

User Guide

NTC-40WV – Industrial Indoor 3G Router with Voice



Copyright

Copyright© 2015 NetComm Wireless Limited. All rights reserved.

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



Note: This document is subject to change without notice.

Save our environment

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

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

Please be responsible and protect our environment.

This manual covers the following products:

NetComm Wireless NTC-40WV

DOCUMENT VERSION	DATE
1.0 - Initial document release	29/01/2014
1.1 – Updated for firmware v2.0.4.1 release	11/04/2014
1.2 – Updated for firmware v2.0.11.1 release	15/07/2014
1.3 – Updated for firmware v2.0.19.1 release	16/09/2014
1.4 – Updated for firmware v2.0.21.1 release	02/12/2014
1.5 – Updated for firmware v2.0.24.3 release. Updated OpenVPN and System log sections. Added Lightweight M2M section. Added new SMS commands. Added instructions for SSH key generation. HTTPS key management renamed to Server certificate. Other minor corrections.	1/04/2015
1.6 – Updated for v2.0.27.1 firmware. Updated IPSec configuration, port forwarding configuration, WAN configuration and Lightweight M2M sections. Added Wireless Distribution System (WDS) feature description and TCP connect-on-demand endpoint description.	26/06/2015

Table 1 - Document Revision History

Table of contents

Overview	6
Introduction	6
Target audience.....	6
Prerequisites	6
Notation	6
Product introduction.....	7
Product overview.....	7
Package contents.....	7
Product features.....	8
Hardware overview	9
LED indicators.....	9
Interfaces	10
Configuring your Router	12
Inserting the SIM Card	12
Setting Up the Cellular Router	12
Polarity of DC Power Plug Screw Terminal.....	12
Installation and configuration of the NTC-40WV router	13
Powering the router	13
DC power via 2-pin connector.....	13
DC power via field terminated power source.....	13
Installing the router	13
Advanced configuration	14
Status	15
Networking.....	18
Data connection	18
Connecting to the mobile broadband network	19
Manually configuring a connection profile.....	19
Confirming a successful connection	21
Transparently bridging the mobile broadband connection via PPPoE.....	21
Operator settings.....	23
Operator settings.....	24
SIM security settings.....	24
Unlocking a PIN locked SIM.....	24
Enabling/Disabling SIM PIN protection.....	26
Changing the SIM PIN code.....	26
Unlocking a PUK locked SIM.....	27
LAN	28
LAN configuration.....	28
DHCP	29
Wireless settings.....	32
AP basic.....	32
AP advanced.....	34
AP MAC filtering	35
AP station info	35
AP hotspot.....	36
Client configuration.....	39
Wireless Distribution System (WDS).....	41
What is WDS?	41
Configuring WDS	41
Ethernet LAN/WAN.....	46
Interface assignment.....	46
WAN configuration.....	47
WAN failover.....	48
Link monitor	49
Ping monitor.....	49
Routing	51
Static	51
RIP.....	53
Redundancy (VRRP) configuration.....	54
Port forwarding.....	55
DMZ.....	57
Router firewall.....	58
MAC / IP / Port filtering	59
Creating a MAC / IP / Port filtering rule	59

VPN	61
IPSec	61
Configuring an IPSec VPN	61
OpenVPN	64
Configuring an Open VPN server	64
OpenVPN Server	64
Configuring an OpenVPN Client	67
Configuring an OpenVPN P2P Connection	69
PPTP-Client	70
Configuring the PPTP Client	70
GRE tunnelling	72
Configuring GRE tunnelling	72
Services	74
Dynamic DNS	74
Network time (NTP)	75
Configuring Timezone settings	75
Configuring NTP settings	75
Data stream manager	76
Endpoints	76
Streams	81
Data stream applications	83
PADD	84
Remote management	85
SNMP	85
TR-069	87
OMA Lightweight M2M configuration	89
Auto dial configuration	91
USSD	92
Voice	93
Event notification	94
Notification configuration	94
Destination configuration	96
Email settings	97
SMS messaging	98
Setup	98
SMS forwarding configuration	99
Redirect to mobile	99
Redirect to TCP / UDP server address	99
New message	100
Inbox / Sent Items	101
Diagnostics	102
SMS diagnostics and command execution configuration	102
White List for diagnostic or execution SMS	104
Sending an SMS Diagnostic Command	105
Types of SMS diagnostic commands	105
SMS acknowledgment replies	105
SMS command format	106
List of basic commands	107
List of get/set commands	108
List of basic RDB variables	108
Network scan and manual network selection by SMS	109
SMS diagnostics examples	111
System	114
System log	114
IPSec log	114
Event notification log	115
System log settings	116
System configuration	118
Settings backup and restore	118
Upload	119
Updating the Firmware	119
Package manager	122
Administration	123
Administration settings	123
HTTPS key management	125
SSH Key Management	128
LED operation mode	130
Watchdogs	131
Configuring Periodic Ping settings	133

Disabling the Periodic Ping reset function	133
Configuring a Periodic reboot	133
Reboot	134
Logging out	134
Appendix A: Tables	135
Appendix B: Default Settings	136
Restoring factory default settings	137
Using the web-based user interface	137
Using the reset button on the interface panel of the router	137
Appendix C: Recovery mode	138
Accessing recovery mode	138
Status	139
Log	139
Application Installer	140
Settings	140
Reboot	140
Appendix D: HTTPS - Uploading a self-signed certificate	141
Appendix E: Obtaining a list of RDB variables	143
Technical Data	144
Additional Product Information	145
Using the NTC-40WV to make and receive telephone calls	145
Handset requirements	145
Maximum REN Loading	145
How to place a call	145
How to receive a call	145
Answering an incoming call when on a call	145
Accessing voicemail	145
Call feature codes	146
List of Mobile Broadband Service Provider APNs	148
Legal & Regulatory Information	149
Contact	151

Overview

Introduction




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

Target audience



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

Prerequisites

Before continuing with the installation of your NTC-40WV router, please confirm that have the following:

-  A device with a working Ethernet network adapter.
-  A web browser such as Internet Explorer, Mozilla Firefox or Google Chrome.
-  A flathead screwdriver if field terminated power is required.

Telephony Requirements

-  Standard analogue PSTN or cordless PSTN phone handset (DECT) with an RJ11 port.
(ISDN phone handsets are not supported)
-  RJ11 cable

Notation

The following symbols are used in this user guide:



The following note requires attention.



The following note provides a warning.



The following note provides useful information.

Product introduction

Product overview

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

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

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

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

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







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

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

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

Package contents

The NTC-40WW package consists of:

-  NetComm Wireless NTC-40 - HSPA+ M2M WiFi Router
-  1 x Power supply (9-28VDC)
-  1 x Quick Start Guide
-  2 x 3G Antennas (SMA connector)
-  2 x WiFi Antennas (SMA connector)
-  1 x RJ-45 Ethernet Cable

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

Product features

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

Hardware overview

LED indicators

There are a total of five LED's on the router.

Listed below are the specifications of the LEDs and their corresponding colours.

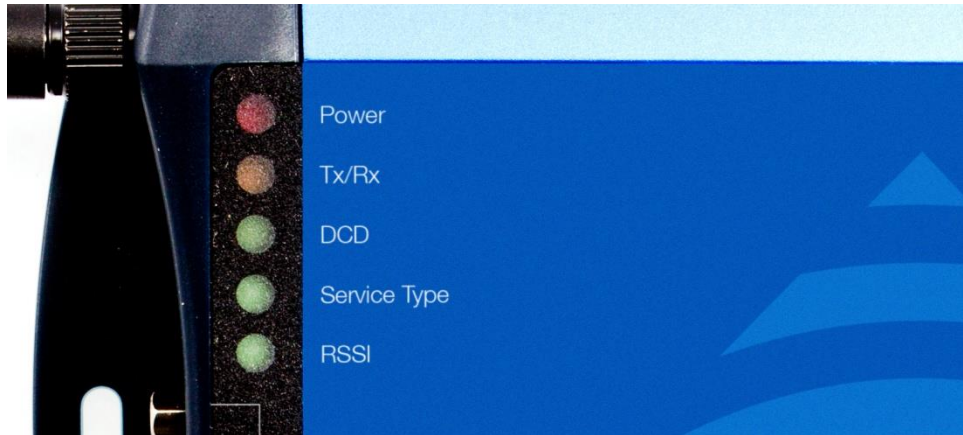


Figure 1: NTC-40W LEDs

LED	DISPLAY	DESCRIPTION
POWER (red)	Solid ON	The red Power LED indicates power has been applied to the router from the DC power input jack.
TX Rx (amber)	Solid ON	The amber LED will illuminate upon data being sent to or received from the cellular network.
DCD (green)	Solid ON	The green Data Carrier Detect LED illuminates to indicate a data connection.
Service Type (green)	The green LED will illuminate when cellular network coverage is detected.	
	Solid ON	3G: Indicates UMTS/HSPA available coverage
	Flashing	EDGE: Indicates EDGE available coverage
	Off	2G: Indicates GSM/GPRS available coverage only.
RSSI (green)	This green LED shows Received Signal Strength. There are three possible states that the RSSI LED can operate in, based upon signal level.	
	Solid ON	Strong: Indicates the RSSI level is -86dbm
	Flashing Once a Second	Medium: Indicates the RSSI level is -110dbm and -86dbm
	Off	Fair: Indicates the RSSI level is less than -110dbm

Table 2 - LED Descriptions

Interfaces

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

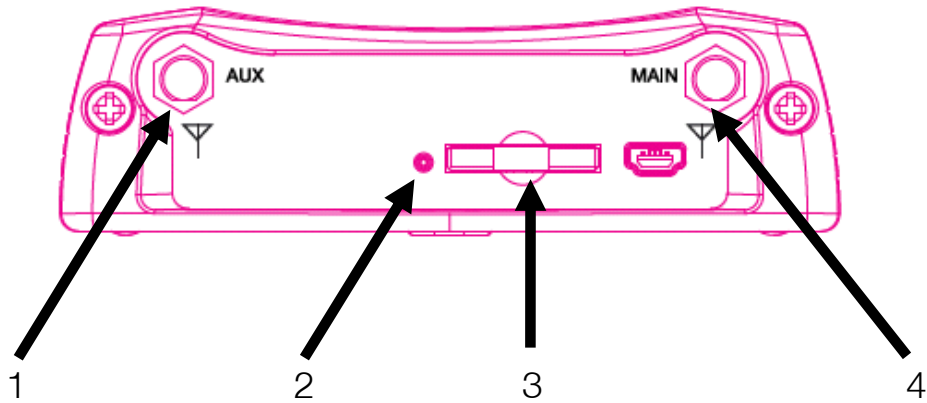


Figure 2 - Bottom Mounted interfaces

ITEM	INTERFACE	FUNCTION
1	Diversity Receive 3G Antenna	Connect one of the 3G antennas here
2	SIM Card Reader Tray Eject button	Push in with a paper clip to eject the SIM card reader tray.
3	SIM Card Reader Tray	Insert the SIM Card reader tray with a SIM inserted here.
4	Main 3G Antenna	Connect one of the 3G antennas here.

Table 3 - Bottom Mounted interfaces

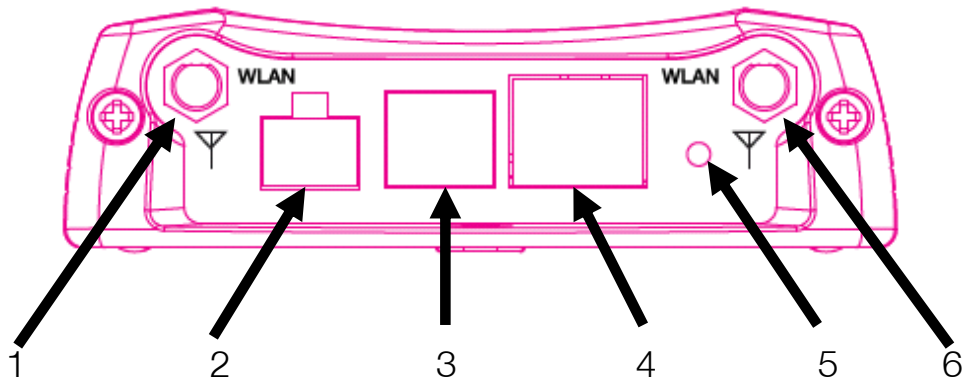


Figure 3 - Top Mounted Interfaces

ITEM	INTERFACE	FUNCTION
1	WiFi Antenna Port	Connect one of the WiFi antennas here.
2	Captive Power Terminal	Connect the supplied power cable here.
3	RJ11 Telephone Cable Port	Connect a PSTN telephone here in order to make calls via the 3G connection.
4	RJ-45 Ethernet Port	Connect an Ethernet cable here. The RJ-45 Ethernet port has two LEDs; a green LED indicating the link status and an amber one indicating the speed of the link. When an Ethernet cable is connected and the link LED is illuminated, the amber speed LED illuminates to indicate a 100Mbps connection and extinguishes to indicate a 10Mbps connection.
5	Reset button	<p>The reset button has multiple functions.</p> <ul style="list-style-type: none"> Reboot the device: Press and hold the reset button down for no longer than 5 seconds. All LEDs remain off, when the button is released the green LEDs flash once and the router reboots. Reboot to recovery mode: Press and hold the reset button down for between 5 and 15 seconds. When the LEDs are flashing, release the button and the amber LED flashes. The router reboots into recovery mode. Factory reset the device: Press and hold the reset button down for more than 15 seconds. When all the LEDs are off, release the button. The Red LED flashes to confirm the factory reset process. If you change your mind after holding the reset button down for more than 15 seconds, you can cancel the factory reset by removing the power source before releasing the button or by releasing the button and quickly pressing it once more.
6	WiFi Antenna Port	Connect one of the WiFi antennas here.





Table 4 - Top Mounted interfaces



Note: The amber speed LED on the RJ-45 Ethernet port remains illuminated when no Ethernet cable is attached. The reading of the speed LED is only valid when an Ethernet cable is connected and the green link LED is illuminated.

Configuring your Router

You will need the following hardware components to set up the router:

-  Power supply (9-28VDC)
-  Ethernet cable
-  Laptop or PC
-  Active SIM card

Inserting the SIM Card

Use a paperclip to press the SIM Eject button to eject the SIM card tray. Place the SIM card in the SIM card tray. Make sure the SIM card is inserted correctly by inserting the SIM with the gold side facing down into the SIM card bay and in the direction as shown below:

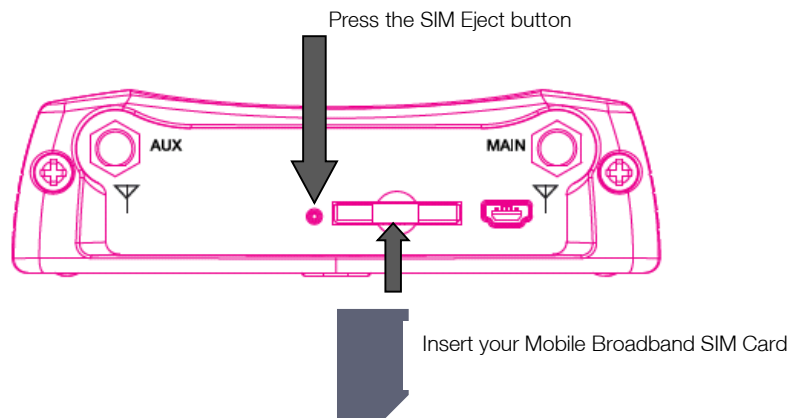


Figure 4 - Inserting the SIM Card

Setting Up the Cellular Router

Attach the supplied antennas to the router by screwing them onto the antenna connectors. Connect the power adapter to the mains and plug the output into the power jack of the router. When power is correctly supplied to the router, the red power LED on the panel illuminates.

Polarity of DC Power Plug Screw Terminal



Figure 5 – Locking Two-way Power Terminal Block

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

Table 5 - Locking power block pin outs

Installation and configuration of the NTC-40WV router

Powering the router

The NTC-40WV router can be powered in one of two ways:

1. DC power input via 2-pin connector (9-28V DC)
2. DC power input via field terminated power source (9-28V DC)

The red power LED on the router lights up when a power source is connected.

DC power via 2-pin connector

The DC input jack can accept power from a separately sold DC power supply. Both a standard temperature range DC power supply and an extended temperature range DC power supply are available to purchase as accessories.

To supply the router with DC Power via the 2-pin connector, remove the attached green terminal block from your router and connect the external DC power supply to the router's green DC power jack.

DC power via field terminated power source

If an existing 9-28V DC power supply is available, you can insert the wires into the supplied terminal block to power your router. Use a flathead screwdriver to tighten the terminal block screws and secure the power wires, making sure the polarity of the wires are correctly matched for your particular unit, as illustrated below.

Installing the router

After you have mounted the router and connected a power source, follow these steps to complete the installation process.

1. Connect equipment that requires network access to the Ethernet port of your router. This may be your computer for advanced configuration purposes, or your end equipment which requires data access via the NTC-40WV router. You can connect one device directly, or several devices using a network switch.
2. Ensure the external power source is switched on and wait 2 minutes for your NTC-40WV router to start up. To check the status of your router, compare the LED indicators on the device with those listed in the [LED Indicators](#) section of this guide.

Advanced configuration

The NTC-40WW router comes with pre-configured settings that should suit most customers. For advanced configuration, log in to the web-based user interface of the router.

To log in to the web-based user interface:

1. Open a web browser (e.g. Internet Explorer, Firefox, Safari), type <http://192.168.1.1> into the address bar and press **Enter**. The web-based user interface log in screen is displayed.

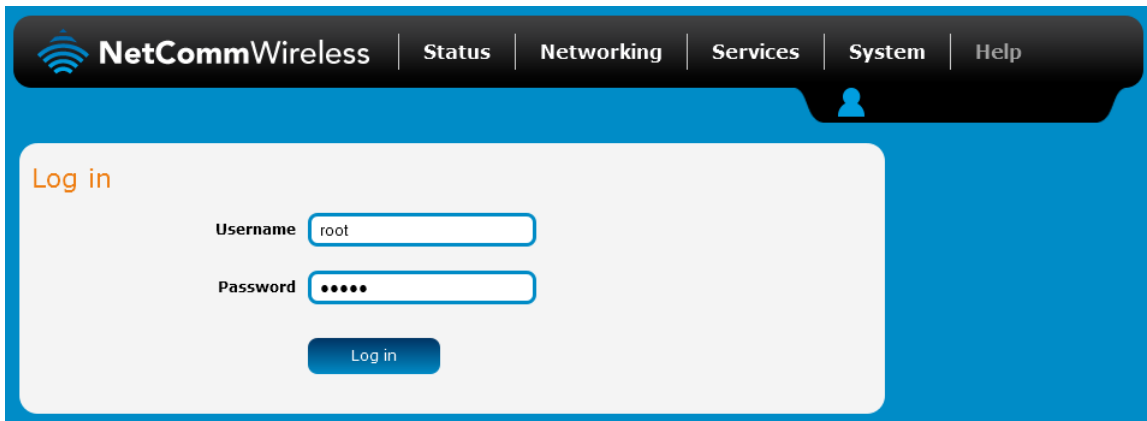


Figure 6 – Log in prompt for the web-based user interface

2. Enter the login username and password. If this is the first time you are logging in or you have not previously configured the password for the “root” or “admin” accounts, you can use one of the default account details to log in.

ROOT MANAGER ACCOUNT	
Username:	root
Password:	admin

Table 6 - Management account login details – Root manager

ADMIN MANAGER ACCOUNT	
Username:	admin
Password:	admin



Table 7 - Management account login details – Admin manager

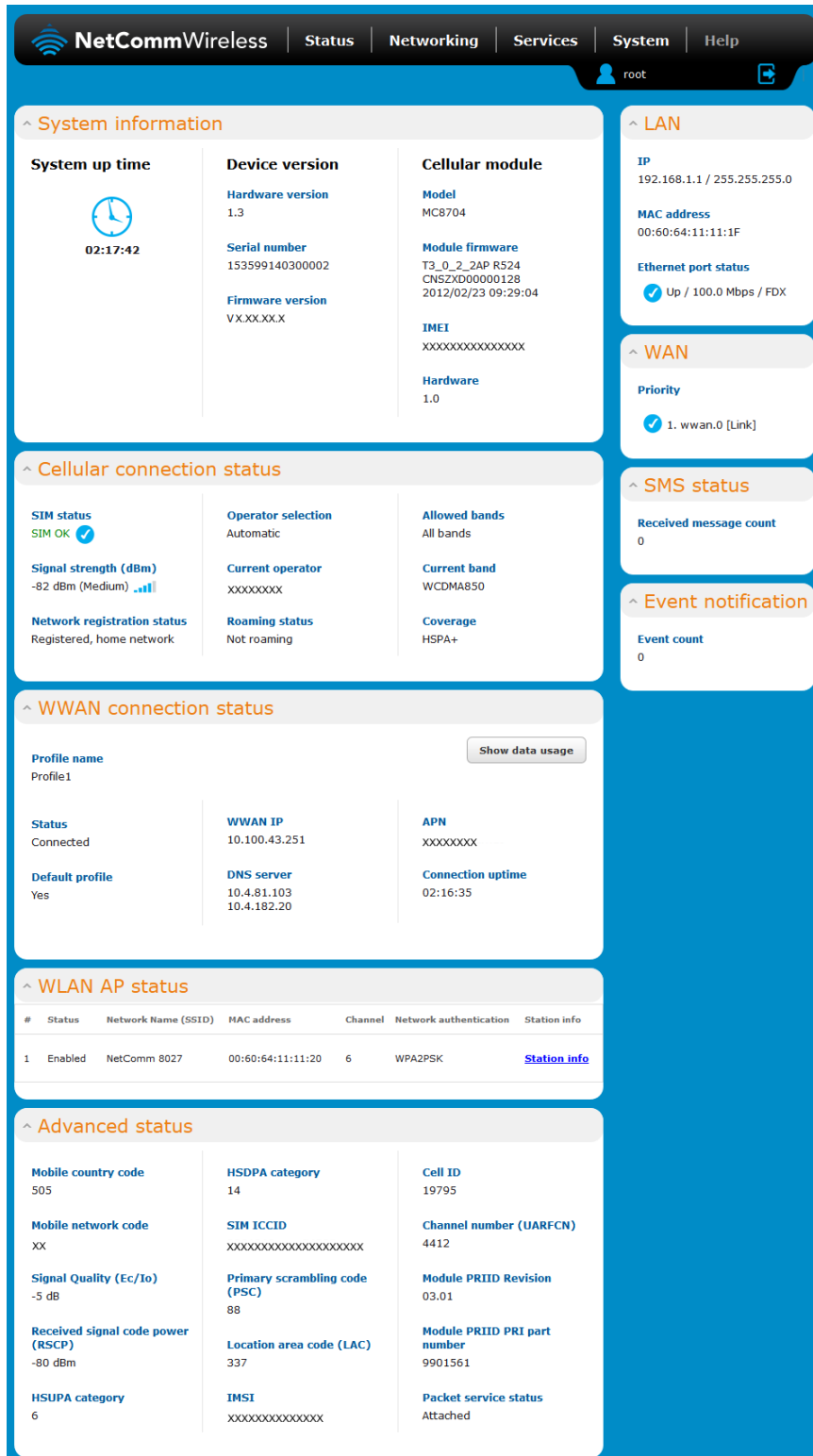


Note: To access all features of the router, you must use the root manager account. For security reasons, we highly recommend that you change the passwords for the root and admin accounts upon initial installation. You can do so by navigating to the System and then Administration page.

The Status page is displayed when you have successfully logged in.

Status

The status page of the web interface provides system related information and is displayed when you log in to the NTC-40WV router management console. The status page shows System information, LAN details, Cellular connection status, Packet data connection status and Advanced status details. You can toggle the sections from view by clicking the  or  buttons to show or hide them. Extra status boxes will appear as additional software features are enabled (e.g. VPN connectivity).



The screenshot shows the NetCommWireless web interface with the following sections:

- System information:**
 - System up time:** 02:17:42
 - Device version:** Hardware version 1.3, Serial number 153599140300002, Firmware version VX.XX.XX.X
 - Cellular module:** Model MC8704, Module firmware T3_0_2_ZAP R524 CNSZXD00000128 2012/02/23 09:29:04, IMEI XXXXXXXXXXXXXXX, Hardware 1.0
- LAN:** IP 192.168.1.1 / 255.255.255.0, MAC address 00:60:64:11:11:1F, Ethernet port status Up / 100.0 Mbps / FDX
- WAN:** Priority 1. wwan.0 [Link]
- Cellular connection status:**
 - SIM status:** SIM OK
 - Signal strength (dBm):** -82 dBm (Medium)
 - Network registration status:** Registered, home network
 - Operator selection:** Automatic
 - Current operator:** XXXXXXXX
 - Roaming status:** Not roaming
 - Allowed bands:** All bands
 - Current band:** WCDMA850
 - Coverage:** HSPA+
- SMS status:** Received message count 0
- Event notification:** Event count 0
- WWAN connection status:**
 - Profile name:** Profile1 (Show data usage)
 - Status:** Connected
 - Default profile:** Yes
 - WWAN IP:** 10.100.43.251
 - DNS server:** 10.4.81.103, 10.4.182.20
 - APN:** XXXXXXXX
 - Connection uptime:** 02:16:35
- WLAN AP status:**

#	Status	Network Name (SSID)	MAC address	Channel	Network authentication	Station info
1	Enabled	NetComm 0027	00:60:64:11:11:20	6	WPA2PSK	Station info
- Advanced status:**
 - Mobile country code:** 505
 - Mobile network code:** XX
 - Signal Quality (Ec/Io):** -5 dB
 - Received signal code power (RSCP):** -80 dBm
 - HSUPA category:** 6
 - HSDPA category:** 14
 - SIM ICCID:** XXXXXXXXXXXXXXXXXX
 - Primary scrambling code (PSC):** 88
 - Location area code (LAC):** 337
 - IMSI:** XXXXXXXXXXXXXXX
 - Cell ID:** 19795
 - Channel number (UARFCN):** 4412
 - Module PRIID Revision:** 03.01
 - Module PRIID PRI part number:** 9901561
 - Packet service status:** Attached

Figure 7 - The Status page

ITEM	DEFINITION
System information	
System up time	The current uptime of the router.
Board version	The hardware version of the router.
Serial number	The serial number of the router.
Firmware version	The firmware version of the router
Model	The type of phone module and the firmware version of the module.
Module firmware	The firmware revision of the phone module.
IMEI	The International Mobile Station Equipment Identity number used to uniquely identify a mobile device.
Hardware	The hardware version of the module.
LAN	
IP	The IP address and subnet mask of the router.
MAC address	The MAC address of the router.
Ethernet port status	Displays the current status of the Ethernet port and its operating speed.
WAN	
Priority	Displays the priority of the available WAN connections.
SMS status	
Received message count	Displays the number of SMS messages that have been received by the router.
Event notification	
Notification count	Displays the number of notifications sent using the Event notification feature.
Cellular connection status	
SIM Status	Displays the activation status of the router on the carrier network.
Signal strength (dBm)	The current signal strength measured in dBm
Network registration status	The status of the router's registration for the current network.
Operator selection	The mode used to select an operator network.
Current operator	The current operator network in use.
Roaming status	The roaming status of the router.
Allowed bands	The bands to which the router may connect.
Current band	The current band being used by the router.
Coverage	The type of mobile coverage being received by the router.
WWAN connection status	
Profile name	The name of the active profile.
Status	The connection status of the active profile.
Default profile	Indicates whether the current profile in use is the default profile.
WWAN IP	The IP address assigned by the mobile broadband carrier network.
DNS server	The primary and secondary DNS servers for the WWAN connection.
APN	The Access Point Name currently in use.
Connection uptime	The length of time of the current mobile connection session.
WLAN status	
Status	Shows the current status of the wireless LAN network.
Network Name (SSID)	Shows the network name (SSID) of the wireless network.
Channel	Shows the channel that the wireless network is configured to operate on.
Network authentication	The type of security/encryption in use on the wireless network.
Station Info	Click the Station Info link to be taken to the station information page providing more information on the wireless network.
Advanced status	
Mobile country code	The Mobile Country Code (MCC) of the router.
Mobile network code	The Mobile Network Code (MNC) of the router.

Signal quality (Ec/NO)	A measurement of the portion of the received signal that is usable. This is 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.
HSUPA category	Displays the HSUPA category (1-9) for the current uplink
HSDPA category	Displays the HSDPA category (1-8) for the current downlink.
SIM ICCID	The Integrated Circuit Card Identifier of the SIM card used with the router, a unique number up to 19 digits in length.
Primary scrambling code (PSC)	The Primary scrambling code for the current signal.
Location area code (LAC)	The ID of the cell tower grouping the current signal is broadcasting from.
Routing area code (RAC)	A subdivision of the location area used with GPRS.
IMSI	The International mobile subscriber identity is a unique identifier of the user of a cellular network.
Cell ID	A unique code that identifies the base station from within the location area of the current mobile network signal.
Channel number (UARFCN)	The channel number of the current 3G/2G connection.
Module PRIID Revision	Module version used for customization.
Module PRIID PRI part number	The part number of the Module PRIID.

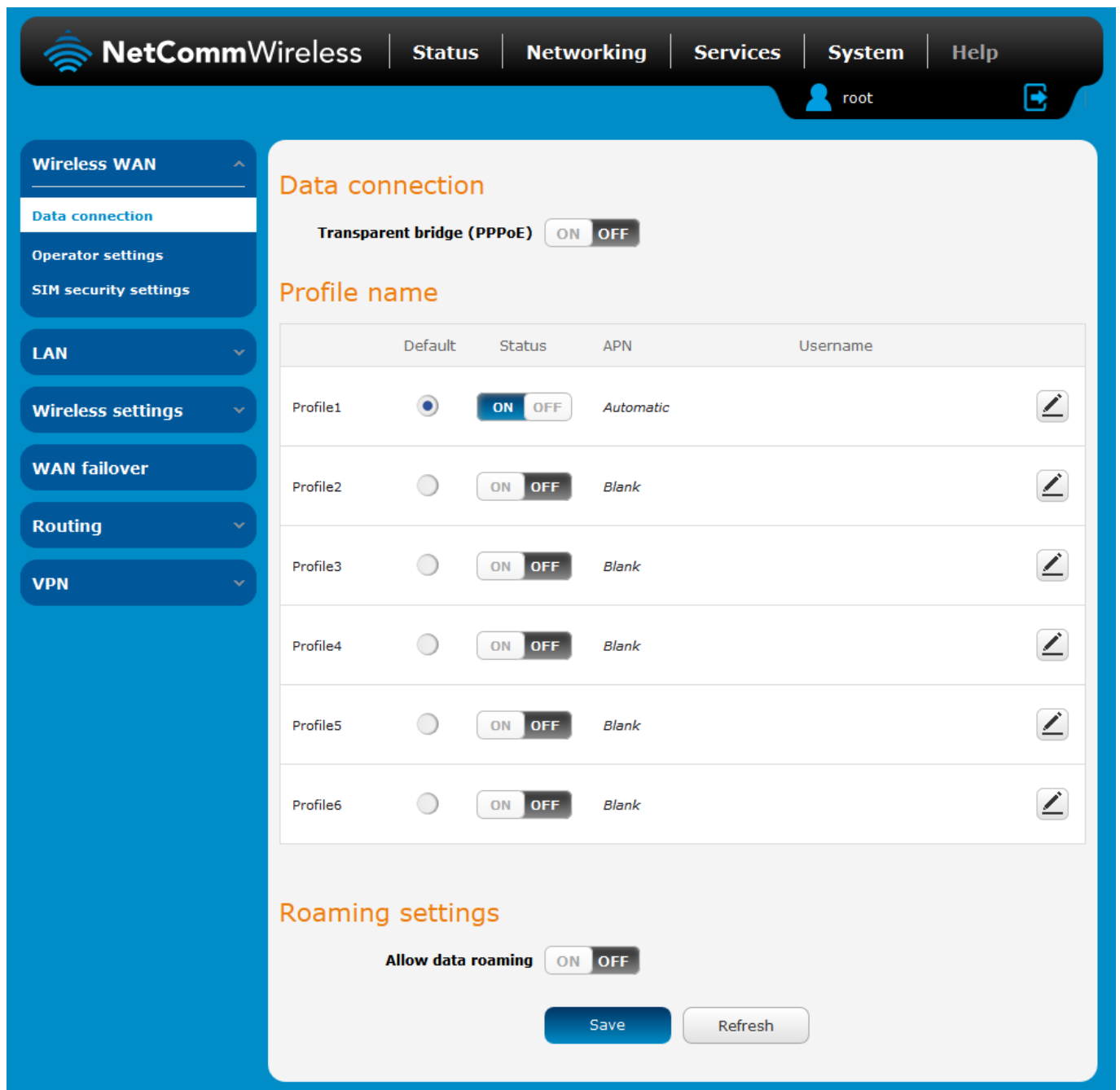
Table 8 - Status page item details

Networking

The Networking section provides configuration options for Wireless WAN, LAN, Routing and VPN connectivity.

Data connection

The data connection page allows you to configure and enable/disable the connection profile. To access this page, click on the **Networking** menu, and under the **Wireless WAN** menu, select the **Data connection** item.



The screenshot shows the NetCommWireless web interface. The top navigation bar includes 'Status', 'Networking', 'Services', 'System', and 'Help'. The user is logged in as 'root'. The left sidebar shows a menu with 'Wireless WAN' expanded, containing 'Data connection', 'Operator settings', and 'SIM security settings'. Other menu items include 'LAN', 'Wireless settings', 'WAN failover', 'Routing', and 'VPN'. The main content area is titled 'Data connection' and features a 'Transparent bridge (PPPoE)' toggle set to 'ON'. Below this is a 'Profile name' table with columns for 'Default', 'Status', 'APN', and 'Username'. The table lists six profiles: Profile1 (selected, ON, Automatic), Profile2 (OFF, Blank), Profile3 (OFF, Blank), Profile4 (OFF, Blank), Profile5 (OFF, Blank), and Profile6 (OFF, Blank). Each profile has an edit icon. At the bottom, there is an 'Allow data roaming' toggle set to 'ON' and 'Save' and 'Refresh' buttons.

	Default	Status	APN	Username
Profile1	<input checked="" type="radio"/>	ON OFF	Automatic	
Profile2	<input type="radio"/>	ON OFF	Blank	
Profile3	<input type="radio"/>	ON OFF	Blank	
Profile4	<input type="radio"/>	ON OFF	Blank	
Profile5	<input type="radio"/>	ON OFF	Blank	
Profile6	<input type="radio"/>	ON OFF	Blank	

Figure 8 – Data connection settings

ITEM	DEFINITION
Data connection	
Transparent Bridge (PPPoE)	Toggles the transparent bridge function on and off.
Profile name list	
Default	Sets the corresponding profile to be the default gateway for all outbound traffic except traffic for which there are configured static route rules or profile routing settings.
Status	Toggles the corresponding profile on and off. If your carrier supports it, two profiles may be turned on simultaneously.
APN	The APN configured for the corresponding profile.
Username	The username used to log on to the corresponding APN.
Roaming settings	
Allow data roaming	When set to ON , the router will allow local devices to access the Wireless WAN network when the it is roaming onto a foreign network. When set to OFF , the router will deny network access to data services when roaming onto a foreign network. This setting is OFF by default.

Table 9 - Data connection item details

Connecting to the mobile broadband network

The router supports the configuration of up to six APN profiles; these profiles allow you to configure the settings that the router will use to connect to the 2G/3G network and switch easily between different connection settings.

For advanced networking purposes, you may activate a maximum of two profiles simultaneously (dependant on network support). When activating two connection profiles, you should avoid selecting two profiles with the same APN as this can cause only one profile to connect. Similarly, activating two profiles which are both configured to automatically determine an APN can cause a conflict and result in neither profile establishing a connection. We recommend that the two active connection profiles have differing, manually configured APNs to avoid connection issues and ensure smooth operation.

Manually configuring a connection profile

To manually configure a connection profile:

1. Click the **Edit** button corresponding to the Profile that you wish to modify. The data connection profile settings page is displayed.

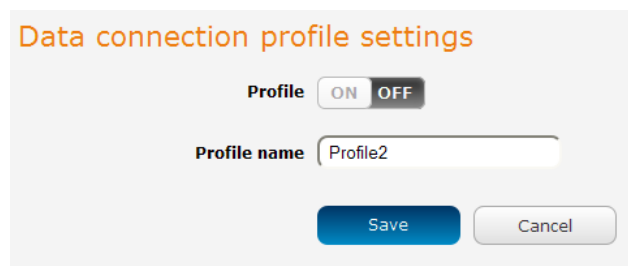
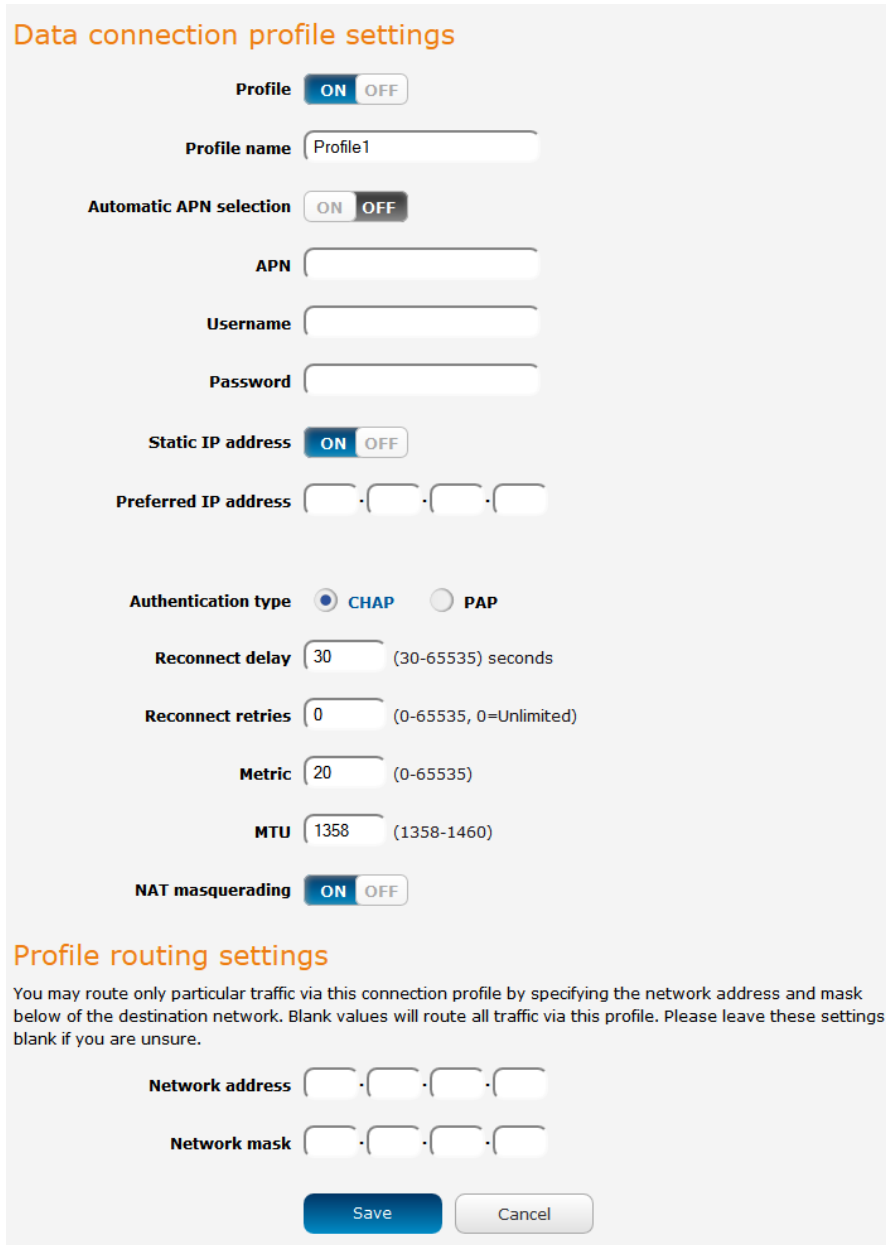


Figure 9 - Data connection profile settings

- Click the **Profile** toggle key to turn the profile on. Additional settings appear.



Data connection profile settings

Profile ON OFF

Profile name

Automatic APN selection ON OFF

APN

Username

Password

Static IP address ON OFF

Preferred IP address

Authentication type CHAP PAP

Reconnect delay (30-65535) seconds

Reconnect retries (0-65535, 0=Unlimited)

Metric (0-65535)

MTU (1358-1460)

NAT masquerading ON OFF

Profile routing settings

You may route only particular traffic via this connection profile by specifying the network address and mask below of the destination network. Blank values will route all traffic via this profile. Please leave these settings blank if you are unsure.

Network address

Network mask

Figure 10 - Data connection settings - Profile turned on

- In the **Profile name** field, enter a name for the profile. This name is only used to identify the profile on the router.
- Ensure that the **Automatic APN selection** toggle key is set to off. If it is not, click it to toggle it to the off position.
- In the **APN** field, enter the APN Name (Access Point Name) and if required, use the **Username** and **Password** fields to enter your login credentials.
- If your mobile broadband carrier allows you to select a preferred IP address, select the **Static IP address** toggle key to turn it to the **ON** position then enter your preferred IP address into the **Preferred IP address** field.
- Next to **Authentication** type, select either CHAP or PAP depending on the type of authentication used by your provider.
- The **Reconnect delay** field specifies the number of seconds to wait between connection attempts. The default setting of 30 seconds is sufficient in most cases but you may modify it to wait up to 65535 seconds if you wish.
- The **Reconnect retries** field specifies the number of times to attempt a network connection if the router fails to establish a connection. It is set to 0 by default which causes the router to attempt to reconnect indefinitely.
- The **Metric** value is used by router to prioritise routes (if multiple are available) and is set to 20 by default. This value is sufficient in most cases but you may modify it if you are aware of the effect your changes will have on the service.

11. The **MTU** field allows you to modify the Maximum Transmission Unit used on the connection. Do not change this unless instructed to by your carrier.
12. Use the **NAT Masquerading** toggle key to turn NAT Masquerading on or off. NAT masquerading, also known simply as NAT is a common routing feature which allows multiple LAN devices to appear as a single WAN IP via network address translation. In this mode, the router modifies network traffic sent and received to inform remote computers on the internet that packets originating from a machine behind the router actually originated from the WAN IP address of the router's internal NAT IP address. This may be disabled if a framed route configuration is required and local devices require WAN IP addresses.
13. For advanced networking such as using dual simultaneous PDP contexts, you may wish to configure a particular profile to route only certain traffic via that profile by configuring a custom address and mask of traffic to send via that profile. To do this, in the Profile routing settings section, enter the **Network address** and **Network mask** of the remote network. If you do not want to use this feature, or are unsure, please leave these fields blank, which will not designate any particular traffic to be routed via this profile. For more information on configuring Profile routing settings, see the [Setting a default gateway with two active connection profiles](#) example.
14. Click the **Save** button when you have finished entering the profile details.

Confirming a successful connection

After configuring the packet data session, and ensuring that it is enabled, click on the Status menu item at the top of the page to return to the Status page. When there is a mobile broadband connection, the **WWAN** section is expanded showing the details of the connection and the Status field displays **Connected**. To see details on the connected session, you can click the **Show data usage** button.

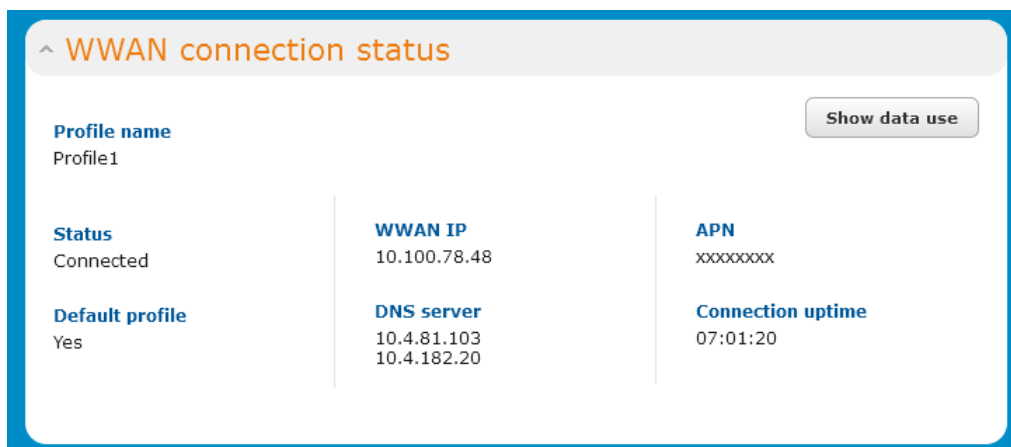


Figure 11 - WWAN connection status section

Transparently bridging the mobile broadband connection via PPPoE

If desired, you can have a client device connected to the Ethernet port initiate the mobile broadband connection using a PPPoE session. This is particularly useful in situations where you wish to provide Wireless WAN data access to an existing router which you want to have full public WAN IP access and have control over routing functionality.

To enable transparent bridging via PPPoE:

1. Click the **Networking** menu item from the top menu bar.
2. On the Data connection page, click the **Transparent bridge (PPPoE)** toggle key so that it is ON.

Data connection

Transparent bridge (PPPoE) ON OFF

In this mode the unit acts as an Ethernet Bridge instead of as an IP Router. This is facilitated by PPPoE which forwards the WAN IP/DNS information to a downstream LAN device and facilitates transparent network connectivity. To use this feature, you need to initiate a PPPoE client connection from a downstream device (such as an Ethernet Router or computer) which is then accepted by the router. The router operates a PPPoE server and will activate a PDP context using the username/password from the PPPoE client connection and the APN configured on this page. This allows control over the PDP context activation by the downstream device. Once enabled in this mode, some router functionality will no longer be applicable and will cease to function (e.g Connect on demand, routing, VPN, TR-069, Router firewall, remote access, and others). Only a single downstream device is permitted Wireless WAN connectivity and all traffic is forwarded to that device. Please note in this mode, the downstream device is responsible for all network security as the built-in firewall has no effect.

