

# Outdoor HSPA+ WiFi Router with Voice



## USER GUIDE

#### Copyright

Copyright© 2013 NetComm Wireless Limited. All rights reserved.

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



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

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.

NetComm NTC-30WV

DOCUMENT VERSION	DATE
1.0- Initial document release	09/10/2012
2.0- Added Appendix describing Recovery mode	24/01/2013

*Table 1 - Document Revision History*

## Table of Contents

Overview .....	4
Product Introduction .....	6
Physical Dimensions and Indicators .....	7
NTC-30WV Default Settings .....	12
Implementation and Deployment Scenario .....	14
Installation and Configuration of the NTC-30WV .....	15
Captive Power Terminal Block.....	16
Logging on via the web-based user interface.....	18
Status .....	19
Advanced Status .....	21
Internet Settings .....	23
Mobile Broadband .....	23
LAN .....	28
Routing .....	30
VPN .....	35
USSD.....	42
Wireless Settings .....	43
Basic.....	43
Advanced.....	51
MAC / IP / Port Filter.....	52
Station List .....	53
Services .....	54
Dynamic DNS.....	54
NTP .....	54
System Monitor .....	55
SNMP .....	56
SMS.....	57
Auto Dial .....	67
System.....	67
Log .....	67
Load / Save.....	68
Administration.....	72
System Configuration.....	73
TR-069.....	74
Logoff .....	75
Reboot.....	75
Technical Data.....	76
Additional Product Information .....	77
Appendix A: Tables.....	81
Appendix B: Recovery mode .....	82
Legal and Regulatory .....	83

# Overview

## Introduction

This document details the process of installing the NTC-30WV as well as mounting and deployment advice. This advice will include a few demonstration deployments and an explanation of related technologies that are suitable for this Outdoor HSPA+ WiFi Router.

## Target Audience

This document is expected to be utilised by system integrators or experienced hardware installers who are comfortable with all aspects of IP based networking and have an understanding of wireless based technologies.

## Professional Installation Instructions

Please be advised that due to the unique functions supplied by this product, the device is intended for use with licensed third-parties only. The product will be distributed through controlled distribution channels and should be installed by trained professionals. It will not be sold directly to the general public through retail stores.

### 1. Installation Personnel

This product is designed for specific applications and needs to be installed by qualified personnel who have RF and related rule knowledge. The general user shall not attempt to install or change the settings.

### 2. Installation Location

The product shall be installed at a location where the radiating antenna can be kept at least 30cm from a nearby person in normal operation conditions to meet regulatory RF exposure requirements.

### 3. External Antenna

Use only antennae which have been approved by NetComm Wireless Limited. Non-approved antennae may produce unwanted spurious or excessive RF transmitting power which may lead to the violation of FCC/IC limit and is prohibited.

### 4. Installation Procedure

Please refer to the rest of this manual for further details.

### 5. Warning

Please carefully select the installation position and make sure that the final output power does not exceed the limit set force in relevant rules. The violation of the rules could lead to serious federal penalties.

The following maximum Transmit powers should be observed during configuration:

PEAK TRANSMIT POWER	
802.11b	16.29 dBm
802.11g	23.98 dBm
802.11n – 20 MHz	24.51 dBm
802.11n – 40 MHz	24.06 dBm

Table 2: Maximum Transmit Power Levels

AVERAGE TRANSMIT POWER	
802.11b	14.11 dBm
802.11g	13.32 dBm
802.11n – 20 MHz	13.38 dBm
802.11n – 40 MHz	13.21 dBm

*Table 3: Average Transmit Power Levels*

## Prerequisites

Before continuing with the installation of your NTC-30WV, 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.

## 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 outdoor fixed wireless data gateway designed for rugged deployments in remote environments and industrial applications
- Ideal for providing primary and backup wireless connectivity over 3G UMTS networks
- Maximum data speed in downlink 21Mbps (HSDPA) and 5.76Mbps in uplink (HSUPA)
- Embedded high-performance 3G cellular modem supporting HSPA+/EDGE/GPRS
- IP67 and environmentally rated chassis to withstand extreme weather conditions
- Extended temperature tolerance in operation -25 to 75°C
- 2.4 GHz band wireless LAN access point with 2x2 MIMO antenna technology
- IEEE 802.11n standard for wireless data speeds up to 300Mbps
- Ethernet 10/100 connectivity with Power over Ethernet Injector for universal deployment
- Analogue telephone connectivity (CS Voice) for complete landline replacement (optional configuration)
- Alternative DC power input available as a optional extra to suit diverse installation environments
- Built-in VPN clients for a secure connection over a public cellular network

## Package Contents

The NTC-30WV series package consists of:

- NetComm NTC-30WV - Outdoor HSPA+ WiFi Router
- 2 x WiFi Antennas (N Type female)
- 2 x 3G Antennas (N Type female)
- Mounting Bracket
- 4 x Wall mounting screws (Diameter = 6mm, Length = 25mm)
- 4 x Mounting screws (Diameter = 6mm, Length = 14.85mm)
- IP67 Water-proof Plug Cable Gland
- Ferrite Core
- 2 x Hose Clamps for pole mounting
- Wireless Security Card
- Power DC cable 10m (open ended)

If any of these items are missing or damaged, please contact NetComm Support immediately by visiting the NetComm Support website at: <http://www.netcommwireless.com/contact-forms/support>

## Product Features

The NetComm Wireless outdoor router (NTC-30WV) is designed to deliver high speed internet to homes and businesses with otherwise little to no Internet access available. The NTC-30WV is a robust 3G (HSPA+) router which can be pole or wall mounted and connects to a 3G network. The NTC-30WV features a powerful antenna system and wireless radio together in a single unit. This tight integration between the radio receiver and antenna system in an outdoor unit provides great benefits to signal strength compared with separated solutions involving signal degradation along lengthy antenna cabling.

The integrated telephone adapter connects a standard analogue phone handset to the NTC-30WV. It allows for phone calls to be made over the 3G UMTS network for a full landline replacement. The router integrates a powerful Sierra Wireless module (MC8704) and delivers download speeds of up to 21Mbps which is then transmitted via Ethernet to a WiFi router inside the property.

Power is delivered to the outdoor router via Power over Ethernet technology making installation quick and easy as there is no power source required at the outdoor mount point, and both power and data can be provided via a single cable from inside the property. With an IP67 rating, the device also withstands diverse temperature and weather environments.

---

<sup>1</sup> Maximum wireless signal rate and coverage values are derived from IEEE Standard 802.11g and 802.11n specifications. Actual wireless speed and coverage are dependent on network and environmental conditions included but not limited to volume of network traffic, building materials and construction/layout.

# Physical Dimensions and Indicators

## LED Indicators

The NTC-30WV uses 7 LEDs to display the current system and connection status.



Figure 1 - NTC-30WV LED Indicators








NTC-30WV			
LED INDICATOR	ICON	COLOUR	DEFINITION
High Signal		Green	High 3G Signal strength available.
Medium to High Signal		Green	Medium to High 3G Signal strength available.
Medium Signal		Green	Medium 3G Signal strength available.
Low to Medium Signal		Green	Low to Medium 3G Signal strength available.
Low Signal		Green	Low 3G Signal strength available.
Internet		Green	Router is currently connected to the Internet.
Power		Red	Unit is powered on.

Table 4 - LED Indicators

The 5 LEDs also indicate whether the device is MEP locked, SIM is not inserted and if the SIM is PIN or PUK locked by flashing in certain patterns. Below is a table outlining the various LED flash sequences and their meanings.

LED PATTERN	DESCRIPTION
All signal LEDs flash ON and OFF every 2 seconds	SIM not inserted
The signal LEDs flash in a pattern with one, three and 5 LEDs flashing in a sequence.	MEP Lock
The signal LEDs flash in a sequential order starting with the Low signal LED to the High signal LED.	SIM is PIN locked
The signal LEDs flash in a sequential order starting with the High signal LED to the Low signal LED.	SIM is PUK locked



## Physical Dimensions

The following page lists the physical dimensions of the NTC-30WV, as well as the physical dimensions of the antennas and the included mounting bracket which can be used to attach the NTC-30WV to a pole or to provide a wall / ceiling mount.



Figure 2 – NTC-30WV Dimensions

NTC-30WV (WITHOUT ANTENNAS ATTACHED)	
Length	255 mm
Depth	80 mm
Height	240 mm
Weight	1750 g (w/o mounting bracket and antennas)

Table 5 - Device Dimensions

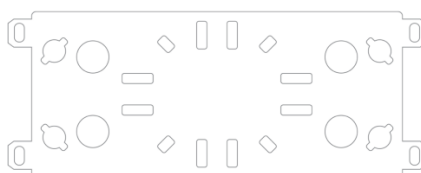


Figure 3 – NTC-30WV Mounting Bracket

NTC-30WV MOUNTING BRACKET	
Length	110 mm
Depth	12 mm
Height	290 mm
Weight	410 g (w/o NTC-30WV attached)

Table 6 - Mounting Bracket Dimensions



Figure 4 - NTC-30WV Antenna

NTC-30WV 3G AND WIFI ANTENNA	
Length	180 mm
Diameter	20 mm
Weight	60 g (w/o NTC-30WV attached)

Table 7 - Antenna Dimensions

## Interfaces

The following interfaces are available on the NTC-30WV:

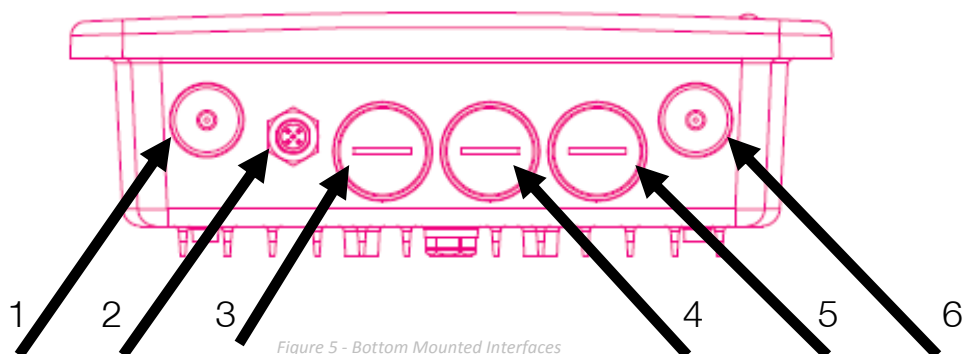


Figure 5 - Bottom Mounted Interfaces

ITEM	INTERFACE	FUNCTION
1	WiFi Antenna Connector (TNC)	Connect one of the WiFi antennas here.
2	DC Power Port	Connect the optional DC Power supply to the NTC-30WV.
3	10/100Base-TX Ethernet RJ-45 (w/Auto MDX) Port	Connect the NTC-30WV to an Ethernet enabled device or Switch and deliver power through Power over Ethernet (PoE) technology.
4	RJ-11 Port.	An analogue phone handset can be connected to the RJ-11 to make calls over the 3G network.
5	Mini USB 2.0 Console Port	Connect a Mini USB cable to access the NTC-30WV console.
	Reset	Reset the NTC-30WV to Factory Defaults.
	SIM Card Reader	Insert an active SIM to provide 3G connectivity.
6	WiFi Diversity Antenna Connector (TNC)	Connect one of the WiFi antennas here.

Table 8 - Bottom Mounted Integrated Interfaces

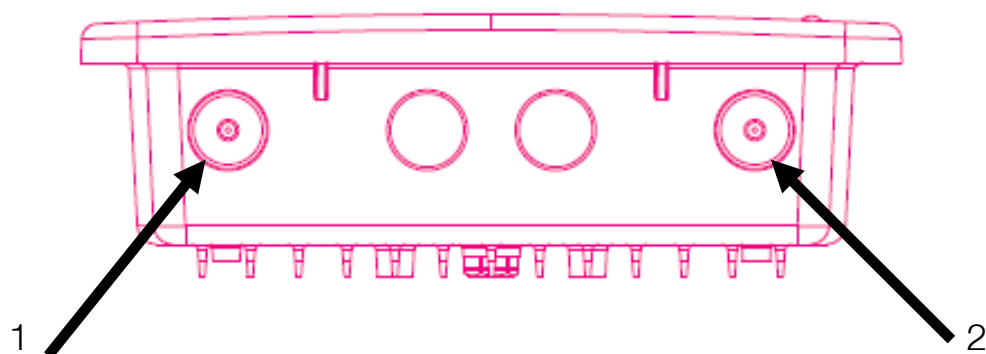


Figure 6 - Top Mounted Interfaces

ITEM	INTERFACE	FUNCTION
1	1 x 3G Main antenna connector (Type N)	Connect one of the 3G antennas here.
2	1 x 3G Aux antenna connector (Type N)	Connect one of the 3G antennas here.

Table 9 - Top Mounted Interfaces

# NTC-30WV Default Settings

The following tables list the default settings for the NTC-30WV.

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

Table 10 - LAN Management Default Settings

WIRELESS (WIFI)	
SSID:	NetComm XXXX (where XXXX is 4 random numbers)
Security:	WPA2-PSK
Security Key:	XXXXXXXXXX (where XXXXXXXXXXX are 10 random characters)

Table 11 – 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 12 - Web Interface Default Settings



Note: The admin manager account allows you to manage most of the settings of the router except functions such as Firmware Upgrade, Device Configuration Backup, Mobile Broadband Connection settings, and Reset to Factory Default Settings, which are privileged only to the root manager account. First time users should use the root manager account to configure Mobile Broadband settings.

## Restoring Factory Default Settings

Restoring the NTC-30WV factory default settings will erase any configuration changes you have made. You may encounter situations where you need to restore the factory defaults on your router, 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-30WV:

- 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-30WV 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

Hold the reset button down until all LEDs on the front panel of the router stop flashing simultaneously and then release the button. The router will restore the factory default settings and reboot.

Once you have reset your NTC-30WV 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` and password `admin`.

