Copyright

Copyright© 2014 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-6908
- NetComm Wireless NTC-6908-02
- NetComm Wireless NTC-6520

<table>
<thead>
<tr>
<th>DOCUMENT VERSION</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 - Initial document release</td>
<td>24/01/2014</td>
</tr>
<tr>
<td>1.1 – Updated Appendix E: Serial port wiring</td>
<td>21/05/2014</td>
</tr>
</tbody>
</table>

Table 1 - Document Revision History
# Table of Contents

Overview ................................................................................................................................. 4  
Introduction ............................................................................................................................. 4  
Target audience ...................................................................................................................... 4  
Prerequisites ........................................................................................................................... 4  
Notation ................................................................................................................................... 4  

Product introduction .............................................................................................................. 5  
   Product overview .................................................................................................................. 5  
   Package contents .................................................................................................................. 5  
   Product features ................................................................................................................... 6  
Hardware overview ............................................................................................................... 7  
   LED indicators ....................................................................................................................... 7  
   Interfaces ............................................................................................................................... 8  

Configuring your Router ....................................................................................................... 10  
   Setting Up the Cellular Router ............................................................................................ 10  
Installation and configuration of the NTC-6000 Series router ............................................. 11  
   Powering the router ............................................................................................................. 11  
   Installing the router ............................................................................................................ 11  
Advanced configuration ......................................................................................................... 12  
Status ...................................................................................................................................... 13  

Networking ........................................................................................................................... 15  
   Data Connection .................................................................................................................. 15  
   Operator settings ................................................................................................................ 19  
   SIM security settings ......................................................................................................... 20  
   LAN .................................................................................................................................... 26  
   Routing ............................................................................................................................... 30  
   VPN ..................................................................................................................................... 40  

Services ................................................................................................................................... 53  
   Dynamic DNS ..................................................................................................................... 53  
   Network time (NTP) ............................................................................................................. 54  
   Data stream manager ......................................................................................................... 55  
   Legacy data managers ....................................................................................................... 60  
   Watchdogs .......................................................................................................................... 63  
   SNMP .................................................................................................................................. 66  
   TR-069 ................................................................................................................................. 68  
   GPS (NTC-6908 only) ......................................................................................................... 70  
   SMS messaging .................................................................................................................. 73  
   Diagnostics ........................................................................................................................ 77  
   Sending an SMS Diagnostic Command ............................................................................ 79  

System ..................................................................................................................................... 88  
   Log ...................................................................................................................................... 88  
   System Configuration ......................................................................................................... 91  
   HTTPS key management .................................................................................................... 98  
   SSH Key Management ....................................................................................................... 101  

Appendix A: Tables .............................................................................................................. 105  
Appendix B: Default Settings ............................................................................................... 106  
Restoring factory default settings ......................................................................................... 107  
Appendix C: Recovery mode ................................................................................................. 108  
   Accessing recovery mode ................................................................................................. 108  
   Status .................................................................................................................................. 109  
   Log ..................................................................................................................................... 109  
   Application Installer ......................................................................................................... 110  
   Settings ............................................................................................................................... 110  
   Reboot ............................................................................................................................... 110  

Appendix D: HTTPS - Uploading a self-signed certificate ................................................... 111  
Appendix E: Serial port wiring ............................................................................................. 113  

Technical Data ....................................................................................................................... 114  

Legal & Regulatory Information ........................................................................................... 115  
   Intellectual Property Rights ............................................................................................. 115  
   Customer Information ....................................................................................................... 115  
   Consumer Protection Laws ............................................................................................... 115  
   Product Warranty ............................................................................................................. 116  
   Limitation of Liability ....................................................................................................... 116  

Contact ................................................................................................................................... 117
Overview

Introduction
This document provides you all the information you need to set up, configure and use the NetComm Wireless NTC-6000 Series 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-6000 Series 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.

Notation
The following symbols are used in this user guide:

⚠️ The following note requires attention.

⚠️ The following note provides a warning.

ℹ️ The following note provides useful information.
Product introduction

Product overview

An NTC-6000 series router allows you to build wide area networks utilizing the superior speeds supported by 3G UMTS networks. Employing an embedded 3G UMTS modem module the router offers downlink speeds of up to 7.2Mbps and uplink speeds of up to 5.76Mbps.

The NTC-6000 series provides you with 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.

Designed with remote installation in mind the NTC-6000 series supports multi-level system monitoring giving you peace of mind the device will keep the lines of communication up and open.

In the event of system corruption, a built-in recovery mode provides the facility to re-install the system software to the router and resume normal operations quickly. The recovery mode is described in more detail in an appendix to this guide.

Package contents

The NetComm Wireless NTC-6000 Series router package consists of:

- 1x NTC-6000 Series router
- 2x 3G antennas
- 1x 1.5m yellow Ethernet cable 8P8C
- 1x quick start guide

If any of these items are missing or damaged, please contact NetComm Wireless Support immediately. The NetComm Wireless Support website can be found at: [http://support.netcommwireless.com](http://support.netcommwireless.com).
Product features

- Intelligent industrial cellular router platform supporting various networks and service types UMTS/HSDPA/HSUPA & GSM/GPRS/EDGE
- High-speed Atmel 400MHz ARM9-based Microcontroller.
- Antenna diversity to improve fringe performance on global HSPA networks.
- Wide area data access speeds in 3G mode up to 7.2Mbps in downlink (HSDPA category 8) and up to 5.76Mbps in uplink (HSUPA category 6).
- Wide area data access speeds in 2G mode up to 236 kbps (EDGE multi slot class 12).
- Rugged metal housing and temperature-hardened electronic components - extended operating temperature -30 to 70°C.
- Wide input voltage range: 8 – 28V DC. Suitable for diverse environments and applications.
- Embedded Linux operating system allowing for the installation of custom applications.
- Web user interface for easy centralized configuration and management from any computer or smartphone with multi-level administrator access.
- 10/100Base-TX port for Ethernet connections.
- RS-232 port for connection to serial devices.
- PAD mode via the serial port.
- PAD Daemon in simultaneous Server and Client mode
- Integrated GPS for remote position tracking-location mapping via Google Maps.
- VPN client for establishing a secure connection over public networks.
- Supports SNMP with cellular specific MIB, PPPoE, MAC /NET address filtering, DHCP/DHCP relay, Dynamic DNS and advanced routing RIP/VRRP
- Supports NAT, Port forwarding and a DMZ Host
- Configurable APN profiles
- Supports manual network scan, system monitoring, diagnostic log viewer.
- Web user interface for easy centralized configuration and management from any PC or smartphone
- Remote diagnostics, configuration and firmware update over the air (FOTA)
- SMS client allowing advanced SMS diagnostics and command execution
- Software Development Kit (SDK) for the creation of custom applications
- Dual system management - recovery mode to restore router system software in the event of corruptions locally or remotely.
- TR 069 functionality for ACS server management.
## 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.

![Router with LED indicators](image)

**Figure 1: NTC-6000 Series LEDs**

<table>
<thead>
<tr>
<th>LED</th>
<th>DISPLAY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>POWER (red)</strong></td>
<td>Solid ON</td>
<td>The red Power LED indicates power has been applied to the router from the DC power input jack.</td>
</tr>
<tr>
<td><strong>TX Rx (amber)</strong></td>
<td>Solid ON</td>
<td>The amber LED will illuminate upon data being sent to or received from the cellular network.</td>
</tr>
<tr>
<td><strong>DCD (green)</strong></td>
<td>Solid ON</td>
<td>The green Data Carrier Detect LED illuminates to indicate a data connection.</td>
</tr>
<tr>
<td><strong>Service Type (green)</strong></td>
<td>Solid ON, Flashing, Off</td>
<td>The green LED will illuminate when cellular network coverage is detected.</td>
</tr>
<tr>
<td><strong>RSSI (green)</strong></td>
<td>Solid ON, Flashing Once a Second, Off</td>
<td>This green LED shows Received Signal Strength. There are three possible states that the RSSI LED can operate in, based upon signal level.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Strong: Indicates the RSSI level is -86dbm</th>
<th>Medium: Indicates the RSSI level is -110dbm and -86dbm</th>
<th>Fair: Indicates the RSSI level is less than -110dbm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Solid ON</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Flashing Once a Second</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Off</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table 2* - LED Descriptions
Interfaces

**Figure 2 - Interfaces – Left Side View**

- **Receive Diversity Socket (SMA)**
- **Main Antenna Socket (SMA)**
- **Indicator LEDs**
- **Serial RS-232 Port (DB-9 DCE)**

**Figure 3 - Interfaces – Right Side View**

- **Ethernet Port (RJ-45)**
- **Reset Button**
- **SIM Card Reader**
- **Locking Power Terminal Block**

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Antenna Socket</td>
<td>SMA female connector for external antenna.</td>
</tr>
<tr>
<td>Receive Diversity Antenna Socket</td>
<td>SMA female connector for external antenna.</td>
</tr>
<tr>
<td>Serial RS-232 Port</td>
<td>For connecting to a terminal using a DB9-F cable.</td>
</tr>
<tr>
<td>Indicator LEDs</td>
<td>Indicates the connection strength, service type, data traffic, data carrier connection and network connection strength.</td>
</tr>
<tr>
<td>Power Terminal Block</td>
<td>Terminate power wires here and connect to DC power source (8-28V). Correct polarity is shown on page 10.</td>
</tr>
</tbody>
</table>

**Reset Button**

The reset button has multiple functions:

- 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.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Port</td>
<td>For direct connection to your devices through a hub or network router.</td>
</tr>
<tr>
<td>SIM Card Reader</td>
<td>For insertion and removal of SIM card.</td>
</tr>
</tbody>
</table>

Table 3: Router Interface Ports
Configuring your Router

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

- Power supply (8-28VDC)
- 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]

<table>
<thead>
<tr>
<th>PIN</th>
<th>SIGNAL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>V+</td>
<td>Voltage +</td>
</tr>
<tr>
<td>-</td>
<td>V-</td>
<td>Ground</td>
</tr>
</tbody>
</table>
Installation and configuration of the NTC-6000 Series router

Powering the router
The NTC-6000 Series router can be powered in one of two ways:

1. DC power input via 2-pin connector (8-28V DC)
2. DC power input via field terminated power source (8-28V 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 8-28V 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-6000 Series 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-6000 Series 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-6000 Series 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://192.168.20.1` into the address bar and press Enter. The web-based user interface log in screen is displayed.

![Log in prompt for the web-based user interface](image)

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.

<table>
<thead>
<tr>
<th>ACCOUNT</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROOT MANAGER ACCOUNT</td>
<td>root</td>
<td>admin</td>
</tr>
<tr>
<td>ADMIN MANAGER ACCOUNT</td>
<td>admin</td>
<td>admin</td>
</tr>
</tbody>
</table>

Table 5 - Management account login details – Root manager

Table 6 - 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-6000 Series 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).

