, APN, local and remote addresses of the WWAN connection.
Provider	The current 3G service provider detected.
Coverage	The type of 3G connection available for use.
IMEI	The IMEI (International Mobile Equipment Identity) of the router, a unique code for identifying devices on a GSM network.
Frequency	The frequency band currently in use.
Signal Strength	The strength of the 3G signal detected
SIM Status	The status of the SIM currently inserted into the router.

Table 10 - Status page items

To view the LAN, PPPoE or PPTP status individually, click on their relevant links below the green menu bar. To view them all, click on the All Status link.



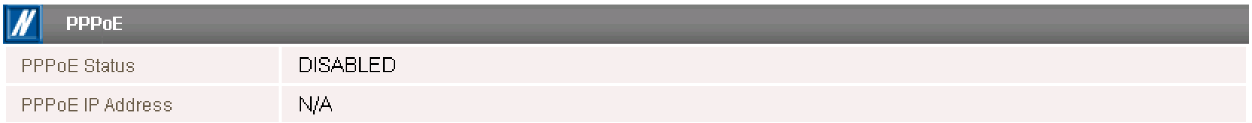
LAN

IP	192.168.1.1 / 255.255.255.0
MAC Address	02:00:88:CC:20:8D

Figure 8 - Status Page - LAN Details

ITEM	DEFINITION
IP	The current LAN IP Address and Subnet Mask.
MAC Address	The current MAC Address of the LAN port.

Table 11 - Status Page - LAN Details



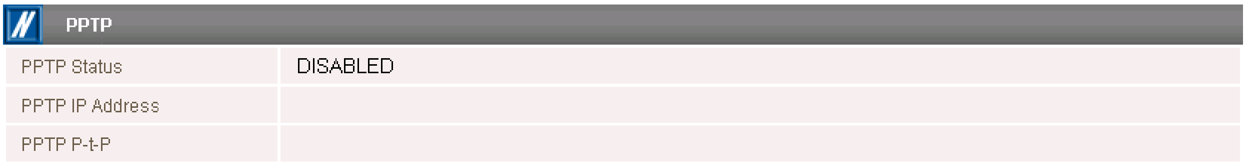
PPPoE

PPPoE Status	DISABLED
PPPoE IP Address	N/A

Figure 9 - Status Page - PPPoE Details

ITEM	DEFINITION
PPPoE Status	The current status of the PPPoE connection.
PPPoE IP Address	The current PPPoE IP Address in use.

Table 12 - Status Page - PPPoE Details



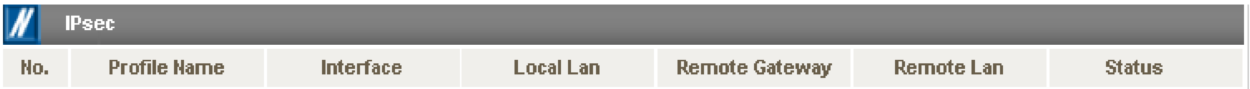
PPTP

PPTP Status	DISABLED
PPTP IP Address	
PPTP P-t-P	

Figure 10 - Status Page - PPTP Details

ITEM	DEFINITION
PPTP Status	The current status of the PPTP connection.
PPTP IP Address	The current PPTP connection IP Address.
PPTP P-t-P	The current PPTP Remote Gateway Address.

Table 13 - Status Page - PPTP Details

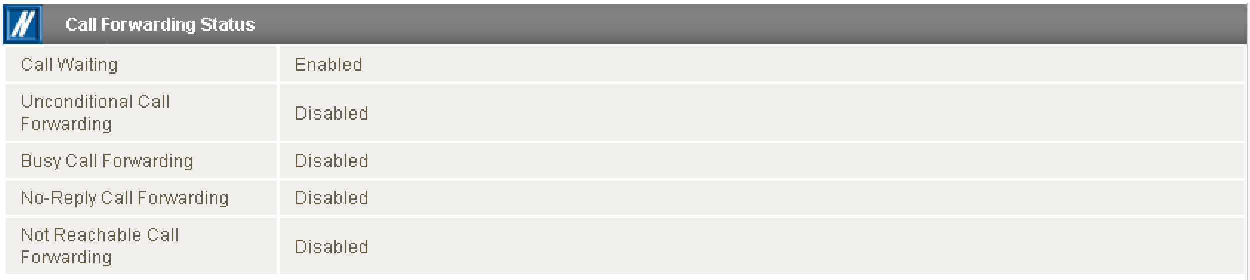


IPsec

No.	Profile Name	Interface	Local Lan	Remote Gateway	Remote Lan	Status

ITEM	DEFINITION
No	The number of the IPSec tunnel.
Profile Name	The Profile name of the IPSec tunnel.
Interface	The interface used by the IPSec tunnel.
Local LAN	The local LAN IP address of the IPSec tunnel.
Remote Gateway	The Remote Gateway IP address of the IPSec tunnel.
Remote LAN	The Remote LAN IP address of the IPSec tunnel.
Status	The current status of the IPSec tunnel.

Table 14: Status Page - IPSec Details



Call Forwarding Status

Call Waiting	Enabled
Unconditional Call Forwarding	Disabled
Busy Call Forwarding	Disabled
No-Reply Call Forwarding	Disabled
Not Reachable Call Forwarding	Disabled

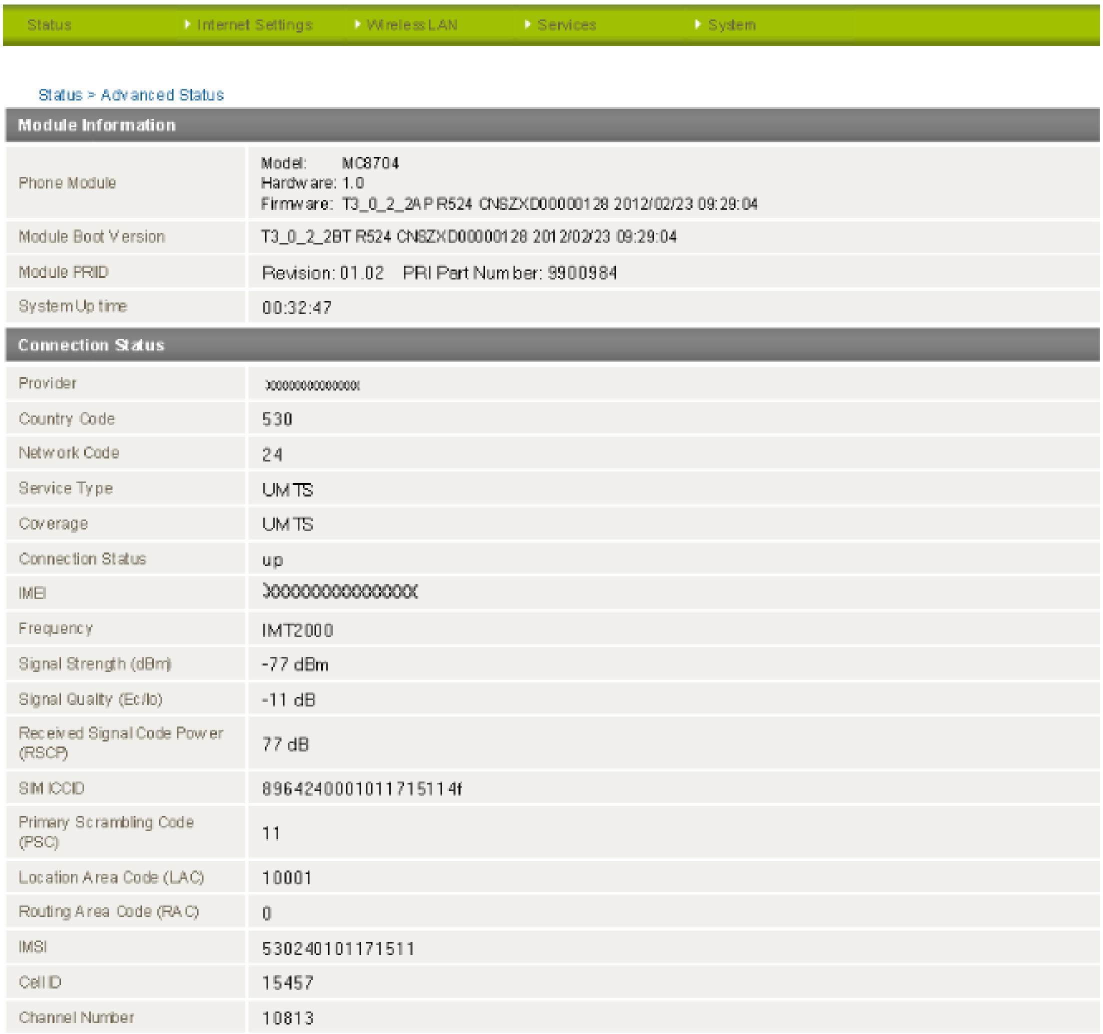
ITEM	DEFINITION
Call Waiting	Call waiting allows for indication and answering of an incoming telephone whilst an existing call is underway.
Unconditional Call Forwarding	Call forwarding Unconditional will divert all incoming calls to a phone number that you desire.

Busy Call Forwarding	Call forwarding busy will divert all incoming calls to a phone number that you desire only if your telephone is busy on another call.
No-Reply Call Forwarding	Call forwarding busy will divert all incoming calls to a phone number that you desire only if there is no reply from your telephone.
Not Reachable Call Forwarding	Call forwarding not reachable will divert all incoming calls to a phone number that you desire only if your telephone is unreachable by the network.

Table 15: Status Page - Call Forwarding Settings

Advanced Status

The Advanced Status page provides advanced system related information and is displayed when you click on the Advanced Status button at the bottom of the NTC-40WV status page. The Advanced Status page shows information regarding the on-board 3G module as well as statistics of the current 3G connection.



Module Information	
Phone Module	Model: MC8704 Hardware: 1.0 Firmware: T3_0_2_2AP R524 CNSZXD00000128 2012/02/23 09:29:04
Module Boot Version	T3_0_2_2BT R524 CNSZXD00000128 2012/02/23 09:29:04
Module PRID	Revision: 01.02 PRI Part Number: 9900984
System Up time	00:32:47
Connection Status	
Provider	xxxxxxxxxxxxxxx
Country Code	530
Network Code	24
Service Type	UMTS
Coverage	UMTS
Connection Status	up
IMEI	XXXXXXXXXXXXXXX
Frequency	IMT2000
Signal Strength (dBm)	-77 dBm
Signal Quality (Ec/Io)	-11 dB
Received Signal Code Power (RSCP)	77 dB
SIM ICCID	896424000101171511 4f
Primary Scrambling Code (PSC)	11
Location Area Code (LAC)	10001
Routing Area Code (RAC)	0
IMSI	530240101171511
Cell ID	15457
Channel Number	10813

Figure 11: Status - Advanced Status

Please see Table 14 on the following page for a description of the Advanced Status page items.

Advanced Status Item Details

ITEM	DEFINITION
Phone Module	The phone module name, hardware and firmware version
Module Boot Version	The installed boot loader version of the phone module.
Module PRID	The Protocol ID of the phone module.
System Uptime	The time in minutes and seconds that the router has been up.
Provider	The current connection's 3G provider.
Country Code	Each country has a unique code that helps to identify the 3G network.
Network Code	Each 3G provider has a unique network code for network identification purposes.
Service Type	The type of 3G service the current connection is using. Many networks use both a 3G and 2G connection simultaneously.
Coverage	The coverage type of 3G service the current connection is using.
Connection Status	The current status of the router's connection.
IMEI	The International Mobile Equipment Identity number unique to each cellular network device.
Frequency	The frequency of the current connection.
Signal Strength (dBm)	The signal strength of the 3G connection measured in decibels.
Signal Quality (Ec/Io)	A measurement of the portion of the received signal that is usable. This is basically the signal strength minus the signal noise level.
Received Signal Code Power (RSCP)	The power level of the signal on the current connection's particular channel.
SIM ICCID	The Integrated Circuit Card Identifier of the SIM card used with the router, a unique number up to 19 digits in length.
Primary Scrambling Code (PSC)	The Primary Scrambling Code for the current signal.
Location Area Code (LC)	The ID of the cell tower grouping the current signal is broadcasting from.
Routing Area Code (RAC)	The Routing Area Code is a subset of the Location Code and helps to identify the group of or individual cell towers the current connection's is broadcasting from.
IMSI	The International Mobile Subscriber Identity is a unique identification for the current 3G connection.
Cell ID	A unique code that identifies the base station from within the Location Area where the current 3g signal.
Channel Number	The channel number of the current 3G connection.

Table 16: Status - Advanced Status Item Details

Internet Settings

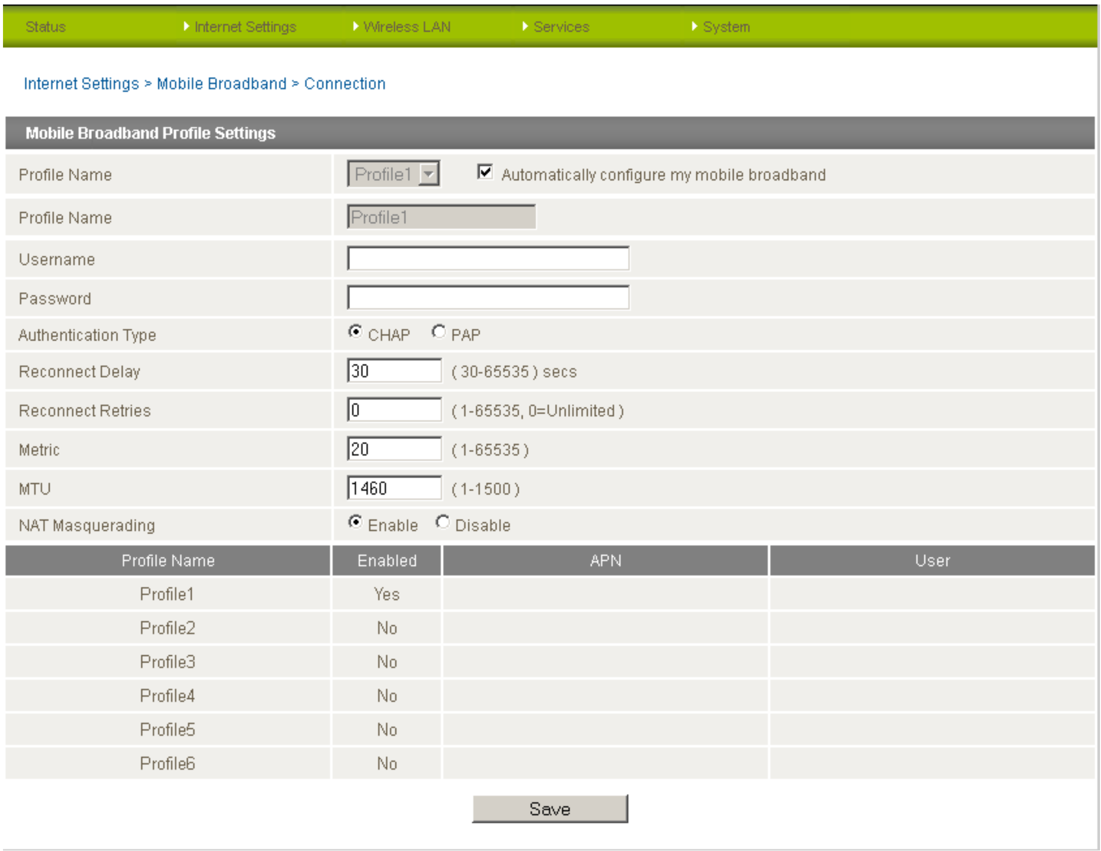
This section describes how to set up the router to initiate a mobile broadband connection. There are 2 different ways to set up a mobile broadband connection via PPP:

- Initiating the PPP Connection directly from the router (most common).
- Initiating the PPP Connection from a different PPP client (i.e. laptop or router) with the router running in transparent PPPoE mode.

Mobile Broadband

Connection

Click on the "Internet Settings" menu followed by "Mobile Broadband" and then the "Connection" menu item on the right.



Internet Settings > Mobile Broadband > Connection

Mobile Broadband Profile Settings

Profile Name	Profile1 ☑ Automatically configure my mobile broadband
Profile Name	Profile1
Username	
Password	
Authentication Type	● CHAP ○ PAP
Reconnect Delay	30 (30-65535) secs
Reconnect Retries	0 (1-65535, 0=Unlimited)
Metric	20 (1-65535)
MTU	1460 (1-1500)
NAT Masquerading	● Enable ○ Disable

Profile Name	Enabled	APN	User
Profile1	Yes		
Profile2	No		
Profile3	No		
Profile4	No		
Profile5	No		
Profile6	No		

Figure 12 - Connection Settings

<u>To connect using a Connection profile</u>

The router supports multiple APN profiles; these profiles allow you to configure the settings that the router will use to connect to the 3G network. By default, the "Profile 1" profile is selected. If the "Automatically configure my mobile broadband" option is selected the router should automatically detect the applicable APN from the inserted SIM after a reboot.

You can also manually enter the connection details by performing the following steps:

1. Select the profile that you wish to configure
2. Enter a name for the connection (if needed) in the "Change Profile Name" field.
3. Select the appropriate connection type.
4. Enter the APN (and if required the username and password).
5. Select "Enable" for the Auto Connect option.
6. Select the Authentication Type.
7. Enter the Reconnect Delay (if needed - the default should be suitable in most cases).
8. Enter the number of Reconnection attempts the router should make.
9. Enter the network metric for the connection.
10. Select to enable or disable NAT Masquerading for the connection.

11. Click Save

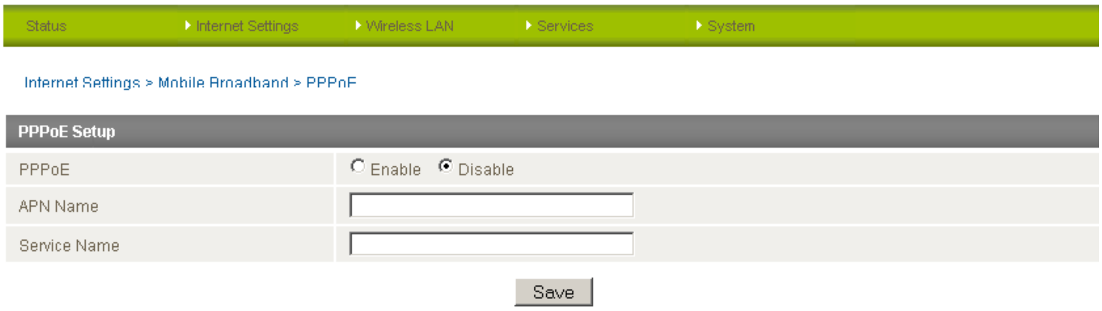
To confirm successful connection

1. Click on the Status menu item at the top of the page to return to the Status page.
2. The WWAN (mobile broadband) status should be "up".
3. The Local field should show the current IP address that the network has allocated for the router.
4. Congratulations. Your new router is now ready to use!

PPPoE

The PPPoE page is used to configure a transparent PPPoE connection. This can be used to provide a bridged connection.

To enable PPPoE mode, firstly ensure the "Auto Connect" is disabled in all the profiles on the "Connection" configuration page by clicking on the "Internet Settings" menu followed by "Mobile Broadband" and then the "Connection" menu item on the right and select each connection profile and disable the Auto Connection option and save the updated settings..



Internet Settings > Mobile Broadband > PPPoE

PPPoE Setup

PPPoE	○ Enable ● Disable
APN Name	
Service Name	

Figure 13 - PPPoE Settings

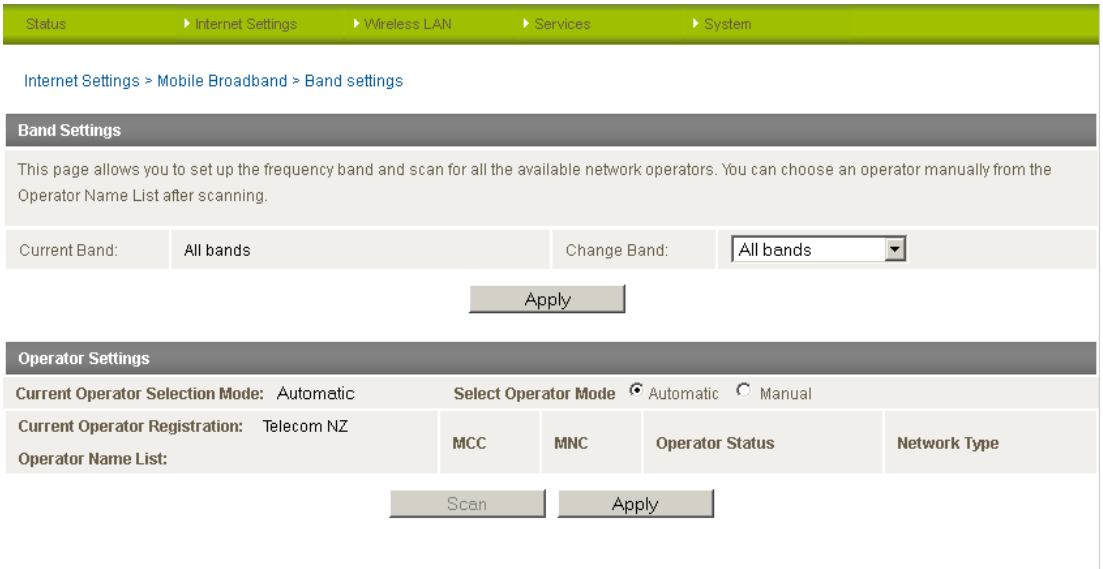
1. Select "Enable" to enable PPPoE.
2. Specify the APN supplied by your 3G provider.
3. Specify a "Service Name". *(Optional)*

This is particularly useful if you have more than one PPPoE router or modem on a single Ethernet network.

Click "Save" to save your settings and enable PPPoE.

Band / Provider

The band settings page enables you to select which frequency band you will use for your connection and enable you to scan for available network operators in your area.



Internet Settings > Mobile Broadband > Band settings

Band Settings

This page allows you to set up the frequency band and scan for all the available network operators. You can choose an operator manually from the Operator Name List after scanning.

Current Band:	All bands	Change Band:	All bands

Apply

Operator Settings

Current Operator Selection Mode: Automatic   Select Operator Mode ● Automatic ○ Manual

Current Operator Registration: Telecom NZ Operator Name List:	MCC	MNC	Operator Status	Network Type

Scan Apply

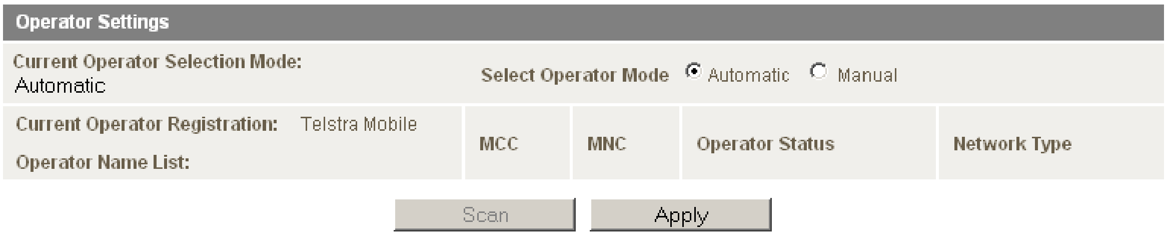
Figure 14 - Band / Provider Selection

You may want to do this if you're using the router in a country with multi frequency networks that may not all support HSPA. You can select the router to only connect on the network frequencies that suit your requirements.

Make your selection from the “Change Band:” drop down list.

The default setting of “All bands” should be appropriate for the majority of users.

You can also scan for available 3G service providers in your area by selecting “Manual” for the “Current Operator Selection Mode” and then clicking the scan button.