# Implementation and Deployment Scenario

The NTC-30WV is a robust 3G (DC-HSPA+ ) router that connects to the 3G network and is mounted either on the wall or a pole and positioned in an optimal position on the outside of a property. The NTC-30WV features a powerful antenna system and radio modem together in the one unit in an outdoor location. This tight integration between the radio receiver and antenna system in an outdoor unit provides great benefits to signal strength compared with alternate separated solutions involving signal degradation along lengthy antenna cabling.

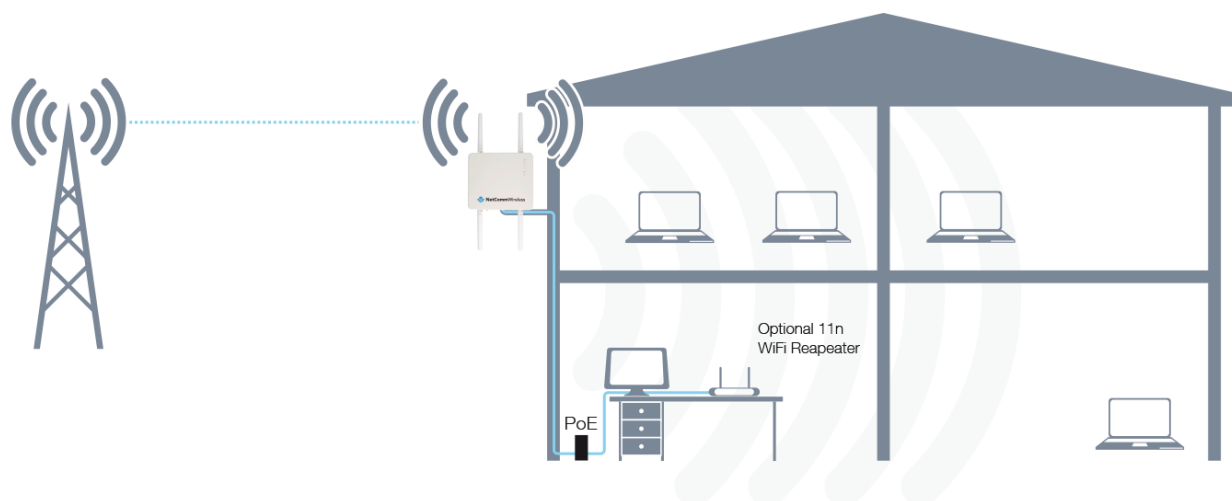


Figure 7 - Typical NTC-30WV Deployment - House

Power is delivered to the outdoor router via Power over Ethernet technology (as shown above) making installation quick and easy as there is no power source required at the outdoor mount point, and both power and data can be provided via a single cable from inside the property. With an IP67 rated enclosure, the device also withstands diverse temperature and weather environments. Utilising an 802.11n WiFi repeater further increases the WiFi range of the NTC-30WV meaning a wireless connection is possible in all corners of your house or property.

The NTC-30WV is able to be mounted either to a pole or secured directly to a wall, allowing flexibility in the choice of an installation location.

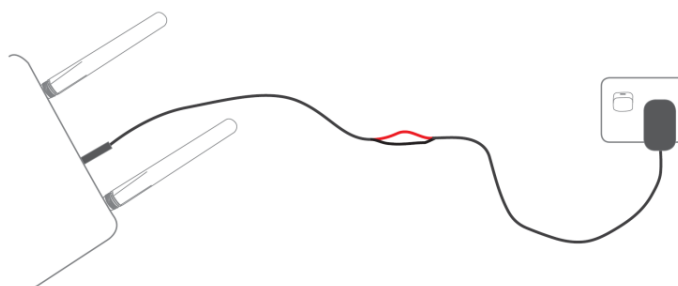
# Installation and Configuration of the NTC-30WV

## Hardware Installation

Please refer to the NTC-30WV Installation Guide (available from the NetComm Wireless website) for instructions on assembling, mounting and placing the NTC-30WV.

## Powering the Router via DC Power Supply

Below is a diagram summarising the assembly when connecting via DC power supply. Please refer to page 7 of the Quick Start Guide for more detail on how to connect the NTC-30WV via DC Power Supply.



*Figure 8 - Example of how to connect the NTC-30WV when connecting via DC power supply*

## Powering the Router via a Power over Ethernet (PoE) Cable (Optional)

Please refer to the Installation Guide for step-by-step instructions on connecting the devices. Below is a diagram summarising the assembly when connecting via optional Power over Ethernet cable.

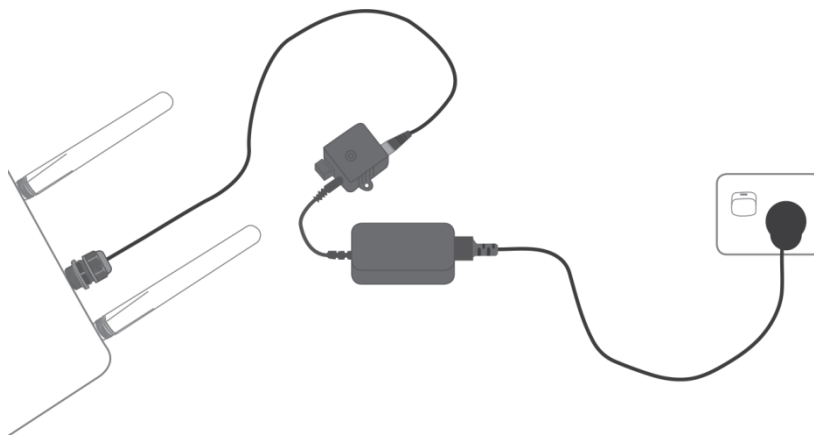


Figure 9 – Example of how to connect the NTC-30WV when connecting via optional Power over Ethernet (PoE) cable



Note: The DC Injector supplies 48V. Do not use this power supply for anything except for powering the outdoor gateway.

### Captive Power Terminal Block

The following table displays the pin outs for the Locking Power Block on the PoE Injector.



Figure 10 - Locking Power Terminal Block

PIN	SIGNAL	DESCRIPTION
1	V+	Voltage+
2	GND	Ground
3	V-	Voltage-

Table 13 - Locking Power Block Pin Outs



Figure 11 - Assembly of the PoE Injector and the Captive Terminal Block



## Connecting wirelessly

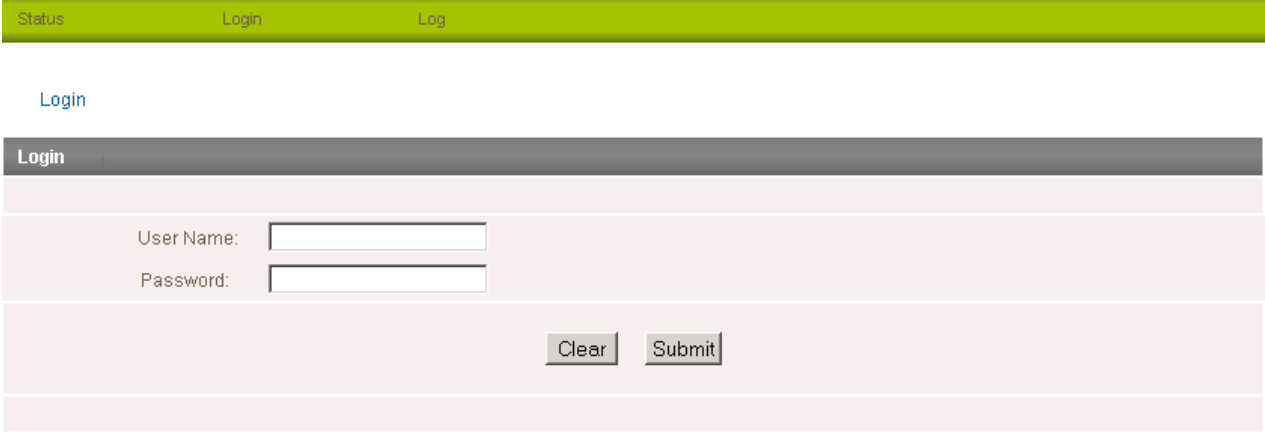
1. Ensure WiFi is enabled on your device (e.g. computer/laptop/smartphone).
2. Scan for wireless networks in your area and connect to the network name that matches the Wireless network name configured on the NTC-30WV. The default wireless network name is printed on the security card included in the package.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

## Configuring the NTC-30WV

### Logging on via the web-based user interface

To log in to the management console and view the status and make changes to your NTC-30WV, please follow the steps below:

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



The screenshot shows the web-based user interface for the NTC-30WV router. It features a green navigation bar at the top with three tabs: 'Status', 'Login', and 'Log'. Below the navigation bar, there is a 'Login' link. The main content area has a 'Login' header, followed by 'User Name:' and 'Password:' labels next to input fields. At the bottom are 'Clear' and 'Submit' buttons.

Figure 12 - Login prompt for the Web based User Interface

After logging in, the Status page is displayed.

## Status

The status page provides system related information and is displayed when you login to the NTC-30WV management console. By default, the status page will show System Information, Ethernet Port Status, WWAN Status, IPsec Status and the 3G service connection details.

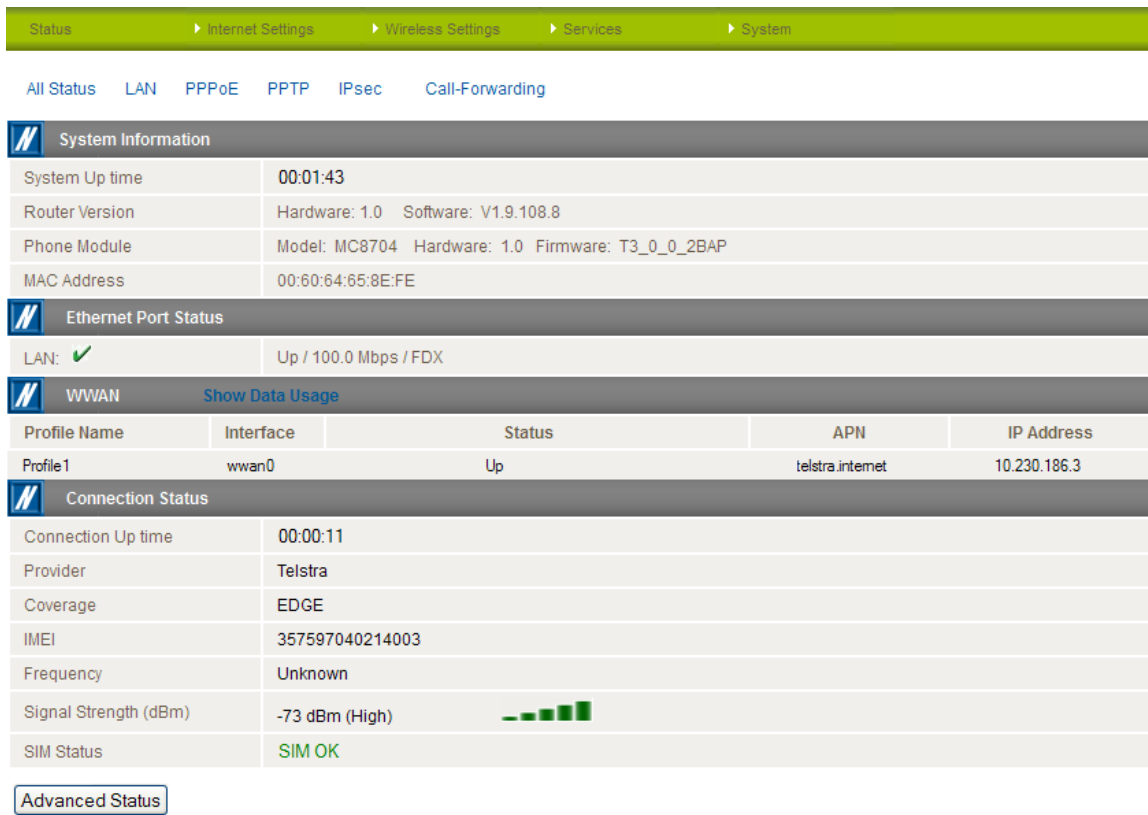


Figure 13 - The Status Page

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, the firmware version of the module and the current module temperature.
MAC Address	The MAC Address of the router which serves as a unique identifier of network devices.
Ethernet Port Status	The current speed and status of the Ethernet port.
WWAN	The current connection profile, Interface, status, APN, and local address of the WWAN connection.
IPsec	The current connection profile, Interface, status, Local LAN address, Remote Gateway address, Remote LAN address and the status of the IPsec connection. If none are configured, this should be empty.
Provider	The current 3G service provider detected.
Coverage	The type of 3G connection available for use.
IMEI	The IMEI of the router.
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 14 - Status page items

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

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

Figure 14 - 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 15 - Status Page - LAN Details

PPPoE	
PPPoE Status	DISABLED
PPPoE IP Address	N/A

Figure 15 - 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 16 - Status Page - PPPoE Details

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

Figure 16 - 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 17 - Status Page - PPTP Details

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

Figure 17 - Status Page - IPSec Details

ITEM	DEFINITION
No.	The IPSec tunnel number.
Profile Name	The name assigned to the IPSec profile.
Interface	The current interface used by the IPSec tunnel.
Local LAN	The local IP address making up one end of the IPSec tunnel.
Remote Gateway	The WAN gateway of the other end of the IPSec tunnel.
Remote LAN	The WAN IP Address that the IPSec tunnel is connecting to.
Status	The current condition of the IPSec tunnel.

Table 18 - 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 18 - Status Page - Call Forwarding Status Details



ITEM	DEFINITION
Call Waiting	Displays the status of the call waiting function.
Unconditional Call Forwarding	Displays the status of unconditional call forwarding. Unconditional call forwarding is a forward placed on all calls as soon as they reach the phone, regardless of the status of the handset.
Busy Call Forwarding	Displays the status of the busy call forwarding function and the destination calls are forwarded to in the case where the phone is busy and an incoming call is received.
No-Reply Call Forwarding	Displays the status of the no-reply call forwarding function and the destination calls are forwarded to in the case that a call is received and goes unanswered.
Not Reachable Call Forwarding	Displays the status of the not reachable call forwarding function and the destination calls are forwarded to in the case that a call can't be routed to a handset.

