

HSPA+ M2M WiFi Router with Voice



USER GUIDE

Copyright

Copyright© 2012 NetComm Wireless Limited. All rights reserved.

The information contained herein is proprietary to NetComm Wireless. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NetComm Wireless.



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 Wireless NTC-40WV

DOCUMENT VERSION	DATE
1.0- Initial document release	05/12/2011
2.0- Revised	20/11/2012

Table 1 - Document Revision History

Table of Contents

Overview	4
Product Introduction	5
Product Overview	5
Package Contents	5
Product Features	6
Physical Dimensions and Indicators	7
LED Indicators	7
Physical Dimensions	8
Interfaces	10
NTC-40WV Default Settings	11
Restore Factory Default Settings	12
Implementation and Deployment Scenario	13
Installation and Configuration of the NTC-40WV	14
Connecting via an Ethernet cable	14
Connecting via wireless	14
Configuring the NTC-40WV	14
Web based User Interface	15
Status	16
Advanced Status	19
Internet Settings	21
Mobile Broadband	21
LAN	27
Routing	30
VPN	35
Wireless Settings	45
Configuration	45
Advanced	53
MAC Filtering	54
Station List	55
Services	56
Dynamic DNS	56
NTP	56
System Monitor	57
SNMP	58
SMS	59
Auto Dial	69
System	70
Log	70
Load / Save	71
Administration	75
System Configuration	76
Logoff	77
Reboot	78
Technical Data	79
RJ-45 Connector	80
Captive Power Terminal Block	80
Additional Product Information	81
Using the NTC-40WV to make and receive telephone calls	81
Handset requirements	81
Maximum REN Loading	81
How to place a call	81
How to receive a call	81
Answering an incoming call when on a call	81
Accessing voicemail	81
Call feature codes	82
List of Mobile Broadband Service Provider APNs	85
Appendix A: Tables	86
Legal and Regulatory	87

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 Router, 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, 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



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.
- Embedded NetComm Linux OS and Software Development Kit (SDK).
- Remote diagnostics, configuration and firmware upgrade capabilities.
- Supports PPPoE, RIP, VRRP, Dynamic DNS, MAC /NET address filtering, Open VPN, DHCP/DHCP relay.
- Management and configuration via web user interface, SNMP or SMS.

Package Contents

The NTC-40WW package consists of:

- NetComm Wireless NTC-40 - 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 Wireless Support immediately by visiting the NetComm Wireless Support website at: <http://support.netcommwireless.com>

Product Features

The NTC-40WV is a robust 3G (HSPA+) router 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 mobile broadband module and delivers download speeds of up to 21Mbps which is then transmitted via Ethernet to a WiFi router inside the property.

Utilising a NetComm Wireless M2M router allows customers to significantly reduce the cost of 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 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

Below is a list of 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-40 to a pole or to provide a wall / ceiling mount.

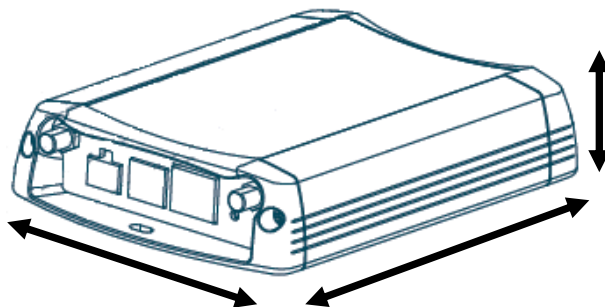


Figure 2 – NTC-40WV Dimensions

NTC-40WV (WITHOUT ANTENNAS ATTACHED)	
Length	155 mm
Depth	104 mm
Height	30 mm
Weight	330 g

Table 3 - Device Dimensions

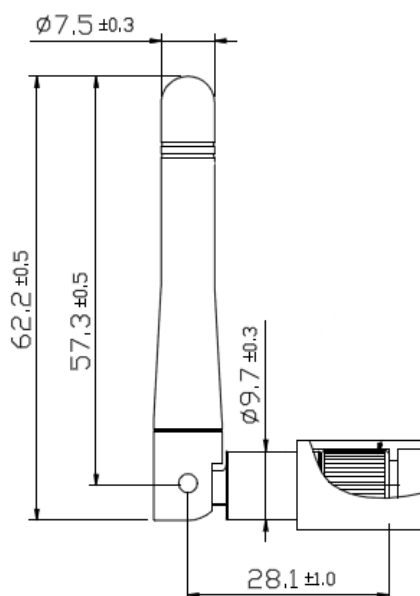


Figure 3 - NTC-40WV 2.4GHz WiFi Antenna

2.4GHZ WIFI ANTENNAS	
Length	32mm (when folded up at 90 degrees as per diagram)
Depth	10mm
Height	62mm

Table 4- 2.4GHz WiFi Antenna Dimensions

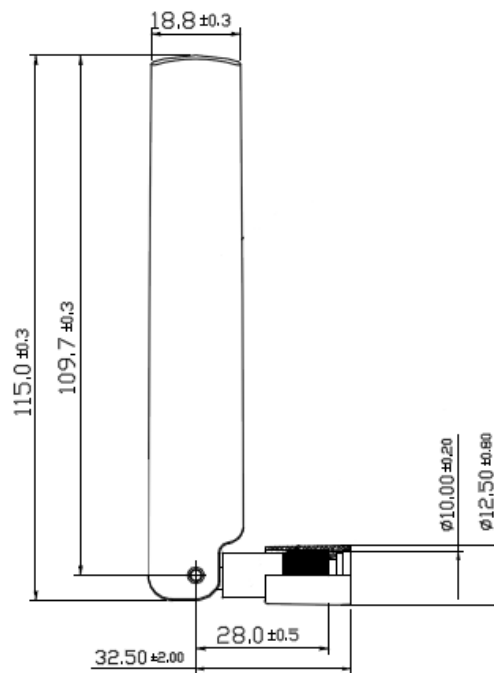


Figure 4 - 3G Antenna

3G ANTENNAS	
Length	35mm (when folded up at 90 degrees as per diagram)
Depth	13mm
Height	115mm

Table 5 - 3G Antenna Dimensions

Interfaces

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

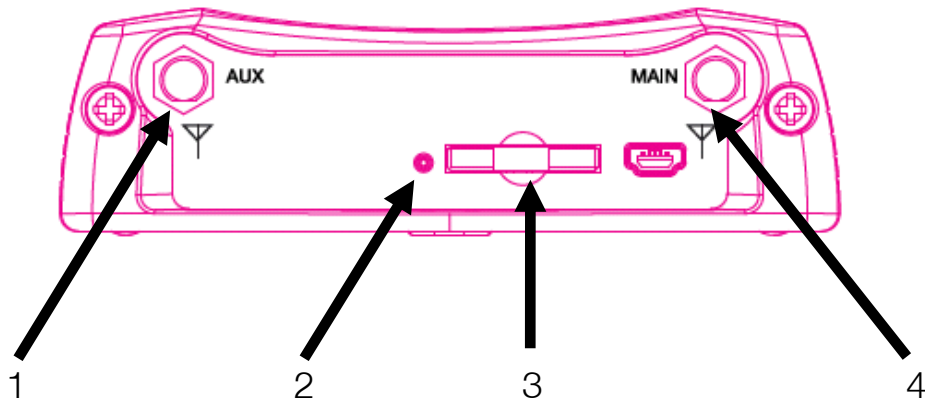


Figure 5 - Bottom Mounted interfaces

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	Main 3G Antenna	Connect one of the 3G antennas here.

Table 6 - Bottom Mounted interfaces

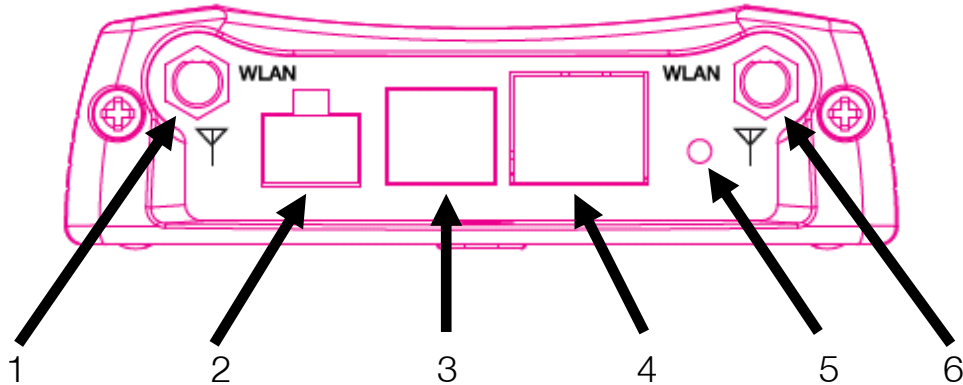


Figure 6 - Top Mounted Interfaces

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 7 - Top Mounted 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 8 - LAN Management Default Settings

WIRELESS (WIFI)	
SSID:	NetComm 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 9 - WiFi Default Settings



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

ADMIN MANAGER ACCOUNT		ROOT MANAGER ACCOUNT	
Username:	admin	Username:	root
Password:	admin	Password:	admin

Table 10 - Web Interface Default Settings



The admin manager account allows users to manage all settings of the router except functions such as Firmware Upgrade, Mobile Broadband Connection Settings, Device Configuration Backup and Restore and Reset to Factory Default Settings, which are privileged only to the Root manager account.

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

Table 11 - Telnet Access

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 are asked to perform a factory reset by support staff.

There are two methods you can use to restore factory default settings on your NTC-40WV:

- Using the web-based user interface
- Using the reset button on the interface panel of the router

Using the web-based user interface

In order to restore your router to its factory default settings, please follow these steps:

1. Ensure that your NTC-40WV router is powered on (for at least 10 seconds);
2. Use a paper clip or a pencil tip to depress the reset button for ten seconds and release. At this point, the reset is in progress. Do not power off the unit.
3. Logon to the default web interface page at <http://192.168.1.1> using `root` as the User Name and `admin` as the password. You will be re-directed into the gateway recovery mode. Select the **System** menu option and then click **Load/Save**. Press the Restore button to complete the factory reset.
4. 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.

Using the reset button on the interface panel of the router

Use a pen to depress the Reset button on the device for 10 seconds. The router will restore the factory default settings and reboot.

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 NTC-40WV HSPA+ M2M WiFi Router 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 of 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 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.

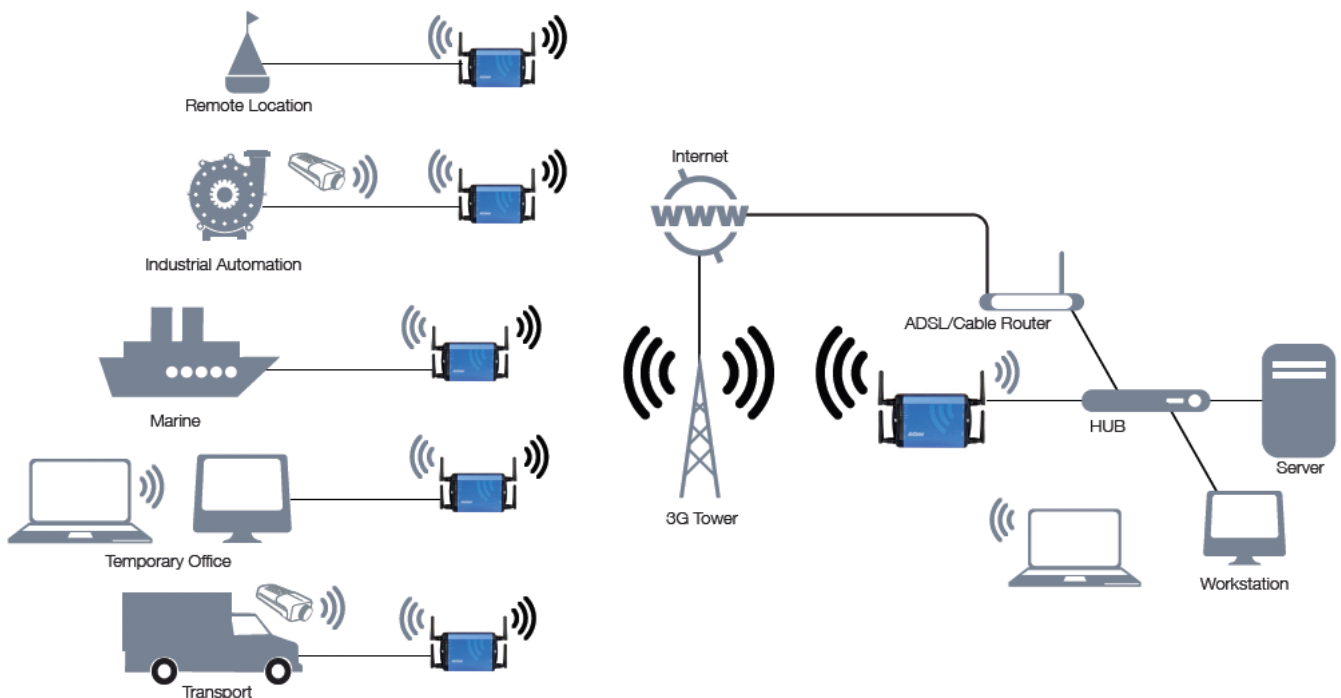


Figure 7 - Typical NTC-40WV Deployment

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.