Operator Settings

Current Operator Selection Mode: Automatic   Select Operator Mode ● Automatic ○ Manual

Current Operator Registration: Telstra Mobile Operator Name List:	MCC	MNC	Operator Status	Network Type

Scan Apply

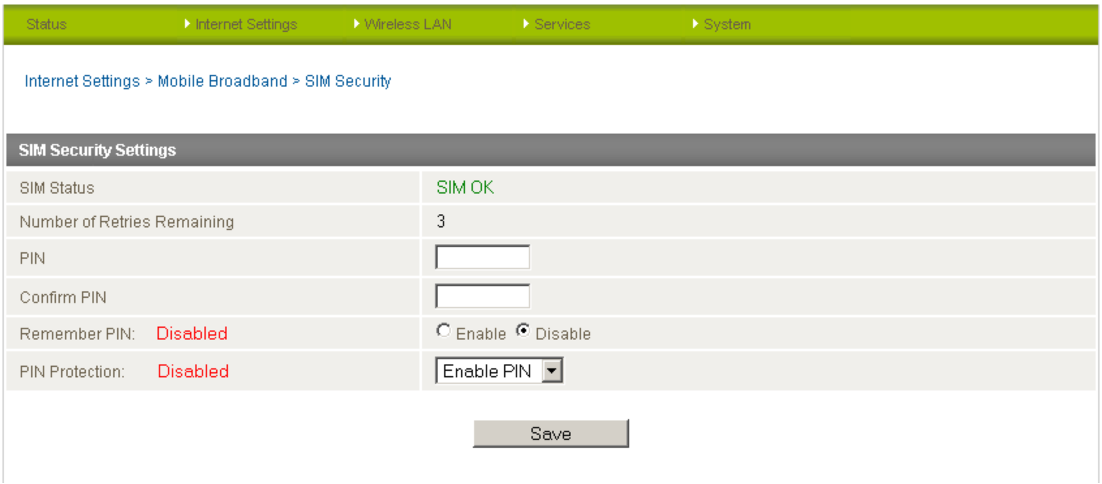
Figure 15 - Manual Operator Selection

A list of the detected 3G service carriers in your area will be displayed. Select the most appropriate 3G service from the list shown and click “Apply”.

The default setting of “Automatic” should be appropriate for the majority of users and locations.

SIM Security

The SIM Security page can be used for authenticating SIM cards that have been configured with a security PIN code. The security PIN code protection can also be enabled or disabled on this page.

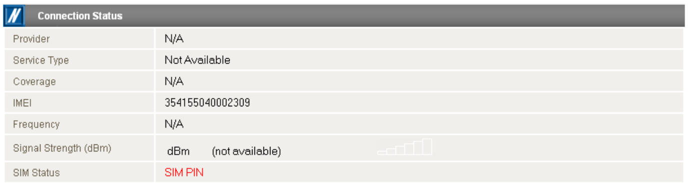


Internet Settings > Mobile Broadband > SIM Security

SIM Security Settings	
SIM Status	SIM OK
Number of Retries Remaining	3
PIN	
Confirm PIN	
Remember PIN: Disabled	○ Enable ● Disable
PIN Protection: Disabled	Enable PIN

Figure 16 - Internet Settings - Mobile Broadband - SIM Security

If the SIM card is locked you will need to unlock it with a PIN provided with your SIM card. You can find out if the SIM is locked by viewing the SIM Status on the Status page:

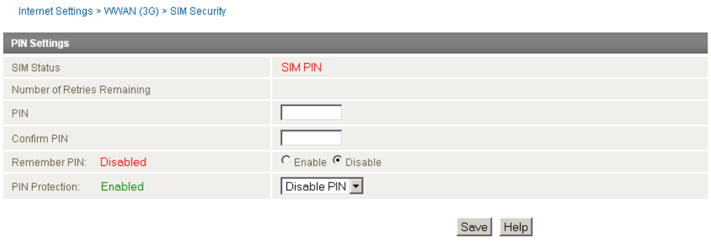


Connection Status	
Provider	N/A
Service Type	Not Available
Coverage	N/A
IMEI	354155040002309
Frequency	N/A
Signal Strength (dBm)	dBm (not available)
SIM Status	SIM PIN

Figure 17 - SIM Security - Status Page Warning

If the SIM Status is "**SIM PIN**" as above then do the following:

a) Click on the "Internet Settings" menu at the top of the page and then the "SIM Security" item from the WWAN (3G) menu item on the right.



Internet Settings > WWAN (3G) > SIM Security

PIN Settings	
SIM Status	SIM PIN
Number of Retries Remaining	
PIN	
Confirm PIN	
Remember PIN: Disabled	○ Enable ● Disable
PIN Protection: Enabled	Disable PIN

Figure 18 - SIM Security - SIM PIN Needed

b) Enter the PIN code in the "**PIN**" field and then enter it again in the "**Confirm PIN**" field to confirm the PIN code.

Please note: You can also select to "**Remember PIN**" so that entering the PIN code each time the SIM is inserted is not required. Alternatively you can also disable SIM PIN protection by selecting to "**Disable PIN**" from the "PIN Protection" drop down menu.

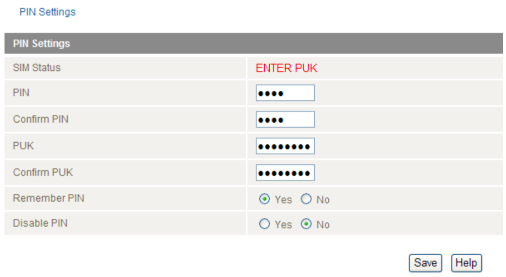
c) Click Save.

Enter PUK

After three incorrect attempts at entering the PIN code, you are requested to enter a PUK code.

Please note: You will need to contact your 3G provider to obtain this number.

Your carrier will issue you a PUK code to enable you to unlock the SIM and enter a new PIN code. Enter the new PIN and PUK codes and click Save.



PIN Settings

PIN Settings	
SIM Status	ENTER PUK
PIN	••••
Confirm PIN	••••
PUK	••••••••
Confirm PUK	••••••••
Remember PIN	● Yes ○ No
Disable PIN	○ Yes ● No

Figure 19 - SIM Security - SIM PUK Needed

Remember PIN

This feature allows the router to automatically send the PIN to the SIM each time the SIM asks for it (usually at power up).

This enables the SIM to be PIN Locked (to prevent unauthorised re-use of the SIM elsewhere), while still allowing the router to connect to the cellular service.

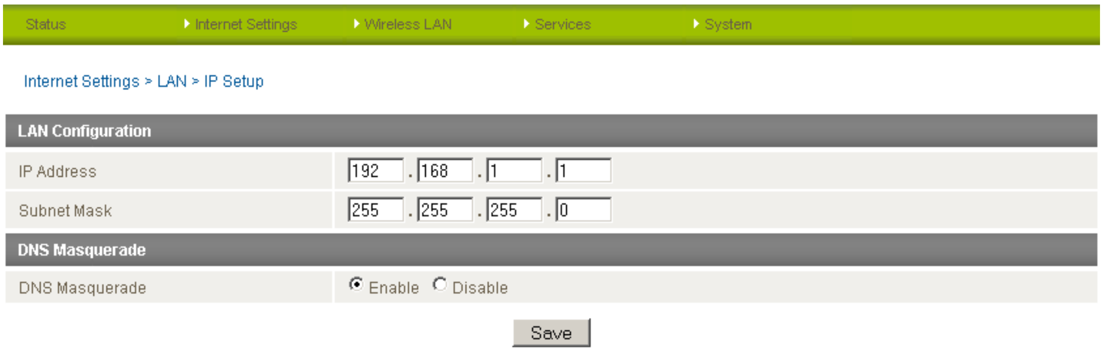
When this feature is enabled the PIN entered by the user when they set the “Remember PIN” feature is encrypted and stored locally in the router. The next time the SIM asks the router for the PIN the router decrypts the PIN and automatically sends it to the SIM without user intervention.

When this feature is disabled and the SIM is PIN locked, the PIN must be manually entered via the router's configuration interface. This is clearly not desirable where the router is unattended.

LAN

IP Setup

The IP Setup page is used to configure the LAN Settings of the router and to enable or disable DNS Masquerade.



LAN Configuration	
IP Address	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 255 . 0
DNS Masquerade	
DNS Masquerade	● Enable ○ Disable

Figure 20 - IP Setup Settings

The default IP of the Ethernet port is 192.168.1.1 with subnet mask 255.255.255.0. To change this, enter the new IP Address and/or Subnet mask and click “Save”.

Please note: If the IP address has changed you will have to re-enter the new IP address configured in your browser to access the configuration pages.

DNS Masquerading

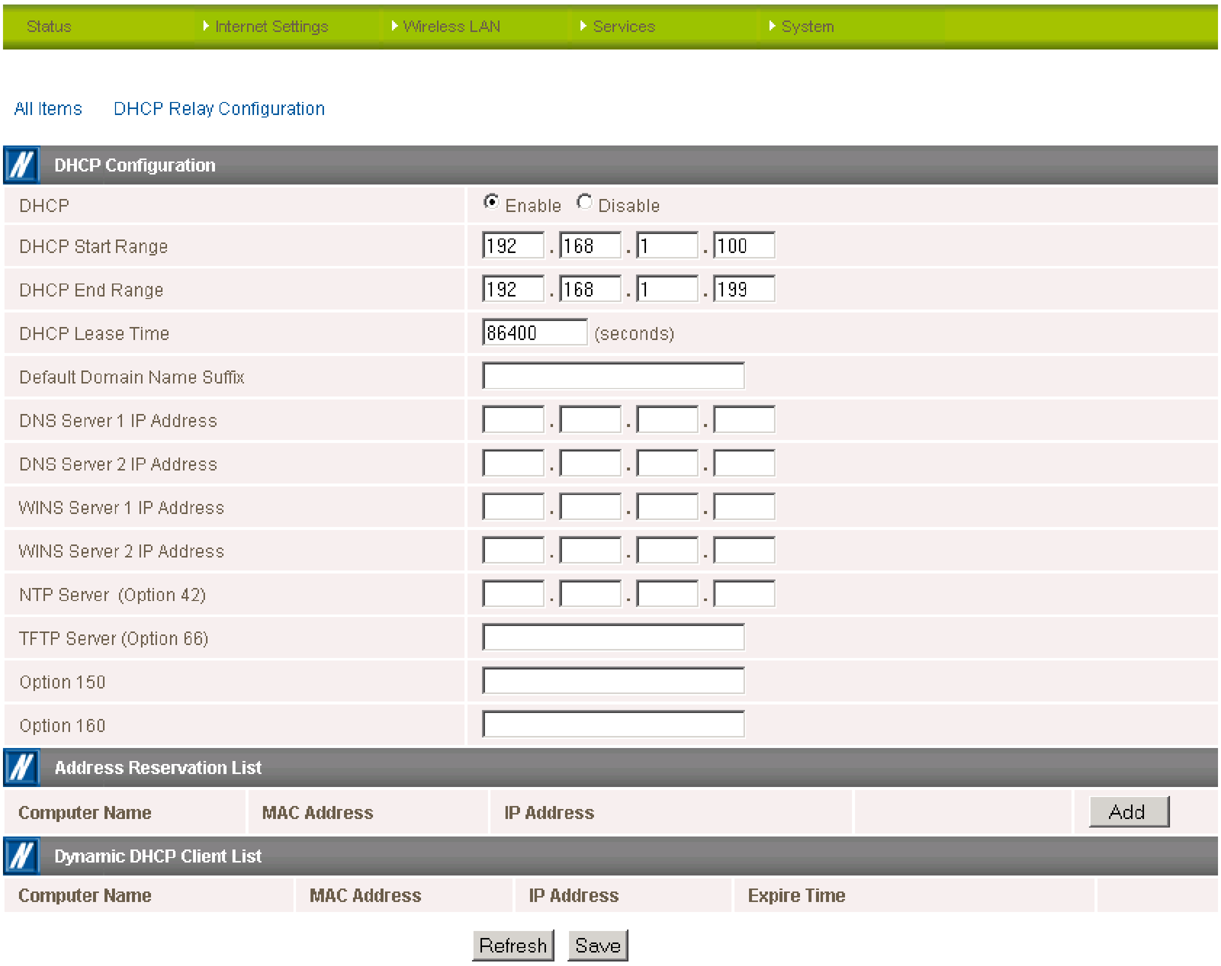
DNS masquerading allows the router to forward DNS requests to dynamically assigned DNS servers. Clients on the router's LAN can then use the router as a DNS server without needing to know of the dynamically assigned DNS servers assigned by the cellular network.

There should be no need to disable this feature in most cases, however, if you need to do so simply select “Disable” and click the Save button.

DHCP

The DHCP page is used to adjust the DHCP settings used by the router. The DHCP settings are then passed onto any device connecting via DHCP.

You can manually set the DHCP Start and End range, the DHCP Lease time, the default Domain name suffix, Primary and Secondary DNS Server, the Primary and Secondary WINS Server, as well as the NTP, TFTP and Option 150/Option 160 (VoIP options) settings.



DHCP Configuration	
DHCP	● Enable ○ Disable
DHCP Start Range	192 . 168 . 1 . 100
DHCP End Range	192 . 168 . 1 . 199
DHCP Lease Time	86400 (seconds)
Default Domain Name Suffix	
DNS Server 1 IP Address	. . .
DNS Server 2 IP Address	. . .
WINS Server 1 IP Address	. . .
WINS Server 2 IP Address	. . .
NTP Server (Option 42)	. . .
TFTP Server (Option 66)	
Option 150	
Option 160	

Address Reservation List

Computer Name	MAC Address	IP Address		Add

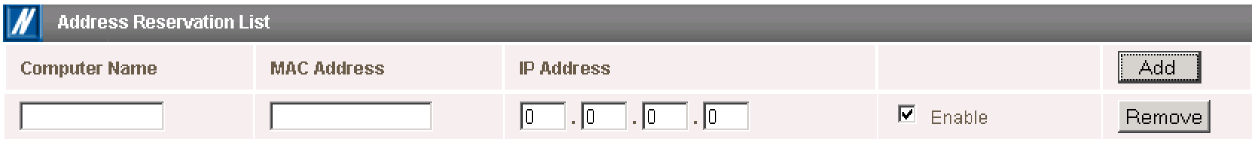
Dynamic DHCP Client List

Computer Name	MAC Address	IP Address	Expire Time	

Figure 21 - DHCP Settings

After entering the applicable details, click "Save".

You can also assign a particular IP address to a specific device every time that device makes a DHCP request as follows:



Address Reservation List

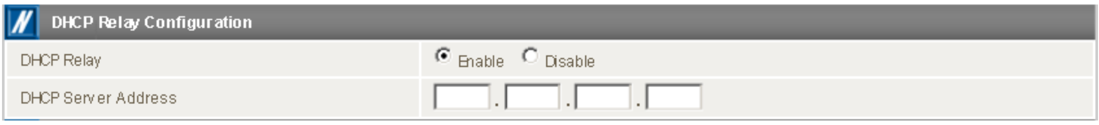
Computer Name	MAC Address	IP Address		Add
		0 . 0 . 0 . 0	☑ Enable	Remove

Figure 22 - DHCP Settings - Fixed Mapping

1. Click the "Add" button.
2. Enter a name for the computer or device.
3. Enter the computer or device's MAC address.
4. Enter the IP address to assign to the device.
5. Click the "Save" button.

DHCP Relay Configuration

To relay the DHCP function from a remote DHCP server select the “DHCP Relay Configuration” link at the top of the page.



DHCP Relay Configuration

DHCP Relay	● Enable ○ Disable
DHCP Server Address	___ . ___ . ___ . ___

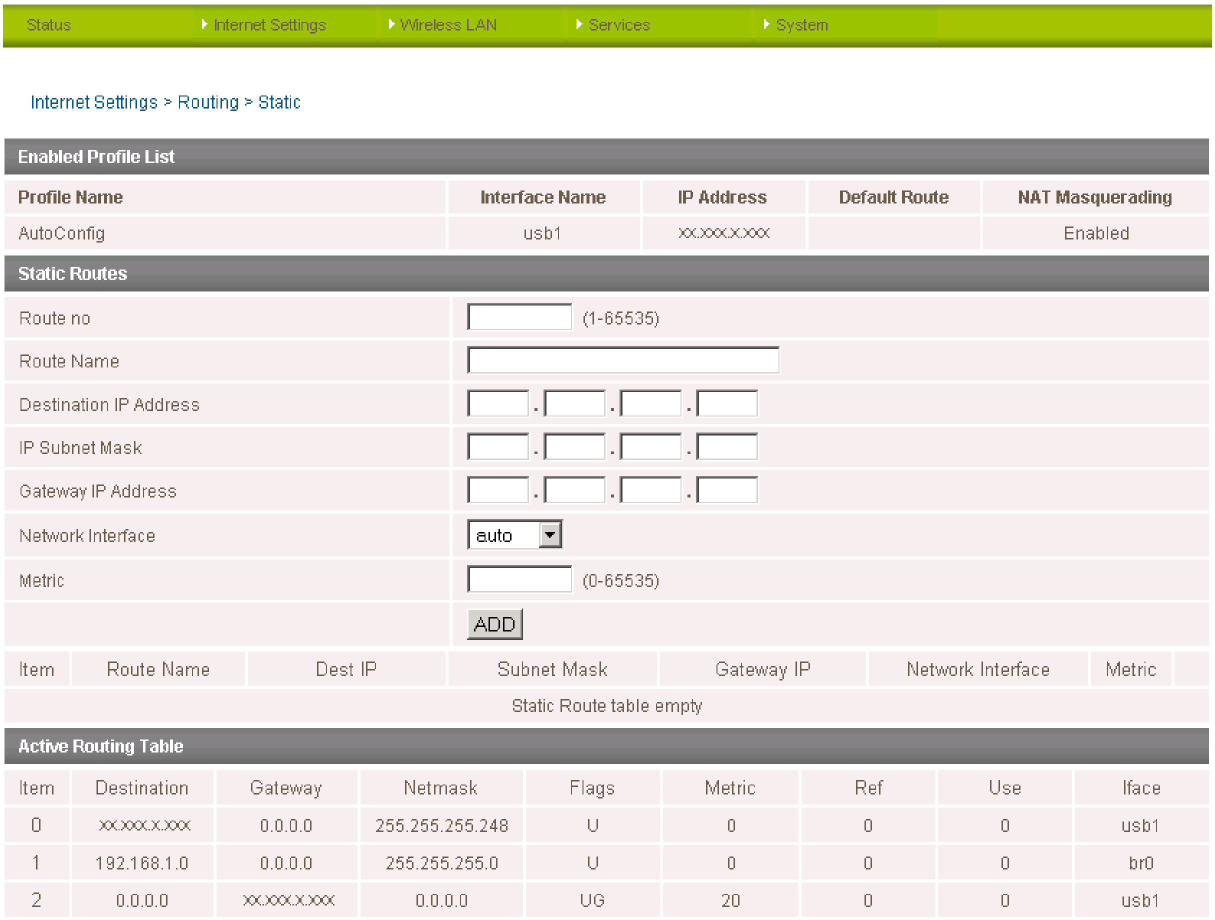
Figure 23: Internet Settings - LAN - DHCP - DHCP Relay Configuration

1. Set the “DHCP Relay” option to Enable.
2. Enter the IP Address of the DHCP Server you wish to relay to.

Routing

Static

The Static Route page is used to add or delete static routes. Static routes can be used to facilitate communication between devices on different networks.



Internet Settings > Routing > Static

Enabled Profile List

Profile Name	Interface Name	IP Address	Default Route	NAT Masquerading
AutoConfig	usb1	xx.xxx.x.xxx		Enabled

Static Routes

Route no	(1-65535)
Route Name	
Destination IP Address	. . .
IP Subnet Mask	. . .
Gateway IP Address	. . .
Network Interface	auto
Metric	(0-65535)
	ADD

Item	Route Name	Dest IP	Subnet Mask	Gateway IP	Network Interface	Metric	
Static Route table empty							

Active Routing Table

Item	Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Iface
0	xx.xxx.x.xxx	0.0.0.0	255.255.255.248	U	0	0	0	usb1
1	192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
2	0.0.0.0	xx.xxx.x.xxx	0.0.0.0	UG	20	0	0	usb1

Figure 24 - Static Route Settings

Some routes are added by default by the router on initialisation such as the Ethernet subnet route for routing to a device on the Ethernet subnet. A PPP route is also added upon obtaining a WAN PPP connection.

Adding Static Routes

- Enter the required values in the fields (as shown above) for route being added.
- Click the “ADD” button.

Please note: You must increment the “Route no” by 1 for each route in the “Route no” field otherwise that route will be overwritten.

The Active Routing table at the bottom will then show the new route added.

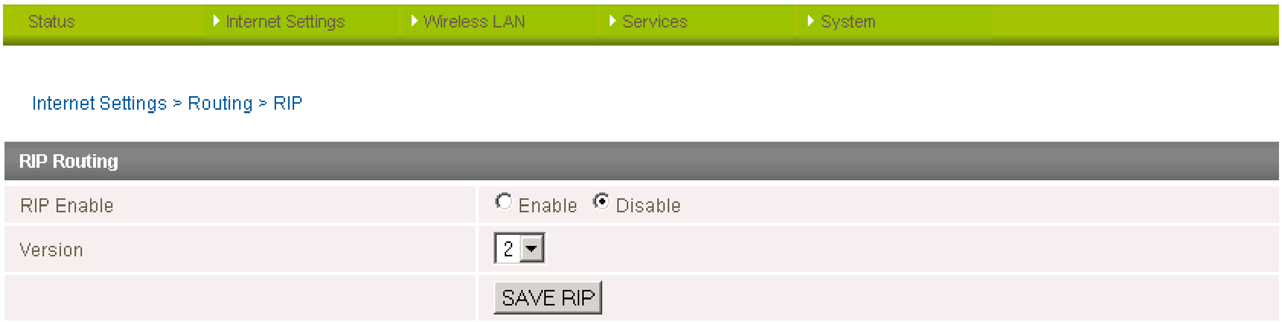
Deleting Static Routes

Click the “Delete Entry” text (in blue).

RIP

RIP (Routing Information Protocol) is used for advertising routes to other routers. Thus all the routes in the router's routing table will be advertised to other nearby routers. For example, the route for the router's Ethernet subnet could be advertised to a Router on the PPP interface side so that a Router on this network will know how to route to a device on the router's Ethernet subnet. You will have to add the routes appropriately in the Static Routes section – see Adding Static Routes.

Please note: Some routers will ignore RIP.



RIP Routing

RIP Enable	○ Enable ● Disable
Version	2
	SAVE RIP

Figure 25 - RIP Settings

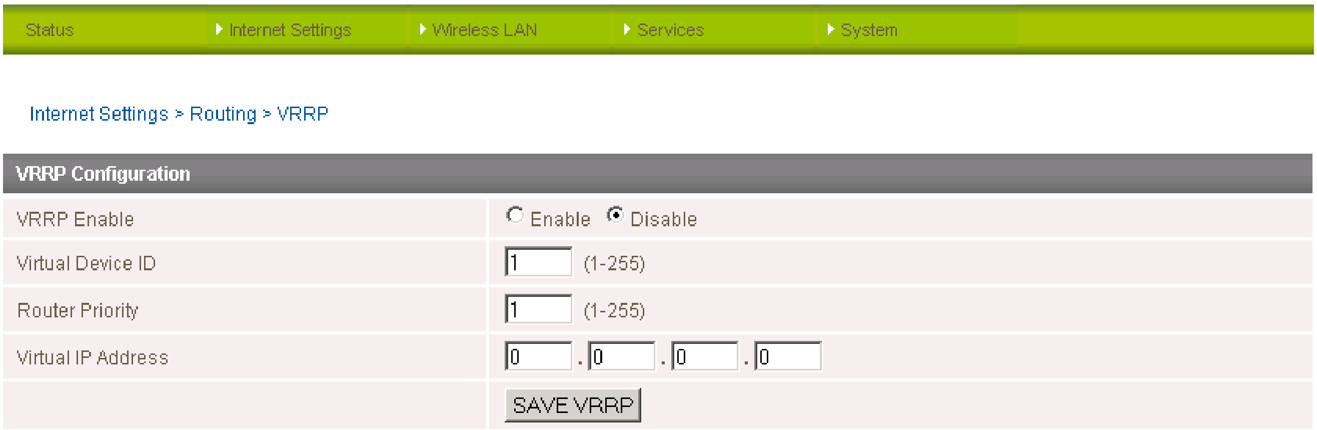
- Click Enable for the “RIP Enable” option.
- Select the RIP version.
- Click the “Save RIP” button.

VRRP

Virtual Router Redundancy Protocol (VRRP) is a non-proprietary redundancy protocol designed to increase the availability of the default gateway servicing hosts on the same subnet. This increased reliability is achieved by advertising a “virtual router” (an abstract representation of master and backup routers acting as a group) as a default gateway to the host(s) instead of one physical router. Two or more physical routers are then configured to stand for the virtual router, with only one doing the actual routing at any given time. If the current physical router that is routing the data on behalf of the virtual router fails, an arrangement is made for another physical router to automatically replace it. The physical router that is currently forwarding data on behalf of the virtual router is called the master router.

Master routers have a priority of 255 and backup router(s) can have priority between 1 and 254.

A virtual router must use 00-00-5E-00-01-XX as its (MAC) address. The last byte of the address (XX) is the Virtual Router Identifier (VRID), which is different for each virtual router in the network. This address is used by only one physical router at a time, and is the only way that other physical routers can identify the master router within a virtual router.