Transparent bridge mode configuration

APN name

Service name

Figure 12 - Transparent bridge configuration

3. In the APN name field, enter the APN that you wish to use for the mobile broadband connection.
4. (Optional) In the Service name field, enter a name that allows you to easily identify the connection.
5. Click the **Save** button to confirm the settings.
6. Click the Status menu item from the top menu bar to see the transparent bridging status.

^ **Transparent bridge mode**

Status
ENABLED

IP
N/A / 255.255.255.255

APN name
Blank

Service name
Blank

Figure 13 - Transparent bridge mode status

7. Next you must configure your downstream device connected via Ethernet to the NTC-40WV to initiate a network connection using a PPPoE client. The username and password used by the downstream device for the PPPoE session will be passed on and used by the NTC-40WV as the packet data (PDP) context authentication settings.

Operator settings

The Operator 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.

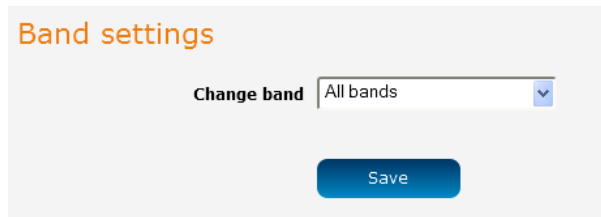


Figure 14 - Band settings



Note: In order to change the operator's band settings, the data connection must be disabled. When you access this page, you are prompted to disable the data connection if it is already active.

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

Use the **Change band** drop down list to select the band you wish to use.

The following band settings options are available:

NTC-40WV
WCDMA 900/2100
WCDMA All
GSM ALL
GSM 900/1800
All bands

Table 10 - Band settings

It is not necessary to change the default setting of **All bands** in most cases. In fact, locking to a particular band can cause connection difficulties if the device is moved to a location where the forced band selection is no longer available.

When **All bands** is selected, the router attempts to find the most suitable band based on the available networks for the inserted SIM card.

The GSM All and the WCDMA all options allow you to force the device to lock to either 2G networks only, or 3G networks only.

Click the **Save** button to save and apply your selection.

Operator settings

The operator settings feature allows you perform a scan of available networks, and to optionally lock to a particular network returned by the network scan. To scan for available networks, set the **Select operator mode** from automatic to **Manual** then click the scan button. This operation can take a few minutes and requires that the packet data session be disconnected prior to scanning.

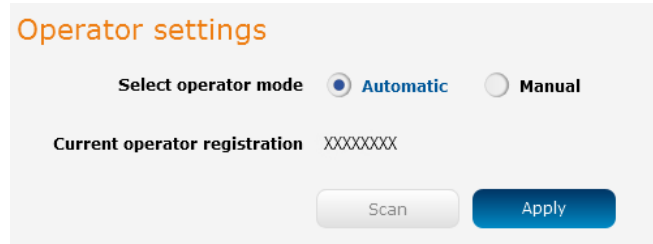


Figure 15 - Operator settings

A list of the detected 3G service carriers in your area is displayed.

	Operator name list	MCC	MNC	Operator status	Network type
<input checked="" type="radio"/>	Telstra	505	01	Current	UMTS (3G)
<input type="radio"/>	Telstra	505	01	Available	GSM (2G)
<input type="radio"/>	vodafone AU	505	03	Forbidden	GSM (2G)
<input type="radio"/>	YES OPTUS	505	02	Forbidden	GSM (2G)
<input type="radio"/>	YES OPTUS	505	02	Forbidden	UMTS (3G)
<input type="radio"/>	vodafone AU	505	03	Forbidden	UMTS (3G)

Figure 16 - Detected operator list

Select the most appropriate 3G service from the list shown and click **Apply**.

When **Select operator mode** is set to **Automatic**, the router selects the most appropriate operator based on the inserted SIM card. This is the default option and is sufficient for most users.

SIM security settings

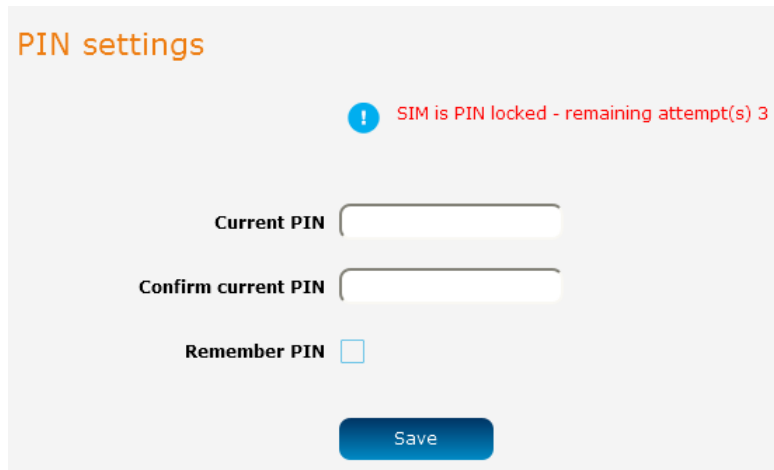
The SIM security settings page can be used for authenticating SIM cards that have been configured with a security PIN.

Unlocking a PIN locked SIM

If the SIM card is locked, you will receive a notice when you access the Status page after which you will be directed to the PIN settings page to enter the PIN. The PIN settings page lists the status of the SIM at the top of the page.

If you are not redirected to the PIN settings page, to unlock the SIM:

- a) Click on the **Networking** menu from the top menu bar, and then click **SIM security settings**.



PIN settings

SIM is PIN locked - remaining attempt(s) 3

Current PIN

Confirm current PIN

Remember PIN

Save

Figure 17 - SIM security settings - SIM PIN locked

- b) Enter the PIN in the **Current PIN** field and then enter it again in the **Confirm current PIN** field to confirm the PIN.
- c) If you are placing the router in a remote, unattended location, you may wish to check the **Remember PIN** option. 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.

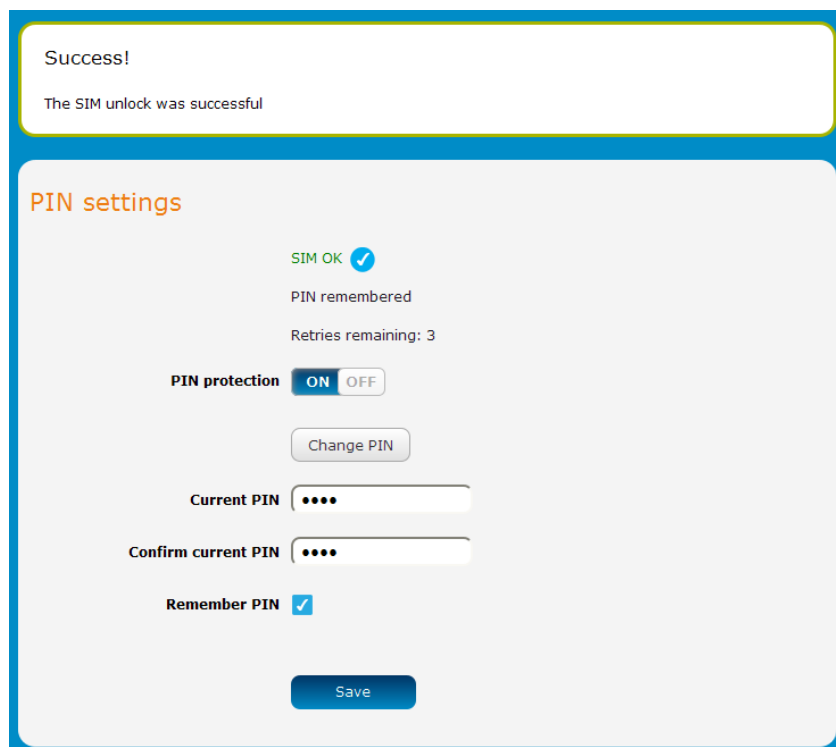
When this feature is enabled, the PIN you enter when setting the **Remember PIN** feature is encrypted and stored locally on the router. The next time the SIM asks the router for the PIN, the router decrypts the PIN and automatically sends it to the SIM without user intervention.

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



Note: Select **Remember PIN** if you do not want to enter the PIN code each time the SIM is inserted.

- d) Click the **Save** button. If successful, the router displays the following screen:



Success!

The SIM unlock was successful

PIN settings

SIM OK ✓

PIN remembered

Retries remaining: 3

PIN protection **ON** OFF

Change PIN

Current PIN ●●●●

Confirm current PIN ●●●●

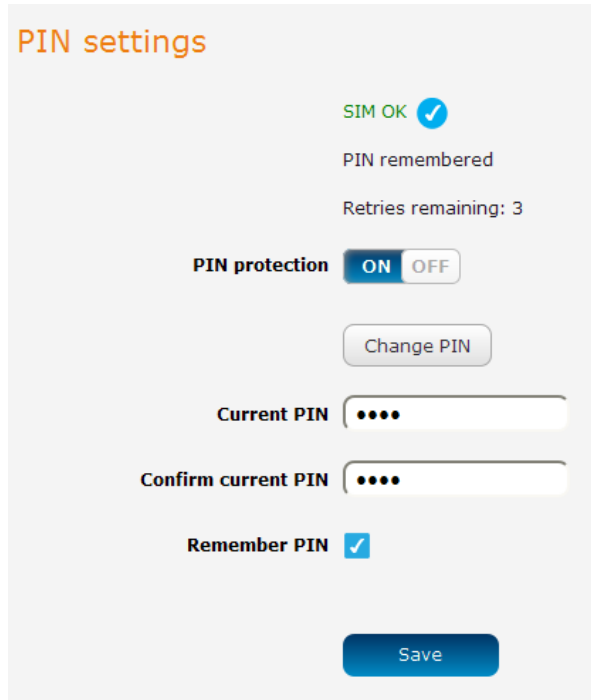
Remember PIN ✓

Save

Figure 18 - SIM security settings - SIM unlock successful

Enabling/Disabling SIM PIN protection

The security PIN protection can be turned on or off using the **PIN protection** toggle key.



PIN settings

SIM OK

PIN remembered

Retries remaining: 3

PIN protection ON OFF

Change PIN

Current PIN

Confirm current PIN

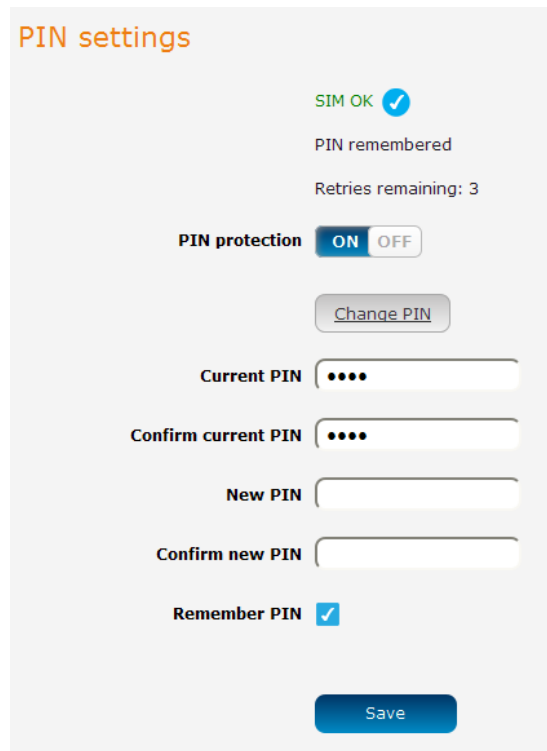
Remember PIN

Save

Figure 19 - PIN Settings

Changing the SIM PIN code

If you would like to change the PIN, click the **Change PIN** button and enter the current PIN into the **Current PIN** and **Confirm current PIN** fields, then enter the desired PIN into the **New PIN** and **Confirm new PIN** fields and click the **Save** button.



PIN settings

SIM OK

PIN remembered

Retries remaining: 3

PIN protection ON OFF

Change PIN

Current PIN

Confirm current PIN

New PIN

Confirm new PIN

Remember PIN

Save

Figure 20 - PIN settings - Change PIN

When the PIN has been changed successfully, the following screen is displayed:

Success!

Your settings have been changed successfully

PIN settings

SIM OK

PIN remembered

PIN protection ON OFF

Current PIN

Confirm current PIN

Remember PIN

Figure 21 - SIM security settings – PIN unlock successful

Unlocking a PUK locked SIM

After three incorrect attempts at entering the PIN, the SIM card becomes PUK (Personal Unblocking Key) locked and you are requested to enter a PUK code to unlock it.



Note: To obtain the PUK unlock code, you must contact your service provider.

You will be issued a PUK to enable you to unlock the SIM and enter a new PIN. Enter the new PIN and PUK codes. Click the **Save** button when you have finished entering the new PIN and PUK codes.

Oops, something went wrong...

Your SIM is PUK locked now. Please enter the PUK code to unlock. You have 10 remaining attempt(s).

PIN settings

! SIM is PUK locked

Current PIN

Confirm current PIN

PUK

Confirm PUK

Remember PIN

Figure 22 - SIM security - SIM PUK locked

LAN

LAN configuration

The LAN configuration page is used to configure the LAN settings of the router and to enable or disable DNS Masquerading.

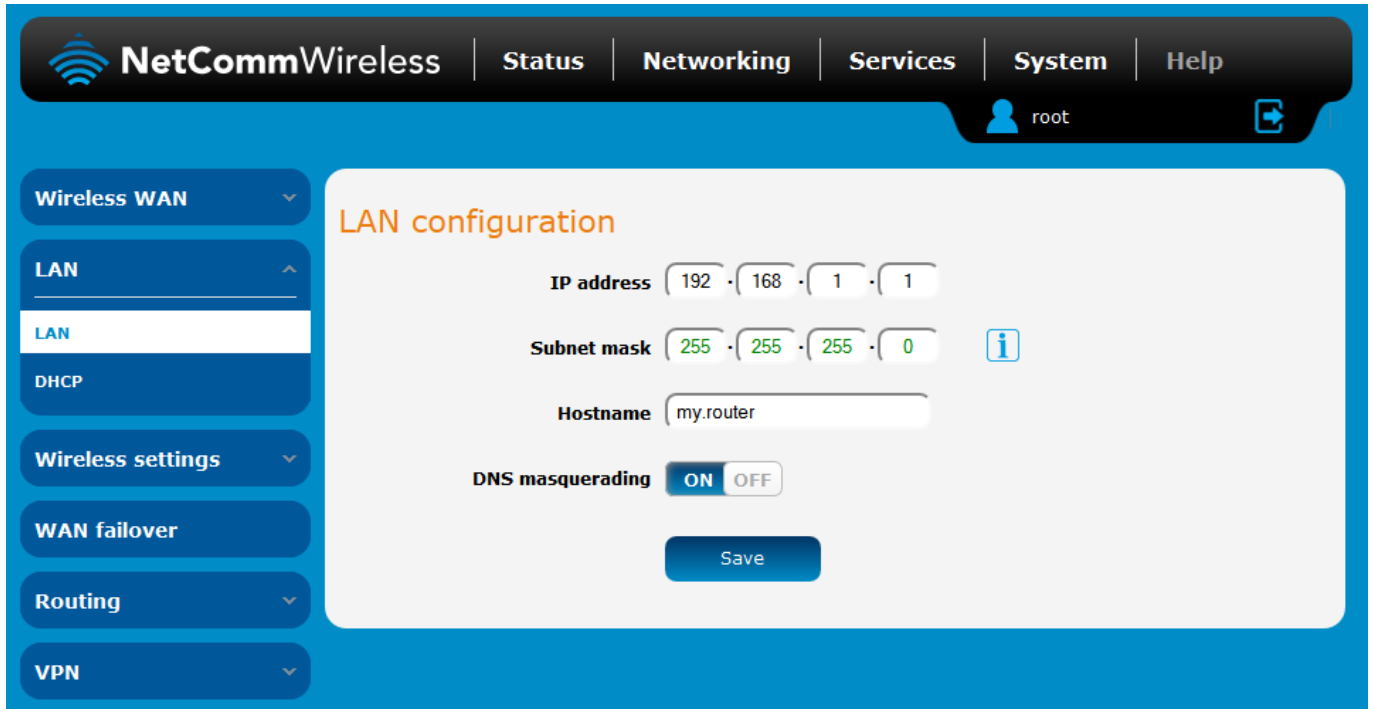


Figure 23 – LAN configuration settings

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



Note: If you change the IP address, remember to reboot the router and enter the new IP address into your browser address bar.

DNS masquerading

DNS masquerading allows the router to proxy DNS requests from LAN clients to dynamically assigned DNS servers. When enabled, clients on the router's LAN can then use the router as a DNS server without needing to know the dynamically assigned cellular network DNS servers.

With DNS masquerading **ON**, the DHCP server embedded in the NTC-40WV router hands out its own IP address (e.g. 192.168.1.1) as the DNS server address to LAN clients. The downstream clients then send DNS requests to the NTC-40WV router which proxies them to the upstream DNS servers.

With DNS masquerading **OFF**, the DHCP server hands out the upstream DNS server IP addresses to downstream clients directly, so that downstream clients send DNS requests directly to the upstream DNS servers without being proxied by the NTC-40WV router.

You may also override the DNS Masquerading option by specifying custom DNS Server IP addresses in the DHCP Server configuration mentioned in the next section of this guide. In this case the DHCP server assigns downstream devices the manually configured addresses and the DNS Masquerading option is ignored.

In most cases, it is not necessary to disable DNS masquerading but if you need to, click the **DNS masquerading** toggle key to turn it **OFF** and then click the **Save** button.

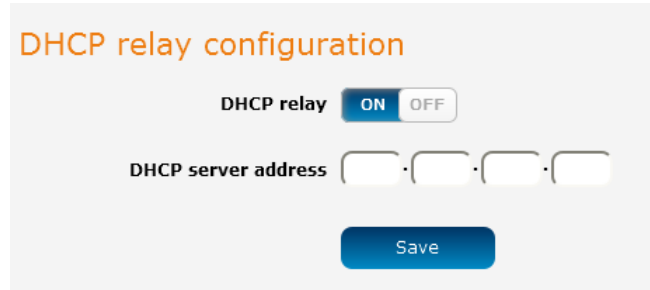
DHCP

The DHCP page is used to adjust the settings used by the router's built in DHCP Server which assigns IP addresses to locally connected devices.

DHCP relay configuration

In advanced networks configurations where the NTC-40WW router should not be responsible for DHCP assignment, but instead an existing DHCP server is located on the Wireless WAN or LAN connections, the clients behind the NTC-40WW router are able to communicate with the DHCP server when DHCP relay is enabled. This enables the NTC-40WW router to accept client broadcast messages and to forward them onto another subnet.

To configure the router to act as a DHCP relay agent click the **DHCP relay** toggle key to turn it **ON** and enter the DHCP server address into the **DHCP server address** field. DHCP relay is disabled by default.

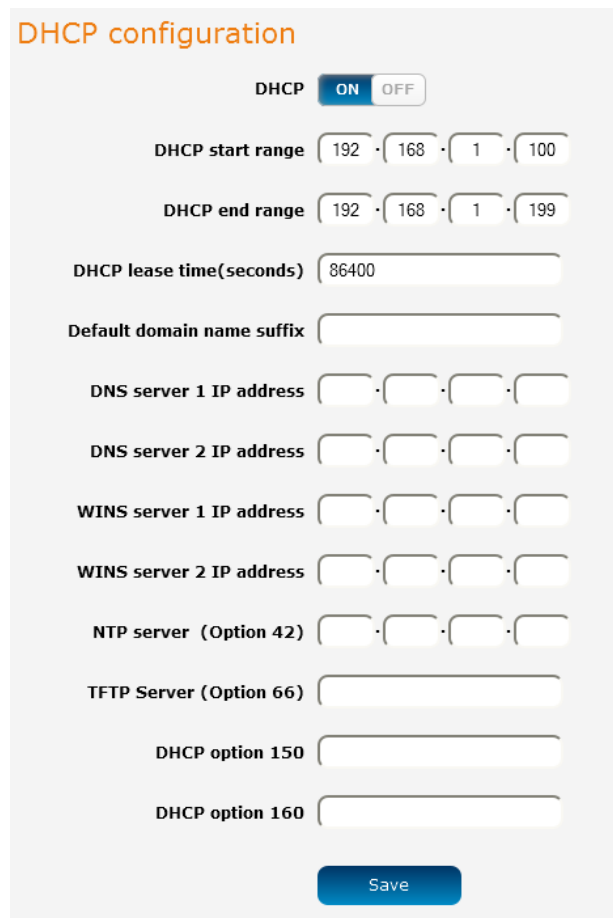


The screenshot shows the 'DHCP relay configuration' interface. At the top, the title 'DHCP relay configuration' is displayed in orange. Below it, there is a 'DHCP relay' toggle switch currently set to 'ON'. Underneath, the 'DHCP server address' field is shown as four empty input boxes separated by dots. At the bottom of the form is a blue 'Save' button.

Figure 24 – DHCP relay configuration

DHCP configuration

You can manually set the start and end address range to be used to automatically assign addresses within, the lease time of the assigned address, the default domain name suffix, primary and secondary DNS server, the primary and secondary WINS server, as well as the advanced DHCP settings such as NTP, TFTP and Option 150/Option 160 (VoIP options).



The screenshot shows the 'DHCP configuration' interface. The title 'DHCP configuration' is in orange. A 'DHCP' toggle switch is set to 'ON'. The 'DHCP start range' is set to 192.168.1.100 and the 'DHCP end range' is set to 192.168.1.199. The 'DHCP lease time(seconds)' is set to 86400. Below these are fields for 'Default domain name suffix', 'DNS server 1 IP address', 'DNS server 2 IP address', 'WINS server 1 IP address', 'WINS server 2 IP address', 'NTP server (Option 42)', 'TFTP Server (Option 66)', 'DHCP option 150', and 'DHCP option 160'. A blue 'Save' button is at the bottom.

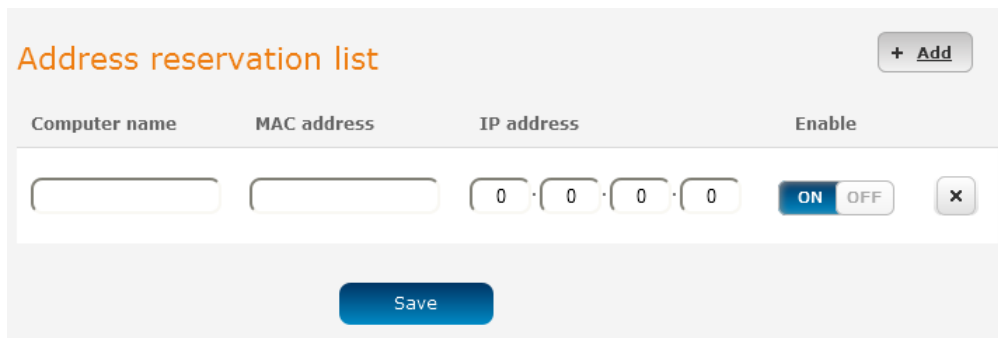
Figure 25 - DHCP configuration

OPTION	DESCRIPTION
DHCP start range	Sets the first IP address of the DHCP range
DHCP end range	Sets the last IP address of the DHCP range
DHCP lease time (seconds)	The length of time in seconds that DHCP allocated IP addresses are valid
Default domain name suffix	Specifies the default domain name suffix for the DHCP clients. A domain name suffix enables users to access a local server, for example, server1, without typing the full domain name server1.domain.com
DNS server 1 IP address	Specifies the primary DNS (Domain Name System) server's IP address.
DNS server 2 IP address	Specifies the secondary DNS (Domain Name System) server's IP address.
WINS server 1 IP address	Specifies the primary WINS (Windows Internet Name Service) server IP address
WINS server 2 IP address	Specifies the secondary WINS (Windows Internet Name Service) server IP address
NTP server (Option 42)	Specifies the IP address of the NTP (Network Time Protocol) server
TFTP Server (Option 66)	Specifies the TFTP (Trivial File Transfer Protocol) server
DHCP option 150	This is used to configure Cisco IP phones. When a Cisco IP phone starts, if it is not pre-configured with the IP address and TFTP address, it sends a request to the DHCP server to obtain this information. Specify the string which will be sent as a reply to the option 150 request.
DHCP option 160	This is used to configure Polycom IP phones. When a Polycom IP phone starts, if it is not pre-configured with the IP address and TFTP address, it sends a request to the DHCP server to obtain this information. Specify the string which will be sent as a reply to the option 160 request.

Enter the desired DHCP options and click the **Save** button.

Address reservation list

DHCP clients are dynamically assigned an IP address as they connect, but you can reserve an address for a particular device using the address reservation list.



The screenshot shows a web interface for configuring an address reservation list. At the top right, there is a '+ Add' button. Below it is a table with four columns: 'Computer name', 'MAC address', 'IP address', and 'Enable'. The 'Computer name' and 'MAC address' fields are empty text boxes. The 'IP address' field is a numeric input with four segments, each containing a '0'. To the right of the IP address field is a toggle switch labeled 'ON' and 'OFF', currently set to 'ON'. There is also a small 'x' icon to the right of the toggle. At the bottom center of the form is a blue 'Save' button.

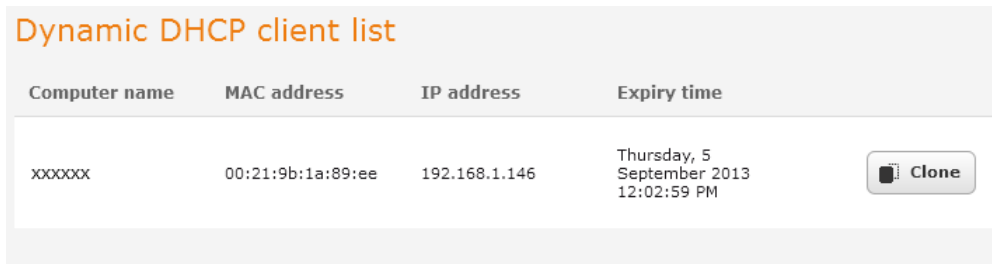
Figure 26 – DHCP – Address reservation list

To add a device to the address reservation list:

1. Click the **+Add** button.
2. In the **Computer Name** field enter a name for the device.
3. In the **MAC Address** field, enter the device's MAC address.
4. In the **IP Address** fields, enter the IP address that you wish to reserve for the device.
5. If the **Enable** toggle key is not set to **ON**, click it to switch it to the **ON** position.
6. Click the **Save** button to save the settings.

Dynamic DHCP client list

The Dynamic DHCP client list displays a list of the DHCP clients. If you want to reserve the current IP address for future use, click the **Clone** button and the details will be copied to the address reservation list fields. Remember to click the **Save** button under the **Address reservation list** section to confirm the configuration.



The screenshot shows a web interface titled "Dynamic DHCP client list". It contains a table with the following columns: "Computer name", "MAC address", "IP address", and "Expiry time". A single row of data is visible, with a "Clone" button to its right.


Computer name	MAC address	IP address	Expiry time	
xxxxxx	00:21:9b:1a:89:ee	192.168.1.146	Thursday, 5 September 2013 12:02:59 PM	

Figure 27 - Dynamic DHCP client list

Wireless settings

The Wireless Settings pages allow you to configure the WiFi settings of the router. The NTC-40WV is capable of running both access point and wireless client modes simultaneously, however, they must both use the same channel number.

AP basic

The basic page provides options for turning the WiFi access point on or off, modes of operation, frequency and security settings.

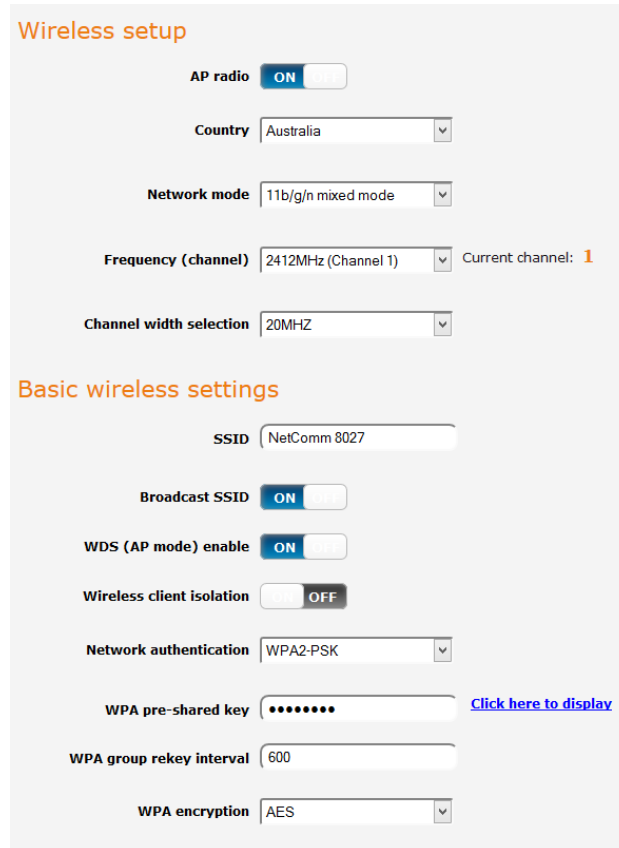


Figure 28 - Wireless Settings – Basic

OPTION	DEFINITION
AP radio on/off	WiFi is turned on by default. Changing this option to OFF will turn OFF the wireless access point functionality on the NTC-40WV and you will not be able to connect to it with a wireless client.
Country	Select the country you are operating the NTC-40WV in.
Network mode	There are 6 possible network modes to use depending on the capability of your devices' wireless network cards. Each mode represents one or more wireless network protocols. Each wireless device will be capable of receiving some but possibly not all of wireless broadcast protocol types. They are: <ul style="list-style-type: none"> • 802.11b/g/n mixed mode. • 802.11b only. • 802.11g only. • 802.11n only. • 802.11b/g/n mixed mode.
Frequency (Channel)	Select the wireless channel of the access point that the wireless signal will broadcast on.
Channel width selection	A higher channel width typically results in higher throughput, however, interference can lead to reduced performance. The 20 MHz channel width also allows legacy devices to be used.
SSID and security settings	
SSID	The SSID (Service Set Identifier or Network Name) in use for the wireless network.
Broadcast SSID	Toggles whether the router broadcasts the SSID or whether it is hidden from wireless network scans.
WDS (AP mode) enable	Toggles the WDS function in access point mode for this router. For more information, see the WDS section of this guide.
Wireless client isolation	When wireless client isolation is enabled, clients connected to the same network (SSID) are unable to communicate with other clients on the same network.
Network authentication	The wireless security settings. See below for in depth analysis.
WPA pre-shared key	The wireless security key or wireless password.
WPA group rekey interval	The time in seconds before a new key is generated.
WPA encryption	The type of WPA encryption. Currently only AES is allowed. TKIP options have been removed as the WiFi Alliance no longer considers it secure.

Table 11 - Wireless Configuration - Basic Configuration Items

AP advanced

The advanced wireless configuration page allows you to modify advanced wireless access point settings of your router. These settings are set to optimal settings for most situations and should not be changed unless you are aware of the effect that your changes will have.

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.

Maximum number of connected clients (range 1 - 127, default 31)

Client idle timeout sec (range 60 - 600, default 300)

Beacon interval ms (range 20 - 999, default 100)

Delivery traffic indication message(DTIM) rate beacon intervals (range 1 - 255, default 2)

Fragment threshold (range 256 - 2346, default 2346)

RTS threshold (range 1 - 2347, default 2347)

TX power (range 1 - 100, default 100)

Short preamble ON OFF

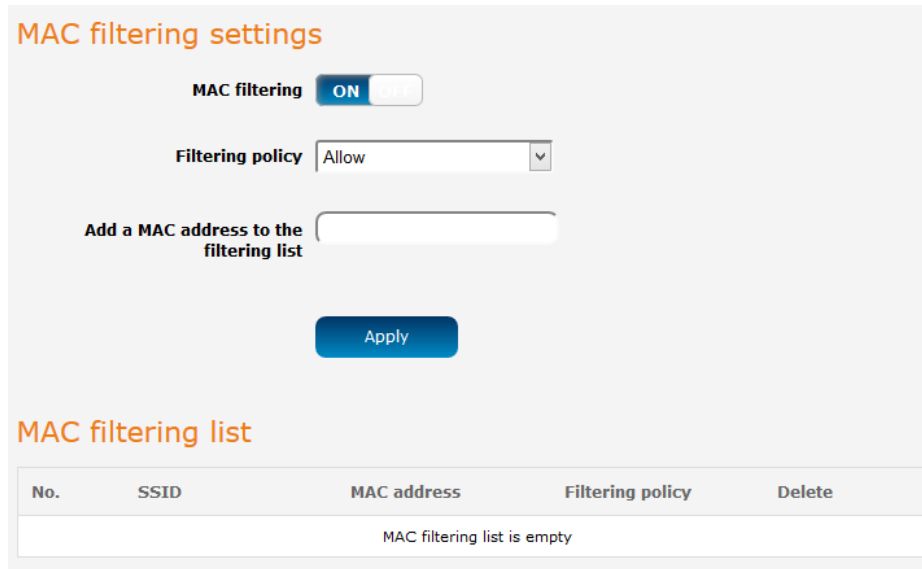
Figure 29 - Wireless Settings - Advanced

OPTION	DEFINITION
Maximum number of connected clients	The maximum number of wireless clients that may connect to the access point. The default setting is 31. This may be a maximum of 255.
Client idle timeout	The time in seconds that a wireless client session can be idle before the router cancels the session and defines the wireless client as not connected.
Beacon interval	Interval of time in which the wireless router broadcasts a beacon which is used to synchronize the wireless network.
Delivery traffic indication message (DTIM) rate.	Enter a value in milliseconds between 1 and 255 for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
Fragment threshold	This specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
RTS threshold	When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
TX power	This determines the transmitting or output power of the antenna.
Short preamble	Enable or disable short preambles in use on the wireless network. Using short preambles should improve throughput, however some wireless network adapters must use long preambles.

Table 12 - Wireless Settings - Advanced Configuration Items

AP MAC filtering

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



MAC filtering settings

MAC filtering ON OFF

Filtering policy

Add a MAC address to the filtering list

MAC filtering list

No.	SSID	MAC address	Filtering policy	Delete
MAC filtering list is empty				

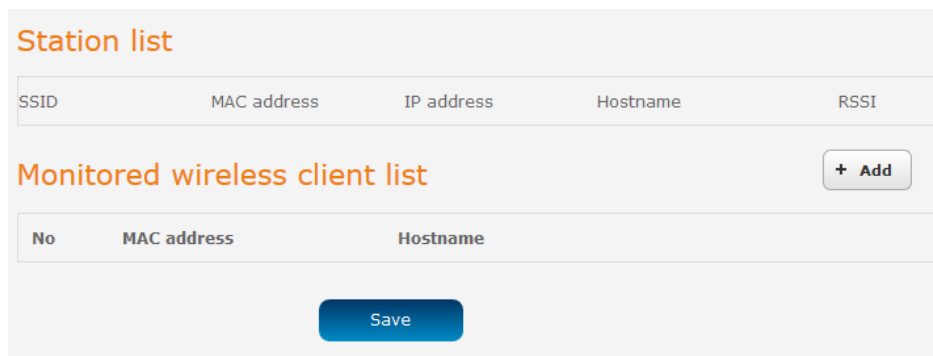
Figure 30 - MAC Filtering

AP station info

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

Monitoring a wireless client

The Event notification feature provides the ability to send alerts when certain events occurs on the router. One of these is to send alerts when a monitored client connects or disconnects. To monitor a connected client, click the **Monitor** button corresponding to its entry in the Station list. Alternatively, you can manually add a wireless client to the monitored wireless client list by clicking on the **+Add** button, then entering the MAC address and Hostname in the appropriate fields that appear in the list. When you have finished selecting clients to monitor, click the **Save** button.



Station list

SSID	MAC address	IP address	Hostname	RSSI
(Empty list)				

Monitored wireless client list

No	MAC address	Hostname
(Empty list)		

Figure 31 - Wireless Station List

AP hotspot

The wireless hotspot feature provides internet access to WiFi clients with the option of forcing users to agree to terms of use. This feature is often used where wireless access is provided to customers in a public area and allows you to configure a speed limit on the network, limit the number of clients, configure idle and session timeouts and select to authenticate with remote RADIUS servers.

To access the AP hotspot page, click on the **Networking** menu at the top of the screen, click on the **Wireless settings** menu on the left then select the **AP hotspot** menu item.

To enable the hotspot:

Select the **Hotspot functionality** toggle key so that it is in the **ON** position.

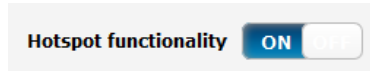


Figure 32 – Hotspot functionality toggle key

If the wireless AP radio is not enabled, you are presented with the following message.

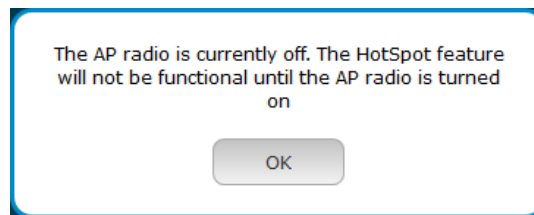


Figure 33 – AP radio is off notification

In this case, select the **AP basic settings** menu item on the left, select the **AP mode** toggle key so that it is in the **ON** position, then click the **Save** button.

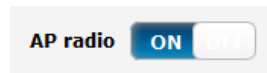


Figure 34 – AP mode toggle key

Select the **AP hotspot** menu item on the left and select the Hotspot functionality toggle key so that it is in the ON position. Additional options are displayed. Refer to the screenshot and table below for further details. When you have finished configuring the hotspot settings, click the **Save** button.




Note: When using the Hotspot feature, we recommend that you set the Network authentication mode on the Basic page for the Hotspot's SSID to **Open** so that wireless users are not made to authenticate twice.

Wireless hotspot configuration

Hotspot functionality ON OFF

Public hotspot service ON OFF

SSID

Max client connections (1-127) 

Max downlink bandwidth kbits/second

Max uplink bandwidth kbits/second

Session timeout minutes

Idle timeout minutes

Starting IP address · · ·

Netmask · · ·

Authentication options

Local user settings

Radius settings

Router access permissions

Local LAN ON OFF

Router management interface ON OFF

Page redirect

Page redirect ON OFF

Redirect URL (exclude http://)

Page customization

Upload file (tar.gz,zip,bz2)

Customization files usage

Use default files

Use uploaded customization files

Landing page filename

Landing page

Landing page

Terms of use

Internal terms of use Simple text message


External terms of use URL of terms of use page 

Figure 35 - Wireless hotspot configuration

ITEM	DESCRIPTION
Hotspot functionality	Turns the wireless hotspot feature on or off.
Public hotspot service	When enabled, you may configure a managed public hotspot service account.
LAN interface	Specifies the LAN interface to use for the wireless hotspot.
Max client connections	The maximum number of wireless clients permitted to connect to the wireless hotspot.
Max downlink bandwidth	The maximum downlink speed in kilobits per second.
Max uplink bandwidth	The maximum uplink speed in kilobits per second.
Session timeout	The number of minutes that a client may use the WAN connection before being forced to authenticate again.
Idle timeout	The number of minutes that a client may be idle before being forced to authenticate again.
Starting IP address	The starting IP address for the wireless hotspot network. The starting IP address is assigned to the router and subsequent addresses are assigned to clients as they connect.
Netmask	The network mask of the LAN IP range.
Authentication option	Selects whether to use the Local user settings or a remote RADIUS server to authenticate users on the wireless hotspot.
Radius settings	
Radius server 1	Primary RADIUS Server domain name e.g. radius.netcomm.com
Radius server 2	Backup RADIUS Server domain name e.g. radius.netcomm.com
Authentication port	The port used for RADIUS authentication e.g. 1205
SSID	This is usually the SSID of the hotspot and is used during the authentication process.
Shared secret	The WPA pre-shared key on the wireless network.
Re-enter shared secret	The WPA pre-shared key on the wireless network.
Page redirect	
Page redirect	Page redirect: redirects the user to a specified website after they have authenticated or agreed to terms of use. Allow internet access: allows internet access upon successful authentication or agreement with terms of use.
Redirect URL	Enter the URL (excluding http://) that you wish to redirect the user to after they have agreed to the terms of use.
Router access permissions	
Local LAN	Turning this on allows wireless hotspot clients to access clients on the local LAN and vice versa.
Router management interface	Turning this on allows wireless hotspot clients to access the router's management interface.
Page customization	
Upload file	You can package your own HTML files in a .zip, .tar.gz or .bz2 file to use as a landing page. Click the "Choose a file" button then locate the archive on your computer. Click the "Upload" button to send the archive to the router.
Customization files usage	This allows you to select whether to use the default landing page files or to use a customized set that you have uploaded.
Landing page filename	Enter the name of the file in your landing page archive that you wish to use as the initial landing page.
Terms of use	
Internal terms of use	Enter the terms and conditions as a standard text message in this field.
External terms of use	Select this option to use a terms of use page which is remote. Enter the URL of the page excluding http://

Table 13 – Wireless hotspot settings



Note: Some web browsers may experience an issue where a reconfiguration of the "External terms of use" URL causes the terms and conditions link to refresh the hotspot login page. To work around this problem, clear the web browser's cache.

Client configuration

As a wireless client, the NTC-40WV is able to connect to another wireless access point to gain network or internet access. The Client configuration page provides the ability to turn on or off the wireless radio, find nearby access points and configure a connection to an access point.

The NTC-40WV may run both Access Point and Client simultaneously, however, since they share the wireless channel, both client and access point must use the same channel.

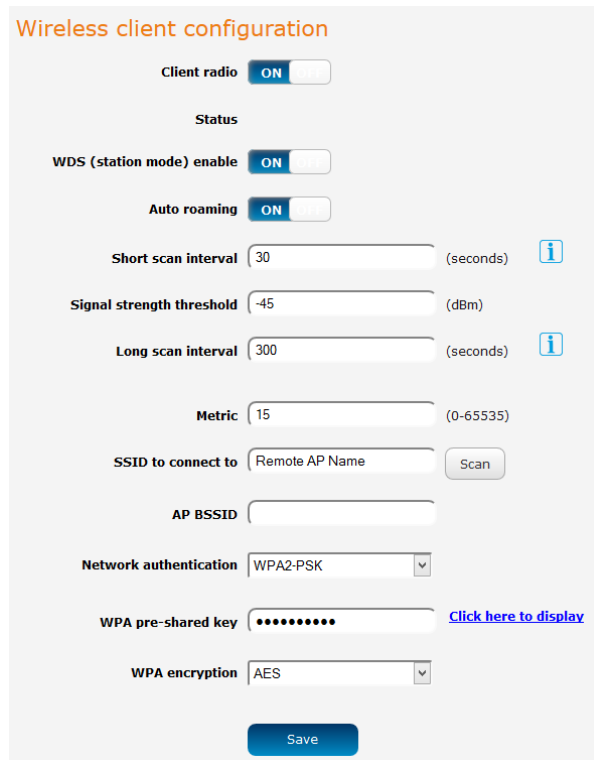


Figure 36 - Wireless settings - Client configuration

OPTION	DEFINITION
Client radio on/off	Turns the wireless radio on or off.
Status	Displays the current channel and connection status of the wireless client.
Auto roaming	Toggles the automatic roaming feature of the router. This is useful in situations where the router is mounted in a vehicle and is required to connect to various wireless routers with the same SSID. When this is enabled, the AP BSSID field is ignored.
Short scan interval	When the wireless signal strength is above (weaker than) the value listed in the Signal strength threshold field, the router scans for wireless networks at this interval.
Signal strength threshold	The signal strength threshold that determines whether the router considers the WiFi signal to be weak and therefore which scan interval to use to scan for another wireless network.
Long scan interval	When the wireless signal strength is below (stronger than) the value listed in the Signal strength threshold field, the router scans for wireless networks at this interval.
Metric	The metric value is used by the router to prioritise routes.
SSID to connect	Enter the SSID of the network you wish to connect to or you may use the Scan button to discover nearby networks.
AP BSSID	The BSSID or MAC address of the access point to which you are connecting.
Frequency (channel)	The channel to be used for the client connection. This must be the same as the channel in operation on the access point function of the NTC-40WV as the channel is shared between the functions.
Network authentication	The type of authentication in use on the network.
WPA pre-shared key	Enter the pre-shared key required to join the wireless network.
WPA encryption	Select the type of encryption in use on the network.

Table 14 - Wireless settings – Client Configuration

Scanning for a network

To find a nearby network to connect to, click the **Scan** button. A list of discovered networks appears at the bottom of the screen. Click the corresponding **Connect** button for the network to which you would like to connect.

Access Point List

No.	SSID	BSSID	Security	Channel	Signal Strength	Wireless Mode	Action
1	XXXXXXXXXX	00:04:ed:ef:c1:19	WPA2PSK/TKIPAES	1	99	11b/g/n	Connect
2	XXXXXXXXXX	4c:5e:0c:43:a5:e7	NONE	1	100	11b/g/n	Connect
3	XXXXXXXXXX	6a:04:ed:ef:c1:1a	WPA1PSKWPA2PSK/TKIPAES	1	94	11b/g/n	Connect
4	XXXXXXXXXX	00:1f:a4:92:d4:fb	WPA2PSK/AES	1	100	11b/g/n	Connect

Figure 37 - Access point list

The network's details are copied across to the Client configuration page. If the wireless network is secured, enter the authentication details, then click the **Save** button.

Wireless Distribution System (WDS)

What is WDS?

A wireless distribution system (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. WDS makes it possible to configure a network where a single router acts as a gateway while other routers in the network provide additional geographical coverage for wireless clients, acting as bridges and redirecting traffic through the same gateway. WDS provides layer 2 bridging and preserves the MAC addresses of stations connected through the WDS network. The advantage of WDS when compared with a daisy chain of access points is that you can have one network covering a larger geographical area and allow those clients to easily roam between the access points while retaining their IP addresses. It also means that they are not isolated from each other and allows for easier configuration since you do not need to configure many port forwarding rules on each access point.