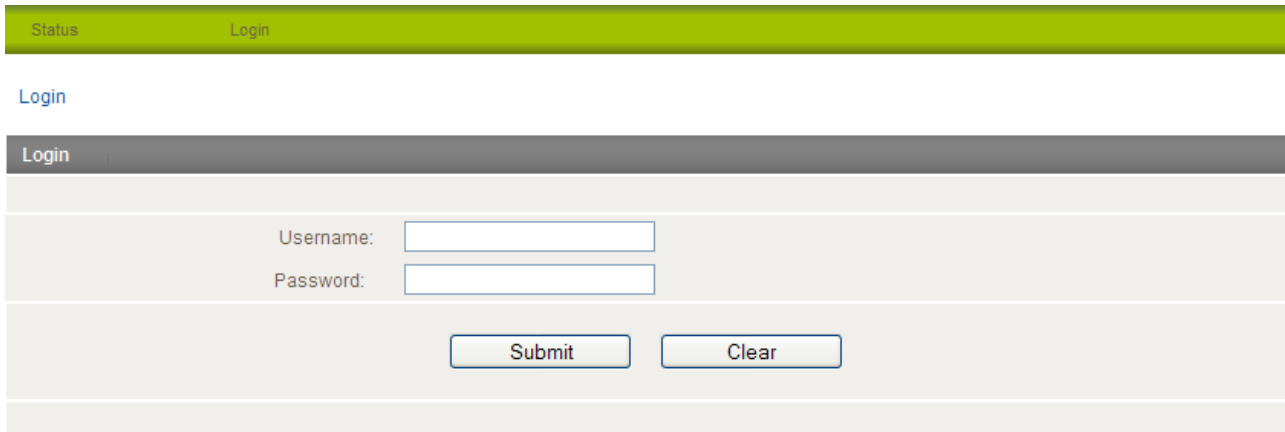
Configuring the NTC-40WV

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 and click the “Submit” button. For the first time set up please log on with username “root” and password “admin” for accessing mobile broadband configuration.



The screenshot shows the login interface of the NetCommWireless management console. At the top, there is a green navigation bar with 'Status' and 'Login' links. Below this, the 'Login' section is highlighted with a dark grey header. The main area contains a form with two input fields labeled 'Username:' and 'Password:'. At the bottom of the form are two buttons: 'Submit' and 'Clear'.

Figure 8 - 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.

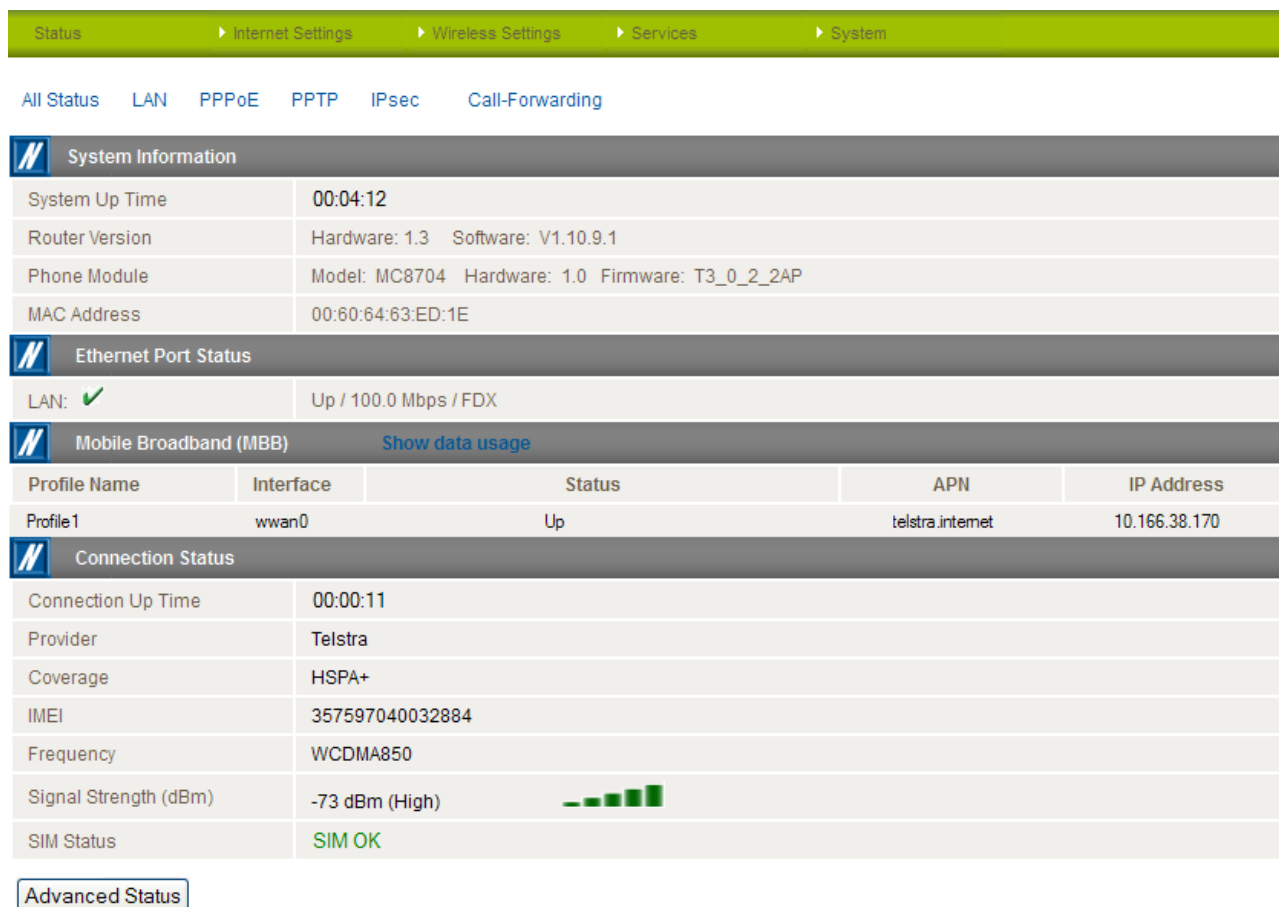


Figure 9 - The Status Page

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 12 - 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	192.168.20.1 / 255.255.255.0
MAC Address	00:60:64:63:ED:1E

Figure 10 - 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 13 - Status Page - LAN Details

PPPoE	
PPPoE Status	DISABLED
PPPoE IP Address	N/A

Figure 11 - 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 14 - Status Page - PPPoE Details

PPTP					
No.	Profile Name	Remote Server Address	P-t-P Local	P-t-P Remote	Status

Figure 12 - 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 15 - Status Page - PPTP Details

IPSec						
No.	Profile Name	Interface	Local LAN	Remote Gateway	Remote LAN	Status

Figure 13 - Status Page - IPSec Details

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 16: Status Page - IPSec Details

Call Forwarding Status	
Call Waiting	Disabled
Unconditional Call Forwarding	Disabled
Busy Call Forwarding	Enabled (+61101)
No-Reply Call Forwarding	Enabled (+61101)
Not Reachable Call Forwarding	Enabled (+61101)

Figure 14 - Status Page - Call Forwarding Status Details



Note: The Call Forwarding Status section is only available if the Voice Call Function is enabled.

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 17: 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-40WW status page. The Advanced Status page shows information regarding the on-board 3G module as well as statistics of the current 3G connection.

Status

Internet Settings

Wireless Settings

Services

System

Status > Advanced Status

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 PRIID	Revision: 1.2 PRI Part Number: 9900984
System Up Time	04:45:20

Connection Status

Provider	Telstra
Country Code	505
Network Code	1
Coverage	HSPA+
Connection Status	Up
IMEI	357597040032884
Frequency	WCDMA850
Signal Strength	-71 dBm
Signal Quality (Ec/Io)	-16 dB
Received Signal Code Power (RSCP)	-74 dB
HSUPA Category	6
HSDPA Category	14
SIM ICCID	89610191498543000007
Primary Scrambling Code (PSC)	96
Location Area Code (LAC)	337
Routing Area Code (RAC)	0
IMSI	50501505013473874378
Cell ID	19793
Channel Number (UARFCN)	4436
MSISDN	N/A

Figure 15: 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.
MSISDN	The Mobile Subscriber ISDN Number uniquely identifying a subscription in a GSM or a UMTS mobile network.

Table 18: 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.

Status ▶ Internet Settings ▶ Wireless Settings ▶ Services ▶ System

[Internet Settings](#) > [Mobile Broadband](#) > [Connection](#)

Mobile Broadband Profile Settings	
Profile Name	<div>Profile1 ▼</div> <input type="checkbox"/> Automatically configure my mobile broadband
APN Name	<input type="text"/>
Mobile Broadband Connection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="text"/>
Authentication Type	<input checked="" type="radio"/> CHAP <input type="radio"/> PAP
Reconnect Delay	<input type="text" value="30"/> (30-65535) secs
Reconnect Retries	<input type="text" value="0"/> (1-65535, 0=Unlimited)
Metric	<input type="text" value="20"/> (1-65535)
MTU	<input type="text" value="1400"/> (1400-1430)
NAT Masquerading	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

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

Figure 16 - Connection Settings

To connect using a Connection profile

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 “Automatically configure my mobile broadband” option is selected. This automatically detects the most appropriate APN from the inserted SIM by querying a database on the router.

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

1. Remove the check from the “Automatically configure my mobile broadband” box
2. Select the profile that you wish to configure from the “Profile Name” drop down list.
3. Enter the APN Name (Access Point Name) and if required, the username and password.
4. Select Enable for the “Mobile Broadband Connection” option. If there is already another profile enabled you will need to select that profile first and disable it since only one profile can be used at a time.
5. Select the Authentication Type.
6. Enter the Reconnect Delay (if needed - the default should be suitable in most cases).
7. Enter the number of Reconnection attempts the router should make.
8. Enter the network metric for the connection.
9. Select to enable or disable NAT Masquerading for the connection.
10. Click Save.

To confirm successful connection

Click on the Status menu item at the top of the page to return to the Status page.

If the Mobile Broadband connection has been established successfully, the WWAN status will be “Up”. The IP Address field shows the current IP address that the network has allocated for the router. The mobile broadband internet connection is now ready to use.

Restoring the Automatic Configuration option after manually configuring an APN profile

When you have manually configured an APN and want to have the router automatically configure your broadband connection again, you must first set “Mobile Broadband Connection” to Disable for that profile and then remove the APN Name from the “APN Name” field and click “Save”. This is because the router saves the manually configured APN profile in flash memory and will always try to connect to that APN first regardless of whether “Automatically configure my mobile broadband” is enabled.

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..

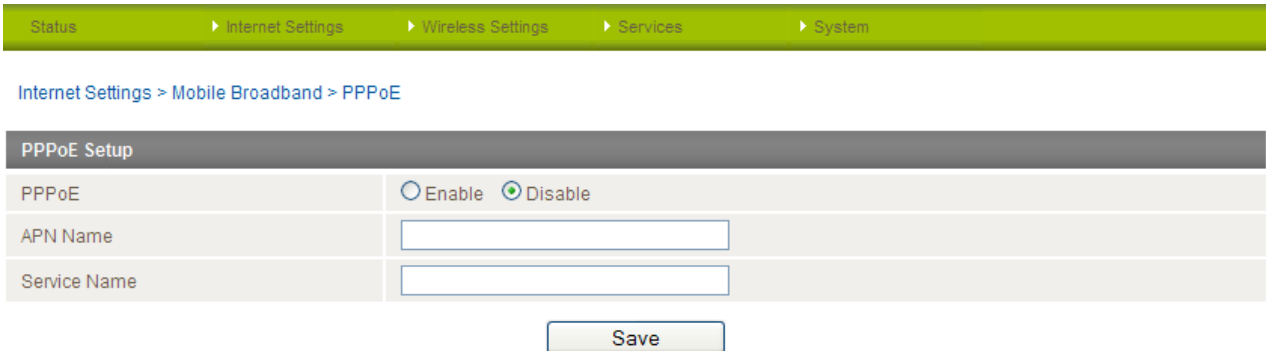


Figure 17 - PPPoE Settings

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.

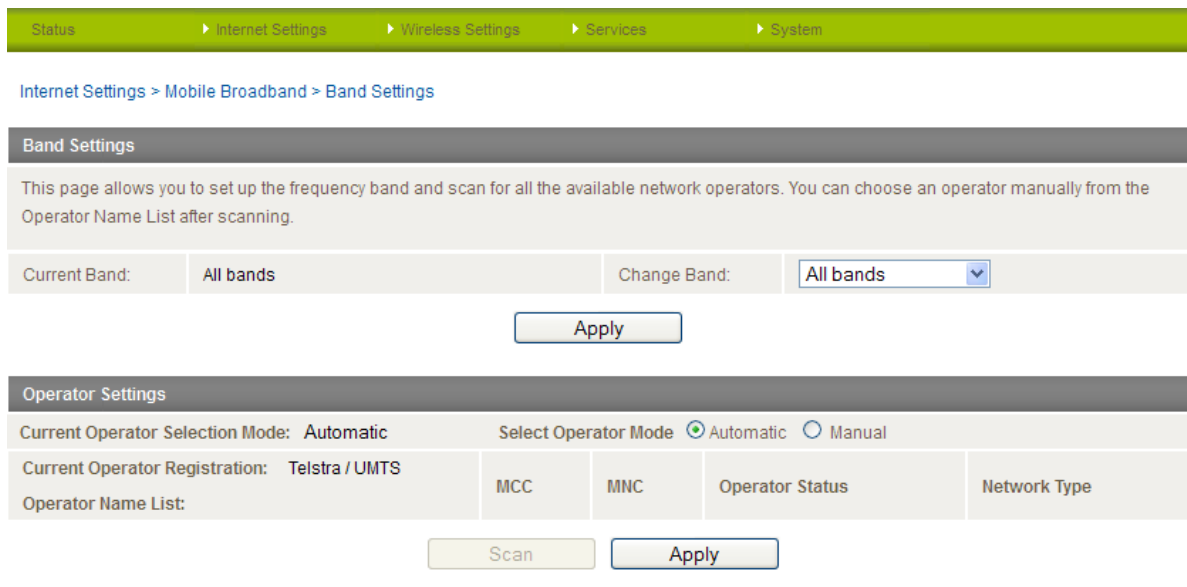


Figure 18 - Band / Operator Selection

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.