Internet Settings > Routing > VRRP

VRRP Configuration	
VRRP Enable	○ Enable ● Disable
Virtual Device ID	1 (1-255)
Router Priority	1 (1-255)
Virtual IP Address	0 . 0 . 0 . 0

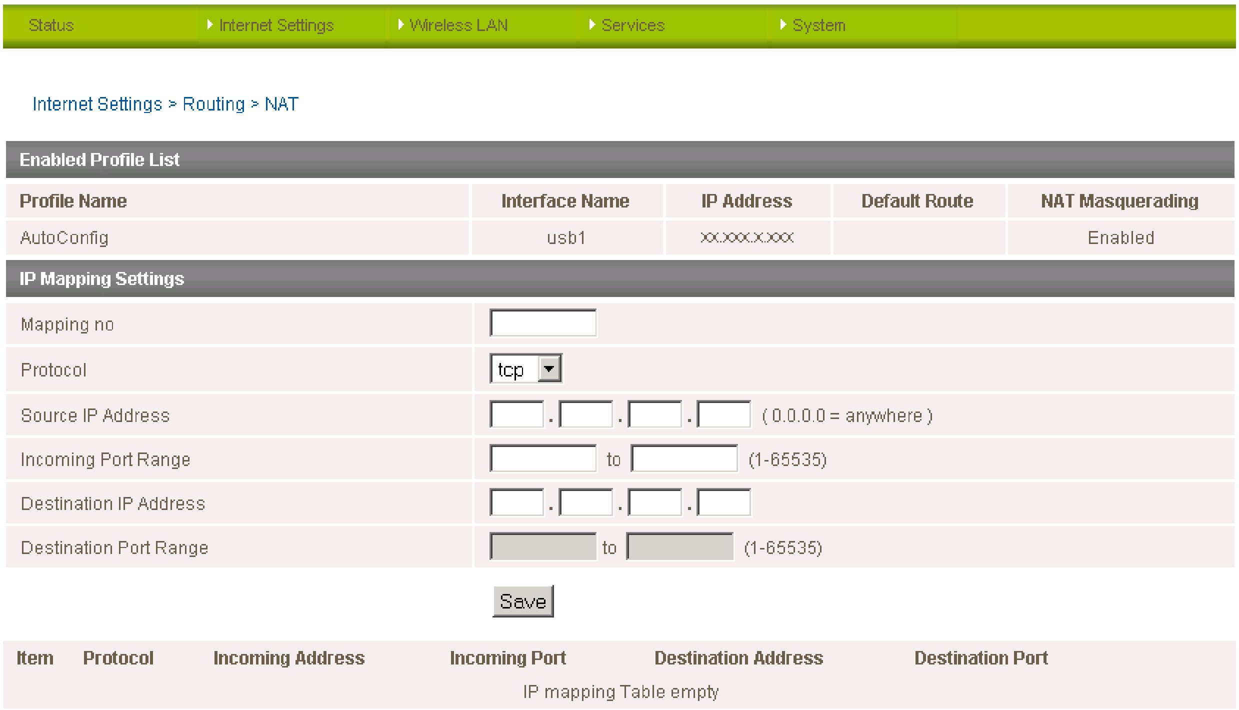
Figure 26 - VRRP Settings

1. Click Enable for the “VRRP Enable” option to activate VRRP.
2. Enter an ID – this is the VRRP ID which is different for each virtual router on the network.
3. Enter a priority – a higher value is a higher priority.
4. Enter the VRRP IP address – this is the virtual IP address that both virtual routers share.
5. Click the “Save VRRP” button.

Please note: Configuring VRRP changes the MAC address of the Ethernet port and therefore if you want to resume with the web configuration you must use the new IP address (VRRP IP) or on a command prompt type: arp –d <ip address> (i.e. arp –d 192.168.1.1) to clear the arp cache.(old MAC address).

NAT

The NAT page is used to configure the Network Address Translation rules currently in use on the router. The router is in NAT mode by default.



Internet Settings > Routing > NAT

Enabled Profile List

Profile Name	Interface Name	IP Address	Default Route	NAT Masquerading
AutoConfig	usb1	xx.xxx.x.xxx		Enabled

IP Mapping Settings

Mapping no	
Protocol	tcp
Source IP Address	. . . (0.0.0.0 = anywhere)
Incoming Port Range	to (1-65535)
Destination IP Address	. . .
Destination Port Range	to (1-65535)

Item	Protocol	Incoming Address	Incoming Port	Destination Address	Destination Port

IP mapping Table empty

Figure 27 - NAT Settings

This is only needed if you need to map inbound requests to a specific port on the WAN IP address to a device connected on the Ethernet interface, e.g. a web camera.

How to configure Port Forwarding

OPTION	DEFINITION
Mapping no	Enter a number to uniquely identify the port mapping rule. 1 to as many as needed.
Protocol	Specify the protocol to use for the port mapping rule. Options are TCP, UDP or All protocols.
Source IP Address	Specifies either a "Friendly" IP address that is allowed to access the router or a wildcard IP address of 0.0.0.0 that allows all IP addresses to access the router.
Incoming Port Range	Specify the external port(s) to listen to.
Destination IP Address	Local Area Network IP Address of device to forward inbound requests to.
Destination Port Range	Local Area Network Port(s) to forward connections to.

Table 17 - NAT Configuration Items

1. Enter the IP Mapping configuration information as appropriate.
2. Click the "Save" button.

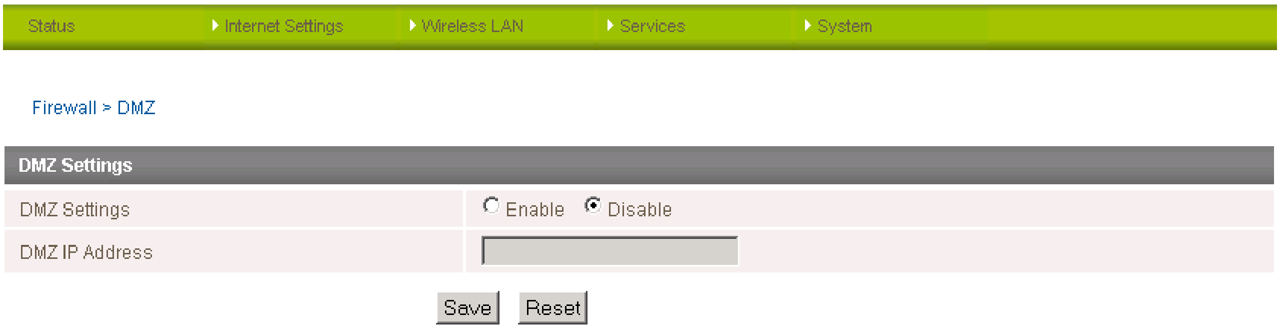
Please note: If the "Incoming Port Range" specifies a single port (as above) then the destination port can be set to any port. If the "Incoming Port Range" specifies a range of port numbers then the "Destination Port Range" MUST be the same as the "Incoming Port Range".

To delete a port forwarding rule, click on the corresponding "Delete Entry" link from the list of IP Mappings.

DMZ

The Demilitarised Zone (DMZ) enables a device to utilise a direct connection to the WAN. This means any incoming connections are forwarded directly to this device.

The DMZ page is used to specify the IP Address of the device to this feature.



DMZ Settings

DMZ Settings	○ Enable ● Disable
DMZ IP Address	

Figure 28 - DMZ Settings

1. Select Enable for the “DMZ Settings” option to enable the DMZ host function.
2. Enter the IP Address of the device to be the DMZ host into the “DMZ IP Address” field.
3. Click the “Save” button.

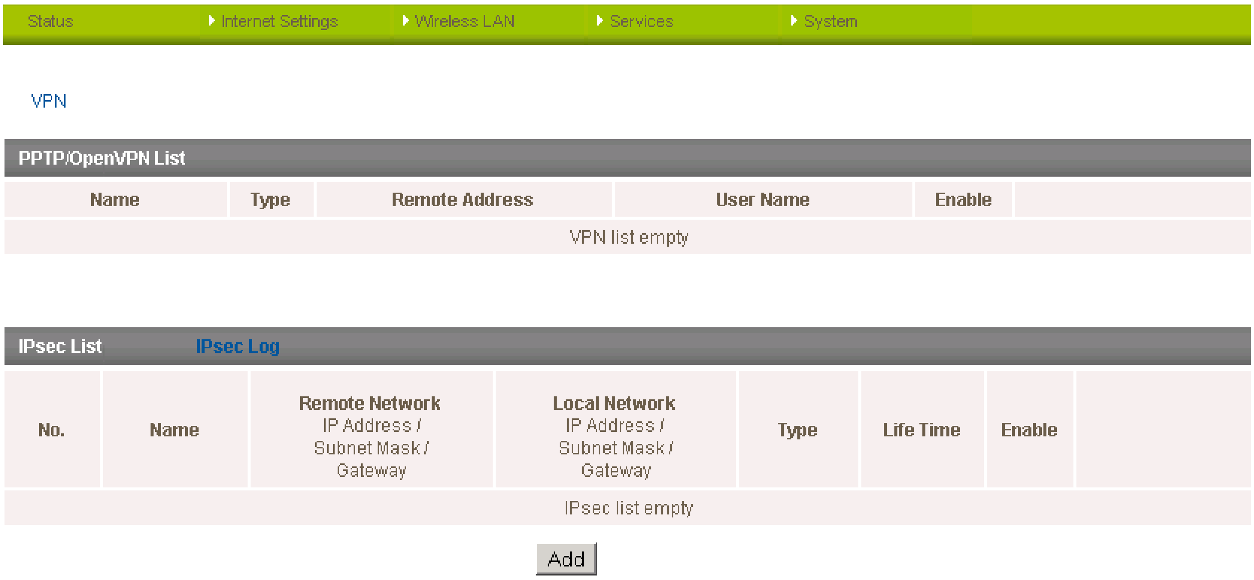
VPN

A Virtual Private Network (VPN) is a tunnel providing a private link between two networks or devices over a public network. Data to be sent via a VPN needs to be encapsulated and as such is generally not visible to public network.

The advantages of a VPN connection include:

- Data Protection
- Access Control
- Data Origin Authentication
- Data Integrity

How to configure a VPN connection



VPN

PPTP/OpenVPN List

Name	Type	Remote Address	User Name	Enable	
VPN list empty					

No.	Name	Remote Network IP Address / Subnet Mask / Gateway	Local Network IP Address / Subnet Mask / Gateway	Type	Life Time	Enable	
IPsec list empty							

Figure 29 - VPN Connection Details

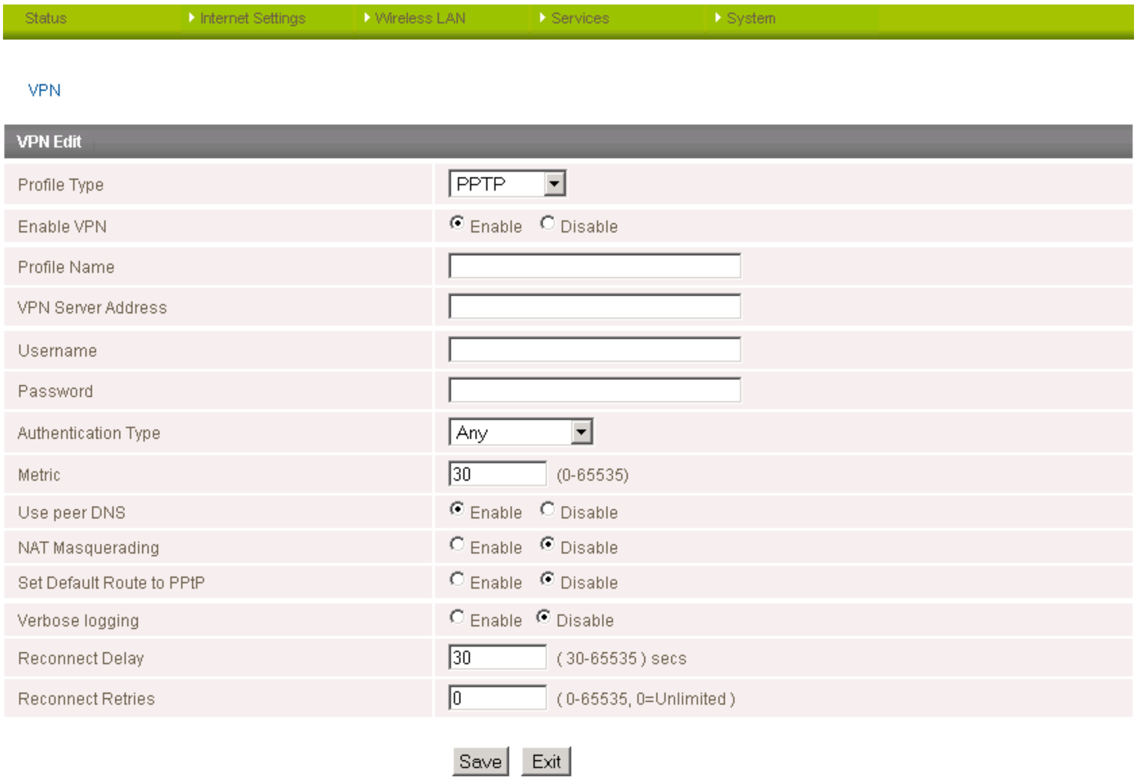
1. Click “Add” and select the type of VPN connection you would like to configure. You can select from the following types of VPN connection:

- PPTP
- GRE
- OpenVPN
- IPSec

Each VPN connection has different configuration requirements. For more information on the VPN functionality available, please refer to the VPN document available from the NetComm Website.

The following pages detail the configuration options available for the different VPN connection types.

PPTP



Profile Type	PPTP
Enable VPN	● Enable ○ Disable
Profile Name	
VPN Server Address	
Username	
Password	
Authentication Type	Any
Metric	30 (0-65535)
Use peer DNS	● Enable ○ Disable
NAT Masquerading	○ Enable ● Disable
Set Default Route to PPtP	○ Enable ● Disable
Verbose logging	○ Enable ● Disable
Reconnect Delay	30 (30-65535) secs
Reconnect Retries	0 (0-65535, 0=Unlimited)

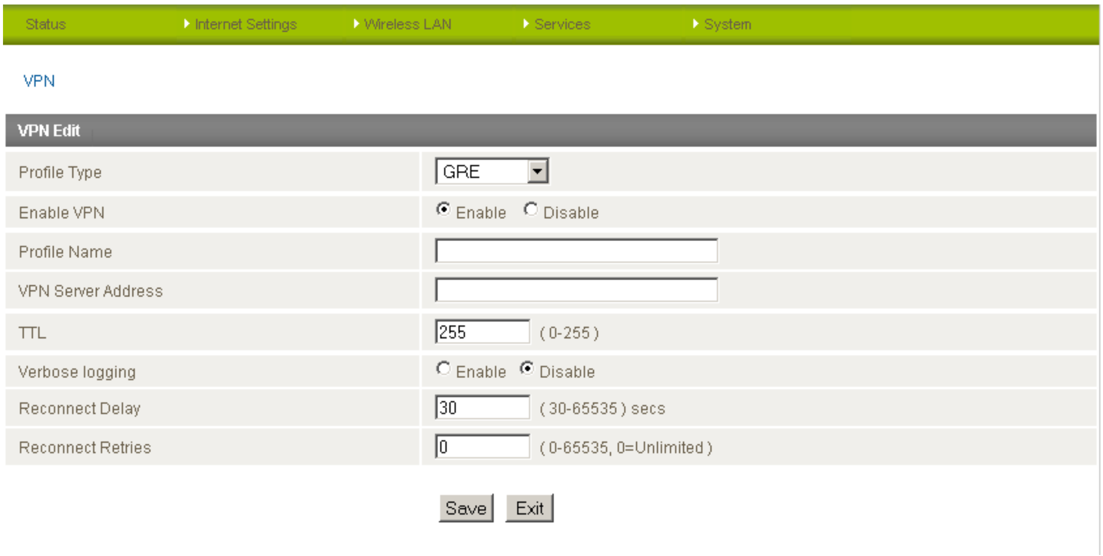
Figure 30 - VPN Connection Settings - PPTP

ITEM	DEFINITION
Profile Type	Select the type of VPN connection to use.
Enable VPN	Enable or Disable the VPN connection.
Profile Name	A name used to identify the VPN connection.
VPN Server Address	The IP Address on which the VPN server is running.
Username	The username required to login to the VPN service.
Password	The password required to login to the VPN service.
Authentication Type	The authentication type required for connecting to the VPN service.
Metric	The route metric to apply to the VPN connection.
Use peer DNS	Select whether to use the VPN server DNS settings or not.
NAT Masquerading	Select whether to use NAT Masquerading for the VPN connection.
Set Default Route to PPtP	Make the VPN connection the default route for traffic to use.
Verbose Logging	Enable extended logging information for the VPN connection.
Reconnect Delay	The delay before attempting to reconnect to the VPN service.
Reconnect Retries	The number of times to attempt to reconnect to the VPN service.

Table 18 - PPTP Configuration Items

GRE

The Generic Route Encapsulation (GRE) protocol is used in addition to Point-to-Point Tunnelling Protocol (PPTP) to create VPNs (virtual private networks) between clients and servers or between clients only. Once a PPTP control session establishes the VPN tunnel GRE is used to securely encapsulate the data or payload.



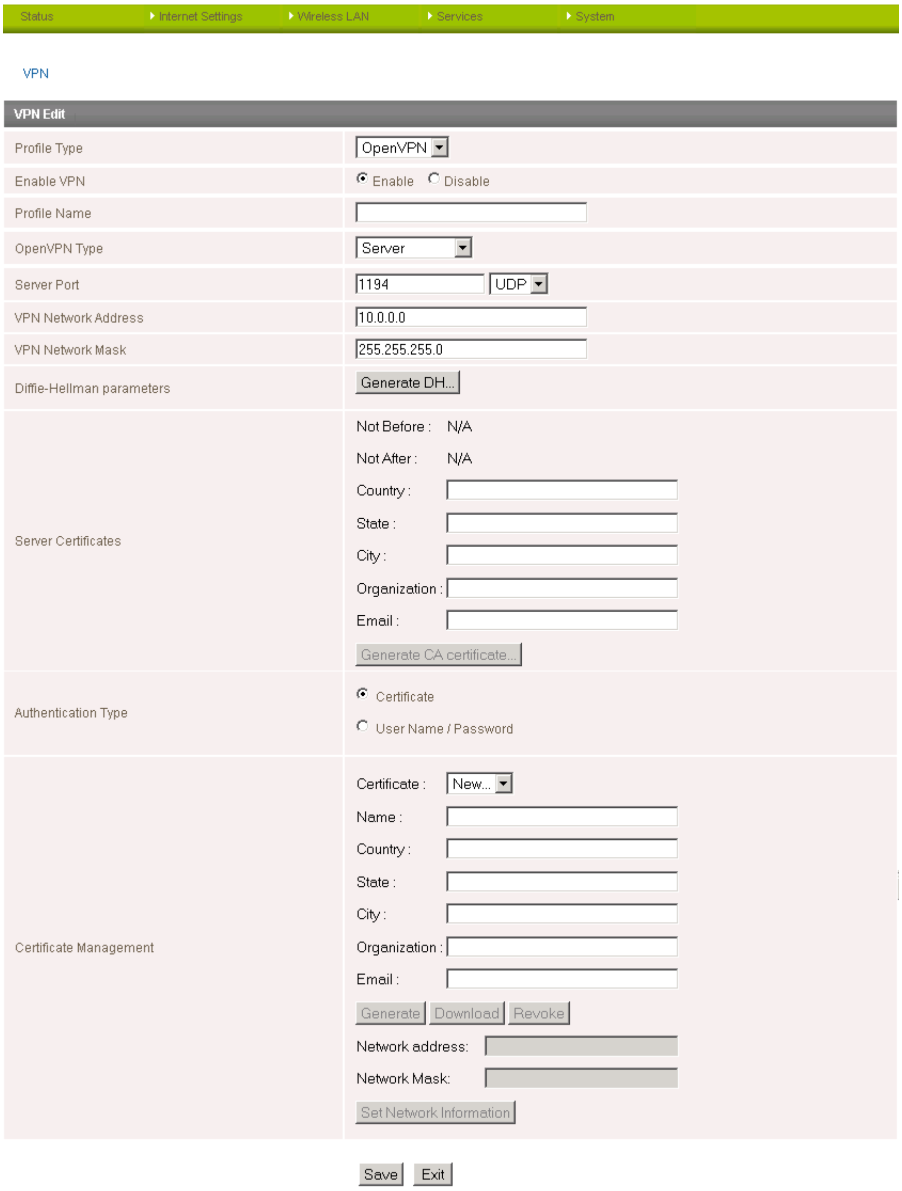
VPN Edit

Profile Type	GRE
Enable VPN	● Enable ○ Disable
Profile Name	
VPN Server Address	
TTL	255 (0-255)
Verbose logging	○ Enable ● Disable
Reconnect Delay	30 (30-65535) secs
Reconnect Retries	0 (0-65535, 0=Unlimited)

ITEM	DEFINITION
Profile Type	Select the type of VPN connection to use.
Enable VPN	Enable or Disable the VPN connection.
Profile Name	A name used to identify the VPN connection.
VPN Server Address	The IP Address on which the VPN server is running.
TTL	The Time To Live field, an 8-bit field used to remove an undeliverable data packet from a network to avoid unnecessary network traffic across the internet. The default value of 255 is the upper limit on the time that an IP datagram can exist. The value is reduced by at least one for each hop the data packet takes to the next router on the route to the datagram's destination. If the TTL field reaches zero before the datagram arrives at its destination the data packet is discarded and an error message is sent back to the sender.
Verbose Logging	Enable extended logging information for the VPN connection.
Reconnect Delay	The delay before attempting to reconnect to the VPN service.
Reconnect Retries	The number of times to attempt to reconnect to the VPN service.

Table 19: VPN - GRE Settings

OpenVPN



VPN

VPN Edit

Profile Type	OpenVPN ▾
Enable VPN	● Enable ○ Disable
Profile Name	
OpenVPN Type	Server ▾
Server Port	1194 UDP ▾
VPN Network Address	10.0.0.0
VPN Network Mask	255.255.255.0
Diffie-Hellman parameters	Generate DH...
Server Certificates	Not Before : N/A Not After : N/A Country : State : City : Organization : Email : Generate CA certificate...
Authentication Type	● Certificate ○ User Name / Password
Certificate Management	Certificate : New... ▾ Name : Country : State : City : Organization : Email : Generate Download Revoke Network address: Network Mask: Set Network Information

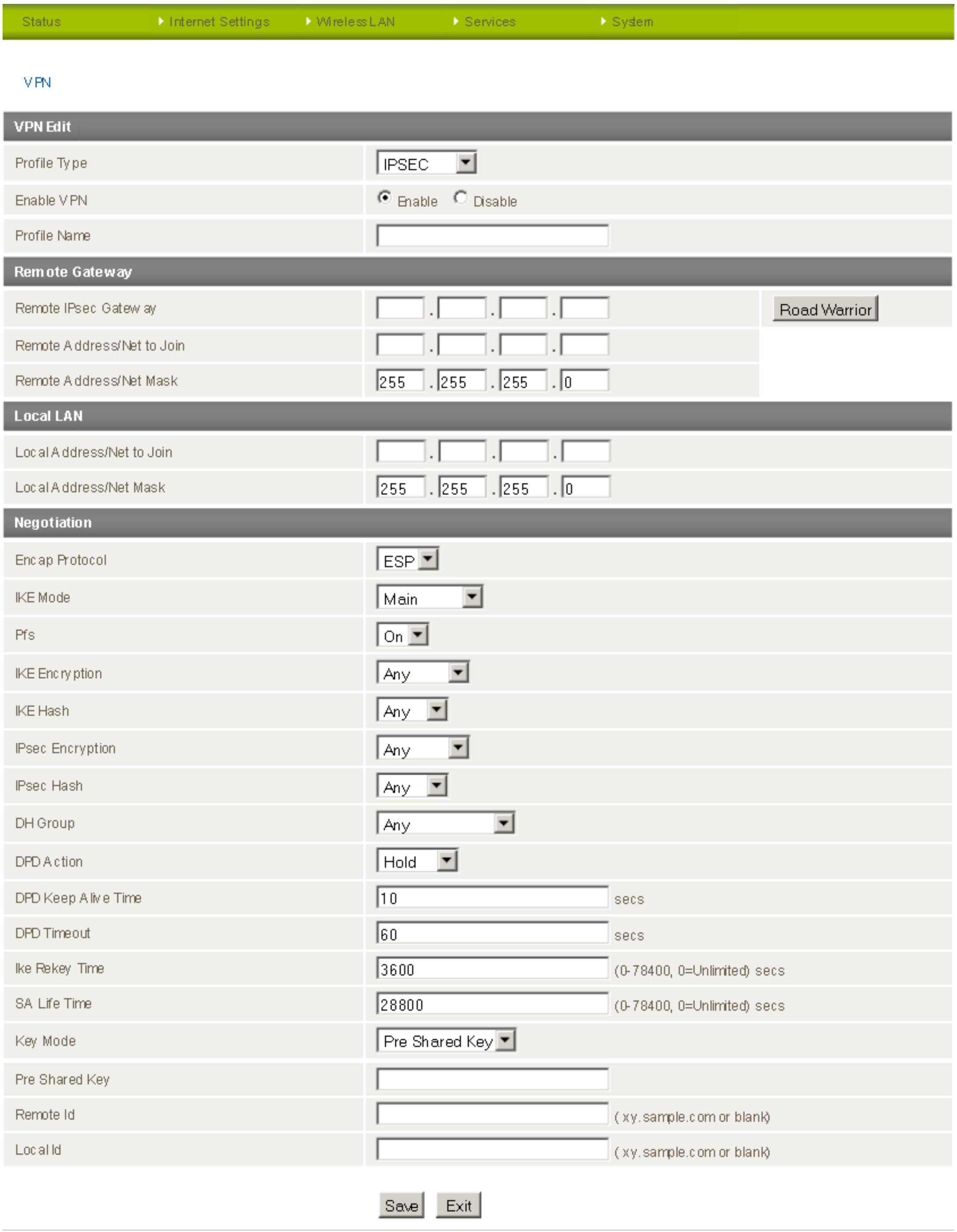
Save Exit

Figure 31 - VPN Connection Settings - OpenVPN

ITEM	DEFINITION
Profile Type	Select the type of VPN connection to use.
Enable VPN	Enable or Disable the VPN connection.
Profile Name	A name used to identify the VPN connection.
OpenVPN Type	Select the type of OpenVPN session to use.
Server Port	Enter the port the OpenVPN server is running on.
VPN Network Address	Enter the network address for use on the VPN connection.
VPN Network Mask	Enter the network mask for use on the VPN connection.
Diffie-Hellman parameters	Generate the server and client keys used by the VPN connection.
Server Certificates	Enter the applicable details to identify the OpenVPN server and create a CA certificate based on this information.
Authentication Type	Select the type of authentication in use for the VPN connection. You can select from: - Certificate - User Name / Password Each type of Key mode requires different configuration options. For more information, please refer to the VPN Document available from the NetComm Website.