#### System Information

<table>
<thead>
<tr>
<th>Device version</th>
<th>Cellular module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board version 1.3</td>
<td>Model MCE900W</td>
</tr>
<tr>
<td>Serial number 19000014821</td>
<td>Module firmware K2.6.5.0AP C/NGFW.A7.2.6.5.0AP.JMNM1526.GAC.20160318.11:50:40</td>
</tr>
<tr>
<td>Firmware version V2.0.4.1</td>
<td>IMEI 000000000000000</td>
</tr>
</tbody>
</table>

#### Cellular Module

- **Model**: MCE900W
- **Module Firmware**: K2.6.5.0AP C/NGFW.A7.2.6.5.0AP.JMNM1526.GAC.20160318.11:50:40
- **IMEI**: 000000000000000
- **Hardware**: 1.0

#### Cellular Connection Status

- **SIM Status**: SIM OK
- **Signal strength (dBm)**: -62 dBm (Medium)
- **Network registration status**: Registered, home network
- **Operator selection**: Auto
- **Current operator**: WCDMA 850
- **Roaming status**: Not roaming
- **Allowed bands**: Auto-band
- **Current band**: WCDMA 850
- **Coverage**: Combined service

#### WWAN Connection Status

- **Profile name**: X00000
- **Status**: Connected
- **Default profile**: Yes
- **WWAN IP**: 10.100.4.167
- **DHCP server**: 10.4.81.103 10.4.182.20
- **APN**: unknown
- **Connection uptime**: 01:38:44

#### Advanced Status

- **Mobile country code**: 505
- **Mobile network code**: XX
- **Signal Quality (Ec/No)**: -15 dB
- **Received Signal power (RSSI)**: -63 dBm
- **SIM ICCID**: 8962019114965430000007
- **Primary scrambling code (PSC)**: 88
- **Location area code (LAC)**: 327
- **Routing area code (RAC)**: 0
- **IMSI**: 000000000000000
- **Call ID**: 99792
- **Channel number (GSM)**: 4436
- **Module PREID Revision**: 3.2
- **Module PREID PRE part number**: 9992461

---

*Figure 7 - The Status page*
<table>
<thead>
<tr>
<th>ITEM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System information</strong></td>
<td></td>
</tr>
<tr>
<td>System up time</td>
<td>The current uptime of the router.</td>
</tr>
<tr>
<td>Board version</td>
<td>The hardware version of the router.</td>
</tr>
<tr>
<td>Serial number</td>
<td>The serial number of the router.</td>
</tr>
<tr>
<td>Firmware version</td>
<td>The firmware version of the router</td>
</tr>
<tr>
<td>Model</td>
<td>The type of phone module and the firmware version of the module.</td>
</tr>
<tr>
<td>Module firmware</td>
<td>The firmware revision of the phone module.</td>
</tr>
<tr>
<td>IMEI</td>
<td>The International Mobile Station Equipment Identity number used to uniquely identify a mobile device.</td>
</tr>
<tr>
<td><strong>LAN</strong></td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td>The IP address and subnet mask of the router.</td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address of the router.</td>
</tr>
<tr>
<td>Ethernet port status</td>
<td>Displays the current status of the Ethernet port and its operating speed.</td>
</tr>
<tr>
<td><strong>Cellular connection status</strong></td>
<td></td>
</tr>
<tr>
<td>SIM Status</td>
<td>Displays the activation status of the router on the carrier network.</td>
</tr>
<tr>
<td>Signal strength (dBm)</td>
<td>The current signal strength measured in dBm.</td>
</tr>
<tr>
<td>Network registration status</td>
<td>The status of the router’s registration for the current network.</td>
</tr>
<tr>
<td>Operator selection</td>
<td>The mode used to select an operator network.</td>
</tr>
<tr>
<td>Current operator</td>
<td>The current operator network in use.</td>
</tr>
<tr>
<td>Roaming status</td>
<td>The roaming status of the router.</td>
</tr>
<tr>
<td>Allowed bands</td>
<td>The bands to which the router may connect.</td>
</tr>
<tr>
<td>Current band</td>
<td>The current band being used by the router.</td>
</tr>
<tr>
<td>Coverage</td>
<td>The type of mobile coverage being received by the router.</td>
</tr>
<tr>
<td><strong>WWAN connection status</strong></td>
<td></td>
</tr>
<tr>
<td>Profile name</td>
<td>The name of the active profile.</td>
</tr>
<tr>
<td>Status</td>
<td>The connection status of the active profile.</td>
</tr>
<tr>
<td>Default profile</td>
<td>Indicates whether the current profile in use is the default profile.</td>
</tr>
<tr>
<td>WWAN IP</td>
<td>The IP address assigned by the mobile broadband carrier network.</td>
</tr>
<tr>
<td>DNS server</td>
<td>The primary and secondary DNS servers for the WWAN connection.</td>
</tr>
<tr>
<td>APN</td>
<td>The Access Point Name currently in use.</td>
</tr>
<tr>
<td>Connection uptime</td>
<td>The length of time of the current mobile connection session.</td>
</tr>
<tr>
<td><strong>Advanced status</strong></td>
<td></td>
</tr>
<tr>
<td>Mobile country code</td>
<td>The Mobile Country Code (MCC) of the router.</td>
</tr>
<tr>
<td>Mobile network code</td>
<td>The Mobile Network Code (MNC) of the router.</td>
</tr>
<tr>
<td>Signal quality (Ec/N0)</td>
<td>A measurement of the portion of the received signal that is usable. This is the signal strength minus the signal noise level.</td>
</tr>
<tr>
<td>Received signal code power (RSCP)</td>
<td>The power level of the signal on the current connection’s particular channel.</td>
</tr>
<tr>
<td>HSPDA category</td>
<td>Displays the HSUPA category (1-5) for the current uplink.</td>
</tr>
<tr>
<td>HSDPA category</td>
<td>Displays the HSDPA category (1-8) for the current downlink.</td>
</tr>
<tr>
<td>SIM ICCID</td>
<td>The Integrated Circuit Card Identifier of the SIM card used with the router, a unique number up to 19 digits in length.</td>
</tr>
<tr>
<td>Primary scrambling code (PSC)</td>
<td>The Primary scrambling code for the current signal.</td>
</tr>
<tr>
<td>Location area code (LAC)</td>
<td>The ID of the cell tower grouping the current signal is broadcasting from.</td>
</tr>
<tr>
<td>Routing area code (RAC)</td>
<td>A subdivision of the location area used with GPRS.</td>
</tr>
<tr>
<td>IMSI</td>
<td>The International mobile subscriber identity is a unique identifier of the user of a cellular network.</td>
</tr>
<tr>
<td>Cell ID</td>
<td>A unique code that identifies the base station from within the location area of the current mobile network signal.</td>
</tr>
<tr>
<td>Channel number (UARFCN)</td>
<td>The channel number of the current 3G/2G connection.</td>
</tr>
<tr>
<td>Module PRID Revision</td>
<td>Module version used for customization.</td>
</tr>
<tr>
<td>Module PRID PRI part number</td>
<td>The part number of the Module PRID.</td>
</tr>
</tbody>
</table>

Table 7: 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.

Figure 8 – Data connection settings
### Data connection item details

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data connection</td>
<td>Toggles the transparent bridge function on and off.</td>
</tr>
<tr>
<td>Transparent Bridge (PPPoE)</td>
<td>Toggles the transparent bridge function on and off.</td>
</tr>
<tr>
<td>Profile name list</td>
<td>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.</td>
</tr>
<tr>
<td>Status</td>
<td>Toggles the corresponding profile on and off. If your carrier supports it, two profiles may be turned on simultaneously.</td>
</tr>
<tr>
<td>APN</td>
<td>The APN configured for the corresponding profile.</td>
</tr>
<tr>
<td>Username</td>
<td>The username used to log on to the corresponding APN.</td>
</tr>
<tr>
<td>Roaming settings</td>
<td>When set to ON, the router will allow local devices to access the Wireless WAN network when 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.</td>
</tr>
</tbody>
</table>

### 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.

![Data connection profile settings](image-url)
2. Click the **Profile** toggle key to turn the profile on. Additional settings appear.

### Data connection profile settings

- **Profile**
  - **Profile name**: Profile2
  - **Automatic APN selection**

### APN settings

<table>
<thead>
<tr>
<th><strong>APN</strong></th>
<th><strong>Username</strong></th>
<th><strong>Password</strong></th>
</tr>
</thead>
</table>

### Authentication type

- **CHAP**
- **PAP**

<table>
<thead>
<tr>
<th><strong>Reconnect delay</strong></th>
<th><strong>30</strong> (30-65535) seconds</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Reconnect retries</strong></th>
<th><strong>0</strong></th>
<th>(0-65535, 0=Unlimited)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Metric</strong></th>
<th><strong>20</strong></th>
<th>(0-65533)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>MTU</strong></th>
<th><strong>1500</strong></th>
<th>(1226-1400)</th>
</tr>
</thead>
</table>

### NAT masquerading settings

- **ON**
- **OFF**

---

3. In the **Profile name** field, enter a name for the profile. This name is only used to identify the profile on the router.

4. 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.

5. 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.

6. Next to **Authentication type**, select either CHAP or PAP depending on the type of authentication used by your provider.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.
12. 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.

13. 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.

![WWAN connection status](image-url)
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.

![Band settings](image)

**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:

<table>
<thead>
<tr>
<th>NTC-6908</th>
<th>NTC-6908-02</th>
<th>NTC-6520</th>
</tr>
</thead>
<tbody>
<tr>
<td>UMTS 850MHz, 2G</td>
<td>GSM 900/1800</td>
<td>All bands</td>
</tr>
<tr>
<td>UMTS 850MHz Only</td>
<td>WCDMA 900/2100</td>
<td>WCDMA 2100</td>
</tr>
<tr>
<td>2G</td>
<td>WCDMA 900/2100</td>
<td>WCDMA 850/1900</td>
</tr>
<tr>
<td>WCDMA All</td>
<td>2G</td>
<td>GSM 850/1900</td>
</tr>
<tr>
<td>Autoband</td>
<td>WCDMA 850</td>
<td>GSM ALL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>NTC-6908-02</th>
<th>NTC-6520</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSM 900/1800</td>
<td>WCDMA 2100</td>
<td>WCDMA 2100 GSM 850/1900</td>
</tr>
<tr>
<td>WCDMA 900/2100</td>
<td>WCDMA 850/1900</td>
<td>WCDMA 850/1900</td>
</tr>
<tr>
<td>2G</td>
<td>WCDMA 850/2100</td>
<td>WCDMA 850</td>
</tr>
<tr>
<td>WCDMA ALL</td>
<td>WCDMA 850</td>
<td>WCDMA 850</td>
</tr>
<tr>
<td>Autoband</td>
<td>WCDMA 900</td>
<td>WCDMA 900/2100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>NTC-6520</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSM 850/1900</td>
<td>WCDMA 2100</td>
</tr>
<tr>
<td>WCDMA 900/1800</td>
<td>WCDMA 850</td>
</tr>
<tr>
<td>WCDMA 850/1900</td>
<td>WCDMA 900</td>
</tr>
<tr>
<td>WCDMA 900/2100</td>
<td></td>
</tr>
<tr>
<td>WCDMA 850/1900</td>
<td></td>
</tr>
</tbody>
</table>

**Table 9 - 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 to 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.