Select a band from the "Change Band:" drop down list.

The following band settings options are available:

- WCDMA 900/2100
- WCDMA ALL
- GSM ALL
- GSM 900/1800
- All Bands

It is not necessary to change the default setting of "All bands" in most cases. When "All bands" is selected, the router attempts to find the most suitable band based on the inserted SIM card.

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.

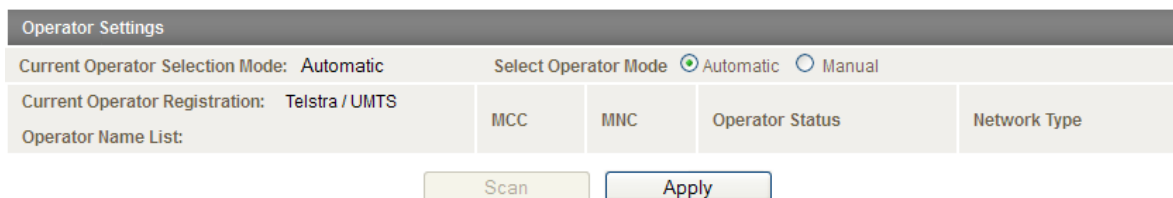


Figure 19 - Manual Operator Selection

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 "Automatic" option is sufficient for most users. It will choose the most appropriate operator based on the inserted SIM card.

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	<input type="text"/>
Confirm PIN	<input type="text"/>
Remember PIN: Disabled	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
PIN Protection: Enabled	Enable PIN <input type="button" value="v"/>

Figure 20 - 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	
Connection Up Time	00:00:00
Provider	Limited Service
IMEI	357597040032884
Frequency	WCDMA850
Signal Strength (dBm)	-69 dBm (High) 
SIM Status	SIM PIN Locked

Figure 21 - SIM Security - Status Page Warning

If the SIM Status is “SIM PIN Locked” as above then do the following:

- Click on the “Internet Settings” menu at the top of the page, then “Mobile Broadband” and then “SIM Security”.

[Internet Settings > Mobile Broadband > SIM Security](#)

SIM Security Settings	
SIM Status	SIM PIN Locked
Number of Retries Remaining	3
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>
Remember PIN: Disabled	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
PIN Protection: Enabled	

Figure 22 - SIM Security - SIM PIN Needed

- Enter the PIN code in the “PIN” field and then enter it again in the “Confirm PIN” field to confirm the PIN code.



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.

- Click Save.

Enter PUK

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



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.

[Internet Settings](#) > [Mobile Broadband](#) > [SIM Security](#)

SIM Security Settings	
SIM Status	PUK Locked
Number of Retries Remaining	10
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>
PUK	<input type="text"/>
Confirm PUK	<input type="text"/>
Remember PIN:	Disabled <input type="radio"/> Enable <input checked="" type="radio"/> Disable
PIN Protection:	Enabled

Figure 23 - 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.

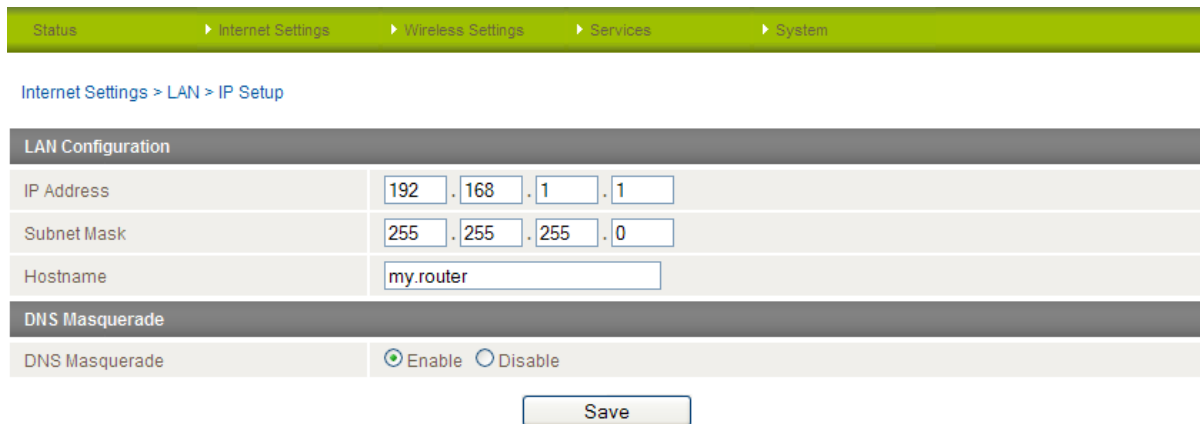


Figure 24 - IP Setup Settings

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”.

Additionally, a hostname can be configured to identify the device on the network.



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.

Status
Internet Settings
Wireless Settings
Services
System

Internet Settings > LAN > DHCP

DHCP Configuration

DHCP	<input checked="" type="radio"/> Enable <input type="radio"/> 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	0 . 0 . 0 . 0
DNS Server 2 IP Address	0 . 0 . 0 . 0
WINS Server 1 IP Address	0 . 0 . 0 . 0
WINS Server 2 IP Address	0 . 0 . 0 . 0
NTP Server (Option 42)	0 . 0 . 0 . 0
TFTP Server (Option 66)	
Option 150	
Option 160	

DHCP Relay Configuration

DHCP Relay	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DHCP Server Address	0 . 0 . 0 . 0

Address Reservation List

Computer Name	MAC Address	IP Address	
			Add

DHCP Client List

Computer Name	MAC Address	IP Address	Expire Time	
pdg26	00:40:f4:ce:fa:1e	192.168.1.190	Friday, 2 January 1970 11:00:47 AM	Clone

Save

Figure 25 - 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	
		0 . 0 . 0 . 0	<input checked="" type="checkbox"/> Enable Remove

Figure 26 - 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

The router can also be configured to act as a DHCP Relay Agent on this page. DHCP Relay is disabled by default.

DHCP Relay Configuration	
DHCP Relay	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DHCP Server Address	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

Figure 27: Internet Settings - LAN - DHCP - DHCP Relay Configuration

To relay the DHCP function from a remote DHCP server:

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.

[Status](#) > [Internet Settings](#) > [Wireless Settings](#) > [Services](#) > [System](#)

[Internet Settings](#) > [Routing](#) > [Static](#)

Static Routes							
Item No.	<input type="text"/> (1-65535) Only required if you want to edit the existing mapping						
Route Name	<input type="text"/>						
Destination IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>						
IP Subnet Mask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>						
Gateway IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>						
Network Interface	<input type="text" value="Auto"/> ▼						
Metric	<input type="text"/> (1-65535)						
<input type="button" value="Add"/>							
Item	Route Name	Destination IP Address	Subnet Mask	Gateway IP Address	Network Interface	Metric	
1	My Route	192.168.1.103	255.255.255.0	192.168.1.1	auto	1	Delete Entry

Active Routing Table								
Item	Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Interface
1	192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
2	0.0.0.0	10.167.35.141	0.0.0.0	UG	20	0	0	wwan0

Figure 28 - 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.

 Note: You must increment the "Route no" by 1 for each route in the "Route no" field otherwise that route will be overwritten.

The new static route will be displayed at the bottom of the Static Routes section.

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.



Note: Some routers will ignore RIP.

[Status](#) ▶ [Internet Settings](#) ▶ [Wireless Settings](#) ▶ [Services](#) ▶ [System](#)

[Internet Settings](#) > [Routing](#) > [RIP](#)

RIP Routing	
RIP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Version	2 ▼
<div>Save</div>	

Figure 29 - 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.

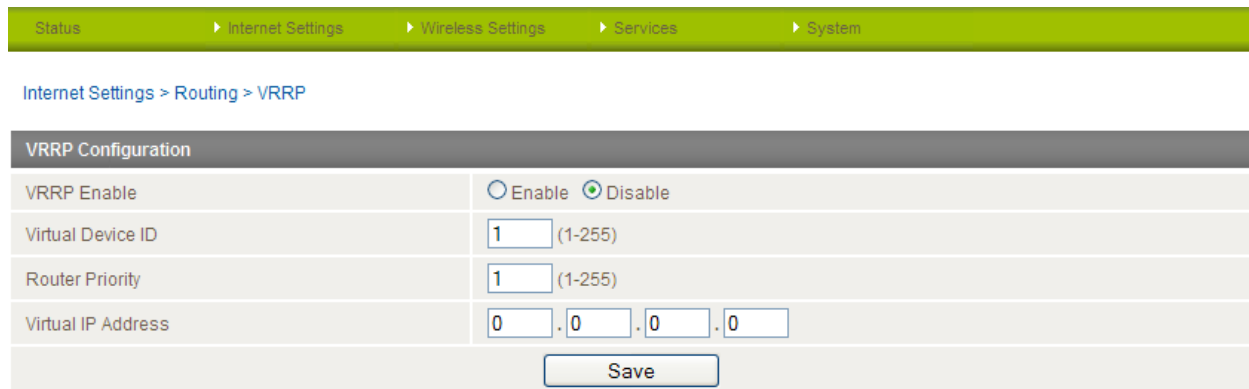


Figure 30 - VRRP Settings

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” button to save the new settings.



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.

Status
Internet Settings
Wireless Settings
Services
System

Internet Settings > Routing > NAT

IP Mapping Settings	
Item Number	<input type="text"/> (1-65535) Only required if you want to edit the existing mapping
Protocol	TCP <input type="button" value="v"/>
Source IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> (0.0.0.0 = anywhere)
Incoming Port Range	<input type="text"/> - <input type="text"/> 1-65535
Destination IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Destination Port Range	<input type="text"/> - <input type="text"/> 1-65535

Item	Protocol	Incoming Address	Incoming Port	Destination Address	Destination Port
The IP mapping table is empty					

Figure 31 - 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
Item Number	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 19 - NAT Configuration Items

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



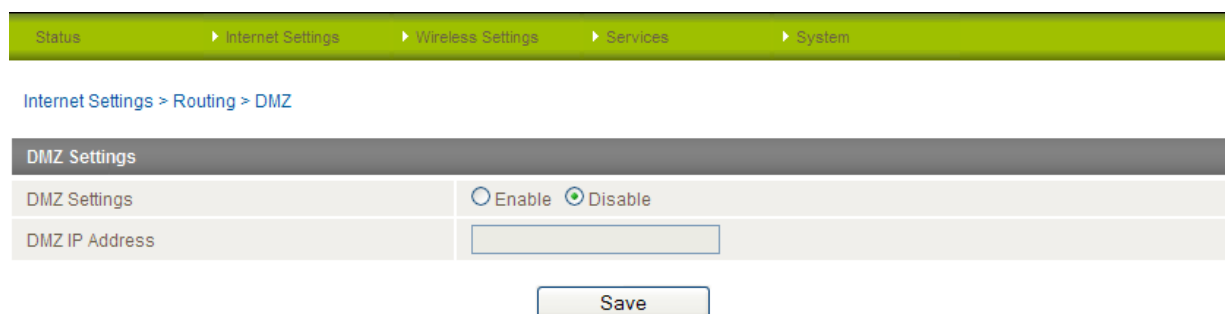
Note: If the "Incoming Port Range" specifies a single port (as above) then the destination port can be set to any port. If the "Incoming Port Range" specifies a range of port numbers then the "Destination Port Range" MUST be the same as the "Incoming Port Range".

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	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DMZ IP Address	<input type="text"/>

Figure 32 - 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

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 Wireless Website.

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

IPSec

IPSec operates on Layer 3 of the OSI model and as such can protect higher layer protocols. IPSec is used for both Site to Site VPN and Remote Access VPN. The NTC-30WV Outdoor WiFi Router supports IPSec end points and can be configured with Site to Site VPN tunnels with third party VPN routers.

How to configure an IPSec VPN connection

From the menu at the top of the screen, click “Internet Settings” then “VPN” and “IPSec”. A list of configured IPSec VPN connections is displayed.

Status

▶ Internet Settings

▶ Wireless Settings

▶ Services

▶ System

Internet Settings > VPN > IPsec

IPsec List

IPsec Log

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

Add

Figure 33 - IPSec VPN List

Click the “Add” button to begin configuring an IPSec VPN connection.



[Status](#) [Internet Settings](#) [Wireless Settings](#) [Services](#) [System](#)

[Internet Settings](#) > [VPN](#) > [IPsec](#)

VPN IPsec Edit

Enable This IPsec Profile	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Profile Name	<input type="text"/>

Remote Gateway

Remote IPsec Gateway	<input type="text"/> Road Warrior
Remote Address/Net to Join	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Remote Address/Net Mask	<input type="text"/> 255 . <input type="text"/> 255 . <input type="text"/> 255 . <input type="text"/> 0

Local LAN

Local Address/Net to Join	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Local Address/Net Mask	<input type="text"/> 255 . <input type="text"/> 255 . <input type="text"/> 255 . <input type="text"/> 0

Negotiation

Encap Protocol	<input type="text"/> ESP <input type="button" value="v"/>
IKE Mode	<input type="text"/> Main <input type="button" value="v"/>
PFS	<input type="text"/> ON <input type="button" value="v"/>
IKE Encryption	<input type="text"/> Any <input type="button" value="v"/>
IKE Hash	<input type="text"/> Any <input type="button" value="v"/>
IPsec Encryption	<input type="text"/> Any <input type="button" value="v"/>
IPsec Hash	<input type="text"/> Any <input type="button" value="v"/>
DH Group	<input type="text"/> Any <input type="button" value="v"/>
DPD Action	<input type="text"/> Hold <input type="button" value="v"/>
DPD Keep Alive Time	<input type="text"/> 10 <input type="text"/> secs
DPD Timeout	<input type="text"/> 60 <input type="text"/> secs
IKE Rekey Time	<input type="text"/> 3600 <input type="text"/> (0-78400, 0=Unlimited) secs
SA Life Time	<input type="text"/> 28800 <input type="text"/> (0-78400, 0=Unlimited) secs
Key Mode	<input type="text"/> Pre Shared Key <input type="button" value="v"/>
Pre Shared Key	<input type="text"/>
Remote Id	<input type="text"/> (xy.sample.com or blank)
Local Id	<input type="text"/> (xy.sample.com or blank)

Figure 34 - VPN Connection Settings – IPsec

The table on the following page describes each of the fields of the IPsec VPN Connection Settings page.