Table 20 - OpenVPN Configuration Items

IPSEC



VPN Edit	
Profile Type	IPSEC
Enable VPN	● Enable ○ Disable
Profile Name	
Remote Gateway	
Remote IPsec Gateway	. . . (Road Warrior)
Remote Address/Net to Join	. . .
Remote Address/Net Mask	255 . 255 . 255 . 0
Local LAN	
Local Address/Net to Join	. . .
Local Address/Net Mask	255 . 255 . 255 . 0
Negotiation	
Encap Protocol	ESP
IKE Mode	Main
Pfs	On
IKE Encryption	Any
IKE Hash	Any
IPsec Encryption	Any
IPsec Hash	Any
DH Group	Any
DPD Action	Hold
DPD Keep Alive Time	10 secs
DPD Timeout	60 secs
Ike Rekey Time	3600 (0-78400, 0=Unlimited) secs
SA Life Time	28800 (0-78400, 0=Unlimited) secs
Key Mode	Pre Shared Key
Pre Shared Key	
Remote Id	(xy.sample.com or blank)
Local Id	(xy.sample.com or blank)

Figure 32 - VPN Connection Settings – IPSec

Please see Table 18 on the following page for details of the IPSec VPN Connection Settings page.

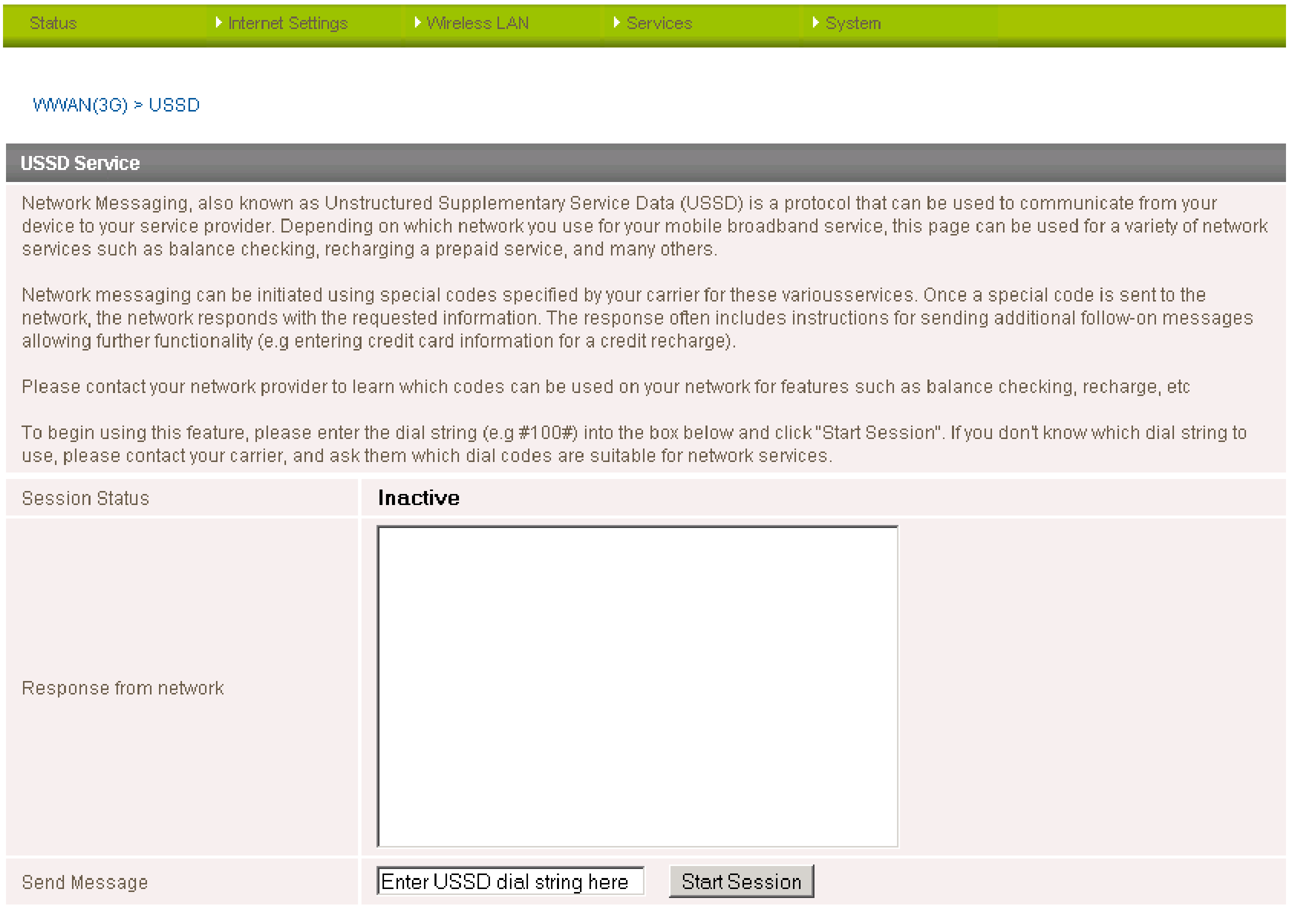
IPSec VPN Connection Settings – Item Details

ITEM	DEFINITION
Profile Type	Select the type of VPN connection to use.
Enable VPN	Enable or Disable the VPN connection.
Profile Name	A name used to identify the VPN connection.
Remote IPSec Gateway	The IP address that the IPSec server is running on.
Road Warrior	Click this to configure the VPN connection for Road Warrior (connection from a dynamic IP Address) use.
Remote Address/Net to Join	Enter the Remote IP address or Network for use on the VPN connection.
Remote Address/Net Mask	Enter the Netmask in use on the remote network.
Local Address/Net to Join	Enter the Local IP address or Network for use on the VPN connection.
Local Address/Net Mask	Enter the Netmask in use on the local network.
Encap Protocol	Select the encapsulation protocol to use with the VPN connection.
IKE Mode	Select the IKE mode to use with the VPN connection.
Pfs	Select whether or not to use PFS for the VPN connection.
IKE Encryption	Select the IKE encryption type to use with the VPN connection.
IKE Hash	Select the IKE Hash type to use for the VPN connection.
IPSec Encryption	Select the IPSec encryption type to use with the VPN connection.
IPSec Hash	Select the IPSec Hash type to use for the VPN connection.
DH Group	Select the appropriate DH Group for use with the VPN connection.
DPD Action	Select the appropriate DPD Action to use on the VPN connection.
DPD Keep Alive Time	Enter the time in seconds for DPD to keep alive.
DPD Timeout	Enter the time in seconds for DPD to timeout.
IKE Rekey Time	Enter the appropriate IKE Rekey time for the VPN connection.
SA Life Time	Enter the appropriate SA Life time for the VPN connection.
Key Mode	Select the type of key mode in use for the VPN connection. You can select from: - Pre Shared Key - RSA Keys - Certificates Each type of Key mode requires different configuration options. For more information, please refer to the VPN Document available from the NetComm Website.

Table 21 - IPSec Configuration Items

USSD

The USSD page is used to send USSD (short SMS style) messages to the 3G service provider.



USSD Service

Network Messaging, also known as Unstructured Supplementary Service Data (USSD) is a protocol that can be used to communicate from your device to your service provider. Depending on which network you use for your mobile broadband service, this page can be used for a variety of network services such as balance checking, recharging a prepaid service, and many others.

Network messaging can be initiated using special codes specified by your carrier for these variousservices. Once a special code is sent to the network, the network responds with the requested information. The response often includes instructions for sending additional follow-on messages allowing further functionality (e.g entering credit card information for a credit recharge).

Please contact your network provider to learn which codes can be used on your network for features such as balance checking, recharge, etc

To begin using this feature, please enter the dial string (e.g #100#) into the box below and click "Start Session". If you don't know which dial string to use, please contact your carrier, and ask them which dial codes are suitable for network services.

Session Status	**Inactive**
Response from network	
Send Message	Enter USSD dial string here [Start Session]

Figure 33 - USSD Messaging

USSD is a real-time messaging service usually utilised to perform mobile account related tasks such as the following:

- Checking available credit for a mobile service account.
- Obtaining more credit for a mobile service account.
- Verifying your mobile account information.

Enter the USSD message to be sent in the “Send Message” field at the bottom of the screen and then click “Start Session”.

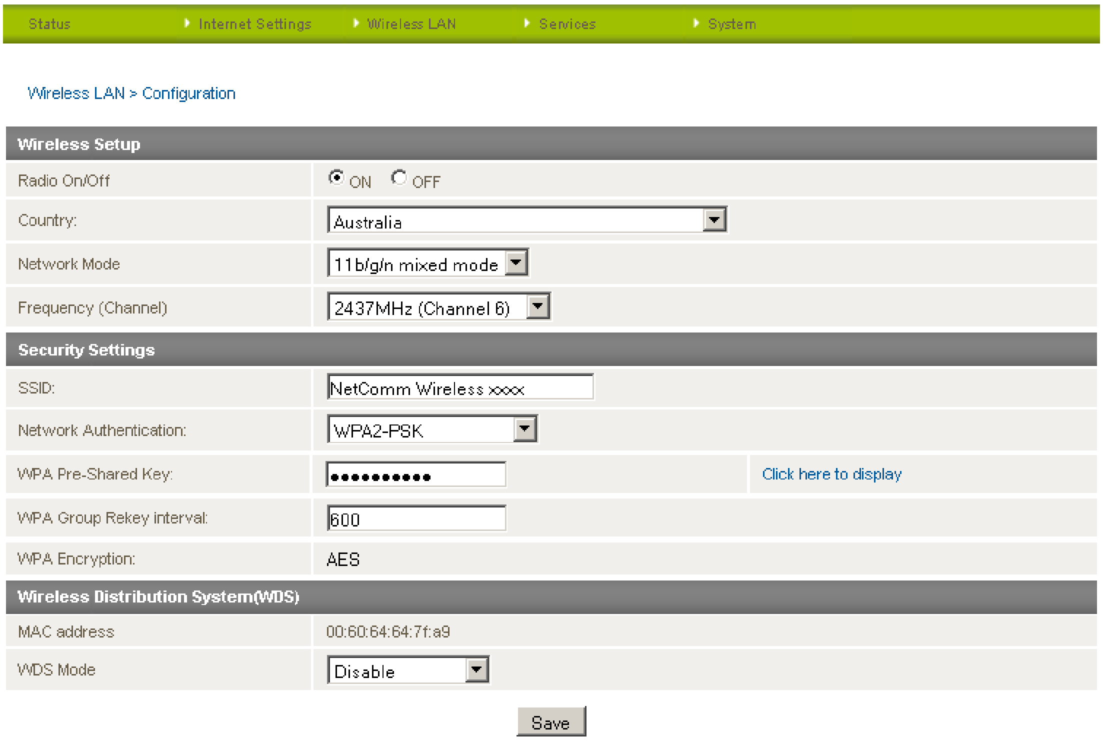
Any responses from your 3G Service Provider will be displayed in the “Response from Network” box in the middle of the page.

Please contact your 3G Service provider for a list of available USSD commands for your 3G service.

Wireless LAN

Configuration

The configuration page is used to define the basic wireless settings for the NTC-40WV such as the SSID and Wireless Security in use.



Wireless Setup

Radio On/Off: ● ON ○ OFF

Country: Australia

Network Mode: 11b/g/n mixed mode

Frequency (Channel): 2437MHz (Channel 6)

Security Settings

SSID: NetComm Wireless xxxx

Network Authentication: WPA2-PSK

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

WPA Group Rekey interval: 600

WPA Encryption: AES

Wireless Distribution System(WDS)

MAC address: 00:60:64:64:7f:a9

WDS Mode: Disable

Figure 34 - Wireless Configuration - Basic Settings

OPTION	DEFINITION
Radio On/Off	WiFi is turned on by default. Changing this option to OFF will turn OFF the wireless functionality on the NTC-40WV and you will not be able to connect wirelessly.
Country	Select the country you are operating the NTC-40WV in.
Network Mode	There are 6 possible network modes to use depending on the capability of your devices' wireless network cards. Each mode represents one or more wireless network protocols. Each wireless device will be capable of receiving some but possibly not all of wireless broadcast protocol types. They are: ● 802.11b/g/n mixed mode. ● 802.11b only. ● 802.11g only. ● 802.11n only. ● 802.11b/g/n mixed mode.
Frequency (Channel)	Select the wireless channel that the wireless signal will broadcast on.
SSID	The SSID (Service Set IDentifier or Network Name) in use for the wireless network.
Network Authentication	The wireless security settings. See below for in depth analysis.
WPA Pre-Shared Key	The wireless security key or wireless password.
WPA Group Rekey Interval	The time in seconds before a new key is generated.
WPA Encryption	The type of WPA encryption. Options include AES, TKIP or TKIP + AES.
MAC Address	The MAC address of the wireless network card.
WDS Mode	The Status of the WDS (Wireless Distribution System) Mode

Table 22 - Wireless Configuration - Basic Configuration Items

Click 'Apply' to save any changes to the settings.

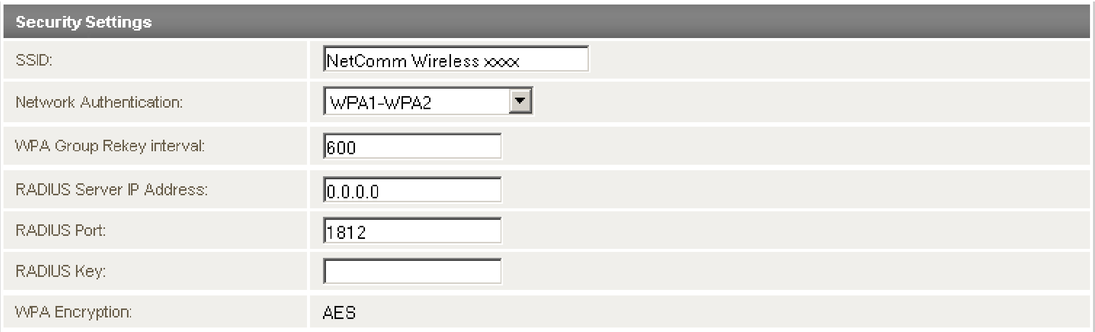
Wireless Security Settings

You may choose from the following wireless security options:

- Open
- Shared
- WPA
- WPA-PSK
- WPA2
- WPA2- PSK
- WPA-PSK-WPA2-PSK
- WPA1-WPA2
- 802.1x.

WPA1/WPA2

WPA (WiFi Protected Access) authentication is suitable for enterprise applications. It must be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. It provides a stronger encryption and authentication solution.



Security Settings

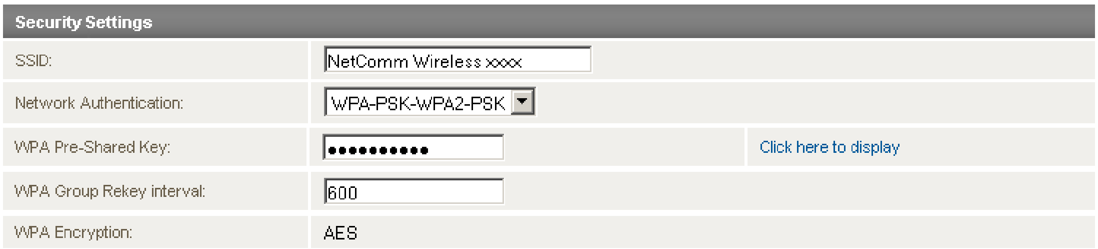
SSID:	NetComm Wireless xxxx
Network Authentication:	WPA1-WPA2
WPA Group Rekey interval:	600
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA Encryption:	AES

Figure 35 - Advanced View – WiFi Security Settings - WPA1/WPA2

WPA-PSK/WPA2-PSK

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

Please note that the configuration for WPA2, WPA-PSK-WPA2-PSK, WPA-PSK and WPA2-PSK is identical.



Security Settings

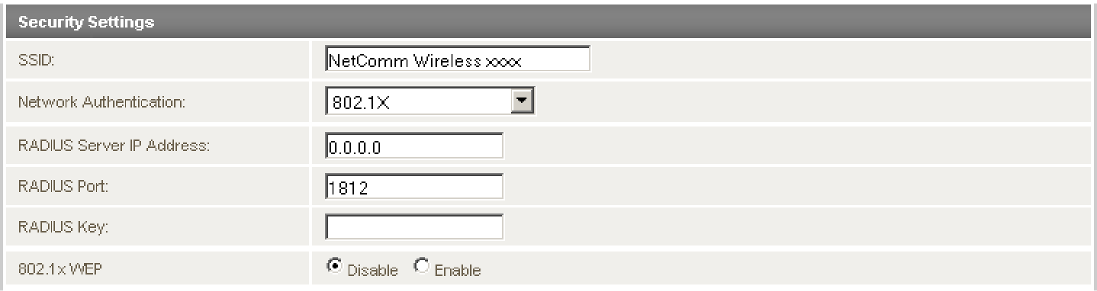
SSID:	NetComm Wireless xxxx	
Network Authentication:	WPA-PSK-WPA2-PSK	
WPA Pre-Shared Key:	●●●●●●●●●●●	Click here to display
WPA Group Rekey interval:	600	
WPA Encryption:	AES	

Figure 36 - Advanced View – WiFi Security Settings - WPA-PSK/WPA2-PSK

Please note: Your NTC-40WV uses WPA2-PSK by default. Check your Wireless Security Card or the device label on the bottom of the NTC-40WV for your default SSID and Security key to begin connecting your wireless devices.

802.1x

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



Security Settings

SSID:	NetComm Wireless xxxx
Network Authentication:	802.1X
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
802.1x WEP	● Disable ○ Enable

Figure 37 - Advanced View – WiFi *Security Settings - 802.1x*

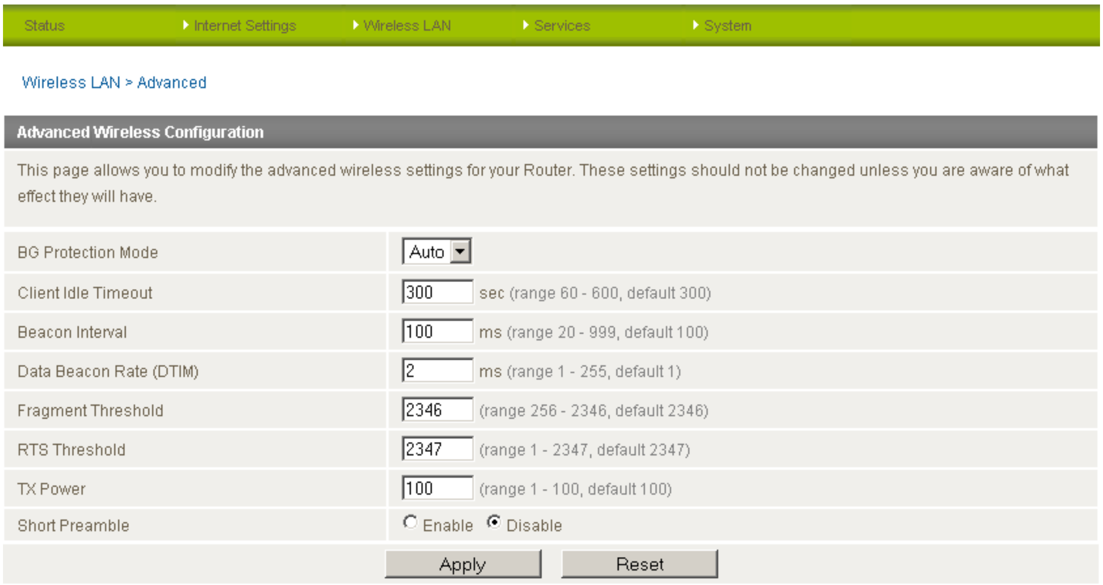
Please note: After configuring wireless security, you also need to configure your wireless adapter to use the same security settings before you can connect wirelessly. Not all wireless adapters support WPA-PSK/WPA2-PSK/WPA/WPA2 security.

Please refer to your wireless adapter user guide for more details. It is strongly recommended to set up a simple wireless security such as WPA-PSK (when the wireless client supports WPA-PSK) in order to secure your network.

Most wireless adapters in computers and laptops support at least WEP and WPA.

Advanced

The Advanced page is used to modify the advanced wireless settings for the router. These settings should not be changed unless you are aware of what effect they will have.



Wireless LAN > Advanced

Advanced Wireless Configuration

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

BG Protection Mode	Auto
Client Idle Timeout	300 sec (range 60 - 600, default 300)
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	2 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	○ Enable ● Disable

Figure 38 - Wireless Settings - Advanced

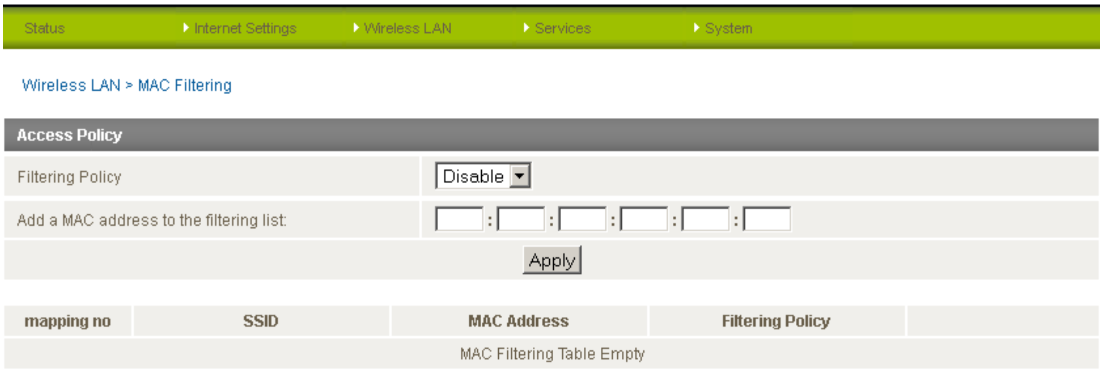
OPTION	DEFINITION
BG Protection Mode	A protective designed to prevent collisions among 802.11b/g modes. Mode options include Auto, On, or Off.
Client Ide Timeout	The time in seconds that a wireless client session can be idle before the router cancels the session and defines the wireless client as not connected.
Beacon Interval	Interval of time in which the wireless router broadcasts a beacon which is used to synchronize the wireless network.
Data Beacon Rate (DTIM)	Enter a value in milliseconds between 1 and 255 for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
Fragmentation Threshold	This specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
RTS Threshold	When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
TX Power	This determines the transmitting or output power of the antenna.
Short Preamble	Enable or disable short preambles in use on the wireless network. Using short preambles should improve throughput, however some wireless network adapters must use long preambles.