![Operator settings](Image)

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

<table>
<thead>
<tr>
<th>Operator name list</th>
<th>MCC</th>
<th>MNC</th>
<th>Operator status</th>
<th>Network type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telstra</td>
<td>563</td>
<td>01</td>
<td>Current</td>
<td>UMTS (3G)</td>
</tr>
<tr>
<td>Telstra</td>
<td>563</td>
<td>01</td>
<td>Available</td>
<td>GSM (2G)</td>
</tr>
<tr>
<td>Vodafone AU</td>
<td>565</td>
<td>03</td>
<td>Forbidden</td>
<td>GSM (2G)</td>
</tr>
<tr>
<td>Yes OPTUS</td>
<td>565</td>
<td>02</td>
<td>Forbidden</td>
<td>UMTS (3G)</td>
</tr>
<tr>
<td>Yes OPTUS</td>
<td>565</td>
<td>02</td>
<td>Forbidden</td>
<td>UMTS (3G)</td>
</tr>
<tr>
<td>Vodafone AU</td>
<td>565</td>
<td>03</td>
<td>Forbidden</td>
<td>UMTS (3G)</td>
</tr>
</tbody>
</table>

![Detected operator list](Image)

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.
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:
Figure 16 - SIM security settings - SIM unlock successful

Success!
The SIM unlock was successful

PIN settings

SIM OK: ✔
PIN remembered
Retries remaining: 3

PIN protection

Change PIN

Current PIN

Confirm current PIN

Remember PIN

Save
Enabling/Disabling SIM PIN protection
The security PIN protection can be turned on or off using the PIN protection toggle key.

![PIN settings](image-url)

Figure 17 - 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.

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

![PIN settings](image)
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.
LAN

LAN configuration

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

The default IP of the Ethernet port is 192.168.20.1 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-6000 Series router hands out its own IP address (e.g. 192.168.20.1) as the DNS server address to LAN clients. The downstream clients then send DNS requests to the NTC-6000 Series 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-6000 Series 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-6000 Series 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-6000 Series router are able to communicate with the DHCP server when DHCP relay is enabled. This enables the NTC-6000 Series 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.

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).
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP start range</td>
<td>Sets the first IP address of the DHCP range</td>
</tr>
<tr>
<td>DHCP end range</td>
<td>Sets the last IP address of the DHCP range</td>
</tr>
<tr>
<td>DHCP lease time (seconds)</td>
<td>The length of time in seconds that DHCP allocated IP addresses are valid</td>
</tr>
<tr>
<td>Default domain name suffix</td>
<td>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</td>
</tr>
<tr>
<td>DNS server 1 IP address</td>
<td>Specifies the primary DNS (Domain Name System) server’s IP address.</td>
</tr>
<tr>
<td>DNS server 2 IP address</td>
<td>Specifies the secondary DNS (Domain Name System) server’s IP address.</td>
</tr>
<tr>
<td>WINS server 1 IP address</td>
<td>Specifies the primary WINS (Windows Internet Name Service) server IP address</td>
</tr>
<tr>
<td>WINS server 2 IP address</td>
<td>Specifies the secondary WINS (Windows Internet Name Service) server IP address</td>
</tr>
<tr>
<td>NTP server (Option 42)</td>
<td>Specifies the IP address of the NTP (Network Time Protocol) server</td>
</tr>
<tr>
<td>TFTP Server (Option 66)</td>
<td>Specifies the TFTP (Trivial File Transfer Protocol) server</td>
</tr>
<tr>
<td>DHCP option 150</td>
<td>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.</td>
</tr>
<tr>
<td>DHCP option 160</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

### Address reservation list

<table>
<thead>
<tr>
<th>Computer name</th>
<th>MAC address</th>
<th>IP address</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>ON</td>
</tr>
</tbody>
</table>

*Figure 24 – 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.

<table>
<thead>
<tr>
<th>Computer name</th>
<th>MAC address</th>
<th>IP address</th>
<th>Expiry time</th>
</tr>
</thead>
<tbody>
<tr>
<td>xxxxxx</td>
<td>00:21:0b:1a:80:1e</td>
<td>192.168.1.146</td>
<td>Thursday, 5 September 2013 12:02:59 PM</td>
</tr>
</tbody>
</table>

Figure 25 - Dynamic DHCP client list
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 26 - 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.
Active routing list
Static routes are displayed in the Active routing list.

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

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.

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>` (e.g. `arp -d 192.168.20.1`) 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-6908](http://support.netcommwireless.com/product/m2m-wireless-series/ntc-6908) 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.

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 Source 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 network 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.
To delete a port forwarding rule, click the \(\times\) 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.

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.
MAC / IP / Port filtering

The MAC/IP/Port filter feature allows you to 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.

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.
5. Enter the details of the rule in the section that is displayed and click the Save button.
6. 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.

### Table 10 - Current MAC/IP/Port filtering rules in effect

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

Figure 38 - MAC/IP/Port filter settings

Figure 39 - 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-6000 Series 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.

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

IPSec profile [ON OFF]
Profile name

Remote IPSec address
Remote LAN address: 0 0 0 0 0
Remote LAN subnet mask: 255 255 255 0
Local LAN address: 0 0 0 0 0
Local LAN subnet mask: 255 255 255 0

Encapsulation type: ESP
IKE mode: Main
PFS: ON
IKE encryption: Any
IKE hash: Any
IPSec encryption: Any
IPSec hash: Any
DH group: Any

DPD action: Hold
DPD keep alive time: 10 secs
DPD timeout: 60 secs
IKE re-key time: 3600 [0-78400, 0=Unlimited] secs
SA life time: 28800 [0-78400, 0=Unlimited] secs
Key mode: Pre-shared keys

Pre-shared key
Remote ID: (xy.sample.com or blank)
Local ID: (xy.sample.com or blank)

Save  Exit

Figure 41 – IPSec profile edit
The following table describes each of the fields of the IPSec VPN Connection Settings page.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec profile</td>
<td>Enables or disables the VPN profile.</td>
</tr>
<tr>
<td>Profile name</td>
<td>A name used to identify the VPN connection profile.</td>
</tr>
<tr>
<td>Remote IPSec address</td>
<td>The IP address or domain name of the IPSec server.</td>
</tr>
<tr>
<td>Remote LAN address</td>
<td>Enter the IP address of the remote network for use on the VPN connection.</td>
</tr>
<tr>
<td>Remote LAN subnet mask</td>
<td>Enter the subnet mask in use on the remote network.</td>
</tr>
<tr>
<td>Local LAN address</td>
<td>Enter the IP address of the local network for use on the VPN connection.</td>
</tr>
<tr>
<td>Local LAN subnet mask</td>
<td>Enter the subnet mask in use on the local network.</td>
</tr>
<tr>
<td>Encapsulation type</td>
<td>Select the encapsulation protocol to use with the VPN connection. You can choose ESP, AH or Any.</td>
</tr>
<tr>
<td>IKE mode</td>
<td>Select the IKE mode to use with the VPN connection. You can choose Main, Aggressive or Any.</td>
</tr>
<tr>
<td>PFS</td>
<td>Choose whether Perfect Forward Secrecy is ON or OFF for the VPN connection.</td>
</tr>
<tr>
<td>IKE encryption</td>
<td>Select the cipher type to use for the Internet Key Exchange.</td>
</tr>
<tr>
<td>IKE hash</td>
<td>Select the IKE Hash type to use for the VPN connection. The hash is used for authentication of packets for the key exchange.</td>
</tr>
<tr>
<td>IPSec encryption</td>
<td>Select the IPSec encryption type to use with the VPN connection.</td>
</tr>
<tr>
<td>IPSec hash</td>
<td>Select the IPSec hash type to use for the VPN connection. The hash is used for authentication of packets for the VPN connection.</td>
</tr>
<tr>
<td>DH group</td>
<td>Select the desired Diffie-Hellman group to use. Higher groups are more secure but also require longer to generate a key.</td>
</tr>
<tr>
<td>DPD action</td>
<td>Select the desired Dead Peer Detection action. This is the action to take when a dead Internet Key Exchange Peer is detected.</td>
</tr>
<tr>
<td>DPD keep alive time</td>
<td>Enter the time in seconds for the interval between Dead Peer Detection keep alive messages.</td>
</tr>
<tr>
<td>DPD timeout</td>
<td>Enter the time in seconds of no response from a peer before Dead Peer Detection times out.</td>
</tr>
<tr>
<td>IKE re-key time</td>
<td>Enter the time in seconds between changes of the encryption key. To disable changing the key, set this to 0.</td>
</tr>
<tr>
<td>SA life time</td>
<td>Enter the time in seconds for the security association lifetime.</td>
</tr>
<tr>
<td>Key mode</td>
<td>Select the type of key mode in use for the VPN connection. You can select from: Pre Shared Key, RSA keys, Certificates.</td>
</tr>
<tr>
<td>Pre-shared key</td>
<td>The pre-shared key is the key that peers used to authenticate each other for Internet Key Exchange.</td>
</tr>
<tr>
<td>Remote ID</td>
<td>Specifies the domain name of the remote network.</td>
</tr>
<tr>
<td>Local ID</td>
<td>Specifies the domain name of the local network.</td>
</tr>
<tr>
<td>Update Time</td>
<td>Displays the last time the key was updated.</td>
</tr>
<tr>
<td>Local RSA Key Upload</td>
<td>Select the RSA key file for the local router here by clicking the Browse button.</td>
</tr>
<tr>
<td>Remote RSA Key Upload</td>
<td>Select the RSA key file for the remote router here by clicking the Browse button.</td>
</tr>
<tr>
<td>Private key Passphrase</td>
<td>The Private key passphrase of the router is the passphrase used when generating the router’s private key using OpenSSL CA.</td>
</tr>
<tr>
<td>Key / Certificate</td>
<td>Select the type of key or certificate to use for authentication. You can select Local private key, Local public certificate, CA certificate, CRL certificate.</td>
</tr>
<tr>
<td>IPSec Certificate Upload</td>
<td>Select the IPSec certificate to upload by clicking the Browse button.</td>
</tr>
</tbody>
</table>

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-6908](http://support.netcommwireless.com/product/m2m-wireless-series/ntc-6908) 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, 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-6908 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 connections is displayed.

![OpenVPN server list](image)

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

OpenVPN Server

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. Select 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. Next to Diffie-Hellman parameters, select appropriate encryption key size then click the Generate DH button. This will create an encryption key to secure your OpenVPN connection. Default key size is (1024) bit.
7. Under Server Certificates, enter the required details. All fields must be completed. The Country field must consist of two characters only. When the details have been entered, click the Generate CA certificate button to generate the Certificate Authority (CA) certificate based on this information.
8. Under the Server certificates section, select the Authentication type that you would like to use for the OpenVPN Server.

Note: The Diffie-Hellman parameters can take up to 10 minutes to generate. Please be patient.
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.

![Certificate Management](image)

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

Profile name
Type
Server port
VPN network address
VPN network subnet mask
Diffie-Hellman parameters

Server certificates
Not before
Net after
Country
State
City
Organisation
Email

Authentication type
— Certificate
— Username / Password

Certificate management
Certificate
Name
Country
State
City
Organisation
Email

Generate
Revokes
Download P12
Download TGZ

Remote network address
Remote network subnetmask

Set network information
Save
Exit

Figure 44 – 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.

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.

![Certificate upload](image)

Username / Password Authentication
Enter the username and password to authenticate with the OpenVPN server.

![Username / Password](image)

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.

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.
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 Tunnelling 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.

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

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 65335 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 65335.

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-6908](http://support.netcommwireless.com/product/m2m-wireless-series/ntc-6908) 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.

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

3. Click the Enable GRE Tunnel toggle key to switch it to the ON position.
4. In the **Profile name** field, 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-6908](http://support.netcommwireless.com/product/m2m-wireless-series/ntc-6908) 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.

