



USER GUIDE

Preface




This manual provides information relating to the installation, operation, and application of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be broken or malfunctioning, please contact technical support for immediate service by email at Technical.Support@netcommwireless.com

For product updates, new product releases, manual revisions, or software upgrades, please visit our website at www.netcommwireless.com

Important Safety Instructions

With reference to unpacking, installation, use and maintenance of your electronic device, the following basic guidelines are recommended:

-  Do not use or install this product near water to avoid fire or shock hazard. For example, near a bathtub, kitchen sink, laundry tub., or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
-  Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on or mistreat the cord.
-  To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are unobstructed.



WARNING: Disconnect the power line from the device before servicing.

Copyright

Copyright©2011 NetComm Wireless Limited.

All rights reserved.

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



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 center and processed separately from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router 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.

DOCUMENT VERSION	DATE	CHANGE HISTORY
1.0	June 2010	Internal Release Version (FW 1.52)
1.2	November 2010	Initial Public Release (FW v1.57)
2.1	February 2011	Added GPS and Modem configuration sections (FW v1.7.0)
2.2	June 2011	Added SMS Tools configuration documentation (FW v1.7.1.5)
2.3	June 2012	Added TR069 configuration sections (FW v 1.9.79.6)

Table 1: NTC-6000 Series User Manual Document History

Table of Contents

Introduction.....	5
Overview	5
Features	6
Hardware Overview.....	7
LED Overview.....	7
Overview of the Router Interfaces	8
Configuring your Router.....	10
Inserting the SIM Card.....	10
Setting Up the Cellular Router	10
Preparing Your Computer.....	12
Accessing the Router Web User Interface.....	17
Unlocking the SIM Card.....	18
Band / Provider Selection	22
Locking To a Specific Band.....	22
Choosing Your Mobile Broadband Provider Manually.....	23
Establishing a Connection to a Cellular Network.....	24
Ethernet Related Commands.....	27
Virtual Private Networks	29
Configuring a PPTP / GRE connection	29
OpenVPN	31
IPSec	33
Routing Configuration	35
How to Configure RIP.....	36
How to Configure VRRP	37
NAT configuration	38
Services Features	39
Services Features	40
GPS	45
SMS Tools	46
NSUpdate.....	57
PADD 錯誤! 尚未定義書籤。	
System Features	58
Viewing the system log	58
Remote Administration.....	59
Restoring a Copy of the Router's Configuration.....	61
Remote Firmware Upgrade	64
Package Manager.....	65
System Configuration.....	66
TR-069.....	67
Troubleshooting	69
Common problems and solutions	69
Specifications.....	72
Hardware Specifications.....	72
Legal & Regulatory Information	75
Intellectual Property Rights.....	75
Customer Information.....	75
Consumer Protection Laws.....	75
Product Warranty	76
Limitation of Liability.....	76

Contact 78

Introduction

Thank you for purchasing an Industrial HSPA Cellular Network Router from NetComm. This manual illustrates how to set-up and configure your router appropriately for your chosen task. The router is primarily managed and configured via a web browser. This manual will take you through the steps required to configure and use your unit correctly.

Additionally, the router may be configured via the serial (V.24) port using "AT" (V.250) commands. This method of operation is further detailed in the document: NTC-6000Series_V250 (AT) Manual_V1-1-0.

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 the user a point-to-point or point-to-multi-point communications link in a single, compact and resilient unit.

As a fully featured cellular router, it supports a large number of communication interfaces and protocols to meet the demands of today's telemetry and WAN applications.

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

In the event of system corruption, a built-in recovery mode provides the facility to re-install the system software to the router and resume normal operations quickly. Using the recovery console is further detailed in the document NTC-6XXX Firmware Upgrade VX.X.X.pdf that is part of all NTC-6000 series firmware upgrade packs released, which are available for download in the support section of our website at www.netcommwireless.com.

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.
- Embedded Sierra HSPA modem module MC8790V (NTC-6908) or MC8792V (NTC-6909) with Qualcomm MSM6290 chipset.
- 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 – 28 V 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.
- 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/RRP
- Supports NAT, Port forwarding and a DMZ Host
- Configurable APN profiles (drop-down list)
- Supports manual network scan
- System monitoring, diagnostic log viewer.
- Web user interface for easy centralized configuration and management from any PC or smart phone
- 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 Overview

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

Listed below are the specifications of the LED's and their corresponding colours.