Table 23 - Wireless Settings - Advanced Configuration Items

Click the “Save” button to save any advanced settings changes.

MAC Filter

The Wireless LAN MAC filter feature ensures the network accessibility for the wireless client devices can be controlled. When the MAC filter is enabled with an Allow policy only those wireless clients whose MAC address is listed in the MAC filter list will be able to gain network access. All other wireless client devices will be denied network access. When the MAC filter is enabled with a Reject policy all wireless client devices listed whose MAC address is listed in the MAC filter list will be denied network access. All other wireless client devices will be allowed network access.



Wireless LAN > MAC Filtering

Access Policy

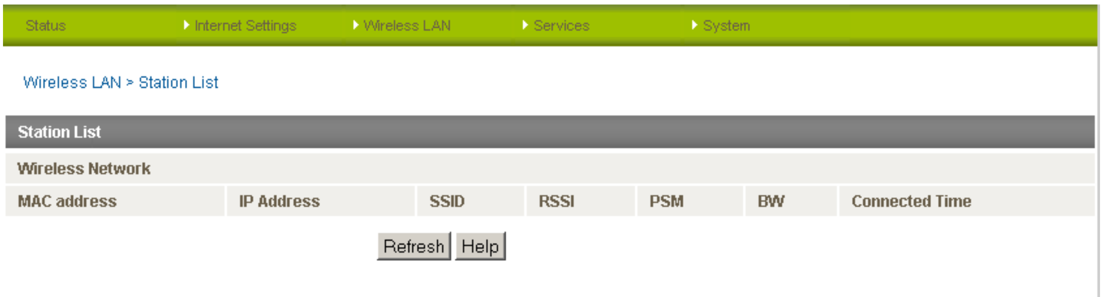
Filtering Policy	Disable
Add a MAC address to the filtering list:	_ : _ : _ : _ : _ : _

mapping no	SSID	MAC Address	Filtering Policy	
MAC Filtering Table Empty				

Figure 39 - Wireless LAN - MAC Filter

Station List

The Station List page shows the number of devices currently connected to your NTC-40WV via Wireless. The MAC address, Host Name and IP address of these devices are displayed.



Wireless LAN > Station List

Station List

Wireless Network

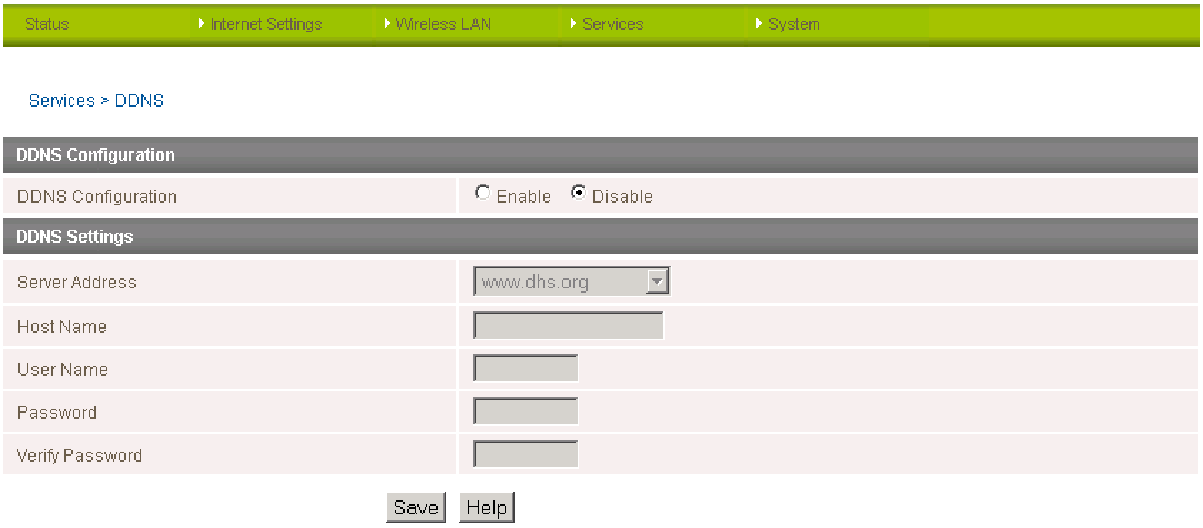
MAC address	IP Address	SSID	RSSI	PSM	BW	Connected Time

Figure 40 - Wireless Station List

Services

DDNS

The DDNS page is used to configure the Dynamic DNS feature of the router. A number of dynamic DNS hosts are offered to select from.



Services > DDNS

DDNS Configuration	
DDNS Configuration	○ Enable ● Disable
DDNS Settings	
Server Address	www.dhs.org
Host Name	
User Name	
Password	
Verify Password	

Figure 41 - DDNS Settings

Dynamic DNS provides a method for the router to update an external name server with the current WAN IP address.

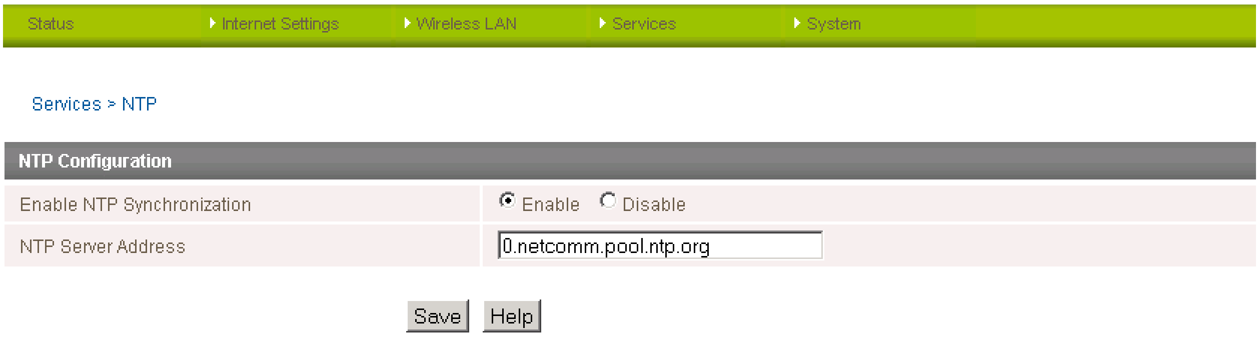
To configure dynamic DNS:

1. Click the Enable option for the “DDNS Configuration” field.
2. Select the Dynamic DNS service that you wish to use. Enter your dynamic DNS account credentials.
3. Click the “Save” button to save the new settings.

NTP

The NTP (Network Time Protocol) settings page allows the NTC-40WV to synchronise its internal clock with a global Internet Time server. This setting provides an accurate timekeeping function for features such as System Log entries and Firewall settings where the current system time is displayed and recorded.

Any NTP server available publicly through the internet can be used. The default NTP server is 0.netcomm.pool.ntp.org.



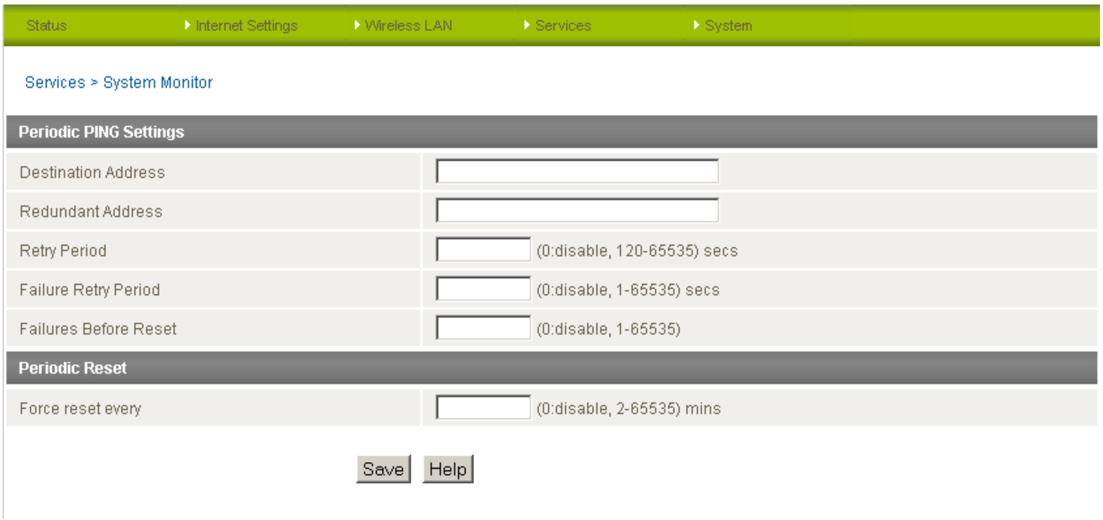
Services > NTP

NTP Configuration	
Enable NTP Synchronization	● Enable ○ Disable
NTP Server Address	0.netcomm.pool.ntp.org

Figure 42 - NTP Settings

System Monitor

The System Monitor page is used to configure the behaviour of the Periodic Piing monitor function.



Services > System Monitor

Periodic PING Settings	
Destination Address	
Redundant Address	
Retry Period	(0:disable, 120-65535) secs
Failure Retry Period	(0:disable, 1-65535) secs
Failures Before Reset	(0:disable, 1-65535)
Periodic Reset	
Force reset every	(0:disable, 2-65535) mins

Figure 43 - System Monitor Settings

The Periodic Ping Reset Monitor configures the router to transmit controlled ping packets to 2 specified IP addresses. Should the router not receive responses to the pings, the router will reboot.

This works as follows:

1. After every “Periodic Ping Timer” configured interval, the router sends 3 consecutive pings to the “Destination Address”.
2. If all 3 pings fail the router sends 3 consecutive pings to the “Redundant Address”.
3. The router then sends 3 consecutive pings to the “Destination Address” and 3 consecutive pings to the “Redundant Address” every “Failure Retry Period” configured interval.
4. If all accelerated pings in step 3 above fail the number of times configured in “Failures Before Reset”, the router reboots.
5. If any ping succeeds the router returns to step 1 and does not reboot.

Please note: The “Periodic Ping Timer” should never be set to a value less than 60 seconds; this is to allow the router time to reconnect to the cellular network following a reboot.

<u>How to disable the Periodic Ping Monitor</u>

To disable the Periodic Ping Reset Monitor simply set the “Retry Period” field to 0.

Please note: The traffic generated by the periodic ping feature is counted as chargeable usage, please keep this in mind when selecting how often to ping.

<u>How to configure a Forced Reset</u>

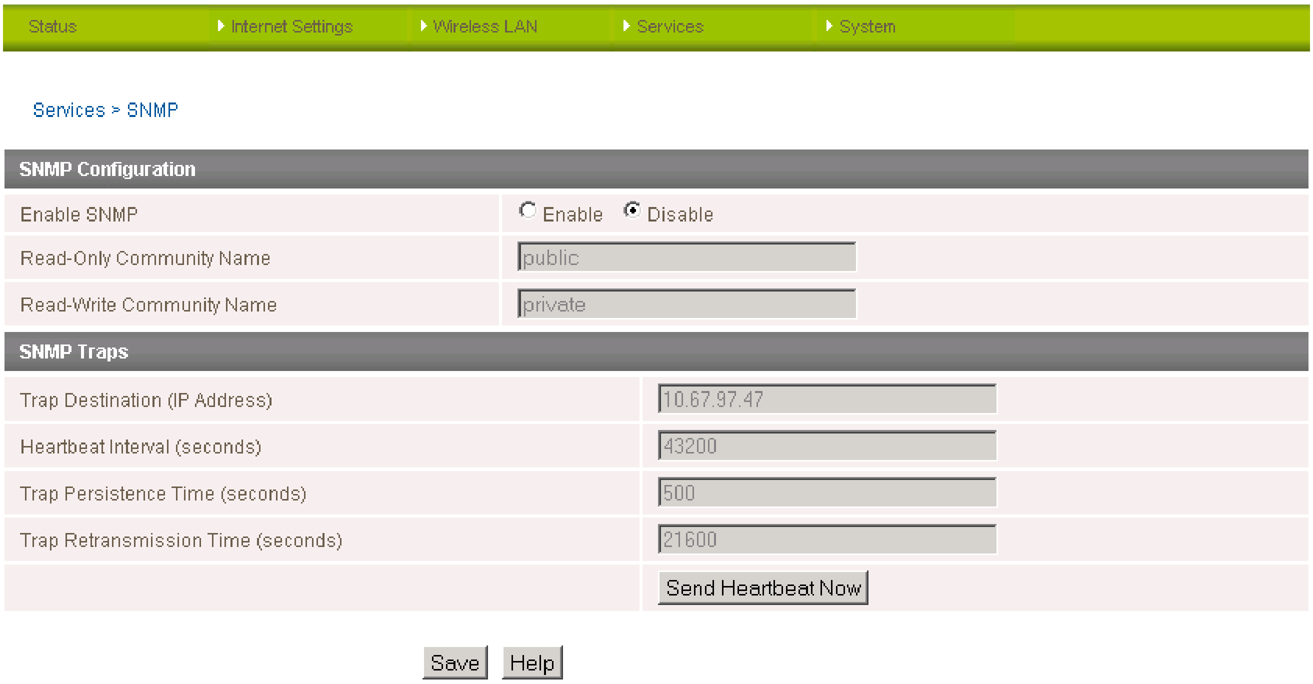
This facility is available by clicking on the “Services” menu followed by the “System Monitor” menu item on the right.

The router can be configured to automatically reboot after a period of time specified in minutes. While this is not necessary, it does ensure that in the case of remote installations, it will reboot the router if some anomaly occurs.

The default value is 0 which disables the “Forced Reset Every” field. The maximum value is 65535 minutes.

SNMP

The SNMP page is used to configure the SNMP features of the router.



SNMP Configuration	
Enable SNMP	○ Enable ● Disable
Read-Only Community Name	public
Read-Write Community Name	private

SNMP Traps	
Trap Destination (IP Address)	10.67.97.47
Heartbeat Interval (seconds)	43200
Trap Persistence Time (seconds)	500
Trap Retransmission Time (seconds)	21600
	Send Heartbeat Now

Figure 44 - SNMP Settings

SNMP (Simple Network Management Protocol) is used to remotely monitor the router for conditions that may warrant administrative attention. It can be used to retrieve information from the router such as the signal strength, the system time, the interface status, etc.

To configure SNMP:

1. Select Enable for the “Enable SNMP” option.
2. Enter Community Names or leave them as the default settings.

Community names are used as a type of security to prevent access to reading and/or writing to the routers configuration. It is recommended to change the Community names to something other than the default settings when using this feature.

3. Click the “Save” button to save any changes to the settings.

ITEM	DEFINITION
Trap Destination (IP Address)	The IP Address SNMP data is to be sent to.
Heartbeat Interval (seconds)	The number of seconds between SNMP heartbeats.
Trap Persistence Time (seconds)	The length of time an SNMP trap persists.
Trap Retransmission Time (seconds)	The length of time between SNMP trap retransmissions.

Table 24 - SNMP Configuration Options

You can also trigger an SNMP Heartbeat manually by clicking the “Send Heartbeat Now” button.

SMS

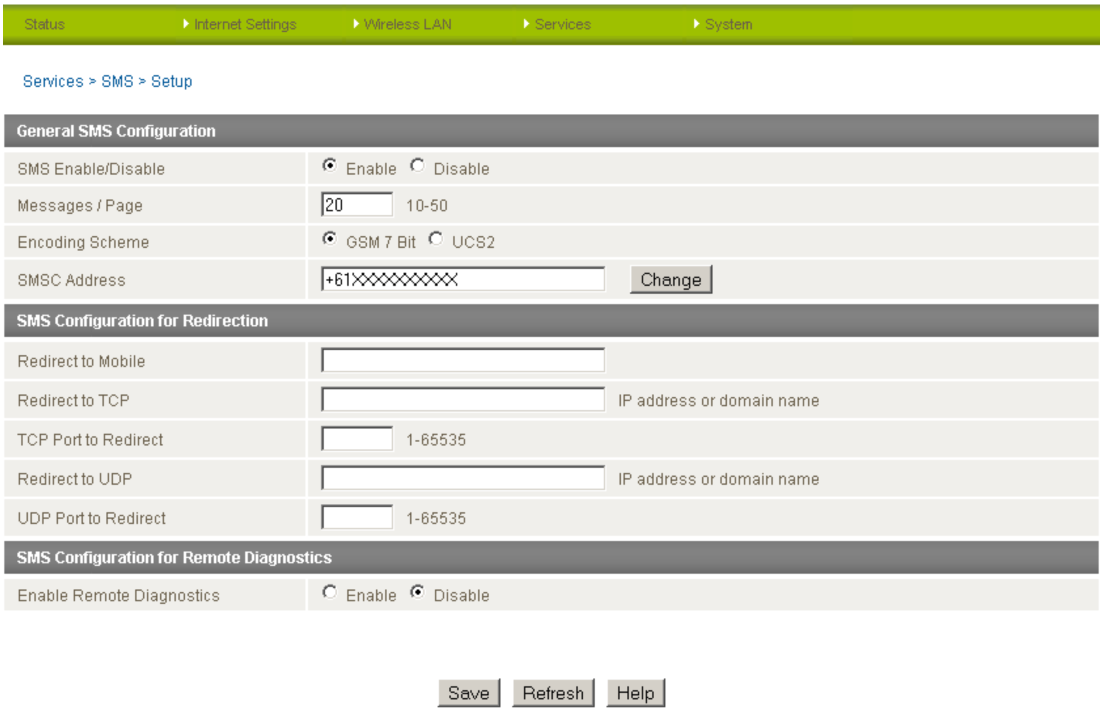
The SMS pages are used to perform functions using the built-in SMS tools application. The SMS Tools application offers basic SMS functionality such as sending a message, receiving a message and redirecting an incoming message to another destination. You can also utilise this feature to read and change run-time variables on the router.

Basic functionality supported:

- Ability to send a text message via a 3G network and store in permanent storage.
- Ability to receive a text message via a 3G network and store in permanent storage.
- Ability to forward incoming text messages via a 3G network to another remote destination which may be a TCP/UDP server or other mobile devices.
- Ability to read run-time variables from the device (e.g. uptime) and send result to a remote destination which may be a TCP/UDP server or other mobile devices.
- Ability to change live configuration on the device (e.g. connection APN).
- Ability to execute supported commands (e.g. reboot).

Setup

General SMS functionality is enabled by default. You can open the Setup page in order to configure additional settings. To do this, click on “Services”, then “SMS” and then “Setup”.



Services > SMS > Setup

General SMS Configuration

SMS Enable/Disable	● Enable ○ Disable
Messages / Page	20 10-50
Encoding Scheme	● GSM 7 Bit ○ UCS2
SMSC Address	+61XXXXXXXXXX Change

SMS Configuration for Redirection

Redirect to Mobile	
Redirect to TCP	IP address or domain name
TCP Port to Redirect	1-65535
Redirect to UDP	IP address or domain name
UDP Port to Redirect	1-65535

SMS Configuration for Remote Diagnostics

Enable Remote Diagnostics	○ Enable ● Disable

Figure 45 - SMS Function Setup

OPTION	DEFINITION
SMS Enable/Disable	The option to switch off the SMS function.
Messages / Page	Enter the number of SMS messages to display per page.
Encoding Scheme	The encoding method used for SMS messages.
SMSC Address	The short message service centre (SMSC) address is the number of your mobile brodband SMS provider.
Redirect to Mobile	Forward incoming text messages to the remote destination defined.
Redirect to TCP	Forward incoming text messages to the remote TCP destination defined.
TCP Port to redirect	The TCP port on which to connect to the remote destination on.
Redirect to UDP	Forward incoming text messages to the remote UDP destination defined.
UDP Port to redirect	The UDP port on which to connect to the remote destination on.
Enable Remote Diagnostics	Enable diagnostics to be performed by a specially crafted SMS message.

Table 25 -SMS Setup Settings

Table 26 - SMS Setup Configuration Items

Incoming text messages can be redirected to another mobile device and/or a TCP/UDP message server.

The following page details the options available via the SMS function.

Redirect To Mobile

You can forward incoming text messages to a different destination number. This destination number can be another mobile phone or 3G router phone number. To disable the feature, simply delete the number in the 'Redirect To Mobile" field and click the "Save" button.

For Example:

If someone sends a text message and "Redirect to Mobile" is set to "0412345678", this text message is stored on the router and forwarded to "0412345678" at the same time.

Redirect to TCP & TCP Port, Redirect to UDP & UDP Port

You can also forward incoming text messages to a TCP/UDP based destination. The TCP or UDP server can be any kind of public or private server if the server accepts incoming text-based message.

The TCP/UDP address can be an IP address or domain name. The port number range is from 1 to 65535. Please refer to your TCP/UDP based SMS server configuration for which port to use.

For Example:

If someone sends a text message and "Redirect to TCP" is set to "192.168.20.3" and "2002", this text message is stored in the router and forwarded to "192.168.20.3" on port "2002" at the same time.

SMS Configuration for Remote Diagnostics

Enable Remote Diagnostics

Enable or disable the Remote Diagnostics feature. If this setting is enabled all incoming text messages are parsed and tested for if they contain Remote Diagnostics commands.

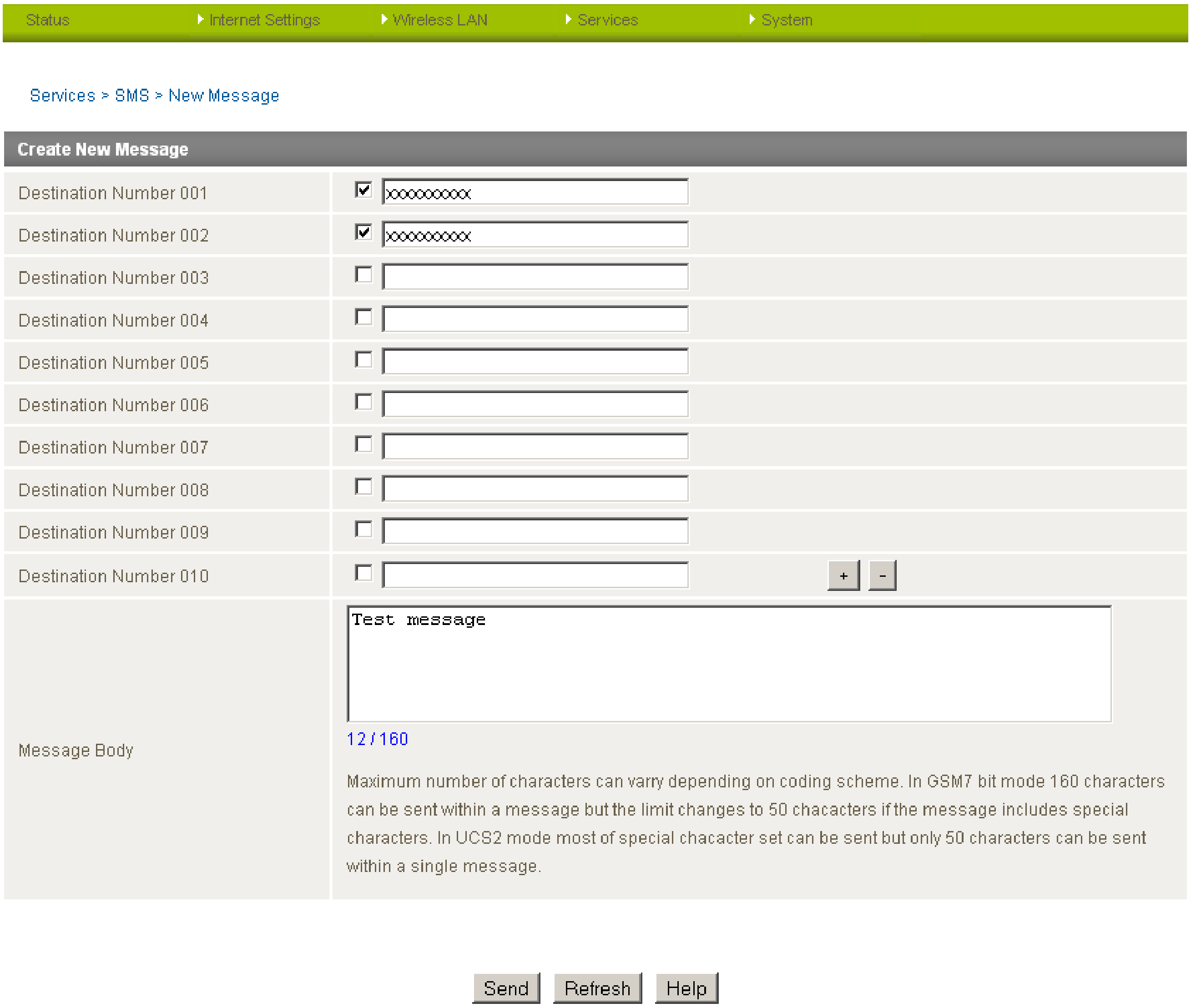
If Remote Diagnostics commands are found, the router executes those commands. This feature is disabled by default.