The NetComm Wireless NTC-30WW and NTC-40WW routers use the 4-address frame format specified in the IEEE 802.11-1999 standard, but since the standard does not define how stations should interact to exchange frames in this format, the WDS function on NetComm Wireless routers is not guaranteed to work with implementations from other vendors.

Configuring WDS

The following instructions describe how to configure a basic WDS setup between two routers where one of them has an active SIM card and acts as an access point and another which has no SIM card and connects to the AP as a client in order to provide network access to its wireless clients. The diagram below illustrates the network configuration.

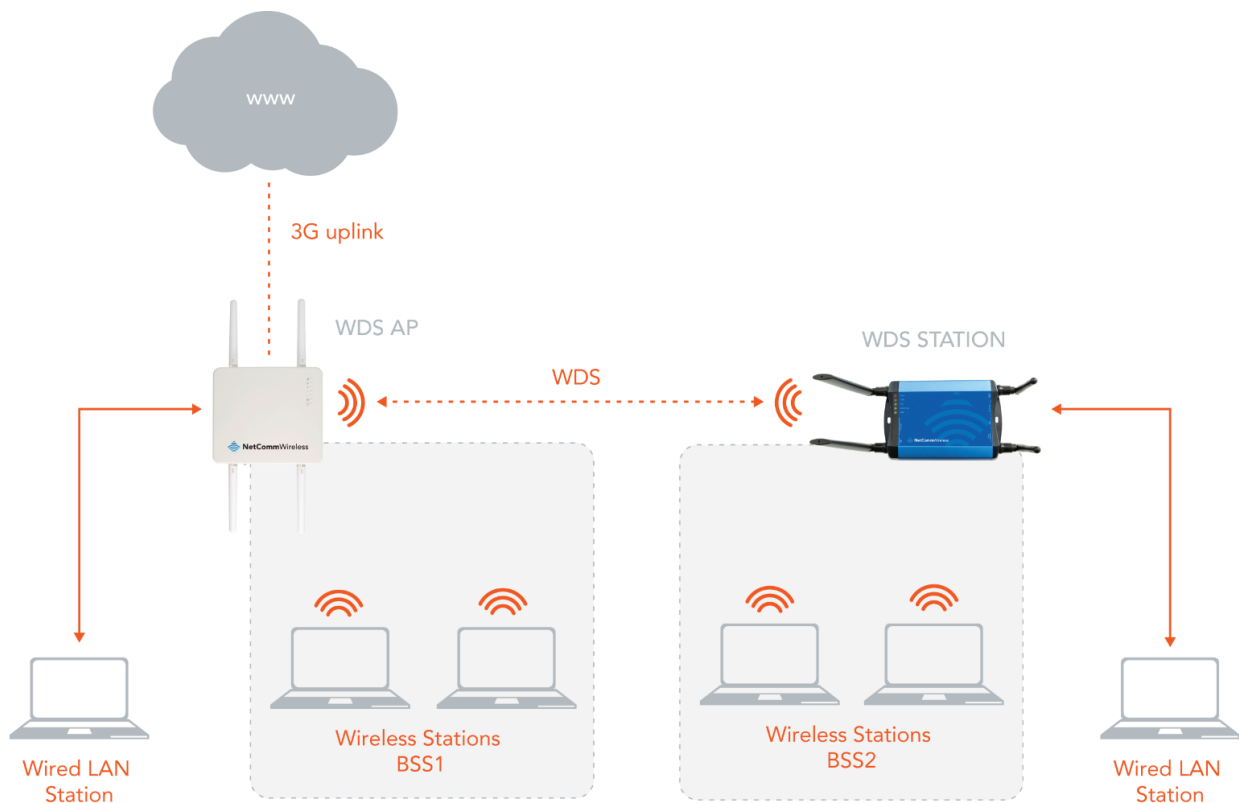


Figure 38 - Basic WDS configuration example



Note:

- The device acting as a client (station) must have DHCP disabled and must not have the same IP address or an IP address within the DHCP range of the WDS AP.
- The following features are incompatible with WDS:
 - WDS Access Point: Hot spot, Wireless client isolation
 - WDS Station: WiFi interface cannot be used as one of the failover interfaces, no auto roaming.

WDS AP configuration

1. Navigate to **Networking -> Wireless settings -> AP basic**.
2. Ensure that the **AP radio** toggle key is set to the **ON** position.
3. In the **Frequency (channel)** drop down list, select a channel. WDS cannot operate when the access point is set to AUTO, so you must select a specific channel.
4. In the **SSID** field, enter a network name for the WDS network.
5. Select the **WDS (AP mode) enable** toggle key so that it is in the **ON** position.
6. Set the other wireless settings as you require. Refer to the [AP basic](#) section for further detail.

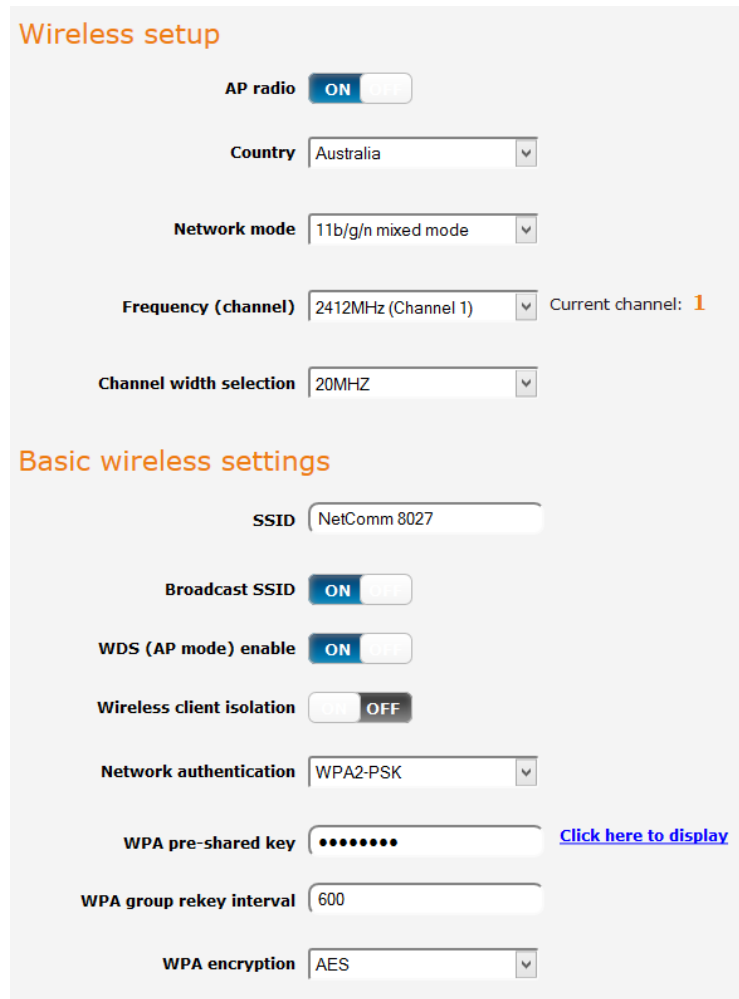


Figure 39 - WDS AP example configuration

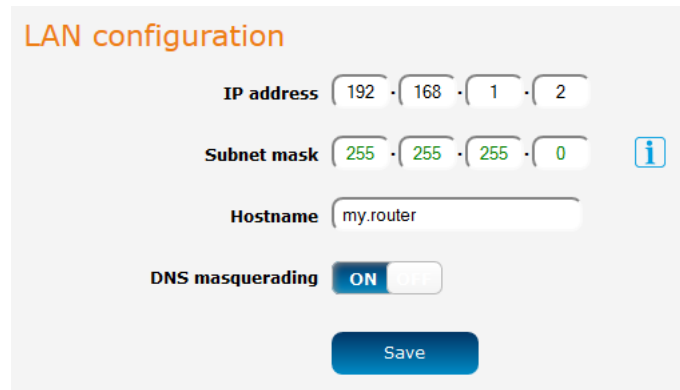
7. Click the **Save** button. A warning is displayed.

Warning: Please note that if you change your Security Key or Network Name and you are connected to this router wirelessly, then you will need to re-scan and re-connect to this router with the new settings after applying your changes. Are you sure you want to continue?

Click the **OK** button. Your settings are saved.

WDS Station configuration

1. Navigate to **Networking -> LAN -> LAN**. Change the IP address of the router so that it is not the same as the WDS AP's address or in the WDS AP's DHCP range. In this example, the WDS station is configured to have the IP address 192.168.1.2 while the WDS AP is 192.168.1.1.



The screenshot shows the 'LAN configuration' page. It features four input fields: 'IP address' with values 192, 168, 1, and 2; 'Subnet mask' with values 255, 255, 255, and 0; 'Hostname' with the value 'my.router'; and a 'DNS masquerading' toggle switch currently set to 'ON'. A blue 'Save' button is located at the bottom of the form.

Figure 40 - WDS Station - LAN configuration

2. Navigate to **Networking -> LAN -> DHCP**. Click the **DHCP** toggle key to turn DHCP **OFF**.



The screenshot shows two sections: 'DHCP relay configuration' with a toggle switch set to 'OFF', and 'DHCP configuration' with a toggle switch also set to 'OFF'. A blue 'Save' button is at the bottom.

Figure 41 - WDS Station - DHCP configuration

3. Click the **Save** button.
4. Navigate to **Networking -> Wireless settings -> AP basic**
5. Use the **Frequency (channel)** drop down list to select the same channel you chose for the WDS AP.
6. In the **SSID** field, enter the same network name that you entered for the WDS AP and ensure that the security settings are identical to the WDS AP settings. Note that for a basic two participant network, the device acting as the station does not require **WDS (AP mode) enable** turned on.

Wireless setup

AP radio ON

Country

Network mode

Frequency (channel) Current channel: **1**

Channel width selection

Basic wireless settings

SSID

Broadcast SSID ON

WDS (AP mode) enable ON OFF

Wireless client isolation ON OFF

Network authentication

WPA pre-shared key [Click here to display](#)

WPA group rekey interval

WPA encryption

Figure 42 - WDS Station AP basic page example configuration

7. Click the **Save** button.

Warning: Please note that if you change your Security Key or Network Name and you are connected to this router wirelessly, then you will need to re-scan and re-connect to this router with the new settings after applying your changes. Are you sure you want to continue?

Click the **OK** button.

8. Navigate to **Networking -> Wireless settings -> Client configuration**.
9. Click the **Client radio** toggle key so that it is in the **ON** position.
10. Click the **Save** button.
11. Next to the **SSID to connect to** field, click the **Scan** button. A list of discovered networks appears at the bottom of the page. Find the SSID (network name) that you configured on the WDS AP and click the corresponding **Connect** button.

24	NetComm 8027	00:60:64:11:11:20	WPA2-PSK	AES	1	-63.00	<input type="button" value="Connect"/>
----	--------------	-------------------	----------	-----	---	--------	--

The WPA-pre-shared key field is selected, prompting you to enter the passphrase to connect to the access point. Enter the pre-shared key, and ensure that other settings such as the WPA encryption are the same as the WDS AP, then click the **Save** button.

Wireless client configuration

Client radio ON OFF

Status

WDS (station mode) enable ON OFF

Auto roaming ON OFF

Metric (0-65535)

SSID to connect to

AP BSSID

Network authentication

WPA pre-shared key [Click here to display](#)

WPA encryption

Figure 43 - WDS Station Client configuration example

12. Confirm that the WDS network is active by viewing Status page of both the WDS AP and the WDS Station. Note that the WDS AP displays 1 Active WDS station/peer and the WDS Station status page shows it is in WDS mode with the Status “up”.

WLAN AP status

#	Status	Network Name (SSID)	MAC address	Channel	Network authentication	Station info
1	Enabled	NetComm 8027	00:60:64:11:11:20	1	WPA2PSK	Station info

Active WDS stations/peers

1

Figure 44 - WDS AP Status page

WLAN client connection status

Remote SSID NetComm 8027	Security WPA2PSK	Status up
BSSID 00:60:64:11:11:20	Upstream AP MAC address 00:60:64:11:11:20	Mode WDS

Figure 45 - WDS Station Status page

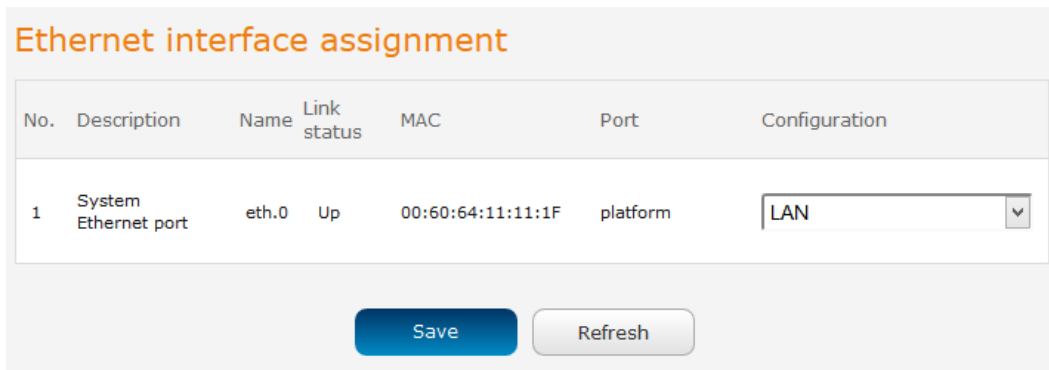
Ethernet LAN/WAN

The Ethernet LAN/WAN pages provide configuration options for the built-in Ethernet port.

Interface assignment

The Interface assignment page displays the Ethernet interfaces and allows you to configure whether they operate in LAN or WAN mode.

To access the Interface assignment page, click on the **Networking** menu at the top of the screen, click on the **Ethernet LAN/WAN** menu on the left then select the **Ethernet group** menu item.



No.	Description	Name	Link status	MAC	Port	Configuration
1	System Ethernet port	eth.0	Up	00:60:64:11:11:1F	platform	LAN

Figure 46 - Ethernet WAN interface assignment

OPTION	DEFINITION
#	A number identifying the interface on the router.
Description	A description of the type of interface.
Name	The name used to identify the interface on the router.
Link status	Displays whether the interface is inserted
MAC	The MAC address of the interface.
Port	The type of port.
Configuration	Select whether the port operates as a LAN or WAN port.

Table 15 - Ethernet group configuration items



Note: When you assign a WAN configuration to the Ethernet port, you will no longer be able to access the router interface via the Ethernet port. Please ensure that you have configured WiFi or remote access over the 3G network before configuring the Ethernet port as a WAN interface.

WAN configuration

The WAN configuration page allows you to configure the connection type and metric of the available WAN connections. To access the WAN configuration page, click on the **Networking** menu at the top of the screen, click on the **Ethernet LAN/WAN** menu on the left then select the **Ethernet WAN** menu item.

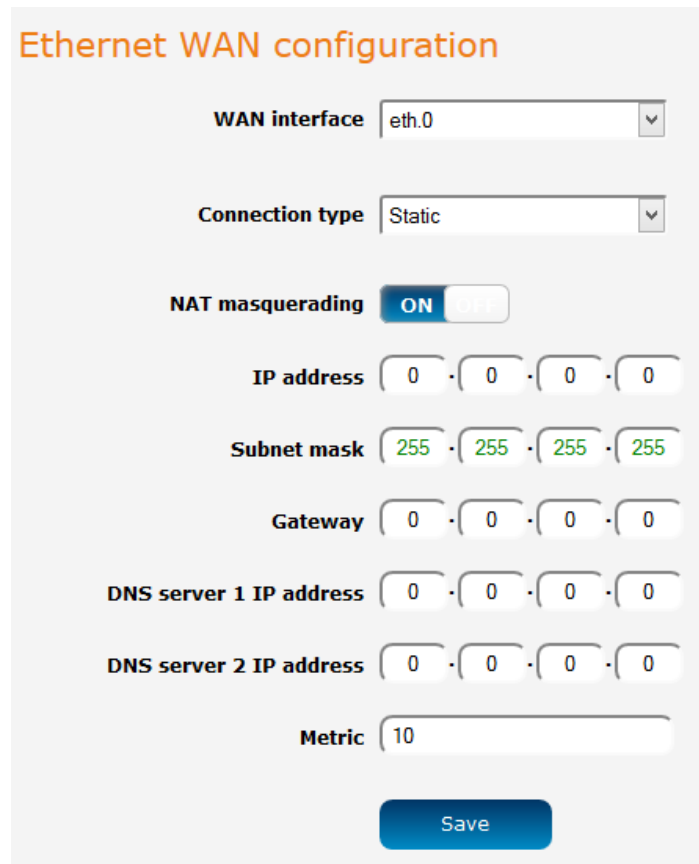


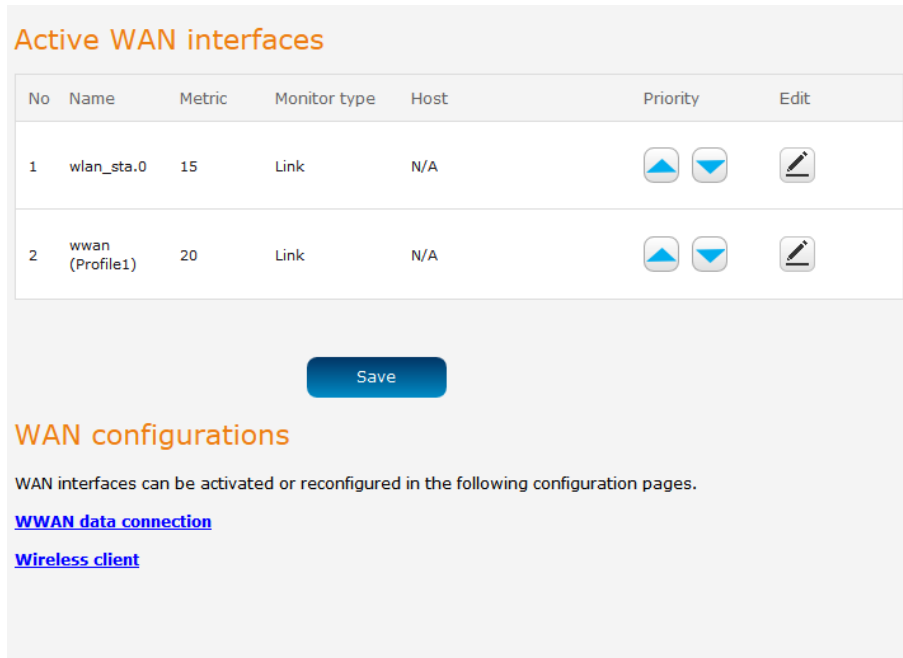
Figure 47 - Ethernet WAN configuration

OPTION	DEFINITION
WAN Ethernet	Use this field to select the WAN interface to configure.
Connection Type	Selects whether the WAN interface has static IP settings or DHCP.
NAT masquerading	NAT masquerading allows the router to modify the packets sent and received to inform remote computers on the internet that packets originating from a machine behind the router actually originated from the WAN IP address of the router's internal NAT IP address.
IP address	The IP address to assign to the selected WAN interface.
Subnet mask	The Subnet mask of the IP address above.
Gateway	The gateway to assign this WAN interface.
DNS server 1 IP address	The first DNS server for the WAN interface.
DNS server 2 IP address	The second DNS server for the WAN interface.
Metric	The metric value is used to define the priority of the interface. Lower metric values indicate higher priority.



Table 16 - Ethernet WAN configuration options

WAN failover

The WAN failover page displays a summary of the configured WAN interfaces and their priorities (Metric). Lower metric values determine higher priority. The priority of the interfaces can be adjusted using the up and down arrows in the Priority column. When the interface with the highest priority goes down, the router fails over to the next highest priority interface. The method used to determine whether an interface is “up” or “down” is defined by the Monitor setting.



Active WAN interfaces

No	Name	Metric	Monitor type	Host	Priority	Edit
1	wlan_sta.0	15	Link	N/A	<input type="button" value="▲"/> <input type="button" value="▼"/>	
2	wwan (Profile1)	20	Link	N/A	<input type="button" value="▲"/> <input type="button" value="▼"/>	

Save

WAN configurations

WAN interfaces can be activated or reconfigured in the following configuration pages.

[WWAN data connection](#)

[Wireless client](#)

Figure 48 - WAN summary

To edit an interface, select the edit icon for the interface you wish to edit. The Failover configuration page is displayed.



Failover configuration - wlan_sta.0

Priority

Monitoring method

Verbose logging ON OFF

back

Figure 49 – Failover configuration – hardware link

OPTION	DESCRIPTION
Priority	The priority (metric) is a numeric value which determines which interface has priority. Lower priority values mean higher priority.
Monitoring method	Specifies the means used to determine whether the link is up or down.
Verbose logging	When enabled, this logs verbose comments in the system log related to the failover monitoring.

Table 17 - Failover configuration - Hardware link monitoring

Link monitor

By default, an interface is monitored by its link status. This means that the router switches to the WWAN (Profile1) interface when the physical link to eth.0 is broken (i.e. the cable is disconnected or some other hardware fault causes the physical connection to fail). If this is your preferred method of monitoring, select the **Hardware link** option and click the **Save** button to complete the configuration.

Ping monitor

Alternatively, controlled ping packets can be used to determine the status of the link. These are small packets of data that the router sends to a remote address and if the connection is healthy, a reply is received. They are sent indefinitely at regular intervals that you specify. For each WAN interface that is ping monitored, you may specify two separate internet addresses and interval timers for the tests.

Each WAN interface is independently monitored according to its own distinct settings, following the process outlined below.

- At a regular interval stipulated by the **Periodic ping timer** setting, the router sends 3 ping requests via the interface to both the first and second destination addresses simultaneously. If it receives a reply to any of those pings, it deems the connection to be healthy and continues pinging them at the **Periodic ping timer** interval.
- If the router does not receive a response to all six pings by the start of the next **Periodic ping timer** interval, it registers this failure as a **Fail count** and continues to send pings to both destination addresses at the **Retry timer** interval (typically set at a shorter interval than the Periodic ping timer since there may be a problem). If a response is received to any of those pings, the router returns to sending pings according to the **Periodic ping timer** setting.
- However, if after another period defined by the **Retry timer** setting the router again does not receive a response to any of the pings, it registers another **Fail count**.
- The router repeats the retry process until it either receives a ping response (and returns to testing the interface according to the **Periodic ping timer**) or the number configured in the **Fail count** field is reached. In the latter case, that ping monitored interface is marked as unavailable, at which point the router automatically reroutes packets according to the configured priorities of the remaining WAN interfaces.

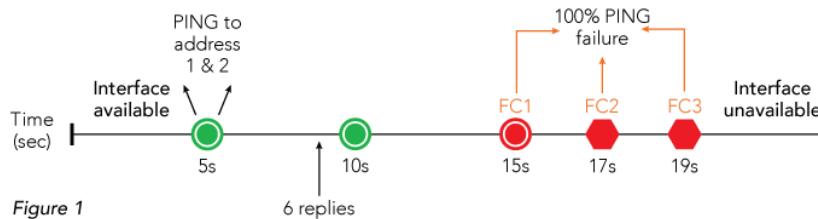


Figure 1

- The process for returning an unavailable interface to an available state is similar to the above process. When an interface is marked unavailable by the ping monitor, the router continues to retry pings to the two destination addresses via that interface according to the **Retry timer** setting until it receives a 100% successful response to the six pings before the next retry. The router then switches to the **Periodic ping timer** interval, waiting for 100% successful responses for an amount of consecutive periods that equal the configured **Fail count** setting, at which point the WAN interface is marked available.

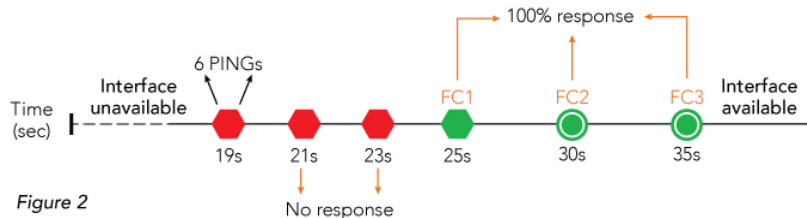
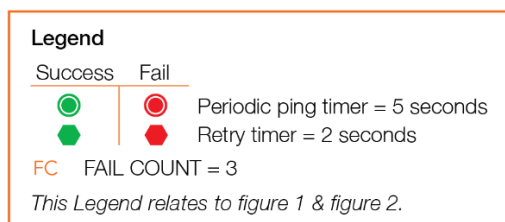


Figure 2



To configure the ping monitor type:

1. Select the Edit  button corresponding to the eth.0 interface.

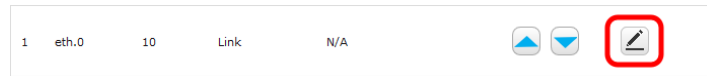
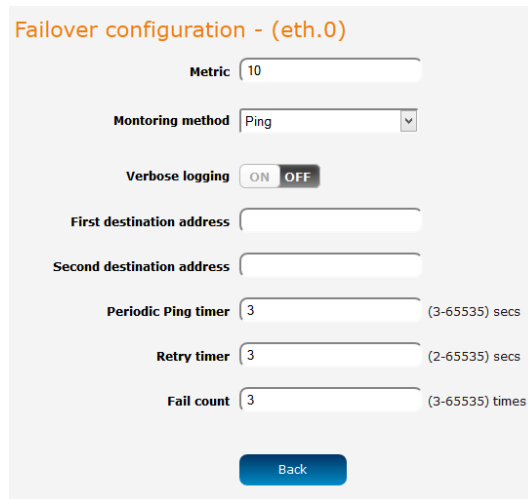


Figure 50 - Ping monitor Edit option

2. Use the **Monitoring method** drop down list to select **Ping**.



Failover configuration - (eth.0)

Metric:

Monitoring method:

Verbose logging: ON OFF

First destination address:

Second destination address:

Periodic Ping timer: (3-65535) secs

Retry timer: (2-65535) secs

Fail count: (3-65535) times

Figure 51 - Ping monitor fail over configuration

3. In the **First destination address** field, enter a website address or IP address to which the router should send the first round of ping requests.
4. In the **Second destination address** field, enter a website address or IP address to which the router should send the second round of ping requests.
5. In the **Periodic Ping timer** field, enter an integer between 3 and 65535 for the number of seconds the router should wait between ping attempts.
6. In the **Retry timer** field, enter an integer between 2 and 65535 for the number of seconds the router should wait between retry ping attempts, i.e. pings to the second destination address.
7. In the **Fail count** field, enter an integer between 3 and 65535 for the number of times a retry ping should fail before the router fails over to the next WAN interface. Click the **Back** button.

The Active WAN interfaces are displayed once again, this time showing that the Ping monitor type is in use for eth.0 and the host which will be pinged.

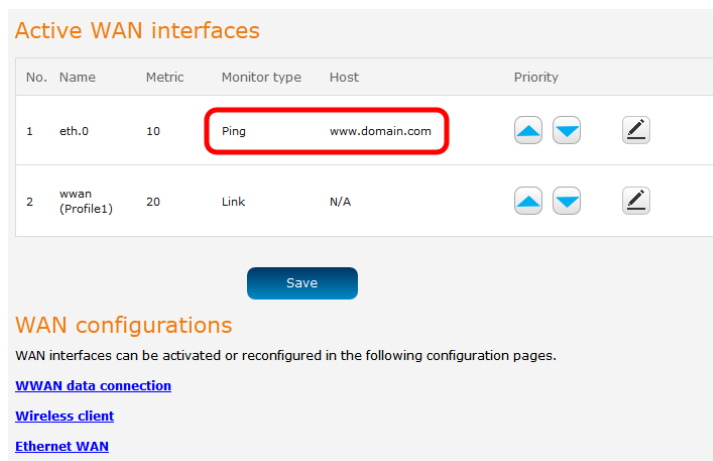


Figure 52 - Active WAN interfaces

Click the **Save** button to save the settings. The WAN failover configuration is complete.

Routing

Static

Static routing is the alternative to dynamic routing used in more complex network scenarios and is used to facilitate communication between devices on different networks. Static routing involves configuring the routers in your network with all the information necessary to allow the packets to be forwarded to the correct destination. If you change the IP address of one of the devices in the static route, the route will be broken.

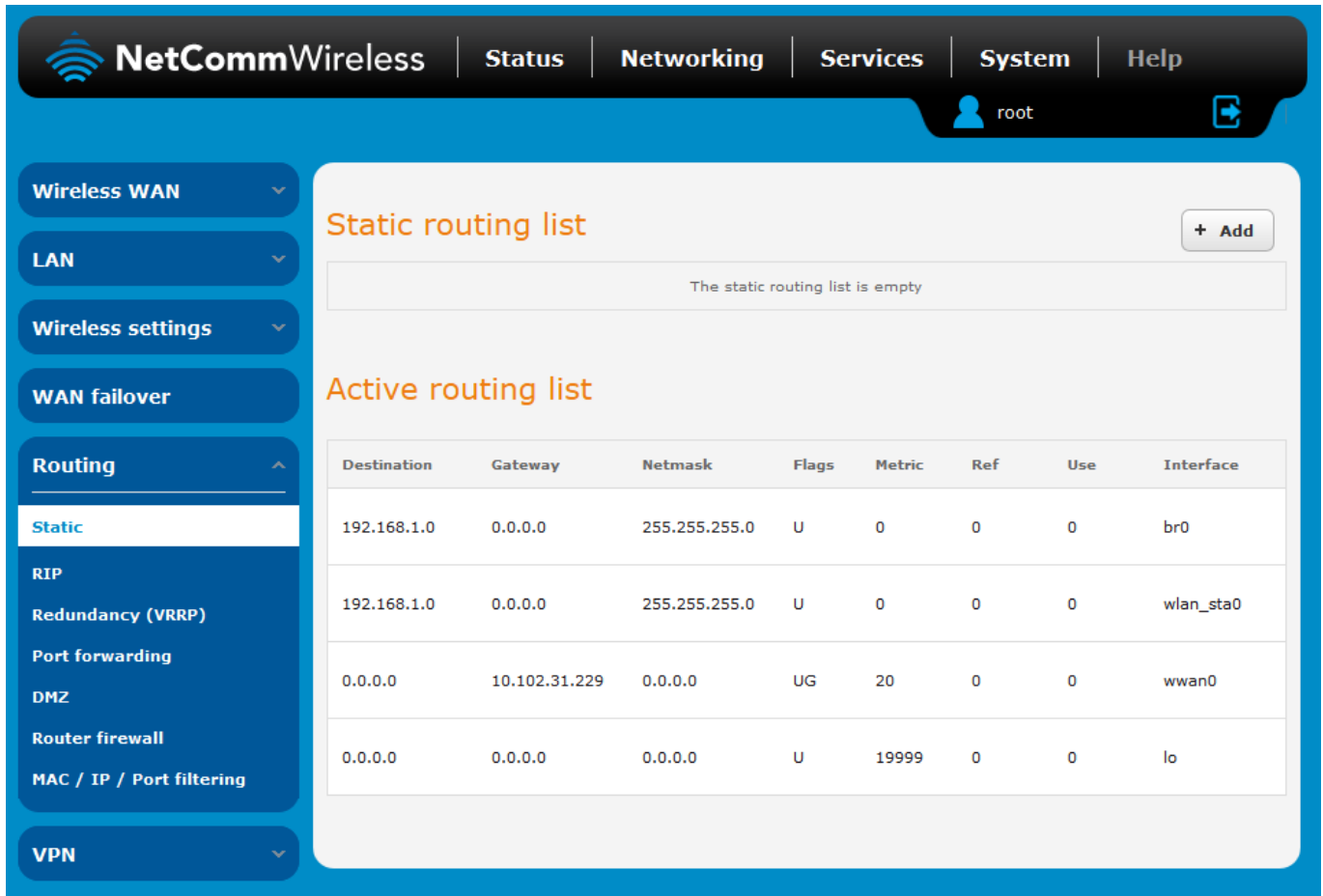


Figure 53 - Static routing list

Some routes are added by default by the router on initialization such as the Ethernet subnet route for routing to a device on the Ethernet subnet.

Adding Static Routes

To add a new route to the static routing list, click the **+Add** button. The Static routes page appears.

1. In the **Route name** field, type a name for the route so that it can be identified in the static routing list.
2. From the **Network interface** drop down list, select the interface for which you would like to create a static route.
3. In the **Destination IP address** field, enter the IP address of the destination of the route.
4. In the **IP subnet mask** field, enter the subnet mask of the route.
5. In the **Gateway IP address** field, enter the IP address of the gateway that will facilitate the route.
6. In the **Metric** field enter the metric for the route. The metric value is used by the router to prioritise routes. The lower the value, the higher the priority. To give the route the highest priority, set it to 0.
7. Click the **Save** button to save your settings.

Static routes

Route name

Network interface

Destination network address · · ·

Destination subnet mask · · ·

Gateway IP address · · ·

Metric (0-65535)

Figure 54 - Adding a static route

Active routing list

Static routes are displayed in the Active routing list.

Active routing list

Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Interface
0.0.0.0	10.100.157.33	0.0.0.0	UG	20	0	0	wwan0
10.100.157.32	0.0.0.0	255.255.255.240	U	0	0	0	wwan0
10.100.157.39	0.0.0.0	255.255.255.255	UH	0	0	0	wwan0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
192.168.20.0	192.168.1.101	255.255.255.0	UG	0	0	0	br0

Figure 55 - Active routing list

Deleting static routes

From the static routing list, click the  icon to the right of the entry you wish to delete.

Static routing list



Route name	Destination network address	Subnet mask	Gateway IP address	Network interface	Metric		
MyRoute	192.168.20.0	255.255.255.0	192.168.1.101	auto	0		

Figure 56 - Deleting a static route

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. Static routes must be added manually according to your requirements. See [Adding Static Routes](#).



Note: Some routers will ignore RIP.

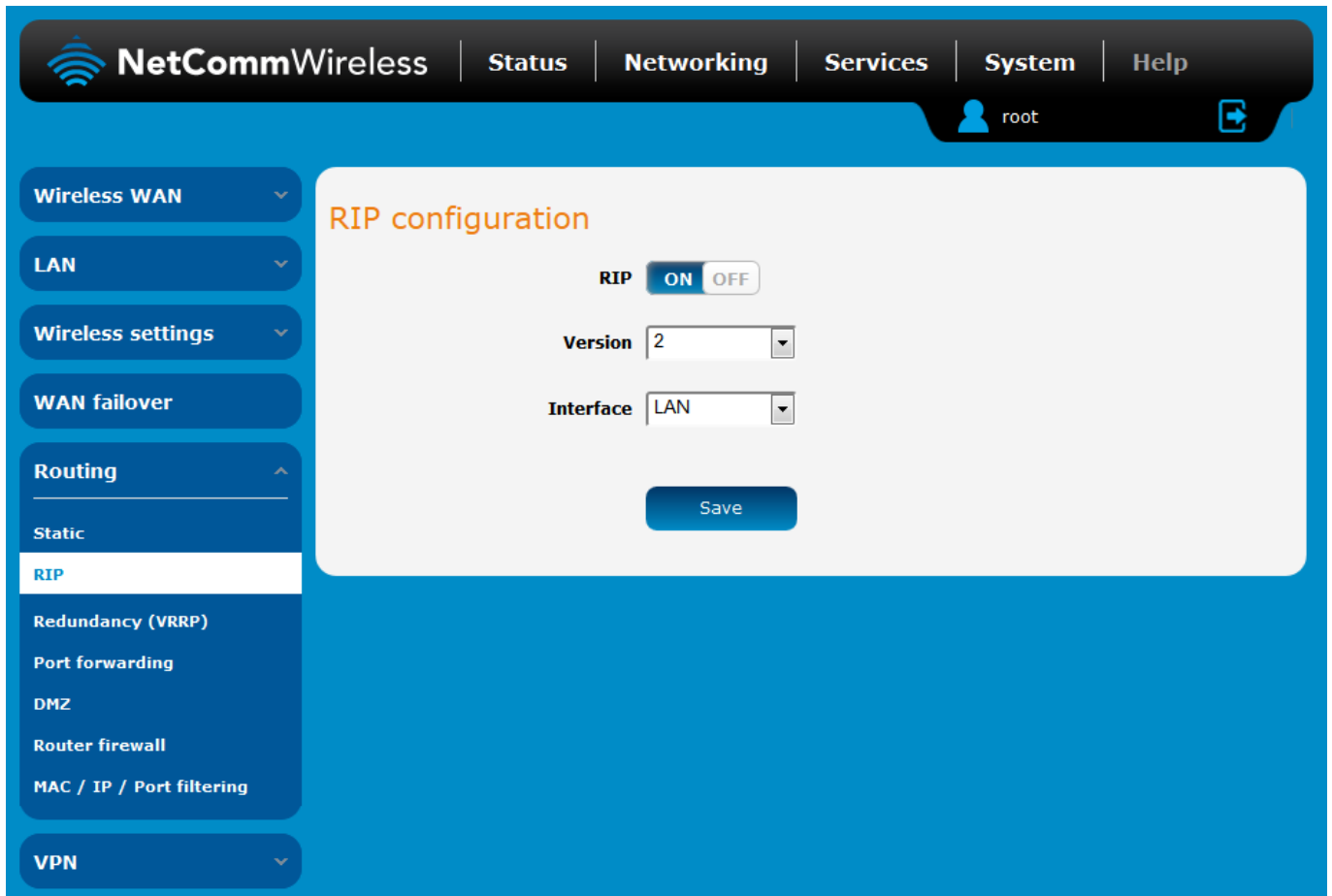


Figure 57 - RIP configuration

To enable Routing Information Protocol (RIP)

1. Click the **RIP** toggle key to switch it to the **ON** position.
2. Using the **Version** drop down list, select the version of RIP that you would like to use.
3. Select the interface for which you want RIP to apply. You can choose the **LAN** interface, the **WWAN** interface or **BOTH**.
4. Click the **Save** button to confirm your settings.

Redundancy (VRRP) configuration

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 a 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.

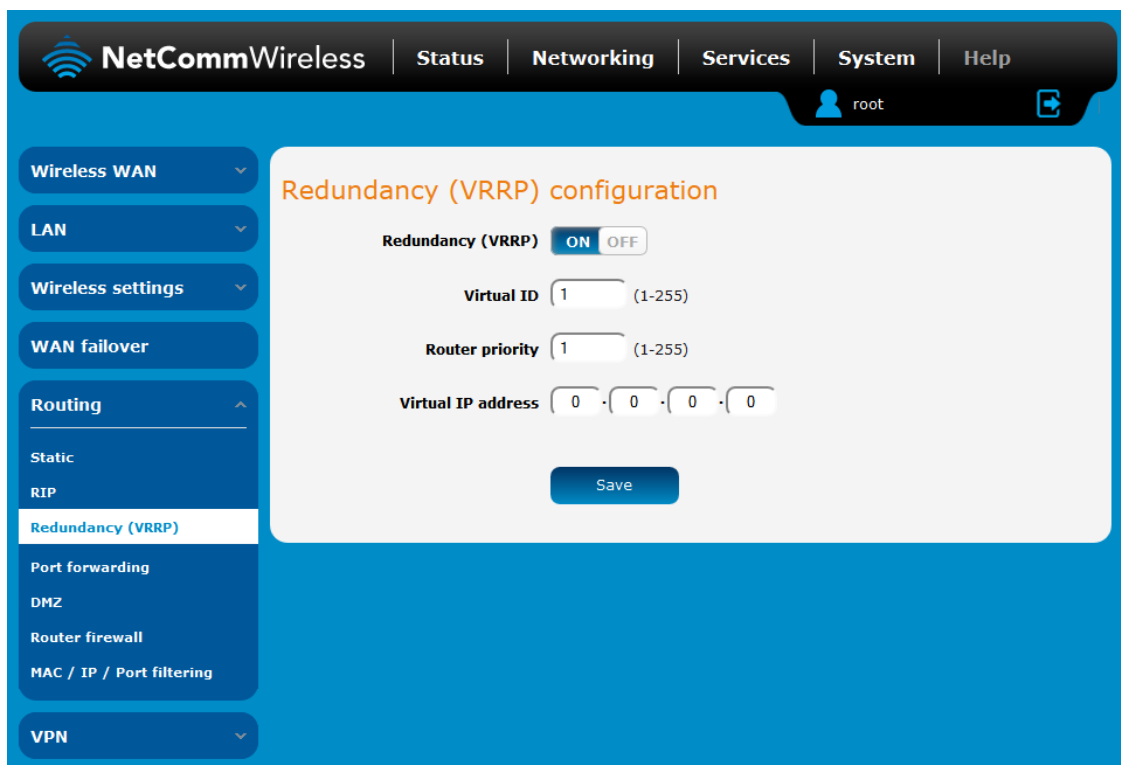


Figure 58 - VRRP configuration

To configure VRRP, configure multiple devices as follows and connect them all via an Ethernet network switch to downstream devices.

1. Click the **Redundancy (VRRP)** toggle key to activate VRRP.
2. In the **Virtual ID** field, enter an ID between 1 and 255. This is the VRRP ID which is different for each virtual router on the network.
3. In the **Router priority** field, enter a value for the priority – a higher value is a higher priority.
4. The **Virtual IP address** field is used to specify the VRRP IP address – this is the virtual IP address that both virtual routers share.
5. Click the **Save** button to save the new settings.



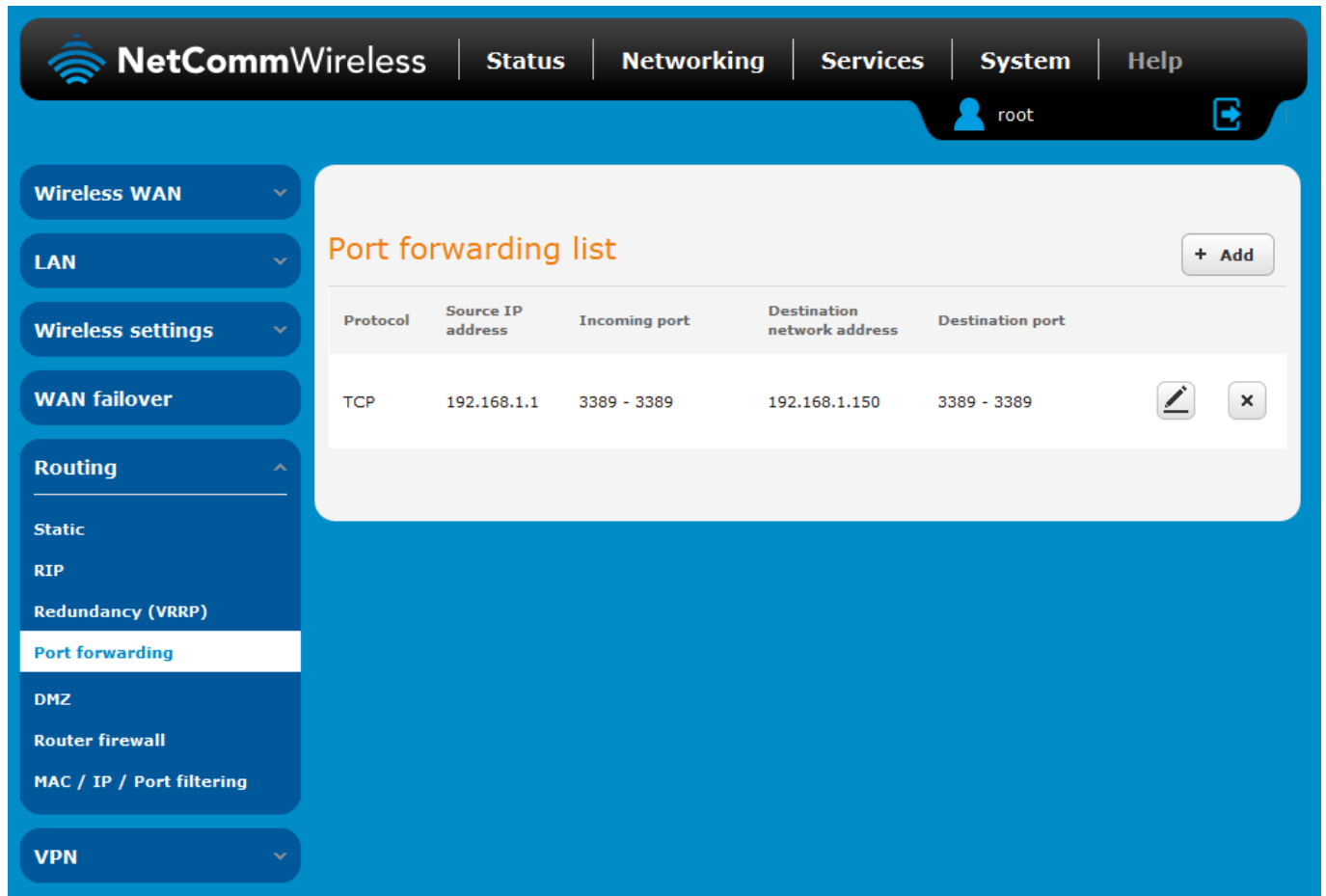
Note: Configuring VRRP changes the MAC address of the Ethernet port and therefore if you want to resume with the web configuration you must use the new IP address (VRRP IP) or on a command prompt type: `arp -d <ip address>` (i.e. `arp -d 192.168.1.1`) to clear the arp cache.(old MAC address).



Note: For more detail on configuring VRRP, please visit the product page on the NetComm Wireless website at <http://support.netcommwireless.com/product/m2m-wireless-series/ntc-40w> and click on FAQs/Self Help.

Port forwarding

The Port forwarding list is used to configure the Network Address Translation (NAT) rules currently in effect on the router.