![DDNS configuration screenshot](image)

Figure 53 – 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-6000 Series 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.

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, the built-in serial 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 send the GPS data received by the module (in NMEA format) through a serial port (by means of a USB-to-Serial cable). 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
- GPS Data (for devices with GPS receiver)

![Endpoints list](image)
To create an endpoint:

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

   ![Figure 56 - Creating an endpoint](image)

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.
   - **Serial port (generic)**: This creates a generic serial port as an endpoint defaulting to the commonly used settings as shown below.

   ![Figure 57 - Serial port (generic) endpoint configuration](image)

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

   ![Figure 58 - TCP server endpoint configuration](image)
**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 configuration](image)

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

![UDP server endpoint configuration](image)

**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 configuration](image)
GPS data: This creates a GPS data endpoint.

4. Click the OK button. The router displays a screen with configuration options for your chosen endpoint type.
5. Enter the options for your endpoint as required.
6. Click the Save button. The Endpoints list is displayed with the newly created endpoint listed and a summary of the settings your configured.

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:
7. Click the +Add button on the right side of the page.

The Edit data stream page is displayed.
8. In the Data stream name field, enter a name for the Data stream.
9. 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.
10. 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 GPS data out of the built-in serial port. 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.

![Edit data stream](image)

**Figure 65 - Edit data stream**

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

![Data stream list](image)

**Figure 66 - Data stream list**
Legacy data managers

Modem emulator

Modem emulator allows you to connect legacy equipment such as an RTU or PLC to the serial port of the router in place of a traditional dial-up modem. The NTC-6000 series router emulates the dial-up modem’s behaviour and passes the serial data over the IP network.

Figure 67 - Modem emulator
<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Modern emulator</strong></td>
<td></td>
</tr>
<tr>
<td>Activate</td>
<td>Turns on or off the modem emulator function of the router.</td>
</tr>
<tr>
<td>Serial port name</td>
<td>The device name of the serial port.</td>
</tr>
<tr>
<td>Serial port status</td>
<td>The configuration status of the serial port. This will display whether there are any conflicts with the serial port preventing modem emulator from working properly.</td>
</tr>
<tr>
<td><strong>Modern settings</strong></td>
<td></td>
</tr>
<tr>
<td>Baud rate</td>
<td>The serial (V.24) port baud rate. By default the serial line format is 8 data bits, No parity, 1 Stop bit. Refer to the AT (V.250) AT Command Manual if you need to change the serial line format.</td>
</tr>
<tr>
<td>Inter character timeout</td>
<td>The Modern emulator buffers any bytes received from the serial port until either 512 bytes have been received or no bytes have been received for “Inter Character Timeout” milliseconds, it will then send any bytes in the buffer to the remote host.</td>
</tr>
<tr>
<td>Id</td>
<td>When the ID field is not blank (empty) the defined ID will be sent to the remote host as follows: For UDP the 1st &lt;n&gt; bytes of each datagram sent will be set to the contents of the ID field, data follows immediately after the ID for TCP the ID is transmitted once immediately after the connection is established</td>
</tr>
<tr>
<td>Ignore string</td>
<td>When the “Ignore String” field is not blank (empty) the router will strip any character sequence that matches the “Ignore String” from the data stream received from the serial port.</td>
</tr>
<tr>
<td><strong>Connection settings</strong></td>
<td></td>
</tr>
<tr>
<td>Connect to</td>
<td>Determines how the router behaves when it receives an “ATD” command on the serial port.</td>
</tr>
<tr>
<td>DTR action</td>
<td>Determines how the router responds to change of state of the serial port DTR line</td>
</tr>
<tr>
<td>Flow control</td>
<td>• Off - Serial port flow control off</td>
</tr>
<tr>
<td>RI action</td>
<td>Determines how the router controls the state of the serial port RI line</td>
</tr>
<tr>
<td>Circuit auto answer rings</td>
<td>Sets the number of incoming rings after which the router will answer incoming circuit switched data calls.</td>
</tr>
<tr>
<td>Auto dial number</td>
<td>Sets the number the router will dial if DTR Auto Dial is enabled ad DTR changes state.</td>
</tr>
<tr>
<td><strong>Profile-specific settings (these items may be configured separately for each of the 4 connection profiles)</strong></td>
<td></td>
</tr>
<tr>
<td>Profile</td>
<td>Choose the profile that you want to configure.</td>
</tr>
<tr>
<td>Remote Host</td>
<td>In client mode (router connects to host) this is the remote host to which the router will connect. In server mode (remote host connects to router) the router will only accept incoming connections from the specified host. If you specify 0.0.0.0 the router will accept incoming connections from any host.</td>
</tr>
<tr>
<td>Port</td>
<td>TCP/UDP port number to use</td>
</tr>
<tr>
<td>Local encoding</td>
<td>Refer to the AT (V.250) Command Manual for details of this parameter, this is normally disabled.</td>
</tr>
<tr>
<td>Mode</td>
<td>Selects the mode of operation for the chosen profile. Mode may be TCP, UDP or GMTP.</td>
</tr>
<tr>
<td>Auto answer</td>
<td>When enabled the router accepts incoming connections (enables server mode)</td>
</tr>
</tbody>
</table>

Table 12 - Modern emulator options
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.

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

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

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. 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 2 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.

Periodic reboot

<table>
<thead>
<tr>
<th>First destination address</th>
<th>Second destination address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Periodic Ping timer</td>
<td>Periodic Ping accelerated timer</td>
</tr>
<tr>
<td>Fail count</td>
<td>(0=disable, 60-65535) secs</td>
</tr>
<tr>
<td>Force reboot every</td>
<td>Randomise reboot time</td>
</tr>
<tr>
<td></td>
<td>(0=disable, 1-65535) times</td>
</tr>
</tbody>
</table>

Figure 69 - 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. Should the watchdog 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.
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**.
SNMP

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

![SNMP Configuration Screen](image)

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 router's 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](image)

Figure 72 - 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.

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.
GPS (NTC-6908 only)

If using NTC-6908 routers, you can make use of location-based services, monitor field deployed hardware or find your current location. The GPS Status window provides up to date information about the current location and the current GPS signal conditions (position dilution of precision (PDOP), horizontal dilution of precision (HDOP) and vertical dilution of precision (VDOP)) of the router.

GPS configuration

To access the GPS configuration screen, select the Services item from the top menu bar then the GPS item on the left. Finally, select the GPS configuration menu item.

To use the GPS function, set the GPS operation toggle key to ON and click the Save button.

GPS configuration

<table>
<thead>
<tr>
<th>GPS operation</th>
<th>ON</th>
<th>OFF</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Save</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

GPS applications

<table>
<thead>
<tr>
<th>Google maps</th>
<th></th>
<th></th>
</tr>
</thead>
</table>

GPS status

Positioning data source: Stand-alone GPS

Date & Time: Friday, 13 December 2013, 3:48:02 PM

Latitude & Longitude: 33.46° 42.901° S, 131.08° 94.124° E

Altitude & GEOID height: 82.3 m, 24.6 m

Ground speed: 0.0 km/h, 0.0 knots

PDOP & HDOP & VDOP: 2.1, 1.9, 0.9

Standalone GPS device status: Normal

Number of satellites: 11

Satellites status

<table>
<thead>
<tr>
<th>Index</th>
<th>In Use</th>
<th>PRN</th>
<th>SNR</th>
<th>Elevation</th>
<th>Azimuth</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✔️</td>
<td>01</td>
<td>30</td>
<td>17</td>
<td>129</td>
</tr>
<tr>
<td>2</td>
<td>✔️</td>
<td>04</td>
<td>24</td>
<td>25</td>
<td>016</td>
</tr>
<tr>
<td>3</td>
<td>✔️</td>
<td>07</td>
<td>25</td>
<td>05</td>
<td>042</td>
</tr>
<tr>
<td>4</td>
<td>✔️</td>
<td>08</td>
<td>25</td>
<td>35</td>
<td>049</td>
</tr>
<tr>
<td>5</td>
<td>✔️</td>
<td>09</td>
<td>33</td>
<td>42</td>
<td>040</td>
</tr>
<tr>
<td>6</td>
<td>✔️</td>
<td>15</td>
<td>19</td>
<td>26</td>
<td>257</td>
</tr>
<tr>
<td>7</td>
<td>✔️</td>
<td>17</td>
<td>20</td>
<td>83</td>
<td>170</td>
</tr>
<tr>
<td>8</td>
<td>✔️</td>
<td>28</td>
<td>35</td>
<td>41</td>
<td>122</td>
</tr>
<tr>
<td>9</td>
<td>✔️</td>
<td>11</td>
<td>N/A</td>
<td>02</td>
<td>139</td>
</tr>
<tr>
<td>10</td>
<td>✔️</td>
<td>24</td>
<td>N/A</td>
<td>14</td>
<td>222</td>
</tr>
<tr>
<td>11</td>
<td>✔️</td>
<td>26</td>
<td>N/A</td>
<td>37</td>
<td>302</td>
</tr>
<tr>
<td>12</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Figure 74 – GPS configuration
The **Google maps** button provides a quick shortcut to show your router’s current position on a map.

**Mobile Station Based Assisted GPS configuration**

To access the Mobile Station Based Assisted GPS configuration screen, select the **Services** item from the top menu bar then the **GPS** item on the left. Finally, select the **MSB (A-GPS)** menu item. This function is only available on models with built-in GPS capability.

Mobile Station Based Assisted GPS (MSB A-GPS) enables your router to download GNSS data which supply orbital data to GPS receiver, enabling it to lock to the satellites more rapidly. The GNSS data is stored on the router to assist the GPS in locating the router.

To set up automatic updates of GNSS data, set the **A-GPS Enable** toggle key to the **ON** position and use the drop down lists to configure the automatic retry options. Each retry, the router checks for an updated GNSS data file and downloads the GNSS data if newer than the currently stored data.

**Note:** When new GNSS data is available and the router performs an update, up to 40MB of data may be downloaded. Please keep this in mind if your mobile broadband plan has usage restrictions.

![Mobile Station Based Assisted GPS configuration](image)

**Table 13 - Mobile Station Based Assisted GPS configuration options**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-GPS Enable</td>
<td>Enables or disables the mobile station based assisted GPS function.</td>
</tr>
<tr>
<td>Maximum Retry Count</td>
<td>Sets the maximum number of times the router should attempt to triangulate its position.</td>
</tr>
<tr>
<td>Retry delay (minute)</td>
<td>Sets the number of minutes the router should wait between attempts to triangulate its position.</td>
</tr>
<tr>
<td>Automatic Update Period (day)</td>
<td>Sets the number of days that the router should automatically update the A-GPS data. The maximum update period is 7 days.</td>
</tr>
</tbody>
</table>

The **GNSS data last update** field represents the time that the GNSS data file was created while the **GNSS data expires** field indicates the time that this data is valid until. The **A-GPS last update** field specifies the last time the router attempted to retrieve an update to the GNSS data.

You may manually force the router to check for an update regardless of the next scheduled update time by clicking the **Update Now** button.

When you have finished configuring the settings, click the **Save** button to save the changes.
Odometer

To access the Odometer screen, select the **Services** item from the top menu bar then the **GPS** item on the left. Finally, select the **Odometer** menu item.