Please note: It is possible to adjust settings and prevent your router from functioning correctly. If this occurs, you will need to perform a factory reset in order to restore normal operation.

It is highly recommended to enable security when utilising this feature.

New Message

The New Message page can be used to send an SMS text messages to one or multiple recipients.



Create New Message

Destination Number 001	☑ xxxxxxxxxx
Destination Number 002	☑ xxxxxxxxxx
Destination Number 003	□
Destination Number 004	□
Destination Number 005	□
Destination Number 006	□
Destination Number 007	□
Destination Number 008	□
Destination Number 009	□
Destination Number 010	□
Message Body	Test message 12 / 160 Maximum number of characters can varry depending on coding scheme. In GSM7 bit mode 160 characters can be sent within a message but the limit changes to 50 chacacters if the message includes special characters. In UCS2 mode most of special chacacter set can be sent but only 50 characters can be sent within a single message.

Figure 46 - New SMS Message

A new SMS message can be sent to a maximum of 100 recipients at the same time. After sending the message, the result is displayed next to the destination number as "Success" (in blue) or "Failure" (in red).

By default 10 recipient entry fields are shown on this page however you can increase or decrease this number by pressing the + or – button at right side of the last recipient entry field.

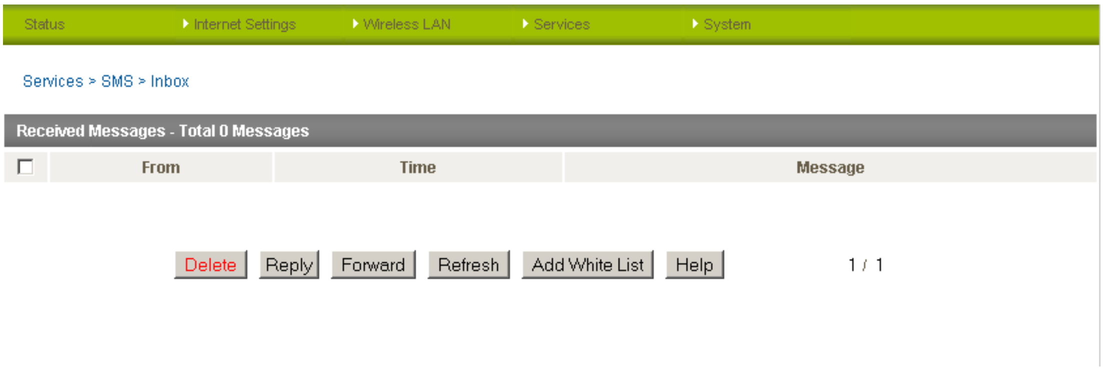
You can select to enable or disable individual message recipients by selecting the checkbox beside each entered number.

After entering the appropriate recipient numbers, type your SMS message in the "Message Body" field and then click the "Send" button.

Inbox / Outbox

You can check all sent SMS messages in the SMS Outbox or you can read, delete, reply or forward an SMS message to another mobile device from the SMS Inbox.

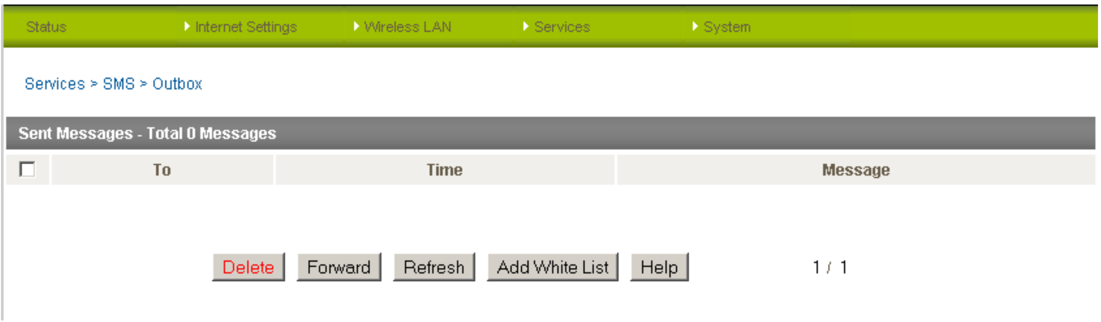
You are also able to add the SMS message sender to the “White List” which is used to secure the Remote Diagnostics feature. Simply select the sender or recipient number and click the “Add White List” button.



Received Messages - Total 0 Messages

□	From	Time	Message

Figure 47 - SMS Inbox



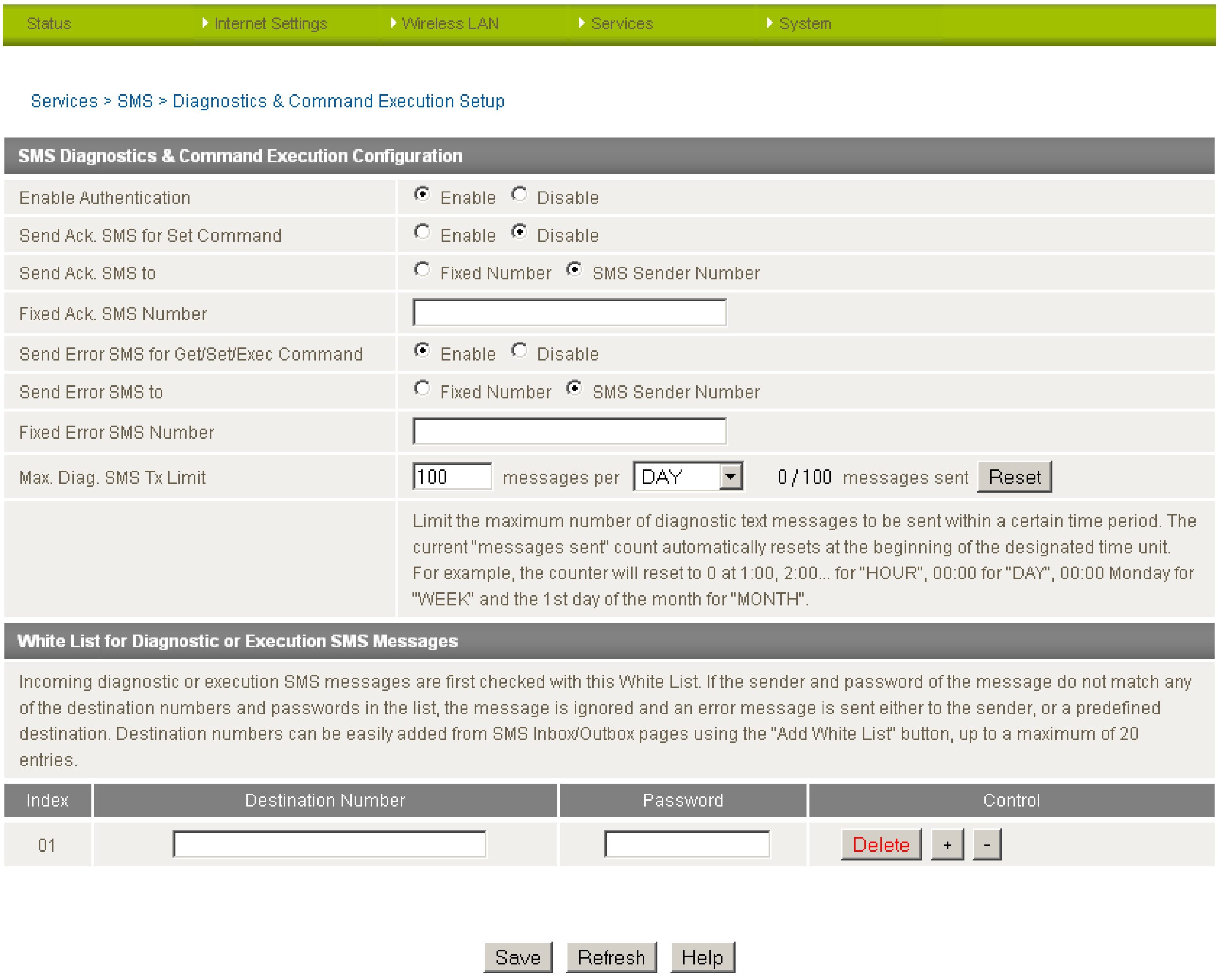
Sent Messages - Total 0 Messages

□	To	Time	Message

Figure 48 - SMS Outbox

Diagnostics

The Diagnostics page is used to configure the SMS Diagnostics and Command execution configuration. This enables you to change the configuration or check on the status of the router via SMS commands.



Services > SMS > Diagnostics & Command Execution Setup

SMS Diagnostics & Command Execution Configuration

Enable Authentication	● Enable ○ Disable
Send Ack. SMS for Set Command	○ Enable ● Disable
Send Ack. SMS to	○ Fixed Number ● SMS Sender Number
Fixed Ack. SMS Number	
Send Error SMS for Get/Set/Exec Command	● Enable ○ Disable
Send Error SMS to	○ Fixed Number ● SMS Sender Number
Fixed Error SMS Number	
Max. Diag. SMS Tx Limit	100 messages per DAY 0 / 100 messages sent Reset
	Limit the maximum number of diagnostic text messages to be sent within a certain time period. The current "messages sent" count automatically resets at the beginning of the designated time unit. For example, the counter will reset to 0 at 1:00, 2:00... for "HOUR", 00:00 for "DAY", 00:00 Monday for "WEEK" and the 1st day of the month for "MONTH".

White List for Diagnostic or Execution SMS Messages

Incoming diagnostic or execution SMS messages are first checked with this White List. If the sender and password of the message do not match any of the destination numbers and passwords in the list, the message is ignored and an error message is sent either to the sender, or a predefined destination. Destination numbers can be easily added from SMS Inbox/Outbox pages using the "Add White List" button, up to a maximum of 20 entries.

Index	Destination Number	Password	Control
01			Delete + -

Figure 49 - SMS Diagnostics Settings

The following section details the configuration items available.

Enable Authentication

Enable or disable checking the sender's phone number against the allowed sender "White List" for incoming Diagnostics/Command Execution SMS messages.

If authentication is enabled, the router will check if the sender's number exists in the "White List". If it exists, the router then checks the password in the incoming message against the password in the "White List" for the corresponding sending number. If they match, the Diagnostics/Command is executed.

If the number does not exist in "White List" or the password does not match, the router does not execute the incoming Diagnostics/Command Execution SMS message.

This is enabled by default.

It is highly recommended to enable security when utilising the Diagnostics/Command Execution feature.

Send Ack. SMS for Set Command

Enable or disable sending an acknowledge message after execution of a "Set" command. If disabled the router does not send any acknowledgement after execution of a "Set" command.

This can be useful to determine if a command was received and executed by the router. This is disabled by default.

Send Ack. SMS to

This field defines the destination to send an acknowledgement message function to after the execution of a "Set" command.

If "Fixed Ack. SMS Number" is selected, the acknowledgement message will be sent to the predefined number in the "Fixed Ack. SMS Number" field. If the SMS Sender Number is selected, the acknowledgement message will be sent to sender directly. The default setting is to use "SMS Sender Number".

Fixed Ack. SMS Number

This field defines the destination number to which acknowledgement messages are sent after the execution of a "Set" command.

Send Error SMS for Get/Set/Exec Command

Enable or disable the sending of an error message resulting from the execution of a Get/Set/Exec command.

If disabled, the router does not send any error notifications after the execution of a Get/Set/Exec command. This function is disabled by default.

Send Error SMS to

Select the destination of the error messages from the execution of a Get/Set/Exec command.

If "Fixed Number" is selected, any error messages will be sent to the predefined number in the "Fixed Error SMS Number" field. If "SMS Sender Number" is selected, any error messages will be sent to the sender directly.
The default setting is to use "SMS Sender Number".

Fixed Error SMS Number

The destination number to which error messages from the execution of a Get/Set/Exec command should be sent.

Max. Diag. SMS Tx Limit

You can set the maximum number of acknowledgement and error messages sent when an SMS Diagnostics and/or Command is executed. You can set the maximum limit on a per hour/day/week or month basis.

The default is to send a maximum of 100 messages per day.

You can check the current sent message count by looking next to the "Max. Diag. SMS Tx Limit" field. If the maximum number has been exceeded, you can also reset sent the message counter by pressing the "Reset" button. The Total transmitted message count resets after a reboot or at the beginning of the time frame specified.

Please note: Times displayed are in UTC format.

For Example:

- If the time frame is set to "HOUR" and the current time is "04:30", then the counter will reset to zero at "05:00".
- If time frame is set to "DAY" and current date and time is "04:30" 17th of March, then the counter will reset to zero at "00:00" 18th of March.
- If time period is set to "WEEK" and current date and time is "04:30" Saturday, then the counter will reset to zero at "00:00" on the coming Monday.
- If time period is set to "MONTH" and current date and time is "04:30" 17th of March, then the counter will reset to zero at "00:00" 1st of April.

White List

A maximum number of 20 entries can be stored in the router.

If Authentication is enabled, any incoming Diagnostics/Command Execution SMS messages are processed only if the sender's number exists in White List and the message password matches with the password specified in the White List.

One blank entry is shown by default and you can add or delete an entry by pressing the "+" or "–" button. The White List numbers and passwords can be cleared by pressing the "Delete" button. To add an entry, simply enter the appropriate phone number and password and click "Save".

Message Storage for Diagnostic Messages

Diagnostic messages (Diagnostic commands, acknowledgements and error notification messages) sent to remote destination are stored in the Inbox/Outbox.

Security

In order to provide security for SMS command execution, it is recommended that all SMS commands be subject to successful authentication against the White List as well as setting a password for each phone number entered. This prevents unauthorised or accidental execution of SMS commands.

SMS Command format

Generic Format for reading variables:

get VARIABLENAME

PASSWORD get VARIABLENAME

Generic Format for writing to variables:

set VARIABLENAME=VALUE

PASSWORD set VARIABLENAME=VALUE

Generic Format for executing a command:

execute COMMAND

PASSWORD execute COMMAND

Replies

Upon receipt of successfully formatted, authenticated (if required) command, the router will reply to the SMS in the following format:

TYPE	SMS CONTENTS	NOTES
Get Command	"VARIABLENAME=VALUE"	
Set Command	"Successfully set VARIABLENAME to VALUE"	Only sent if the acknowledgment message function is enabled
Execute Command	"Successfully executed command COMMAND"	

Table 27 - SMS Diagnostic Command Syntax

Where "VARIABLENAME" is the name of the value to be read

Where "VARIABLENAME(x)" is the name of another value to be read

Where "VALUE" is the content to be written to the "VARIABLENAME"

Where "COMMAND" is a supported command to be executed by the device (e.g. reboot).

Where "PASSWORD" is the password (if configured) for the corresponding sender number specified in the White List.

Multiple commands can be sent in the same message, if separated by a semicolon.

For Example:

get VARIABLENAME1; get VARIABLENAME2; get VARIABLENAME3

PASSWORD get VARIABLENAME1; get VARIABLENAME2

set VARIABLENAME=VALUE1 ; set VARIABLENAME2=VALUE2

PASSWORD set VARIABLENAME1=VALUE1; set VARIABLENAME2=VALUE2; set VARIABLENAME3=VALUE3

If required, values can also be bound by an apostrophe, double apostrophe or back tick.

For Example:

"set VARIABLE='VALUE'"

"set VARIABLE="VALUE""

"set VARIABLE=`VALUE`"

"get VARIABLE"

A password (if required), only needs to be specified once per SMS, but can be prefixed to each command if desired.

"PASSWORD get Variable1"; "get VARABLE2"

"PASSWORD set VARIABLE1=VALUE1"; "set VARIABLE2=VALUE2"

If the command sent includes the “reboot” command and has already passed the White List password check, the device keeps this password and executes the remaining command line after the reboot with this same password.

For Example:
“PASSWORD execute reboot; get Variable1”; “get VARABLE2”
“PASSWORD execute reboot; PASSWORD get Variable1”; “get VARABLE2”

Commands are case insensitive, however variable names and values are case sensitive.

List of valid commands (which can be used in conjunction with the execute command):

“pdpcycle”, “pdpdown” and “pdpup” commands can have a profile number suffix ‘x’ added. Without the suffix specified, the command operates against the current active profile or last active profile.

#	COMMAND NAME	DESCRIPTION
1	Reboot	Immediately perform a soft reboot
2	pdpcycle or pdpcyclex	Disconnect (if connected) and reconnect the 3G connection. If a profile number is selected in the command, try to disconnect/reconnect the specified profile in case the profile is active. If no profile number is selected, try to disconnect/reconnect the current active profile. These commands report an error if no profile number is selected and there is no currently activated profile.
3	pdpdown or pdpdownx	Disconnect the PDP. If a profile number is selected in the command, try to disconnect the specified profile in case the profile is active. If no profile number is selected, try to disconnect the current active profile. These commands report an error if no profile number is selected and there is no currently activated profile.
4	pdpup or pdpupx	Reconnect the PDP. If a profile number is selected in the command, try to connect with the specified profile. If no profile number is selected, try to connect to the last active profile. The router will check the currently activated profile and disconnect this profile before executing the command. These commands report an error if no profile number is selected and there is no stored last active profile number.

Table 28 - List of Valid SMS Diagnostic Commands

List of valid variables:

Where “x” is a profile number (1-6). If no profile is specified, variables are read or written to for the current active profile. If a profile is specified, variable are read or written to for the specified profile number (‘x’).

#	RDB VARIABLE NAME	SMS VARIABLE NAME	READ/WRITE	DESCRIPTION	EXAMPLE
0	link.profile.x.enable link.profile.x.apn link.profile.x.user link.profile.x.pass link.profile.x.auth_type link.profile.x.iplocal link.profile.x.status	profile or profilex	RW	Profile	Read: (profile no,apn,user,pass,auth,iplocal,status) 1,Telstra.internet,username,password, chap,202.44.185.111,up Write: (apn, user, pass,auth) Telstra.internet,username,password
1	link.profile.x.apn	apn or apnx	RW	APN	telstra.internet
2	link.profile.x.user	username or usernamex	RW	3G username	Guest, could also return “null”
3	link.profile.x.pass	password or password	RW	3G password	Guest, could also return “null”
4	link.profile.x.auth_type	authtype or authtypex	RW	3G Authentication type	"pap" or"chap"
5	link.profile.x.iplocal	wanip or wanipx	R	WAN IP address	202.44.185.111
6	wwan.0.radio.information.signal_strength	rssi	R	3G signal strength	65 dBm
7	wwan.0.imei	imei	R	IMEI number	359102128941027512
8	statistics.usage_current	usage	R	3G data usage of current session	“Rx 500 bytes, Tx 1024 bytes, Total 1524 bytes” or “Rx 0 byte, Tx 0 byte, Total 0 byte” when wwan down
9	statistics.usage_current	wanuptime	R	Up time of current 3G session	1 days 02:30:12 or 0 days 00:00:00 when wwan down
10	/proc/uptime	deviceuptime	R	Device up time	1 days 02:30:12

11	wwan.0.system_network_status.current_band	band	R	Current 3G frequency	WCDMA 850

Table 29 - List of SMS Diagnostics Variables

SMS Diagnostics Examples

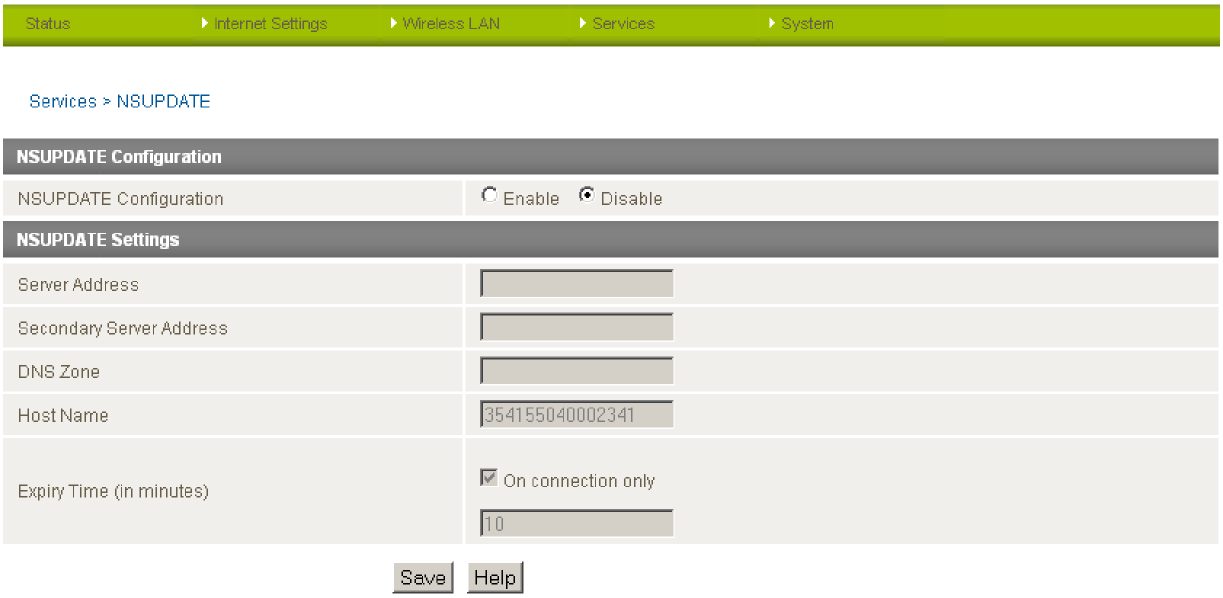
The examples below demonstrate various combinations of supported commands. This is not a complete list. To obtain a complete list, please contact NetComm.

DESCRIPTION	AUTHENTICATION	INPUT EXAMPLE
Send SMS to change APN	Not required	set apn1=Telstra.internet set apn2=”3netaccecss”
	Required	Password1234 set apn1=Telstra.internet Password1234 set apn2=3netaccecss
Send SMS to change the 3G username	Not required	set username=’NetComm’
	Required	Password1234 set username= ”NetComm”
Send SMS to change the 3G password	Not required	set password= `NetComm`
	Required	Password1234 set password= `NetComm`
Send SMS to change the 3G authentication	Not required	set authtype= ‘pap’
	Required	Password1234 set authtype = pap
Send SMS to reboot	Not required	execute reboot
	Required	Password1234 execute reboot
Send SMS to check the WAN IP address	Not required	get wanip
	Required	Password1234 get wanip
Send SMS to check the 3G signal strength	Not required	get rssi
	Required	Password1234 get rssi
Send SMS to check the IMEI number	Not required	get imei
	Required	Password1234 get imei
Send SMS to check the current band	Not required	get band
	Required	Password1234 get band
Send SMS to Disconnect (if disconnected) and reconnect the 3G connection	Not required	execute pdpcycle
	Required	Password1234 execute “pdpcycle1”
Send SMS to disconnect the 3G connection	Not required	exceute pdpdown1
	Required	Password1234 execute “pdpdown1”
Send SMS to connection the 3G connection	Not required	execute pdpup
	Required	Password1234 execute pdpup1
Send multiple get command	Not required	get wanip; get rssi
	Required	Password1234 get wanip; get rssi
Send multiple set command	Not required	set apn1=”3netaccecss”; set password1=’NetComm’
	Required	Password1234 set apn=”3netaccecss”; set password=NetComm

Table 30 - SMS Diagnostics - Example Commands

NS Update

NS Update is used to update an internal DNS resource. This can be used to enable a fully qualified domain name (FQDN) to be used to access the router.



NSUPDATE Configuration	○ Enable ● Disable
Server Address	
Secondary Server Address	
DNS Zone	
Host Name	354155040002341
Expiry Time (in minutes)	☑ On connection only 10

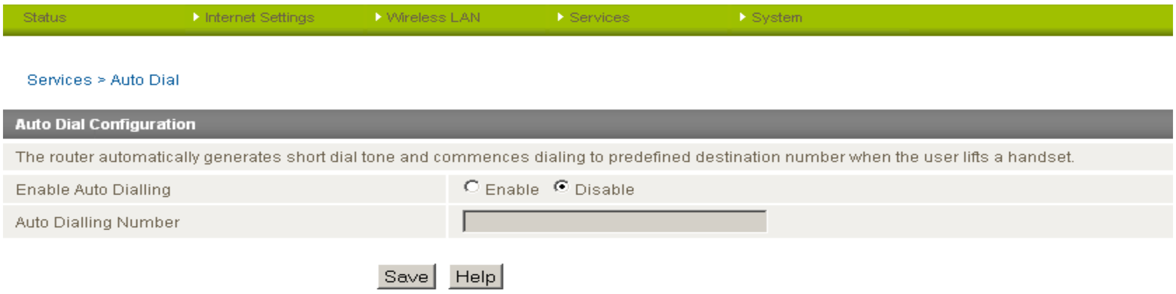
Figure 50 - NS Update Settings

OPTION	DEFINITION
NSUPDATE Configuration	Enable or disable the NS Update function.
Server Address	The address of the NS server to update the DNS entry for the router on.
Secondary Server Address	The address of the secondary NS server to update the DNS entry for the router on.
DNS Zone	The DNS zone the routers DNS entry is contained within.
Host Name	The hostname of the router to put in the DNS entry.
Expiry Time (in minutes)	The number of minutes the DNS entry will remain valid before an update is performed. You can also select to only perform an update when the WWAN connection becomes available.