ITEM	DEFINITION
Enable This IPSec Profile	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	<p>Select the type of key mode in use for the VPN connection. You can select from:</p> <ul style="list-style-type: none"> - Pre Shared Key - RSA Keys - Certificates <p>Each type of Key mode requires different configuration options. For more information, please refer to the VPN Document available from the NetComm Website.</p>

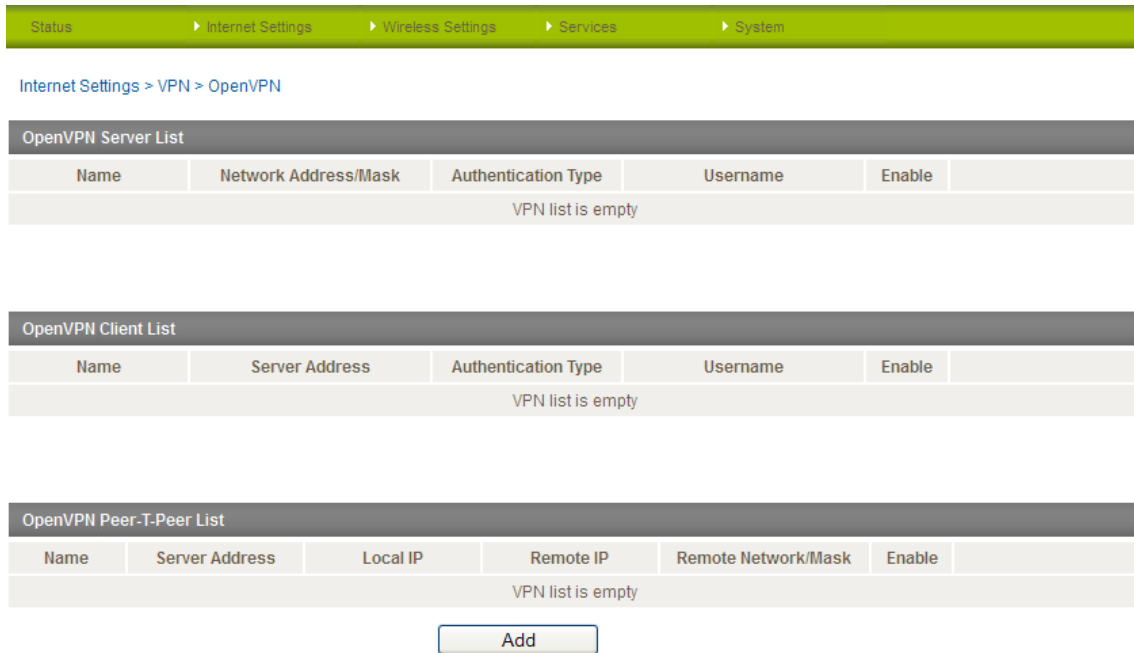
Table 20 - IPSec Configuration Items

OpenVPN

OpenVPN is an open source virtual private network (VPN) program for creating point-to-point or server-to-multi-client encrypted tunnels between host computers. It can traverse network address translation (NAT) and firewalls and allows authentication by certificate, pre-shared key or username and password. OpenVPN works well through proxy servers and can run over TCP and UDP transports. Support for OpenVPN is available on several operating systems, including Windows, Linux, Mac OS, Solaris, OpenBSD, FreeBSD, NetBSD and QNX.

How to configure an OpenVPN VPN connection

From the menu at the top of the screen, click “Internet Settings” then “VPN” and “OpenVPN”. A list of configured OpenVPN VPN connections is displayed.



Status > Internet Settings > Wireless Settings > Services > System

Internet Settings > VPN > OpenVPN

OpenVPN Server List

Name	Network Address/Mask	Authentication Type	Username	Enable
VPN list is empty				

OpenVPN Client List

Name	Server Address	Authentication Type	Username	Enable
VPN list is empty				

OpenVPN Peer-T-Peer List

Name	Server Address	Local IP	Remote IP	Remote Network/Mask	Enable
VPN list is empty					

Figure 35 - OpenVPN VPN List

Click the “Add” button to begin configuring an OpenVPN VPN connection.

Status > Internet Settings > Wireless Settings > Services > System

Internet Settings > VPN > OpenVPN

OpenVPN Edit

Enable OpenVPN	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Profile Name	<input type="text"/>
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	<p>Not Before: N/A</p> <p>Not After: N/A</p> <p>Country: <input type="text"/></p> <p>State: <input type="text"/></p> <p>City: <input type="text"/></p> <p>Organization: <input type="text"/></p> <p>Email: <input type="text"/></p> <p>Generate CA certificate...</p>
Authentication Type	<input checked="" type="radio"/> Certificate <input type="radio"/> Username / Password
Certificate Management	<p>Certificate: New...</p> <p>Name: <input type="text"/></p> <p>Country: <input type="text"/></p> <p>State: <input type="text"/></p> <p>City: <input type="text"/></p> <p>Organization: <input type="text"/></p> <p>Email: <input type="text"/></p> <p>Generate Download Revoke</p> <p>Network Address: <input type="text"/></p> <p>Network Mask: <input type="text"/></p> <p>Set Network Information</p>

[Save](#) [Exit](#)

Figure 36 - VPN Connection Settings - OpenVPN

ITEM	DEFINITION
Enable OpenVPN	Enable or Disable the OpenVPN 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	<p>Select the type of authentication in use for the VPN connection. You can select from:</p> <ul style="list-style-type: none"> - Certificate - User Name / Password <p>Each type of Key mode requires different configuration options. For more information, please refer to the VPN Document available from the NetComm Wireless Website.</p>

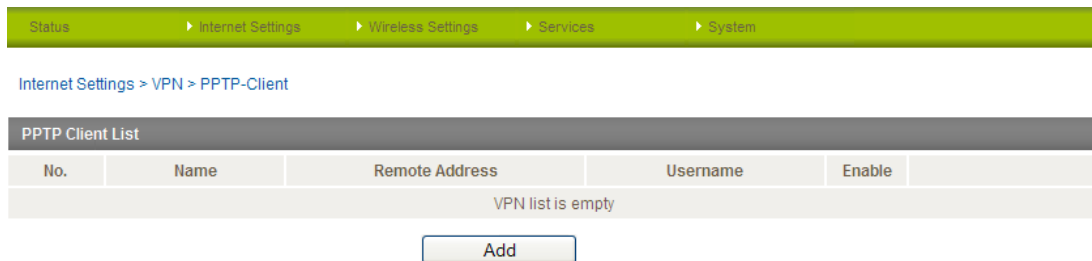
Table 21 - OpenVPN Configuration Items

PPTP-Client

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks using a TCP and GRE tunnel to encapsulate PPP packets. PPTP operates on Layer 2 of the OSI model and is included on Windows computers.

How to configure PPTP-Client VPN connection

From the menu at the top of the screen, click "Internet Settings" then "VPN" and "PPTP-Client". A list of configured PPTP-Client VPN connections is displayed.

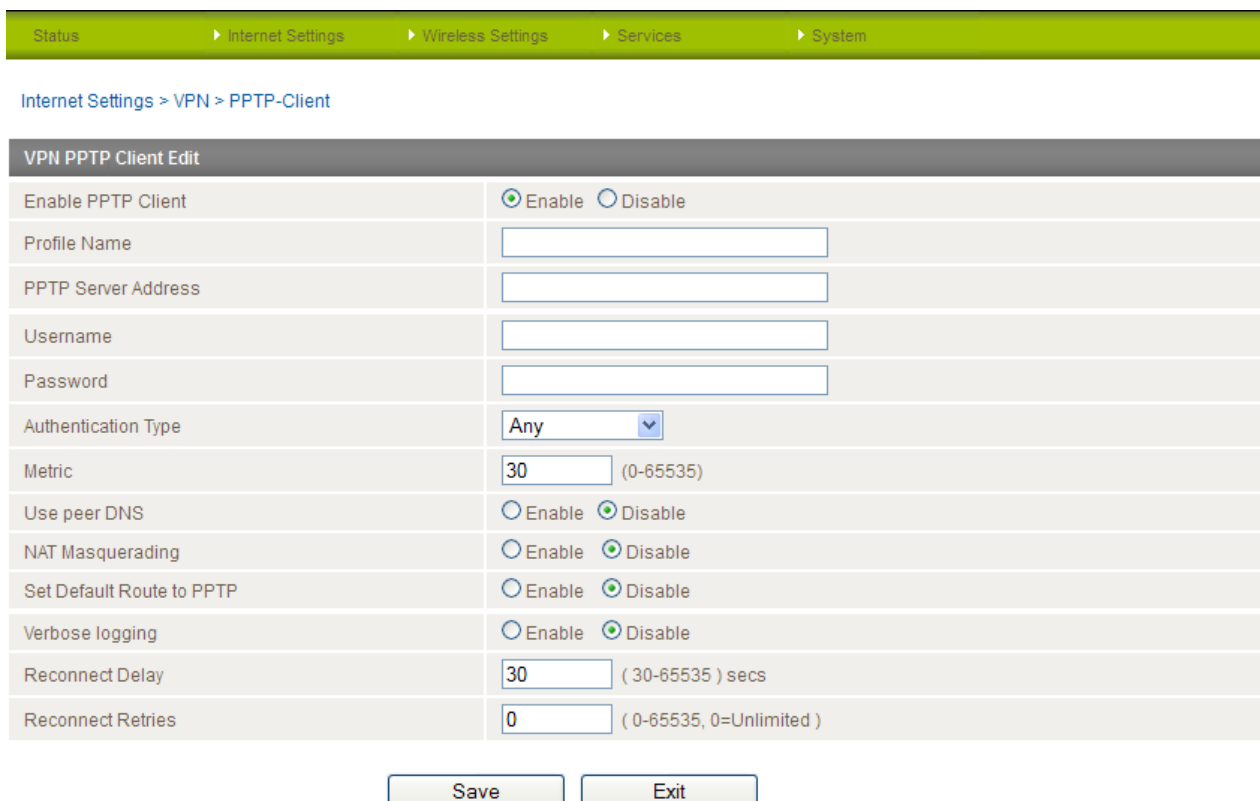


No.	Name	Remote Address	Username	Enable
VPN list is empty				

Add

Figure 37 - PPTP Client List

Click the "Add" button to begin configuring an PPTP-Client VPN connection.



Enable PPTP Client	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Profile Name	<input type="text"/>
PPTP Server Address	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Authentication Type	Any
Metric	30 (0-65535)
Use peer DNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
NAT Masquerading	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Set Default Route to PPTP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Verbose logging	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Reconnect Delay	30 (30-65535) secs
Reconnect Retries	0 (0-65535, 0=Unlimited)

Save Exit

Figure 38 - VPN Connection Settings - PPTP

ITEM	DEFINITION
Enable PPTP Client	Enable or Disable the VPN connection.
Profile Name	A name used to identify the VPN connection.
PPTP 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.

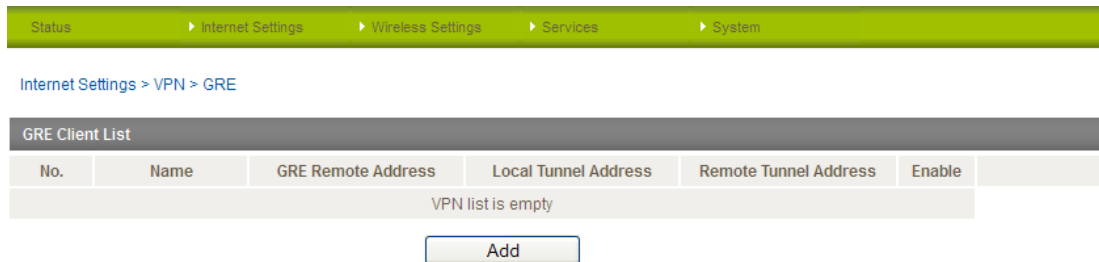
Table 22 - PPTP Configuration Items

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.

How to configure a GRE VPN connection

From the menu at the top of the screen, click “Internet Settings” then “VPN” and “GRE”. A list of configured GRE VPN connections is displayed.