Table 19 - Status Page - Call Forwarding Status Details

## Advanced Status

To view further information regarding the phone module onboard the gateway and the current connection press the “Advanced Status” button.

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

[Status > Advanced Status](#)

Module Information	
Phone Module	Model: MC8704 Hardware: 1.0 Firmware: T3_0_0_2BAP R474 CNSZXD00000128 2011/11/25 10:13:57
Module Boot Version	T3_0_0_2BBT R474 CNSZXD00000128 2011/11/25 10:13:57
Module PRIID	Revision: 1.0 PRI Part Number: 9901561
System Up time	00:47:13

Connection Status	
Provider	Telstra
Country Code	505
Network Code	1
Coverage	UMTS
Connection Status	Up
IMEI	357597040214003
Frequency	WCDMA850
Signal Strength	-73 dBm
Signal Quality (Ec/Io)	-22 dB
Received Signal Code Power (RSCP)	-78 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	19796
Channel Number	4412

Figure 19 - Advanced Status Page

ITEM	DEFINITION
Phone Module	The phone module name, hardware and firmware version
Module Boot version	The installed bootloader version of the phone module.
Module PRID	The Protocol ID of the phone module.
System Uptime	The time in minutes and seconds that the gateway 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.
Coverage	The coverage type of 3G service the current connection is using.
Connection Status	The current status of the gateway'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 (Echo/Location)	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. A unique number up to 19 digits in length.
Primary Scrambling Code (PSC)	The Primary Scrambling Code for the current signal.
Location Area Code (LAC)	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 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 of the current 3g signal.
Channel Number	The channel number of the current 3G connection.

Table 20 - Advanced Status Page

## Internet Settings

This section describes how to set up the router to initiate a WWAN connection. There are 2 different ways to set up a WWAN 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="password"/>
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		

Save

Figure 20 - 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. Select each connection profile and disable the Auto Connection option then save the updated settings.

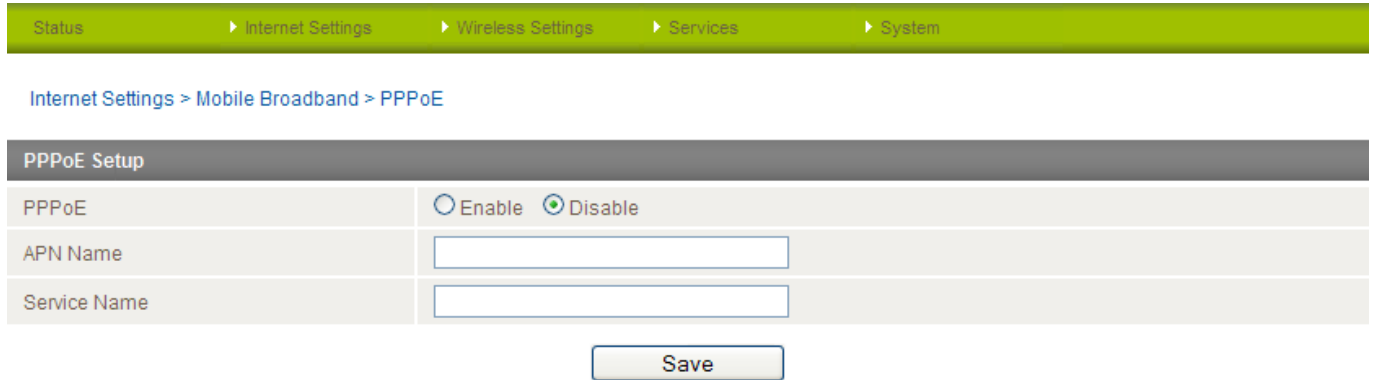


Figure 21 - PPPoE Settings

1. Select “Enable” to enable PPPoE.
2. Specify the APN supplied by your 3G provider.

(Optional)

3. Specify a “Service Name”.

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 enables you to scan for available network operators in your area.

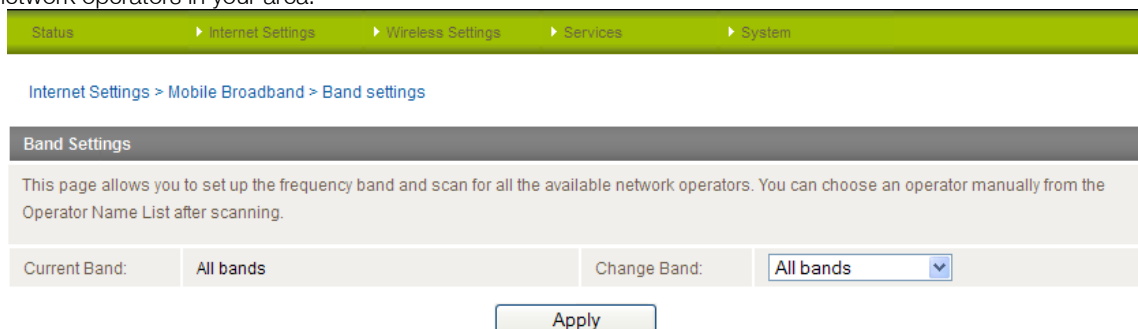


Figure 22 - Band / Provider Selection

You may want to do this if you're using the router in a country with multiple 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

In most cases it is not necessary to change the default setting of "All bands". 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.

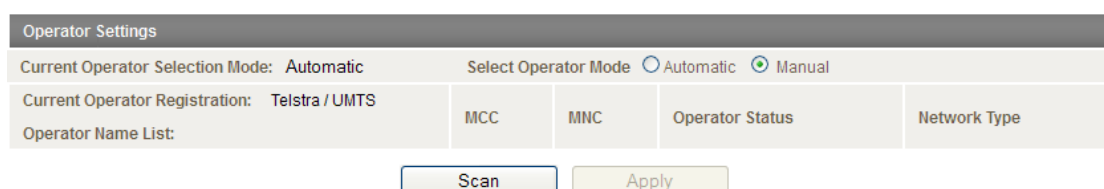


Figure 23 - Manual Operator Selection

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

If the SIM card is locked you will need to unlock it with a PIN provided with your SIM card.

You can find out if the SIM is locked by viewing the SIM Status on the Status page:

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

Figure 24 - SIM Security - Status Page Warning

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

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

Internet Settings > WWAN (3G) > SIM Security

PIN Settings	
SIM Status	<b>SIM PIN</b>
Number of Retries Remaining	
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>
Remember PIN: <b>Disabled</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
PIN Protection: <b>Enabled</b>	<input type="button" value="Disable PIN"/>
<input type="button" value="Save"/> <input type="button" value="Help"/>	

Figure 25 - SIM Security - SIM PIN Needed

2. 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.

3. 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.

PIN Settings

PIN Settings	
SIM Status	<b>ENTER PUK</b>
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>
PUK	<input type="text"/>
Confirm PUK	<input type="text"/>
Remember PIN	<input checked="" type="radio"/> Yes <input type="radio"/> No
Disable PIN	<input type="radio"/> Yes <input checked="" type="radio"/> No
<input type="button" value="Save"/> <input type="button" value="Help"/>	

Figure 26 - 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.

## IP Setup

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

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

[Internet Settings](#) > [LAN](#) > [IP Setup](#)

LAN Configuration	
Ethernet IP Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
Ethernet Subnet Mask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
DNS Masquerade	
DNS Masquerade	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Figure 27 - 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".



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 LAN](#)   [Services](#)   [System](#)

[All Items](#)   [DHCP Relay Configuration](#)

 **DHCP Configuration**

DHCP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DHCP Start Range	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="100"/>
DHCP End Range	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="199"/>
DHCP Lease Time	<input type="text" value="86400"/> (seconds)
Default Domain Name Suffix	<input type="text"/>
DNS Server 1 IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
DNS Server 2 IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
WINS Server 1 IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
WINS Server 2 IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
NTP Server (Option 42)	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
TFTP Server (Option 66)	<input type="text"/>
Option 150	<input type="text"/>
Option 160	<input type="text"/>

 **Address Reservation List**

Computer Name	MAC Address	IP Address	
			<input type="button" value="Add"/>

 **Dynamic DHCP Client List**

Computer Name	MAC Address	IP Address	Expire Time

Figure 28 - DHCP Settings

After entering the applicable details, click the “Save” button.

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	
<input type="text"/>	<input type="text"/>	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>	<input type="button" value="Add"/>
			<input checked="" type="checkbox"/> Enable <input type="button" value="Remove"/>

Figure 29 - DHCP Settings - Fixed Mapping

1. Click the “Add” button.
2. Enter a name for the computer or device into the “Computer Name” textbox.
3. Enter the computer’s or device’s MAC address into the “MAC Address” textbox.
4. Enter the IP address you wish to assign to the device in the IP Address text boxes.
5. Select the Enable checkbox to enable the rule.
6. Click the “Save” button to save the new settings.

## 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

**Enabled Profile List**

Profile Name	Interface Name	IP Address	Default Route	NAT Masquerading
Enabled Profile List is empty				

**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	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>						
Subnet Mask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>						
Gateway IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>						
Network Interface	auto <input type="button" value="v"/>						
Metric	<input type="text"/> (0-65535)						
<input type="button" value="Add"/>							

Item No.	Route Name	Destination IP	Subnet Mask	Gateway IP	Network Interface	Metric	
0	Static Route 1	192.168.1.3	255.255.255.0	192.168.1.1	auto	1	<a href="#">Delete Entry</a>

**Active Routing Table**

Item No.	Destination IP	Subnet Mask	Gateway IP	Network Interface	Metric	Flags	Ref	Use
0	192.168.1.0	255.255.255.0	0.0.0.0	br0	0	U	0	0

Figure 30 - 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 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 LAN ▶ Services ▶ System

Internet Settings > Routing > RIP

RIP Routing	
RIP Enable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Version	<input type="text" value="2"/>
<input type="button" value="SAVE RIP"/>	

Figure 31 - RIP Settings

1. Click the Enable option on the RIP Page.
2. Select the RIP version you wish to use.
3. Click the "Save RIP" button to save the settings.

## 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 32 - VRRP Settings

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



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](#)

Enabled Profile List				
Profile Name	Interface Name	IP Address	Default Route	NAT Masquerading
Enabled Profile List is empty				

IP Mapping Settings	
Item No.	<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"/> to <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"/> to <input type="text"/> (1-65535)

Item No.	Protocol	Source IP Address	Incoming Port Range	Destination IP Address	Destination Port Range
The IP mapping table is empty					

Figure 33 - NAT Settings

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

## How to configure Port Forwarding

OPTION	DEFINITION
Mapping no	Number to identify the port mapping, numbered from 1 to as many as needed.
Protocol	Specify the protocol to use for the port mapping. Options include TCP, UDP and All protocols.
Source IP Address	This field 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	This field specifies the external port(s) to listen to.
Destination IP Address	The Local Area Network Address of device to forward inbound requests to.
Destination Port Range	The Local Area Network Port(s) to forward connections to.

Table 21 - NAT Configuration Items

1. Enter the IP Mapping configuration information as appropriate.
2. Click the "Save" button to save any changes to the settings.



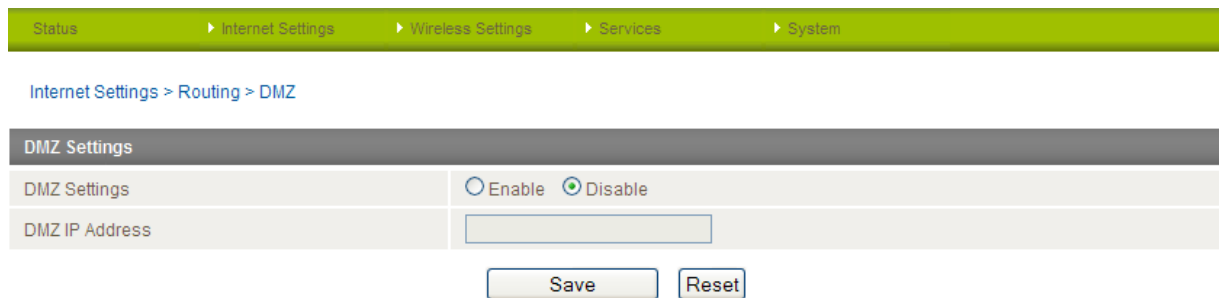
Note: If the "Incoming Port Range" specifies a single port (as above) then the destination port can be set to any port. If the "Incoming Port Range" specifies a range of port numbers then the "Destination Port Range" MUST be the same as the "Incoming Port Range".

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 34 - DMZ Settings

1. Click the "Enable" button.
2. Enter the IP Address of the device you wish to become the DMZ host.
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 tunnel needs to be encapsulated and as such is generally not visible to public networks.

The advantages of a VPN connection include:

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

### How to configure a VPN connection

Move your mouse over the **Internet Settings** menu and then move your mouse over **VPN**. You can select from the following types of VPN connection:

- IPSec
- PPTP-Client
- OpenVPN
- GRE

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.

Status		Internet Settings		Wireless Settings		Services		System	
Internet Settings > VPN > IPSec									
<b>VPN IPsec Edit</b>									
Enable This IPsec Profile	<input checked="" type="radio"/> Enable <input type="radio"/> Disable								
Profile Name	<input type="text"/>								
<b>Remote Gateway</b>									
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					
<b>Local LAN</b>									
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					
<b>Negotiation</b>									
Encap Protocol	ESP								
IKE Mode	Main								
Pfs	On								
IKE Encryption	Any								
IKE Hash	Any								
IPsec Encryption	Any								
IPsec Hash	Any								
DH Group	Any								
DPD Action	Hold								
DPD Keep Alive Time	<input type="text"/> 10							secs	
DPD Timeout	<input type="text"/> 60							secs	
Ike Rekey Time	<input type="text"/> 3600							(0-78400, 0=Unlimited) secs	
SA Life Time	<input type="text"/> 28800							(0-78400, 0=Unlimited) secs	
Key Mode	Pre Shared Key								
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)	
<input type="button" value="Save"/> <input type="button" value="Exit"/>									

Figure 35 - VPN - IPSec Settings page

Please view the IPSec field descriptions on the following page.