Table 31 - NS Update Configuration Items

Auto Dial

Auto Dial is used to automatically dial the configured number as soon as the telephone handset is picked up. You can specify any telephone number you wish.



The router automatically generates short dial tone and commences dialing to predefined destination number when the user lifts a handset.

Enable Auto Dialling	○ Enable ● Disable
Auto Dialling Number	

Figure 51 - Auto Dial Settings

ITEM	DEFINITION
Enable Auto Dialling	Enable or disable the auto dialling function of the router.
Auto Dialling Number	Enter the number to be automatically dialled when the attached handset is picked up.

Table 32 - Auto Dial Configuration Items

After entering the required auto dial telephone number, click the “Save” button.

System

Log

The Log page is used to download or display the current System Log of the router.

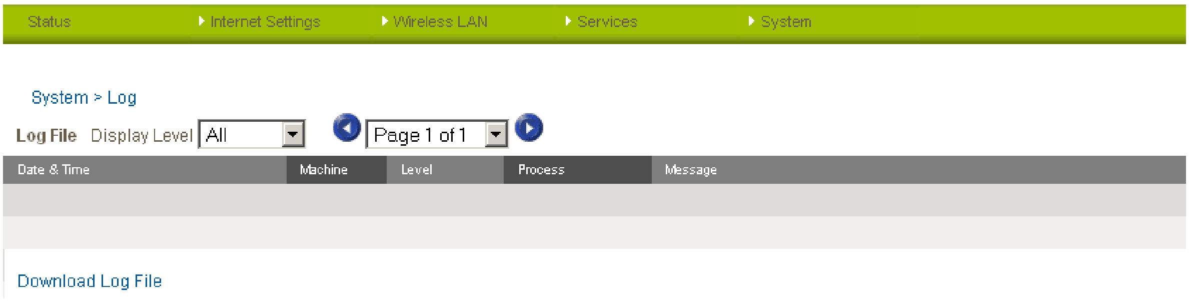


Figure 52 - System Log

The System Log enables you to troubleshoot any issues you may be experiencing with your router.

Selecting the appropriate logging level will show you either informational messages about your router or every message produced when “All” is selected.

ITEM	DEFINITION
All	Display all system log messages.
Debug	Show extended system log messages with full debugging level details.
Info	Show informational messages only.
Notice	Show normal system logging information.
Warning	Show warning messages only.
Error	Show error condition messages only.

Table 33 - System Log Detail Levels

You can also download the current System Log to your computer for off-line viewing. To do this, click the “Download Log File” link at the bottom of the page.

Load / Save

Settings

The settings page is used to backup or restore the routers configuration or to reset it to factory defaults. In order to view the settings page you must be logged into the web user interface as “root” using the password “admin”.

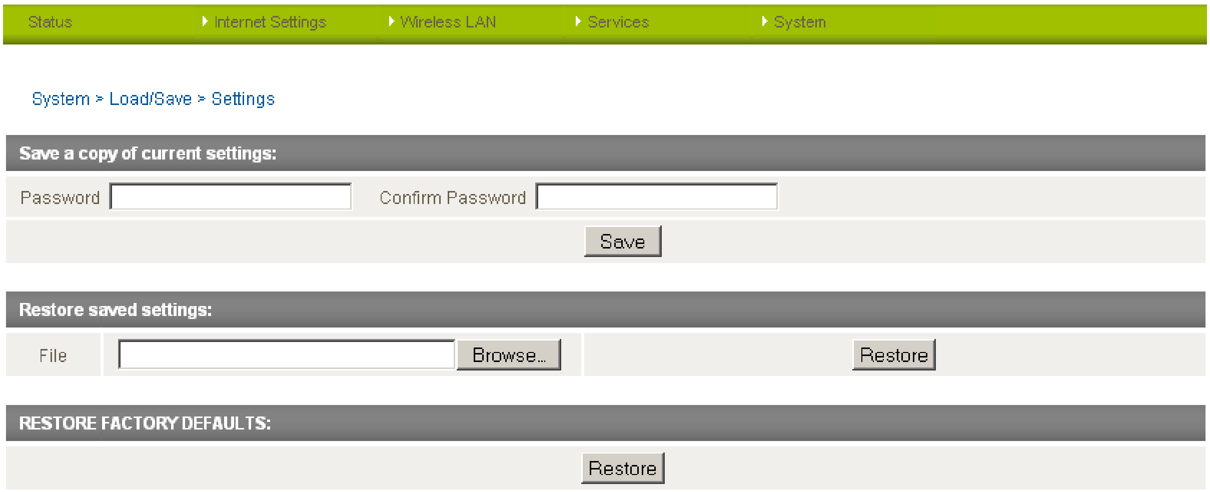


Figure 53 - Load / Save Configuration Page

Please note: In order to perform an update, you must be logged into the router as the root user (see the Remote Administration section for more details).

To save a copy of the routers configuration

1. Key in the root manager Password and click Save

This will download a copy of the current settings from the router to your PC.

Please note: The following conditions apply:-

- It is NOT possible to edit the contents of the file downloaded; if you modify the contents of the configuration file in any way you will not be able to restore it later.
- You may change the name of the file if you wish but the filename extension must remain “.cfg”

To restore a copy of the routers configuration

1. Click the “Browse” button.
2. Select the configuration file you wish to restore.
3. Click the “Restore” button.

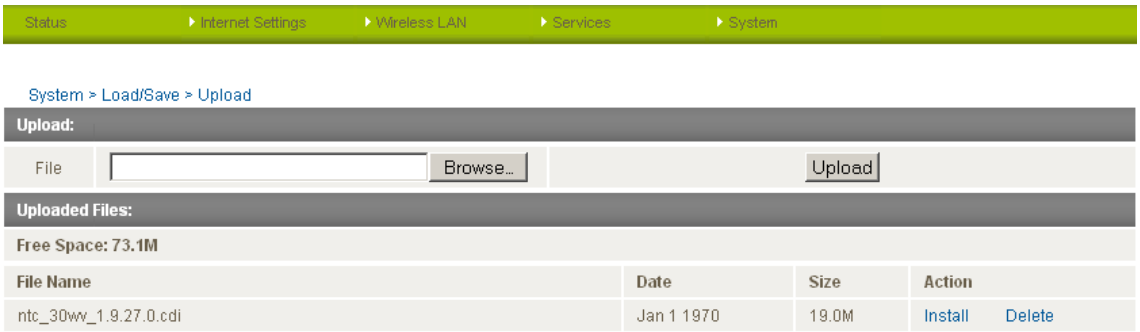
To restore the routers configuration to the factory defaults

Click Restore to restore the factory default configuration.

The router will then restart with the factory default configuration loaded.

Upload

The Upload page enables you to upload firmware files or user created application packages to the NTC-40WV.



System > Load/Save > Upload

Upload:

File

Uploaded Files:

Free Space: 73.1M

File Name	Date	Size	Action
ntc_30wv_1.9.27.0.cdi	Jan 1 1970	19.0M	Install Delete

Figure 54 - Upload Page

The firmware of the router can be updated locally via LAN connection and also via remote access. Both upgrade types follow a similar process.

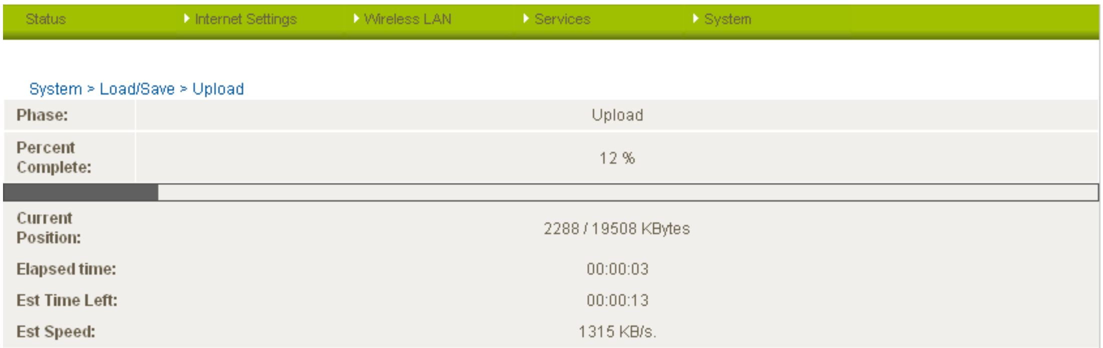
Please note: In order to perform an update, you must be logged into the router as the root user (see the Remote Administration section for more details).

Local firmware upgrade

The firmware update process has two steps. The first step is to upload and install the system recovery image onto the router.

You can do this by clicking on the browse button and then to navigate to where the recovery image upgrade file is located on your computer.

Once you have selected the system recovery image file to use, click Upload to upload the file. You will then see a progress bar as shown in the screenshot below. The upload has finished when the status bar reaches 100%.



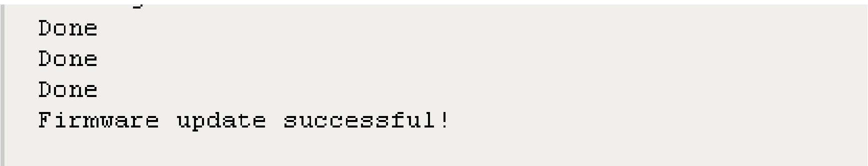
System > Load/Save > Upload

Phase:	Upload
Percent Complete:	12 %
Current Position:	2288 / 19508 KBytes
Elapsed time:	00:00:03
Est Time Left:	00:00:13
Est Speed:	1315 KB/s.

Figure 55 - Local Firmware Upgrade - Upload Firmware

When the upload has completed, the screen should refresh and list the system recovery file you have just uploaded. Click on the "Install" link to the right of this.

Once you should see a message reading "Done" as shown in the screenshot below.



```
Done
Done
Done
Firmware update successful!
```

Figure 56 - Local Firmware Upgrade - Firmware Update

Press and hold the reset button for approximately 5 – 10 seconds until the LEDs on the front of the router start to flash in an ON / OFF sequence and then release it. The router will now boot into the system recovery mode.

The second step is to upload and install the main system software image. To do this, open your web browser (e.g. Internet Explorer/Firefox/Safari) and navigate to http://192.168.1.1/

Click “Login” and type “root” in the Username and “admin” in the Password fields (without quotes). Then click on “Submit”.

The banner at the top of the page should be different to show that the router is currently in recovery console mode.

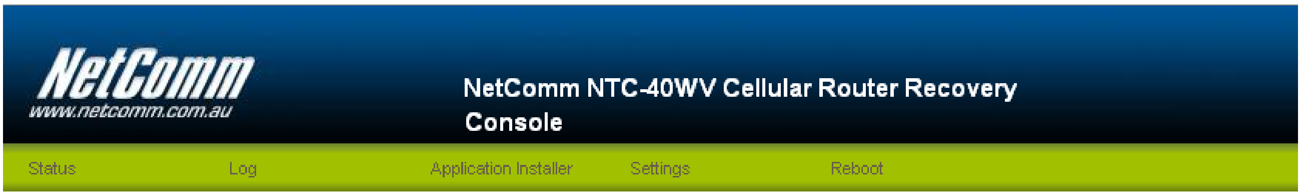
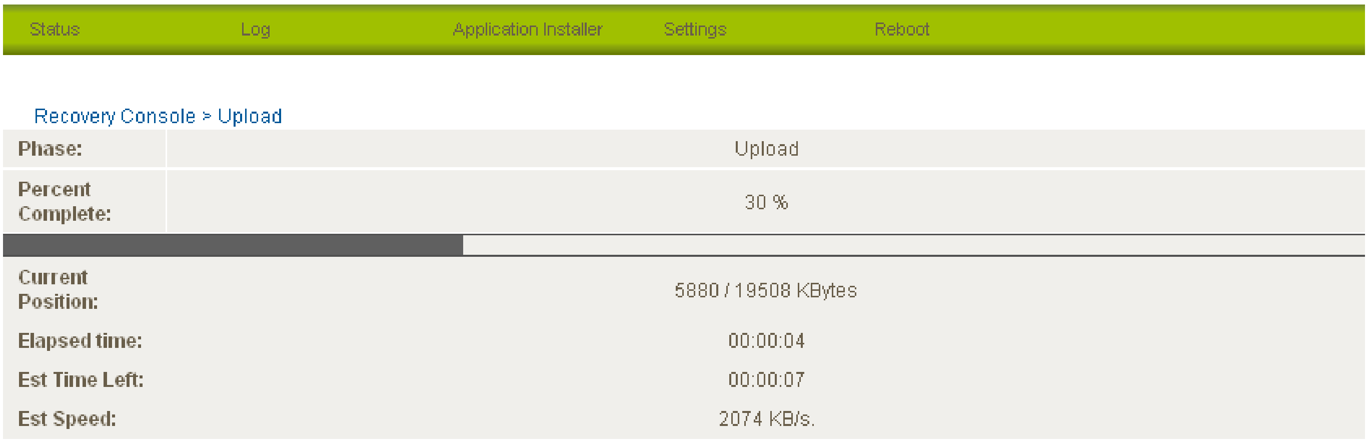


Figure 57 - Recovery Console Banner

To upload the main system software, click on “Application Installer” from the menu at the top of the page and then click on the browse button and navigate to where the main system image upgrade file is located on your computer.

Once you have selected the recovery image file to use, click Upload to upload the file. You will then see a progress bar as shown in the screenshot below. The upload has finished when the status bar reaches 100%.

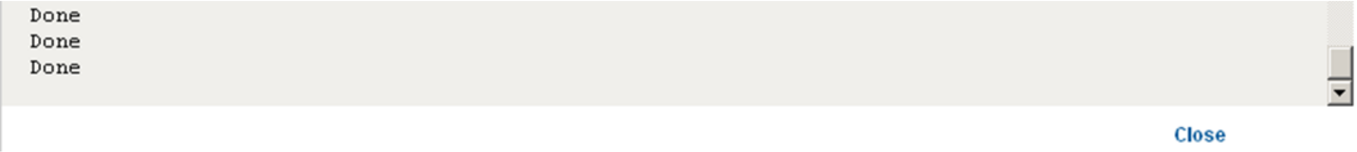


Phase:	Upload
Percent Complete:	30 %
Current Position:	5880 / 19508 KBytes
Elapsed time:	00:00:04
Est Time Left:	00:00:07
Est Speed:	2074 KB/s.

Figure 58 - Recovery Console - Upload Firmware

When the upload has completed, the screen should refresh and show the file you have just uploaded. Click on the “Install” link to the right of this.

Once you see “Done” shown as per the screenshot below, click on “Reboot” at the top of the page and then click the “Reboot” button to restart the router.



```
Done
Done
Done
```

Figure 59 - Recovery Console - Firmware Update

The router will confirm you want to restart and then start up with the new system software loaded.

Remote firmware upgrade

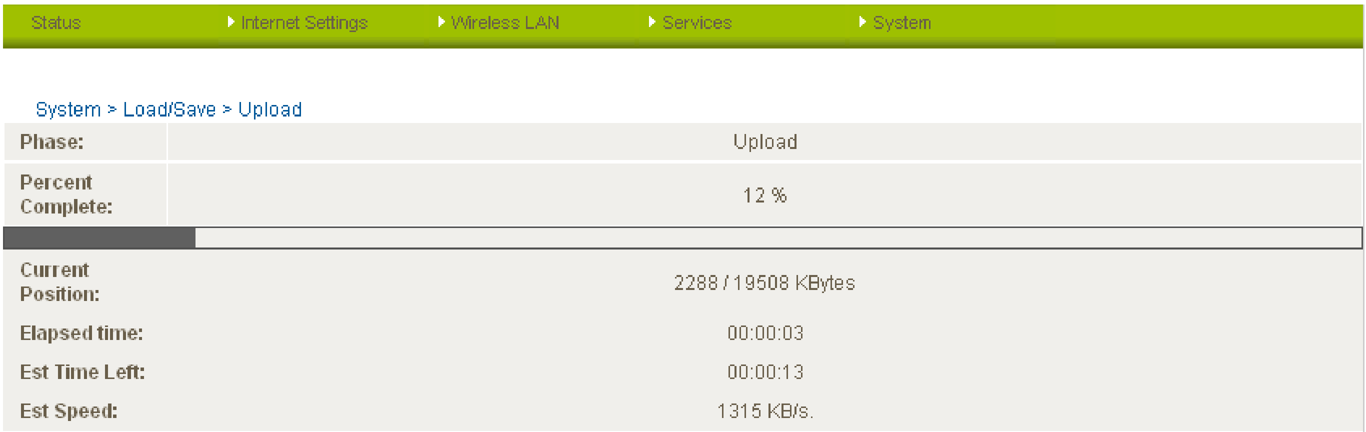
The remote firmware update process has one step:

1. Upload and install the main system image to the router.

Please note: Do not interrupt the power during a remote firmware upgrade, as this may render the router unable to start up and will require a local system recovery upload to be performed.

Upload and install the system recovery image onto the router. You can do this by clicking on the browse button and then to navigate to where the recovery image upgrade file is located on your computer.

Once you have selected the recovery image file to use, click Upload to upload the file. You will then see a progress bar as shown in the screenshot below. The upload has finished when the status bar reaches 100%.

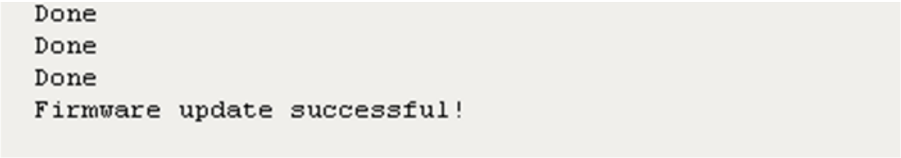


Phase:	Upload
Percent Complete:	12 %
Current Position:	2288 / 19508 KBytes
Elapsed time:	00:00:03
Est Time Left:	00:00:13
Est Speed:	1315 KB/s.

Figure 60 - Remote Firmware Upgrade - Upload Firmware

When the upload has completed, the screen should refresh and list the file you have just uploaded. Click on the “Install” link to the right of this.

Once you see “Done” shown as per the screenshot below, the router will have automatically reboot, and installed the new main system image. It should also reconnect to your selected Internet service.



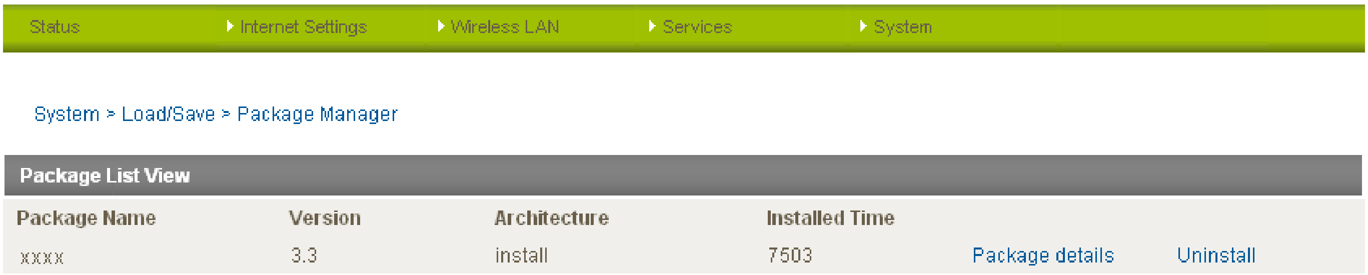
```
Done
Done
Done
Firmware update successful!
```

Figure 61 - Remote Firmware Upgrade - Firmware Update

Please note: This process can take up to 10 minutes.

Package Manager

The Package Manager page is used to provide details of any user installed packages on the router.



Package Name	Version	Architecture	Installed Time		
xxxx	3.3	install	7503	Package details	Uninstall

Figure 62 - Package Manager Items

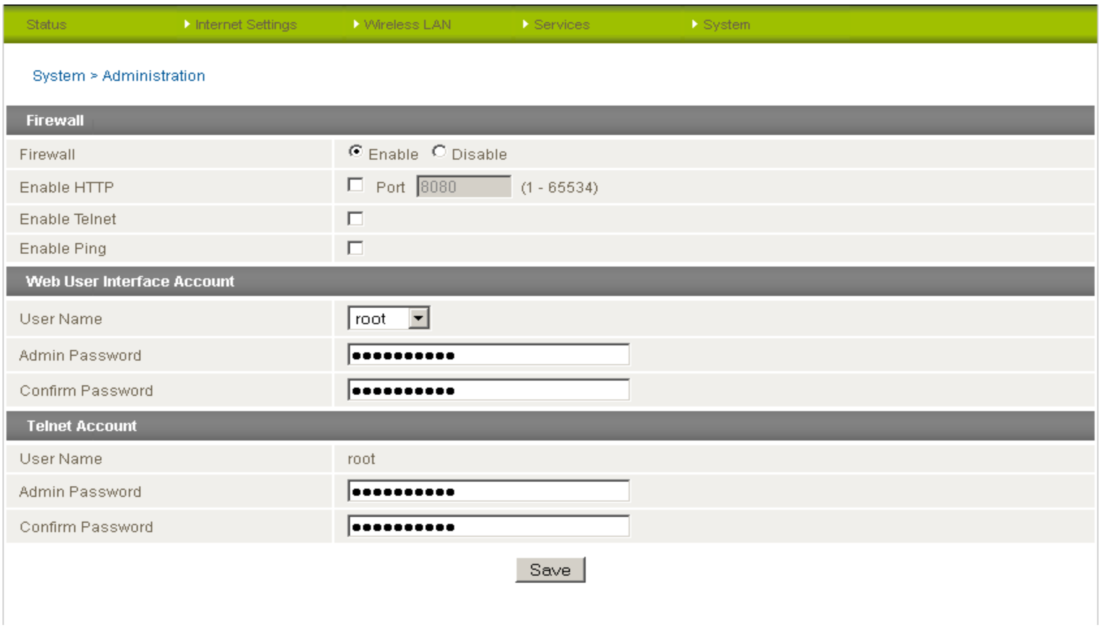
The Package Name, Version, Architecture, Install time are shown and the package content details are available by clicking on the blue “Package Details” link.

Alternatively, if you want to remove a package, click the blue “Uninstall” link.

Please note: For more information on creating software packages for the NTC-40WV, please refer to the SDK document available from the NetComm website.

Administration

The Administration page is used to enable or disable the firewall, remote administration, telnet access and ping responses.



Firewall

Firewall	● Enable ○ Disable
Enable HTTP	□ Port 8080 (1 - 65534)
Enable Telnet	□
Enable Ping	□

Web User Interface Account

User Name	root
Admin Password	●●●●●●●●●●●
Confirm Password	●●●●●●●●●●●

Telnet Account

User Name	root
Admin Password	●●●●●●●●●●●
Confirm Password	●●●●●●●●●●●

Figure 63 - Administration Configuration Items

OPTION	DEFINITION
Firewall	Enable or disable the in-built firewall on the router.
Enable HTTP	Enable or disable remote HTTP access to the router. You can also set the port you would like remote HTTP access to be available on.
Enable Telnet	Enable or disable telnet (command line) access to the router.
Enable Ping	Enable or disable ping responses on the WWAN connection.
Web User Interface Account	
Username	Select the username you would like to change the password for.
Admin Password	Enter the new password for the selected user account.
Confirm Password	Re-enter the new password for the selected user account.
Telnet Account	
Username	Select the telnet account username you would like to change the password for.
Admin Password	Enter the new telnet account password for the selected user account.
Confirm Password	Re-enter the new telnet account password for the selected user account.

Table 34 - Administration Configuration Items

Please note: The password will only be changed if you enter two matching passwords. It is not necessary to change the password if you are only changing the incoming port number.

To access the router's configuration pages remotely from a remote computer, perform the following steps:

1. Open a new browser window (e.g. Internet Explorer, Firefox, Safari ...).
2. In the address bar, enter the router's WAN IP address and assigned port number, e.g. "10.10.10.10: 8080".