The GPS may be used to record the distance that the router has travelled. To do this, set the **Odometer** toggle key to the **ON** position as in the screenshot below. You can toggle the unit of measurement by clicking the **Display imperial / Display metric** button. The threshold setting adjusts the router’s sensitivity to movement so that movement within the specified radius from the starting point does not register as distance travelled. When you have finished configuring the Odometer settings, click the **Save** button to ensure the settings are stored on the router.

![Odometer options](image)

### Table 14 - Odometer configuration options

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Odometer reading</td>
<td>The number of metres/kilometres that the device has travelled since the time listed in the Odometer start time field.</td>
</tr>
<tr>
<td>Display imperial / Display metric</td>
<td>Toggles the Odometer reading between metric and imperial measurements.</td>
</tr>
<tr>
<td>Odometer start time</td>
<td>The time that recording of distance travelled began.</td>
</tr>
<tr>
<td>Reset odometer</td>
<td>Resets the odometer reading to 0 and the Odometer start time to the current time.</td>
</tr>
<tr>
<td>Odometer</td>
<td>Toggles the Odometer function on and off.</td>
</tr>
<tr>
<td>Threshold</td>
<td>Specifies the minimum distance that the router must travel from its current position before the Odometer reading increases.</td>
</tr>
</tbody>
</table>

*Figure 76 – Odometer options*
### SMS messaging

The NTC-6000 Series 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-6000 Series router to download and install a firmware upgrade.
- Ability to trigger the NTC-6000 Series router to download and apply a configuration file.

To access the SMS messaging functions of the NTC-6000 Series 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.

*Figure 77 - General SMS Configuration*
### Table 15: SMS Setup Settings

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General SMS configuration</strong></td>
<td></td>
</tr>
<tr>
<td>SMS messaging</td>
<td>Toggles the SMS functionality of the router on and off.</td>
</tr>
<tr>
<td>Messages per page (10-50)</td>
<td>The number of SMS messages to display per page. Must be a value between 10 and 50.</td>
</tr>
<tr>
<td>Encoding scheme</td>
<td>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.</td>
</tr>
<tr>
<td><strong>SMS forwarding configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Forwarding</td>
<td>Toggles the SMS forwarding function of the router on and off.</td>
</tr>
<tr>
<td>Redirect to mobile</td>
<td>Enter a mobile number as the destination for forwarded SMS messages.</td>
</tr>
<tr>
<td>TCP server address</td>
<td>Enter an IP address or domain name as the destination for forwarded SMS messages using TCP.</td>
</tr>
<tr>
<td>TCP port</td>
<td>The TCP port on which to connect to the remote destination.</td>
</tr>
<tr>
<td>UDP server address</td>
<td>Enter an IP address or domain name as the destination for forwarded SMS messages using UDP.</td>
</tr>
<tr>
<td>UDP port</td>
<td>The UDP port on which to connect to the remote destination.</td>
</tr>
</tbody>
</table>

**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.

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 79 - SMS Inbox**

**Figure 80 - SMS Outbox**

<table>
<thead>
<tr>
<th>ICON</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Forward button. Click this button to open a new message window where you can forward the corresponding message to another recipient.</td>
</tr>
<tr>
<td>📩</td>
<td>Reply button. Click this button to open a new message window where you can reply to the sender.</td>
</tr>
<tr>
<td>📌</td>
<td>Add to White list. Click this button to add the sender’s mobile number to the white list on the router.</td>
</tr>
<tr>
<td>✗</td>
<td>Delete button. Click this button to delete the corresponding message.</td>
</tr>
<tr>
<td>🔄</td>
<td>Refresh button. Click this button to refresh the inbox or outbox to see new messages.</td>
</tr>
</tbody>
</table>

**Table 16 - 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.

![Figure 81 - SMS diagnostics and command execution configuration](image)

**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-6000 Series router will automatically reply to certain types of commands received, such as get commands, or execute commands. However acknowledgement replies from the NTC-6000 Series 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 acknowledgement 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 is /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.

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.

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:

- password6576 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:

<table>
<thead>
<tr>
<th>TYPE</th>
<th>SMS CONTENTS</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>get command</td>
<td>&quot;VARIABLE=VALUE&quot;</td>
<td></td>
</tr>
<tr>
<td>set command</td>
<td>&quot;Successfully set VARIABLE to VALUE&quot;</td>
<td>Only sent if the acknowledgment message function is enabled</td>
</tr>
<tr>
<td>execute command</td>
<td>&quot;Successfully executed command COMMAND&quot;</td>
<td></td>
</tr>
</tbody>
</table>

Table 17: 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.

<table>
<thead>
<tr>
<th>#</th>
<th>COMMAND NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>reboot</td>
<td>Immediately performs a soft reboot.</td>
</tr>
<tr>
<td>2</td>
<td>pdpcycle</td>
<td>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.</td>
</tr>
<tr>
<td>3</td>
<td>pdpdown</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>pdpup</td>
<td>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.</td>
</tr>
<tr>
<td>5</td>
<td>factorydefaults</td>
<td>Performs a factory reset on the router. Be aware that this command also clears the SMS white list on the router.</td>
</tr>
<tr>
<td>6</td>
<td>download</td>
<td>Performs a download and install of a Firmware Upgrade (.cdi), Config File (.tar.gz) or a help document (.pdf) file. 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. 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. 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. 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 Note: Authenticated FTP addresses may be used following the format as defined in RFC1738, for example: ftp://username:password@serveraddress/directory/filename.cdi</td>
</tr>
<tr>
<td>7</td>
<td>ssh.genkeys</td>
<td>Instructs the router to generate new public SSH keys.</td>
</tr>
<tr>
<td>8</td>
<td>ssh.clearkeys</td>
<td>Instructs the router to clear the client public SSH key files.</td>
</tr>
</tbody>
</table>

Table 18 - 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.

<table>
<thead>
<tr>
<th>COMMAND NAME</th>
<th>EXAMPLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>get status</td>
<td>get status</td>
<td>Returns the Module firmware version, LAN IP Address, Network State, Network operator and RSSI.</td>
</tr>
<tr>
<td>get sessionhistory</td>
<td>get sessionhistory</td>
<td>Returns the time and date of recent sessions along with the total amount of data sent and received for each session.</td>
</tr>
<tr>
<td>set syslogserver</td>
<td>set syslogserver=123.45.67.89:514</td>
<td>Sets a remote syslog server IP or hostname and port.</td>
</tr>
<tr>
<td>get plmnscan</td>
<td>get plmnscan</td>
<td>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.</td>
</tr>
<tr>
<td>get forceplmn</td>
<td>get forceplmn</td>
<td>Sets the operator and network type selection mode (Automatic/Manual), in addition to the MCC and MNC values.</td>
</tr>
<tr>
<td>get pppoe</td>
<td>get pppoe</td>
<td>Returns the PPPoE status, currently configured dial string and service name.</td>
</tr>
<tr>
<td>set pppoe</td>
<td>set pppoe=1, telstra.internet, test</td>
<td>Sets the PPPoE status on, APN to telstra.internet, and service name to test.</td>
</tr>
<tr>
<td>get ledmode</td>
<td>get ledmode</td>
<td>Returns the status of the LED operation mode.</td>
</tr>
<tr>
<td>set ledmode</td>
<td>set ledmode=10</td>
<td>Sets the LED operation mode to be always on or to turn off after the specified number of minutes.</td>
</tr>
<tr>
<td>get ssh.proto</td>
<td>get ssh.proto</td>
<td>Returns the SSH protocol in use.</td>
</tr>
<tr>
<td>set ssh.proto</td>
<td>set ssh.proto=1,2</td>
<td>Sets the SSH Protocol to protocol 1, 2 or both (1,2).</td>
</tr>
<tr>
<td>get ssh.passauth</td>
<td>get ssh.passauth</td>
<td>Returns the status of the SSH Enable password authentication option.</td>
</tr>
<tr>
<td>set ssh.passauth</td>
<td>set ssh.passauth=1</td>
<td>Sets the SSH Enable password authentication option on or off.</td>
</tr>
<tr>
<td>get ssh.keyauth</td>
<td>get ssh.keyauth</td>
<td>Returns the status of the SSH Enable key authentication option.</td>
</tr>
<tr>
<td>set ssh.keyauth</td>
<td>set ssh.keyauth=1</td>
<td>Sets the SSH Enable key authentication option on or off.</td>
</tr>
</tbody>
</table>

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”).

<table>
<thead>
<tr>
<th>#</th>
<th>RDB VARIABLE NAME</th>
<th>SMS VARIABLE NAME</th>
<th>READ/ WRITE</th>
<th>DESCRIPTION</th>
<th>EXAMPLE VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>link.profile.1.enable</td>
<td>profile</td>
<td>RW</td>
<td>Profile</td>
<td>Read: (profile no,apn,user,pass,auth_type,iplocal,status) 1.apn,username,password, chap,202.44.185.111,up</td>
</tr>
<tr>
<td>2</td>
<td>link.profile.1.user</td>
<td>username</td>
<td>RW</td>
<td>3G username</td>
<td>Guest, could also return “null”</td>
</tr>
<tr>
<td>3</td>
<td>link.profile.1.pass</td>
<td>password</td>
<td>RW</td>
<td>3G password</td>
<td>Guest, could also return “null”</td>
</tr>
<tr>
<td>4</td>
<td>link.profile.1.auth_type</td>
<td>authtype</td>
<td>RW</td>
<td>3G Authentication type</td>
<td>“pap” or “chap”</td>
</tr>
<tr>
<td>5</td>
<td>link.profile.1.iplocal</td>
<td>wanip</td>
<td>R</td>
<td>WAN IP address</td>
<td>202.44.185.111</td>
</tr>
<tr>
<td>6</td>
<td>wwan.0.radio.information.signal_strength</td>
<td>rssi</td>
<td>R</td>
<td>3G signal strength</td>
<td>“Rx 500 bytes, Tx 1024 bytes, Total 1524 bytes” or “Rx 0 byte, Tx 0 byte, Total 0 byte” when wwan down</td>
</tr>
<tr>
<td>7</td>
<td>wwan.0.imei</td>
<td>imei</td>
<td>R</td>
<td>IMEI number</td>
<td>3573470500000177</td>
</tr>
<tr>
<td>8</td>
<td>statistics.usage_current</td>
<td>usage</td>
<td>R</td>
<td>3G data usage of current session</td>
<td>“Rx 500 bytes, Tx 1024 bytes, Total 1524 bytes” or “Rx 0 byte, Tx 0 byte, Total 0 byte” when wwan down</td>
</tr>
<tr>
<td>9</td>
<td>statistics.usage_current</td>
<td>wanuptime</td>
<td>R</td>
<td>Up time of current 3G session</td>
<td>1 days 02:30:12 or 0 days 00:00:00 when wwan down</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>NETWORK TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Indicates a 3G network</td>
</tr>
<tr>
<td>1</td>
<td>Indicates a 2G network</td>
</tr>
</tbody>
</table>