## VPN - IPsec Field Descriptions

ITEM	DEFINITION
Profile Type	Select the type of VPN connection to use.
Enable VPN	Enable or Disable the VPN connection.
Profile Name	A name used to identify the VPN connection.
Remote IPsec Gateway	The IP address that the IPsec server is running on.
Road Warrior	Click this to configure the VPN connection for Road Warrior (connection from a dynamic IP Address) use.
Remote Address/Net to Join	Enter the Remote IP address or Network for use on the VPN connection.
Remote Address/Net Mask	Enter the subnet mask 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 subnet mask 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 (Dead Peer Detection) Action to use on the VPN connection.
DPD Keep Alive Time	The time in seconds to keep alive a VPN tunnel where DPD has detected a dead peer.
DPD Timeout	The time in seconds before DPD will 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"> <li>• Pre Shared Key</li> <li>• RSA Keys</li> <li>• Certificates</li> </ul> <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>

## 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.

Status
Internet Settings
Wireless LAN
Services
System

VPN

VPN Edit

Profile Type
OpenVPN

Enable VPN
☒ Enable
☐ Disable

Profile Name

OpenVPN Type
Server

Server Port
1194
UDP

VPN Network Address
10.0.0.0

VPN Network Mask
255.255.255.0

Diffie-Hellman parameters
Generate DH...

Server Certificates

Not Before: N/A
Not After: N/A
Country:
State:
City:
Organization:
Email:
Generate CA certificate...

Authentication Type
☒ Certificate
☐ User Name / Password

Certificate Management

Certificate: New...
Name:
Country:
State:
City:
Organization:
Email:
Generate
Download
Revoke
Network address:
Network Mask:
Set Network Information

Save
Exit

Figure 36 - VPN Connection Settings - OpenVPN

ITEM	DEFINITION
Profile Type	Select the type of VPN connection to use.
Enable VPN	Enable or Disable the VPN connection.
Profile Name	A name used to identify the VPN connection.
OpenVPN Type	Select the type of OpenVPN session to use.
Server Port	Enter the port the OpenVPN server is running on.
VPN Network Address	Enter the network address for use on the VPN connection.
VPN Network Mask	Enter the network mask for use on the VPN connection.
Diffie-Hellman parameters	Generate the server and client keys used by the VPN connection.
Server Certificates	Enter the applicable details to identify the OpenVPN server and create a CA certificate based on this information.
Authentication Type	<p>Select the type of authentication in use for the VPN connection. You can select from:</p> <ul style="list-style-type: none"> <li>• Certificate</li> <li>• User Name / Password</li> </ul> <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 22 - 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.

Status ▶ Internet Settings ▶ Wireless Settings ▶ Services ▶ System

[Internet Settings > VPN > PPTP-Client](#)

VPN PPTP Client Edit

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	<input type="text" value="Any"/> ▼
Metric	<input type="text" value="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	<input type="text" value="30"/> (30-65535) secs
Reconnect Retries	<input type="text" value="0"/> (0-65535, 0=Unlimited)

Figure 37 - VPN Connection Settings - PPTP

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

Table 23 - PPTP Configuration Items



## GRE

When you select GRE, a list of configured GRE VPNs is displayed. Click the “Add” button to configure a GRE VPN connection.

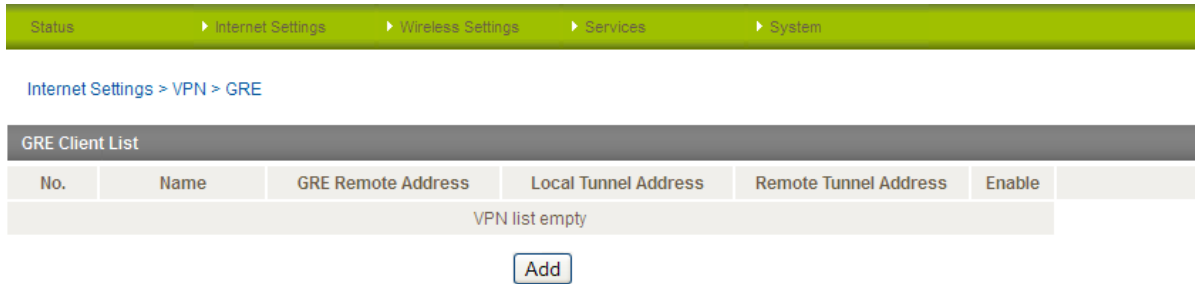


Figure 38 - GRE VPN List

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco that works in conjunction with PPTP to create a virtual private network.

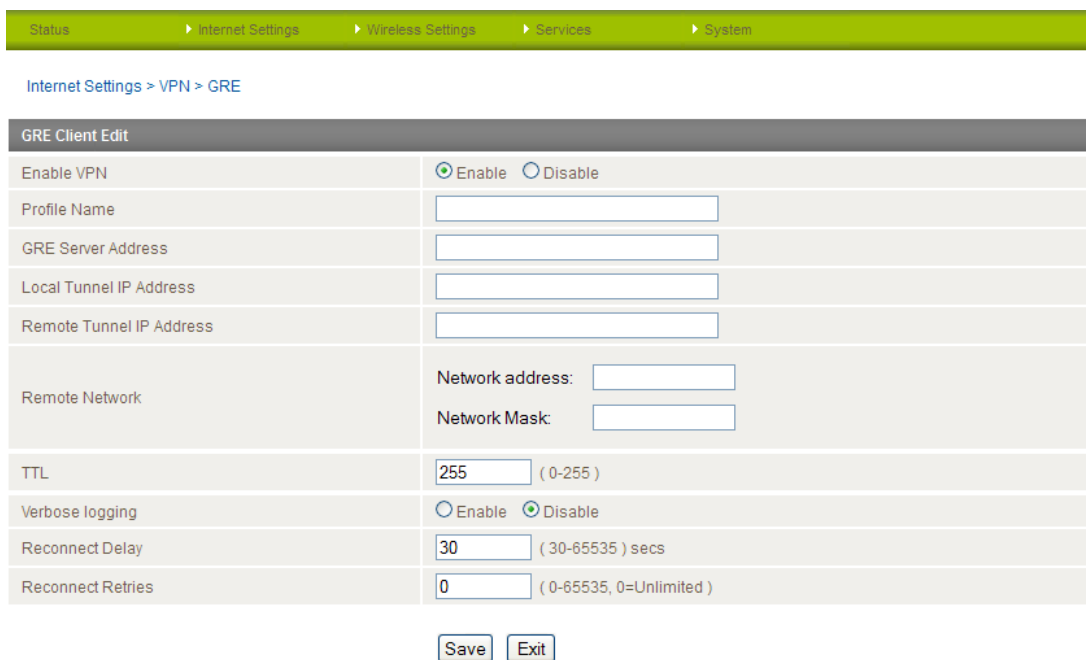


Figure 39 - GRE VPN Settings

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 IP Address	The Local IP address of the VPN tunnel.
Remote Tunnel IP 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 24 - GRE VPN 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	<b>Inactive</b>
Response from network	<div></div>
Send Message	<input type="text" value="Enter USSD dial string here"/> <input type="button" value="Start Session"/>

Figure 40 - 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

### Basic

The basic configuration page is used to define the basic wireless settings for the NTC-30WV such as the SSID and the type of 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: 3	
Security Settings	
SSID:	NetComm 8361
Network Authentication:	WPA2-PSK
WPA Pre-Shared Key:	•••••••• <a href="#">Click here to display</a>
WPA Group Rekey interval:	600
WPA Encryption:	AES
Wireless Distribution System (WDS)	
MAC address	00:60:64:65:8e:ff
WDS Mode	Disable

Save

Figure 41 - 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-30WV and you will not be able to connect wirelessly.
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"> <li>11 b/g mixed mode</li> <li>11b only</li> <li>11g only</li> <li>11n only</li> <li>11 b/g/n mixed mode</li> </ul> If you are not sure which protocol to use set this option to 11 b/g/n mixed mode.
Frequency	The frequency or wireless channel that the router is broadcasting with. Recommended channels are 1, 6 or 11.
SSID	The SSID (Service Set Identifier) aka network name in use for the wireless network.
Network Authentication	The wireless security settings for the router. Please see below for further details.
WPA Pre-Shared Key	The wireless password in use by the router.
WPA Group Rekey interval	This is the time in seconds before a new key is generated.
WPA Encryption	The type of WPA encryption used with the wireless security settings.
MAC Address	The MAC Address of the Wireless Access Point.
WDS Mode	Set Wireless Distribution System (WDS) to enable or disable.

Table 25 - Wireless Configuration - Basic Configuration Items

Click 'Apply' to save the settings.

## Security Settings

You may choose from the following wireless security options:

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

### WPA1/WPA2

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

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

Figure 42 - Advanced View – WiFi Security Settings - WPA1/WPA2

### WPA-PSK/WPA2-PSK

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



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

Security Settings	
SSID:	NetComm XXXX
Network Authentication:	WPA2-PSK
WPA Pre-Shared Key:	<div>••••••••</div> <a href="#">Click here to display</a>
WPA Group Rekey interval:	600
WPA Encryption:	AES

Figure 43 - Advanced View – WiFi Security Settings - WPA-PSK/WPA2-PSK



Note: Your NTC-30WV uses WPA2-PSK by default. Check the Wireless Security Card or the device label on the bottom of the NTC-30WV for your default SSID and Security key to begin connecting your wireless devices.

## 802.1x

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

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

Figure 44 - 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:

Status				
Internet Settings				
Wireless Settings				
Services				
System				
All Status LAN PPPoE PPTP IPsec Call-Forwarding				
<b>System Information</b>				
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			
<b>Ethernet Port Status</b>				
LAN:	Up / 100.0 Mbps / FDX			
<b>Mobile Broadband (MBB)</b> <a href="#">Show data usage</a>				
Profile Name	Interface	Status	APN	IP Address
Profile1	wwan0	Up	telstra.internet	10.166.96.37
<b>Connection Status</b>				
Connection Up Time	00:01:56			
Provider	Telstra			
Coverage	UMTS			
IMEI	357597040032884			
Frequency	WCDMA850			
Signal Strength (dBm)	-69 dBm (High)			
SIM Status	SIM OK			
<a href="#">Advanced Status</a>				

Figure 45 - WDS - Access Point 1 Status

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

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

Figure 46 - WDS - Access Point 1 LAN IP Setup

- Enable the DHCP Server on Access Point 1:

<a href="#">Status</a> <a href="#">Internet Settings</a> <a href="#">Wireless Settings</a> <a href="#">Services</a> <a href="#">System</a>				
Internet Settings > LAN > DHCP				
<b>DHCP Configuration</b>				
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 47 - 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) <span>Current Channel: 1</span>
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 48 – 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"> <li>11 b/g mixed mode</li> <li>11b only</li> <li>11g only</li> <li>11n only</li> <li>11 b/g/n mixed mode</li> </ul> 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 26 - 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.



System Information

System Up Time	01:57:28
Router Version	Hardware: 1.0 Software: V1.10.10.0
Phone Module	Model: MC8704 Hardware: 1.0 Firmware: T3_0_0_2BAP
MAC Address	00:60:64:65:8E:FE

Ethernet Port Status

LAN:	Up / 100.0 Mbps / FDX
------	-----------------------

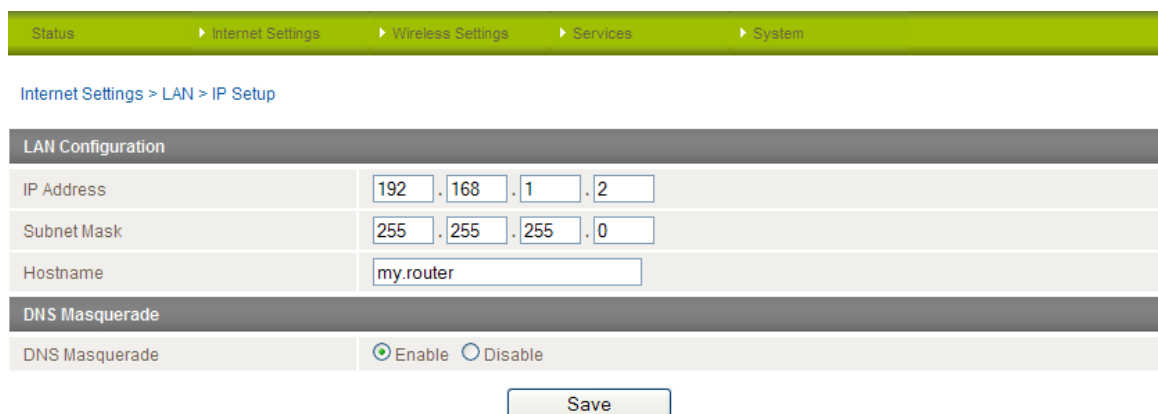
Mobile Broadband (MBB) [Show data usage](#)

Profile Name	Interface	Status	APN	IP Address
Connection Status				
Connection Up Time	00:00:00			
Provider	Limited Service			
IMEI	357597040214003			
Frequency	WCDMA850			
Signal Strength (dBm)	-67 dBm (High)			
SIM Status	SIM removed			

[Advanced Status](#)

Figure 49 – WDS - Access Point 2 Status

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



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
----------------	---

[Save](#)

Figure 50 - 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		Add
DHCP Client List				
Computer Name	MAC Address	IP Address	Expire Time	

Save

Figure 51 - 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) ▼ <span style="float: right;">Current Channel: 1</span>
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:	<input type="text"/>
Network Key 3:	<input type="text"/>
Network Key 4:	<input type="text"/>
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	<input type="text"/>
AP MAC Address3	<input type="text"/>
AP MAC Address4	<input type="text"/>

Figure 52 - WDS – Access Point 2 Repeater Mode Setup

The Wireless Distribution System setup is now complete.