Protocol	Source IP address	Incoming port	Destination network address	Destination port	
TCP	192.168.1.1	3389 - 3389	192.168.1.150	3389 - 3389	 

Figure 59 – Port forwarding list

The purpose of the port forwarding feature is to allow mapping of inbound requests to a specific port on the WAN IP address to a device connected on the Ethernet interface.

Adding a port forwarding rule

To create a new port forwarding rule:

1. Click the **+Add** button. The port forwarding settings screen is displayed.
2. Use the **Protocol** drop down list to select the type of protocol you want to use for the rule. The protocols selections available are **TCP**, **UDP** and **All**.
3. In the **Source IP address** field, enter a “friendly” address that is allowed to access the router or a wildcard IP address (0.0.0.0) that allows all IP addresses to access the router.
4. The **Original destination port range (From)** and **(To)** fields are used to specify the port(s) on the source side that are to be forwarded. This allows you to send a range of consecutive port numbers by entering the first in the range in the **(From)** field and the last in the range in the **(To)** field. To forward a single port, enter the port in the **(From)** field and repeat it in the **(To)** field.
5. In the **Destination IP address** field, enter the IP address of the client to which the traffic should be forwarded.
6. The **Destination port range (From)** and **(To)** fields are used to specify the port(s) on the destination side that are to be forwarded. If the Source port range specifies a single port then the destination port may be configured to any port. If the Source port range specifies a range of port numbers then the Destination port range must be the same as the Source port range.
7. Click the **Save** button to confirm your settings.

Port forwarding settings

Protocol

Source IP address · · ·

Original destination port range (From) (1-65535) (To) (1-65535)

Destination IP address · · ·

Destination port range (From) (1-65535) (To) (1-65535)

Figure 60 - Port forwarding settings

To delete a port forwarding rule, click the button on the Port forwarding list for the corresponding rule that you would like to delete.

DMZ

The Demilitarized Zone (DMZ) allows you to configure all incoming traffic on all protocols to be forwarded to a selected device behind the router. This feature can be used to avoid complex port forwarding rules, but it exposes the device to untrusted networks as there is no filtering of what traffic is allowed and what is denied.

The DMZ configuration page is used to specify the IP Address of the device to use as the DMZ host.

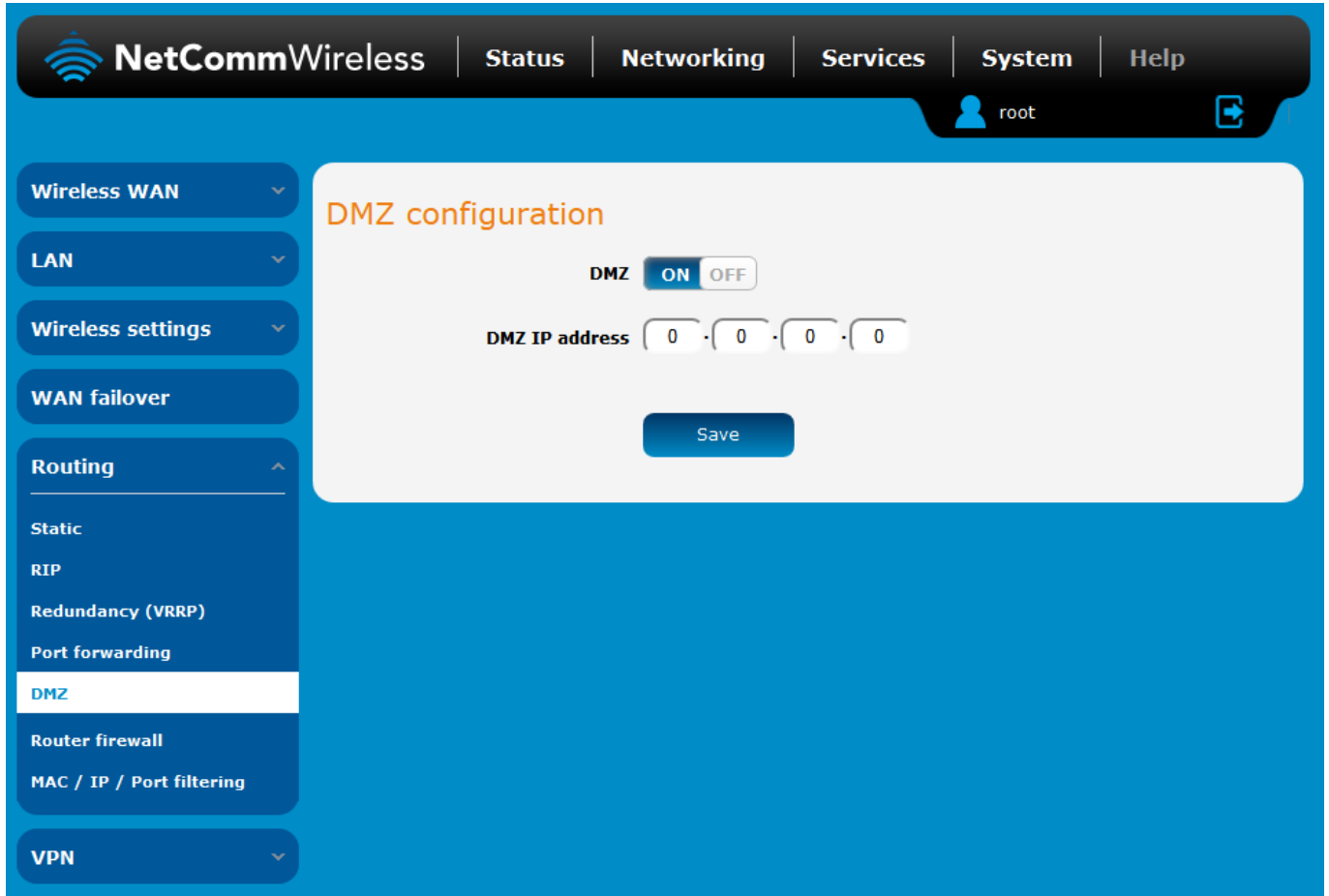


Figure 61 - DMZ configuration

1. Click the DMZ toggle key to turn the DMZ function **ON**.
2. Enter the IP Address of the device to be the DMZ host into the **DMZ IP Address** field.
3. Click the **Save** button to save your settings.

Router firewall

The Router firewall page is used to enable or disable the in-built firewall on the router. When enabled, the firewall performs stateful packet inspection on inbound traffic from the wireless WAN and blocks all unknown services, that is, all services not listed on the Services configuration page of the router.

With respect to the other Routing options on the Networking page, the firewall takes a low priority. The priority of the firewall can be described as:

DMZ > MAC/IP/Port filtering rules > MAC/IP/Port filtering default rule > Router firewall rules

In other words, the firewall is of the lowest priority when compared to other manual routing configurations. Therefore, a MAC/IP/Port filtering rule takes priority in the event that there is a conflict of rules. When DMZ is enabled, MAC/IP/Port filtering rules and the router firewall are ignored but the router will still honour the configuration of the Remote router access control settings listed under Administration Settings.

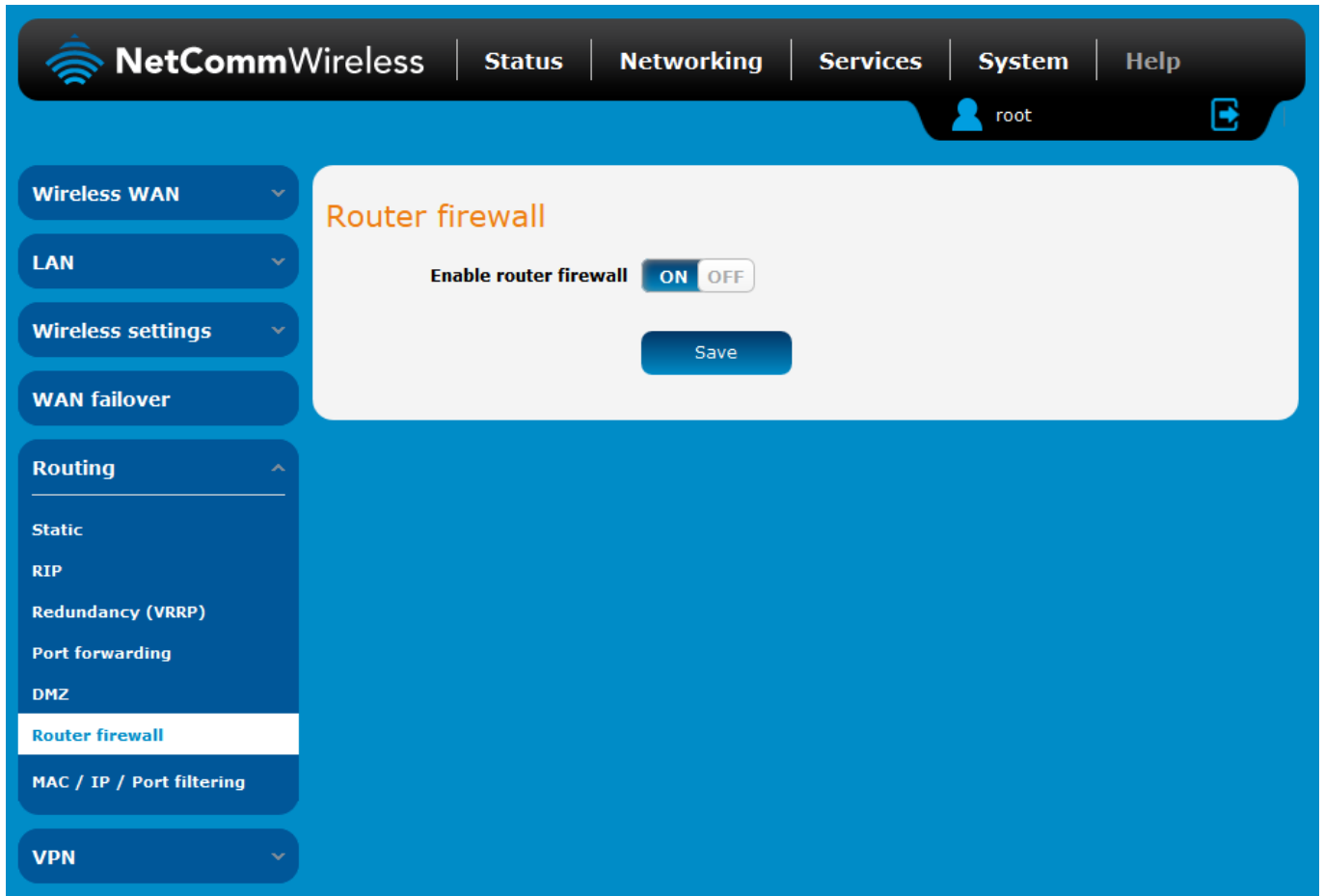


Figure 62 - Router firewall toggle key

MAC / IP / Port filtering

The MAC/IP/Port filter feature allows you apply a policy to the traffic that passes through the router, both inbound and outbound, so that network access can be controlled. When the filter is enabled with a default rule of “Accepted”, all connections will be allowed except those listed in the “Current MAC / IP / Port filtering rules in effect” list. Conversely, when the default rule is set to “Dropped”, all connections are denied except for those listed in the filtering rules list.

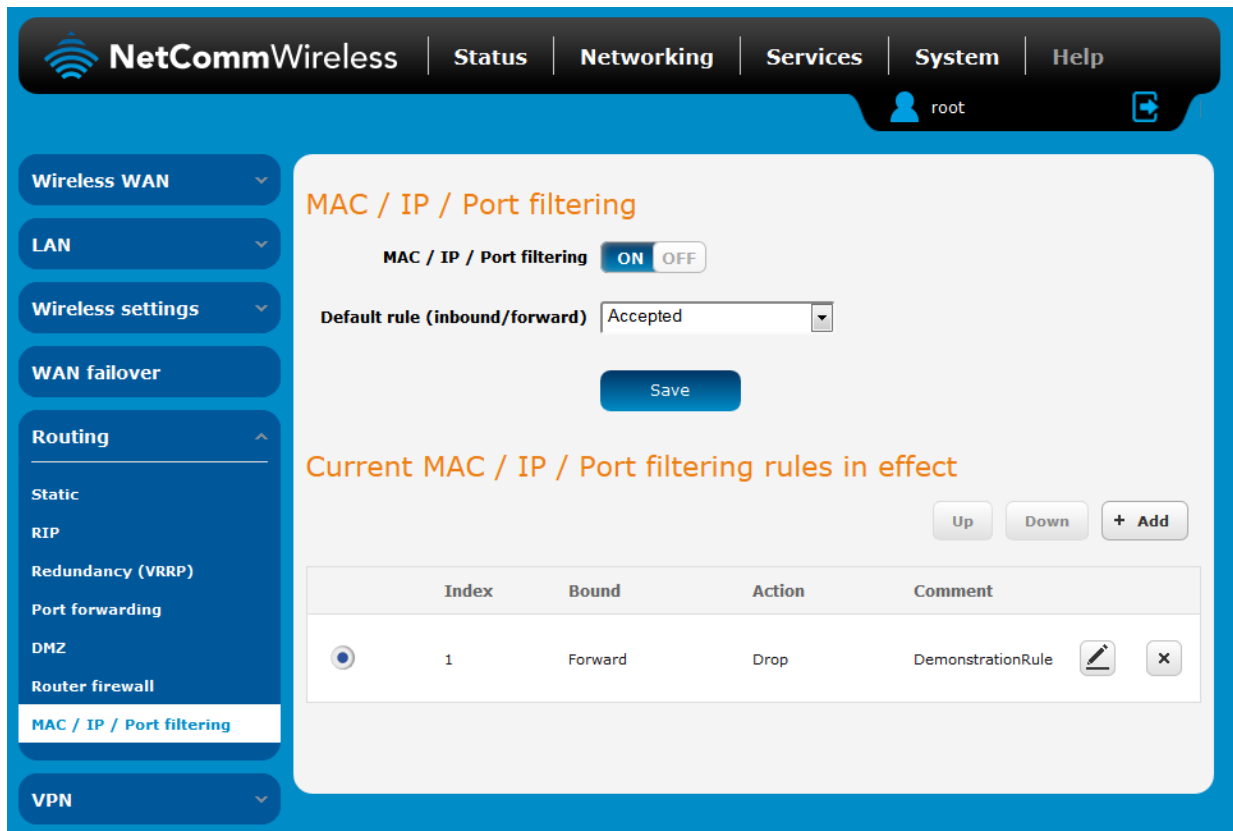


Figure 63 - MAC / IP / Port filtering



Note: When enabling MAC / IP / Port filtering and setting the default rule to “Dropped”, you should ensure that you have first added a filtering rule which allows at least one known MAC/IP to access the router, otherwise you will not be able to access the user interface of the router without resetting the router to factory default settings.

Creating a MAC / IP / Port filtering rule

To create a filtering rule:

1. Click the **MAC / IP / Port filtering** toggle key to switch it to the **ON** position.
2. Using the **Default rule (inbound/forward)** drop down list, select the default action for the router to take when traffic reaches it. By default, this is configured to **Accepted**. If you change this to **Dropped**, you should first configure a filter rule that allows at least one device access to the router, otherwise you will effectively be locked out of the router.
3. Click the **Save** button to confirm the default rule.
4. In the Current MAC / IP / Port filtering rules in system section, click the **+Add** button.



Figure 64 - Current MAC / IP / Port filtering rules in effect

- Enter the details of the rule in the section that is displayed and click the **Save** button.

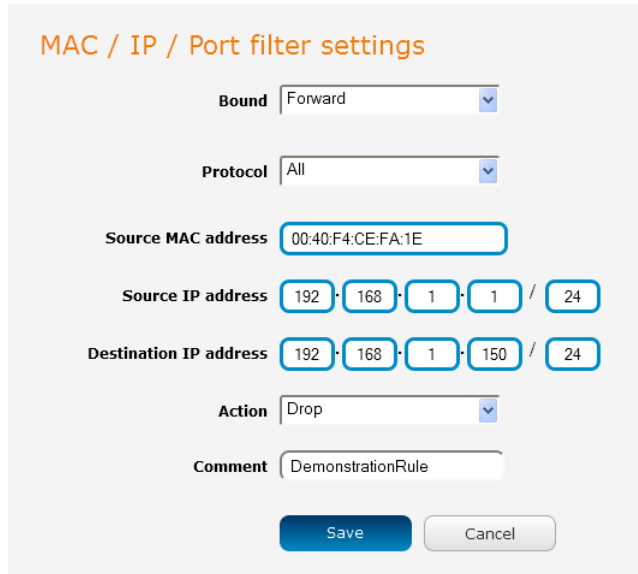




Figure 65 - MAC / IP / Port filtering settings

OPTION	DESCRIPTION
Bound	Use the drop down list to select the direction of the traffic for which you want to apply to the rule. Inbound refers to all traffic that is entering the router including data entering from the WAN and the LAN. Outbound refers to all traffic exiting the router including traffic leaving in the direction of the WAN and traffic leaving in the direction of the LAN. Forward specifies traffic that enters on the LAN or WAN side and is forwarded to the opposite end.
Protocol	Use the drop down list to select the protocol for the rule. You can have the rule apply to All protocols, TCP , UDP , UDP/TCP or ICMP .
Source MAC Address	Enter the MAC address in six groups of two hexadecimal digits separated by colons (:). e.g. 00:40:F4:CE:FA:1E
Source IP Address	Enter the IPv4 address that the traffic originates from and the subnet mask using CIDR notation.
Destination IP Address	Enter the IPv4 address that the traffic is destined for and the subnet mask using CIDR notation.
Action	Select the action to take for traffic which meets the above criteria. You can choose to Accept or Drop packets. When the default rule is set to Accept , you cannot create a rule with an Accept action since the rule is redundant. Likewise, if the default rule is set to Dropped you cannot create a rule with a Drop action.
Comment	[Optional] Use this field to enter a comment as a meaningful description of the rule.

Table 18 - Current MAC / IP / Port filtering rules in effect

- The new rule is displayed in the filtering rules list. You can edit the rule by clicking the  **Edit** button or delete the rule by clicking the  button.

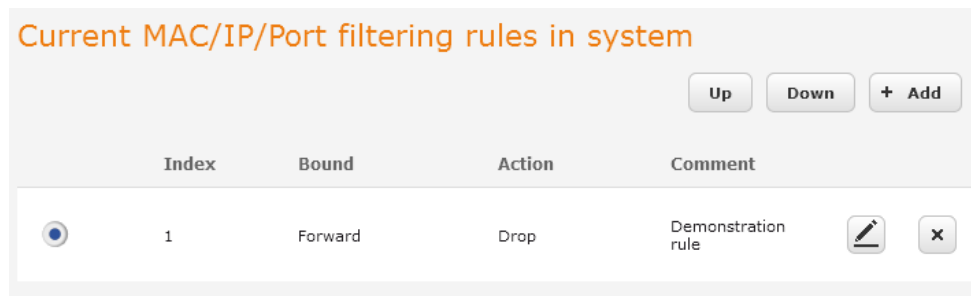


Figure 66 - Completed filtering rule

VPN

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

The advantages of a VPN connection include:

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

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



Note: The following descriptions are an overview of the various VPN options available. More detailed instructions are available in separate whitepapers on the NetComm Wireless website.

IPSec

IPSec operates on Layer 3 of the OSI model and as such can protect higher layered protocols. IPSec is used for both site to site VPN and Remote Access VPN. The NTC-40WW router supports IPSec end points and can be configured with Site to Site VPN tunnels with third party VPN routers.

Configuring an IPSec VPN

From the menu at the top of the screen, click **Networking** and under the VPN section, click **IPSec**. A list of configured IPSec VPN connections is displayed.

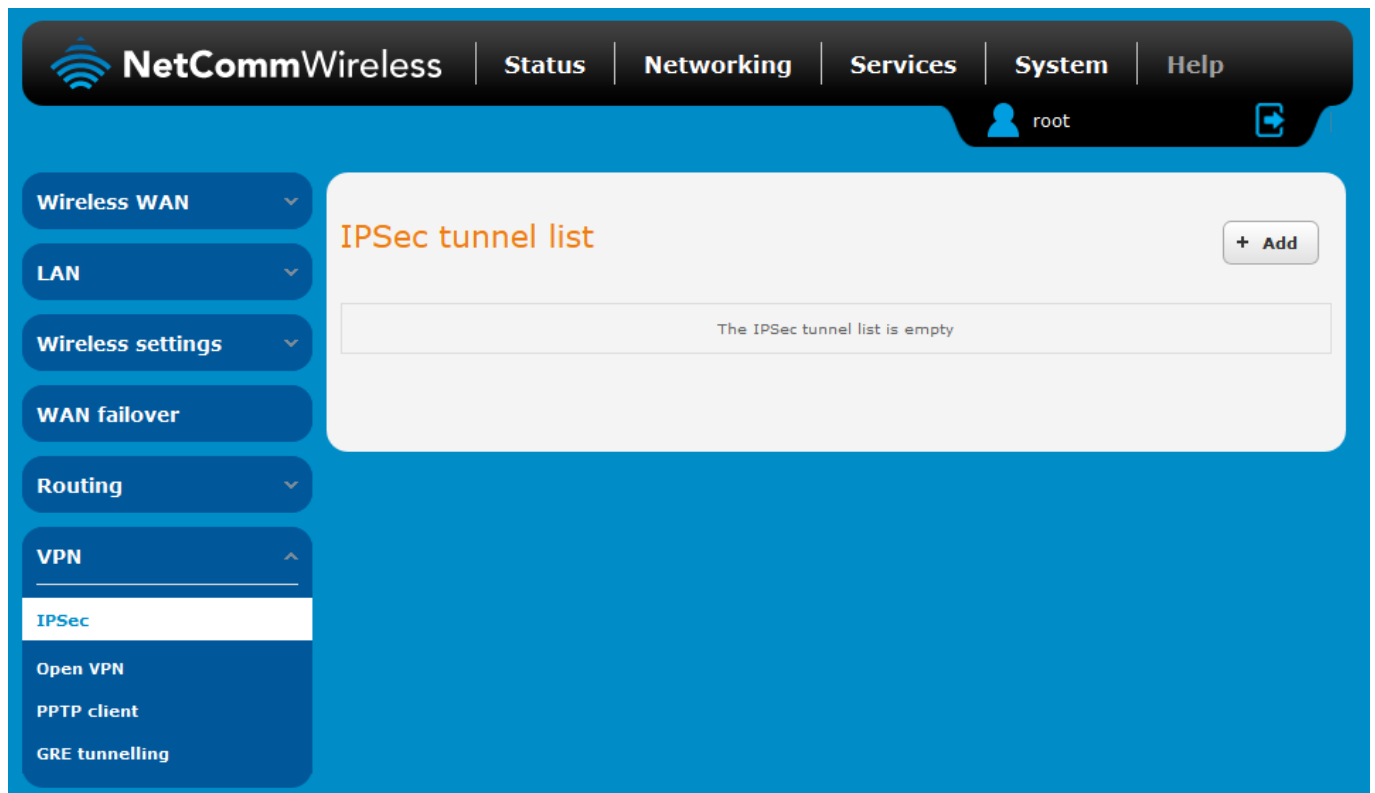


Figure 67 - IPSec VPN List

Click the **+Add** button to begin configuring an IPSec VPN connection.

IPSec profile edit

IPSec profile ON OFF

Profile name

Phase 1 parameters

Remote IPSec address

Key mode

Pre-shared key

Remote ID (xy.sample.com or blank)

Local ID (xy.sample.com or blank)

IKE mode

PFS

IKE encryption

IKE hash

DH group

IKE re-key time (0-78400, 0=Unlimited) secs

DPD action

DPD keep alive time secs

DPD timeout secs

SA life time (0-78400, 0=Unlimited) secs

Phase 2 parameters

Remote LAN address · · ·

Remote LAN subnet mask · · ·

Local LAN address · · ·

Local LAN subnet mask · · ·

Encapsulation type

IPSec encryption

IPSec hash

Figure 68 – IPSec profile edit

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

ITEM	DEFINITION
IPSec profile	Enables or disables the VPN profile.
Profile name	A name used to identify the VPN connection profile.
Remote IPSec address	The IP address or domain name of the IPSec server.
Key mode	Select the type of key mode in use for the VPN connection. You can select from: <ul style="list-style-type: none"> • Pre Shared Key • RSA keys • Certificates
Pre-shared key	The pre-shared key is the key that peers used to authenticate each other for Internet Key Exchange.
Update Time	Displays the last time the key was updated.
Local RSA Key Upload	Select the RSA key file for the local router here by clicking the Browse button.
Remote RSA Key Upload	Select the RSA key file for the remote router here by clicking the Browse button.
Private key Passphrase	The Private key passphrase of the router is the passphrase used when generating the router's private key using OpenSSL CA.
Key / Certificate	Select the type of key or certificate to use for authentication. You can select Local private key, Local public certificate, Remote public certificate, CA certificate, CRL certificate.
IPSec Certificate Upload	Select the IPSec certificate to upload by clicking the Browse button.
Remote ID	Specifies the domain name of the remote network.
Local ID	Specifies the domain name of the local network.
IKE mode	Select the IKE mode to use with the VPN connection. You can choose Main, Aggressive or Any .
PFS	Choose whether Perfect Forward Secrecy is ON or OFF for the VPN connection.
IKE encryption	Select the cipher type to use for the Internet Key Exchange.
IKE hash	Select the IKE Hash type to use for the VPN connection. The hash is used for authentication of packets for the key exchange.
DH group	Select the desired Diffie-Hellman group to use. Higher groups are more secure but also require longer to generate a key.
IKE re-key time	Enter the time in seconds between changes of the encryption key. To disable changing the key, set this to 0.
DPD action	Select the desired Dead Peer Detection action. This is the action to take when a dead Internet Key Exchange Peer is detected.
DPD keep alive time	Enter the time in seconds for the interval between Dead Peer Detection keep alive messages.
DPD timeout	Enter the time in seconds of no response from a peer before Dead Peer Detection times out.
SA life time	Enter the time in seconds for the security association lifetime.
Remote LAN address	Enter the IP address of the remote network for use on the VPN connection.
Remote LAN subnet mask	Enter the subnet mask in use on the remote network.
Local LAN address	Enter the IP address of the local network for use on the VPN connection.
Local LAN subnet mask	Enter the subnet mask in use on the local network.
Encapsulation type	Select the encapsulation protocol to use with the VPN connection. You can choose ESP, AH or Any .
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. The hash is used for authentication of packets for the VPN connection.

Table 19 - IPSec Configuration Items



Note: For more detail on configuring IPSec, please visit the product page on the NetComm Wireless website at <http://support.netcommwireless.com/product/m2m-wireless-series/ntc-40w> and click on FAQs/Self Help.

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.



Note: For more detail on configuring OpenVPN, please visit the product page on the NetComm Wireless website at <http://support.netcommwireless.com/product/m2m-wireless-series/ntc-40wv> and click on FAQs/Self Help.

Configuring an Open VPN server

From the menu at the top of the screen, click **Networking** and from the VPN section on the left, click **OpenVPN**. A list of configured OpenVPN VPN connections is displayed.

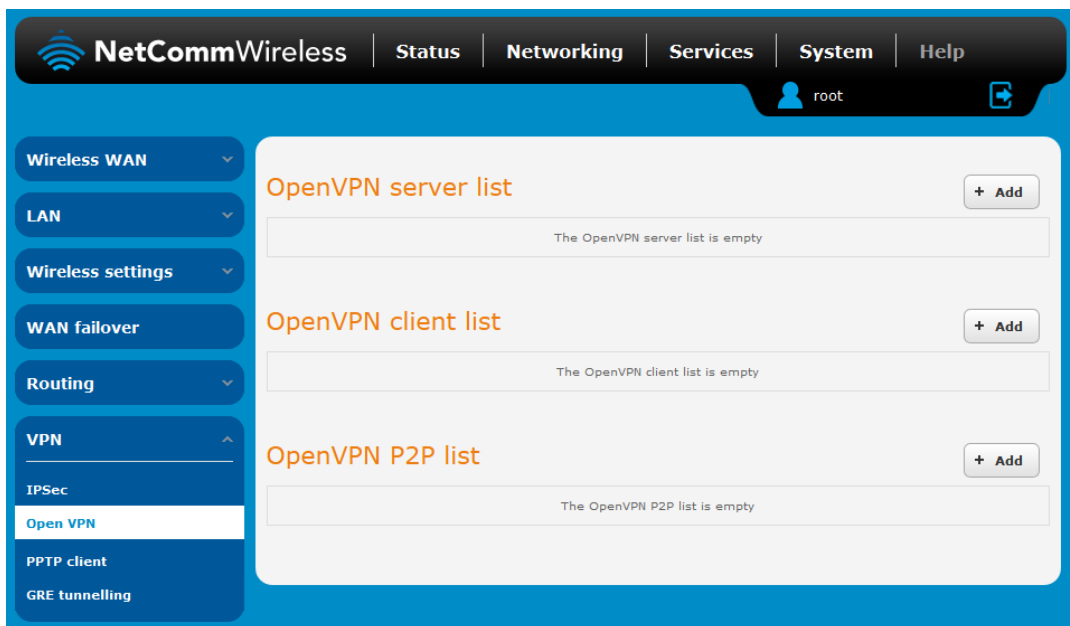
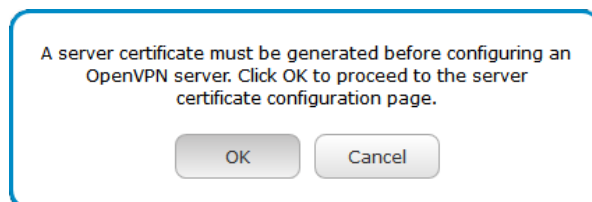


Figure 69 - OpenVPN VPN List

Click the **+Add** button for the type of OpenVPN server/client you would like to configure.

OpenVPN Server

When you select the **+Add** button to add an OpenVPN server, the router checks whether there are existing server certificates. If no server certificate is found, you are informed that you must generate a certificate before configuring the OpenVPN server.



Click on the **OK** button to be taken to the **Server certificate** page. For more information on generating server certificates, refer to the Server certificate section of this guide. When you have created the certificate, return to the OpenVPN server configuration page and continue with the steps below.

To configure an OpenVPN Server:

1. Click the **OpenVPN profile** toggle key to switch it to the **ON** position.
2. Type a name for the OpenVPN server profile you are creating.

3. In the **Type** drop down list, select the OpenVPN connection type (TUN/TAP). Default is **TUN**.
4. Use the **Server** port field to select a port number and then use the drop down list to select a packet type to use for your OpenVPN Server. The default OpenVPN port is 1194 and default packet type is UDP.
5. In the **VPN network address** and **VPN network subnet mask** fields, enter the IP address and network subnet mask to assign to your VPN. This is ideally an internal IP address which differs from your existing address scheme.
6. The **Server certificates** section displays the details of the certificate. If you wish to change the certificate, click the **Change** button.
7. HMAC or Hash-based Message Authentication Code is a means of calculating a message authentication code through the use of a cryptographic hash function and a cryptographic key. If you wish to use the HMAC signature as an additional key and level of security, under the SSL/TLS handshake section, click the **Use HMAC Signature** toggle key so that it is in the **ON** position, then click the **Generate** button so that the router can randomly generate the key. The Server key timestamp field is updated with the time that the key was generated. Click the **Download** button to download the key file so that it can be uploaded on the client.
8. Select an Authentication type. Authentication may be done using a **Certificate** or **Username / Password**.

Certificate Authentication

In the Certificate Management section, enter the required details to create a client certificate. All fields are required. When you have finished entering the details, click the **Generate** button.

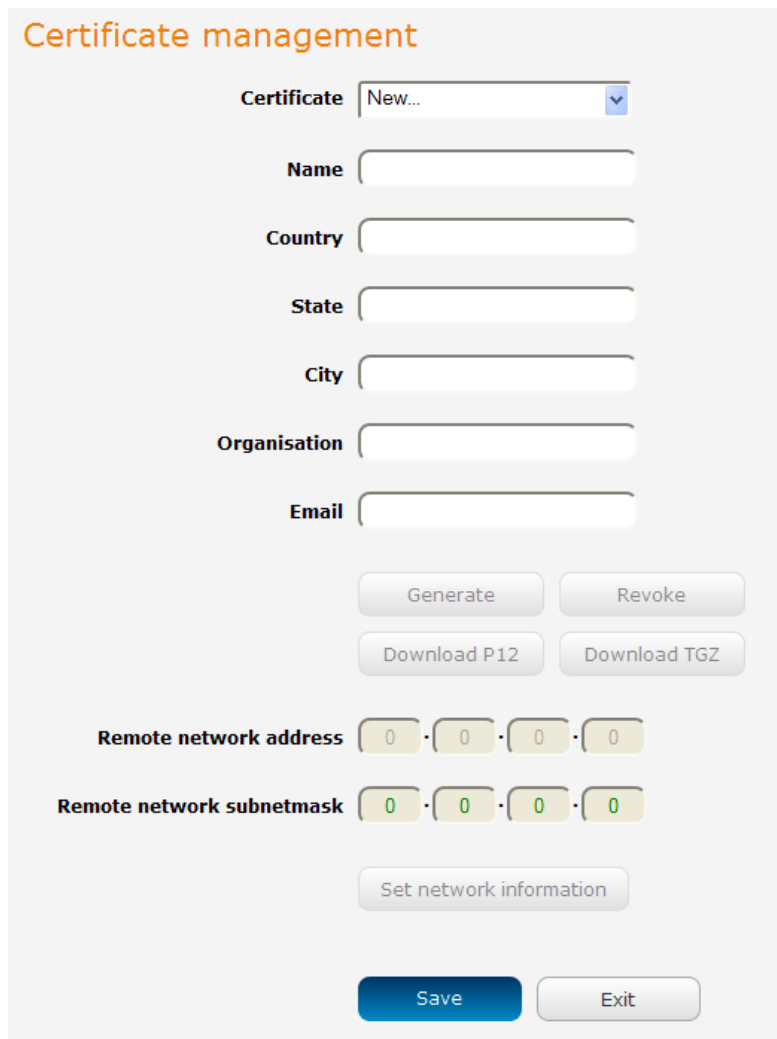


Figure 70 - OpenVPN server configuration – Certificate management

When it is done, you can click the **Download P12** button or the **Download TGZ** button to save the certificate file depending on which format you would like. If for some reason the integrity of your network has been compromised, you can return to this screen and use the Certificate drop down list to select the certificate and then press the **Revoke** button to disable it.

Optional: To inform the OpenVPN server of the network address scheme of the currently selected certificate, enter the network address and network subnet mask in the respective fields and click the **Set network information** button. If you do not enter the remote subnet here, any packet requests from the server to the client will not be received by the client network because it is not aware of the remote client's subnet.

OpenVPN server edit

OpenVPN profile ON

Profile name

Type TUN

Server port 1194 UDP

VPN network address . . .

VPN network subnet mask 255 . 255 . .

Server certificates

Not before Mar 13 04:21:03 2015 GMT

Not after Mar 10 04:21:03 2025 GMT

Country AU

State NSW

City Sydney

Organisation NetComm Wireless

Email techsupport@netcommwireless.com

SSL/TLS handshake

Use HMAC Signature ON

Server key timestamp 2015-03-13 16:49:48

Authentication type

Certificate Username / Password

Certificate management

Certificate New...

Name

Country

State

City

Organisation

Email

Remote network address 0 . 0 . 0 . 0

Remote network subnetmask 0 . 0 . 0 . 0

Figure 71 – OpenVPN server profile settings

Username / Password Authentication

In the Username/Password section, enter the username and password you would like to use for authentication on the OpenVPN Server. Click the **Download CA certificate** or **Download CA TGZ depending on file format** button to save the **ca.crt** file. This file will need to be provided to the client.



Note: If you wish to have more than one client connect to this OpenVPN server, you must use Certificate authentication mode as Username/Password only allows for a single client connection.

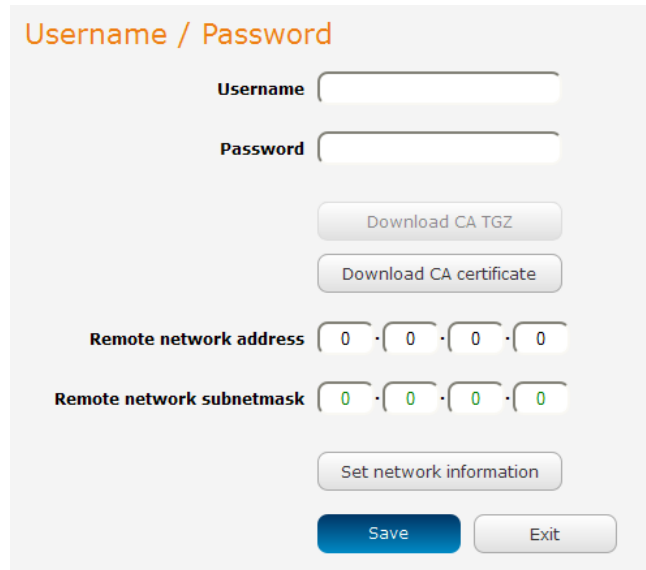


Figure 72 - OpenVPN Server – Username / Password section

Optional: To inform the OpenVPN server of the network address scheme of the currently selected certificate, enter the network address and network subnet mask in the respective fields and click the **Set Network Information** button. If you do not enter the remote subnet here, any packet requests from the server to the client will not be received by the client network because it is not aware of the remote client's subnet.

When you have finished entering all the required information, click **Save** to finish configuring the OpenVPN server.

Configuring an OpenVPN Client

1. Click the **OpenVPN profile** toggle key to switch it to the **ON** position.
2. In the **Profile name** field, type a name for the OpenVPN client profile you are creating.
3. In the **Server IP** address field, type the WAN IP address /host domain name of the OpenVPN server.
4. Select OpenVPN connection type (TUN/TAP). Default is **TUN**.
5. Use the **Server** port field to select a port number and then use the drop down list to select a packet type to use for the OpenVPN server. The default OpenVPN port is 1194 and default packet type is UDP.
6. If the **Default gateway** option is applied on the OpenVPN client page, the OpenVPN server will enable connections to be made to other client networks connected to it. If it is not selected, the OpenVPN connection allows for secure communication links between this router and the remote OpenVPN server only.
7. Use the **Authentication type** options to select the Authentication type that you would like to use for the OpenVPN client.

Certificate Authentication

In the Certificate upload section at the bottom of the screen, click the **Browse** button and locate the certificate file you downloaded when you configured the OpenVPN server. When it has been selected, click the **Upload** button to send it to the router.

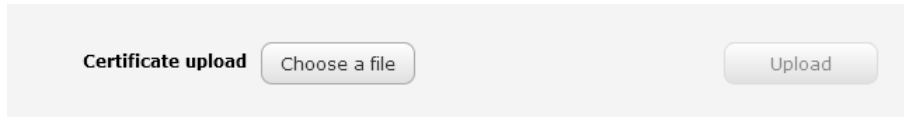


Figure 73 - OpenVPN client - Certificate upload

Username / Password Authentication

Enter the username and password to authenticate with the OpenVPN server.

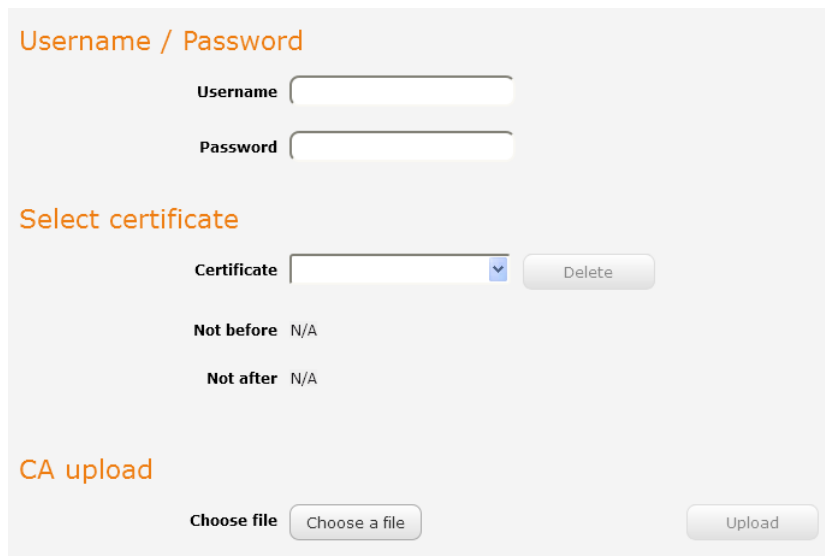


Figure 74 - OpenVPN Client - Username/Password section

Use the **Browse** button to locate the CA certificate file you saved from the OpenVPN Server and then press the **Upload** button to send it to the router.

Certificate and Username / Password Authentication

This is a combination of both the Certificate and Username / Password authentication methods providing additional levels of security since the client must know the username / password combination and be in possession of the certificate.

- If you have an additional SSL/TLS key created on the server, click on the **Use HMAC Signature** toggle key so that it is in the **ON** position. Select the **Choose a file** button then locate the key file on your computer. Click the **Upload** button to upload it to the router.

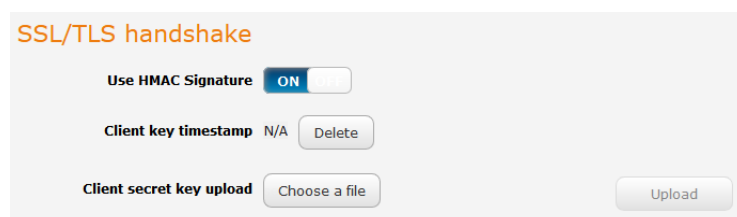


Figure 75 - OpenVPN Client - SSL/TLS key upload

- Click the **Save** button to complete the OpenVPN Client configuration.

Configuring an OpenVPN P2P Connection

To configure an OpenVPN peer-to-peer connection:

1. Set the **OpenVPN** profile toggle key to switch it to the **ON** position.
2. In the **Profile name** field, type a name for the OpenVPN P2P profile you are creating.
3. On the router designated as the server, leave the **Server IP address** field empty. On the router designated as the client, enter the **WAN IP address/host domain name** of the server.

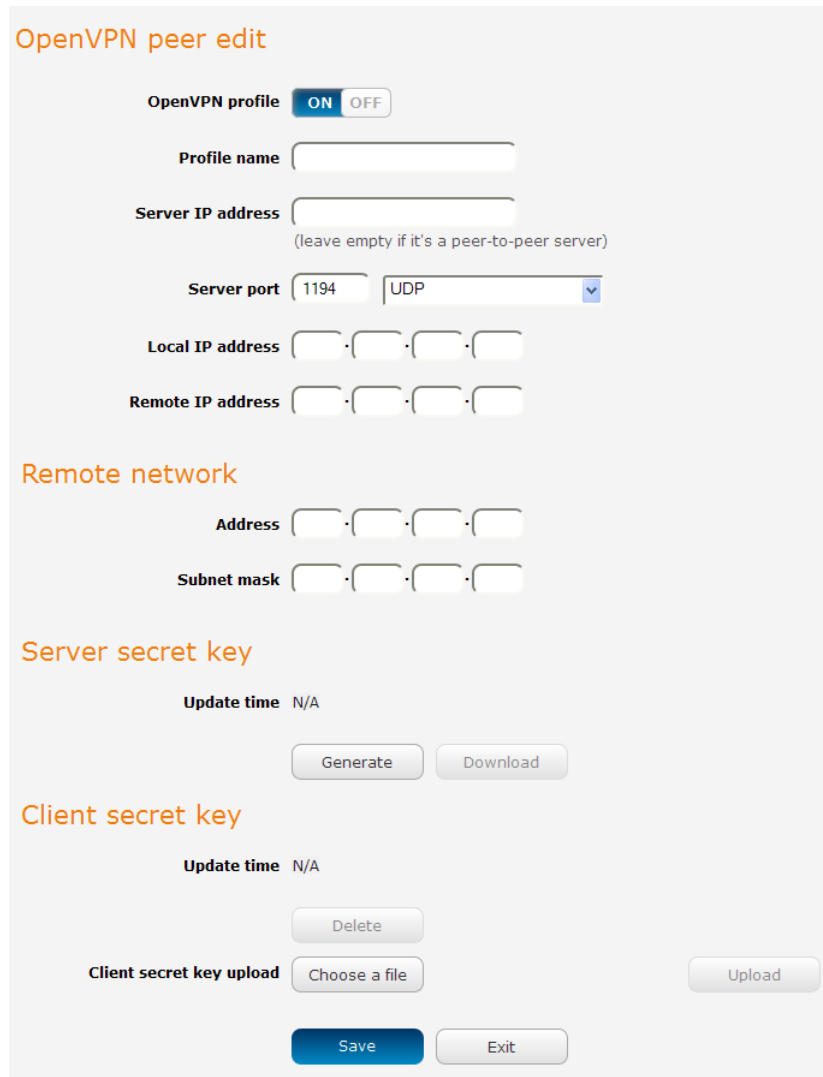


Figure 76 - OpenVPN P2P mode settings

4. Use the **Server** port field to select a port number and then use the drop down list to select a packet type to use for the OpenVPN server. The default OpenVPN port is 1194 and default packet type is UDP.
5. In the **Local IP Address** and **Remote IP Address** fields, enter the respective local and remote IP addresses to use for the OpenVPN tunnel. The slave should have the reverse settings of the master.
6. Under the Remote network section, enter the network **Address** and network **Subnet mask**. The Network Address and Network Mask fields inform the Master node of the LAN address scheme of the slave.
7. Press the **Generate** button to create a secret key to be shared with the slave. When the timestamp appears, you can click the **Download** button to save the file to exchange with the other router.
8. When you have saved the secret key file on each router, use the **Browse** button to locate the secret key file for the master and then press the **Upload** button to send it to the slave. Perform the same for the other router, uploading the slave's secret key file to master.
9. When they are uploaded click the **Save** button to complete the peer-to-peer OpenVPN configuration.

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.

Configuring the PPTP Client

To configure the PPTP client:

1. From the menu bar at the top of the screen, click **Networking** and then from the **VPN** section on the left side of the screen, click **PPTP client**. The PPTP client list is displayed.