Table 22 - Operator status codes returned by get plmnscan SMS command

<table>
<thead>
<tr>
<th>OPERATOR STATUS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Indicates an available operator which may be selected.</td>
</tr>
<tr>
<td>2</td>
<td>Indicates a forbidden operator which may not be selected (applies only to generic SIM cards).</td>
</tr>
<tr>
<td>4</td>
<td>Indicates the currently selected operator.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>AUTHENTICATION</th>
<th>INPUT EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send SMS to change the data connection username</td>
<td>Not required</td>
<td>set username= “NetComm”</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD set username= “NetComm”</td>
</tr>
<tr>
<td>Send SMS to change the data connection password</td>
<td>Not required</td>
<td>set password= “NetComm”</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD set password= “NetComm”</td>
</tr>
<tr>
<td>Send SMS to change the data connection authentication</td>
<td>Not required</td>
<td>set authtype= pap</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD set authtype = pap</td>
</tr>
<tr>
<td>Send SMS to reboot</td>
<td>Not required</td>
<td>execute reboot</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD execute reboot</td>
</tr>
<tr>
<td>Send SMS to check the WAN IP address</td>
<td>Not required</td>
<td>get wanip</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD get wanip</td>
</tr>
<tr>
<td>Send SMS to check the mobile signal strength</td>
<td>Not required</td>
<td>get rssi</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD get rssi</td>
</tr>
<tr>
<td>Send SMS to check the IMEI number</td>
<td>Not required</td>
<td>get imei</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD get imei</td>
</tr>
<tr>
<td>Command Description</td>
<td>Required/Not Required</td>
<td>Example Syntax</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Send SMS to check the current band</td>
<td>Not required</td>
<td>get band</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD get band</td>
</tr>
<tr>
<td>Send SMS to Disconnect (if connected) and reconnect the data connection</td>
<td>Not required</td>
<td>execute pppd</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD execute pppd</td>
</tr>
<tr>
<td>Send SMS to disconnect the data connection</td>
<td>Not required</td>
<td>execute pppd</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD execute pppd</td>
</tr>
<tr>
<td>Send SMS to connect the data connection</td>
<td>Not required</td>
<td>execute pppd</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD execute pppd</td>
</tr>
<tr>
<td>Send multiple get command</td>
<td>Not required</td>
<td>get wanip; get rssi</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD get wanip; get rssi</td>
</tr>
<tr>
<td>Send multiple set command</td>
<td>Not required</td>
<td>set ssh.genkeys=1; set username=test; set auth=pap</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD set ssh.genkeys=1; set username=test; set auth=pap</td>
</tr>
<tr>
<td>Send SMS to reset to factory default settings</td>
<td>Not required</td>
<td>execute factory defaults</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD execute factory defaults</td>
</tr>
<tr>
<td>Send SMS to retrieve status of router</td>
<td>Not required</td>
<td>get status</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD get status</td>
</tr>
<tr>
<td>Send SMS to retrieve the history of the session, including start time, end time and total data usage</td>
<td>Not required</td>
<td>get sessionhistory</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD get sessionhistory</td>
</tr>
<tr>
<td>Send SMS to configure the router to send syslog to a remote syslog server</td>
<td>Not required</td>
<td>set syslogserver=123.209.56.78</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD set syslogserver=123.209.56.78</td>
</tr>
<tr>
<td>Send SMS to wake up the router, turn on the default gateway and trigger the 'connect on demand' profile if in waiting state.</td>
<td>Not required</td>
<td>execute wakeup</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD execute wakeup</td>
</tr>
<tr>
<td>Send SMS to perform firmware upgrade when firmware is located on HTTP server</td>
<td>Not required</td>
<td>execute download <a href="http://download.com:8080/firmware_image.cdi">http://download.com:8080/firmware_image.cdi</a>; execute download <a href="http://download.com:8080/firmware_image_r.cdi">http://download.com:8080/firmware_image_r.cdi</a></td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD execute download <a href="http://download.com:8080/firmware_image.cdi">http://download.com:8080/firmware_image.cdi</a>; PASSWORD execute download <a href="http://download.com:8080/firmware_image_r.cdi">http://download.com:8080/firmware_image_r.cdi</a></td>
</tr>
<tr>
<td>Send SMS to perform firmware upgrade when firmware is located on FTP server</td>
<td>Not required</td>
<td>execute download ftp://username:<a href="mailto:password@download.com">password@download.com</a>/firmware_image.cdi; execute download ftp://username:<a href="mailto:password@download.com">password@download.com</a>/firmware_image_r.cdi</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD execute download ftp://username:<a href="mailto:password@download.com">password@download.com</a>/firmware_image.cdi; PASSWORD execute download ftp://username:<a href="mailto:password@download.com">password@download.com</a>/firmware_image_r.cdi</td>
</tr>
<tr>
<td>Send SMS to download and install IPK package located on HTTP server</td>
<td>Not required</td>
<td>execute download <a href="http://download.com:8080/package.ipk">http://download.com:8080/package.ipk</a></td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD execute download <a href="http://download.com:8080/package.ipk">http://download.com:8080/package.ipk</a></td>
</tr>
<tr>
<td>Send SMS to download and install IPK package located on FTP server</td>
<td>Not required</td>
<td>execute download ftp://username:<a href="mailto:password@download.com">password@download.com</a>:8080/package.ipk</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD execute download ftp://username:<a href="mailto:password@download.com">password@download.com</a>:8080/package.ipk</td>
</tr>
<tr>
<td>Send SMS to turn off PPPoE</td>
<td>Not required</td>
<td>set pppoe=0</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD set pppoe=0</td>
</tr>
<tr>
<td>Send SMS to retrieve the PPPoE status, currently configured dial string and service name</td>
<td>Not required</td>
<td>get pppoe</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD get pppoe</td>
</tr>
<tr>
<td>Send SMS to set the LED mode timeout to 10 minutes</td>
<td>Not required</td>
<td>set ledmode=10</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD set ledmode=10</td>
</tr>
<tr>
<td>Send SMS to retrieve the current LED mode</td>
<td>Not required</td>
<td>get ledmode</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD get ledmode</td>
</tr>
<tr>
<td>Retrieve current SSH protocol</td>
<td>Not required</td>
<td>get ssh.proto</td>
</tr>
<tr>
<td>Feature</td>
<td>Required/Not required</td>
<td>Command</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-----------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Select SSH protocol</td>
<td>Not required</td>
<td>set ssh.proto=1</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD set ssh.proto=1</td>
</tr>
<tr>
<td>Retrieve password authentication status</td>
<td>Not required</td>
<td>get ssh.passauth</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD get ssh.passauth</td>
</tr>
<tr>
<td>Enable/disable password authentication on host</td>
<td>Not required</td>
<td>set ssh.passauth=1 or set ssh.passauth=0</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD set ssh.passauth=1 or PASSWORD set ssh.passauth=0</td>
</tr>
<tr>
<td>Generate set of public/private keys on the host</td>
<td>Not required</td>
<td>execute ssh.genkeys</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD execute ssh.genkeys</td>
</tr>
<tr>
<td>Clear client public keys stored on host</td>
<td>Not required</td>
<td>execute ssh.clearkeys</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>PASSWORD execute ssh.clearkeys</td>
</tr>
</tbody>
</table>

*Table 23: SMS diagnostics example commands*
System

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

System log
The System Log enables you to troubleshoot any issues you may be experiencing with your NTC-6000 Series router. To access the System Log page, click on the System menu. The System Log is displayed.

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++).

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
Enable the log to non-volatile memory option

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.

Use a 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-6000 Series router to output log data to a remote syslog server:

1. Click on the System menu from the top menu bar. The System log item is displayed.
2. Under the Remote syslog server section, enter the IP address or hostname of the syslog server in the IP / Hostname 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. 192.168.20.102:514. If you do not specify a port number, the router will use the default UDP port 514.
3. Click the Save button to save the configuration.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug</td>
<td>Show extended system log messages with full debugging level details.</td>
</tr>
<tr>
<td>Info</td>
<td>Show informational messages only.</td>
</tr>
<tr>
<td>Notice</td>
<td>Show normal system logging information.</td>
</tr>
<tr>
<td>Error</td>
<td>Show error condition messages only.</td>
</tr>
</tbody>
</table>

![Log file](image) Figure 85 - System log

![Table](image) Table 24 - System log detail levels
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.

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.
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-6000 Series router by configuring one router with your desired settings, backing them up to a file and then restoring that file to multiple NTC-6000 Series routers.

![Settings backup and restore](image)

**Figure 87 – 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-6000 Series 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 192.168.20.1 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-6000 Series 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.

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-6000 Series 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_6908_x.x.x.x_r.cdi while the main system firmware image is named ntc_6908_x.x.x.x.cdi.
5. Click the Upload button. The firmware image is uploaded to the storage on the router.
6. Repeat steps 4 and 5 for the main system firmware image.

7. 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.

8. 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.
9. 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.

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

![Figure 92 — Installing main firmware image](image)

11. 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.

<table>
<thead>
<tr>
<th>Application name</th>
<th>Version</th>
<th>Architecture</th>
<th>Time installed</th>
<th>Package details</th>
<th>Uninstall</th>
</tr>
</thead>
<tbody>
<tr>
<td>demonstration-app</td>
<td>1.3</td>
<td>arm</td>
<td>Friday, 0 September 2018 10:06:16 AM</td>
<td>Package details</td>
<td>Uninstall</td>
</tr>
</tbody>
</table>

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 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.

---

**Figure 94 - Administration page**
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.
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-6000 Series router contains a self-signed digital certificate which is identical on all NTC-6000 Series 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 HTTPS key management.
2. Enter the certificate details using the appropriate fields. Each field must be completed in order to generate a certificate.