Please note: You can find the router's WAN IP address by clicking on the "Status" menu. The Local field in the WWAN section shows the router's WAN IP address.

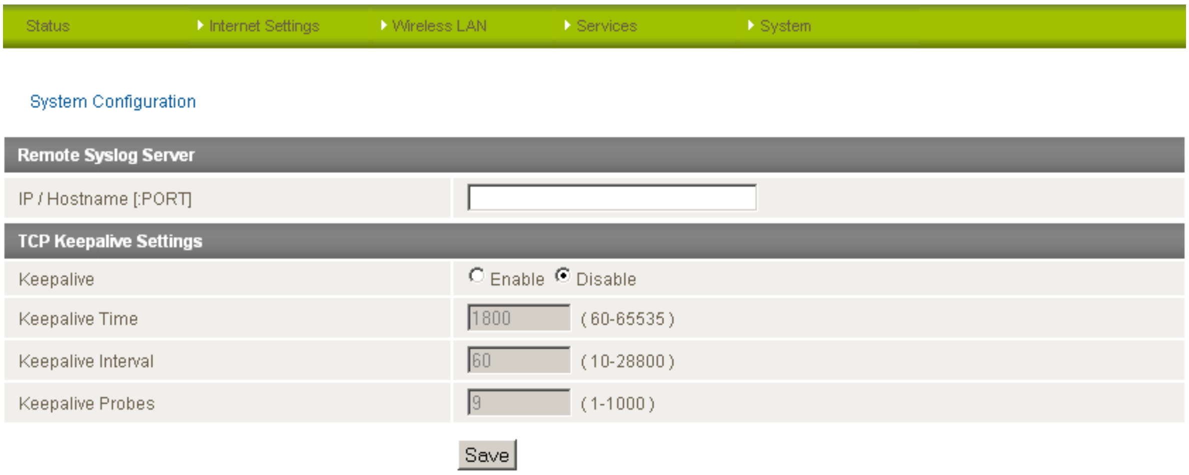
3. Click "Login" and type "admin" or "root" in the Username and "admin" in the Password fields (without quotes). Then click on "Submit".

Please note: To perform functions like Firmware upgrade, device configuration backup and to restore and reset the router to factory defaults, you need to login as the root user.

System Configuration

The System configuration page is used to specify an external syslog server and the TCP Keepalive settings.

TCP Keepalive can be used to ensure the WWAN connection does not disconnect due to inactivity.



System Configuration

Remote Syslog Server	
IP / Hostname [:PORT]	
TCP Keepalive Settings	
Keepalive	○ Enable ● Disable
Keepalive Time	1800 (60-65535)
Keepalive Interval	60 (10-28800)
Keepalive Probes	9 (1-1000)

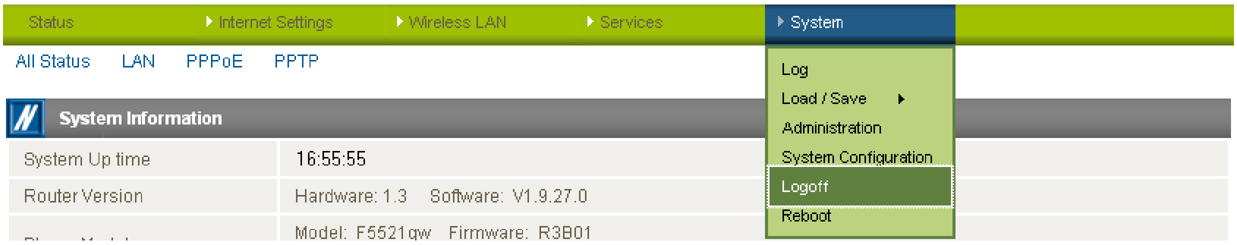
Figure 64 - System Configuration Items

OPTION	DEFINITION
IP / Hostname [:PORT]	The IP address and port of the external syslog server you would like logging information sent to.
Keepalive	Enable or Disable the TCP Keepalive function.
Keepalive Time	The interval between the last packet sent and the first TCP keepalive packet being sent.
Keepalive Interval	The time between subsequent TCP Keepalive packets.
Keepalive Probes	The number of TCP Keepalive packets to send.

Table 35 - System Configuration Items

Logoff

The logoff item will log you out of your web configuration session.



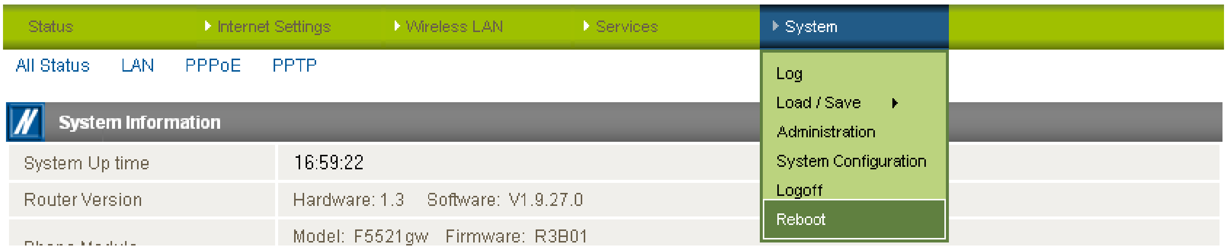
System Information

System Up time	16:55:55
Router Version	Hardware: 1.3 Software: V1.9.27.0
	Model: F5521gw Firmware: R3B01

Figure 65 - Logoff

Reboot

The reboot item will reboot the router. This can be useful if you have made configuration changes you want to implement or want to reboot the router.



System Information

System Up time	16:59:22
Router Version	Hardware: 1.3 Software: V1.9.27.0
	Model: F5521gw Firmware: R3B01

Figure 66 - Reboot Router

Technical Data

The following table lists the hardware specifications of the NTC-40WV.

MODEL	NETCOMM NTC-40WV
CPU	Atmel AT91SAM9G45 Microcontroller (ARM9)
Modem Module/Chipset	Sierra MC8704 / Qualcomm MDM8200A
Wireless LAN Chipset	IEEE 802.11b/g/n, up to 16 concurrent users
Memory	RAM: 64MB DRAM Storage: 256MB Flash
Operating System	Embedded Linux 2.6
UMTS bands	Quad-Band: 850/900/1900/2100Mhz
GSM bands	Quad-Band: 850/900/1800/1900Mhz
Maximum Data Throughput / 3G Radio interface	Downlink: 21 Mbps (HSPA Evolution); EDGE/GPRS 247Kbps); Uplink: Uplink: 5.76 Mbps (HSPA Evolution); EDGE/GPRS 247Kbps
Wireless Frequency	2.4 ~ 2.438Ghz
Peak Data Rate (Wireless)	300 Mbps (MIMO)
Wireless Security	WEP 64-bit, WEP 128-bit, WPA, WPA-PSK, WPA2-PSK, Mixed WPA-PSK/WPA2-PSK, TKIP, AES
Connectivity	1x Fast Ethernet 10/100Base-TX w/ Auto MDIX 1x Mini USB 2.0 Console Port 1x Voice port (RJ-11)
SIM Card Reader	1 x Lockable SIM Card Tray Reader, Push to Release
Antenna connectors	Cellular: 2 x detachable SMA (MIMO) WLAN: 2 x detachable Reverse SMA (MIMO)
LED Indicators	One power supply indicator One Cellular network type detected Indicator One Tx/Rx Data Transmit Indicator One Carrier Detect indicator One Received Signal Strength indiator
Operating Temperature	Platform: -20˚C to +85˚C Module: -20˚C to +60˚C (Normal Operating Temperature)
Power input	DC-in Port: 8 ~ 28V AC/DC Power Adapter: 100-240V AC to 12V DC/1.5A
Power Consumption	Standby Input Current: 110mA @ 12V DC 3G Active Current: 300mA @ 12V DC Maximum Input Current: 560mA @ 12V DC

Table 36 - Technical Specifications for the NTC-40WV

RJ-45 Connector

The following table lists the pin outs for the RJ-45 Ethernet connector.

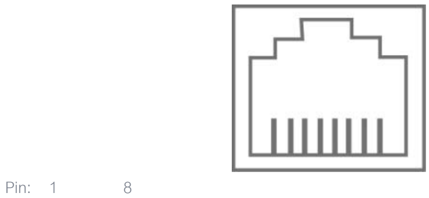


Figure 67 - The RJ-45 Connector

PIN	SIGNAL	DESCRIPTION
1	TX+	Transmit Data+
2	TX-	Transmit Data-
3	RX+	Receive Data+
4	Unused	Unused
5	Unused	Unused
6	RX-	Receive Data-
7	Unused	Unused
8	Unused	Unused

Table 37 - RJ-45 Connector Pin Outs

Captive Power Terminal Block

The following table displays the pin outs for the Locking Power Block on the DC adapter.

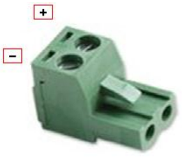


Figure 68 - Locking Power Terminal Block

PIN	SIGNAL	DESCRIPTION
+	V+	Voltage+
-	V-	Voltage-

Table 38 - Locking Power Block Pin Outs

Electrical Specifications

The NTC-40WV is capable of operating over a wide range of input voltages from 8 ~ 28V.

It is recommended that the NTC-40WV be powered using the supplied DC-in power supply.

Environmental Specifications / Tolerances

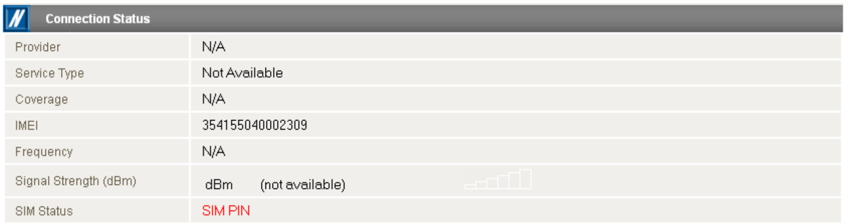
The industrial enclosure of the NTC-40WV makes it able to operate over a wide variety of temperatures from -10˚C to +65˚C.

Additional Product Information

Unlocking the SIM

If the SIM card is locked you will need to unlock it with the appropriate PIN code.

You can find out if the SIM is locked by viewing the SIM Status at the bottom of the Status page.

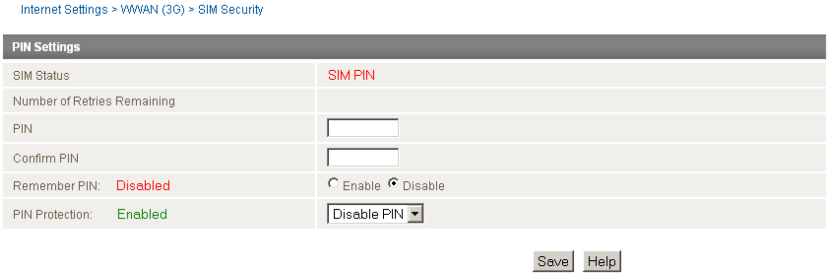


Connection Status	
Provider	N/A
Service Type	Not Available
Coverage	N/A
IMEI	354155040002309
Frequency	N/A
Signal Strength (dBm)	dBm (not available)
SIM Status	SIM PIN

Figure 69 - Checking the SIM PIN Status

If the SIM Status is "SIM PIN" as above then do the following:

d) Click on the "Internet Settings" menu at the top of the page and then the "SIM Security" item from the WWAN (3G) menu item on the right.



Internet Settings > WWAN (3G) > SIM Security

PIN Settings	
SIM Status	SIM PIN
Number of Retries Remaining	
PIN	
Confirm PIN	
Remember PIN: Disabled	○ Enable ● Disable
PIN Protection: Enabled	Disable PIN ▾

Figure 70 - Entering the SIM PIN

e) Enter the PIN code in the "PIN" field and then enter it again in the "Confirm PIN" field to confirm the PIN code.

Please note: You can also select to "Remember PIN" so that entering the PIN code each time the SIM is inserted is not required. Alternatively you can also disable SIM PIN protection by selecting to "Disable PIN" from the "PIN Protection" drop down menu.

f) Click the "Save" button to save any changes to the settings.

Using the NTC-40WV to make and receive telephone calls

The NTC-40WV provides circuit switched voice services via a telephony line interface offering the ability to make and receive telephone calls via a regular analogue telephone using the 3G mobile network.

Please note: Please refer to your mobile service provider for activation of your voice service and information about the call charges that apply.

Handset requirements

The NTC-40WV allows you to make telephone calls over the 3G network using a standard analogue telephone via the built in RJ-11 Phone port. Please refer to the documentation provided by the manufacturer of your analogue telephone for assistance with the operation of your telephone handset.

Maximum REN Loading

Please note that each of the line interfaces on the NTC-40WV is capable of supporting multiple analogue telephones connected via splitters. The ringer equivalence number (REN) for each line is 5. Therefore, a maximum of 5 handsets each with a REN number of 1 can be connected to each line port.

Before you start making any phone calls, make sure you have checked the following:

1. You have an activated 3G SIM card inserted prior to powering on the NTC-40WV.
2. Your NTC-40WV is powered on and in running condition.
3. A working analogue telephone connected into the Line port.
4. You hear the dial tone after lifting the handset.

How to place a call

To make a call, simply lift the handset and dial the number following the instructions provided by your telephone handset manufacturer.

How to receive a call

When an incoming call is received, the phone connected to the NTC-40WV will ring. Answer the telephone following the instructions provided by your telephone handset manufacturer to conduct the call.

If there is no phone connected to the NTC-40WV, all incoming calls will be transferred to Voicemail (if enabled on the device).

Answering an incoming call when on a call

Call waiting enables a 2nd incoming call to be received while you are on a call. To answer a call waiting call, perform a hook-flash (clicking “flash” button, or briefly depressing the hook button) and then click button 2. The incoming call should then be answered. Upon performing another hook-flash, waiting for 2 seconds and then clicking button 2, you will be returned to the original telephone call.

Accessing voicemail

To access your voicemail, please dial *98 and follow the voice prompts.

Call feature codes

Quick Reference Table

The NTC-40WV supports a number of call feature codes for supplementary services.

FEATURE	ACTIVATION	DEACTIVATION	STATUS
Caller ID	#31# (to unblock caller ID for outgoing calls)	*31# (to block caller ID for outgoing calls)	*#31#
Call Waiting	*43#	#43#	*#43#
Call Forwarding Unconditional	*21*<Directory Number>#	#21#	*#21#
Call Forwarding No Answer	*61*<Directory Number>#	#61#	*#61#
Call Forwarding Busy	*24*<Directory Number>#	#24#	*#24#
Call Forwarding Unreachable	*62*<Directory Number>#	#62#	*#62#

Table 39 - Additional Product Information - Call Feature Codes Quick Reference

Caller ID

Caller ID transmits a caller's number to the called party's telephone equipment when the call is being set up but before the call is answered. Where available, caller ID can also provide a name associated with the calling telephone number.

- To force Caller ID to be blocked for an outbound call, dial *31#, and hang up after you hear 2 low pitch beeps.
- To force Caller ID to be unblocked for an outbound call, dial #31#, and hang up after you hear 2 high pitch beeps.
- To check the status of Call Waiting, dial *#31#.
  - Caller ID is blocked if you hear 2 low pitch beeps.
  - Caller ID is unblocked if you hear 2 high pitch beeps.

Caller ID Test Steps

1. Dial *31#. Hang up and then out-call a mobile phone. The router phone's number should be blocked;
2. Dial #31#. Hang up and then out-call a mobile phone. The router phone's number should be shown.

Call Waiting

Call waiting allows for indication and answering of an incoming telephone whilst an existing call is underway.

- To disable call waiting, dial #43#, and hang up after you hear 2 high pitch beeps.
- To enable call waiting, dial *43#, and hang up after you hear 2 low pitch beeps.
- To check the status of Call Waiting, dial *#43# or view the advanced status page of the management console.
  - Call waiting is disabled if you hear 2 high pitch beeps.
  - Call waiting is enabled if you hear 2 low pitch beeps.

Call Forwarding

Call forwarding (or call diverting), is a features that allow an incoming call to be redirected to another number depending on the circumstances at the time of receiving the call.

Please note: Please note: Of the four Call forwarding features, the Unconditional feature has the highest priority. Once Call Forwarding Unconditional is enabled, Call Forwarding No Answer, Call Forwarding Busy and Call Forwarding Unreachable are disabled.

.

Call Forwarding Unconditional

Call forwarding Unconditional will divert all incoming calls to a phone number that you desire.

- To enable Call Forwarding Unconditional, dial *21*<Directory Number>#
  (Where directory number is the number you wish to forward calls to)
- Hang up after you hear 2 low pitch beeps.
- To disable Call Forwarding Unconditional, dial #21#
- Hang up after you hear 2 high pitch beeps.

- To check the status of Call Forwarding Unconditional, dial *#21# or view the advanced status page of the management console.
    - Call Forwarding Unconditional is disabled if you hear 2 high pitch beeps.
    - Call Forwarding Unconditional is enabled if you hear 2 low pitch beeps.

Call Forwarding No Answer

Call forwarding No Answer will divert all incoming calls to a phone number that you desire only if the incoming call is not answered.

- To enable Call Forwarding No Answer, dial *61*<Directory Number>#

  (Where directory number is the number you wish to forward calls to)
- Hang up after you hear 2 low pitch beeps.
- To disable Call Forwarding No Answer, dial #61#
- Hang up after you hear 2 high pitch beeps.

To check the status of Call Forwarding No Answer, dial *#61# or view the advanced status page of the management console. Call Forwarding No Answer is disabled if you hear 2 high pitch beeps. Call Forwarding No Answer is enabled if you hear 2 low pitch beeps.

Call Forwarding Busy

Call forwarding busy will divert all incoming calls to a phone number that you desire only if your telephone is busy on another call.

To enable Call Forwarding Busy, dial *24*<Directory Number>#

(Where directory number is the number you wish to forward calls to)

- Hang up after you hear 2 low pitch beeps.
- To disable Call Forwarding Busy, dial #24#
- Hang up after you hear 2 high pitch beeps.
- To check the status of Call Forwarding Busy, dial *#24# or view the advanced status page of the management console.
  - Call Forwarding Busy is disabled if you hear 2 high pitch beeps.
  - Call Forwarding Busy is enabled if you hear 2 low pitch beeps.

Call Forwarding Not Reachable

Call forwarding not reachable will divert all incoming calls to a phone number that you desire only if your telephone is unreachable by the network.

- To enable Call Forwarding Not Reachable dial *62*<Directory Number>#

  (Where directory number is the number you wish to forward calls to)
- Hang up after you hear 2 low pitch beeps.
- To disable Call Forwarding Not Reachable, dial #62#, Hang up after you hear 2 high pitch beeps.
- To check the status of Call Forwarding Not Reachable, dial *#62# or view the advanced status page of the management console.
  - Call Forwarding No Answer is disabled if you hear 2 high pitch beeps.
  - Call Forwarding No Answer is enabled if you hear 2 low pitch beeps.

Conference Call

This can be achieved by performing the following:

1. From the phone connected to the router, make a call to the 1st phone. Afterward perform a hook-flash (click “flash” button, or briefly depressing the hook button) to put the 1st call on hold.
2. Call the 2nd phone number. After the 2nd phone picks up the call, place both calls into one conference call by performing another hook-flash and then pressing button 3.
3. To terminate the conference call hang up the phone connected to the router.

Voice Troubleshooting

What do I do if I have no dial tone?

Please follow the procedure listed below:

1. Check to make sure the phone is plugged into your NTC-40WV on the RJ-11 port (between the power socket and the LAN port).
2. Check to make sure you are using the correct cable (Cat-3 UTP Telephone Cable with RJ-11 plugs).
3. Check to make sure the “SIM status” shows “SIM OK” on the Status page of the Web interface.
4. Check to make sure your 3G SIM card is activated and insert into your NTC-40WV properly.
5. Check and see if you get the dial tone after rebooting your NTC-40WV.

I have noise interference during telephone calls. How can I fix this?

To resolve this issue, try the following:

1. Verify that the RJ-11 cable is securely connected and not damaged.
2. Try to remove any telephone splitters from the connection between your phone and theNTC-40WV.
3. Try rebooting your NTC-40WV.

List of Mobile Broadband Service Provider APNs

MOBILE SERVICE	APN
Australia	
Telstra	Telstra.internet
	Telstra.extranet
Optus – Postpaid	connect
Optus – Prepaid	preconnect
Three – Postpaid	3netaccess
Three – Prepaid	3services
Vodafone – Postpaid	vfinternet.au
Vodafone – Prepaid	vfprepaymbb
Crazy John's	purtona.net
DoDo	dodolns1
Blink	splns888a1
Internode	Internode
Primus	primuslns1
TPG	internet
Exetel	Exetel1
Westnet	Splns555a1
iiNet	iiNet
New Zealand	
Vodafone NZ	www.vodafone.net.nz
CallPlus	www.callplus.net.nz
Slingshot	www.slingshot.net.nz
Telstra Clear	www.telstraclear.net.nz
Telecom NZ XT	wap.telecom.co.nz
2 Degrees	internet

Table 40 - List of Mobile Broadband Service Provider APNs

Appendix A: Tables

Legal and Regulatory

1. Intellectual Property Rights

All intellectual property rights (including copyright and trade mark rights) subsisting in, relating to or arising out this Manual are owned by and vest in NetComm Wireless (ACN 002490486) (**NetComm**) (or its licensors). This Manual does not transfer any right, title or interest in NetComm's (or its licensors') intellectual property rights to you.

You are permitted to use this Manual for the sole purpose of using the NetComm Wireless product to which it relates. Otherwise no part of this Manual may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Wireless.

NetComm and NetComm Wireless is a trademark of NetComm Wireless Limited. All other trademarks are acknowledged to be the property of their respective owners.

2. Customer Information

The Australian Communications & Media Authority (**ACMA**) requires you to be aware of the following information and warnings:

1. This unit may be connected to the Telecommunication Network through a line cord which meets the requirements of the AS/CA S008-2011 Standard.
2. This equipment incorporates a radio transmitting device, in normal use a separation distance of 20cm will ensure radio frequency exposure levels complies with Australian and New Zealand standards.
3. This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACMA. These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:
    - Change the direction or relocate the receiving antenna.
    - Increase the separation between this equipment and the receiver.
    - Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
    - Consult an experienced radio/TV technician for help.
4. The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm Wireless. Failure to do so may cause damage to this product, fire or result in personal injury.

3. Consumer Protection Laws

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

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

4. Product Warranty

All NetComm products have a standard one (1) year warranty from date of purchase, however, some products have an extended warranty option (refer to packaging and the warranty card) (each a **Product Warranty**). To be eligible for the extended warranty option you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering online via the NetComm web site at www.netcomm-commercial.com.au. For all Product Warranty claims you will require proof of purchase. All Product Warranties are in addition to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Section 3 above).

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Section 3 above), the Product Warranty is granted on the following conditions:

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

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Section 3 above), the Product Warranty is automatically voided if:

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

5. Limitation of Liability

This clause does not apply to New Zealand consumers.

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Section 3 above), NetComm accepts no liability or responsibility, for consequences arising from the use of this product. NetComm reserves the right to change the specifications and operating details of this product without notice.

If any law implies a guarantee, condition or warranty in respect of goods or services supplied, and NetComm's liability for breach of that condition or warranty may not be excluded but may be limited, then subject to your rights and remedies under any applicable Consumer Protection Laws which cannot be excluded, NetComm's liability for any breach of that guarantee, condition or warranty is limited to: (i) in the case of a supply of goods, NetComm doing any one or more of the following: replacing the goods or supplying equivalent goods; repairing the goods; paying the cost of replacing the goods or of acquiring equivalent goods; or paying the cost of having the goods repaired; or (ii) in the case of a supply of services, NetComm doing either or both of the following: supplying the services again; or paying the cost of having the services supplied again.

To the extent NetComm is unable to limit its liability as set out above, NetComm limits its liability to the extent such liability is lawfully able to be limited.

6. Warning Statement

FCC Regulations:

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

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

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

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

RF Exposure Information

This device meets the government’s requirements for exposure to radio waves.

This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government.

●This device complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

IC Regulations:

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) this device may not cause interference, and

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

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement."

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

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

IC Radiation Exposure Statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled

environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

The County Code Selection feature is disabled for products marketed in the US/Canada.

For product available in the USA/ Canada markets, only channel 1~11 can be operated. Selection of other channels is not possible.

Contact

Address: NETCOMM WIRELESS 18-20 Orion Road, Lane Cove NSW 2066 Sydney, Australia

ABN: 85 002 490 486

Website: www.netcomm-commercial.com.au

Phone: +61(0)2 9424 2070

Fax: +61(0)2 9424 2010

Email: sales@netcomm.com.au, techsupport@netcomm.com.au