Figure 1: NTC-6000 Series LEDs

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

Table 2: LED Descriptions

Overview of the Router Interfaces

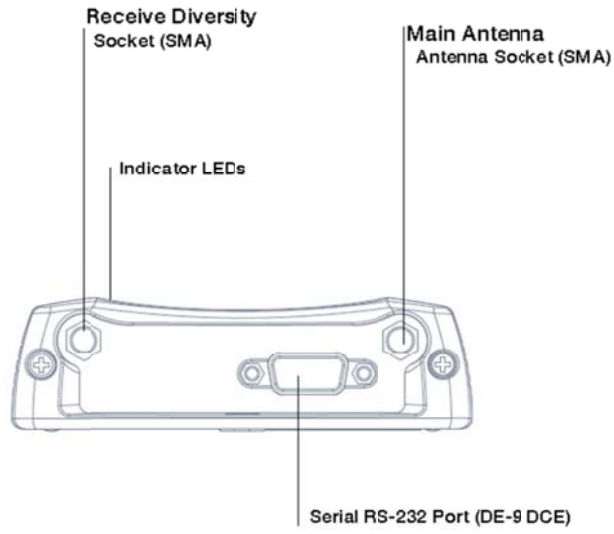


Figure 2: Router Interfaces – Left Side View

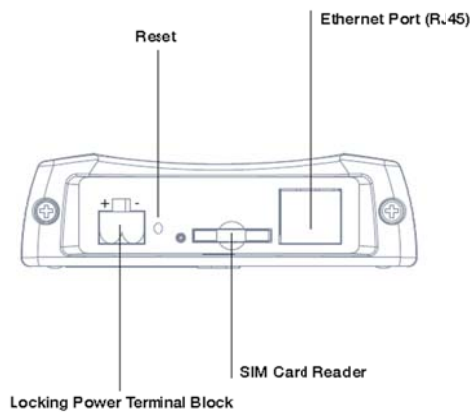






Figure 3: Router Interfaces – Right Side View

FIELD	DESCRIPTION
Main Antenna Socket	Female SMA Connector
Receive Diversity Antenna Socket	Female SMA Connector
Serial RS-232 Port	For connecting to a terminal using a DB9-F cable.
Indicator LEDs	Indicates the connection strength, service type, data traffic, data carrier connection and network connection strength
Power Terminal Block	The screw terminal of the DC power plug and the wide input voltage range of 8-28V DC simplify the installation in different industrial environments
Reset Button	Pressing this button for 10 seconds will set the router into recovery mode where firmware or application packages can be uploaded. After installing new firmware the router must be reset to factory default settings before being reconfigured.
Ethernet Port	For direct connection to your devices through a hub or network router
SIM Card Reader	For insertion and removal of SIM card

Table 3: Router Interface Ports

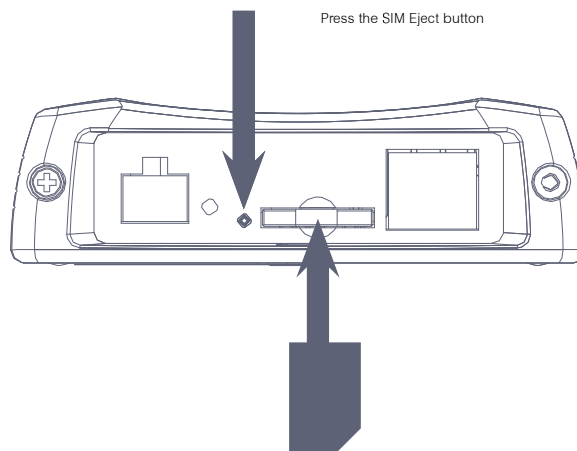
Configuring your Router

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

Press the SIM 'Eject' button to eject SIM card bay. Make sure the SIM card is inserted correctly by inserting the SIM with the gold side facing down on the SIM card bay and in the direction as shown below:

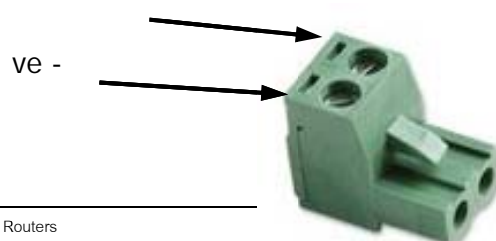


Setting Up the Cellular Router

Attach the supplied antenna to the router by screwing it onto the antenna connector. Connect the power adapter to the mains and plug the output into the power jack of the router. The red power LED on the panel should illuminate



Polarity of DC Power Plug Screw Terminal



Preparing Your Computer

Connect one end of the supplied Ethernet cable to the Ethernet port of your router. Connect the other end of the cable to the LAN port of your computer. Configure your PC's Ethernet interface to use a dynamically assigned IP address by completing one the following steps that correspond to the operating system your computer has installed.

Ethernet interface configuration in Windows XP

- 1 Click on the Start button, select "Control Panel" and then "Network Connections".
- 2 Right click on "Local Area Connection" and select the Properties option to open the configuration dialogue box as shown below:

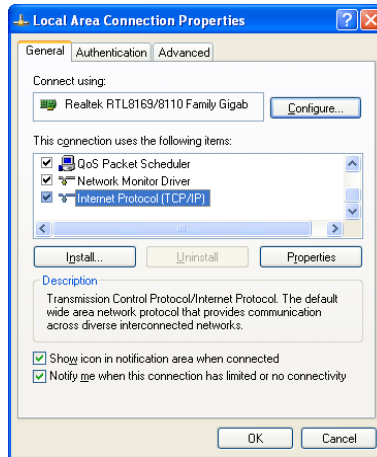


Figure 4: Local Area Connection Properties

- 3 Find and select Internet Protocol (TCP/IP) from the protocol list box and then click the Properties option. The TCP/IP configuration window will pop up as illustrated below. Under the General tab, select the radio button 'Obtain an IP address automatically' and 'Obtain DNS server address automatically'.

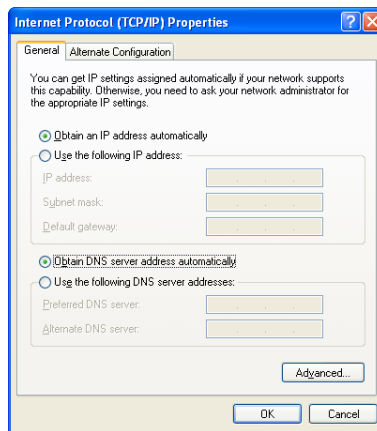


Figure 5: Internet Protocol (TCP/IP) Properties

- 4 Press the OK button to close the TCP/IP configuration window. Then press the Close button to complete the computer preparation for the router.

Ethernet Interface Configuration in Windows Vista

- Click on the Start button. Then select "Control Panel" followed by "Network and Sharing Centre".

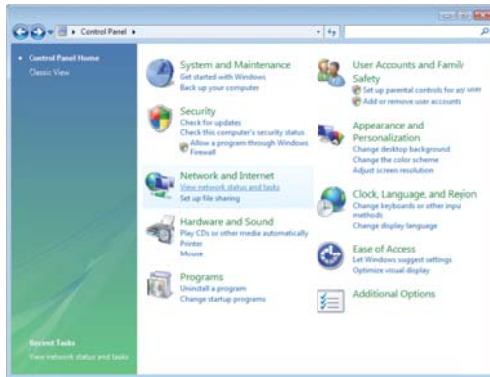


Figure 6: Windows Vista Control Panel

- In the Manage network connections, click on "Manage network connections" to continue.

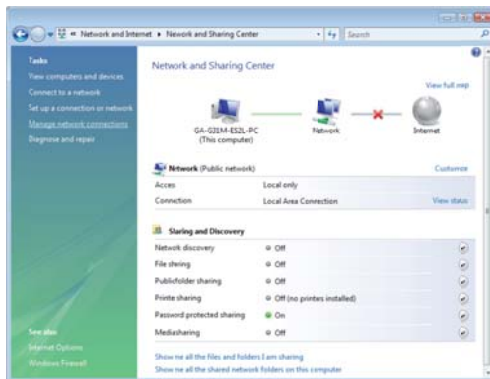


Figure 7: Windows Vista -Network and Sharing Center

- Single RIGHT click on "Local Area connection", then click "Properties".