Note: The Country field must contain a code for the desired country from the list below.
<table>
<thead>
<tr>
<th>CODE</th>
<th>COUNTRY</th>
<th>CODE</th>
<th>COUNTRY</th>
<th>CODE</th>
<th>COUNTRY</th>
<th>CODE</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>AX</td>
<td>Åland Islands</td>
<td>BR</td>
<td>Eritrea</td>
<td>LS</td>
<td>Lesotho</td>
<td>SA</td>
<td>Saudi Arabia</td>
</tr>
<tr>
<td>AD</td>
<td>Andorra</td>
<td>ES</td>
<td>Spain</td>
<td>LT</td>
<td>Lithuania</td>
<td>SB</td>
<td>Solomon Islands</td>
</tr>
<tr>
<td>AE</td>
<td>United Arab Emirates</td>
<td>ET</td>
<td>Ethiopia</td>
<td>LU</td>
<td>Luxemburg</td>
<td>SC</td>
<td>Seychelles</td>
</tr>
<tr>
<td>AF</td>
<td>Afghanistan</td>
<td>FI</td>
<td>Finland</td>
<td>LV</td>
<td>Latvia</td>
<td>SE</td>
<td>Sweden</td>
</tr>
<tr>
<td>AG</td>
<td>Antigua and Barbuda</td>
<td>FJ</td>
<td>Fiji</td>
<td>LY</td>
<td>Libya</td>
<td>SG</td>
<td>Singapore</td>
</tr>
<tr>
<td>AI</td>
<td>Anguilla</td>
<td>FK</td>
<td>Falkland Islands</td>
<td>MA</td>
<td>Morocco</td>
<td>SH</td>
<td>St. Helena</td>
</tr>
<tr>
<td>AL</td>
<td>Albania</td>
<td>FM</td>
<td>Micronesia</td>
<td>MC</td>
<td>Monaco</td>
<td>SI</td>
<td>Slovenia</td>
</tr>
<tr>
<td>AM</td>
<td>Armenia</td>
<td>FO</td>
<td>Faroe Islands</td>
<td>MD</td>
<td>Moldova</td>
<td>SJ</td>
<td>Svalbard and Jan Mayen</td>
</tr>
<tr>
<td>AN</td>
<td>Netherlands Antilles</td>
<td>FR</td>
<td>France</td>
<td>ME</td>
<td>Montenegro</td>
<td>SK</td>
<td>Slovak Republic</td>
</tr>
<tr>
<td>AO</td>
<td>Angola</td>
<td>FX</td>
<td>France, Metropolitan</td>
<td>MG</td>
<td>Madagascar</td>
<td>SL</td>
<td>Sierra Leone</td>
</tr>
<tr>
<td>AQ</td>
<td>Antarctica</td>
<td>GA</td>
<td>Gabon</td>
<td>MH</td>
<td>Marshall Islands</td>
<td>SM</td>
<td>San Marino</td>
</tr>
<tr>
<td>AR</td>
<td>Argentina</td>
<td>GB</td>
<td>Great Britain (UK)</td>
<td>MK</td>
<td>Macedonia</td>
<td>SN</td>
<td>Senegal</td>
</tr>
<tr>
<td>AS</td>
<td>American Samoa</td>
<td>GD</td>
<td>Grenada</td>
<td>ML</td>
<td>Mali</td>
<td>SR</td>
<td>Suriname</td>
</tr>
<tr>
<td>AT</td>
<td>Austria</td>
<td>GE</td>
<td>Georgia</td>
<td>MM</td>
<td>Myanmar</td>
<td>ST</td>
<td>Sao Tome and Principe</td>
</tr>
<tr>
<td>AU</td>
<td>Australia</td>
<td>GF</td>
<td>French Guiana</td>
<td>MN</td>
<td>Mongolia</td>
<td>SU</td>
<td>USSR (former)</td>
</tr>
<tr>
<td>AW</td>
<td>Aruba</td>
<td>GQ</td>
<td>Guernsey</td>
<td>MO</td>
<td>Macau</td>
<td>SV</td>
<td>El Salvador</td>
</tr>
<tr>
<td>AZ</td>
<td>Azerbaijan</td>
<td>GH</td>
<td>Ghana</td>
<td>MP</td>
<td>Northern Mariana</td>
<td>SZ</td>
<td>Swaziland</td>
</tr>
<tr>
<td>BA</td>
<td>Bosnia and Herzegovina</td>
<td>GJ</td>
<td>Gibraltar</td>
<td>MQ</td>
<td>Martinique</td>
<td>TC</td>
<td>Turks and Caicos Islands</td>
</tr>
<tr>
<td>BB</td>
<td>Barbados</td>
<td>GL</td>
<td>Greenland</td>
<td>MR</td>
<td>Mauritania</td>
<td>TD</td>
<td>Chad</td>
</tr>
<tr>
<td>BD</td>
<td>Bangladesh</td>
<td>GM</td>
<td>Gambia</td>
<td>MS</td>
<td>Montserrat</td>
<td>TF</td>
<td>French Southern Territories</td>
</tr>
<tr>
<td>BE</td>
<td>Belgium</td>
<td>GN</td>
<td>Guinea</td>
<td>MT</td>
<td>Malta</td>
<td>TG</td>
<td>Togo</td>
</tr>
<tr>
<td>BF</td>
<td>Burkina Faso</td>
<td>GP</td>
<td>Guadeloupe</td>
<td>MU</td>
<td>Mauritius</td>
<td>TH</td>
<td>Thailand</td>
</tr>
<tr>
<td>BG</td>
<td>Bulgaria</td>
<td>GQ</td>
<td>Equatorial Guinea</td>
<td>MV</td>
<td>Maldives</td>
<td>TJ</td>
<td>Tajikistan</td>
</tr>
<tr>
<td>BH</td>
<td>Bahrain</td>
<td>GR</td>
<td>Greece</td>
<td>MW</td>
<td>Malawi</td>
<td>TK</td>
<td>Tokelau</td>
</tr>
<tr>
<td>BI</td>
<td>Burundi</td>
<td>GS</td>
<td>S. Georgia and S. Sandwich</td>
<td>MX</td>
<td>Mexico</td>
<td>TM</td>
<td>Turkmenistan</td>
</tr>
<tr>
<td>BJ</td>
<td>Benin</td>
<td>GT</td>
<td>Guatemala</td>
<td>MY</td>
<td>Malaysia</td>
<td>TN</td>
<td>Tunisia</td>
</tr>
<tr>
<td>BM</td>
<td>Bermuda</td>
<td>GU</td>
<td>Guam</td>
<td>MZ</td>
<td>Mozambique</td>
<td>TO</td>
<td>Tonga</td>
</tr>
<tr>
<td>BN</td>
<td>Brunei Darussalam</td>
<td>GW</td>
<td>Guinea-Bissau</td>
<td>NA</td>
<td>Namibia</td>
<td>TP</td>
<td>East Timor</td>
</tr>
<tr>
<td>BO</td>
<td>Bolivia</td>
<td>GY</td>
<td>Guyana</td>
<td>NC</td>
<td>New Caledonia</td>
<td>TR</td>
<td>Turkey</td>
</tr>
<tr>
<td>BR</td>
<td>Brazil</td>
<td>HK</td>
<td>Hong Kong</td>
<td>NE</td>
<td>Niger</td>
<td>TT</td>
<td>Trinidad and Tobago</td>
</tr>
<tr>
<td>BS</td>
<td>Bahamas</td>
<td>HM</td>
<td>Heard and McDonald Islands</td>
<td>NF</td>
<td>Norfolk Island</td>
<td>TV</td>
<td>Tuvalu</td>
</tr>
<tr>
<td>BT</td>
<td>Bhutan</td>
<td>HN</td>
<td>Honduras</td>
<td>NG</td>
<td>Nigeria</td>
<td>TW</td>
<td>Taiwan</td>
</tr>
<tr>
<td>BV</td>
<td>Bouvet Island</td>
<td>HR</td>
<td>Croatia (Hrvatska)</td>
<td>NI</td>
<td>Nicaragua</td>
<td>TZ</td>
<td>Tanzania</td>
</tr>
<tr>
<td>BW</td>
<td>Botswana</td>
<td>HT</td>
<td>Haiti</td>
<td>NL</td>
<td>Netherlands</td>
<td>UA</td>
<td>Ukraine</td>
</tr>
<tr>
<td>BZ</td>
<td>Belize</td>
<td>HU</td>
<td>Hungary</td>
<td>NO</td>
<td>Norway</td>
<td>UG</td>
<td>Uganda</td>
</tr>
<tr>
<td>CA</td>
<td>Canada</td>
<td>ID</td>
<td>Indonesia</td>
<td>NP</td>
<td>Nepal</td>
<td>UM</td>
<td>US Minor Outlying Islands</td>
</tr>
<tr>
<td>CC</td>
<td>Cocos (Keeling) Islands</td>
<td>IE</td>
<td>Ireland</td>
<td>NR</td>
<td>Nauru</td>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>CF</td>
<td>Central African Republic</td>
<td>IL</td>
<td>Israel</td>
<td>NT</td>
<td>Neutral Zone</td>
<td>UY</td>
<td>Uruguay</td>
</tr>
<tr>
<td>CH</td>
<td>Switzerland</td>
<td>IM</td>
<td>Isle of Man</td>
<td>NI</td>
<td>Niiu</td>
<td>UZ</td>
<td>Uzbekistan</td>
</tr>
<tr>
<td>CI</td>
<td>Cote D’Ivoire (Ivory)</td>
<td>IN</td>
<td>India</td>
<td>NZ</td>
<td>New Zealand</td>
<td>VA</td>
<td>Vatican City State (Holy See)</td>
</tr>
<tr>
<td>CK</td>
<td>Cook Islands</td>
<td>IO</td>
<td>British Indian Ocean Territory</td>
<td>OM</td>
<td>Oman</td>
<td>VC</td>
<td>Saint Vincent and the Grenadines</td>
</tr>
<tr>
<td>CL</td>
<td>Chile</td>
<td>IS</td>
<td>Iceland</td>
<td>PA</td>
<td>Panama</td>
<td>VE</td>
<td>Venezuela</td>
</tr>
<tr>
<td>CM</td>
<td>Cameroon</td>
<td>IT</td>
<td>Italy</td>
<td>PE</td>
<td>Peru</td>
<td>VG</td>
<td>Virgin Islands (British)</td>
</tr>
<tr>
<td>CN</td>
<td>China</td>
<td>JF</td>
<td>Jersey</td>
<td>PF</td>
<td>French Polynesia</td>
<td>VI</td>
<td>Virgin Islands (U.S.)</td>
</tr>
<tr>
<td>CO</td>
<td>Colombia</td>
<td>JM</td>
<td>Jamaica</td>
<td>PG</td>
<td>Papua New Guinea</td>
<td>VN</td>
<td>Viet Nam</td>
</tr>
<tr>
<td>CR</td>
<td>Costa Rica</td>
<td>JO</td>
<td>Jordan</td>
<td>PH</td>
<td>Philippines</td>
<td>VU</td>
<td>Vanuatu</td>
</tr>
<tr>
<td>CS</td>
<td>Czechoslovakia (former)</td>
<td>JP</td>
<td>Japan</td>
<td>PK</td>
<td>Pakistan</td>
<td>WF</td>
<td>Wallis and Futuna Islands</td>
</tr>
<tr>
<td>CV</td>
<td>Cape Verde</td>
<td>KE</td>
<td>Kenya</td>
<td>PL</td>
<td>Poland</td>
<td>WS</td>
<td>Samoa</td>
</tr>
<tr>
<td>CX</td>
<td>Christmas Island</td>
<td>KG</td>
<td>Kyrgyzstan</td>
<td>PM</td>
<td>St. Pierre and Miquelon</td>
<td>YE</td>
<td>Yemen</td>
</tr>
<tr>
<td>CY</td>
<td>Cyprus</td>
<td>KH</td>
<td>Cambodia</td>
<td>PN</td>
<td>Pitcairn</td>
<td>YT</td>
<td>Mayotte</td>
</tr>
<tr>
<td>CZ</td>
<td>Czech Republic</td>
<td>KI</td>
<td>Kiribati</td>
<td>PR</td>
<td>Puerto Rico</td>
<td>ZA</td>
<td>South Africa</td>
</tr>
<tr>
<td>DE</td>
<td>Germany</td>
<td>KM</td>
<td>Comoros</td>
<td>PS</td>
<td>Palestinian Territory</td>
<td>ZM</td>
<td>Zambia</td>
</tr>
<tr>
<td>DJ</td>
<td>Djibouti</td>
<td>KN</td>
<td>Saint Kitts and Nevis</td>
<td>PT</td>
<td>Portugal</td>
<td>COM</td>
<td>US Commercial</td>
</tr>
<tr>
<td>DK</td>
<td>Denmark</td>
<td>KR</td>
<td>Korea (South)</td>
<td>PW</td>
<td>Palau</td>
<td>EDU</td>
<td>US Educational</td>
</tr>
<tr>
<td>DM</td>
<td>Dominica</td>
<td>KW</td>
<td>Kuwait</td>
<td>PY</td>
<td>Paraguay</td>
<td>GOV</td>
<td>US Government</td>
</tr>
<tr>
<td>DO</td>
<td>Dominican Republic</td>
<td>KY</td>
<td>Cayman Islands</td>
<td>QA</td>
<td>Qatar</td>
<td>INT</td>
<td>International</td>
</tr>
<tr>
<td>DZ</td>
<td>Algeria</td>
<td>KZ</td>
<td>Kazakhstan</td>
<td>RE</td>
<td>Reunion</td>
<td>MIL</td>
<td>US Military</td>
</tr>
<tr>
<td>EC</td>
<td>Ecuador</td>
<td>LA</td>
<td>Laos</td>
<td>RO</td>
<td>Romania</td>
<td>NET</td>
<td>Network</td>
</tr>
<tr>
<td>EE</td>
<td>Estonia</td>
<td>LC</td>
<td>Saint Lucia</td>
<td>RS</td>
<td>Serbia</td>
<td>ORG</td>
<td>Non-Profit Organization</td>
</tr>
<tr>
<td>EG</td>
<td>Egypt</td>
<td>LI</td>
<td>Liechtenstein</td>
<td>RU</td>
<td>Russian Federation</td>
<td>ARPA</td>
<td>Old style Arpanet</td>
</tr>
<tr>
<td>EH</td>
<td>Western Sahara</td>
<td>LK</td>
<td>Sri Lanka</td>
<td>RW</td>
<td>Rwanda</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. 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 96 - New certificate successfully generated message](image-url)
SSH Key Management

Secure Shell (SSH) is a 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.