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

Apply
Reset

Figure 53 - Wireless Settings – Advanced

OPTION	DEFINITION
BG Protection Mode	A protective measure 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 gateway cancels the session and defines the wireless client as not connected.
Beacon Interval:	Interval of time in which the wireless gateway broadcasts a beacon which is used to synchronize the wireless network.
Data Beacon Rate (DTIM)	Enter a value in milliseconds between 1 and 255 for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
Fragmentation Threshold	This specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
RTS Threshold	When the packet size is smaller than the RTS threshold, the wireless gateway will not use the RTS/CTS mechanism to send this packet.
TX Power	This determines the 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.
Broadcast Network Name (SSID)	Use this to show or hide the SSID (wireless network name) of your router.

Table 27 - Wireless Settings - Advanced Configuration Items

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

## MAC / IP / Port Filter

The Wireless LAN MAC / IP / Port filter feature ensures the network accessibility for the wireless client devices can be controlled. When the MAC/IP/Port filter is enabled with a default policy of “Accepted”, the rules that are created indicate which packets to drop while all packets not listed are accepted. When the MAC/IP/Port filter is enabled with a default policy of “Dropped”, the rules that are created indicate which packets to accept while all other packets not listed are dropped. You can create up to 20 rules to control wireless client access.

The HTTP port (80) is enabled by default, allowing access to the web user interface from any wireless client. If you want to restrict access to the web user interface, set this to “Disable” and create a rule to allow access to port 80 for at least one client so that you do not become locked out of the web user interface.

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

[Internet Settings](#) > [Routing](#) > [MAC / IP / Port Filtering](#)

### MAC / IP / Port Filtering

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

#### Basic Settings

MAC / IP / Port Filtering	<input type="button" value="Disable"/>
Default Policy -- The packet that didn't match with any rules would be:	<input type="button" value="Dropped"/>
Allow HTTP(S) Port Always	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Allow Telnet Port Always	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

#### MAC / IP / Port Filter Settings

Source MAC Address	<input type="text"/>
Source IP Address(/Subnet Mask)	<input type="text"/>
Source Port Range	<input type="text"/> - <input type="text"/>
Destination IP Address(/Subnet Mask)	<input type="text"/>
Destination Port Range	<input type="text"/> - <input type="text"/>
Protocol	<input type="button" value="None"/>
Action	<input type="button" value="Accept"/>
Comment	<input type="text"/>

(The maximum rule count is 20.)

#### Current MAC / IP /Port Filtering Rules

Delete	Source MAC Address	Source IP Address (/Subnet Mask)	Destination IP Address (/Subnet Mask)	Protocol	Source Port Range	Destination Port Range	Action	Comment	Packet Count

Packets dropped

Figure 54 - Wireless Settings – MAC / IP / Port Filter

Enter the required details for your rule and click “Save”. The details of the rule appear in the bottom section of the screen. You can select individual rules and delete them.

## Station List

The Station List page shows the number of devices currently connected to your NTC-30WV via WiFi. 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

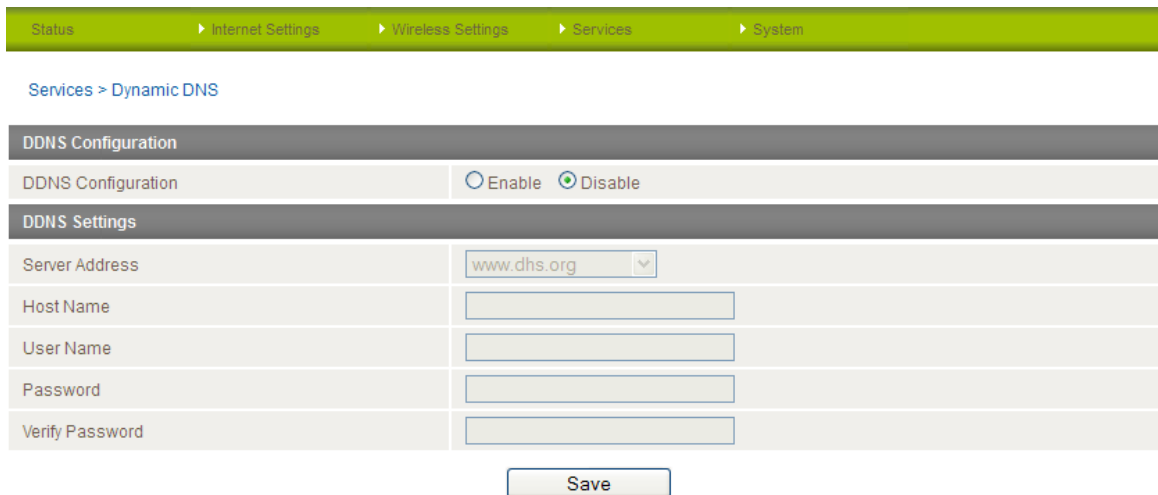
MAC address	IP Address	Host Name	RSSI	PSM	BW	Connected Time
-------------	------------	-----------	------	-----	----	----------------

Figure 55 - Wireless Station List

## Services

### Dynamic DNS

The Dynamic DNS page is used to configure the Dynamic DNS feature of the router. There are a number of dynamic DNS hosts from which you can choose.



The screenshot shows the router's configuration interface. At the top is a navigation bar with links: Status, Internet Settings, Wireless Settings, Services, and System. Below this is a breadcrumb trail: Services > Dynamic DNS. The main section is titled 'DDNS Configuration'. It contains a 'DDNS Configuration' field with radio buttons for 'Enable' and 'Disable', where 'Disable' is selected. Below this is a 'DDNS Settings' section with several input fields: 'Server Address' (a dropdown menu showing 'www.dhs.org'), 'Host Name', 'User Name', 'Password', and 'Verify Password'. At the bottom of this section is a 'Save' button.

Figure 56 - DDNS Settings

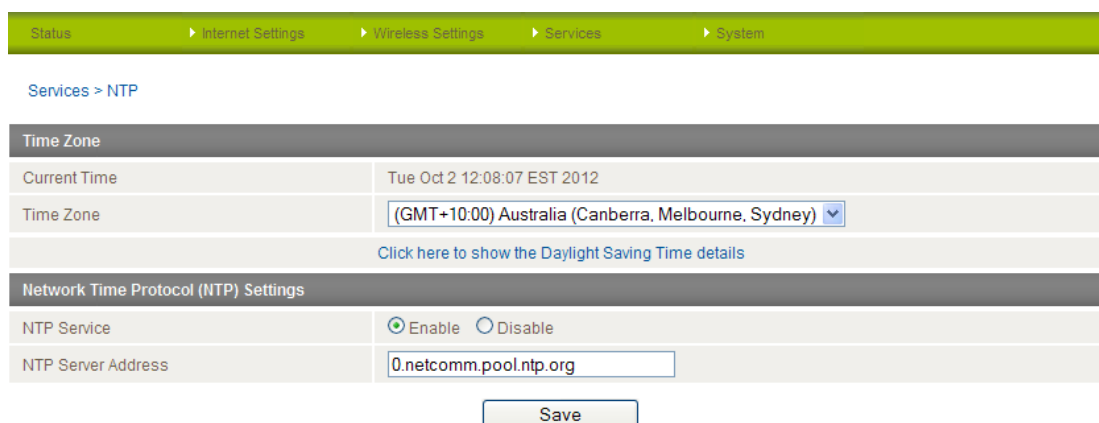
Dynamic DNS provides a method for the router to update an external name server with the current WAN IP address.

To configure dynamic DNS:

1. Select 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 any changes to the settings.

## NTP

The NTP page is used to configure the local time zone and to select the NTP server used for synchronisation.



The screenshot shows the router's configuration interface for NTP settings. At the top is a navigation bar with links: Status, Internet Settings, Wireless Settings, Services, and System. Below this is a breadcrumb trail: Services > NTP. The main section is titled 'Time Zone'. It contains a 'Current Time' field showing 'Tue Oct 2 12:08:07 EST 2012'. Below this is a 'Time Zone' dropdown menu showing '(GMT+10:00) Australia (Canberra, Melbourne, Sydney)'. A link 'Click here to show the Daylight Saving Time details' is also present. Below this is a 'Network Time Protocol (NTP) Settings' section. It contains an 'NTP Service' field with radio buttons for 'Enable' and 'Disable', where 'Enable' is selected. Below this is an 'NTP Server Address' field showing '0.netcomm.pool.ntp.org'. At the bottom of this section is a 'Save' button.

Figure 57 - NTP Settings

The NTP (Network Time Protocol) settings allow your router to synchronise its internal clock with a global Internet Time server. This setting will affect functions such as System Log entries and Firewall settings where the current system time is displayed. You can use the default NTP server or enter one manually if required.

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

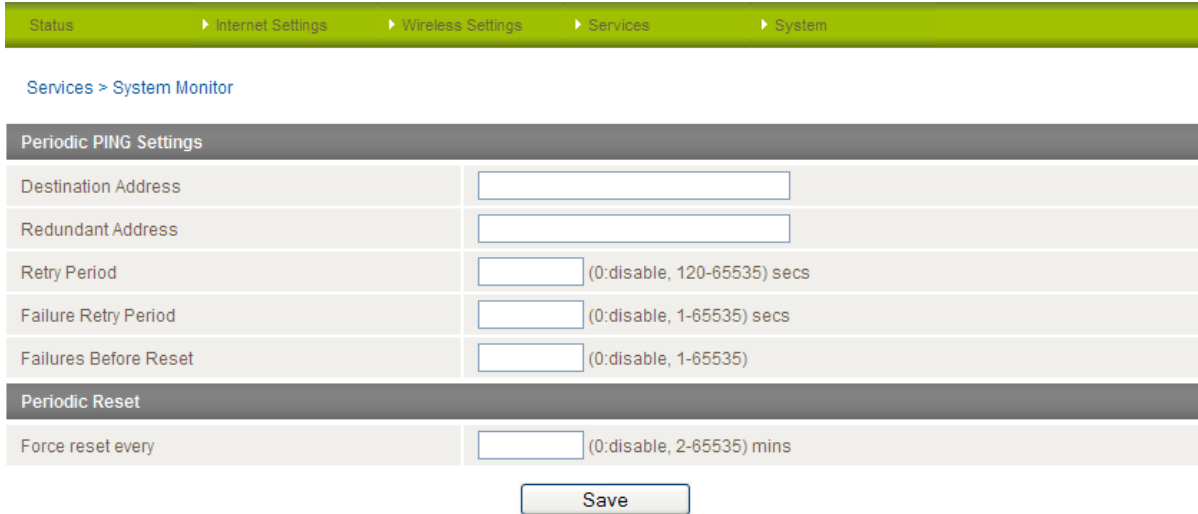


Figure 58 - System Monitor Settings

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 “Fail Count”, 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 Timer. The maximum value is 65535 minutes.

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

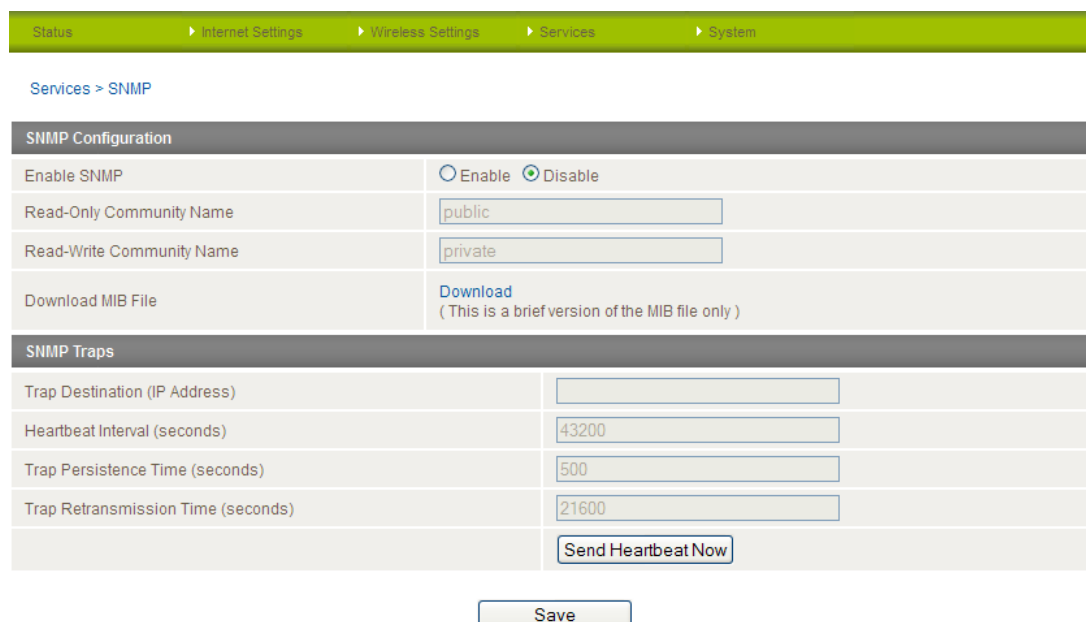


Figure 59 - SNMP Settings

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 the "Enable" option for the Enable SNMP field.
2. Enter the Community Names or leave them as default.



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 when using this feature.

3. Click the "Save" button to save the new 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 28 - SNMP Configuration Options

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



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:

1. Ability to send a text message via a 3G network and store in permanent storage
2. Ability to receive a text message via a 3G network and store in permanent storage
3. 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.
4. 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.
5. Ability to change live configuration on the device (e.g. connection APN).
6. 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”.