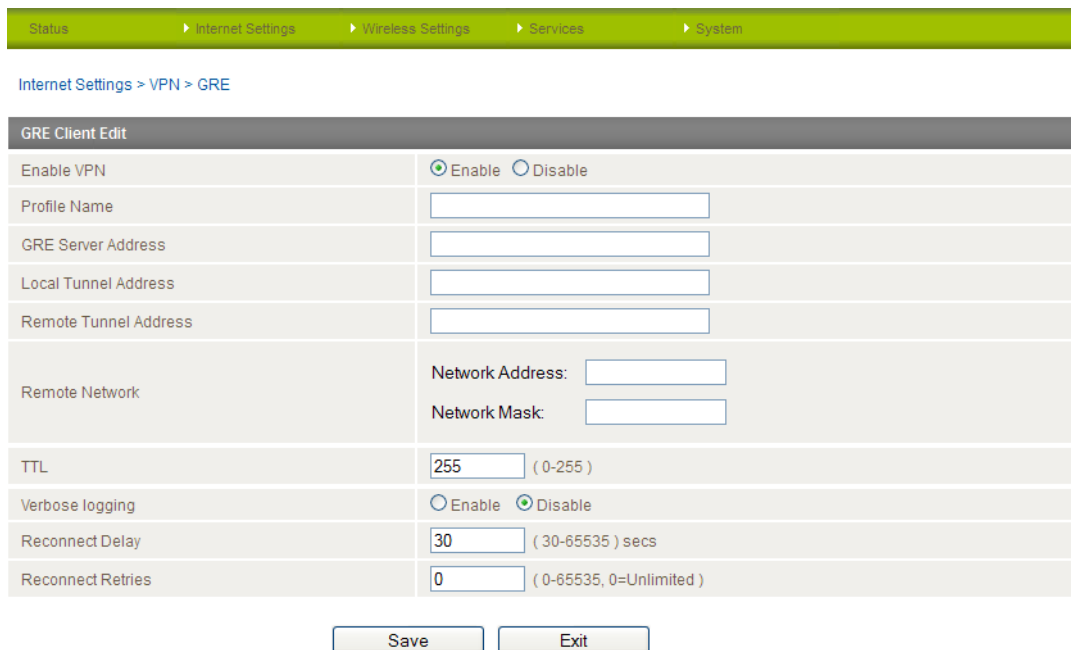


No.	Name	GRE Remote Address	Local Tunnel Address	Remote Tunnel Address	Enable
VPN list is empty					

[Add](#)

Figure 39 - GRE VPN List

Click the “Add” button to begin configuring a GRE VPN connection.



Enable VPN	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Profile Name	<input type="text"/>
GRE Server Address	<input type="text"/>
Local Tunnel Address	<input type="text"/>
Remote Tunnel Address	<input type="text"/>
Remote Network	Network Address: <input type="text"/> Network Mask: <input type="text"/>
TTL	<input type="text" value="255"/> (0-255)
Verbose logging	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Reconnect Delay	<input type="text" value="30"/> (30-65535) secs
Reconnect Retries	<input type="text" value="0"/> (0-65535, 0=Unlimited)

[Save](#) [Exit](#)

Figure 40 - GRE VPN Settings page

ITEM	DEFINITION
Enable VPN	Enable or Disable the VPN connection.
Profile Name	A name used to identify the VPN connection.
GRE Server Address	The IP Address on which the GRE VPN server is running.
Local Tunnel Address	The Local IP address of the VPN tunnel.
Remote Tunnel Address	The Remote IP address of the other end of the VPN tunnel.
Remote Network	Enter the remote network address and subnet mask.
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 23: VPN - GRE Settings

USSD

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

Status	▶ Internet Settings	▶ Wireless Settings	▶ Services	▶ System
--------	---------------------	---------------------	------------	----------

[Internet Settings > USSD](#)

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 various services. 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	<div></div>
Send Message	<input type="text" value="Enter USSD dial string here"/> <input type="button" value="Start Session"/>

Figure 41 - USSD Messaging

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

1. Checking available credit for a mobile service account.
2. Obtaining more credit for a mobile service account.
3. 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 Settings

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.

Status
Internet Settings
Wireless Settings
Services
System

Wireless Settings > Configuration

Wireless Setup	
Radio On/Off	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Country:	Australia
Network Mode	11b/g/n mixed mode
Frequency (Channel)	AUTO
Current Channel: 1	
Security Settings	
SSID:	NetComm 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	00:60:64:63:ed:1f
WDS Mode	Disable

Save

Figure 42 - 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: <ul style="list-style-type: none"> 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 24 - 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:	<input type="text" value="NetComm XXXX"/>
Network Authentication:	<input type="button" value="WPA1-WPA2"/>
WPA Group Rekey interval:	<input type="text" value="600"/>
RADIUS Server IP Address:	<input type="text" value="0.0.0.0"/>
RADIUS Port:	<input type="text" value="1812"/>
RADIUS Key:	<input type="text"/>
WPA Encryption:	AES

Figure 43 - 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 compared 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.



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

Security Settings	
SSID:	<input type="text" value="NetComm XXXX"/>
Network Authentication:	<input type="button" value="WPA-PSK-WPA2-PSK"/>
WPA Pre-Shared Key:	<input type="text" value="••••••••"/> Click here to display
WPA Group Rekey interval:	<input type="text" value="600"/>
WPA Encryption:	AES

Figure 44 - Advanced View – WiFi Security Settings - WPA-PSK/WPA2-PSK



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:	<input type="text" value="NetComm XXXX"/>
Network Authentication:	<input type="text" value="802.1X"/>
RADIUS Server IP Address:	<input type="text" value="0.0.0.0"/>
RADIUS Port:	<input type="text" value="1812"/>
RADIUS Key:	<input type="text"/>
802.1x WEP	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Figure 45 - Advanced View – WiFi Security Settings - 802.1x

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.

WDS Mode

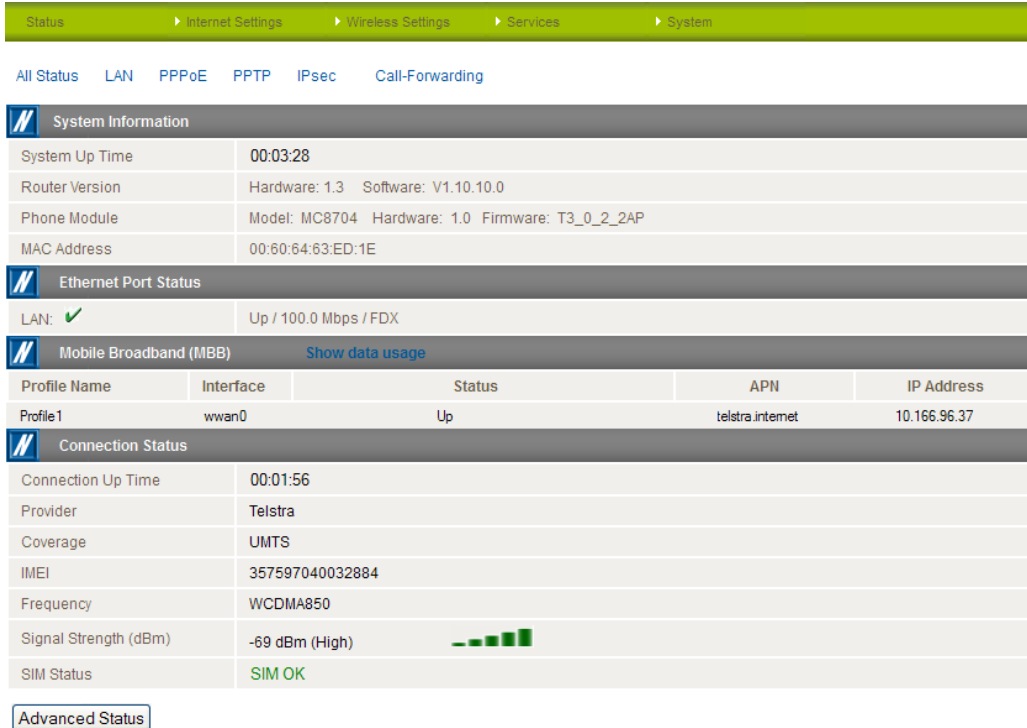
The NTC-30WV supports the configuration of a Wireless Distribution System (WDS). WDS allows you to expand your wireless network with multiple access points. There are two WDS modes available: Bridged Mode and Repeater Mode.

In Bridged mode, the WDS access points communicate with each other but do not communicate with wireless clients. Bridged mode is best used in situations where the client machines connect via Ethernet cable. In Repeater mode, the WDS access points communicate with each other and with wireless clients.

Below is an example of how to configure two NTC-30WV routers to utilise the Repeater mode WDS feature. In this example, Access Point 1 is connected to a mobile broadband network and Access Point 2 and its clients will connect to the internet through Access Point 1.

Access Point 1 – Mobile Broadband Connected

1. Establish a Mobile Broadband connection with Access Point 1:



System Information

System Up Time	00:03:28
Router Version	Hardware: 1.3 Software: V1.10.10.0
Phone Module	Model: MC8704 Hardware: 1.0 Firmware: T3_0_2_2AP
MAC Address	00:60:64:63:ED:1E


Ethernet Port Status

LAN: ✓ Up / 100.0 Mbps / FDX

Mobile Broadband (MBB) [Show data usage](#)

Profile Name	Interface	Status	APN	IP Address
Profile1	wwan0	Up	telstra.internet	10.166.96.37

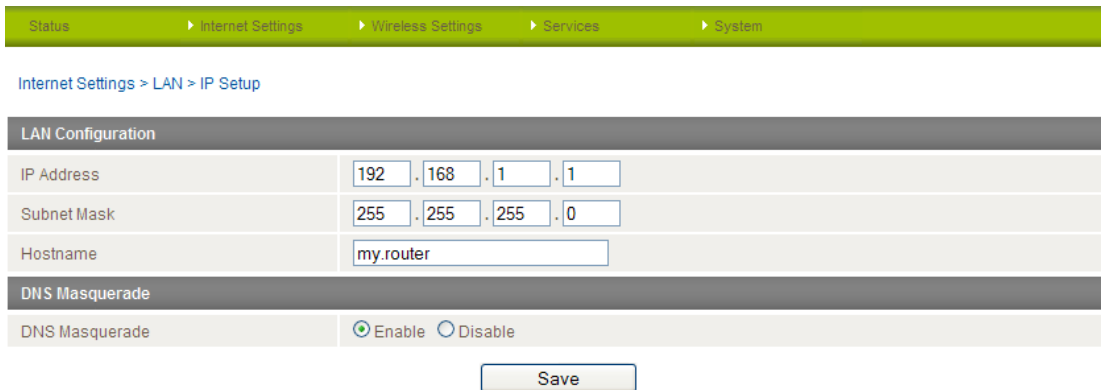
Connection Status

Connection Up Time	00:01:56
Provider	Telstra
Coverage	UMTS
IMEI	357597040032884
Frequency	WCDMA850
Signal Strength (dBm)	-69 dBm (High) 
SIM Status	SIM OK

[Advanced Status](#)

Figure 46 - WDS - Access Point 1 Status

2. Configure the LAN IP Address of Access Point 1. In this example, it is set to the default address of 192.168.1.1:



Internet Settings > LAN > IP Setup

LAN Configuration

IP Address	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 255 . 0
Hostname	my.router

DNS Masquerade

DNS Masquerade ☒ Enable ☐ Disable

[Save](#)

Figure 47 - WDS - Access Point 1 LAN IP Setup

3. Enable the DHCP Server on Access Point 1:

Status ▶ Internet Settings ▶ Wireless Settings ▶ Services ▶ System

Internet Settings > LAN > DHCP

DHCP Configuration	
DHCP	<input checked="" type="radio"/> Enable <input type="radio"/> 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	0 . 0 . 0 . 0
DNS Server 2 IP Address	0 . 0 . 0 . 0
WINS Server 1 IP Address	0 . 0 . 0 . 0
WINS Server 2 IP Address	0 . 0 . 0 . 0
NTP Server (Option 42)	0 . 0 . 0 . 0
TFTP Server (Option 66)	
Option 150	
Option 160	

Figure 48 - WDS - Access Point 1 DHCP Server Settings

4. Click Wireless Settings and then Basic. Enter the required details as listed in the table below:

Status ▶ Internet Settings ▶ Wireless Settings ▶ Services ▶ System

Wireless Settings > Configuration

Wireless Setup	
Radio On/Off	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Country:	Australia
Network Mode	11b/g/n mixed mode
Frequency (Channel)	2412MHz (Channel 1) Current Channel: 1
Security Settings	
SSID:	WDS TestAP1
Network Authentication:	Open
WEP Encryption:	Enabled
Current Network Key:	1
Network Key 1:	12345678901234567890123456 128 bit HEX
Network Key 2:	
Network Key 3:	
Network Key 4:	
Enter 10 hexadecimal digits for 64-bit encryption keys or 26 hexadecimal digits for 128-bit encryption keys.	
Wireless Distribution System (WDS)	
MAC address	00:60:64:63:ed:1f
WDS Mode	Repeater Mode
Encrypt Type	Open (sharing with the main SSID encryption)
AP MAC Address1	00:60:64:65:8e:ff
AP MAC Address2	
AP MAC Address3	
AP MAC Address4	

Save

Figure 49 – WDS - Access Point 1 Repeater Mode Setup

OPTION	DEFINITION
Radio On/Off	The Wireless Radio must be turned on in order to use WDS. Set this to ON.
Country	Select the country where the router is operating.
Network Mode	Depending on the capability of your wireless device's wireless network card select the network mode to use. There are 5 available options. They are: <ul style="list-style-type: none"> • 11 b/g mixed mode • 11b only • 11g only • 11n only • 11 b/g/n mixed mode If you are not sure which protocol to use set this option to 11 b/g/n mixed mode.
Frequency (Channel)	The frequency or wireless channel that the router is broadcasting with. Recommended channels are 1, 6 or 11. You may use any channel except AUTO in order to use WDS.
SSID	The SSID (Service Set Identifier) or network name in use for the wireless network.
Network Authentication	The wireless security settings for the router. When using WDS, the network must be set to Open, however, you can secure it with WEP Encryption.
WEP Encryption	If you wish to use WEP Encryption for the WDS network, select Enabled.
Current Network Key	You can enter up to 4 network keys. Use this drop down list to select the active network key.
Network Key 1-4	The network keys used to encrypt the network. Enter 10 hexadecimal digits for 64-bit encryption keys or 26 hexadecimal digits for 128-bit encryption keys.
MAC Address	This is the MAC Address of the wireless interface of the router. Enter this MAC Address into the client's configuration page to inform the client of the address of this router.
WDS Mode	Selects the WDS Mode to use. Available modes are Disabled, Bridged Mode and Repeater Mode. In this example we are using Repeater Mode which allows client machines to connect wirelessly. In Bridged Mode, an Ethernet connection to the client access point is required.
Encrypt Type	Shows the encryption method currently in use. When WDS Mode is in use, this must be Open.
AP MAC Address1-4	Enter the MAC Address of Access Point 2 and any other client access points in to these fields to inform the server of their addresses.