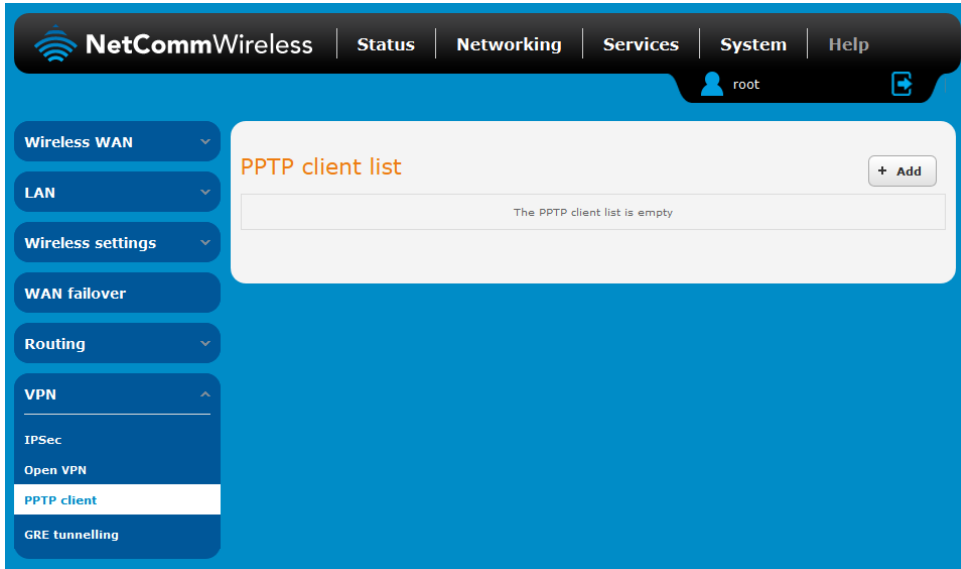


Figure 77 - PPTP client list

2. Click the **+Add** button to begin configuring a new PPTP client profile. The PPTP client edit screen is displayed.

VPN PPTP client edit

Enable PPTP client ON OFF

Profile name

Username

Password

PPTP server

Authentication type ▼

Metric (0-65535)

Use peer DNS ON OFF

NAT masquerading ON OFF

Set PPTP server as default gateway ON OFF

MPPE ON OFF






Extra PPP option

Verbose logging ON OFF

Reconnect delay (30-65535) seconds

Reconnect retries (0-65535, 0=Unlimited)

Figure 78 - VPN PPTP client edit

3. Click the **Enable PPTP client** toggle key to switch it to the **ON** position.
4. In the **Profile name list**, enter a profile name for the tunnel. This may be anything you like and is used to identify the tunnel on the router.
5. Use the **Username** and **Password** fields to enter the username and password for the PPTP account.
6. In the **PPTP server address** field, enter the IP address /host domain name of the PPTP server.
7. From the **Authentication type** drop down list, select the Authentication type used on the server. If you do not know the authentication method used, select **any** and the router will attempt to determine the correct authentication type for you. There are 5 authentication types you can choose from:
 -  CHAP – uses a three way handshake to authenticate the identity of a client.
 -  MS-CHAP v1 – This is the Microsoft implementation of the Challenge Handshake Authentication Protocol for which support was dropped in Windows® Vista.
 -  MS-CHAP v2 - This is the Microsoft implementation of the Challenge Handshake Authentication Protocol which was introduced in Windows® NT 4.0 and is still supported today.
 -  PAP – The Password Authentication Protocol uses a password as a means of authentication and as such, is commonly supported. PAP is not recommended because it transmits passwords unencrypted and is not secure.
 -  EAP – Extensible Authentication Protocol. An Authentication protocol commonly used in wireless networks.
8. The **metric** value helps the router to prioritise routes and must be a number between 0 and 65535. The default value is 30 and should not be modified unless you are aware of the effect your changes will have.
9. The **Use peer DNS** option allows you to select whether the remote clients will use the Domain Name Server of the PPTP server. Click the toggle key to set this to ON or OFF as required.
10. **NAT masquerading** allows the router to modify the packets sent and received to inform remote computers on the internet that packets originating from a machine behind the router actually originated from the WAN IP address of the router's internal NAT IP address. Click the toggle key to switch this to the ON position if you want to use this feature.
11. Set **default route to PPTP** sets all outbound data packets to go out through the PPTP tunnel. Click the toggle key to switch this to the ON position if you want to use this feature.
12. The **Verbose logging** option sets the router to output detailed logs regarding the PPTP connection in the **System Log** section of the router interface.
13. The **Reconnect delay** is the time in seconds that the router will wait before attempting to connect to the PPTP server in the event that the connection is broken. The minimum time to wait is 30 seconds so as to not flood the PPTP server with connection requests, while the maximum time to wait is 65535 seconds.
14. The **Reconnect retries** is the number of connection attempts that the router will make in the event that the PPTP connection goes down. If set to 0, the router will retry the connection indefinitely, otherwise the maximum number of times to retry cannot be greater than 65535.
15. Click the **Save** button to save the changes. The VPN will attempt to connect after your click Save. Click the **Status** button at the top left of the interface to return to the status window and monitor the VPN's connection state.



Note: For more detail on configuring PPTP Client, please visit the product page on the NetComm Wireless website at <http://support.netcommwireless.com/product/m2m-wireless-series/ntc-40wv> and click on FAQs/Self Help.

GRE tunnelling

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

Configuring GRE tunnelling

To configure GRE tunnelling:

1. From the menu bar at the top of the screen, click **Networking** and then from the **VPN** section on the left side of the screen, click **GRE**. The GRE client list is displayed.

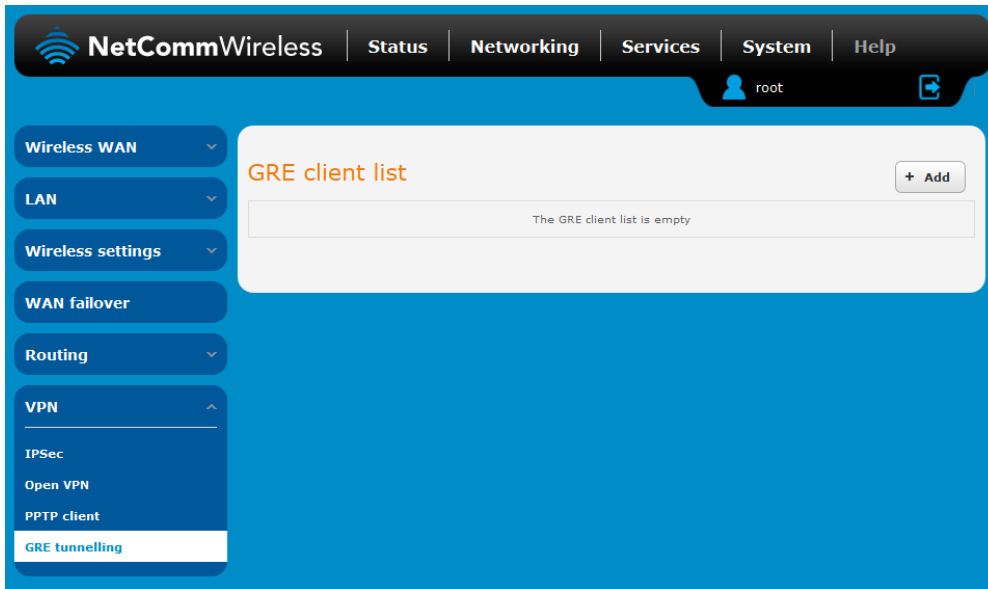


Figure 79 - GRE client list

2. Click the **+Add** button to begin configuring a new GRE tunnelling client profile. The GRE Client Edit screen is displayed.

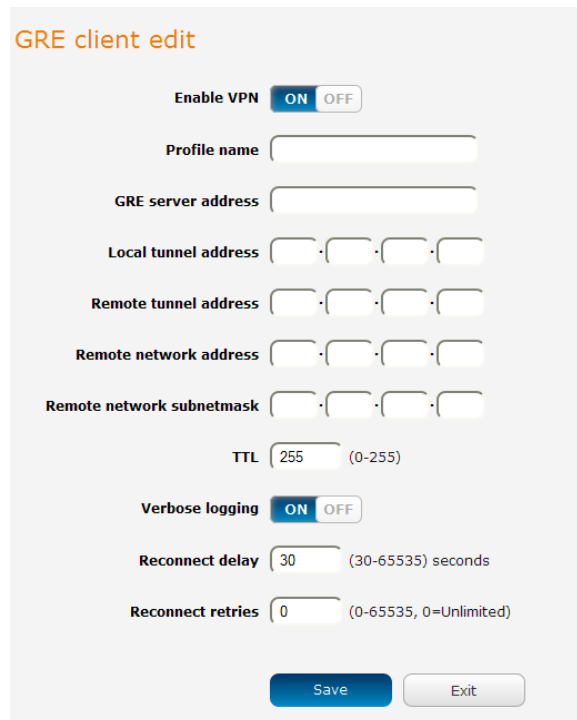


Figure 80 – GRE client edit

3. Click the **Enable GRE Tunnel** toggle key to switch it to the **ON** position.

4. In the **Profile name**, enter a profile name for the tunnel. This may be anything you like and is used to identify the tunnel on the router.
5. In the **GRE server address** field, enter the IP address or domain name of the GRE server.
6. In the **Local tunnel address** field, enter the IP address you want to assign the tunnel locally.
7. In the **Remote tunnel address** field, enter the IP address you want to assign to the remote tunnel.
8. In the **Remote network address** field, enter the IP address scheme of the remote network.
9. In the **Remote network subnetmask** field, enter the subnet mask of the remote network.
10. The **TTL** (Time To Live) field is 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.
11. The **Verbose logging** option sets the router to output detailed logs regarding the GRE tunnel in the **System Log** section of the router interface.
12. The **Reconnect delay** is the time in seconds that the router will wait before attempting to connect to the GRE server in the event that the connection is broken. The minimum time to wait is 30 seconds so as to not flood the GRE server with connection requests, while the maximum time to wait is 65335 seconds.
13. The **Reconnect retries** is the number of connection attempts that the router will make in the event that the GRE connection goes down. If set to 0, the router will retry the connection indefinitely, otherwise the maximum number of times to retry cannot be greater than 65335.
14. Click the **Save** button to save the changes. The VPN will attempt to connect after your click Save. Click the **Status** button at the top left of the interface to return to the status window and monitor the VPN's connection state.



Note: For more detail on configuring GRE, please visit the product page on the NetComm Wireless website at <http://support.netcommwireless.com/product/m2m-wireless-series/ntc-40wy> and click on FAQs/Self Help.

Services

Dynamic DNS

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

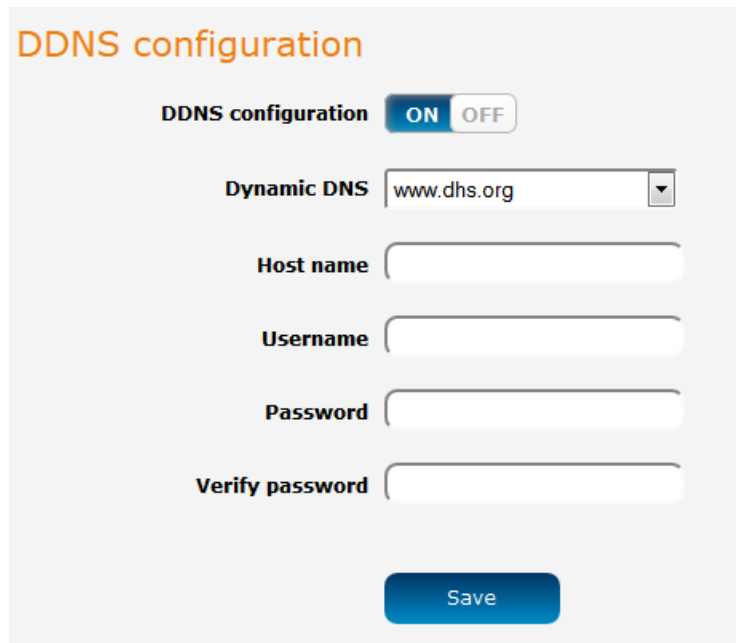











Figure 81 – Dynamic DNS settings

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

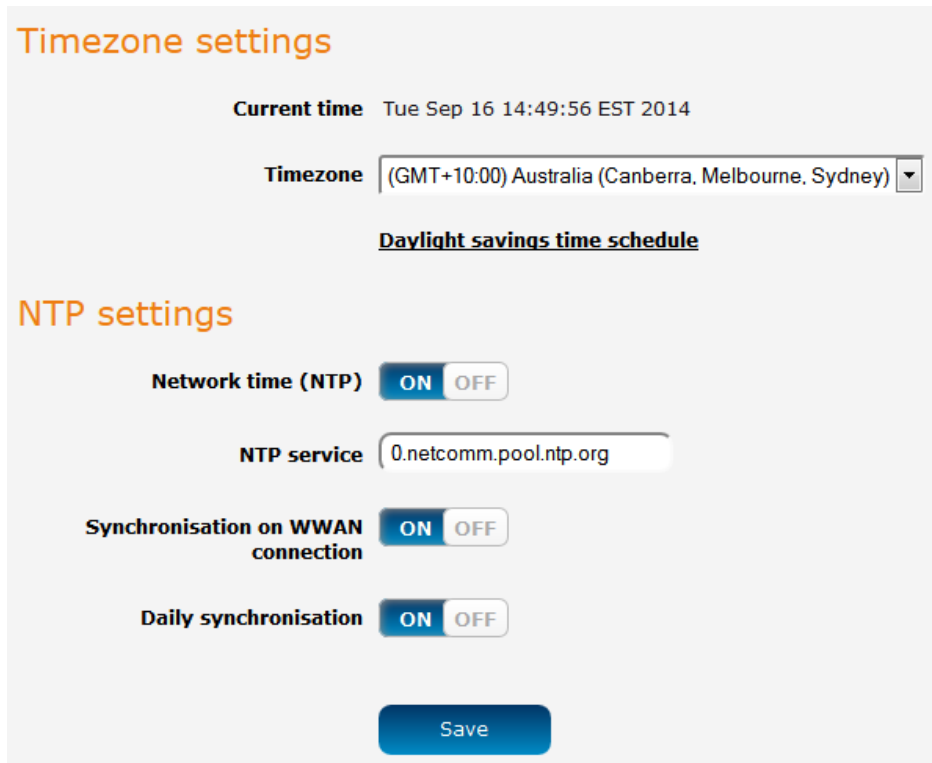
To configure dynamic DNS:

1. Click the **DDNS configuration** toggle key to switch it to the ON position.
2. From the **Dynamic DNS** drop down list, select the Dynamic DNS service that you wish to use. The available DDNS services available are:
 -  www.dhs.org
 -  www.dyndns.org
 -  www.dyns.cx
 -  www.easydns.com
 -  www.justlinux.com
 -  www.no-ip.com
 -  www.ods.org
 -  www.tzo.com
 -  www.zoneedit.com
3. Enter your hostname in 'Host name' field.
4. In the **Username** and **Password** fields, enter the logon credentials for your DDNS account. Enter the password for the account again in the **Verify password** field.
5. Click the **Save** button to save the DDNS configuration settings.

Network time (NTP)

The NTP (Network Time Protocol) settings page allows you to configure the NTC-40WW router to synchronize its internal clock with a global Internet Time server and specify the time zone for the location of the router. This provides an accurate timekeeping function for features such as System Log entries and Firewall settings where the current system time is displayed and recorded.

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



Timezone settings

Current time Tue Sep 16 14:49:56 EST 2014

Timezone (GMT+10:00) Australia (Canberra, Melbourne, Sydney) ▼

Daylight savings time schedule

NTP settings

Network time (NTP) ON OFF

NTP service 0.netcomm.pool.ntp.org

Synchronisation on WWAN connection ON OFF

Daily synchronisation ON OFF

Save

Figure 82 - NTP settings

Configuring Timezone settings

To configure time zone settings:

1. The **Current time** field shows the time and date configured on the router. If this is not accurate, use the **Time zone** drop down list to select the correct time zone for the router. If the selected zone observes daylight savings time, a **Daylight savings time schedule** link appears below the drop down list. Click the link to see the start and end times for daylight savings.
2. When you have selected the correct time zone, click the **Save** button to save the settings.

Configuring NTP settings

To configure NTP settings:

1. Click the **Network time (NTP)** toggle key to switch it to the **ON** position.
2. In the **NTP service** field, enter the address of the NTP server you wish to use.
3. The **Synchronization on WWAN connection** toggle key enables or disables the router from performing a synchronization of the time each time a mobile broadband connection is established.
4. The **Daily synchronisation** toggle key enables or disables the router from performing a synchronization of the time each day.
5. When you have finished configuring NTP settings, click the **Save** button to save the settings.

Data stream manager








The data stream manager provides you with the ability to create mappings between two endpoints on the router. These endpoints may be physical or virtual, for example, a serial port connected to the router’s USB port could be configured as an endpoint or you could configure a TCP Server as an endpoint. You can then configure a virtual data tunnel or “stream” between the endpoints.

The data stream manager provides a wide range of possibilities and expands upon simple PAD functionality to include the forwarding and translation of data between any of the endpoints. For example, you could connect a GPS to the router using a USB-to-Serial cable and send the received GPS Data to a TCP server running on the router. In each case, the logical flow of data is from Endpoint A to Endpoint B.

Customers interested in developing their own applications to create custom endpoints and streams can contact NetComm Wireless about our Software Development Kit.

Endpoints

The first thing to be done in order to create a data stream is to define the endpoints. There are 6 types of endpoint that may be configured:

-  Serial port (generic)
-  TCP Server
-  TCP Client
-  UDP Server
-  UDP Client
-  User defined executable
-  TCP connect-on-demand

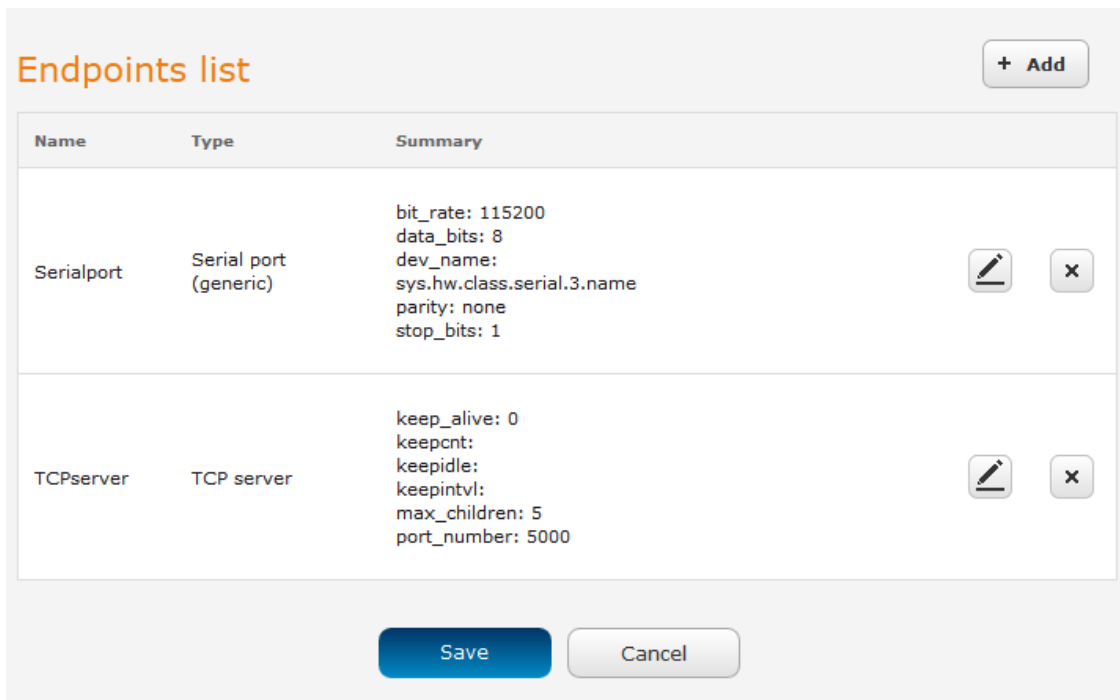


Figure 83 - Endpoints list

Serial port (generic)

This creates a generic serial port as an endpoint defaulting to the commonly used settings as shown below.

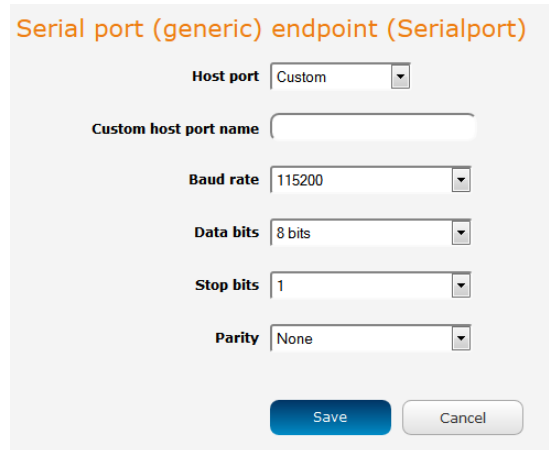


Figure 84 - Serial port (generic) endpoint configuration (Custom)

When the Host port is set to **Custom**, you can use the **Custom host port name** field to manually specify a device path to use, for example, if using a USB-to-Serial adapter you could telnet to the router and issue the command `ls /dev/ttyUSB*` to list the paths of the connected USB devices. To determine the path of the desired USB adapter, issue the command when the adapter is not connected then run the command again when the adapter is connected and compare the output.



Note: Using a custom host port name is not recommended for normal use as the device path can change between power cycles of the router.

TCP server

This creates a TCP server endpoint with the following options available.

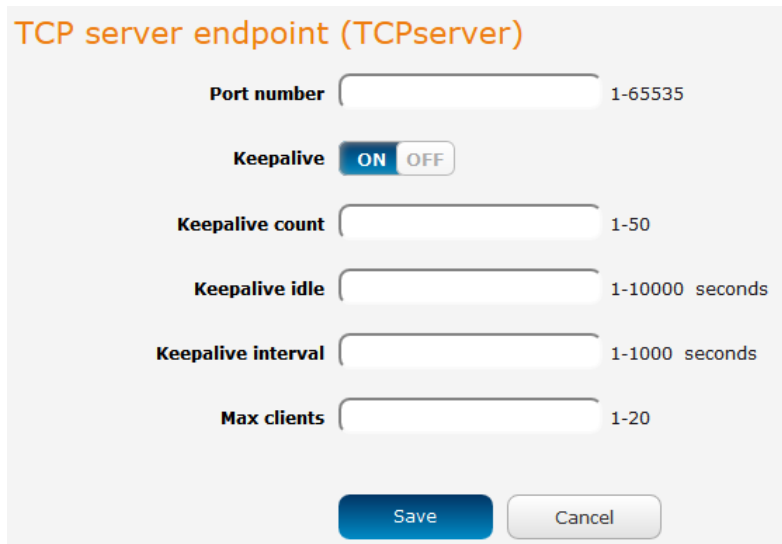
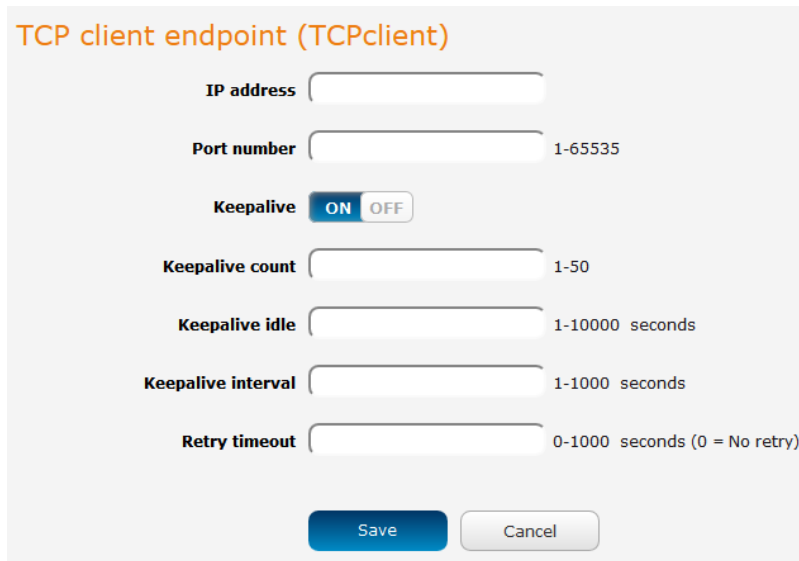


Figure 85 - TCP server endpoint configuration

TCP client

This creates a TCP client endpoint with the following options available. The retry timeout period specifies the number of seconds to wait between attempts to re-establish a connection in the event that it is lost. The client will attempt re-connection indefinitely every Retry timeout interval.



TCP client endpoint (TCPclient)

IP address

Port number 1-65535

Keepalive ON OFF

Keepalive count 1-50

Keepalive idle 1-10000 seconds

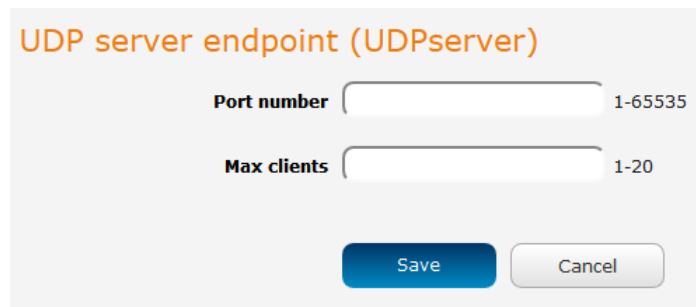
Keepalive interval 1-1000 seconds

Retry timeout 0-1000 seconds (0 = No retry)

Figure 86 - TCP client endpoint configuration

UDP server

This creates a UDP server endpoint with the following options available.



UDP server endpoint (UDPserver)

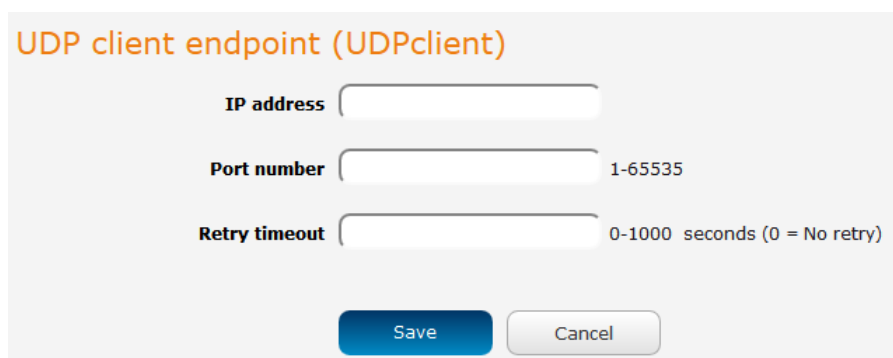
Port number 1-65535

Max clients 1-20

Figure 87 - UDP server endpoint configuration

UDP client

This creates a UDP client endpoint with the following options available. The retry timeout period specifies the number of seconds to wait between attempts to re-establish a connection in the event that it is lost. The client will attempt re-connection indefinitely every Retry timeout interval.



UDP client endpoint (UDPclient)

IP address

Port number 1-65535

Retry timeout 0-1000 seconds (0 = No retry)

Figure 88 - UDP client endpoint configuration

User defined executable

Allows you to specify an executable and parameters to be used as an endpoint. For example, the following executable reads the phone module temperature every second.

```
while true; do rdb_get wwan.0.radio.temperature; sleep 1; done
```

The temperature can then be sent to another endpoint.



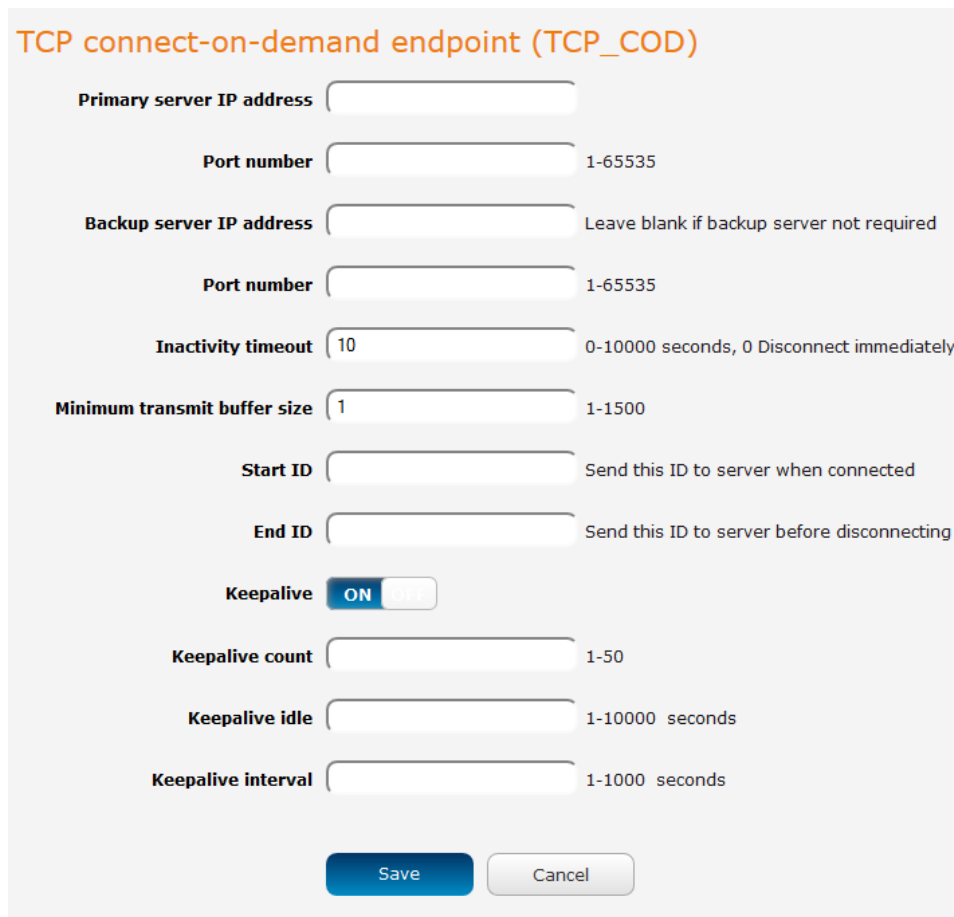
User defined executable endpoint ()

Command

Figure 89 – User defined executable endpoint configuration

TCP connect-on-demand endpoint

The TCP connect-on-demand endpoint allows data to be buffered and then sent to a TCP server when the buffer has been filled. It is primarily useful in situations where you do not want 'keep alive' packets to keep the socket open and create an overhead when the TCP data connection is not in use.



TCP connect-on-demand endpoint (TCP_COD)

Primary server IP address

Port number 1-65535

Backup server IP address Leave blank if backup server not required

Port number 1-65535

Inactivity timeout 0-10000 seconds, 0 Disconnect immediately

Minimum transmit buffer size 1-1500

Start ID Send this ID to server when connected

End ID Send this ID to server before disconnecting

Keepalive ON OFF

Keepalive count 1-50

Keepalive idle 1-10000 seconds

Keepalive interval 1-1000 seconds

Figure 90 – TCP connect-on-demand endpoint configuration

ITEM	DESCRIPTION
Primary server IP address	The IP address of the TCP server to which the router should attempt the initial connection.
Port number	The port number that the TCP server operates on.
Backup server IP address	If connection to the primary server fails, the router will attempt to connect to this address.
Port number	The port number that the backup TCP server operates on.
Inactivity timeout	The period, in seconds, that the socket is considered idle/inactive if no packets are sent. The timer begins at the end of the last sent packet. The valid range is 0-10000 seconds. If this field is set to 0, the client disconnects immediately after sending a packet.
Minimum transmit buffer size	The number of bytes that must be reached before the client decides to transmit.
Start ID	This is a string which, if configured, is sent before any serial data is sent, every time the client connects <START ID><SERIAL DATA>
End ID	This is a string which, if configured, is sent after all serial data, just before the client disconnects <START ID><SERIAL DATA><END ID>
Keepalive	Keepalive sends a message to check that the link is still active or to keep it active.
Keepalive count	The number of keepalive messages to send.
Keepalive idle	The duration between two keepalive transmissions when in idle condition.
Keepalive interval	The duration between two successive keepalive retransmissions.

Table 20 – TCP connect-on-demand endpoint options

To create an endpoint:

1. Click the **+Add** button on the right side of the page. A pop-up window appears.

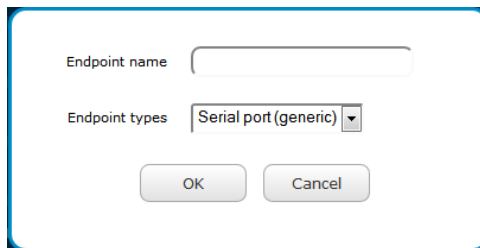


Figure 91 - Creating an endpoint

2. In the **Endpoint name** field, type a name for this endpoint. The name can contain alphanumeric characters only i.e. A-Z, a-z, 0-9.
3. Use the **Endpoint types** drop down list to select the type of endpoint to configure.
4. Click the **OK** button. The router displays a screen with configuration options for your chosen endpoint type. Enter the options for your endpoint as required.
5. Click the Save button. The Endpoints list is displayed with the newly created endpoint listed and a summary of the settings you configured.

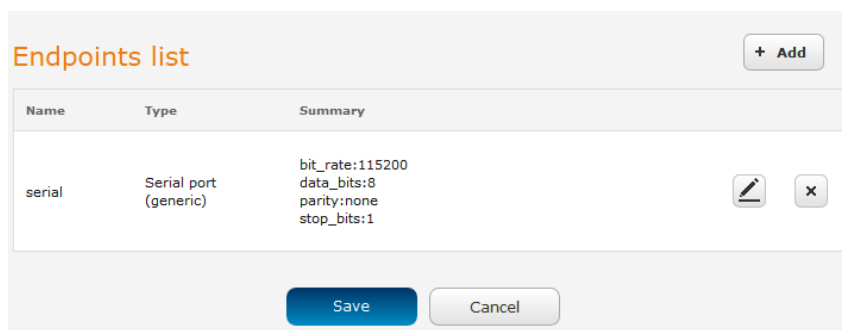


Figure 92 - Endpoints list

Streams

When you have created the required endpoints, you can then proceed to set up a data stream. A data stream sends data from one endpoint to another, performing any transformation of the data as required. When a stream is added, an underlying process on the router checks the validity of the stream, checking for conflicts and illogical configurations.



Notes on data stream operation:

- When any changes to the Data stream manager configuration are detected, all data streams are stopped and restarted as per the new configuration.
- Multiple Modbus clients cannot connect simultaneously to Modbus serial slaves connected to the router.

Every stream requires two endpoints, Endpoint A and Endpoint B. In all cases, the flow of data is from Endpoint A to Endpoint B.

To create a new stream:

1. Click the **+Add** button on the right side of the page.



Figure 93 - Data stream list



The Edit data stream page is displayed.

2. In the **Data stream name** field, enter a name for the Data stream.
3. Under Endpoint A, use the **Endpoint name** drop down list to select one of the endpoints you created previously. This endpoint should be the starting point of the stream. Use the **Mode** drop down list to select the mode of operation of the endpoint. The mode can be thought of as a transformation of the data as it leaves this endpoint. For example, if Endpoint A type is Serial port (generic), the Mode can be set to various Modbus server and client types. This means that upon arrival at Endpoint A, the data will be transformed into the chosen Modbus format, ready to be sent to Endpoint B.
4. Under Endpoint B, use the **Endpoint name** drop down list to select one of the endpoints you created previously. This endpoint should be the destination of the stream. The screenshot below shows a configuration sending data received on an attached serial port to a TCP server running on the router. Use the **Mode** drop down list to select the mode of operation of the endpoint. The mode can be thought of as a transformation of the data as it arrives at this endpoint.

Figure 94 - Edit data stream

5. Click the **Save** button. The new stream appears in the Data stream list.

Data stream list + Add

Name	Endpoint A	Mode	Endpoint B	Mode	Enabled	Status		
SerialtoTCP	Serial	Raw	TCPserver	Raw	Enabled	Running		

Save Cancel

Figure 95 - Data stream list

Data stream applications

ENDPOINT A	ENDPOINT B	ENDPOINT A MODE / ENDPOINT B MODE	ENDPOINTS CAN BE REVERSED	UNDERLYING PROCESS	APPLICATION
1 (Serial), 8 (RS232), 9 (RS485), 10 (RS422)	1 (Serial), 8 (RS232), 9 (RS485), 10 (RS422)	Raw/Raw	N/A	socat	Serial to serial raw data stream
1 (Serial), 8 (RS232), 9 (RS485), 10 (RS422)	2 (TCP Server), 3 (TCP Client), 4 (UDP Server), 5 (UDP Client)	Raw/Raw	Yes	socat	Serial to IP data stream
2 (TCP Server), 4 (UDP Server)	3 (TCP Client), 5 (UDP Client)	Raw/Raw	Yes	socat	Client to server data stream
1 (Serial), 8 (RS232), 9 (RS485), 10 (RS422)	3 (TCP Client)	Modbus Client Agent ASCII, Modbus Client Agent RTU/raw	No	dsm_data_mover	Modbus Client Agent functionality
1 (Serial), 8 (RS232), 9 (RS485), 10 (RS422)	2 (TCP Server)	Modbus Server Gateway ASCII, Modbus Server Gateway RTU/raw	No	dsm_data_mover	Modbus Server Gateway functionality
1 (Serial), 8 (RS232), 9 (RS485), 10 (RS422)	6 (GPS)	Raw/Raw	Yes	socat	Send GPS data to serial port
1 (Serial), 8 (RS232), 9 (RS485), 10 (RS422)	7 (User Executable)	Raw/Raw	Yes	socat	Send standard output of user-executable program to serial port
2 (TCP Server), 3 (TCP Client), 4 (UDP Server), 5 (UDP Client)	6 (GPS)	Raw/Raw	Yes	socat	Send GPS data to TCP or UDP client or server
2 (TCP Server), 3 (TCP Client), 4 (UDP Server), 5 (UDP Client)	7 (User Executable)	Raw/Raw	Yes	socat	Send standard output of user-executable program to TCP or UDP client or server
11 (Modem Emulator)	12 (PPP Server)	Raw/Raw	Yes	modem_emul_ep	Router terminated PPP Server functionality for dial-up PPP clients
11 (Modem Emulator)	13 (IP Modem)	Raw/Raw	Yes	modem_emul_ep	Modem emulation and tunneling via TCP/UDP (replacement for PAD Mode of the old Modem Emulator)
11 (Modem Emulator)	14 (CSD)	Raw/Raw	Yes	modem_emul_ep	Circuit Switched Data calls via 3G/4G module and mobile networks
1 (Serial), 8 (RS232), 9 (RS485), 10 (RS422)	15 (TCP Client Connect on Demand)	Raw/Raw	Yes	dsm_data_mover	Serial to TCP server connection, which is initiated ONLY when data is seen on serial port

Table 21 - Data stream applications

PADD

PAD Daemon is a tool used to encapsulate raw serial data into a TCP packet to be transported over IP to another end point. The server receiving the TCP packets unpacks the data and the original raw serial data is passed out of its serial port to the attached device, thereby creating an invisible IP network to the two serial devices.

The PAD Daemon runs as a background process which can be accessed via the web configuration interface. The PADD configuration page is located under “Services > PADD”. The PADD is used usually with multiple connections or when redundant connections are needed. The PADD has two modes: the PADD TCP/IP Server mode and PADD TCP/IP Client Mode. When PADD is enabled, both the PADD server mode and PADD client mode can be run at the same time.

The PADD configuration page is shown below.

PADD

Activate ON OFF

Serial port status No conflicts

Debug level (0-2)

Serial port settings

Host port

Custom host port name

Baud rate

Data bits

Stop bits

Parity

Flow control

Inter character timeout (x100ms)

End-of-line character ASCII code

Start of line timestamps OFF YYYYMMDDHHMMSS

TCP/IP Server

Listening port 1-65535

Incoming connection is Exclusive Shared

TCP/IP Client

Connect to First available All available

Remote Host 1 Server:Port

Remote Host 2 Server:Port

Remote Host 3 Server:Port

Remote Host 4 Server:Port

Network

Remote server retry period 1-65535 seconds

TCP Keepalive Probes 0-65535 seconds (0=disabled)

Number of probe failures before disconnect 1 - 20

Figure 96 – PADD

A whitepaper with full Instructions on configuring PADD Mode is available at <http://support.netcommwireless.com/product/m2m/ntc-40wv>

Remote management

SNMP

SNMP configuration

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

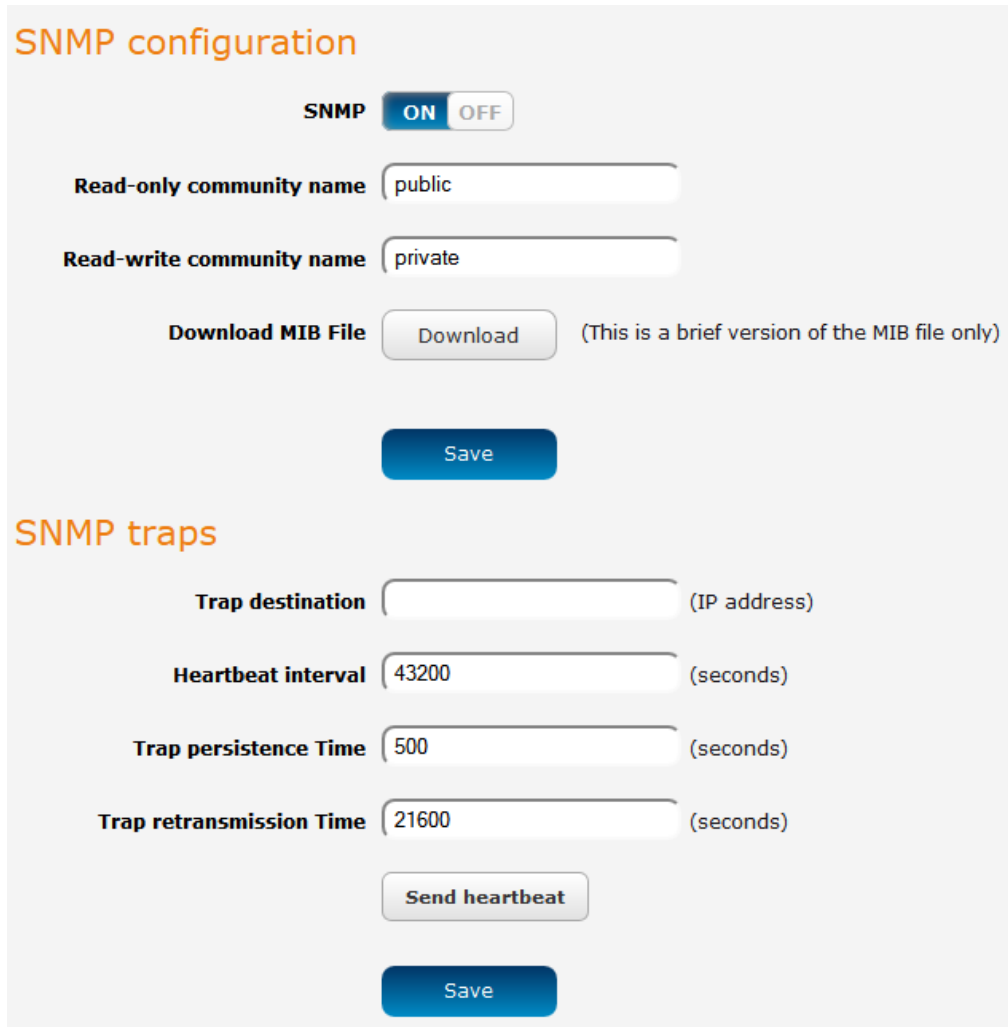


Figure 97 - SNMP configuration

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 and the interface status.

To configure SNMP:

1. Click the **SNMP** toggle key to switch it to the **ON** position.
2. Enter **Read-only community name** and **Read-write community name** which are used for client authentication.



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

3. Click the **Save** button to save any changes to the settings.

The **Download** button displays the Management Information Base (MIB) of the router. The MIB displays all the objects of the router that can have their values set or report their status. The MIB is formatted in the SNMP-related standard RFC1155.

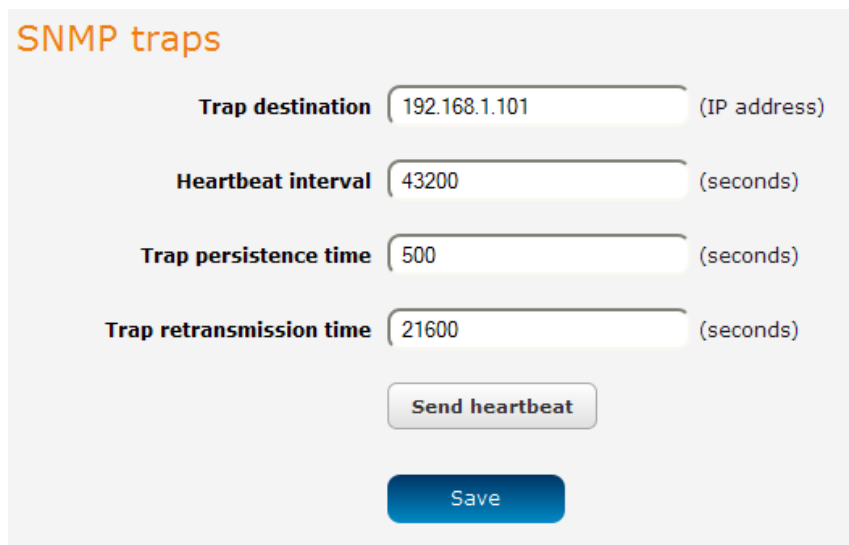
SNMP traps

SNMP traps are messages from the router to the Network Management System sent as UDP packets. They are often used to notify the management system of any significant events such as whether the link is up or down.