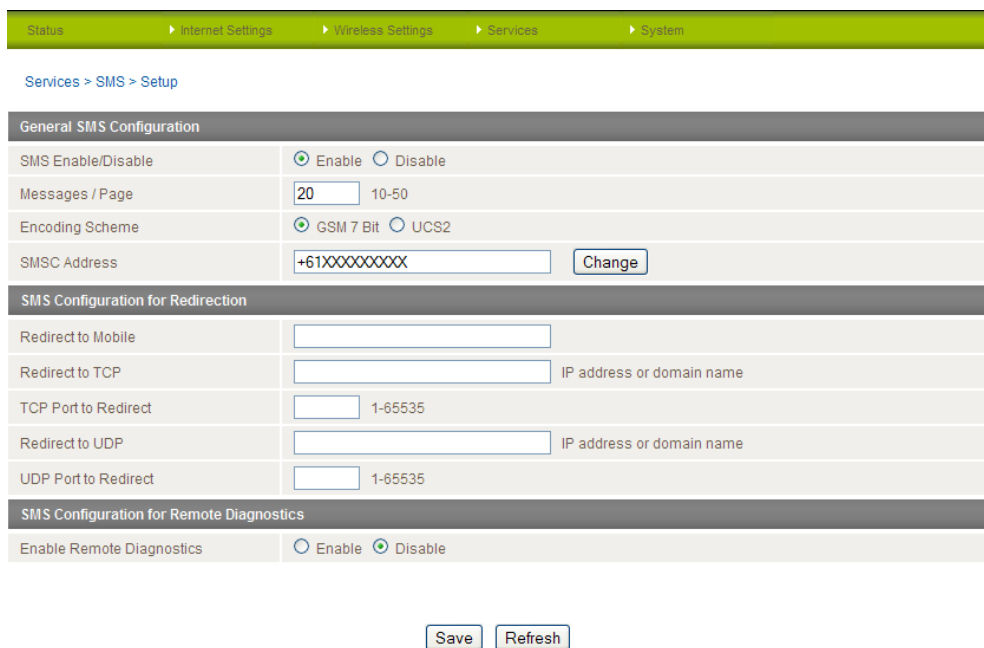


Figure 60 - SMS Function Setup

OPTION	DEFINITION
Messages / Page	Enter the number of SMS messages to display per page.
Encoding Scheme	The encoding method used for SMS messages.
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 29 - SMS Setup Configuration Items

### SMS Configuration for Redirection

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

#### **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 is used to send an SMS text message to 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"/>	
Destination Number 003	<input type="checkbox"/>	
Destination Number 004	<input type="checkbox"/>	
Destination Number 005	<input type="checkbox"/>	
Destination Number 006	<input type="checkbox"/>	
Destination Number 007	<input type="checkbox"/>	
Destination Number 008	<input type="checkbox"/>	
Destination Number 009	<input type="checkbox"/>	
Destination Number 010	<input type="checkbox"/>	+ -

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.

Send
Refresh

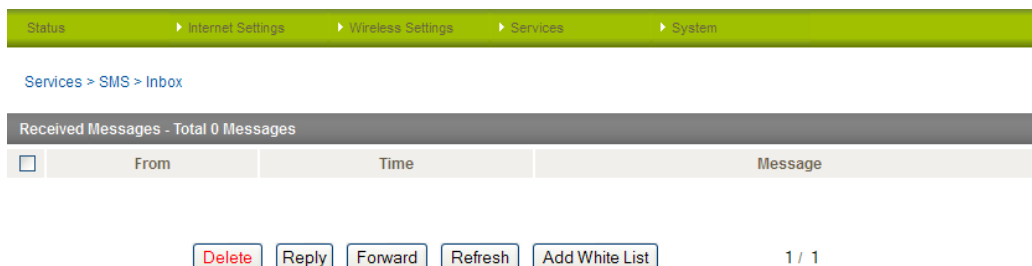
Figure 61 - New SMS Message

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.



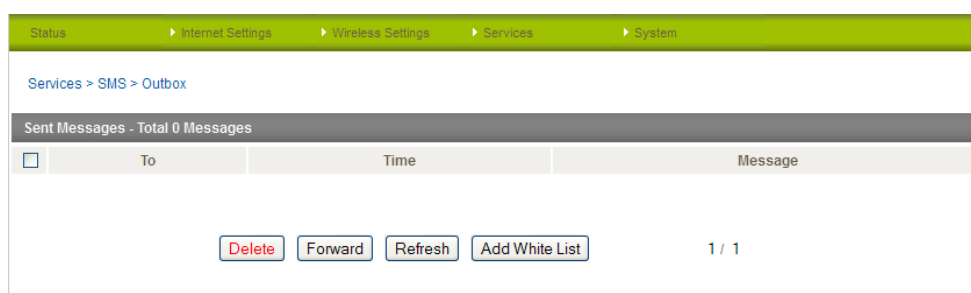
Services > SMS > Inbox

Received Messages - Total 0 Messages

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

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

Figure 62 - SMS Inbox



Services > SMS > Outbox

Sent Messages - Total 0 Messages

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

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

Figure 63 - 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 64 - SMS Diagnostics Settings

The following pages detail 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**

Select destination to send an acknowledgement message 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**

Enter the destination number to which acknowledgement messages will be 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:***

1. If the time frame is set to “HOUR” and the current time is “04:30”, then the counter will reset to zero at “05:00”.
2. If time frame is set to “DAY” and current date and time is “04:30” 17<sup>th</sup> of March, then the counter will reset to zero at “00:00” 18<sup>th</sup> of March.
3. 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.
4. If time period is set to “MONTH” and current date and time is “04:30” 17<sup>th</sup> of March, then the counter will reset to zero at “00:00” 1<sup>st</sup> 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 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 30 - 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 31 - 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 32 - 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 33 - SMS Diagnostics - Example Commands

## Auto Dial

Use this page to configure the NTC-30WV to dial a pre-defined number when you lift the handset of an attached device. To use this function, set Enable Auto Dialling to “Enable” and type the number you want to dial when the handset is lifted.

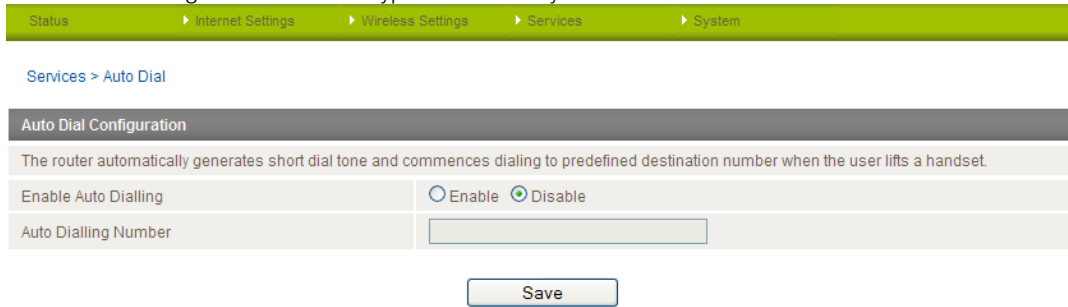


Figure 65 - Auto Dial settings

## System

### Log

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

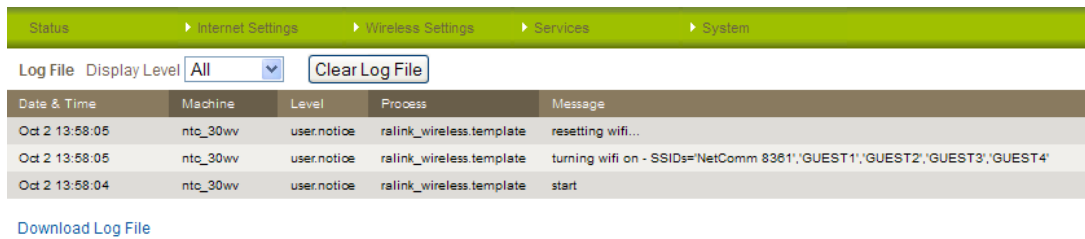


Figure 66 - System Log

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

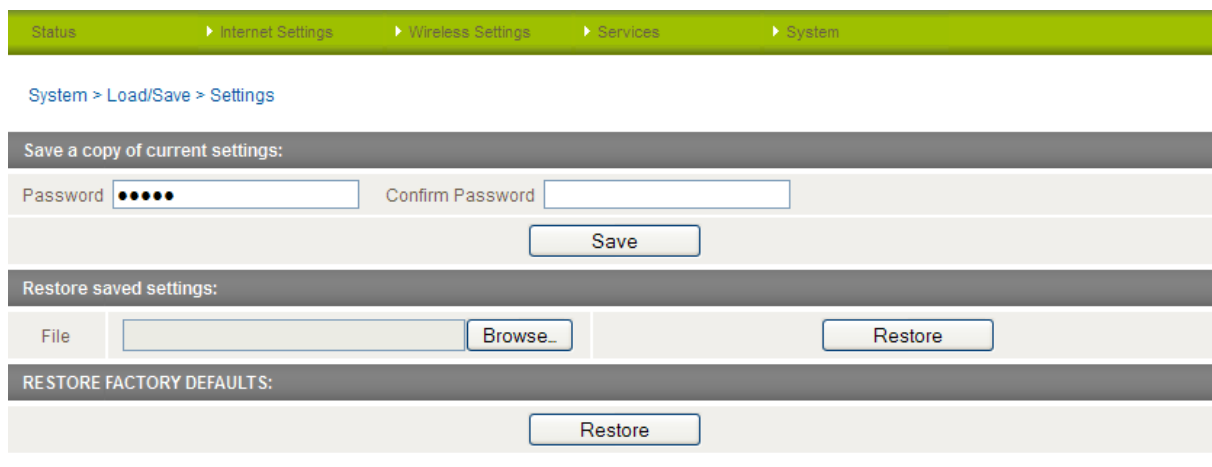
You can also download the current System Log to your computer for off-line viewing. To do this, click the “Download Log File” link at the bottom of the page.



Note: the Load/Save menu is only available to users logged in to the router using the user name `root`. To perform Firmware upgrade, device configuration backup and reset the gateway to factory defaults, you need to login as the root user.

## Settings

The settings page is used to backup or restore the router's configuration or to reset it to factory default settings.



The screenshot shows the 'Load/Save' configuration page. At the top is a navigation bar with links: Status, Internet Settings, Wireless Settings, Services, and System. Below this is a breadcrumb trail: System > Load/Save > Settings. The page is divided into three main sections: 1. 'Save a copy of current settings:' which includes a 'Password' field (with masked dots), a 'Confirm Password' field, and a 'Save' button. 2. 'Restore saved settings:' which includes a 'File' input field, a 'Browse...' button, and a 'Restore' button. 3. 'RESTORE FACTORY DEFAULTS:' which includes a single 'Restore' button.

Figure 67 - 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 under the "Restore Saved settings:" section.
2. Select the previously saved configuration file that you wish to restore to the router.
3. Click the "Restore" button.

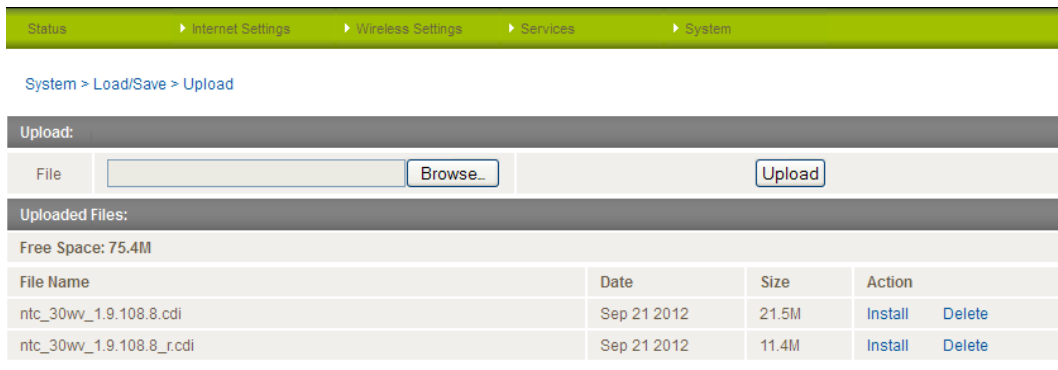
### To restore the router's configuration to the factory defaults

Click the "Restore" button under the "Restore Factory Defaults" section to restore the router to factory default settings.

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-30WV.



File Name	Date	Size	Action
ntc_30wv_1.9.108.8.cdi	Sep 21 2012	21.5M	<a href="#">Install</a> <a href="#">Delete</a>
ntc_30wv_1.9.108.8_r.cdi	Sep 21 2012	11.4M	<a href="#">Install</a> <a href="#">Delete</a>

Figure 68 - Upload Page



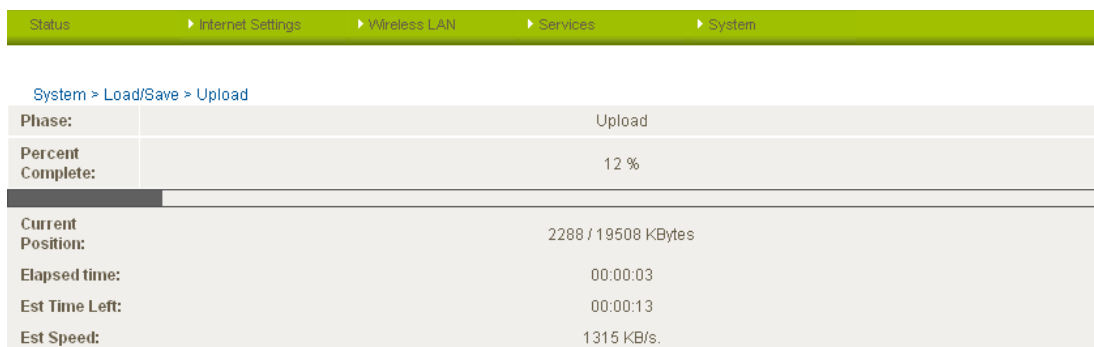
Note: In order to perform an update, you must be logged into the router as the root user (see the Remote Administration section for more details).

## 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 69 - 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 see "Done" shown as per the screenshot below, you can then boot into the system recovery mode to install the main system software.