Figure 97 - 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 you 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.

<table>
<thead>
<tr>
<th>Key type</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh_host_key</td>
<td>2013-09-05 10:19:45</td>
</tr>
<tr>
<td>ssh_host_dsa_key</td>
<td>2013-09-05 10:20:00</td>
</tr>
<tr>
<td>ssh_host_rsa_key</td>
<td>2013-09-05 10:20:02</td>
</tr>
<tr>
<td>ssh_host_ecdsa_key</td>
<td>2013-09-05 10:20:03</td>
</tr>
</tbody>
</table>

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

Click the Upload keys button to upload your own public key 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**.

![LED Operation Mode](image)

**Figure 98 - 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.
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.
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.

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 ...........................................................................................................7
Table 3: Router Interface Ports .......................................................................................................9
Table 4 - Locking power block pin outs..........................................................................................10
Table 5 - Management account login details – Root manager ........................................................12
Table 6 - Management account login details – Admin manager .....................................................12
Table 7 - Status page item details ..................................................................................................14
Table 8 - Data connection item details ..........................................................................................16
Table 9 - Band settings ..................................................................................................................19
Table 10 - Current MAC / IP / Port filtering rules in effect .............................................................39
Table 11 - IPSec Configuration Items ............................................................................................42
Table 12 - Modern emulator options ..............................................................................................61
Table 13 - Mobile Station Based Assisted GPS configuration options .........................................71
Table 14 - Odometer configuration options ...................................................................................72
Table 15 - SMS Setup Settings .......................................................................................................74
Table 16 - Inbox/Outbox icons ........................................................................................................76
Table 17 - SMS Diagnostic Command Syntax ...............................................................................81
Table 18 - List of basic SMS diagnostic commands ....................................................................82
Table 19 - List of get/set commands ..............................................................................................83
Table 20 - List of basic SMS diagnostics RDB variables ...............................................................84
Table 21 - Network types returned by get plmnscan SMS command ...........................................84
Table 22 - Operator status codes returned by get plmnscan SMS command ...............................84
Table 23 - SMS diagnostics example commands .......................................................................87
Table 24 - System log detail levels ................................................................................................89
Table 25 - Administration configuration options ..........................................................................97
Table 26 - LAN Management Default Settings ............................................................................106
Table 27 - Web Interface Default Settings ...................................................................................106
Table 28 - Telnet Access ...............................................................................................................106
Table 29 - RS-232 Wiring ..............................................................................................................106
Table 30 - Technical Specifications of the NTC-6000 series routers .............................................114
Appendix B: Default Settings

The following tables list the default settings for the NTC-6000 Series router.

### LAN (MANAGEMENT)

<table>
<thead>
<tr>
<th>Static IP Address</th>
<th>192.168.20.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>192.168.20.1</td>
</tr>
</tbody>
</table>

Table 26 - LAN Management Default Settings

### ADMIN MANAGER ACCOUNT | ROOT MANAGER ACCOUNT

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>admin</td>
<td>root</td>
<td>admin</td>
</tr>
</tbody>
</table>

Table 27 - 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-6000 SERIES ROUTER TELNET ACCESS

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>admin</td>
</tr>
</tbody>
</table>

Table 28 - Telnet Access
Restoring factory default settings

Restoring factory defaults will reset the NTC-6000 Series router to its factory default configuration. You may encounter a situation where you need to restore the factory defaults on your NTC-6000 Series 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-6000 Series 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://192.168.20.1). 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-6000 Series router to its default settings you will be able to access the device’s configuration web interface using http://192.168.20.1 with username admin or root and password admin.
Appendix C: Recovery mode

The NTC-6000 Series 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-6000 Series 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://192.168.20.1. 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.

NTC-6000 Series Recovery Console

![Recovery console screenshot](image-url)
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.

NTC-5000 Series Recovery Console

<table>
<thead>
<tr>
<th>Status</th>
<th>Log</th>
<th>Application Installer</th>
<th>Settings</th>
<th>Reboot</th>
</tr>
</thead>
</table>

**System Information**
- **System Up time**: 00:02:00
- **Router Version**: Hardware: 1.3 Software: Y2.0.4.1
- **Serial Number**: 199:0001:140221
- **Trigger**: button

**LAN**
- **IP**: 192.168.20.1 / 255.256.255.0
- **MAC Address**: 09:60:64:D2:E3:A3

**Ethernet Port Status**
- **LAN**: Up / 19.6 Mbps / HDX

![Figure 102 - Recovery mode - Status](image)

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.

![Figure 103 - Recovery mode - Log](image)
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.

![Figure 104 - Recovery mode - Application Installer](image)

### 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.

![Figure 105 - Recovery mode – Settings](image)

### 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.

![Figure 106 - Recovery mode - Reboot](image)
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-6000 Series 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 107 - Upload page](image)

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

![Figure 108 - Browse for server.crt](image)
3. Click the **Upload** button to begin uploading it to the router. The file appears in the list of files stored on the router.

4. Repeat steps 2 and 3 for the server key file.

5. 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.
Appendix E: Serial port wiring

The NTC-6000 Series router has a serial interface and acts as the data communications equipment (DCE). The wiring tables below indicate the DCE and DTE devices as well as the signal direction. Shielding cable can optionally be soldered to the chassis and connected to ground.

<table>
<thead>
<tr>
<th>PIN</th>
<th>NAME (DTE DEVICE)</th>
<th>DESCRIPTION</th>
<th>PIN</th>
<th>NAME (DCE DEVICE)</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DCD</td>
<td>Data carrier detect</td>
<td>1</td>
<td>DCD</td>
<td>Data carrier detect</td>
</tr>
<tr>
<td>2</td>
<td>RXD</td>
<td>Receive Data</td>
<td>2</td>
<td>RXD</td>
<td>Receive Data</td>
</tr>
<tr>
<td>3</td>
<td>TXD</td>
<td>Transmit Data</td>
<td>3</td>
<td>TXD</td>
<td>Transmit Data</td>
</tr>
<tr>
<td>4</td>
<td>DTR</td>
<td>Data Terminal Ready</td>
<td>4</td>
<td>DTR</td>
<td>Data Terminal Ready</td>
</tr>
<tr>
<td>5</td>
<td>GND</td>
<td>Ground</td>
<td>5</td>
<td>GND</td>
<td>Ground</td>
</tr>
<tr>
<td>6</td>
<td>DSR</td>
<td>Data Set Ready</td>
<td>6</td>
<td>DSR</td>
<td>Data Set Ready</td>
</tr>
<tr>
<td>7</td>
<td>RTS</td>
<td>Request to Send</td>
<td>7</td>
<td>RTS</td>
<td>Request to Send</td>
</tr>
<tr>
<td>8</td>
<td>CTS</td>
<td>Clear to Send</td>
<td>8</td>
<td>CTS</td>
<td>Clear to Send</td>
</tr>
<tr>
<td>9</td>
<td>RI</td>
<td>Ring Indicator</td>
<td>9</td>
<td>RI</td>
<td>Ring Indicator</td>
</tr>
<tr>
<td>-</td>
<td>FGND</td>
<td>Shield (Soldered to D9 metal shield)</td>
<td>-</td>
<td>FGND</td>
<td>Shield (Soldered to D9 metal shield)</td>
</tr>
</tbody>
</table>

Table 29 - RS-232 Wiring
Technical Data

The following tables list the hardware specifications of the NTC-6000 Series routers.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>NTC-6908</th>
<th>NTC-6908-02</th>
<th>NTC-6520</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>32MB DRAM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>256MB/Byte Flash memory storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UMTS bands</td>
<td>UMTS/HSDPA/HSUPA: 850/1900/2100 MHz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GSM bands</td>
<td>GSM/GPRS/EDGE: 850/900/1800/1900 MHz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Data Throughput / 3G Radio interface</td>
<td>HSDPA/HSUPA data rates: DL: 7.2 Mbps, UL: 5.76 Mbps</td>
<td>HSDPA/HSUPA data rates: DL: 21 Mbps, UL: 5.76 Mbps</td>
<td></td>
</tr>
<tr>
<td>Connectivity</td>
<td>1x Fast Ethernet 10/100Base-TX RJ-45 port with Auto MDI/MDIX</td>
<td>1x Serial RS-232 DE-9 female DCE port</td>
<td></td>
</tr>
<tr>
<td>SIM Card Reader</td>
<td>Locking Tray for SIM/SIM in Mini-SIM card format (25.00 x 15.00 x 0.76 mm)</td>
<td>1x SMA connector for 2G/3G (1x Main and 1x RX Diversity)</td>
<td></td>
</tr>
<tr>
<td>Antenna connectors</td>
<td>2x SMA connectors for 2G/3G (1x Main and 1x RX Diversity)</td>
<td>1x SMA connector for GPS</td>
<td></td>
</tr>
<tr>
<td>LED Indicators</td>
<td>5x LEDs: Power, Service, Tx/Rx, DCD and RSSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>Operating Temperature Range: -30°C ~ +70°C</td>
<td>Storage Temperature Range: -55°C ~ +85°C</td>
<td></td>
</tr>
<tr>
<td>Power input</td>
<td>Captive DECA® Euro Type Terminal Block MC100#50802 (DC Plug with Screw Terminal)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input Voltage Range</td>
<td>8-28V DC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Consumption</td>
<td>Idle: 1.32W (110 mA @ 12V DC)</td>
<td>Active HSDPA connection: 3.68W (300 mA @ 12V DC)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maximum: 6.72W (560 mA @ 12V DC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dimensions &amp; Weight</td>
<td>135mm (L) x 101mm (W) x 29mm (D) / 221g</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>A-Tick, RoHS</td>
<td>A-Tick, CE, FCC, IC</td>
<td>A-Tick, RoHS</td>
</tr>
</tbody>
</table>

Table 30 - Technical Specifications of the NTC-6000 Series routers
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 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:

7. you, or someone else, use the product, or attempt to use it, other than as specified by NetComm Wireless Limited;
8. 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);
9. the fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
10. 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;
11. 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
12. 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