Configuring SNMP traps

To configure SNMP traps:

1. In the **Trap destination** field, enter the IP address to which SNMP data is to be sent.
2. In the **Heartbeat interval** field, enter the number of seconds between SNMP heartbeats.
3. Use the **Trap persistence** field to specify the time in seconds that an SNMP trap persists.
4. Use the **Trap retransmission** time to specify the length of time in seconds between SNMP trap retransmissions.



SNMP traps

Trap destination (IP address)

Heartbeat interval (seconds)

Trap persistence time (seconds)

Trap retransmission time (seconds)

Figure 98 - SNMP traps

To send a manual SNMP Heartbeat, click the **Send heartbeat** button. When you have finished configuring the SNMP traps, click the **Save** button to save the settings.



Note: When a factory reset is performed via SNMP, the SNMP settings are preserved.

TR-069

To access the TR-069 configuration page, click the **Services** menu item, then select the TR-069 menu item on the left.

TR-069 configuration

Enable TR-069 ON OFF

ACS URL

ACS username

ACS password

Verify ACS password

Connection request username

Connection request password

Verify connection request password

Enable periodic ACS informs ON OFF

Inform period (30-2592000) secs

Last inform status

Start at

End at

TR-069 DeviceInfo

Manufacturer NetComm Wireless Limited

ManufacturerOUI 006064

ModelName ntc_40wv

Description NetComm NTC-40WV Cellular Router




ProductClass 40WV Series

SerialNumber 11111F

Figure 99 - TR-069 configuration

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.

TR-069 uses a bi-directional SOAP/HTTP-based protocol based on the application layer protocol and provides several benefits for the maintenance of a field of CPEs:

-  Simplifies the initial configuration of a device during installation
-  Enables easy restoration of service after a factory reset or replacement of a faulty device
-  Firmware and software version management
-  Diagnostics and monitoring



Note: You must have your own compatible ACS infrastructure to use TR-069. In order to access and configure the TR-069 settings you must be logged into the router as the root user.



Note: When a factory reset of the router is performed via TR-069, the TR-069 settings are preserved.

TR-069 configuration

To configure TR-069:

1. Click the **Enable TR-069** toggle key to switch it to the **ON** position.
2. In the **ACS URL** field, enter the Auto Configuration Server's full domain name or IP address.
3. Use the **ACS username** field to specify the username for the Auto Configuration Server.
4. In the **ACS password** and **Verify ACS password** fields, enter the Auto Configuration Server password.
5. In the **Connection Request Username** field, enter the username to use for the connection requests.
6. In the **Connection Request Password** and **Verify password** fields, enter the connection request password.
7. The inform message acts as a beacon to inform the ACS of the existence of the router. Click the **Enable periodic ACS informs** toggle key to turn on the periodic ACS inform messages.
8. In the **Inform Period** field, enter the number of seconds between the inform messages.
9. Click the **Save** button to save the settings.




OMA Lightweight M2M configuration

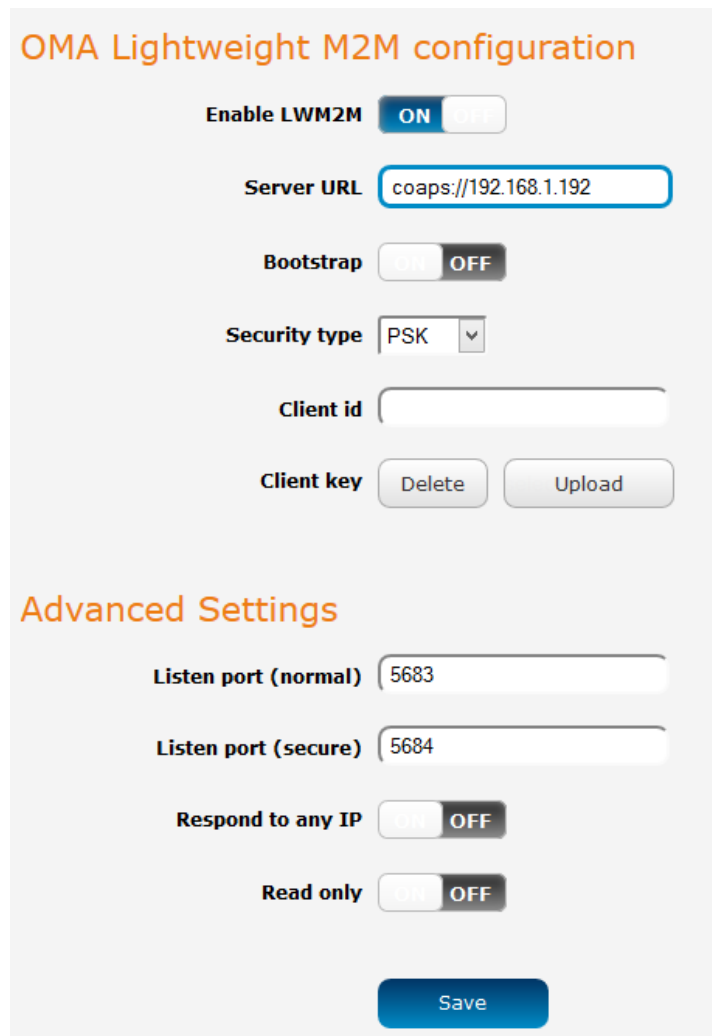


Note: The OMA Lightweight M2M specification has not yet been finalised. As such, the current implementation of OMA-LWM2M is experimental and should not be deployed for regular use. We also do not recommend using OMA-LWM2M while the router is connected to an APN providing a publicly routable IP address.

The OMA Lightweight M2M (OMA-LWM2M) protocol was designed by the Open Mobile Alliance to provide remote device management specifically for M2M devices. It is less taxing on the system and network than OMA-DM and TRS-069. OMA-LWM2M runs over UDP and supports asynchronous notifications when a resource changes.

It provides:

-  Firmware upgrades
-  Device monitoring and configuration
-  Server provisioning



The screenshot shows a web configuration page titled "OMA Lightweight M2M configuration". It features several settings:

- Enable LWM2M:** A toggle switch currently set to "ON".
- Server URL:** A text input field containing "coaps://192.168.1.192".
- Bootstrap:** A toggle switch currently set to "OFF".
- Security type:** A dropdown menu currently set to "PSK".
- Client id:** An empty text input field.
- Client key:** Two buttons labeled "Delete" and "Upload".

Below these settings is a section titled "Advanced Settings":

- Listen port (normal):** A text input field containing "5683".
- Listen port (secure):** A text input field containing "5684".
- Respond to any IP:** A toggle switch currently set to "OFF".
- Read only:** A toggle switch currently set to "OFF".

A large blue "Save" button is located at the bottom of the configuration area.

Figure 100 - OMA Lightweight M2M configuration

ITEM	DESCRIPTION
Enable LWM2M	Toggles the OMA-LWM2M function on and off.
Server URL	The URL of the LWM2M server. This must begin with coap:// or coaps:// and include the server port number. The correct syntax for this field is <code>coap://<server IP or domain name>:<port number></code> . The Server URL field performs validation on the entered address so the field must contain an address in the correct format.
Listen port (normal)	The port that the router listens on for LWM2M.
Listen port (secure)	When using DTLS (coaps), enter the port that the router listens on for secure connections.
Security type (only used when Server URL starts with coaps://)	NoSec – When selected, this uses DTLS with the NULL cipher, therefore, it provides no security.
	PSK – Pre-shared key mode. Keys are typically a string of text saved into a text file. We recommend creating a key at least 32 bytes in size to enhance your security.
	RPK – Raw Public Key. The key is an EC key in DER format. It must contain both public and private keys. When RPK is selected, the Client ID field is not used. You can generate a raw public key using commands such as: <code>openssl ecparam -out 256.key -name secp256r1 -genkey</code> <code>openssl ec -in 256.key -outform der -out 256.der</code>
Client id (only used when Server URL starts with coaps:// and Security type is PSK)	When server is a coaps:// address and security type is set to PSK, the Client id acts as a means of identifying the client, similar to a username.
Client key (only used when Server URL starts with coaps:// and Security type is PSK or RPK)	This field is used to upload the key file used when security type is set to PSK, delete the uploaded key file or show the currently stored key.
Respond to any IP	When turned on, this feature adds a firewall rule that allows the router to respond to any IP address on the designated port. This eases the restrictions that requests must come from servers the client is currently registered with. We recommend that this feature is turned off for normal use.
Bootstrap	When set to the ON position, this specifies that the Server URL field points to a bootstrap server.
Read only	When set to the ON position, this allows read only access to all LWM2M settings. Writing new values and executing commands are not permitted. When set to OFF, values may be read, written and executed.

Table 22 – OMA Lightweight M2M configuration options

Supported objects

The objects and instances used by NetComm Wireless routers are all part of the Open Mobile Alliance and IPSO Alliance approved list. At this time, there are no NetComm-specific objects or instances. For more information on the Lightweight M2M specifications, please visit the Open Mobile Alliance Specifications for Public Comment website:

<http://technical.openmobilealliance.org/Technical/technical-information/specifications-for-public-comment>

Timeouts

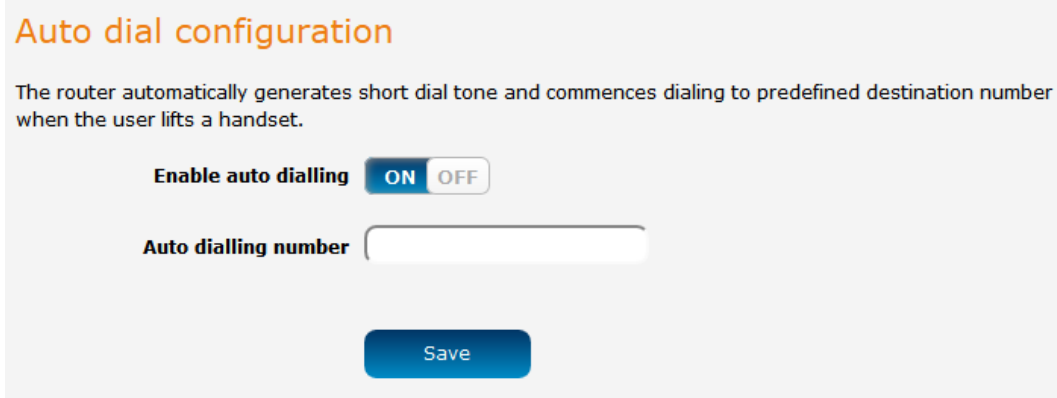
Most mobile networks use stateful firewalls or NAT where the timeout for UDP is approximately 1-2 minutes. If this applies to you, configure your server to change the 'lifetime' (resource 1/0/1) to be shorter than the default 86400. We suggest setting it to 60.

Supported ciphers

- 🌀 TLS_PSK_WITH_AES_128_CBC_SHA256
- 🌀 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- 🌀 NULL (only if "NoSec" explicitly selected)
- 🌀 Others may be negotiated by OpenSSL during connection

Auto dial configuration

Using the Auto dial function, you can configure the router to automatically dial a pre-defined phone number when the handset is lifted.



Auto dial configuration

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

Enable auto dialling ON OFF

Auto dialling number

Figure 101 - Auto dial configuration

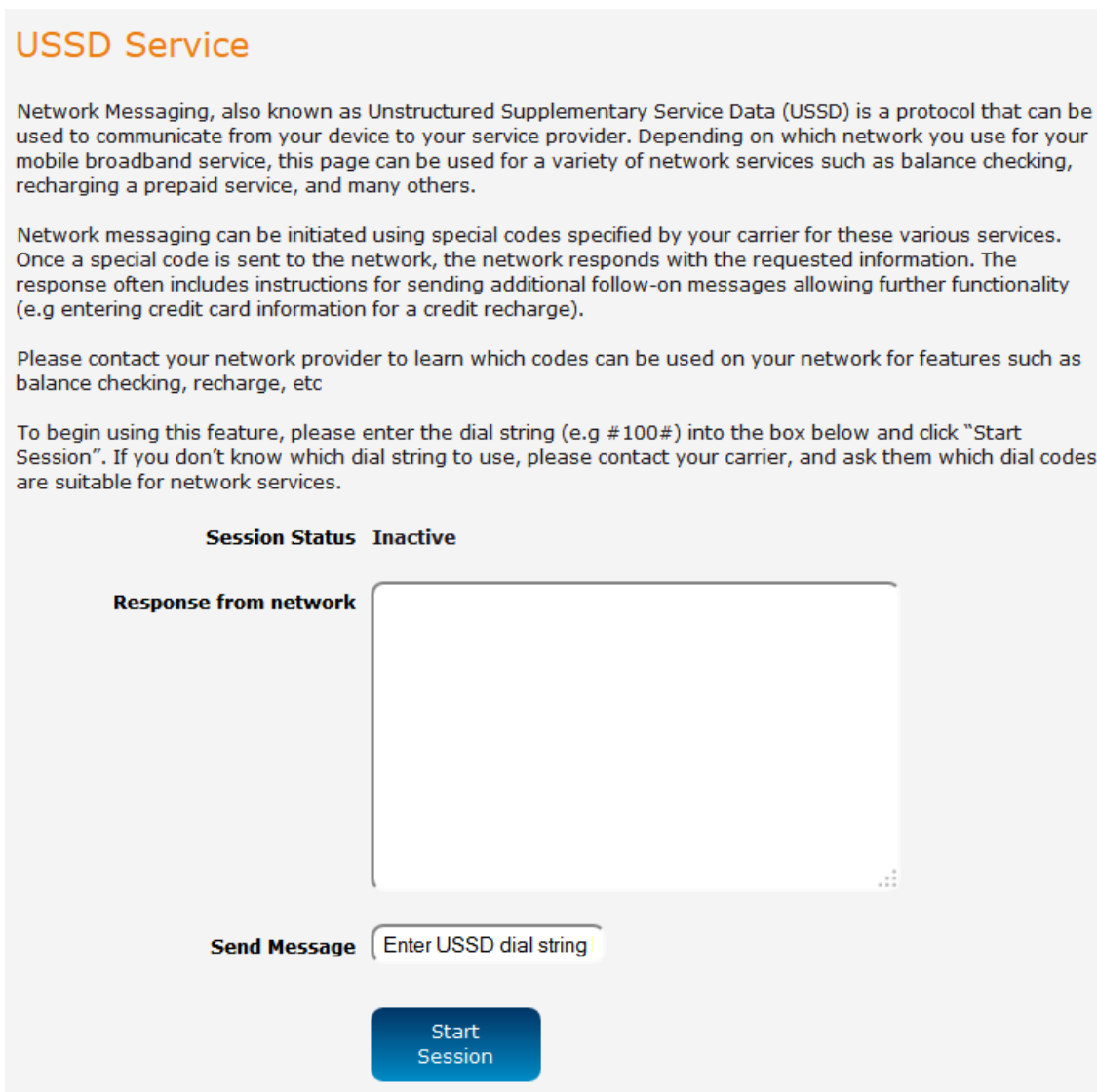
USSD

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.



USSD Service

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

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

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

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

Session Status Inactive

Response from network

Send Message

Start Session

Figure 102 - USSD Service

Voice

The Voice page provides basic toggles to turn the voice feature of the router on or off as well as the ability to enable or disable incoming or outgoing voice calls while the SIM is in a roaming state.

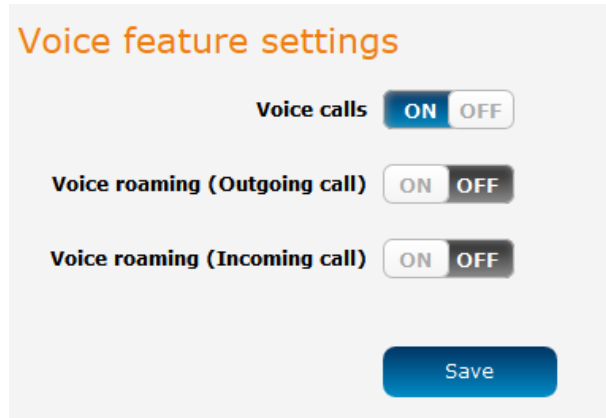


Figure 103 - Voice feature settings

Event notification

The event notification feature is an advanced remote monitoring tool providing you with the ability to send alerts via SMS, e-mail, TCP or UDP when pre-defined system events occur.

Notification configuration

The Notification configuration screen is used to select the event types, methods of notification and the destinations for the notifications. Up to four types of alerts for a particular event may be sent to a single destination profile containing the contact details.

Event notification configuration

Enable event notification ON

Maximum event buffer size (100-10000)

Maximum retry count (1-20)

Event notification log file

Unit ID

Event description	Event number	Email	TCP	UDP	SMS	Destination profile
Unit powered up	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Default"/> ▼
Unit rebooted	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Default"/> ▼
Link status change	3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Default"/> ▼
WWAN IP address change	4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Default"/> ▼
WWAN Registration change	5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Default"/> ▼
WWAN Cell ID change	6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Default"/> ▼
WWAN technology change	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Default"/> ▼
Number of connected Ethernet interfaces change	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Default"/> ▼
Web UI login failure	10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Default"/> ▼
WAN failover instance occurred	12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Default"/> ▼
WiFi clients number changed	13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Default"/> ▼

Figure 104 - Event notification configuration

ITEM	DESCRIPTION
Enable event notification	Toggles the event notification feature on and off.
Maximum event buffer size	Specifies the buffer size for event notifications which failed to be delivered or are yet to be sent. The minimum size is 100 and the maximum is 10000.
Maximum retry count	Specifies the maximum number of attempts that the router will make to deliver an event notification. The range is between 1 and 20.
Event notification log file	Specifies to the location and name of the file used to log the event notification activity.
Event notification prefix	The Unit ID field is used to specify an identifier for the router which are sent in the event notifications so that you know which router has an event.

Table 23 - Event notification configuration options

Event types

There are ten events for which you can configure alerts. Hovering the mouse over the event description provides more details of event notification type.

EVENT	EVENT NUMBER	DESCRIPTION	EXAMPLE MESSAGE
Unit powered up	1	Notification is sent when the unit is powered up through connection of a power source or after a soft-reset.	Power is up
Unit rebooted	2	Notification is sent when the unit is rebooted via Web UI, SMS diagnostics or via command line/telnet session.	Rebooting triggered by internal application
Link status change	3	Notification is sent if the status of the data connection profile or any IPSec/OpenVPN/PPTP/GRE tunnel endpoint changes i.e. the link goes up or down.	Profile 1 WWAN status changed : down --> up
WWAN IP address change	4	Notification is sent if an active data connection profile's WWAN IP address changes.	WWAN IP address changed : N/A --> 10.103.4.149
WWAN Registration change	5	Notification is sent if the network registration status changed between "registered", "unregistered" or "roaming".	WWAN registration status changed : Not registered --> Registered to home network
WWAN Cell ID change	6	Notification is sent if the router connects to a different cell, marked by a changed in the Cell ID.	Cell ID changed : --> 15224145 Cell ID changed : 15224148 --> 15224145
WWAN technology change	7	Notification is sent if the router connects to a different network technology, e.g. 3G/2G.	WWAN network changed : N/A() --> 3G(UMTS) WWAN network changed : 3G(UMTS) --> 2G(GSM)
Number of connected Ethernet interfaces change	8	Notification is sent if there is a change to the number of directly connected Ethernet interfaces.	Ethernet device number changed : 0 --> 1
Web UI login failure	10	Notification is sent if there was a failure to log in to the router via the Web UI.	WEBUI login failed, username root, password
WAN failover instance occurred	12	Notification is sent if a failover between WAN interfaces occurs.	Failover instance occurred: N/A --> wwan.0 Failover instance occurred: eth.0 --> wwan.0
WiFi clients number changed	13	Notification is sent if the number of connected WiFi clients changes.	WiFi clients number changed : 0 --> 1

Table 24 - Event notification – event types

Destinations

A "destination" is a profile on the router containing the contact details of a recipient of event notification alerts i.e. the e-mail address, SMS number, TCP or UDP server addresses of the recipient. The destination profile must contain the details of at least one destination type in order to be used.

Configuring Event notification

To configure the event notification feature:

1. Click the Services menu item at the top of the screen. From the Event notification menu on the left of the screen, select the **Destination configuration** menu item.
2. Click the **+Add** button at the top right corner of the window. The Event destination edit screen is displayed.
3. In the **Destination name** field enter a name for the destination profile then enter the contact details for the each type of destination i.e. Email address, TCP address and port, UDP address and port and/or SMS number.
4. Click the **Save** button when you have entered the required details.

5. From the Event notification menu on the left of the screen, select the **Notification configuration** menu item.
6. Select the **Enable event notification** toggle key to turn it to the **ON** position.
7. If desired, set the **Maximum event buffer size**, **Maximum retry count**, **Event notification log file** and **Event notification prefix** fields. See table 23 for descriptions of these options.
8. From the **Destination** column, use the drop down menus to select the desired destination profiles to use for the corresponding events, then select the checkboxes for the types of notifications to send to the chosen destination profile. If the Destination profile does not contain the required contact details, a pop-up warns you to enter the required details in the Destination profile.
9. Click the **Save** button.



Note: If you have selected the Email notification type for any of the events, you must also configure Email client settings to allow the router to send e-mail messages.

Destination configuration

The Destination configuration screen displays a list of the destination “profiles” that have been configured on the device as well as providing the option to add new profiles.

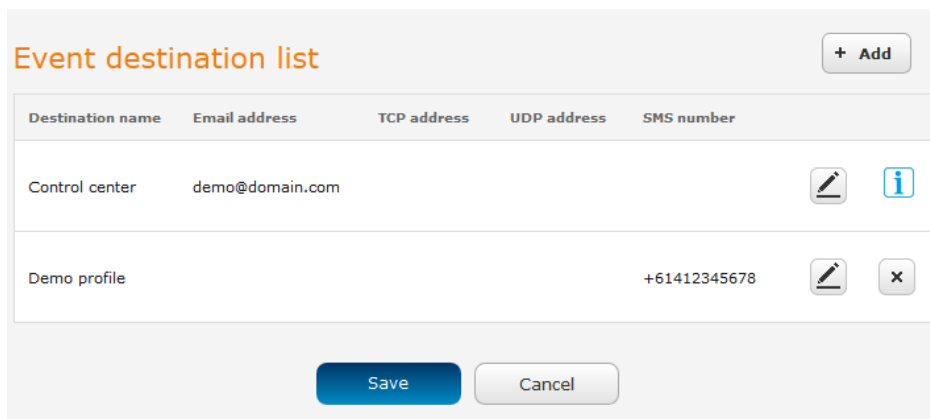


Figure 105 - Event destination list

To add a new destination profile:

1. Click the **+Add** button at the top right corner of the window. The Event destination edit screen is displayed.
2. In the **Destination name** field enter a name for the destination profile then enter the contact details for the each type of destination i.e. Email address, TCP address and port, UDP address and port and/or SMS number.
3. Click the **Save** button when you have entered the required details.

To edit a destination profile:

1. From the Event destination list, click the edit button for the corresponding destination profile. The Event destination edit page is displayed. Make the required changes.
2. Click the **Save** button.

To delete a destination profile:

1. From the Event destination list, select the delete button for the corresponding destination profile that you would like to delete. If the destination profile is linked to an event notification type, the **i** button is displayed instead of the delete button. In this case, you must go to the **Notification configuration** screen and remove the check marks from all the notification types for each event for which the destination profile is configured. When you have done that, return to the Event destination list and select the delete button.
2. Click the **Save** button.

Email settings

The Email settings screen allows the configuration of the email account that is used to send emails in features such as Event notification.

To access the Email settings page, click the **Services** menu item then select the **Email settings** menu item on the left.

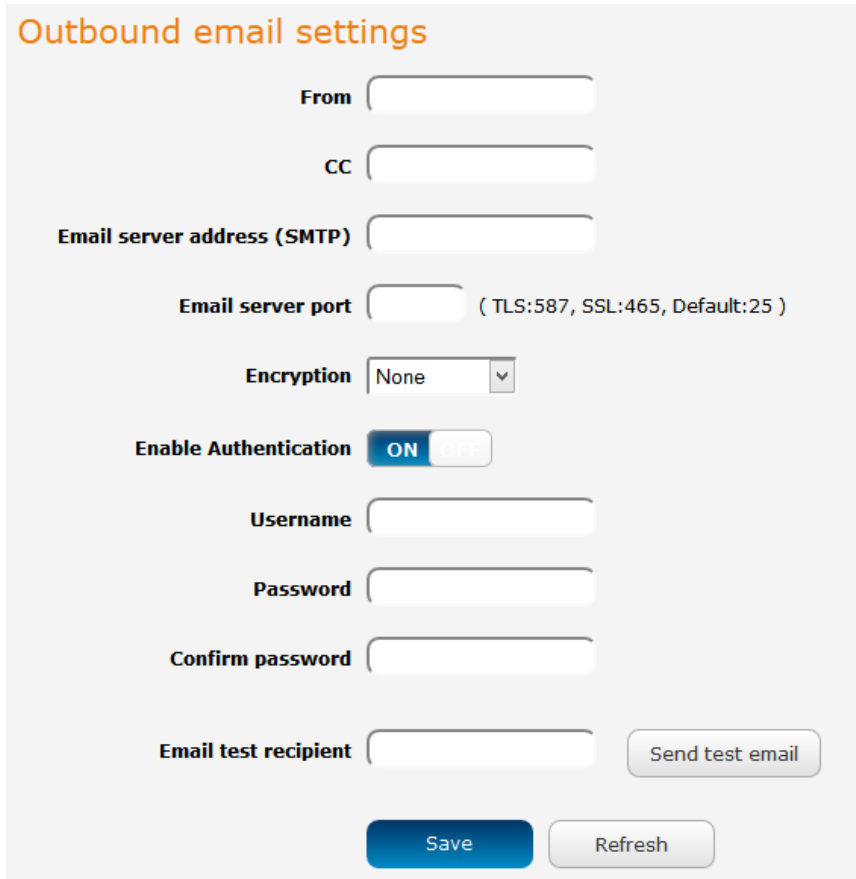


Figure 106 - Email client settings









ITEM	DESCRIPTION
From	Enter the email address of the account you will be using to send emails.
CC	(Optional) Enter an email address which will be copied on all messages sent.
Email server address (SMTP)	Enter the SMTP server address of the email server. This may be an IP address or a hostname.
Email server port	Enter the Email server's SMTP port.
Encryption	Use this drop down list to select the type of encryption to apply to the mail server connection.
Enable Authentication	If your mail server requires account authentication before it allows mail to be sent, enable this option and enter the account details in the Username and Password fields below.
Username	Enter the username of the account to be used for sending emails.
Password	Enter the password of the account to be used for sending emails.
Confirm password	Enter the password of the account to be used for sending emails once more for confirmation.
Email test recipient	Enter an email address to send a test message to, then click the Send test email button.

Table 25 - Email client settings

SMS messaging

The NTC-40WV router offers an advanced SMS feature set, including sending messages, receiving messages, redirecting incoming messages to another destination, as well as supporting remote commands and diagnostics messages.

Some of the functions supported include:

-  Ability to send a text message via a 2G/3G network and store it in permanent storage.
-  Ability to receive a text message via a 2G/3G network and store it in permanent storage.
-  Ability to forward incoming text messages via a 2G/3G network to another remote destination which may be a TCP/UDP server or other mobile devices.
-  Ability to receive run-time variables from the device (e.g. uptime) on request via SMS
-  Ability to change live configuration on the device (e.g. network username) via SMS.
-  Ability to execute supported commands (e.g. reboot) via SMS
-  Ability to trigger the NTC-40WV router to download and install a firmware upgrade
-  Ability to trigger the NTC-40WV router to download and apply a configuration file

To access the SMS messaging functions of the NTC-40WV router, click on the **Services** menu item from the top menu bar, and then select one of the options under the **SMS messaging** section on the left hand menu.

Setup

The Setup page provides the options to enable or disable the SMS messaging functionality and SMS forwarding functionalities of the router. SMS messaging is enabled by default.

General SMS configuration

SMS messaging ON OFF

Messages per page (10-50)

Encoding scheme GSM 7-bit UCS-2

SMSC address

Routing option

Packet-switched

Circuit-switched

Packet-switched preferred

Circuit-switched preferred

SMS forwarding configuration

Forwarding ON OFF

Redirect to mobile

TCP server address

TCP port (1-65535)

UDP server address

UDP port (1-65535)

Figure 107 - General SMS Configuration

OPTION	DEFINITION
General SMS configuration	
SMS messaging	Toggles the SMS functionality of the router on and off.
Messages per page (10-50)	The number of SMS messages to display per page. Must be a value between 10 and 50.
Encoding scheme	The encoding method used for outbound SMS messages. GSM 7-bit mode permits up to 160 characters per message but drops to 50 characters if the message includes special characters. UCS-2 mode allows the sending of Unicode characters and permits a message to be up to 50 characters in length.
SMS forwarding configuration	
Forwarding	Toggles the SMS forwarding function of the router on and off.
Redirect to mobile	Enter a mobile number as the destination for forwarded SMS messages.
TCP server address	Enter an IP address or domain name as the destination for forwarded SMS messages using TCP.
TCP port	The TCP port on which to connect to the remote destination.
UDP server address	Enter an IP address or domain name as the destination for forwarded SMS messages using UDP.
UDP port	The UDP port on which to connect to the remote destination.

Table 26 - SMS Setup Settings

SMS forwarding configuration

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 a 3G router phone number.

For Example:

If someone sends a text message and **Redirect to mobile** is set to “+61412345678”, the text message is stored on the router and forwarded to “+61412345678” at the same time.

To disable redirection to a mobile, clear the **Redirect to mobile** field and click the **Save** button.

Redirect to TCP / UDP server address

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 messages.

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 **TCP server address** is set to “192.168.20.3” and **TCP port** is set to “2002”, this text message is stored in the router and forwarded to “192.168.20.3” on port “2002” at the same time.

To disable redirection to a TCP or UDP address, clear the **TCP server address** and **UDP server address** fields and click the **Save** button.

New message

The New message page can be used to send SMS text messages to a single or multiple recipients.

A new SMS message can be sent to a maximum of 9 recipients at the same time. After sending the message, the result is displayed next to the destination number as “Success” or “Failure” if the message failed to send. By default, only one destination number field is displayed. Additional destination numbers may be added one at a time after entering a valid number for the current destination number field. To add a destination number, click the **+** button and to remove the last destination in the list, click the **-** button.

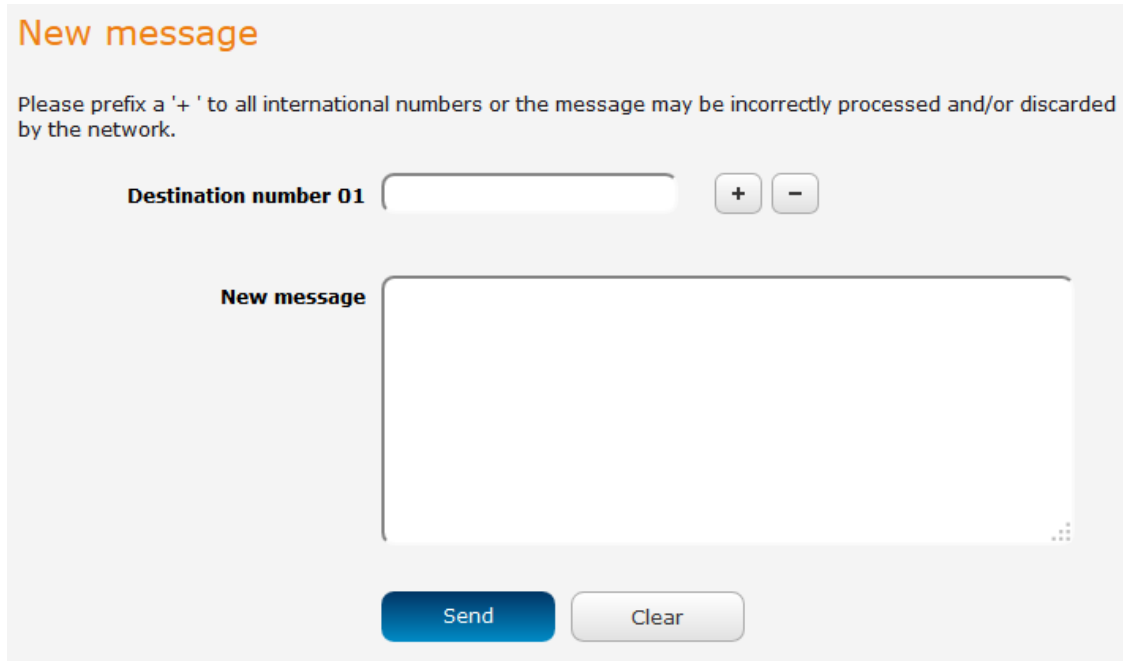


Figure 108 - SMS - New Message

Destination numbers should begin with the “+” symbol followed by the country calling code. To send a message to a destination number, enter the “+” symbol followed by the country calling code and then the destination number.

For example:

To send a message to the mobile destination number 0412345678 in Australia (country calling code 61), enter “+61412345678”.

After entering the required recipient numbers, type your SMS message in the **New message** field. As you type your message, a counter shows how many characters you have entered out of the total number available for your chosen encoding scheme. When you have finished typing your message and you are ready to send it, click the **Send** button.

Inbox / Sent Items

The Inbox displays all received messages that are stored on the router while Sent Items displays all sent messages.



Figure 109 - SMS Inbox

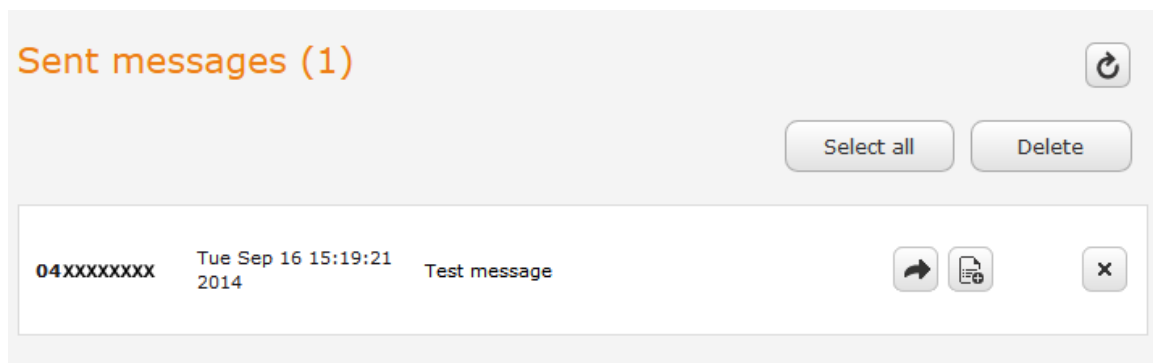


Figure 110 - SMS Outbox






ICON	DESCRIPTION
	Forward button. Click this button to open a new message window where you can forward the corresponding message to another recipient.
	Reply button. Click this button to open a new message window where you can reply to the sender.
	Add to White list. Click this button to add the sender's mobile number to the white list on the router.
	Delete button. Click this button to delete the corresponding message.
	Refresh button. Click this button to refresh the inbox or outbox to see new messages.

Table 27 - Inbox/Outbox icons

Diagnostics

The Diagnostics page is used to configure the SMS diagnostics and command execution configuration. This allows you to change the configuration, perform functions remotely and check on the status of the router via SMS commands.

To access the Diagnostics page, click on the **Services** menu item then select the **SMS** menu on the left and finally select **Diagnostics** beneath it.

SMS diagnostics and command execution configuration

Enable remote diagnostics and command execution ON OFF

Only accept authenticated SMS messages ON OFF

Send Set command acknowledgement replies ON OFF

Access advanced RDB variables ON OFF

Allow execution of advanced commands ON OFF

Send acknowledgement replies to a fixed number the sender's number

Send command error replies ON OFF

Send error replies to a fixed number the sender's number

Send a maximum number of replies per
0 / 100 messages sent

Limit the number of diagnostic text messages that can be sent in a designated time period. Currently, the 'messages sent' count automatically resets at the end of the designated time period. For example, it will reset to zero at 01:00, 02:00, 03:00 etc for 'hour', 00:00 for 'day', 00:00 on Monday for 'week' and the first day of the month for 'month', or at anytime the unit reboots.

White list for diagnostic or execution SMS

All incoming diagnostic or execution text messages are checked against this white list. If the message sender and password don't match any destination numbers and passwords in this white list, the message is ignored and an error message reply is sent to the sender or to a predefined destination. You can add up to 20 destination numbers via the SMS inbox/outbox pages by clicking on 'Add white list'. Alternatively, click on 'Add' below to add a number now.

The white list is empty

Figure 111 - SMS diagnostics and command execution configuration

SMS diagnostics and command execution configuration

The options on this page are described below.

Enable remote diagnostics and command execution

Enables or disables the remote diagnostics feature. If this setting is enabled all incoming text messages are parsed and tested for remote diagnostics commands.

If remote diagnostics commands are found, the router executes those commands. This feature is enabled by default. All remote diagnostic commands that are received are stored in the Inbox.



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



We highly recommended that you use the white list and a password when utilising this feature to prevent unauthorised access. See the [White list](#) description for more information.

Only accept authenticated SMS messages

Enables or disables checking the sender's phone number against the allowed sender white list for incoming diagnostics and 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 (if configured) in the incoming message against the password in the white list for the corresponding sending number. If they match, the diagnostic or command is executed.

If the number does not exist in the white list or the password does not match, the router does not execute the incoming diagnostic or command in the SMS message.

This is enabled by default and it is strongly advised that you leave this feature enabled to maintain security.

Send Set command acknowledgement replies

The NTC-40WV router will automatically reply to certain types of commands received, such as *get* commands, or *execute* commands. However acknowledgement replies from the NTC-40WV router are optional with *set* commands and the *Wakeup* command. This option Enables or disables sending an acknowledgment message after execution of a *set* command or SMS Wakeup command. If disabled, the router does not send any acknowledgment after execution of a *set* command or SMS Wakeup command. All acknowledgment replies are stored in the Outbox after they have been sent. This can be useful to determine if a command was received and executed by the router. This option is disabled by default.

Access advanced RDB variables

By default, this option is turned off and only allows access to the [basic RDB variables](#) listed later in this guide. If this option is enabled, you are able to access the full list of RDB variables via SMS.

Allow execution of advanced commands

By default, this option is turned off and only allows execution of the [basic commands](#) listed later in this guide. If this option is enabled, you are able to execute advanced commands such as those which are common to the Linux command line. For example: "execute ls /usr/bin/sms*" to list the contents of the /etc folder on the router.

Send acknowledgement replies to

This option allows you to specify where to send acknowledgment messages after the execution of a *set*, *get*, or *exec* command.

If a **fixed number** is selected, the acknowledgement message will be sent to the number defined in the **Fixed number to send replies** to field. If **the sender's number** is selected, the acknowledgement message will be sent to the number that the SMS diagnostic or command message originated from. The default setting is to use **the sender's number**.

Fixed number to send replies to

This field defines the destination number to which error messages are sent after the execution of a *get*, *set*, or *exec* command. This field is only displayed when **Send Error SMS to** is set to **Fixed Number**.

Send command error replies

Enables or disables the sending of an error message resulting from the execution of a *get*, *set*, or *exec* command. All error replies are stored in the Outbox after they have been sent.

Send error replies to

When **Send Error SMS for Get/Set/Exec Command** is set to **ON**, this option is used to specify where the error SMS is sent. Use the radio buttons to select either **Fixed Number** or **SMS Sender Number**. When set to **SMS Sender Number** the router will reply to the originating number of the SMS diagnostic or command. When set to **Fixed Number** the router will send the error messages to the number specified in the following field.

Send a maximum number of

You can set the maximum number of acknowledgement and error messages sent when an SMS diagnostic or command is executed. The maximum limit can be set per hour, day, week or month. The router will send a maximum of 100 replies by default.

The number of messages sent is shown below the options. The total transmitted message count resets after a reboot or at the beginning of the time frame specified.

White List for diagnostic or execution SMS

The white list is a list of mobile numbers that you can create which are considered “friendly” to the router. If **Only accept authenticated SMS messages** is enabled in the diagnostics section, the router will compare the mobile number of all incoming diagnostic and command messages against this white list to determine whether the diagnostic or command should be executed. You may optionally configure a password for each number to give an additional level of security. When a password is specified for a number, the SMS diagnostic or command message is parsed for the password and will only be executed if the number and password match.

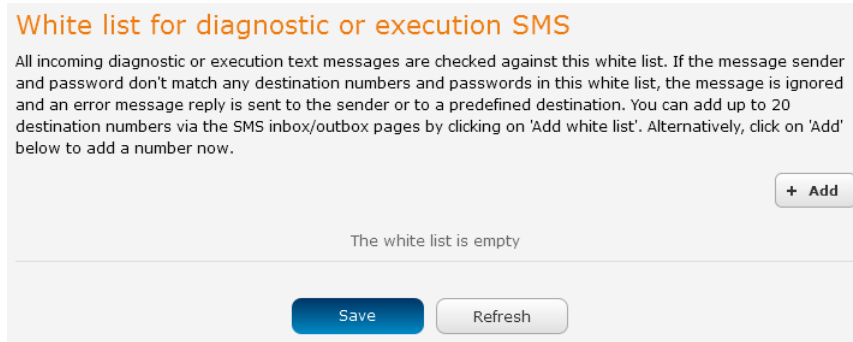


Figure 112 - White list for diagnostic or execution SMS

A maximum of 20 numbers can be stored on the router in the white list. To add a number to the white list, click the “+Add” button.

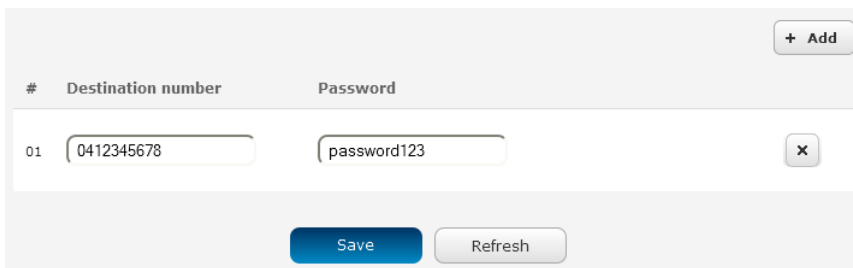




Figure 113 – Adding a number to the SMS white list

The White List numbers and passwords can be cleared by pressing the  button to the right of each entry. To add a number to the white list, enter it in the **Destination number** field and optionally define a password in the **Password** field. When you have finished adding numbers click the **Save** button to save the entries.

Sending an SMS Diagnostic Command

Follow the steps below to configure the router to optionally accept SMS diagnostic commands only from authenticated senders and learn how to send SMS diagnostic commands to the router.

1. Navigate to the **Services > SMS messaging > Diagnostics** page
2. Confirm that the **Enable remote diagnostics and command execution** toggle key is set to the **ON** position. If it is set to **OFF** click the toggle key to switch it to the **ON** position.
3. If you wish to have the router only accept commands from authenticated senders, ensure that **Only accept authenticated SMS messages** is set to the **ON** position. In the **White list for diagnostic or execution SMS messages** section, click the **+Add** button and enter the sender's number in international format into the **Destination number** field that appears. If you wish to also configure a password, enter the password in the **Password** field corresponding to the destination number.
4. If you would prefer to accept SMS diagnostic commands from any sender, set the **Only accept authenticated SMS messages** toggle key to the **OFF** position.




Note: An alternative method of adding a number to the white list is to send an SMS message to the router, navigate to **Services > SMS messaging > Inbox** and then click the  button next to the message which corresponds to the sender's number.






5. Click the **Save** button.

Types of SMS diagnostic commands




There are three types of commands that can be sent; **execute**, **get** and **set**. The basic syntax is as follows:

-  execute COMMAND
-  get VARIABLE
-  set VARIABLE=VALUE

If authentication is enabled, each command must be preceded by the password:

-  PASSWORD execute COMMAND
-  PASSWORD get VARIABLE
-  PASSWORD set VARIABLE=VALUE

The following are some examples of SMS diagnostic commands:

-  password6657 execute reboot
-  get rssi
-  set apn1=testAPNvalue

SMS acknowledgment replies

The router automatically replies to **get** commands with a value and **execute** commands with either a success or error response. **Set** commands will only be responded to if the **Send Set command acknowledgement replies** toggle key is set to **ON**. If the **Send command error replies** toggle key is set to **ON**, the router will send a reply if the command is correct but a variable or value is incorrect, for example, due to misspelling.

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:

Execute COMMAND

PASSWORD execute COMMAND

Replies

Upon receipt of a 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 28 - 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”



Note: Commands, variables and values are case sensitive.

List of basic commands

A list of basic commands which can be used in conjunction with the execute command are listed below:

“pdpcycle”, “pdpdown” and “pdpup” commands can have a profile number suffix ‘x’ added. Without the suffix specified, the command operates against the default profile configured on the profile list page of the Web-UI.

#	COMMAND NAME	DESCRIPTION
1	reboot	Immediately performs a soft reboot.
2	pdpcycle	Disconnects (if connected) and reconnects the data 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	Disconnects the PDP. If a profile number is selected in the command, the router tries 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	Reconnects the PDP. If a profile number is selected in the command, the router tries to connect with the specified profile. If no profile number is selected, the router tries to connect to the last active profile. The gateway will check the currently activated profile and disconnect this profile before executing the command. The router reports an error if no profile number is selected and there is no stored last active profile number.
5	factorydefaults	Performs a factory reset on the router. Be aware that this command also clears the SMS white list on the router.
6	download	<p>Performs a download and install of a Firmware Upgrade (.cdi), Config File (.tar.gz) or a help document (.pdf) file.</p> <p>If the file is a firmware image as in the case of a .cdi file, the router will apply the recovery image first and then the main firmware image. The download location is specified immediately after the command and may be from an HTTP or FTP source URL.</p> <p>If the file is a .tar.gz file, the router will apply the file as a configuration file update for the device and reboot afterwards.</p> <p>If the file is a .pdf, the router will assume this is a user guide document and save it to the router and make the file available for viewing via the help menu on the Web-UI.</p> <p>Note: If your download URL includes any space characters, please encode these prior to transmission according to RFC1738, for example: ftp://username:password@serveraddress/directory%20with%20spaces/filename.cdi</p> <p>Note:</p> <ul style="list-style-type: none"> The execute download command currently does not work with backups that have password protection. Authenticated FTP addresses may be used following the format as defined in RFC1738, for example: ftp://username:password@serveraddress/directory/filename.cdi
7	ssh.genkeys	Instructs the router to generate new public SSH keys.
8	ssh.clearkeys	Instructs the router to clear the client public SSH key files.