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

Figure 70 - 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.

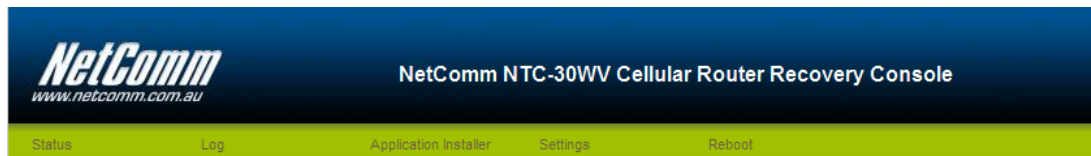


Figure 71 - Recovery Console Banner

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%.

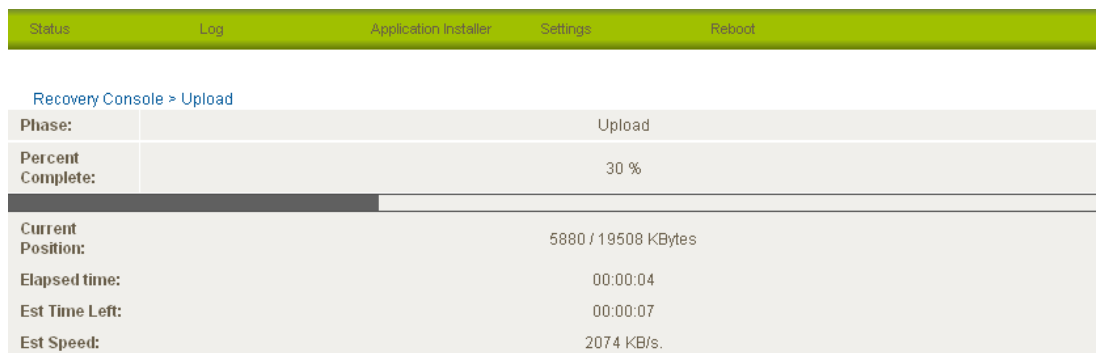


Figure 72 - Recovery Console - Upload Firmware

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.

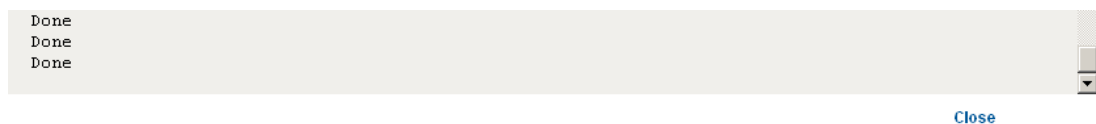


Figure 73 - Recovery Console - Firmware Update

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	
xxxxx	3.3	install	7503	<a href="#">Package details</a> <a href="#">Uninstall</a>

Figure 74 - 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-30WV, please refer to the SDK document available from the NetComm website.

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

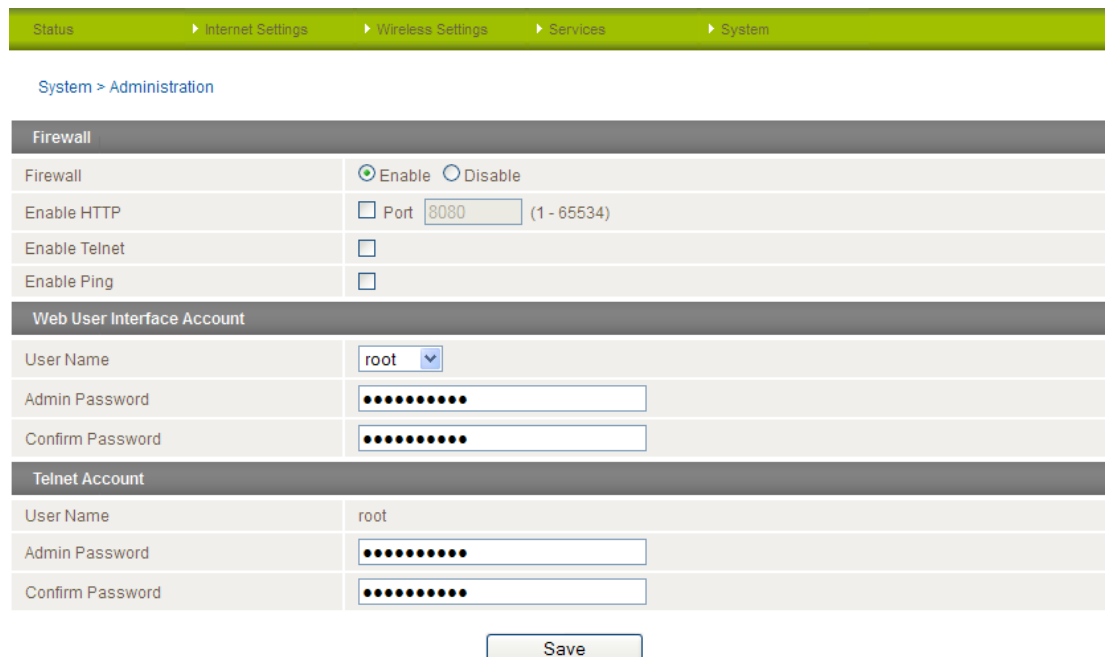



Figure 75 - Administration Configuration Items

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.
<b>Web User Interface Account</b>	
Username	Select the username you would like to change the password for. Root users have write permissions for both the root and admin accounts. Admin users can only update the admin password.
Password	Enter the new password for the selected user account.
Confirm Password	Re-enter the new password for the selected user account.
<b>Telnet Account</b>	
User Name	The Telnet Account settings are only available when logged into the router as the 'root' user.
Password	Enter the new password for the root telnet user account.
Confirm Password	Re-enter the new password for the root telnet 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.

Click "Login" and type admin or root in the Username and admin in the Password fields. 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. The TCP Keepalive can be used to ensure the WWAN connection does not disconnect due to inactivity.

Status
Internet Settings
Wireless Settings
Services
System

### System Configuration

Remote Syslog Server

IP / Hostname [:PORT]

TCP Keepalive Settings

Keepalive
☐ Enable
☒ Disable

Keepalive Time
 ( 60-65535 ) seconds

Keepalive Interval
 ( 10-28800 ) seconds

Keepalive Probes
 ( 1-1000 ) times

LEDs Power Save Settings

LEDs Timeout

LEDs Power Save Status
LED power save mode is disabled

Save

Figure 76 - System Configuration Items

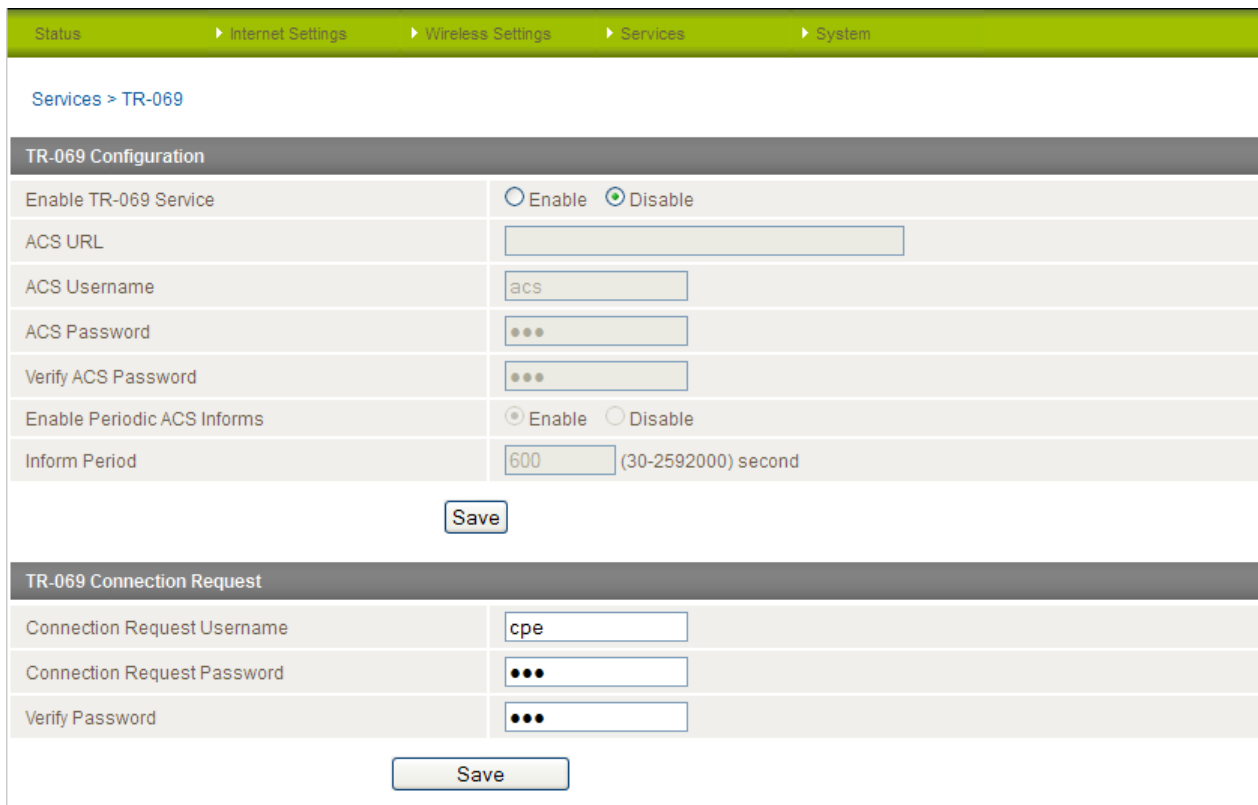
OPTION	DEFINITION
IP / Hostname [:PORT]	The IP address and port of the external syslog server you would like logging information sent to.
<b>TCP Keepalive Settings</b>	
Keepalive	Enable or Disable the TCP Keepalive function.
Keepalive Time	The interval between the last packet sent and the first TCP keepalive packet being sent.
Keepalive Interval	The time between subsequent TCP Keepalive packets.
Keepalive Probes	The number of TCP Keepalive packets to send.
<b>LEDs Power Save Settings</b>	
LEDs Timeout	The length of time before the LEDs on the outside of the router turn off to save power.
LEDs Power Save Status	The status of the LED power saving function.

Table 36 - System Configuration Items

## 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.



The screenshot shows the 'Services > TR-069' configuration page. It has a green navigation bar at the top with links: Status, Internet Settings, Wireless Settings, Services, and System. Below the navigation bar, the page title is 'Services > TR-069'. The main content area is divided into two sections: 'TR-069 Configuration' and 'TR-069 Connection Request'. The 'TR-069 Configuration' section includes fields for 'Enable TR-069 Service' (radio buttons for Enable and Disable, with Disable selected), 'ACS URL' (text input), 'ACS Username' (text input with 'acs'), 'ACS Password' (password input), 'Verify ACS Password' (password input), 'Enable Periodic ACS Informs' (radio buttons for Enable and Disable, with Enable selected), and 'Inform Period' (text input with '600' and '(30-2592000) second'). A 'Save' button is at the bottom of this section. The 'TR-069 Connection Request' section includes fields for 'Connection Request Username' (text input with 'cpe'), 'Connection Request Password' (password input), and 'Verify Password' (password input). A 'Save' button is at the bottom of this section.

Figure 77 - 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.

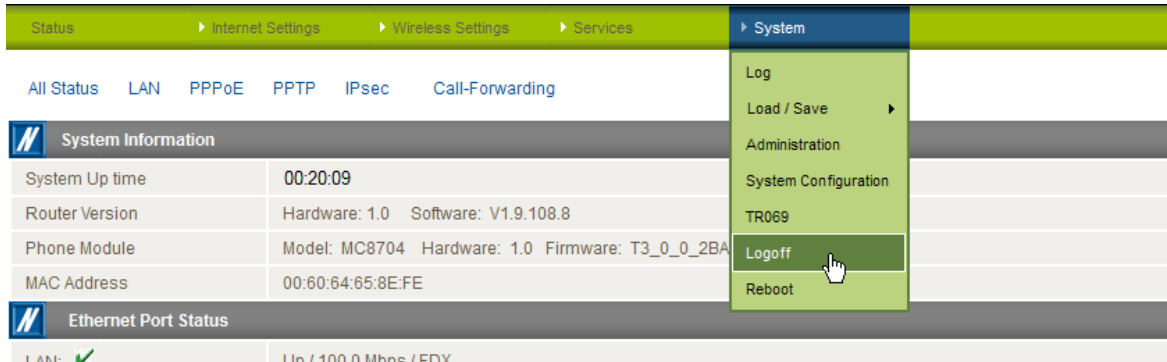


Figure 78 - Logoff

## 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.

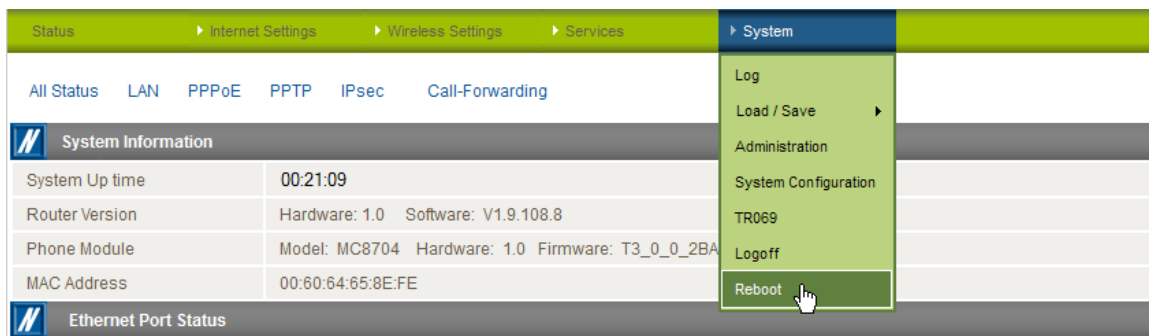


Figure 79 - Reboot Router

# Technical Data

The following table lists the hardware specifications of the NTC-30WV.