Table 25 - WDS Access Point 1 Repeater Mode Settings

When you have entered the required information, click Save:

Access Point 2 – No connection to mobile broadband

- Access Point 2 will act as a repeater for and provide internet access to its clients through Access Point 1 and therefore does not require a Mobile Broadband connection to be established.



Figure 50 – WDS - Access Point 2 Status

6. Configure the LAN IP Address of Access Point 2. In this example, it is set to the default address of 192.168.1.2:

Status ▶ Internet Settings ▶ Wireless Settings ▶ Services ▶ System				
Internet Settings > LAN > IP Setup				
LAN Configuration				
IP Address	192	168	1	2
Subnet Mask	255	255	255	0
Hostname	my.router			
DNS Masquerade				
DNS Masquerade	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<input type="button" value="Save"/>				

Figure 51 - WDS - Access Point 2 LAN IP Setup

7. Set the DHCP Server on Access Point 2 to Disable:

Status ▶ Internet Settings ▶ Wireless Settings ▶ Services ▶ System				
Internet Settings > LAN > DHCP				
DHCP Configuration				
DHCP	<input type="radio"/> Enable <input checked="" type="radio"/> 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	0	0	0	0
DNS Server 2 IP Address	0	0	0	0
WINS Server 1 IP Address	0	0	0	0
WINS Server 2 IP Address	0	0	0	0
NTP Server (Option 42)	0	0	0	0
TFTP Server (Option 66)				
Option 150				
Option 160				
DHCP Relay Configuration				
DHCP Relay	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
DHCP Server Address	0	0	0	0
Address Reservation List				
Computer Name	MAC Address	IP Address		<input type="button" value="Add"/>
DHCP Client List				
Computer Name	MAC Address	IP Address	Expire Time	
<input type="button" value="Save"/>				

Figure 52 - WDS - Access Point 2 DHCP Settings

8. Under Wireless Setup, select the same frequency channel as you did for Access Point 1. Enter an SSID to identify Access Point 2 and set Network Authentication to Open. Copy the Network Authentication and WEP Encryption settings from Access Point 1. Set Access Point 2 to Repeater mode and enter the MAC address of Access Point 1 in the AP MAC Address1 field. The MAC address of Access Point 1 is listed on the same page under Wireless Settings > Basic under the Wireless Distribution System (WDS) section. When you have entered the required information, click Save:

[Status](#) > [Internet Settings](#) > [Wireless Settings](#) > [Services](#) > [System](#)

[Wireless Settings > Configuration](#)

Wireless Setup	
Radio On/Off	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Country:	Australia
Network Mode	11b/g/n mixed mode
Frequency (Channel)	2412MHz (Channel 1) Current Channel: 1

Security Settings	
SSID:	WDS TestAP2
Network Authentication:	Open
WEP Encryption:	Enabled
Current Network Key:	1
Network Key 1:	12345678901234567890123456 128 bit HEX
Network Key 2:	
Network Key 3:	
Network Key 4:	
Enter 10 hexadecimal digits for 64-bit encryption keys or 26 hexadecimal digits for 128-bit encryption keys.	

Wireless Distribution System (WDS)	
MAC address	00:60:64:65:8e:ff
WDS Mode	Repeater Mode
Encrypt Type	Open (sharing with the main SSID encryption)
AP MAC Address1	00:60:64:63:ed:1f
AP MAC Address2	
AP MAC Address3	
AP MAC Address4	

Figure 53 - WDS – Access Point 2 Repeater Mode Setup

The Wireless Distribution System setup is now complete.

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.

[Status](#)
[Internet Settings](#)
[Wireless Settings](#)
[Services](#)
[System](#)

[Wireless Settings > 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	<input type="text" value="Auto"/>
Client Idle Timeout	<input type="text" value="300"/> sec (range 60 - 600, default 300)
Beacon Interval	<input type="text" value="100"/> ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	<input type="text" value="2"/> ms (range 1 - 255, default 1)
Fragment Threshold	<input type="text" value="2346"/> (range 256 - 2346, default 2346)
RTS Threshold	<input type="text" value="2347"/> (range 1 - 2347, default 2347)
TX Power	<input type="text" value="100"/> (range 1 - 100, default 100)
Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Figure 54 - Wireless Settings - Advanced

OPTION	DEFINITION
BG Protection Mode	A protection designed to prevent collisions among 802.11b/g modes. Mode options include Auto, On, or Off.
Client Idle 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.
Fragment Threshold	This specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
RTS Threshold	When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
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 26 - Wireless Settings - Advanced Configuration Items

Click the "Save" button to save any advanced settings changes.

MAC Filtering

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.

Status
Internet Settings
Wireless Settings
Services
System

Wireless Settings > MAC Filtering

Access Policy

Filtering Policy
Disable

Add a MAC address to the filtering list:
 : : : : :

Apply

No.	SSID	MAC Address	Filtering Policy
MAC Filtering Table Empty			

Figure 55 - Wireless LAN - MAC Filtering

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.

Status▶ Internet Settings▶ Wireless Settings▶ Services▶ System

Wireless LAN > Station List

Station List

Wireless Network

MAC address	IP Address	Host Name	RSSI	PSM	BW	Connected Time
-------------	------------	-----------	------	-----	----	----------------

Figure 56 - Wireless Station List

Services

Dynamic DNS

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.

Status ▶ Internet Settings ▶ Wireless Settings ▶ Services ▶ System	
Services > Dynamic DNS	
DDNS Configuration	
DDNS Configuration	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DDNS Settings	
Server Address	<input type="text" value="www.dhs.org"/>
Host Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
Verify Password	<input type="password"/>
<input type="button" value="Save"/>	

Figure 57 – Dynamic DNS 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.

Status ▶ Internet Settings ▶ Wireless Settings ▶ Services ▶ System	
Services > NTP	
Time Zone	
Current Time	Tue Oct 9 14:55:45 EST 2012
Time Zone	<input type="text" value="(GMT+10:00) Australia (Canberra, Melbourne, Sydney)"/>
Click here to show the Daylight Saving Time details	
Network Time Protocol (NTP) Settings	
NTP Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
NTP Server Address	<input type="text" value="0.netcomm.pool.ntp.org"/>
<input type="button" value="Save"/>	

Figure 58 - NTP Settings

System Monitor

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

Status Internet Settings Wireless Settings Services System	
Services > System Monitor	
<div> <div>Periodic PING Settings</div> <div>Display Introduction</div> </div>	
Destination Address	<input type="text"/>
Second Address	<input type="text"/>
Periodic PING Timer	<input type="text"/> (0=disable, 300-65535) secs
Periodic PING Accelerated Timer	<input type="text"/> (0=disable, 60-65535) secs
Fail Count	<input type="text"/> (0=disable, 1-65535) times
<div>Periodic Reboot</div>	
Force reboot every	<input type="text"/> 0 (0=disable, 5-65535) mins
<input type="button" value="Save"/>	

Figure 59 - 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 "Second Address".
3. The router then sends 3 consecutive pings to the "Destination Address" and 3 consecutive pings to the "Second Address" every "Periodic PING Accelerated Timer" 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.



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.

How to disable the Periodic Ping Monitor

To disable the Periodic Ping Reset Monitor simply set to Fail Count 0.



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.

How to configure a Forced Reset

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.

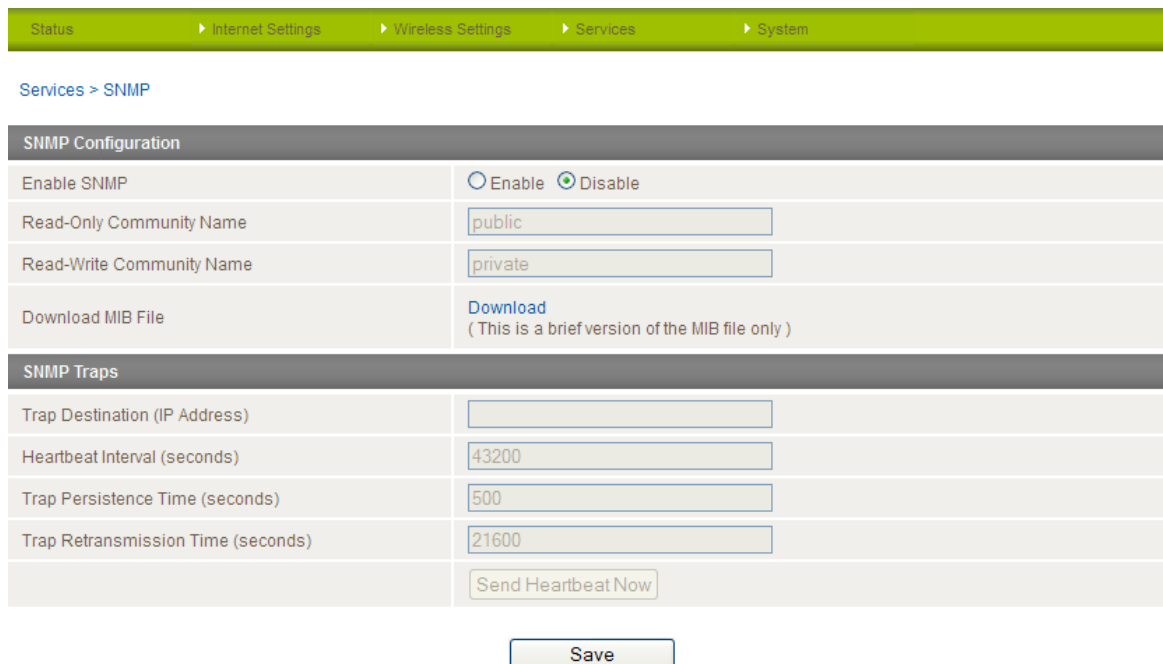


Figure 60 - SNMP Settings

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 27 - 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".

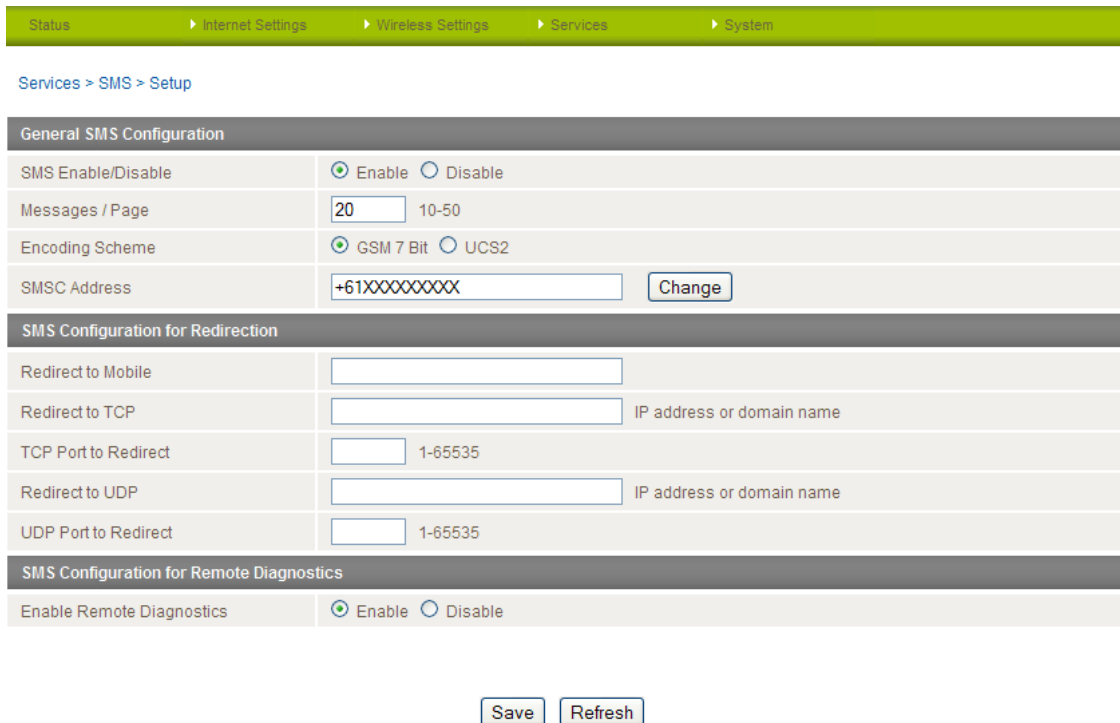


Figure 61 - SMS Function Setup

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 broadband 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 28 -SMS Setup Settings

SMS Configuration for Redirection

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.



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.

[Status](#)
[Internet Settings](#)
[Wireless Settings](#)
[Services](#)
[System](#)

[Services](#) > [SMS](#) > [New Message](#)

Create New Message

Destination Number 001	<input checked="" type="checkbox"/> +61XXXXXXXXXX
Destination Number 002	<input type="checkbox"/> <input type="text"/>
Destination Number 003	<input type="checkbox"/> <input type="text"/>
Destination Number 004	<input type="checkbox"/> <input type="text"/>
Destination Number 005	<input type="checkbox"/> <input type="text"/>
Destination Number 006	<input type="checkbox"/> <input type="text"/>
Destination Number 007	<input type="checkbox"/> <input type="text"/>
Destination Number 008	<input type="checkbox"/> <input type="text"/>
Destination Number 009	<input type="checkbox"/> <input type="text"/>
Destination Number 010	<input type="checkbox"/> <input type="text"/> <input type="button" value="+"/> <input type="button" value="-"/>

Message Body

Test message

12 / 160

Maximum number of characters can vary depending on coding scheme. In GSM7 bit mode 160 characters can be sent within a message but the limit changes to 50 characters if the message includes special characters. In UCS2 mode most of special character set can be sent but only 50 characters can be sent within a single message.