Table 29 - List of basic SMS diagnostic commands

List of get/set commands

The following table is a partial list of get and set commands which may be performed via SMS.

COMMAND NAME	EXAMPLE	DESCRIPTION
get status	get status	Returns the Module firmware version, LAN IP Address, Network State, Network operator and RSSI.
get sessionhistory	get sessionhistory	Returns the time and date of recent sessions along with the total amount of data sent and received for each session.
set syslogserver	set syslogserver=123.45.67.89:514	Sets a remote syslog server IP or hostname and port.
get plmnscan	get plmnscan	Instructs the router to perform a network scan and returns the results by SMS.
set forceplmn	set forceplmn=505,3	Sets the operator to a manual selection made by the user where "505" is the Mobile Country Code for Australia and "3" is the Mobile Network Code for Vodafone. As no network type (i.e. 3G or 2G) is specified, it is selected automatically.
get forceplmn	get forceplmn	Returns the operator and network type selection mode (Automatic/Manual), in addition to the MCC and MNC values
get pppoe	get pppoe	Returns the PPPoE status, currently configured dial string and service name
set pppoe	set pppoe=1, telstra.internet, test	Sets the PPPoE status on, APN to telstra.internet, and service name to test.
get ledmode	get ledmode	Returns the status of the LED operation mode.
set ledmode	set ledmode=10	Sets the LED operation mode to be always on or to turn off after the specified number of minutes.
get ssh.proto	get ssh.proto	Returns the SSH protocol in use.
set ssh.proto	set ssh.proto=1,2	Sets the SSH Protocol to protocol 1, 2 or both (1,2).
get ssh.passauth	get ssh.passauth	Returns the status of the SSH Enable password authentication option.
set ssh.passauth	set ssh.passauth=1	Sets the SSH Enable password authentication option on or off.
get.ssh.keyauth	get.ssh.keyauth	Returns the status of the SSH Enable key authentication option.
set.ssh.keyauth	set.ssh.keyauth=1	Sets the SSH Enable key authentication option on or off.
get download.timeout	get download.timeout	Returns the time in minutes that the router waits before a download times out.
set download.timeout	set download.timeout=20	Sets the time in minutes that the router waits before a download times out. This is set to 10 minutes by default. Supported range is 10 – 1440 minutes.
get install.timeout	get install.timeout	Returns the time in minutes that the router waits before a file that is being installed times out.
set install.timeout	set install.timeout=5	Sets the time in minutes that the router waits before a file that is being installed times out. This is set to 3 minutes by default. Supported range is 3 – 300 minutes.

Table 30 - List of get/set commands

List of basic RDB variables

The following table lists valid variables where "x" is a profile number (1-6). If no profile is specified, variables are read from or written to for the current active profile. If a profile is specified, variables are read from or written to for the specified profile number ('x').

#	RDB VARIABLE NAME	SMS VARIABLE NAME	READ/ WRITE	DESCRIPTION	EXAMPLE VALUE
0	link.profile.1.enable link.profile.1.apn link.profile.1.user link.profile.1.pass link.profile.1.auth_type link.profile.1.iplocal link.profile.1.status	profile	RW	Profile	Read: (profile no,apn,user,pass,auth,iplocal,status) 1,apn,username,password, chap,202.44.185.111,up Write: (apn, user, pass,auth) apn,username,password
2	link.profile.1.user	username	RW	3G username	Guest, could also return "null"
3	link.profile.1.pass	password	RW	3G password	Guest, could also return "null"
4	link.profile.1.auth_type	authtype	RW	3G Authentication type	"pap" or "chap"
5	link.profile.1.iplocal	wanip	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	357347050000177
8	statistics.usage_current	usage	R	3G data usage of current session	"Rx 500 bytes, Tx 1024 bytes, Total 1524 bytes" or "Rx 0 byte, Tx 0 byte, Total 0 byte" when wwan down
9	statistics.usage_current	wanuptime	R	Up time of current 3G session	1 days 02:30:12 or 0 days 00:00:00 when wwan down
10	/proc/uptime	deviceuptime	R	Device up time	1 days 02:30:12
11	wwan.0.system_network_status.current_band	band	R	Current band	WCDMA850

Table 31 - List of basic SMS diagnostics RDB variables

Network scan and manual network selection by SMS

Performing a network scan

The **get plmnscan** SMS command enables you to perform a scan of the cellular networks available at the time of the scan.

It returns the following semi-colon separated information for each network in range:

- MCC
- MNC
- Network Type (3G, 2G)
- Provider's Name
- Operator Status (available, forbidden, current)

The following is an example of a response from the **get plmnscan** SMS command:

```
plmnscan:505,3,7,vodafone AU,4;505,3,1,vodafone AU,1;505,2,7,YES OPTUS,1;505,2,1,YES OPTUS,1;505,1,1,Telstra Mobile,1;505,1,7,Telstra Mobile,1
```

NETWORK TYPE	DESCRIPTION
7	Indicates a 3G network
1	Indicates a 2G network

Table 32 - Network types returned by get plmnscan SMS command

OPERATOR STATUS	DESCRIPTION
1	Indicates an available operator which may be selected.
2	Indicates a forbidden operator which may not be selected (applies only to generic SIM cards).
4	Indicates the currently selected operator.

Table 33 - Operator status codes returned by get plmnscan SMS command



Notes about the network connection status when using the **get plmnscan** command:

- If the connection status is **Up** and connection mode is **Always on**, the **get plmnscan** SMS will cause the connection to disconnect, perform the scan, send the result through SMS and then bring the connection back up again. If the connection status is **Down**, the router will perform the PLMN scan, send the result and keep the connection status down.
- If the connection status is **Waiting** and connection mode is **Connect on demand**, the **get plmnscan** SMS will change the connection status to **Down**, perform the scan, send the result through SMS and then restore the connection status to the **Waiting** state.
- If the connection status is **Up** and connection mode is **Connect on demand**, the **get plmnscan** SMS will cause the connection to disconnect, perform the scan, send the result through SMS, and then restore the connection status to the **Waiting** state unless there is a traffic which triggers a connection in which case the connection status will be set to **Up**.

Setting the router to connect to a network

The router can be instructed by SMS to connect to one of the networks returned by the **get plmnscan** command. The **set forceplmn** command forces the router to connect to a specified operator network (if available) while the **get forceplmn** command retrieves the currently configured network on the router.

Command format:

```
set forceplmn=0|MCC,MNC| MCC,MNC,Network Type
```

For example:

```
set forceplmn=0
```

Sets the selection of operator and network type to automatic mode.

```
set forceplmn=505,3
```

Sets the operator to a manual selection made by the user where “505” is the Mobile Country Code for Australia and “3” is the Mobile Network Code for Vodafone. As no network type (i.e. 3G or 2G) is specified, it is selected automatically.

```
set forceplmn=505,3,7
```

Sets the operator and network type to a manual selection made by the user where “505” is the Mobile Country Code for Australia, “3” is the Mobile Network Code for Vodafone and “7” is the 3G network type.



Notes about the **set forceplmn** command:

1. If the manual selection fails, the device will fall back to the previous ‘good’ network.
2. When enabled, the SMS acknowledgement reply reflects the success or failure of the manual selection with respect to the *set* command and includes the final MNC/MCC that was configured.

Confirming the currently configured operator and network type

You can retrieve the currently configured operator and network type using the **get forceplmn** command.

The **get forceplmn** command returns the operator and network type selection mode (Automatic/Manual), in addition to the MCC and MNC values, for example:

```
Automatic,505,3
```

This response indicates that the operator/network selection mode is Automatic, and the network used is Vodafone AU.

SMS diagnostics examples

The examples below demonstrate various combinations of supported commands. This is not an exhaustive list and serves as an example of possibilities only.

DESCRIPTION	AUTHENTICATION	INPUT EXAMPLE
Send SMS to change the data connection username	Not required	set username='NetComm'
	Required	PASSWORD set username= "NetComm"
Send SMS to change the data connection password	Not required	set password= `NetComm`
	Required	PASSWORD set password= `NetComm`
Send SMS to change the data connection authentication	Not required	set authtype= 'pap'
	Required	PASSWORD set authtype = pap
Send SMS to reboot	Not required	execute reboot
	Required	PASSWORD execute reboot
Send SMS to check the WAN IP address	Not required	get wanip
	Required	PASSWORD get wanip
Send SMS to check the mobile signal strength	Not required	get rssi
	Required	PASSWORD get rssi
Send SMS to check the IMEI number	Not required	get imei
	Required	PASSWORD get imei

Send SMS to check the current band	Not required	get band
	Required	PASSWORD get band
Send SMS to Disconnect (if connected) and reconnect the data connection	Not required	execute pdpcycle
	Required	PASSWORD execute pdpcycle
Send SMS to disconnect the data connection	Not required	execute pdpdown
	Required	PASSWORD execute pdpdown
Send SMS to connect the data connection	Not required	execute pdpup
	Required	PASSWORD execute pdpup
Send multiple get command	Not required	get wanip; get rssi
	Required	PASSWORD get wanip; get rssi
Send multiple set command	Not required	set ssh.genkeys=1; set username=test; set auth=pap
	Required	PASSWORD set ssh.genkeys=1; set username=test; set auth=pap
Send SMS to reset to factory default settings	Not required	execute factorydefaults
	Required	PASSWORD execute factorydefaults
Send SMS to retrieve status of router	Not required	get status
	Required	PASSWORD get status
Send SMS to retrieve the history of the session, including start time, end time and total data usage	Not required	get sessionhistory
	Required	PASSWORD get sessionhistory
Send SMS to configure the router to send syslog to a remote syslog server	Not required	set syslogserver=123.209.56.78
	Required	PASSWORD set syslogserver=123.209.56.78
Send SMS to wake up the router, turn on the default gateway and trigger the 'connect on demand' profile if in waiting state.	Not required	execute wakeup
	Required	PASSWORD execute wakeup
Send SMS to perform firmware upgrade when firmware is located on HTTP server	Not required	execute download http://download.com:8080/firmware_image.cdi execute download http://download.com:8080/firmware_image_r.cdi
	Required	PASSWORD execute download http://download.com:8080/firmware_image.cdi PASSWORD execute download http://download.com:8080/firmware_image_r.cdi
Send SMS to perform firmware upgrade when firmware is located on FTP server	Not required	execute download ftp://username:password@download.com/firmware_image.cdi execute download ftp://username:password@download.com/firmware_image_r.cdi
	Required	PASSWORD execute download ftp://username:password@download.com/firmware_image.cdi PASSWORD execute download ftp://username:password@download.com/firmware_image_r.cdi
Send SMS to download and install IPK package located on HTTP server	Not required	execute download http://download.com:8080/package.ipk
	Required	PASSWORD execute download http://download.com:8080/package.ipk
Send SMS to download and install IPK package located on FTP server	Not required	execute download ftp://username:password@download.com:8080/package.ipk
	Required	PASSWORD execute download ftp://username:password@download.com:8080/package.ipk
Send SMS to turn off PPPoE	Not required	set pppoe=0
	Required	PASSWORD set pppoe=0
Send SMS to retrieve the PPPoE status, currently configured dial string and service name	Not required	get pppoe
	Required	PASSWORD get pppoe
Send SMS to set the LED mode timeout to 10 minutes	Not required	set ledmode=10
	Required	PASSWORD set ledmode=10
Send SMS to retrieve the current LED mode	Not required	get ledmode
	Required	PASSWORD get ledmode
Retrieve current SSH protocol	Not required	get ssh.proto

	Required	PASSWORD get ssh.proto
Select SSH protocol	Not required	set ssh.proto=1
	Required	PASSWORD set ssh.proto=1
Retrieve password authentication status	Not required	get ssh.passauth
	Required	PASSWORD get.ssh.passauth
Enable/disable password authentication on host	Not required	set ssh.passauth=1 or set ssh.passauth=0
	Required	PASSWORD set ssh.passauth=1 or PASSWORD set ssh.passauth=0
Generate set of public/private keys on the host	Not required	execute ssh.genkeys
	Required	PASSWORD execute ssh.genkeys
Clear client public keys stored on host	Not required	execute ssh.clearkeys
	Required	PASSWORD execute ssh.clearkeys

Table 34 - SMS diagnostics example commands

System

The Log pages are used to display or download the System log, IPSec log, and Event notification logs on the router.

System log

The System Log enables you to troubleshoot any issues you may be experiencing with your NTC-40WW router. To access the System Log page, click on the **System** menu. The System Log is displayed.

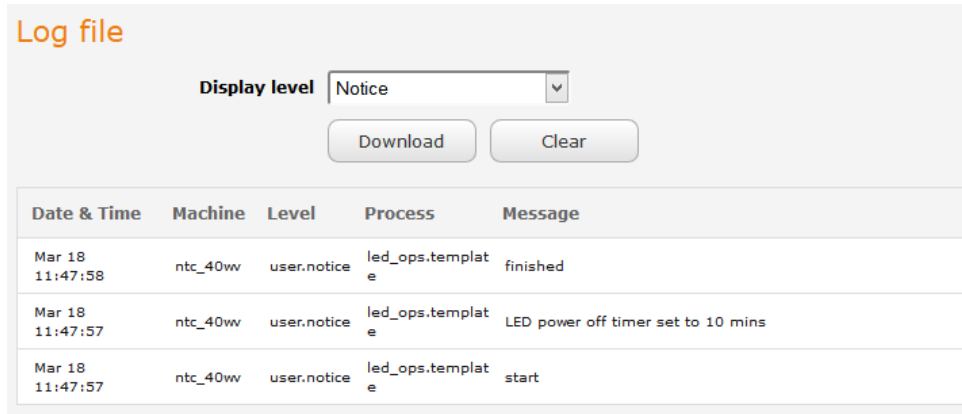


Figure 114 - System log file

Log file

Use the **Display level** drop-down list to select a message level to be displayed. The message levels are described in the table below.

To download the System log for offline viewing, right-click the **Download** button and choose **Save as..** to save the file. To clear the System log, click the **Clear** button. The downloaded log file is in Linux text format with carriage return (CR) only at the end of a line, therefore in order to be displayed correctly with new lines shown, it is recommended to use a text file viewer which displays this format correctly (e.g. Notepad++).

IPSec log

The IPSec log section provides the ability for you to download the log for the IPSec VPN function. This can assist in troubleshooting any problems you may have with the IPSec VPN.

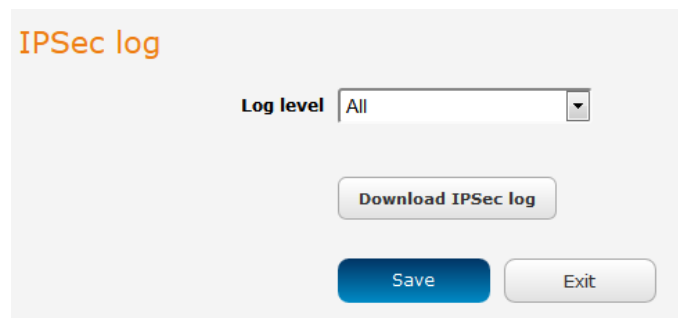


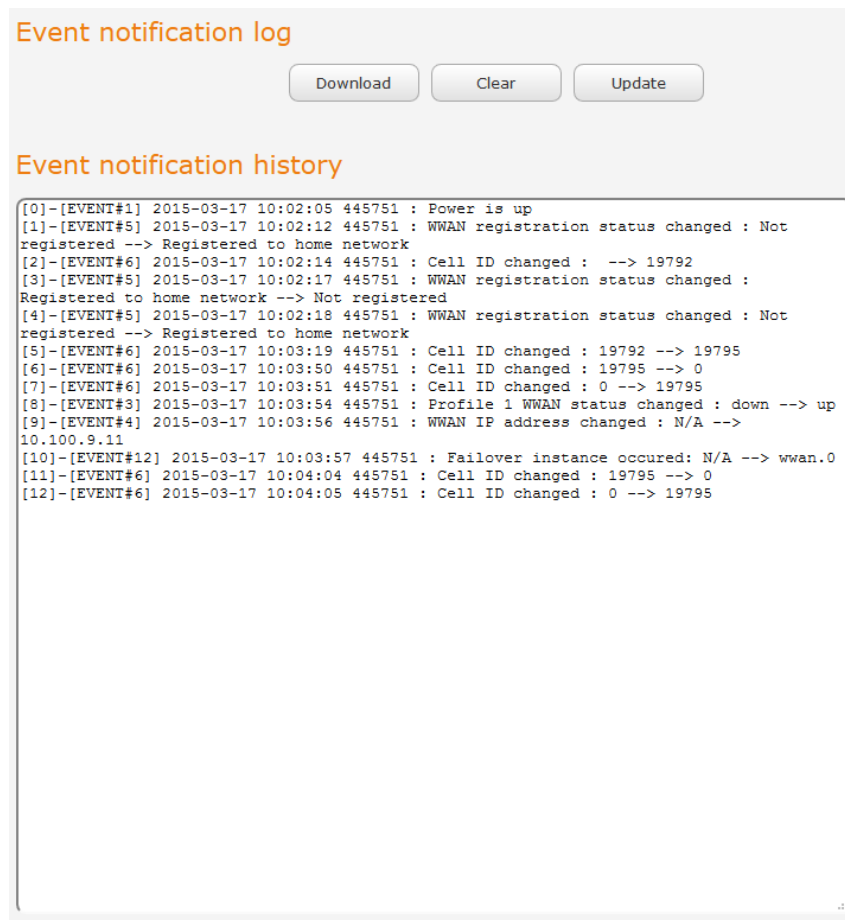
Figure 115 - IPSec log

Use the **Log level** drop down list to specify the type of detail you want to capture in the log and then click the **Save** button. When you change the logging level, any active IPSec VPN tunnels will be disconnected as a change in logging level requires the IPSec service to be restarted.

To download the IPSec log, click the **Download IPSec log** button and you will be prompted to save the file.

Event notification log

The Event notification log section provides the ability for you to download the log for the Event notification function. This can assist in troubleshooting any problems you may have with the Event notification feature.



Event notification log

Download Clear Update

Event notification history

```
[0]-[EVENT#1] 2015-03-17 10:02:05 445751 : Power is up
[1]-[EVENT#5] 2015-03-17 10:02:12 445751 : WWAN registration status changed : Not
registered --> Registered to home network
[2]-[EVENT#6] 2015-03-17 10:02:14 445751 : Cell ID changed : --> 19792
[3]-[EVENT#5] 2015-03-17 10:02:17 445751 : WWAN registration status changed :
Registered to home network --> Not registered
[4]-[EVENT#5] 2015-03-17 10:02:18 445751 : WWAN registration status changed : Not
registered --> Registered to home network
[5]-[EVENT#6] 2015-03-17 10:03:19 445751 : Cell ID changed : 19792 --> 19795
[6]-[EVENT#6] 2015-03-17 10:03:50 445751 : Cell ID changed : 19795 --> 0
[7]-[EVENT#6] 2015-03-17 10:03:51 445751 : Cell ID changed : 0 --> 19795
[8]-[EVENT#3] 2015-03-17 10:03:54 445751 : Profile 1 WWAN status changed : down --> up
[9]-[EVENT#4] 2015-03-17 10:03:56 445751 : WWAN IP address changed : N/A -->
10.100.9.11
[10]-[EVENT#12] 2015-03-17 10:03:57 445751 : Failover instance occurred: N/A --> wwan.0
[11]-[EVENT#6] 2015-03-17 10:04:04 445751 : Cell ID changed : 19795 --> 0
[12]-[EVENT#6] 2015-03-17 10:04:05 445751 : Cell ID changed : 0 --> 19795
```

Figure 116 - Event notification log

Use the **Download event notification history** button to download the log file. The **Update event notification history** button forces a refresh of the log display.

System log settings

To access the System log settings page, click on the **System** menu item then select the **Log** menu on the left and finally select **System log settings** beneath it.

Log data is stored in RAM and therefore, when the unit loses power or is rebooted, it will lose any log information stored in RAM. To ensure that log information is accessible between reboots of the router there are two options:

1. Enable the **Log to non-volatile memory** option
2. Use a remote syslog server

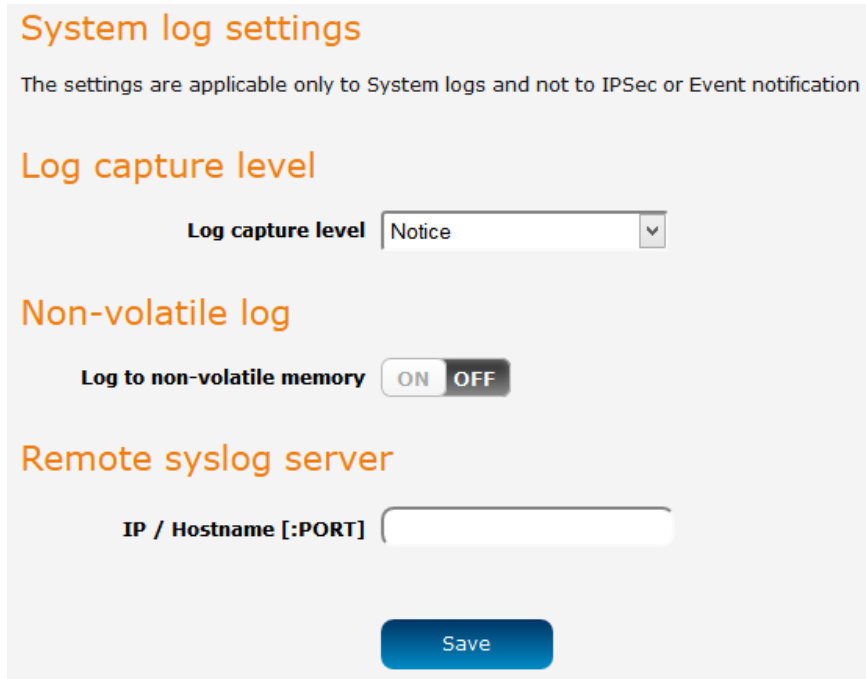


Figure 117 - System log settings

Non-volatile log

When the router is configured to log to non-volatile memory, the log data is stored in flash memory, making it accessible after a reboot of the router. Up to 512kb of log data will be stored before it is overwritten by new log data. Flash memory has a finite number of program-erase operations that it may perform to the blocks of memory. While this number of program-erase operations is quite large, we recommend that you do not enable this option for anything other than debugging to avoid excessive wear on the memory.

Log capture level

The log capture level defines the amount of detail that the system log stores. This setting also affects the Display level setting on the System log page, for example, if this is set to a low level, such as “Error”, the System log will not be able to display higher log levels.

Remote syslog server

The router can be configured to output log data to a remote syslog server. This is an application running on a remote computer which accepts and displays the log data. Most syslog servers can also save the log data to a file on the computer on which it is running allowing you to ensure that no log data is lost between reboots.

To configure the NTC-40WV router to output log data to a remote syslog server:

3. Click on the **System** menu from the top menu bar. The System log item is displayed.
4. Under the **Remote syslog server** section, enter the IP address or hostname of the syslog server in the **IP / Hostname [PORT]** field. You can also specify the port number after the IP or hostname by entering a semi-colon and then the port number e.g. 192.168.1.102:514. If you do not specify a port number, the router will use the default UDP port 514.
5. Click the **Save** button to save the configuration.

Remote syslog server

IP / Hostname [[:PORT]]

Save

Figure 118 – Remote syslog server configuration

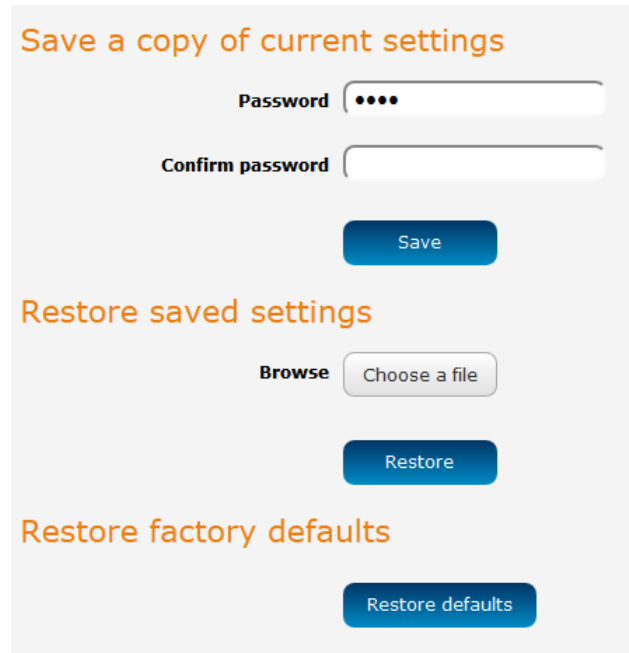
ITEM	DEFINITION
Debug	Show extended system log messages with full debugging level details.
Info	Show informational messages only.
Notice	Show normal system logging information.
Error	Show error condition messages only.

Table 35 - System log detail levels

System configuration

Settings backup and restore

The settings backup and restore page is used to backup or restore the router's configuration or to reset it to factory defaults. In order to view the settings page you must be logged into the web user interface as **root** using the password **admin**. The backup / restore functions can be used to easily configure a large number of NTC-40WV router by configuring one router with your desired settings, backing them up to a file and then restoring that file to multiple NTC-40WV routers.



Save a copy of current settings

Password

Confirm password

Save

Restore saved settings

Browse

Restore

Restore factory defaults

Restore defaults

Figure 119 – Settings backup and restore

Back up your router's configuration

Log in to the web configuration interface, click on the **System** menu and select **Settings backup and restore**.

If you want to password protect your backup configuration files, enter your password in the fields under **Save a copy of current settings** and click on **Save**. If you don't want to password protect your files, just click on **Save**. The router will then prompt you to select a location to save the settings file.



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 as “.cfg”

Restore your backup configuration

1. In the web configuration interface click on the **System** menu and select **Settings backup and restore**.
2. From the **Restore saved settings** section, click on **Browse** or **Choose a file** and select the backup configuration file on your computer.
3. Click **Restore** to copy the settings to the new NTC-40WV router. The router will apply these settings and inform you it will reboot - click on **OK**.

Restoring the router's factory default configuration

Click the **Restore defaults** button to restore the factory default configuration. The router asks you to confirm that you wish to restore factory default settings. If you wish to continue with the restoring of factory defaults, click **OK**.



Note: All current settings on the router will be lost when performing a restore of factory default settings. The device IP address will change to 192.168.1.1 and the default username **root** and default password **admin** will be configured.

Upload

To access the Upload page, click on the **System** menu, then **System Configuration** and then **Upload**.

The Upload page allows you to upload firmware files, HTTPS certificates or user created application packages to the NTC-40WV router. When firmware files have been uploaded, they can also be installed from this page. PDF files, such as this user guide may also be uploaded for access on the router's help page.

For more information on application development, contact NetComm Wireless about our Software Development Kit.

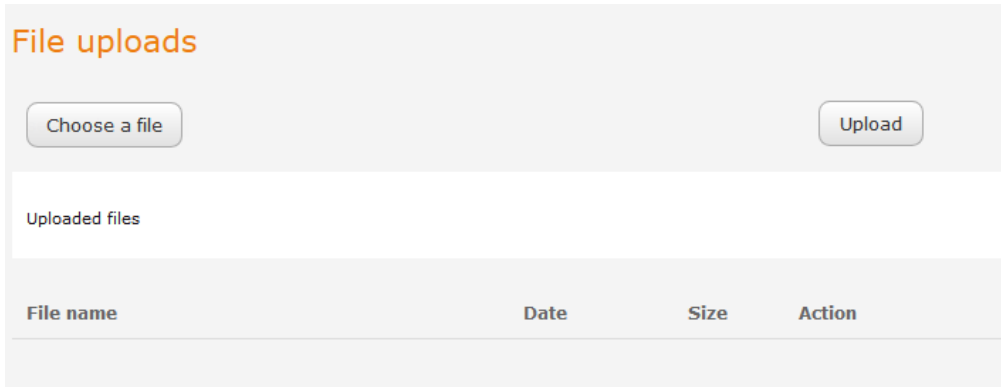


Figure 120 - Upload page

Updating the Firmware

The firmware update process involves first updating the recovery image firmware and then updating the main firmware image.



Note: In order to perform an update, you must be logged into the router with the root manager account (see the [Advanced configuration](#) section for more details).

To update the NTC-40WV router's firmware:

1. Power on the router as described in the [Installing the router](#) section.
2. Log in to the router with the root user account (See the [Advanced configuration](#) section for details)
3. Select the **System** item from the top menu bar, select the **System configuration** item from the menu on the left and then select the **Upload** menu item.
4. Under the **File uploads** section, click the **Choose a file** button. Locate the recovery firmware image file on your computer and click **Open**. The recovery image is named **ntc_40wv_x.x.x.x_r.cdi** while the main system firmware image is named **ntc_40wv_x.x.x.x.cdi**.
5. Click the **Upload** button. The firmware image is uploaded to the storage on the router.

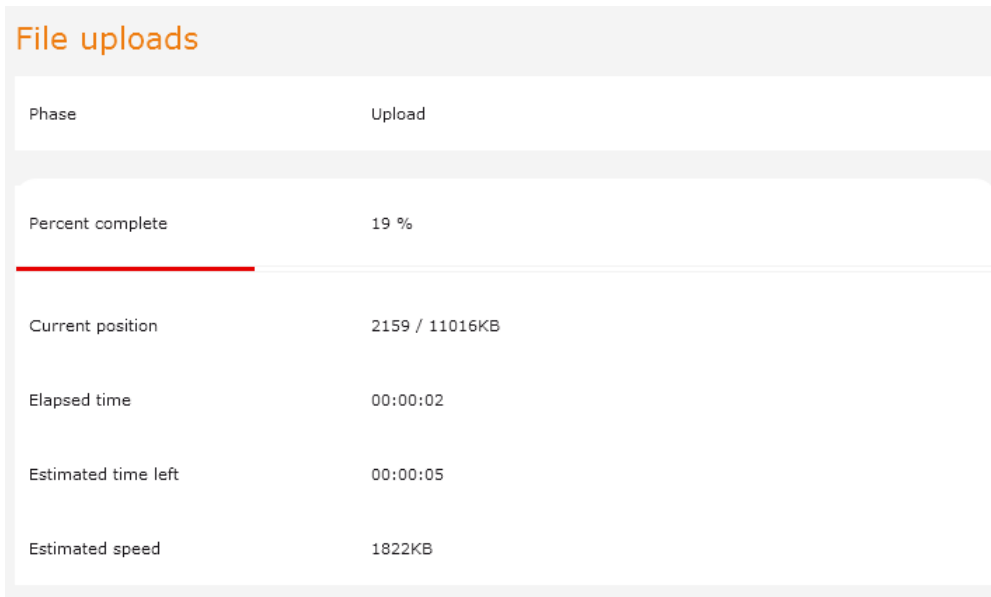


Figure 121 - File upload

- Repeat steps 4 and 5 for the main system firmware image.
- The uploaded firmware images are listed in the **Uploaded files** section. Click the **Install** link next to the recovery image to begin installing the recovery firmware image and then click **OK** on the confirmation window that appears.

File name	Date	Size	Action
ntc_40wv_2.0.0.2.cdi	Jan 22 2014	24.4M	Install Delete
ntc_40wv_2.0.0.2_r.cdi	Jan 22 2014	11.0M	Install Delete
u-boot.bin	Jan 15 2014	247.3K	Install Delete

Figure 122 - Uploaded files

- The recovery firmware image is flashed and when it is complete, the router displays “The firmware update was successful” and returns to the main Upload screen.

```
Erasing 128 Kibyte @ b20000 -- 92 % complete.
Erasing 128 Kibyte @ b40000 -- 93 % complete.
Erasing 128 Kibyte @ b60000 -- 94 % complete.
Erasing 128 Kibyte @ b80000 -- 95 % complete.
Erasing 128 Kibyte @ ba0000 -- 96 % complete.
Erasing 128 Kibyte @ bc0000 -- 97 % complete.
Erasing 128 Kibyte @ be0000 -- 98 % complete.
Erasing 128 Kibyte @ c00000 -- 100 % complete.
Flashing root_r.ubi to "rfs" (/dev/mtd2)
Writing data to block 55 at offset 0x6e0000
Writing data to block 56 at offset 0x700000
Writing data to block 57 at offset 0x720000
Writing data to block 58 at offset 0x740000
Writing data to block 59 at offset 0x760000
Writing data to block 60 at offset 0x780000
Writing data to block 61 at offset 0x7a0000
Done
Done
Done
The firmware update was successful
```

Close

Figure 123 - Recovery firmware flash process

- Click the **Install** link to the right of the main firmware image you uploaded and then click **OK** to confirm that you want to continue with the installation.



Note: Do not remove the power when the router's LEDs are flashing as this is when the firmware update is in process.

- The installation is complete when the countdown reaches zero. The router attempts to redirect you to the Status page.

```
Writing data to block 190 at offset 0x17c0000
Writing data to block 191 at offset 0x17e0000
Writing data to block 192 at offset 0x1800000
Writing data to block 193 at offset 0x1820000
Writing data to block 194 at offset 0x1840000
Done
Done
Done
The firmware update was successful Reboot to main system...
Estimated time remaining: 47 seconds
Estimated time remaining: 42 seconds
Estimated time remaining: 37 seconds
Estimated time remaining: 32 seconds
Estimated time remaining: 27 seconds
Estimated time remaining: 22 seconds
Estimated time remaining: 17 seconds
Estimated time remaining: 12 seconds
Estimated time remaining: 7 seconds
Estimated time remaining: 2 seconds
Redirecting you to the Status page...
```

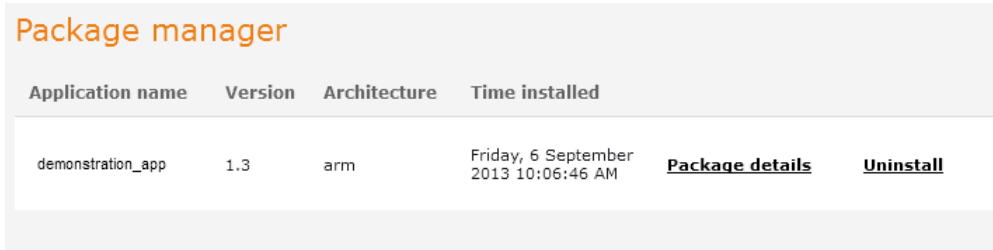
[Close](#)

Figure 124 -- Installing main firmware image

- Hold down the reset button on the router for more than 15 seconds (when all LEDs stop flashing) to reboot and restore the factory default settings of the router. See the [Restoring factory default settings](#) section for more information.

Package manager

The Package Manager page is used to provide details of any user installed packages on the router and allow them to be uninstalled. For more information on application development, contact NetComm Wireless about our Software Development Kit.



Application name	Version	Architecture	Time installed		
demonstration_app	1.3	arm	Friday, 6 September 2013 10:06:46 AM	Package details	Uninstall

Figure 125 – Software applications manager

The Application name, Version number of the application, the architecture type and time of installation are all displayed. Clicking the [Package details](#) link will display a pop-up window with further details of the package.

To uninstall any software applications, click the [Uninstall](#) link.

Administration

Administration settings

To access the Administration Settings page, click on the **System** menu then the **Administration** menu on the left and then click on **Administration Settings**.

The Administration settings page is used to enable or disable protocols used for remote access and configure the passwords for the user accounts used to log in to the router.



Remote router access control

Enable HTTP ON OFF

HTTP management port (Choose a port between 1 and 65534)

Enable HTTPS ON OFF

Remote HTTPS access port (Choose a port between 1 and 65534)

Enable telnet ON OFF

Enable SSH ON OFF

Remote SSH access port (Choose a port between 1 and 65534)

Enable ping ON OFF

Local router access control

Enable local Telnet ON OFF

Enable local SSH ON OFF

Web User Interface account

Username

Password

Confirm password

Telnet/SSH account

Username root

Password (1-126 characters in length)

Confirm password (1-126 characters in length)

Figure 126 - Administration page

OPTION	DEFINITION
Remote router access control	
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.
HTTP management port	Enter a port number between 1 and 65534 to use when accessing the router remotely.
Enable HTTPS	Enable or disable remote HTTPS access to the router using a secure connection.
Remote HTTPS access port	Enter a port number between 1 and 65534 to use when accessing the router remotely over a secure HTTPS connection.
Enable Telnet	Enable or disable remote telnet (command line) access to the router.
Enable SSH	Enable or disable Secure Shell on the router.
Remote SSH Access Port	Enter the port number for remote SSH access. Must be a port number between 1 and 65534.
Enable Ping	Enable or disable remote ping responses on the WWAN connection.
Local router access control (Telnet/SSH)	
Web User Interface account	
Username	Use the drop down list to select the root or admin account to change its web user interface password.
Password	Enter the desired web user interface password.
Confirm password	Re-enter the desired web user interface password.
Telnet/SSH account	
Username	Displays the Telnet/SSH.username. This may not be changed.
Password	Enter the desired Telnet/SSH password.
Confirm password	Re-enter the desired Telnet/SSH password.

Table 36 - Administration configuration options

To access the router's configuration pages remotely:

1. Open a new browser window and navigate to the WAN IP address and assigned port number of the router, for example <http://123.209.130.249:8080>



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

2. Enter the username and password to login to the router and click **Log in**.



Note: To perform functions like Firmware upgrade, device configuration backup and to restore and reset the router to factory defaults, you must be logged in with the root manager account.



WARNING: Using an insecure password will result in your device being compromised. Any resulting damage may not be covered under warranty. It is strongly advised that the password not be a dictionary word, nor should the same password be used across fleets of devices.

WARNING: Using an insecure password will result in your device being compromised. Any resulting damage may not be covered under warranty. It is strongly advised that the selected password not be a dictionary word, nor should the same password be used across fleets of devices.

OK Cancel

HTTPS key management

What is HTTP Secure?

HTTP Secure or HTTPS is the use of the HTTP protocol over an SSL/TLS protocol. It is used primarily to protect against eavesdropping of communication between a web browser and the web site to which it is connected. This is especially important when you wish to have a secure connection over a public network such as the internet. HTTPS connections are secured through the use of certificates issued by trusted certificate authorities such as VeriSign. When a web browser makes a connection attempt to a secured web site, a digital certificate is sent to the browser so that it can verify the authenticity of the site using a built-in list of trusted certificate authorities.

There are two main differences between how HTTPS and HTTP connections work:

1. HTTPS uses port 443 while HTTP uses port 80 by default.
2. Over an HTTPS connection, all data sent and received is encrypted with SSL while over an HTTP connection, all data is sent unencrypted.

The encryption is achieved through the use of a pair of public and private keys on both sides of the connection. In cryptography, a key refers to a numerical value used by an algorithm to alter information (encrypt it), making the information secure and visible only to those who have the corresponding key to recover (decrypt) the information. The public key is used to encrypt information and can be distributed freely. The private key is used to decrypt information and must be secret by its owner.

Each NTC-40WW router contains a self-signed digital certificate which is identical on all NTC-40WW routers. For a greater level of security, the router also supports generating your own unique key. Additionally, you may use third party software to generate your own self-signed digital certificate or purchase a signed certificate from a trusted certificate authority and then upload those certificates to the router.

Generating your own self-signed certificate

To generate your own self-signed certificate:

1. Click the **System** item from the top menu bar, then **Administration** from the side menu bar and then **Server certificate**.
2. Select a **Server key size**. A larger key size takes longer to generate but provides better security.
3. Click the **Generate** button to begin generating Diffie-Hellman parameters.
4. Enter the certificate details using the appropriate fields. Each field must be completed in order to generate a certificate.

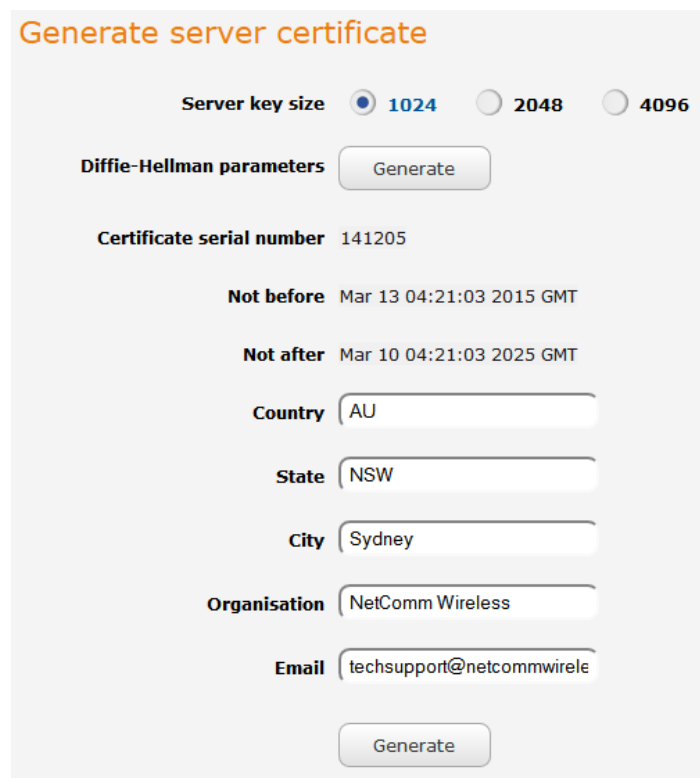


Figure 127 - Generate server certificate



Note: The **Country** field must contain a code for the desired country from the list below.

CODE	COUNTRY	CODE	COUNTRY	CODE	COUNTRY	CODE	COUNTRY
AX	Åland Islands	ER	Eritrea	LS	Lesotho	SA	Saudi Arabia
AD	Andorra	ES	Spain	LT	Lithuania	SB	Solomon Islands
AE	United Arab Emirates	ET	Ethiopia	LU	Luxembourg	SC	Seychelles
AF	Afghanistan	FI	Finland	LV	Latvia	SE	Sweden
AG	Antigua and Barbuda	FJ	Fiji	LY	Libya	SG	Singapore
AI	Anguilla	FK	Falkland Islands (Malvinas)	MA	Morocco	SH	St. Helena
AL	Albania	FM	Micronesia	MC	Monaco	SI	Slovenia
AM	Armenia	FO	Faroe Islands	MD	Moldova	SJ	Svalbard and Jan Mayen
AN	Netherlands Antilles	FR	France	ME	Montenegro	SK	Slovak Republic
AO	Angola	FX	France, Metropolitan	MG	Madagascar	SL	Sierra Leone
AQ	Antarctica	GA	Gabon	MH	Marshall Islands	SM	San Marino
AR	Argentina	GB	Great Britain (UK)	MK	Macedonia	SN	Senegal
AS	American Samoa	GD	Grenada	ML	Mali	SR	Suriname
AT	Austria	GE	Georgia	MM	Myanmar	ST	Sao Tome and Principe
AU	Australia	GF	French Guiana	MN	Mongolia	SU	USSR (former)
AW	Aruba	GG	Guernsey	MO	Macau	SV	El Salvador
AZ	Azerbaijan	GH	Ghana	MP	Northern Mariana	SZ	Swaziland
BA	Bosnia and Herzegovina	GI	Gibraltar	MQ	Martinique	TC	Turks and Caicos Islands
BB	Barbados	GL	Greenland	MR	Mauritania	TD	Chad
BD	Bangladesh	GM	Gambia	MS	Montserrat	TF	French Southern Territories
BE	Belgium	GN	Guinea	MT	Malta	TG	Togo
BF	Burkina Faso	GP	Guadeloupe	MU	Mauritius	TH	Thailand
BG	Bulgaria	GQ	Equatorial Guinea	MV	Maldives	TJ	Tajikistan
BH	Bahrain	GR	Greece	MW	Malawi	TK	Tokelau
BI	Burundi	GS	S. Georgia and S. Sandwich	MX	Mexico	TM	Turkmenistan
BJ	Benin	GT	Guatemala	MY	Malaysia	TN	Tunisia
BM	Bermuda	GU	Guam	MZ	Mozambique	TO	Tonga
BN	Brunei Darussalam	GW	Guinea-Bissau	NA	Namibia	TP	East Timor
BO	Bolivia	GY	Guyana	NC	New Caledonia	TR	Turkey
BR	Brazil	HK	Hong Kong	NE	Niger	TT	Trinidad and Tobago
BS	Bahamas	HM	Heard and McDonald Islands	NF	Norfolk Island	TV	Tuvalu
BT	Bhutan	HN	Honduras	NG	Nigeria	TW	Taiwan
BV	Bouvet Island	HR	Croatia (Hrvatska)	NI	Nicaragua	TZ	Tanzania
BW	Botswana	HT	Haiti	NL	Netherlands	UA	Ukraine
BZ	Belize	HU	Hungary	NO	Norway	UG	Uganda
CA	Canada	ID	Indonesia	NP	Nepal	UM	US Minor Outlying Islands
CC	Cocos (Keeling) Islands	IE	Ireland	NR	Nauru	US	United States
CF	Central African Republic	IL	Israel	NT	Neutral Zone	UY	Uruguay
CH	Switzerland	IM	Isle of Man	NU	Niue	UZ	Uzbekistan
CI	Cote D'Ivoire (Ivory)	IN	India	NZ	New Zealand	VA	Vatican City State (Holy See)
CK	Cook Islands	IO	British Indian Ocean Territory	OM	Oman	VC	Saint Vincent and the
CL	Chile	IS	Iceland	PA	Panama	VE	Venezuela
CM	Cameroon	IT	Italy	PE	Peru	VG	Virgin Islands (British)
CN	China	JE	Jersey	PF	French Polynesia	VI	Virgin Islands (U.S.)
CO	Colombia	JM	Jamaica	PG	Papua New Guinea	VN	Viet Nam
CR	Costa Rica	JO	Jordan	PH	Philippines	VU	Vanuatu
CS	Czechoslovakia (former)	JP	Japan	PK	Pakistan	WF	Wallis and Futuna Islands
CV	Cape Verde	KE	Kenya	PL	Poland	WS	Samoa
CX	Christmas Island	KG	Kyrgyzstan	PM	St. Pierre and	YE	Yemen
CY	Cyprus	KH	Cambodia	PN	Pitcairn	YT	Mayotte
CZ	Czech Republic	KI	Kiribati	PR	Puerto Rico	ZA	South Africa
DE	Germany	KM	Comoros	PS	Palestinian Territory	ZM	Zambia
DJ	Djibouti	KN	Saint Kitts and Nevis	PT	Portugal	COM	US Commercial
DK	Denmark	KR	Korea (South)	PW	Palau	EDU	US Educational
DM	Dominica	KW	Kuwait	PY	Paraguay	GOV	US Government
DO	Dominican Republic	KY	Cayman Islands	QA	Qatar	INT	International
DZ	Algeria	KZ	Kazakhstan	RE	Reunion	MIL	US Military
EC	Ecuador	LA	Laos	RO	Romania	NET	Network
EE	Estonia	LC	Saint Lucia	RS	Serbia	ORG	Non-Profit Organization
EG	Egypt	LI	Liechtenstein	RU	Russian Federation	ARPA	Old style Arpanet
EH	Western Sahara	LK	Sri Lanka	RW	Rwanda		

5. When you have entered all the required details, press the **Generate** button. The certificate takes several minutes to generate. When the certificate has been generated, you are informed that it has been successfully generated and installed. The web server on the router restarts and you are logged out of the router. Click **OK** to be taken back to the login screen.