MODEL	NETCOMM NTC-30WV
<b>Modem Module/Chipset</b>	Sierra Wireless MC8704
<b>Memory</b>	RAM: 64MB DRAM Storage: 256MB Flash
<b>Operating System</b>	Embedded Linux 2.6
<b>UMTS bands</b>	Quad-Band: 850/900/1900/2100Mhz
<b>GSM bands</b>	Quad-Band: 850/900/1800/1900Mhz
<b>Maximum Data Throughput / 3G Radio interface</b>	Downlink: 42 Mbps (HSDPA Cat. 8); Uplink: 5.76 Mbps (HSUPA Cat. 6); EDGE MS Class 12: 236 kbps
<b>Wireless Frequency</b>	2.4 ~ 2.438Ghz
<b>Peak Data Rate (Wireless)</b>	300 Mbps (MIMO)
<b>Wireless Security</b>	WEP 64-bit, WEP 128-bit, WPA, WPA-PSK, WPA2-PSK, Mixed WPA-PSK/WPA2-PSK, TKIP, AES
<b>Connectivity</b>	1 x RJ-45 Fast Ethernet 10/100Base-TX w/ Auto MDIX 1 x Mini USB 2.0 Console Port 1 x Optional Circular IP67 Power Connection (When PoE not used)
<b>SIM Card Reader</b>	1 x Lockable SIM Card Tray Reader, Push to Release
<b>Antenna connectors</b>	Cellular: 2 x detachable TNC (1 x Main and 1 x Rx Diversity) WLAN: 2 x detachable TNC (1 x Main and 1 x Rx Diversity)
<b>LED Indicators</b>	7 LEDs: Power, Network Service, 5 x Signal Strength
<b>Operating Temperature</b>	Normal Operating Temperature: -25 °C to 60 °C Extended Operating Temperature: Module: -25°C to +75°C (Reduced Performance)
<b>Power input</b>	DC-in Port: 9 ~ 28V PoE (IEEE 802.3af): 48V DC AC/DC Power Adapter: 100-240V AC to 12V DC/1.5A
<b>Power Consumption</b>	Standby Input Current: 110mA @ 12V DC 3G Active Current: 300mA @ 12V DC Maximum Input Current: 560mA @ 12V DC
<b>Dimensions &amp; Weight</b>	NTC-30WV: 255mm X 240mm X 80mm / 1750g Mounting Bracket: 290mm X 110mm X 12mm / 410g Antennas: length = 180mm; diameter = 20mm / 60g
<b>Regulatory Compliancy</b>	A-Tick (Australia), CE (Europe), FCC (USA), RoHS, Emark, IP67 Rating

Table 38 - Technical Specifications for the NTC-30WV

# Additional Product Information

## Using the NTC-30WV to make and receive telephone calls

The NTC-30WV 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-30WV 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 the line interface on the NTC-30WV 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 the 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-30WV.
2. Your NTC-30WV 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-30WV 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-30WV, 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 (briefly depressing the hook button). The incoming call should then be answered. Upon hanging up or performing another hook-flash, 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-30WV supports a number of call feature codes for supplementary services.

FEATURE	ACTIVATION	DEACTIVATION	STATUS
Caller ID	#31# (to block an individual call)	*31# (to unblock an individual call)	N/A
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	*67*<Directory Number>#	#67#	*#67#
Call Forwarding Unreachable	*62*<Directory Number>#	#62#	*#62#

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

### Caller ID

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

- To force Caller ID to be blocked for an outbound call, dial #31# followed by the number you wish to dial.
- To force Caller ID to be unblocked for an outbound call, dial \*31# then follow the dialling number.

### 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 (or call diverting), is a feature that allows an incoming call to be redirected to another number depending on the circumstances at the time of receiving the call.



Note: The Call Waiting feature will automatically turn off if you enable Call forwarding. Call Waiting will need to be enabled again after Call Forwarding is 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.

1. To enable Call Forwarding No Answer, dial \*61\*<Directory Number>#  
(Where directory number is the number you wish to forward calls to)
2. Hang up after you hear 2 low pitch beeps.
3. To disable Call Forwarding No Answer, dial #61#
4. Hang up after you hear 2 high pitch beeps.
5. To check the status of Call Forwarding No Answer, dial \*#61# or view the advanced status page of the management console.
  - (a) Call Forwarding No Answer is disabled if you hear 2 high pitch beeps.
  - (b) 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 \*67\*<Directory Number>#

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

1. Hang up after you hear 2 low pitch beeps.
2. To disable Call Forwarding Busy, dial #67#
3. Hang up after you hear 2 high pitch beeps.
4. To check the status of Call Forwarding Busy, dial \*#67# or view the advanced status page of the management console.
  - (a) Call Forwarding Busy is disabled if you hear 2 high pitch beeps.
  - (b) Call Forwarding Busy is enabled if you hear 2 low pitch beeps.

### Call Forwarding Not Reachable

Call forwarding busy will divert all incoming calls to a phone number that you desire only if your telephone is unreachable by the network.

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

### Conference Call

This can be achieved by performing a hook-flash and then by dialling the third party.

Wait for the third party to answer your call and then perform another hook-flash to conference all the parties together.



Note: In order to activate a conference call, you will need to have originated both calls.

### Troubleshooting

What do I do if I have no dial tone?

Please follow the procedure listed below:

1. Check to make sure the phone is plugged into the line port of the NTC-30WV.
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 3G signal strength indication lights on the front of the NTC-30WV are lit up.
4. Check to make sure your 3G SIM card is activated and insert into your NTC-30WV properly.
5. Check and see if you get the dial tone after rebooting your NTC-30WV.

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-30WV.
3. Try rebooting your NTC-30WV.



# Appendix A: Tables

Table 1 - Document Revision History .....	2
Table 2: Maximum Transmit Power Levels .....	4
Table 3: Average Transmit Power Levels.....	5
Table 4 - LED Indicators .....	7
Table 5 - Device Dimensions .....	9
Table 6 - Mounting Bracket Dimensions .....	9
Table 7 - Antenna Dimensions .....	10
Table 8 - Bottom Mounted Integrated Interfaces .....	11
Table 9 - Top Mounted Interfaces .....	11
Table 10 - LAN Management Default Settings .....	12
Table 11 – WiFi Default Settings .....	12
Table 12 - Web Interface Default Settings .....	12
Table 13 - Locking Power Block Pin Outs.....	16
Table 14 - Status page items .....	19
Table 15 - Status Page - LAN Details.....	20
Table 16 - Status Page - PPPoE Details .....	20
Table 17 - Status Page - PPTP Details .....	20
Table 18 - Status Page - IPSec Details.....	20
Table 19 - Status Page - Call Forwarding Status Details .....	21
Table 20 - Advanced Status Page .....	22
Table 21 - NAT Configuration Items .....	33
Table 22 - OpenVPN Configuration Items .....	39
Table 23 - PPTP Configuration Items.....	40
Table 24 - GRE VPN Settings.....	41
Table 25 - Wireless Configuration - Basic Configuration Items.....	43
Table 26 - WDS Access Point 1 Repeater Mode Settings .....	47
Table 27 - Wireless Settings - Advanced Configuration Items.....	51
Table 28 - SNMP Configuration Options.....	56
Table 29 - SMS Setup Configuration Items.....	57
Table 30 - SMS Diagnostic Command Syntax .....	64
Table 31 - List of Valid SMS Diagnostic Commands.....	65
Table 32 - List of SMS Diagnostics Variables .....	65
Table 33 - SMS Diagnostics - Example Commands.....	66
Table 34 - System Log Detail Levels.....	67
Table 35 - Administration Configuration Items .....	72
Table 36 - System Configuration Items .....	73
Table 37 - System - TR-069 Details .....	74
Table 38 - Technical Specifications for the NTC-30WV .....	76
Table 39 - Additional Product Information - Call Feature Codes Quick Reference .....	78

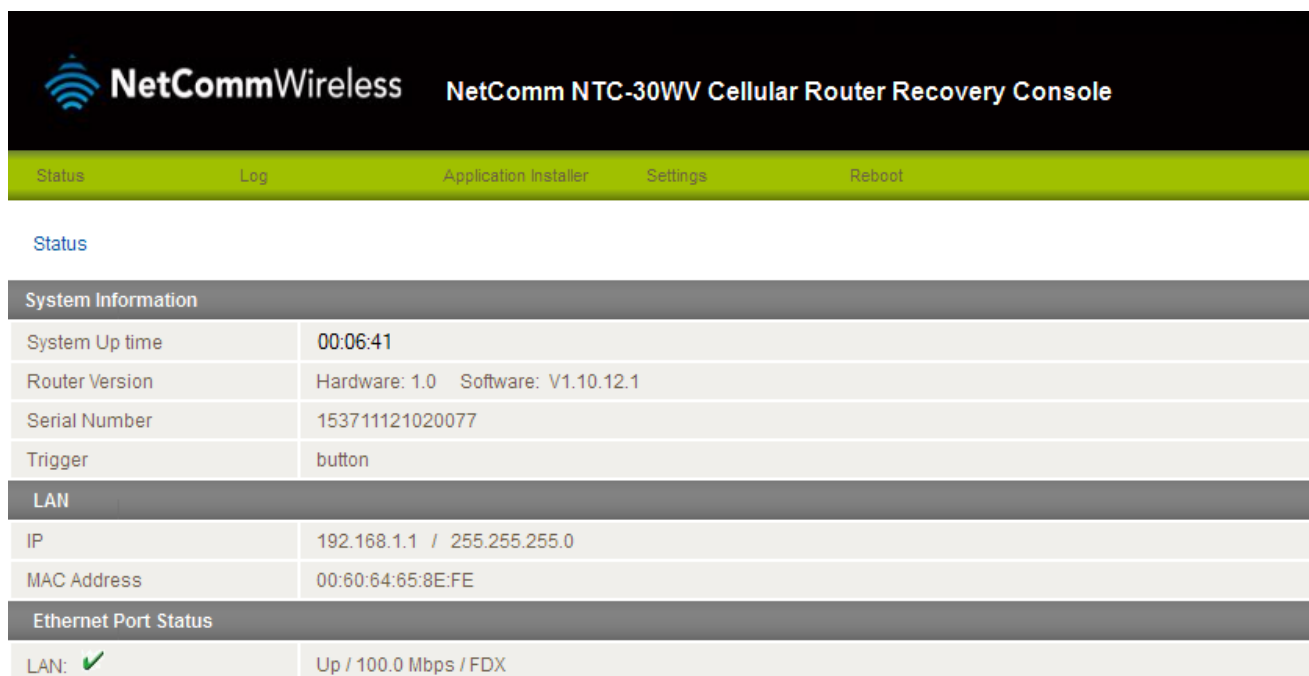
# Appendix B: Recovery mode

The NTC-30WV features two independent operating systems, each with its own file systems. These two systems are referred to as 'Main' and 'Recovery'. It is always possible to use one in order to restore the other in the event that one system becomes damaged or corrupted (such as during a firmware upgrade failure).

Both systems have web interfaces that can be used to manipulate the other inactive system. The router starts up by default in the Main system mode, however the router may be triggered to start in recovery mode if desired.

To start the router in recovery mode:

1. Disconnect the power source from the router.
2. Press and hold the physical reset button on the interface panel of the router. While holding the reset button down, connect the power source and keep holding the reset button down for 5 seconds and then release it. The router boots into recovery mode.
3. In your browser, navigate to <http://192.168.1.1>. The router's recovery mode is hardcoded to use this address regardless of the IP address that was configured in the main system. The router's recovery console is displayed.



**NetCommWireless NetComm NTC-30WV Cellular Router Recovery Console**

Status Log Application Installer Settings Reboot

**Status**

System Information	
System Up time	00:06:41
Router Version	Hardware: 1.0 Software: V1.10.12.1
Serial Number	153711121020077
Trigger	button

LAN	
IP	192.168.1.1 / 255.255.255.0
MAC Address	00:60:64:65:8E:FE


Ethernet Port Status	
LAN: 	Up / 100.0 Mbps / FDX

Figure 80 - Recovery console

The recovery console provides limited functionality. Basic status information is available, as well as access to the System log for troubleshooting. The Application Installer can be used to upload and install different firmware, allowing you to roll back to a previous firmware in the event that an upgrade fails. The Settings menu provides the ability to reset the router to factory default settings and the Reboot tab allows you to perform a soft reboot of the router.

# Legal and Regulatory

## Intellectual Property Rights

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

You are permitted to use this Manual for the sole purpose of using the NetComm 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.

NetComm is a trademark of NetComm. 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 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:
3. Change the direction or relocate the receiving antenna.
4. Increase the separation between this equipment and the receiver.
5. Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
6. Consult an experienced radio/TV technician for help.
7. The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

## Consumer Protection Laws

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

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

## Product Warranty

All NetComm products have a standard one (1) year warranty from date of purchase, however, some products have an extended warranty option (refer to packaging and the warranty card) (each a **Product Warranty**). To be eligible for the extended warranty option you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering online via the NetComm Wireless web site at [www.netcommwireless.com](http://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 and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. the cost of transporting product to and from NetComm's nominated premises is your responsibility;
5. NetComm does not have any liability or responsibility under the Product Warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour; and
6. the customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

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

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

## Limitation of Liability

This clause does not apply to New Zealand consumers.

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

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

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

## FCC Regulations:

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

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

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

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

### ► RF Exposure Information

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

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

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

## IC Regulations:

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

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

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

This Class B digital apparatus complies with Canadian ICES-003.  
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

### IC Radiation Exposure Statement:

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

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

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

# Contact

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

ABN: 85 002 490 486

Website: [www.netcommwireless.com](http://www.netcommwireless.com)

Phone: +61(0)2 9424 2070

Fax: +61(0)2 9424 2010

Email: [sales@netcommwireless.com](mailto:sales@netcommwireless.com) ; [techsupport@netcommwireless.com](mailto:techsupport@netcommwireless.com)