Figure 62 - 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 to the right 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 required 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.

[Status](#) ▶ [Internet Settings](#) ▶ [Wireless Settings](#) ▶ [Services](#) ▶ [System](#)

[Services > SMS > Inbox](#)

Received Messages - Total 0 Messages

<input type="checkbox"/>	From	Time	Message
--------------------------	------	------	---------

[Delete](#) [Reply](#) [Forward](#) [Refresh](#) [Add White List](#) 1 / 1

Figure 63 - SMS Inbox

[Status](#) ▶ [Internet Settings](#) ▶ [Wireless Settings](#) ▶ [Services](#) ▶ [System](#)

[Services > SMS > Outbox](#)

Sent Messages - Total 0 Messages

<input type="checkbox"/>	To	Time	Message
--------------------------	----	------	---------

[Delete](#) [Forward](#) [Refresh](#) [Add White List](#) 1 / 1

Figure 64 - 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.

Status
Internet Settings
Wireless Settings
Services
System

Services > SMS > Diagnostics & Command Execution Setup

SMS Diagnostics & Command Execution Configuration

Enable Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Send Ack. SMS for Set Command	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Send Ack. SMS to	<input type="radio"/> Fixed Number <input checked="" type="radio"/> SMS Sender Number
Fixed Ack. SMS Number	<input type="text"/>
Send Error SMS for Get/Set/Exec Command	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Send Error SMS to	<input type="radio"/> Fixed Number <input checked="" type="radio"/> SMS Sender Number
Fixed Error SMS Number	<input type="text"/>
Max. Diag. SMS Tx Limit	<input type="text" value="100"/> messages per <input type="text" value="DAY"/> 0 / 100 messages sent <input type="button" value="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	<input type="text"/>	<input type="text"/>	<input type="button" value="Delete"/> <input type="button" value="+"/> <input type="button" value="-"/>

Figure 65 - 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.



Note: Times displayed are in UTC format.

For Example:

- If the time frame is set to “HOURL” 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 VARIABLE

PASSWORD get VARIABLE

Generic Format for writing to variables:

set VARIABLE=VALUE

PASSWORD set VARIABLE=VALUE

Generic Format for executing a command:

executeCOMMAND

PASSWORD executeCOMMAND

Replies

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

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

Table 29 - SMS Diagnostic Command Syntax

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

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

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

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 VARIABLE1; get VARIABLE2; get VARIABLE3

PASSWORD get VARIABLE1; get VARIABLE2

set VARIABLE=VALUE1 ; set VARIABLE2=VALUE2

PASSWORD set VARIABLE1=VALUE1; set VARIABLE2=VALUE2; set VARIABLE3=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 VARIABLE2"

"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; getVariable1"; "get VARIABLE2"

"PASSWORD execute reboot; PASSWORD get Variable1"; "get VARIABLE2"

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. Reports 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. Reports 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 gateway will check the currently activated profile and disconnect this profile before executing the command. Reports an error if no profile number is selected and there is no stored last active profile number.

Table 30 - List of Valid SMS Diagnostic Commands

The following table lists 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	rsi	R	3G signal strength	65 dBm
7	wwan.0.imei	imei	R	IMEI number	359102128941027512
8	statistics.usage_current	<u>usage</u>	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 31 - 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	execute 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 32 - SMS Diagnostics - Example Commands

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.



Note: The Auto Dial function is only available when the Voice Call Function is enabled.

[Status](#)
[Internet Settings](#)
[Wireless Settings](#)
[Services](#)
[System](#)

[Services > Auto Dial](#)

Auto Dial Configuration

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

Enable Auto Dialling	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Auto Dialling Number	<input type="text"/>

Save

Figure 66 - 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 33 - 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.

Status ▶ Internet Settings ▶ Wireless Settings ▶ Services ▶ System

Log File
Display Level All
Clear Log File

Date & Time	Machine	Level	Process	Message
Oct 9 15:24:43	ntc_40wv	user.info	kernel	Deleted trigger, pipe=0x00030600, errval=0
Oct 9 15:24:42	ntc_40wv	user.info	kernel	Deleted trigger, pipe=0x00048680, errval=0
Oct 9 15:24:42	ntc_40wv	local5.info	connection_mgr[330]	sending SIGTERM to the process - pid=5515,count=4
Oct 9 15:24:42	ntc_40wv	local5.info	connection_mgr[330]	stopping connection of profile 1
Oct 9 15:24:42	ntc_40wv	user.notice	PPPs	wwan0 DOWN Tue Oct 9 15:24:42 EST 2012
Oct 9 15:24:42	ntc_40wv	user.notice	root	SUSBNET usbnet connection down
Oct 9 15:24:42	ntc_40wv	user.notice	cns_profile	PDP session status changed - [wwan.0.session.0.status]=0'
Oct 9 15:24:42	ntc_40wv	user.notice	cns_profile	PDP command processed - [wwan.0.profile.cmd.command]=deactivate
Oct 9 15:24:41	ntc_40wv	local5.info	connection_mgr[330]	sending SIGTERM to the process - pid=5515,count=3
Oct 9 15:24:41	ntc_40wv	local5.info	connection_mgr[330]	stopping connection of profile 1
Oct 9 15:24:41	ntc_40wv	user.err	kernel	sierra_net 1-2.2:1.7: wwan0: Invalid LSI
Oct 9 15:24:41	ntc_40wv	user.err	kernel	sierra_net 1-2.2:1.7: wwan0: Link type unsupported: 0xff
Oct 9 15:24:40	ntc_40wv	local5.info	connection_mgr[330]	sending SIGTERM to the process - pid=5515,count=2
Oct 9 15:24:40	ntc_40wv	local5.info	connection_mgr[330]	stopping connection of profile 1
Oct 9 15:24:39	ntc_40wv	user.notice	root	SUSBNET using udev interface name NETIF=wwan0
Oct 9 15:24:39	ntc_40wv	local5.info	connection_mgr[330]	sending SIGTERM to the process - pid=5515,count=1
Oct 9 15:24:39	ntc_40wv	local5.info	connection_mgr[330]	stopping connection of profile 1

[Download Log File](#)

Figure 67 - System Log

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

You can use the “Display Level” drop-down list to select a message level to be displayed. The message levels are described in the table below.

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 34 - 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 router's 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".

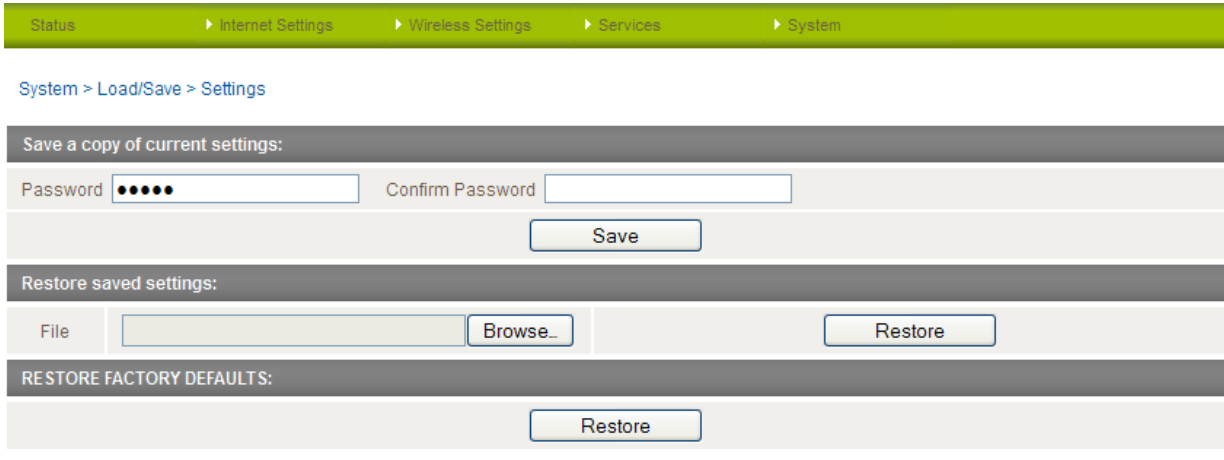


Figure 68 - Load / Save Configuration Page



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 router's configuration

Type the root manager password in both the Password and Confirm Password fields and click the Save button.

You will be prompted to save a copy of the current settings from the router to your PC.



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 router's configuration

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

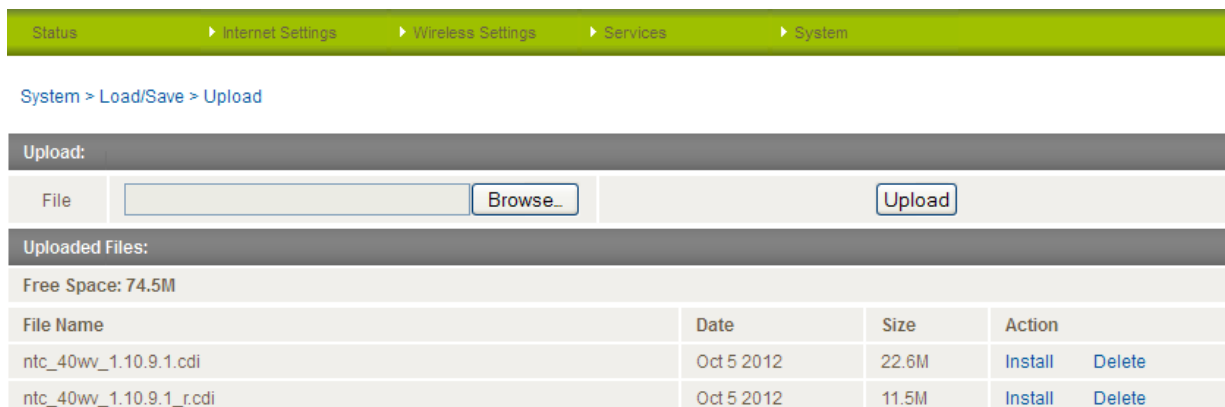
To restore the router's configuration to the factory defaults

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.



File Name	Date	Size	Action
ntc_40wv_1.10.9.1.cdi	Oct 5 2012	22.6M	Install Delete
ntc_40wv_1.10.9.1_r.cdi	Oct 5 2012	11.5M	Install Delete

Figure 69 - 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.



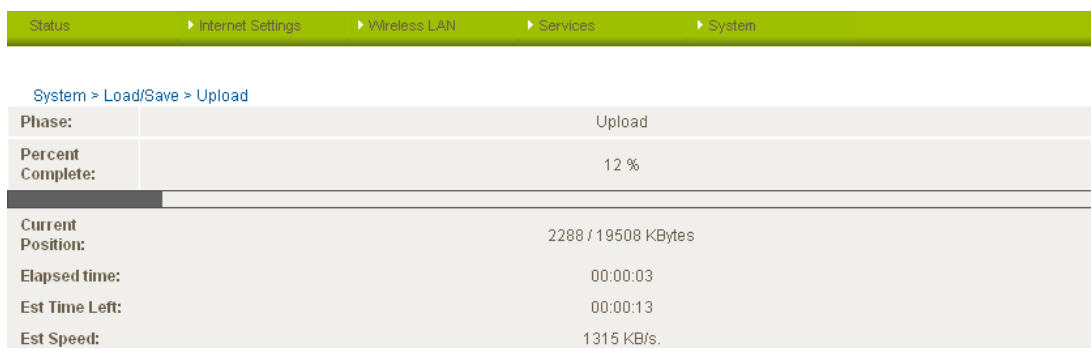
Note: In order to perform an update, you must be logged into the router as the root user (see the Remote Administration section for more details).

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%.



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 70 - 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 71 - 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.

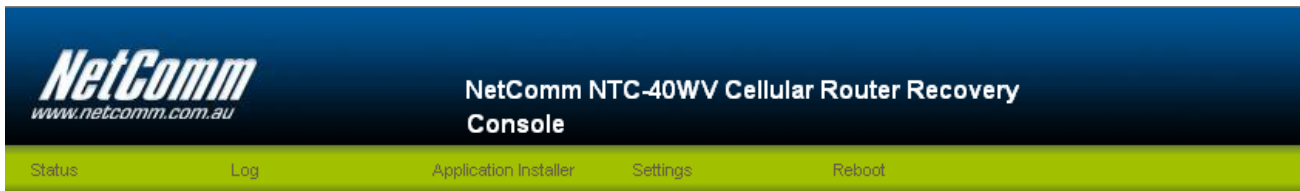


Figure 72 - Recovery Console Banner

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%.

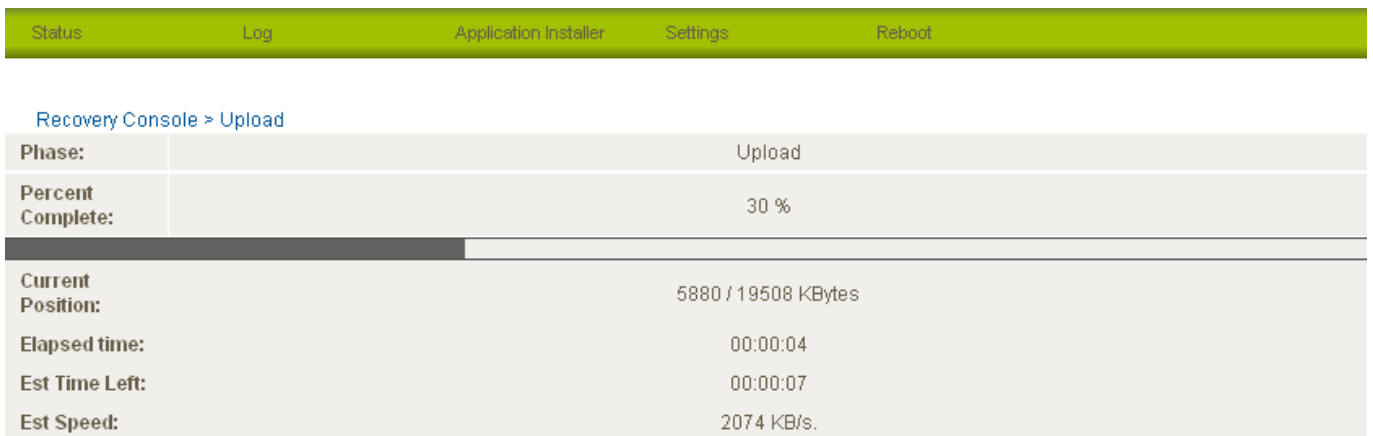


Figure 73 - Recovery Console - Upload Firmware

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.