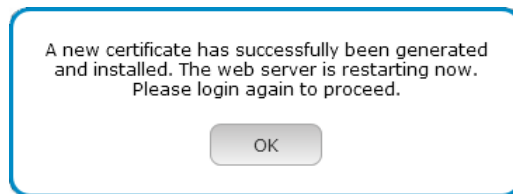


Figure 128 - New certificate successfully generated message

SSH Key Management

Secure Shell (SSH) is UNIX-based command interface and network protocol used to gain secure access to a remote computer, execute commands on a remote machine or to transfer files between machines. It was designed as a replacement for Telnet and other insecure remote shell protocols which send information, including passwords, as plain text.

SSH uses RSA public key cryptography for both connection and authentication. Two common ways of using SSH are:

- 📶 Use automatically generated public-private key pairs to encrypt the network connection and then use password authentication to log on.
- 📶 Use a manually generated public-private key pair to perform the authentication and allow users or programs to log in without using a password.

SSH server configuration

SSH protocol

Enable password authentication ON OFF

Enable key authentication ON OFF

Host key management

Key type	Date
ssh_host_key	1970-01-01 10:01:02
ssh_host_dsa_key	1970-01-01 10:01:09
ssh_host_rsa_key	1970-01-01 10:01:36
ssh_host_ecdsa_key	1970-01-01 10:01:36

Client key management

Username	Hostname	Key type

Figure 129 - SSH Server Configuration

SSH Server Configuration

To configure the SSH server settings:

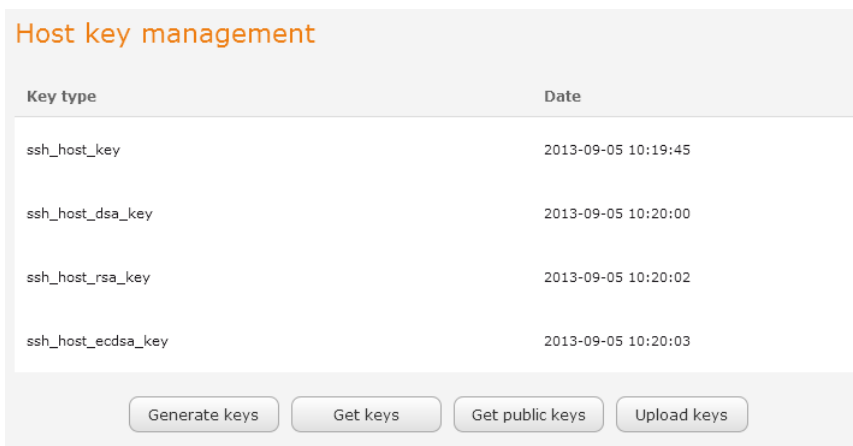
1. Use the SSH Protocol drop down list to select the protocol that you want to use. Protocol 2 is more recent and is considered more secure.
2. Select the types of authentication you want to use by clicking the **Enable password authentication** and **Enable key authentication** toggle keys on or off. Note that you may have both authentication methods on but you may not turn them both off.
3. Click the **Save** button to confirm your settings.

Host key management

SSH keys provide a means of identification using public key cryptography and challenge response authentication. This means that a secure connection can be established without transmitting a password, thereby greatly reducing the threat of someone eavesdropping and guessing the correct credentials.

SSH Keys always come in pairs with one being a public key and the other a private key. The public key may be shared with any server to which you want to connect. When a connection request is made, the server uses the public key to encrypt a challenge (a coded message) to which the correct response must be given. Only the private key can decrypt this challenge and produce the correct response. For this reason, the private key should not be shared with those who do not wish to give authorization.

The Host key management section displays the current public keys on the router and their date and timestamp. These public keys are provided in different formats, including DSA, RSA and ECDSA. Each format has advantages and disadvantages in terms of signature generation speed, validation speed and encryption/decryption speed. There are also compatibility concerns to consider with older clients when using ECDSA, for example.



Host key management

Key type	Date
ssh_host_key	2013-09-05 10:19:45
ssh_host_dsa_key	2013-09-05 10:20:00
ssh_host_rsa_key	2013-09-05 10:20:02
ssh_host_ecdsa_key	2013-09-05 10:20:03

Generate keys Get keys Get public keys Upload keys

Generating new keys

The complete set of keys can be re-generated by selecting the **Generate keys** button. This key generation process takes approximately 30 seconds to complete.

Downloading keys

The **Get keys** button allows you to download the complete set of public and private keys while the **Get public keys** button will download only the set of public keys.

Uploading your own key files

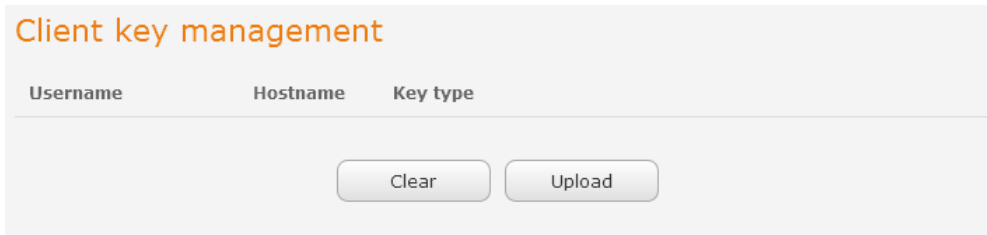
You can generate your own SSH keys and upload them to the router. To generate keys on a Linux-based machine, use the following commands:

```
mkdir keys
cd keys
ssh-keygen -t rsa1 -f ssh_host_key -N ""
ssh-keygen -t dsa -f ssh_host_dsa_key -N ""
ssh-keygen -t rsa -f ssh_host_rsa_key -N ""
ssh-keygen -t ecdsa -f ssh_host_ecdsa_key -N ""
zip -e -P "PASSWORDHERE" -j keys.zip *
```

Click the **Upload keys** button then locate the generated keys to upload them to the router.

Client key management

The Client Key Management section is used for uploading the public key file of clients. To upload a client public key, click the **Upload** button, browse to the file and click **Open**.



When the file is uploaded, it is examined for validity. If the key file is not a valid public key, it will not be uploaded.

LED operation mode

The LED indicators may be turned off after a timeout period for aesthetic or power saving reasons. To access the LED Operation Mode page, click the **System** menu, then **Administration** on the left and finally select **LED Operation Mode**.

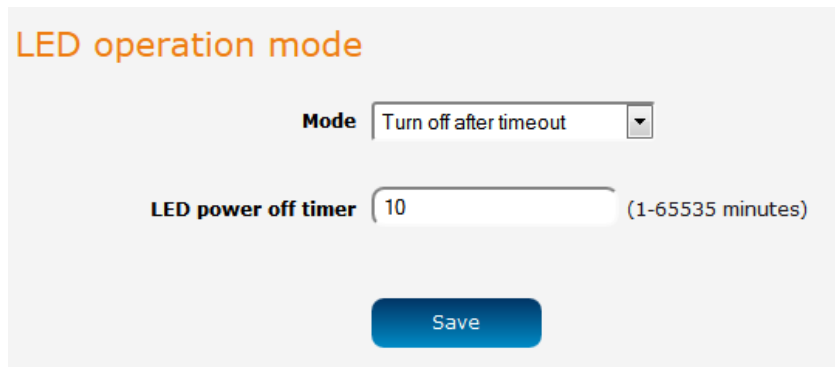


Figure 130 - LED Operation Mode

The **Mode** drop down list sets the operation mode of the LEDs on the front panel of the router. To set the lights to operate at all times, set this to Always on. To set the lights to turn off after a specified period, select **Turn off after timeout**. When configured to turn off after timeout, use the **LED power off timer** field to specify the time in minutes to wait before turning off the LED indicators. The LED Power Off Timer must be an integer between 1 and 65535.

The wait period begins from the time the **Save** button is clicked. When the wait period expires, the LEDs will turn off. If the router is rebooted, the LED power off timer is reset. The router will boot up and wait for the configured time before turning off again.

Watchdogs

To access the Watchdogs page, click the **Services** menu item, then select the **Watchdogs** menu item on the left.

Watchdogs settings

When configured, the watchdog feature transmits controlled ping packets to 1 or 2 user specified IP addresses. Should the watchdog not receive responses to the pings, it will reboot the device in a last resort attempt to restore connectivity.

Please be very careful when considering using this feature in situations where the device is intentionally offline for a particular reason (e.g user configured PDP session disconnect, or the connect on demand feature enabled). This is because the watchdog feature expects to be able to access the internet at all times, and will always eventually reboot the router if access isn't restored by the time the various timers and retries expire.

It is due to the nature of the watchdog being a last resort standalone backup mechanism that it will continue to do its job and reboot the device even when the connect on demand session is idle, or the PDP context is disabled by the user. Therefore, it is recommended to disable this feature if connect on demand is configured, or if the PDP context is intentionally disconnected on occasion.

This feature operates as follows:

A. After every "Periodic Ping timer" configured interval, the router sends 3 consecutive pings to the "First destination address".
B. If all 3 pings fail the router sends 3 consecutive pings to the "Second destination address".
C. The router then sends 3 consecutive pings to the "First destination address" and 3 consecutive pings to the "Second destination address" every "Periodic Ping accelerated timer" configured interval.
D. If all accelerated pings in step C above fail the number of times configured in "Fail count", the router reboots.
E. If any ping succeeds the router returns to step A and does not reboot.

Note: The "Periodic Ping timer" should never be set to a value less than 300 seconds- this is to allow the router time to reconnect to the cellular network following a reboot.

To disable the Watchdog, simply set "Fail count" to 0

First destination address

Second destination address

Periodic Ping timer (0=disable, 300-65535) secs

Periodic Ping accelerated timer (0=disable, 60-65535) secs

Fail count (0=disable, 1-65535) times

Periodic reboot

Force reboot every (0=disable, 5-65535) mins

Randomize reboot time

Figure 131 - Watchdogs Settings

Watchdogs are features which monitor the router for anomalies and restart the router if an anomaly occurs preventing its normal operation. When configured, the watchdogs feature transmits controlled ping packets to 1 or 2 user specified IP addresses to confirm an active connection. If the watchdog does not receive responses to the pings after a specified number of failures, it will reboot the device in a last resort attempt to restore connectivity.

We recommend using caution when implementing this feature in situations where the device is intentionally offline for a particular reason, for example, when Connect-on-demand has been enabled. This is because the watchdog expects to be able to access the internet at all times, and will always eventually reboot the router if access isn't restored by the time the various timers expire and the fail count is reached.

It is due to the nature of the watchdog being a last resort standalone backup mechanism that it will continue to do its job and reboot the device even when the Connect-on-demand session is idle, or the PDP context is disabled by the user. Therefore, we recommended that you disable this feature if Connect-on-demand is configured or if the PDP context is intentionally disconnected on occasion.

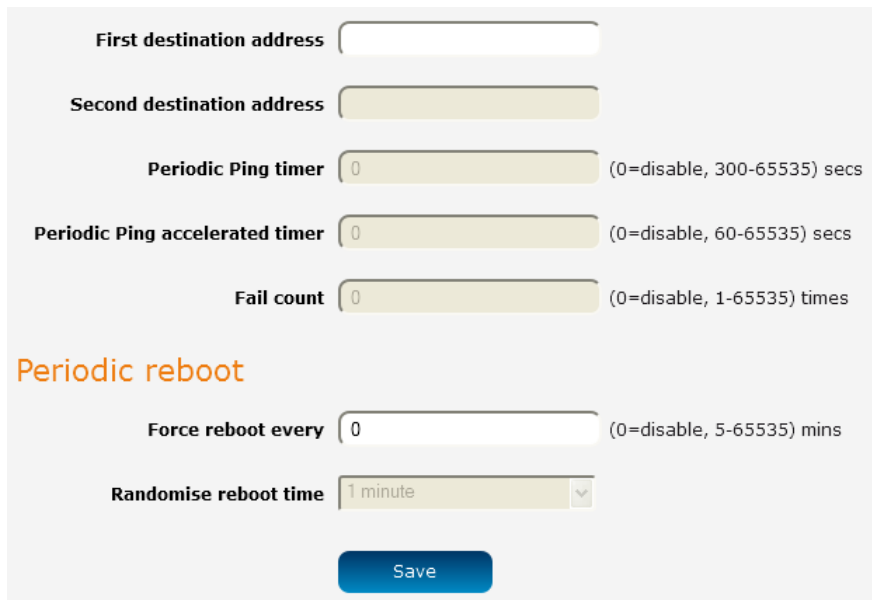
The watchdog works as follows:

- a) The router sends 3 consecutive pings to the first destination address at the interval specified in the **Periodic Ping timer** field.
- b) If all 3 pings to the first destination address fail, the router sends 3 consecutive pings to the second destination address at the **Periodic Ping timer** interval.
- c) If all 3 pings to the second destination address fail, the router sends 3 pings to the first destination address using the **Periodic Ping accelerated timer** interval.
- d) If all 3 accelerated pings to the first destination address fail, the router sends 3 pings to the second destination address at the **Periodic Ping accelerated timer** interval.
- e) If all 3 accelerated pings to the second destination address fail, the router registers this as a fail and returns to step C.
- f) When the number of failures reaches the number configured in the **Fail count** field, the router reboots. If any ping succeeds, the router returns to step A and does not reboot.



Note: The **Periodic Ping timer** should not be set to a value of less than 300 seconds to allow the router time to reconnect to the cellular network following a reboot.

To disable the periodic ping reset monitor, set **Fail count** to 0.



First destination address

Second destination address

Periodic Ping timer (0=disable, 300-65535) secs

Periodic Ping accelerated timer (0=disable, 60-65535) secs

Fail count (0=disable, 1-65535) times

Periodic reboot

Force reboot every (0=disable, 5-65535) mins

Randomise reboot time

Save

Figure 132 – Ping watchdog settings

Configuring Periodic Ping settings

The Periodic Ping settings configure the router to transmit controlled ping packets to 2 specified IP addresses. If the router does not receive responses to the pings, the router will reboot.

To configure the ping watchdog:

1. In the **First destination address** field, enter a website address or IP address to which the router should send the first round of ping requests.
2. In the **Second destination address** field, enter a website address or IP address to which the router should send the second round of ping requests.
3. In the **Periodic Ping timer** field, enter an integer between 300 and 65535 for the number of seconds the router should wait between ping attempts. Setting this to 0 disables the ping watchdog function.
4. In the **Periodic Ping accelerated timer** field, enter an integer between 60 and 65535 for the number of seconds the router should wait between accelerated ping attempts, i.e. pings to the second destination address. Setting this to 0 disables the ping watchdog function.
5. In the **Fail count** field, enter an integer between 1 and 65535 for the number of times an accelerated ping should fail before the router reboots. Setting this to 0 disables the ping watchdog function.

Disabling the Periodic Ping reset function

To disable the Periodic Ping reset function, set **Fail count** to 0.



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

Configuring a Periodic reboot

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, the router will reboot if some anomaly occurs.

1. In the **Force reboot every** field, enter the time in minutes between forced reboots. The default value is 0 which disables the Periodic reboot function. The minimum period between reboots is 5 minutes while the maximum value is 65535 minutes.
2. If you have configured a forced reboot time, you can use the **Randomise reboot time** drop down list to select a random reboot timer. Randomising the reboot time is useful for preventing a large number of devices from rebooting simultaneously and flooding the network with connection attempts. When configured, the router waits for the configured **Force reboot every** time and then randomly selects a time that is less than or equal to the **Randomise reboot time** setting. After that randomly selected time has elapsed, the router reboots.
3. Click the **Save** button to save the settings.



Note: The randomise reboot time is not persistent across reboots; each time the router is due to reboot, it randomly selects a time less than or equal to the **Randomise reboot time**.

Reboot

The reboot option in the System section performs a soft reboot of the router. This can be useful if you have made configuration changes you want to implement.

To reboot the router:

1. Click the **System** menu item from the top menu bar.
2. Click the **Reboot** button from the menu on the left side of the screen.

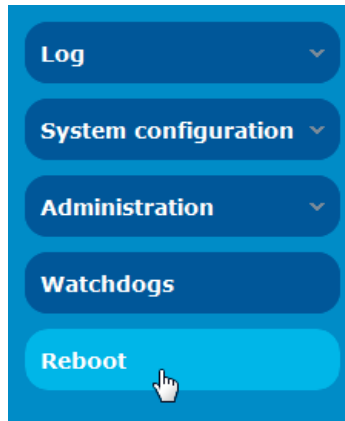


Figure 133 - Reboot menu option

3. The router displays a warning that you are about to perform a reboot. If you wish to proceed, click the **Reboot** button then click **OK** on the confirmation window which appears.




Figure 134 - Reboot confirmation



Note: It can take up to 2 minutes for the router to reboot.

Logging out

To log out of the router, click the  icon at the top right corner of the web user interface.

Appendix A: Tables

Table 1 - Document Revision History	2
Table 2 - LED Descriptions	9
Table 3 - Bottom Mounted interfaces	10
Table 4 - Top Mounted interfaces	11
Table 5 - Locking power block pin outs.....	12
Table 6 - Management account login details – Root manager	14
Table 7 - Management account login details – Admin manager	14
Table 8 - Status page item details	17
Table 9 - Data connection item details	19
Table 10 - Band settings.....	23
Table 11 - Wireless Configuration - Basic Configuration Items	33
Table 12 - Wireless Settings - Advanced Configuration Items.....	34
Table 13 – Wireless hotspot settings.....	38
Table 14 - Wireless settings – Client Configuration	39
Table 15 - Ethernet group configuration items	46
Table 16 - Ethernet WAN configuration options.....	47
Table 17 - Failover configuration - Hardware link monitoring.....	48
Table 18 - Current MAC / IP / Port filtering rules in effect.....	60
Table 19 - IPSec Configuration Items	63
Table 20 – TCP connect-on-demand endpoint options	80
Table 21 - Data stream applications.....	83
Table 22 – OMA Lightweight M2M configuration options.....	90
Table 23 - Event notification configuration options.....	95
Table 24 - Event notification – event types	95
Table 25 - Email client settings.....	97
Table 26 - SMS Setup Settings.....	99
Table 27 - Inbox/Outbox icons.....	101
Table 28 - SMS Diagnostic Command Syntax.....	106
Table 29 - List of basic SMS diagnostic commands	107
Table 30 - List of get/set commands.....	108
Table 31 - List of basic SMS diagnostics RDB variables	109
Table 32 - Network types returned by get plmnscan SMS command	109
Table 33 - Operator status codes returned by get plmnscan SMS command	109
Table 34 - SMS diagnostics example commands.....	113
Table 35 - System log detail levels	117
Table 36 - Administration configuration options.....	124
Table 35 - LAN Management Default Settings.....	136
Table 36 - Web Interface Default Settings	136
Table 37 - Telnet Access	136
Table 38 - Technical Specifications of the NTC-40WV routers.....	144
Table 39 - Additional Product Information - Call Feature Codes Quick Reference	146
Table 40 - List of Mobile Broadband Service Provider APNs.....	148

Appendix B: Default Settings

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

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

Table 37 - LAN Management Default Settings

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

Table 38 - Web Interface Default Settings





Note: The admin manager account allows you to manage all settings of the router except functions such as firmware upgrade, device configuration backup and restore and reset to factory default settings, which are privileged only to the root manager account.

NTC-40WV ROUTER TELNET ACCESS	
Username:	root
Password:	admin



Table 39 - Telnet Access

Restoring factory default settings

Restoring factory defaults will reset the NTC-40WV router to its factory default configuration. You may encounter a situation where you need to restore the factory defaults on your NTC-40WV 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-40WV router:

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

Using the web-based user interface

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

1. Open a browser window and navigate to the IP address of the router (default address is <http://192.168.1.1>). Login to the router using **root** as the User Name and **admin** as the password.
2. Click the **System** item from the top menu bar, then **System configuration** on the left menu and then click **Settings backup and restore**.
3. Under the **Restore factory defaults** section, click the **Restore defaults** button. The router asks you to confirm that you wish to restore factory defaults. Click **OK** to continue. The router sets all settings to default. Click **OK** again to reboot the router.
4. When the Power light returns to a steady red, the reset is complete. The default settings are now restored.

Using the reset button on the interface panel of the router

Use a pen to depress the Reset button on the device for more than 15 seconds. When the LEDs are no longer flashing, release the reset button to restore the router to factory default settings. The red LED flashes indicating that you have initiated a factory reset procedure. If you change your mind after holding the button down for more than 15 seconds, you can cancel the factory reset process by disconnecting the power source while still holding the reset button down. Alternatively, you can release the reset button and quickly press it once more.

When you have reset your NTC-40WV router to its default settings you will be able to access the device's configuration web interface using <http://192.168.1.1> with username **admin** or **root** and password **admin**.

Appendix C: Recovery mode

The NTC-40WV Router 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). The recovery console provides limited functionality and is typically used to restore the main firmware image in the case of a problem.

Accessing recovery mode

Both systems have web interfaces that can be used to manipulate the other inactive system. The NTC-40WV 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. Press and hold the physical reset button on the interface panel of the router for 5 to 15 seconds. When the LEDs on the front panel flash simultaneously, release the reset button. The router then boots into recovery mode.
2. 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.

NetComm Cellular Router Recovery Console


Status	Log	Application Installer	Settings	Reboot
Status				
System Information				
System Up time	00:01:26			
Router Version	Hardware: 1.0 Software: V2.0.4.1			
Serial Number	153711121020105			
Trigger	button			
LAN				
IP	192.168.1.1 / 255.255.255.0			
MAC Address	00:60:64:65:8F:36			
Ethernet Port Status				
LAN: 	Up / 100.0 Mbps / FDX			

Figure 135 - Recovery console

Status

The status page provides basic information such as the system up time, hardware and software router versions, the router's serial number, the method used to trigger the recovery mode, the IP and MAC address of the router and the status of the Ethernet port.

NetComm Cellular Router Recovery Console


Status	Log	Application Installer	Settings	Reboot
Status				
System Information				
System Up time	00:01:26			
Router Version	Hardware: 1.0 Software: V2.0.4.1			
Serial Number	153711121020105			
Trigger	button			
LAN				
IP	192.168.1.1 / 255.255.255.0			
MAC Address	00:60:64:65:8F:36			
Ethernet Port Status				
LAN: 	Up / 100.0 Mbps / FDX			

Figure 136 - Recovery mode - Status

Log

The log page displays the system log which is useful in troubleshooting problems which may have led to the router booting up in recovery mode. The only functionality provided here is the ability to clear the system log, filter by log level and downloading of the log file.

Status	Log	Application Installer	Settings	Reboot
Log File <input type="text" value="Display Level"/> <input type="text" value="All"/> <input type="button" value="Page 1 of 7"/> <input type="button" value="Clear Log File"/>				
Date & Time	Machine	Level	Process	Message
Jan 1 00:00:47	nto_40wv	daemon.warn	dnsmasq-dhcp[328]	Ignoring domain corp.netcomm.com.au for DHCP host name pdg26
Jan 1 00:00:47	nto_40wv	daemon.info	dnsmasq-dhcp[328]	DHCPACK(eth0) 192.168.1.148 00:21:9b:1a:89:ee pdg26
Jan 1 00:00:47	nto_40wv	daemon.info	dnsmasq-dhcp[328]	DHCPREQUEST(eth0) 192.168.1.148 00:21:9b:1a:89:ee
Jan 1 00:00:47	nto_40wv	daemon.info	dnsmasq-dhcp[328]	DHCPPOFFER(eth0) 192.168.1.148 00:21:9b:1a:89:ee
Jan 1 00:00:47	nto_40wv	daemon.warn	dnsmasq[328]	overflow: 5 log entries lost
Jan 1 00:00:05	nto_40wv	daemon.info	dnsmasq[328]	started, version 2.57 cachesize 150
Jan 1 00:00:14	nto_40wv	user.debug	kernel	eth0: no IPv6 routers present
Jan 1 00:00:06	nto_40wv	user.info	appweb	HTTP services are ready with 4 pool threads
Jan 1 00:00:06	nto_40wv	user.info	appweb	Switching to background operation
Jan 1 00:00:06	nto_40wv	user.info	appweb	Listening for HTTP on *:80
Jan 1 00:00:06	nto_40wv	user.info	appweb	Starting host named: "888:80"
Jan 1 00:00:06	nto_40wv	user.info	appweb	Activating module (Loadable) capi
Jan 1 00:00:06	nto_40wv	user.info	appweb	Add copyHandler
Jan 1 00:00:06	nto_40wv	user.info	appweb	Activating module (Loadable) copy
Jan 1 00:00:06	nto_40wv	user.info	kernel	eth0: link up (100/Full)
Jan 1 00:00:06	nto_40wv	user.err	kernel	odcs_gpio: module is already loaded
Jan 1 00:00:06	nto_40wv	user.info	kernel	Start odcsDD, compiled Jan 18 2014 08:25:28
Jan 1 00:00:06	nto_40wv	user.warn	kernel	Disabling lock debugging due to kernel taint
Jan 1 00:00:06	nto_40wv	user.warn	kernel	odcs_DD: module license 'ODCS Proprietary' taints kernel.
Jan 1 00:00:06	nto_40wv	user.info	kernel	Freeing init memory: 108K
Jan 1 00:00:06	nto_40wv	user.info	kernel	devtmpfs: mounted
Jan 1 00:00:06	nto_40wv	user.warn	kernel	VFS: Mounted root (jffs2 filesystem) on device 31:2.
Jan 1 00:00:06	nto_40wv	user.info	kernel	All bugs added by David S. Miller

[Download Log File](#)

Figure 137 - Recovery mode - Log

Application Installer

The Application installer is designed to upload and install main firmware images, upload recovery firmware images, custom applications and HTTPS certificates. Use the **Browse** button to select a file to be uploaded to the router. When it has been selected, press the **Upload** button. The file is sent to the router and when the transfer is complete, the file appears in the Uploaded files list. From the Uploaded files list, you are able to either **Install** or **Delete** a file.

NetComm Cellular Router Recovery Console

Status	Log	Application Installer	Settings	Reboot
--------	-----	-----------------------	----------	--------

[Recovery Console > Upload](#)

Upload:

File	<input type="button" value="Browse..."/> No file selected.	<input type="button" value="Upload"/>
------	--	---------------------------------------

Uploaded Files:

Free Space: 105.6M

File Name	Date	Size	Action

Figure 138 - Recovery mode - Application Installer

Settings

The settings page provides the option of restoring the router to factory default settings. Click the **Restore** button to set the router back to the original factory settings.

Status	Log	Application Installer	Settings	Reboot
--------	-----	-----------------------	----------	--------

[Settings](#)

RESTORE FACTORY DEFAULTS:

Figure 139 - Recovery mode - Settings

Reboot

The reboot page allows you to reboot the router when you have finished using recovery mode. When rebooting the router from recovery mode, the router boots into the main firmware image unless there is some fault preventing it from doing so, in which case the recovery console will be loaded.

Click the **Reboot** button to reboot the router to the main firmware image.

Status	Log	Application Installer	Settings	Reboot
--------	-----	-----------------------	----------	--------

[Reboot](#)

To perform the reboot, click on the "Reboot" button below. You will be asked to confirm your decision.

Figure 140 - Recovery mode - Reboot

Appendix D: HTTPS - Uploading a self-signed certificate

If you have your own self-signed certificate or one purchased elsewhere and signed by a Certificate Authority, you can upload it to the NTC-40WW router using the [Upload](#) page.



Note: Your key and certificate files must be named **server.key** and **server.crt** respectively otherwise they will not work.

To upload your certificate:

1. Click on the **System** item from the top menu bar. From the side menu bar, select **System Configuration** and then **Upload**. The file upload screen is displayed.

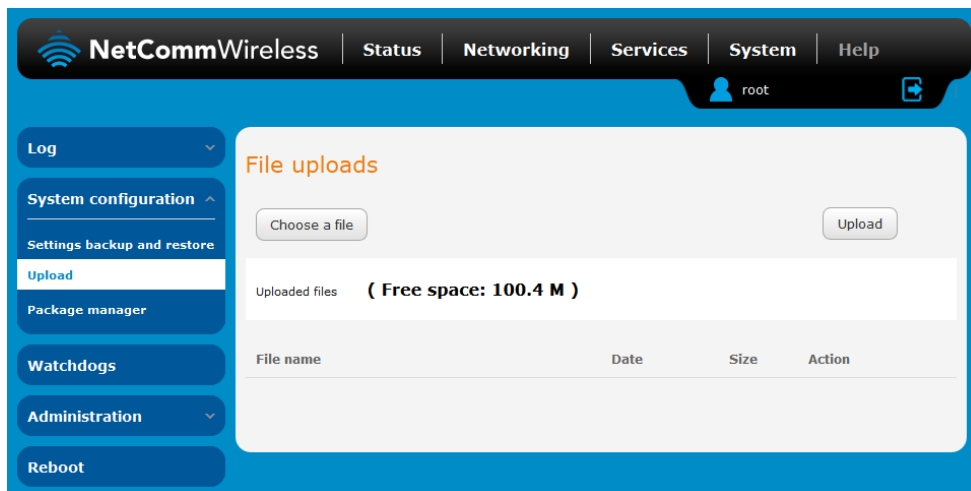


Figure 141 - Upload page

2. Click the **Choose a File** button and locate your server certificate file and click **Open**.

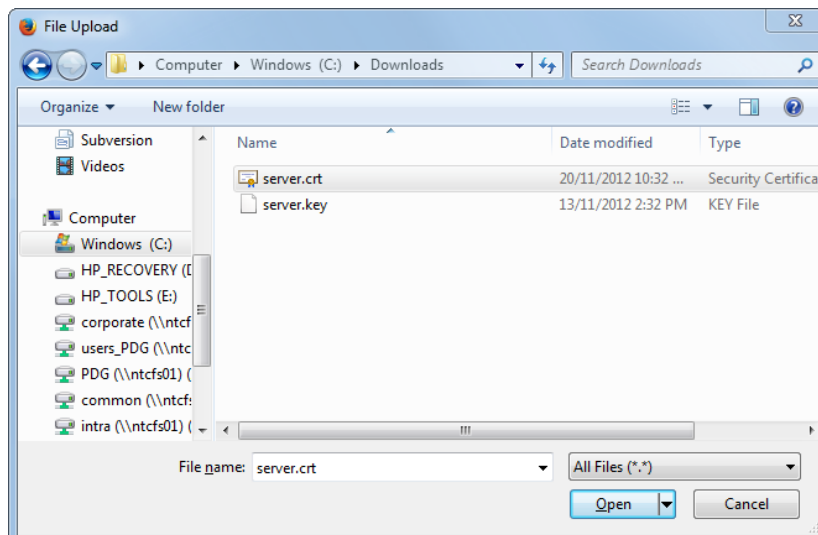


Figure 142 - Browse for server.crt

- Click the **Upload** button to begin uploading it to the router. The file appears in the list of files stored on the router.



Figure 143 - Server certificate file uploaded

- Repeat steps 2 and 3 for the server key file.
- Click the **Install** link next to the server.crt file then click **OK** on the prompt that is displayed. The certificate file is installed. Repeat this for the key file. When each file is installed it is removed from the list of stored files.

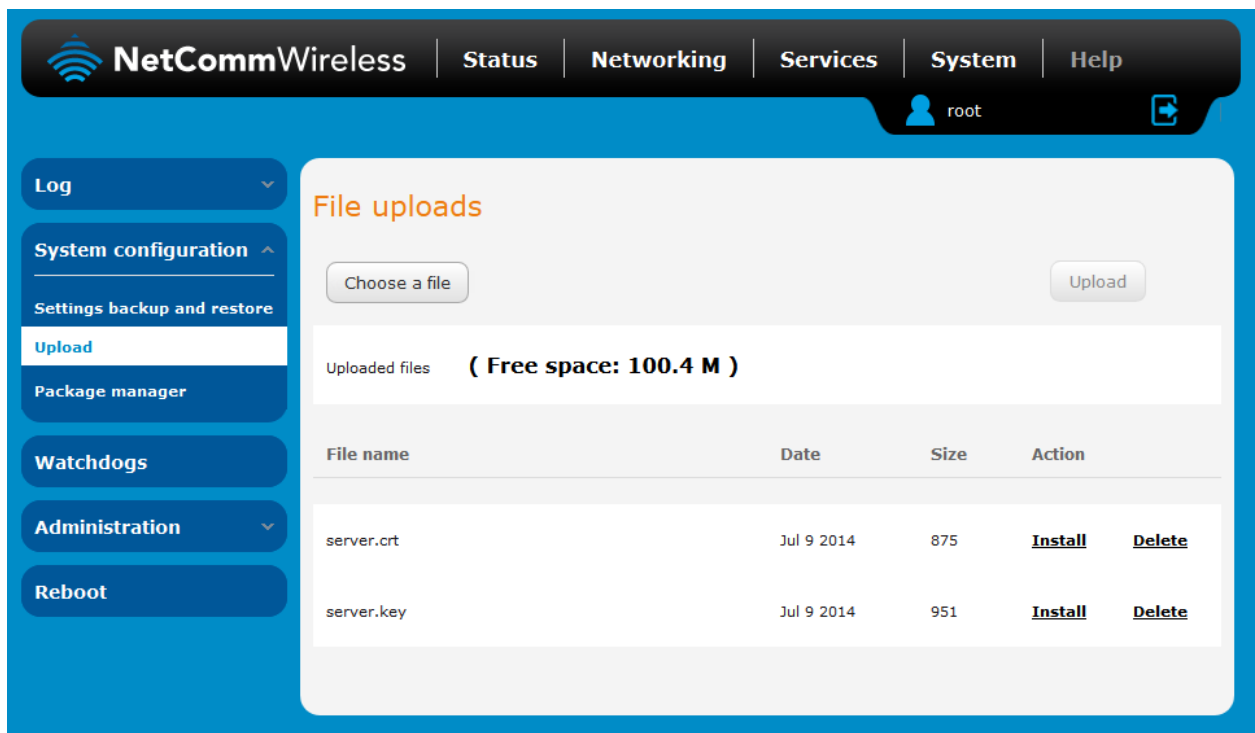


Figure 144 - Installing the server.crt file

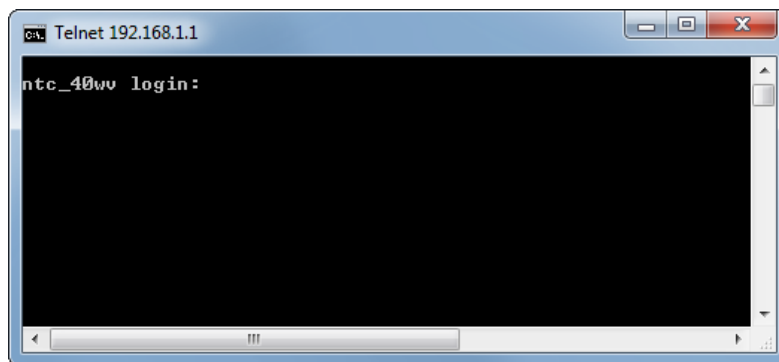
Appendix E: Obtaining a list of RDB variables

The RDB is a database of variables that contain settings on the router. You can retrieve (get) and set the values of these variables through the command-line or via SMS Diagnostics. To access a full list of the RDB variables, follow these steps:

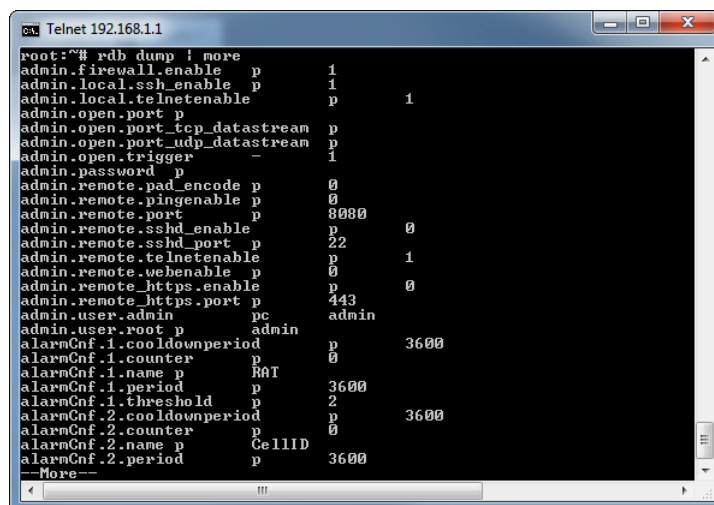
1. Log in to the web user interface as described in the [Advanced configuration](#) section of this guide.
2. Click the **System** menu at the top of the screen, then select the **Administration** menu on the left. Finally, select the **Administration settings** menu item.
3. Click the **Enable Telnet** toggle key so that it is in the **ON** position.



4. Under the **Telnet/SSH account** section, enter a telnet password and then re-enter it in the **Confirm password** field.
5. Click the **Save** button at the bottom of the screen.
6. Open a terminal client such as PuTTY and telnet to the router using its IP address.



7. At the login prompt, type `root` and press Enter. At the password prompt, enter the password that you configured in step 4.
8. At the root prompt, enter the command `rdb dump | more`. This will display a list of every rdb variable on the router one page at a time.



Note: Omitting the `| more` parameter will dump a complete list without pagination. For easier access, some terminal clients such as PuTTY have the ability to log all telnet output to a text file.

Technical Data

The following tables list the hardware specifications of the NTC-40WV router.

COMPONENT	NTC-40WV
RAM	32MB DRAM
Memory	256MByte Flash memory storage
Wireless LAN	IEEE 802.11b/g/n, up to 16 concurrent users
Wireless Frequency	2.4 ~ 2.438Ghz
Peak Data Rate (Wireless)	300 Mbps (MIMO)
UMTS bands	UMTS/HSDPA/HSUPA: 850/900/1900/2100 MHz
GSM bands	GSM/GPRS/EDGE: 850/900/1800/1900 MHz
Maximum Data Throughput / 3G Radio interface	Downlink: 21 Mbps (HSPA Evolution); EDGE/GPRS 247Kbps; Uplink: Uplink: 5.76 Mbps (HSPA Evolution); EDGE/GPRS 247Kbps
Connectivity	1x Fast Ethernet 10/100Base-TX w/ Auto MDIX 1x Voice port (RJ11)
SIM Card Reader	Locking Tray for SIM/SIM in Mini-SIM card format (25.00 x 15.00 x 0.76 mm)
Antenna connectors	Cellular: 2 x detachable SMA (MIMO) WLAN: 2 x detachable Reverse SMA (MIMO)
LED Indicators	5x LEDs. Power, Service, Tx/Rx, DCD and RSSI
Operating Temperature	Normal Operating Temperature: -25 °C to 60 °C Extended Operating Temperature: Module: -25°C to +75°C (Reduced Performance)
Power input	DC-in Port: 9 ~ 28V AC/DC Power Adapter: 100-240V AC to 12V DC/1.5A
Power Consumption	Standby Input Current: 110mA @ 12V DC 3G Active Current: 300mA @ 12V DC Maximum Input Current: 560mA @ 12V DC

Table 40 - Technical Specifications of the NTC-40WV routers

Additional Product Information

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

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



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

Handset requirements

The NTC-40WV allows you to make telephone calls over the 3G network using a standard analogue telephone via the built in RJ11 Phone port. Please refer to the documentation provided by the manufacturer of your analogue telephone for assistance with the operation of your telephone handset.

Maximum REN Loading

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

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

You have an activated 3G SIM card inserted prior to powering on the NTC-40WV.

1. Your NTC-40WV is powered on and in running condition.
2. A working analogue telephone connected into the Line port.
3. You hear the dial tone after lifting the handset.

How to place a call

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

How to receive a call

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

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

Answering an incoming call when on a call

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

Accessing voicemail

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

Call feature codes

Quick Reference Table

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

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

Table 41 - Additional Product Information - Call Feature Codes Quick Reference

Caller ID

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

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

Caller ID Test Steps

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

Call Waiting

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

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

Call Forwarding

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



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

Call Forwarding Unconditional

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

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

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

Call Forwarding No Answer

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

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

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

Call Forwarding Busy

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

To enable Call Forwarding Busy, dial *24*<Directory Number>#
(Where directory number is the number you wish to forward calls to)

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

Call Forwarding Not Reachable

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

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

Conference Call

This can be achieved by performing the following:

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

To terminate the conference call hang up the phone connected to the router.

Voice Troubleshooting

What do I do if I have no dial tone?

Please follow the procedure listed below:

1. Check to make sure the phone is plugged into your NTC-40WV on the RJ11 port (between the power socket and the LAN port).
2. Check to make sure you are using the correct cable (Cat-3 UTP Telephone Cable with RJ11 plugs).
3. Check to make sure the “SIM status” shows “SIM OK” on the Status page of the Web interface.
4. Check to make sure your 3G SIM card is activated and insert into your NTC-40WV properly.
5. Check and see if you get the dial tone after rebooting your NTC-40WV.

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

To resolve this issue, try the following:

1. Verify that the RJ11 cable is securely connected and not damaged.
2. Try to remove any telephone splitters from the connection between your phone and the NTC-40WV.
3. Try rebooting your NTC-40WV.

List of Mobile Broadband Service Provider APNs

MOBILE SERVICE	APN
Australia	
Telstra	telstra.internet
Optus – Postpaid	connect
Optus – Prepaid	preconnect
Three – Postpaid	3netaccess
Three – Prepaid	3services
Vodafone – Postpaid	vfinternet.au
Vodafone – Prepaid	vfprepaymbb
Crazy John’s	purtona.net
DoDo	dodoIns1
Blink	splns888a1
Internode	Internode
Primus	primusIns1
TPG	internet
Exetel	Exetel1
Westnet	SpIns555a1
iiNet	iiNet
New Zealand	
Vodafone NZ	www.vodafone.net.nz
CallPlus	www.callplus.net.nz
Slingshot	www.slingshot.net.nz
Telstra Clear	www.telstraclear.net.nz
Telecom NZ XT	wap.telecom.co.nz
2 Degrees	internet

Table 42 - List of Mobile Broadband Service Provider APNs

Legal & Regulatory Information

Intellectual Property Rights

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

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

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

Customer Information

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

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

Consumer Protection Laws

Australian and New Zealand consumer law in certain circumstances implies mandatory guarantees, conditions and warranties which cannot be excluded by NetComm 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 Wireless products have a standard one (1) year warranty from date of purchase, however, some products have an extended warranty option (refer to packaging and the warranty card) (each a Product Warranty). To be eligible for the extended warranty option you must supply the requested warranty information to NetComm Wireless Limited within 30 days of the original purchase date by registering online via the NetComm Wireless web site at www.netcommwireless.com. For all Product Warranty claims you will require proof of purchase. All Product Warranties are in addition to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Consumer Protection Laws Section above).

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see the [Consumer Protection Laws](#) Section 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 Wireless Limited 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 Wireless Limited recommends that you enable these features to enhance your security.

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

1. you, or someone else, use the product, or attempt to use it, other than as specified by NetComm Wireless Limited;
2. the fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. the fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm Wireless Limited; 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 the [Consumer Protection Laws](#) Section above), NetComm Wireless Limited accepts no liability or responsibility, for consequences arising from the use of this product. NetComm Wireless Limited reserves the right to change the specifications and operating details of this product without notice.

If any law implies a guarantee, condition or warranty in respect of goods or services supplied, and NetComm Wireless'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 Wireless's liability for any breach of that guarantee, condition or warranty is limited to: (i) in the case of a supply of goods, NetComm Wireless Limited doing any one or more of the following: replacing the goods or supplying equivalent goods; repairing the goods; paying the cost of replacing the goods or of acquiring equivalent goods; or paying the cost of having the goods repaired; or (ii) in the case of a supply of services, NetComm Wireless Limited doing either or both of the following: supplying the services again; or paying the cost of having the services supplied again.

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

Contact

Address: NETCOMM WIRELESS LIMITED Head Office

PO Box 1200, Lane Cove NSW 2066 Australia

Phone: +61(0)2 9424 2070

Fax: +61(0)2 9424 2010

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