Figure 74 - Recovery Console - Firmware Update

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

Package Manager

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

Status	▶ Internet Settings	▶ Wireless LAN	▶ Services	▶ System
--------	---------------------	----------------	------------	----------

[System > Load/Save > Package Manager](#)

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

Figure 75 - Package Manager Items

The Package Name, Version, Architecture and Install time are shown while 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.



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.

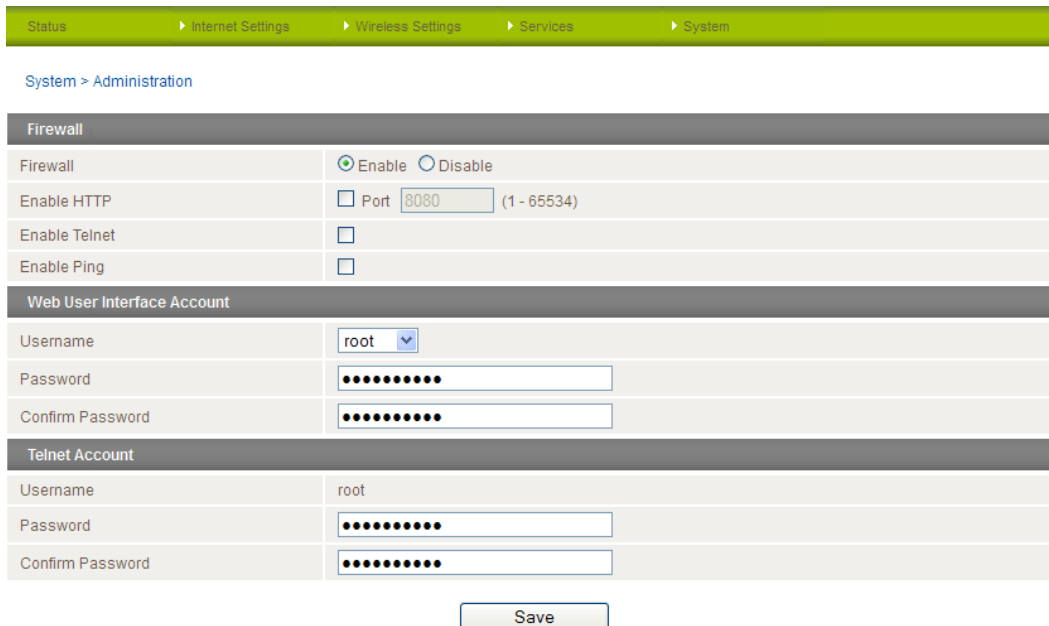


Figure 76 - Administration Configuration Items

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.
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.
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 35 - Administration Configuration Items



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".



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".



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.

Status
Internet Settings
Wireless Settings
Services
System

System > System Configuration

Remote Syslog Server

IP / Hostname [:PORT]

Diagnostics Log

Log to file

☐ Enable
☒ Disable

TCP Keepalive Settings

Keepalive

☐ Enable
☒ Disable

Keepalive Time

(60-65535) seconds

Keepalive Interval

(10-28800) seconds

Keepalive Probes

(1-1000) times

Voice Feature Settings

The router should be rebooted after changing Voice Feature Settings.

Voice Call Function

☐ Enable
☒ Disable

Save

Figure 77 - 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.
Log to file	Enables logging of high level communication between the router and the embedded module. The log is saved to file and can be accessed on the Log page. See the Log section for details.
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.
Voice Call Function	Allows you to enable or disable the voice calling function from the RJ-11 Telephone Cable Port.

Table 36 - System Configuration Items



Note: If the Voice Call Function option is changed, you must click Save and reboot the router for the changes to take effect.

TR-069

The TR-069 (Technical Report 069) protocol is a technical specification also known as CPE WAN Management Protocol (CWMP). It is a framework for remote management and auto-configuration of end-user devices such as customer-premises equipment (CPE) and Auto Configuration Servers (ACS). It is particularly efficient in applying configuration updates across networks to multiple CPEs.

It uses a bi-directional SOAP/HTTP-based protocol based on the application layer protocol.

[Status](#)
[Internet Settings](#)
[Wireless Settings](#)
[Services](#)
[System](#)

[System](#) > [TR-069](#)

TR-069 Configuration

Enable TR-069 Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
ACS URL	<input type="text"/>
ACS Username	<input type="text" value="acs"/>
ACS Password	<input type="password" value="..."/>
Verify ACS Password	<input type="password" value="..."/>
Enable Periodic ACS Informs	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Inform Period	<input type="text" value="600"/> seconds

TR-069 Connection Request

Connection Request Username	<input type="text" value="cpe"/>
Connection Request Password	<input type="password" value="..."/>
Verify Password	<input type="password" value="..."/>

Figure 78 - System - TR-069

OPTION	DEFINITION
Enable TR069 Service	This field provides the option to switch on or off the TR069 feature. ..
ACS URL	This field can be used to enter the domain name or IP address of the Auto Configuration Server (ACS) you wish to use.
ACS Password/Verify ACS Password	This field can be used to enter the password that the Auto Configuration Server (ACS) uses
Enable Periodic ACS Informs	Each session begins with the transmission of an Inform message from the ACS server. If able to the CPE device responds with an Inform Response message. A periodic Inform message verifies that each CPE device is capable of communicating and receiving updates from the ACS server
Keepalive Probes	The number of TCP Keepalive packets to send.
Inform Period	Enter the time in seconds between periodic Inform messages. The maximum time span possible is equivalent to more than 68 years.
Connection Request Username	Enter the TR-069 connection request username here.
Connection Request Password	Enter the TR-069 connection request password here.
Verify Password	Re-enter the TR-069 connection request password here and press the Save button.

Table 37 - System - TR-069 Details

Logoff

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

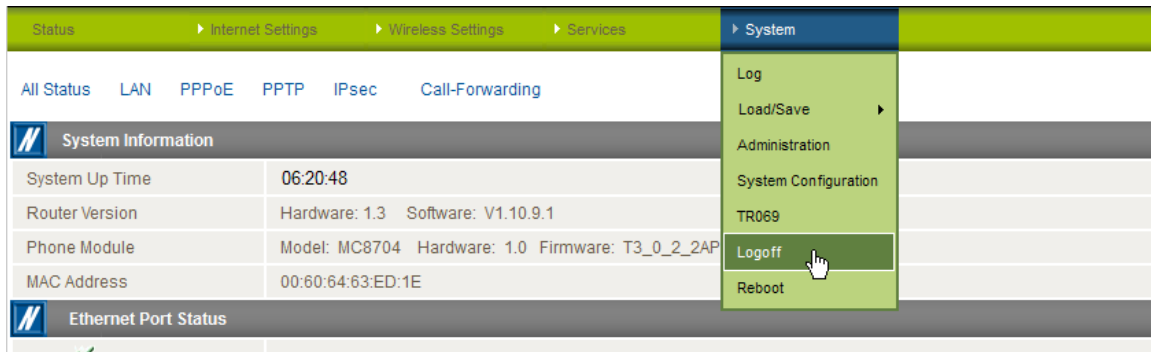


Figure 79 - Logoff

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.

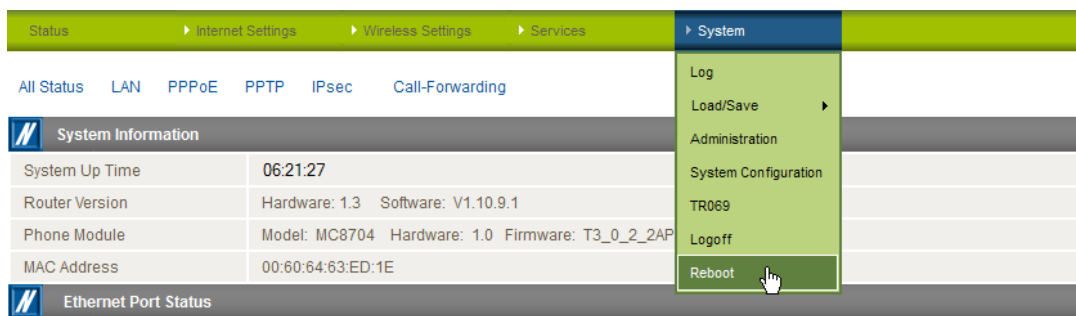


Figure 80 - Reboot Router

Technical Data

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

MODEL	NETCOMM NTC-40WV
Modem Module/Chipset	Sierra MC8704 / Qualcomm MDM8200A
Wireless LAN	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 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 indicator
Operating Temperature	Normal Operating Temperature: -25 °C to 60 °C Extended Operating Temperature: Module: -25°C to +75°C (Reduced Performance)
Power input	DC-in Port: 9 ~ 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 38 - Technical Specifications for the NTC-40WV

RJ-45 Connector

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



Pin: 1 8

Figure 81 - 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 39 - 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 82 - Locking Power Terminal Block

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

Table 40 - Locking Power Block Pin Outs

Additional Product Information

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.



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 41 - 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.



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.

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 the NTC-40WV.
3. Try rebooting your NTC-40WV.

List of Mobile Broadband Service Provider APNs

MOBILE SERVICE	APN
Australia	
Telstra	telstra.internet
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	primuslms1
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 42 - List of Mobile Broadband Service Provider APNs

Appendix A: Tables

Table 1 - Document Revision History	2
Table 2 - LED Indicators	7
Table 3 - Device Dimensions.....	8
Table 4- 2.4GHz WiFi Antenna Dimensions	8
Table 5 - 3G Antenna Dimensions	9
Table 6 - Bottom Mounted interfaces	10
Table 7 - Top Mounted interfaces	10
Table 8 - LAN Management Default Settings	11
Table 9 – WiFi Default Settings.....	11
Table 10 - Web Interface Default Settings.....	11
Table 11 - Telnet Access	11
Table 12 - Status page items.....	16
Table 13 - Status Page - LAN Details	17
Table 14 - Status Page - PPPoE Details	17
Table 15 - Status Page - PPTP Details	17
Table 16: Status Page - IPSec Details	17
Table 17: Status Page - Call Forwarding Settings	18
Table 18: Status - Advanced Status Item Details.....	20
Table 19 - NAT Configuration Items	33
Table 20 - IPSec Configuration Items.....	37
Table 21 - OpenVPN Configuration Items.....	39
Table 22 - PPTP Configuration Items	41
Table 23: VPN - GRE Settings	43
Table 24 - Wireless Configuration - Basic Configuration Items	45
Table 25 - WDS Access Point 1 Repeater Mode Settings	50
Table 26 - Wireless Settings - Advanced Configuration Items.....	53
Table 27 - SNMP Configuration Options.....	58
Table 28 -SMS Setup Settings	59
Table 29 - SMS Diagnostic Command Syntax	65
Table 30 - List of Valid SMS Diagnostic Commands.....	67
Table 31 - List of SMS Diagnostics Variables	67
Table 32 - SMS Diagnostics - Example Commands	68
Table 33 - Auto Dial Configuration Items	69
Table 34 - System Log Detail Levels.....	70
Table 35 - Administration Configuration Items	75
Table 36 - System Configuration Items.....	76
Table 37 - Technical Specifications for the NTC-40WV	79
Table 38 - RJ-45 Connector Pin Outs	80
Table 39 - Locking Power Block Pin Outs.....	80
Table 40 - Additional Product Information - Call Feature Codes Quick Reference	82
Table 41 - List of Mobile Broadband Service Provider APNs	85

Legal and Regulatory

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 Wireless' (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.

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.

Consumer Protection Laws

Australian and New Zealand consumer law in certain circumstances implies mandatory guarantees, conditions and warranties which cannot be excluded by NetComm Wireless 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 Wireless 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.

Product Warranty

All NetComm Wireless 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.netcommwireless.com. 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 Wireless and any other reasonable requirements of NetComm Wireless including producing such evidence of purchase as NetComm Wireless may require;
4. the cost of transporting product to and from NetComm Wireless' nominated premises is your responsibility;
5. NetComm Wireless 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 Wireless' 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 Wireless 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 Wireless;
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 Wireless; or
6. the serial number has been defaced or altered in any way or if the serial number plate has been removed.

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 Wireless accepts no liability or responsibility, for consequences arising from the use of this product. NetComm Wireless 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 Wireless' 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 Wireless' liability for any breach of that guarantee, condition or warranty is limited to: (i) in the case of a supply of goods, NetComm Wireless 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 Wireless 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 Wireless is unable to limit its liability as set out above, NetComm Wireless limits its liability to the extent such liability is lawfully able to be limited.

Contact

Address: NetComm Wireless Limited 18-20 Orion Road, Lane Cove NSW 2066 Sydney, Australia

ABN: 85 002 490 486

Website: www.netcommwireless.com

Phone: +61(0)2 9424 2070

Fax: +61(0)2 9424 2010

Email: sales@netcommwireless.com ; techsupport@netcommwireless.com