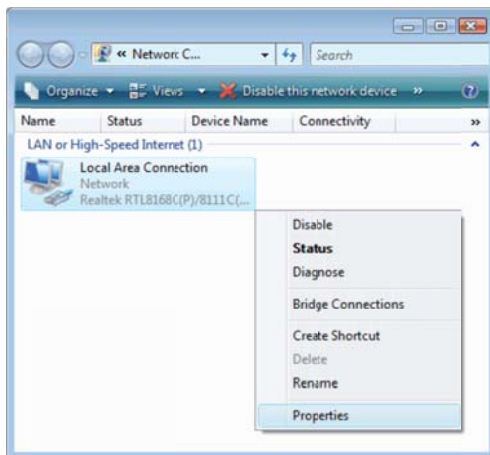


Figure 8: Right Clicking Local Area Connection and Selecting Properties

- The screen will display the information "User Account Control" and click "Continue" to continue and then double click on "Internet Protocol Version 4 (TCP/IPv4)".

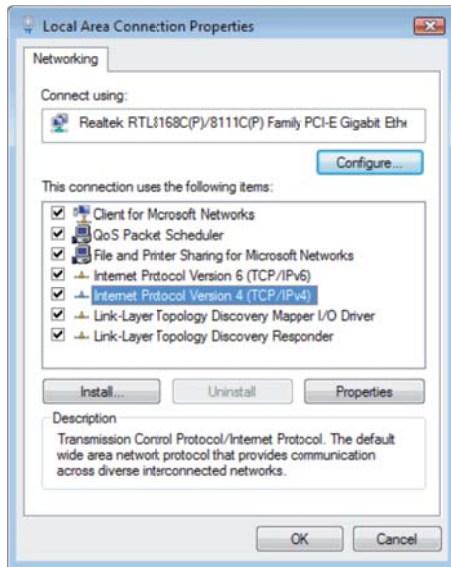


Figure 9: Double Click Internet Protocol Version 4 (TCP/IPv4)

- Select "Obtain an IP address automatically" and "Obtain DNS server address automatically" before clicking on the "OK" button to continue.

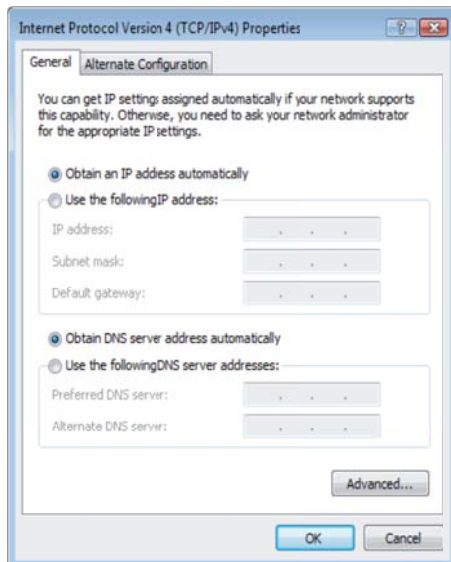


Figure 10: Set Properties to Automatic Settings

- Click on the "OK" button and close the Local Area Connection Properties window to complete the computer preparation for the router.

Ethernet Interface Configuration in Windows 7

- Click on the Start button, select the "Control Panel (in Category View)" option and then click on the "View Network Status and Tasks".



Figure 11: Windows 7 Control Panel

- In the "Network Settings" window select the "Change Adapter Settings" option to continue.

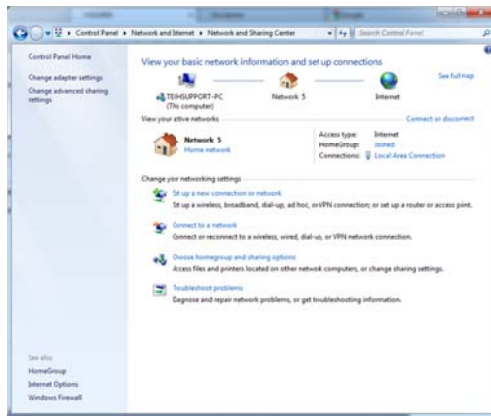


Figure 12: Windows 7 Network and Sharing Center

- Single RIGHT click on "Local Area Connection", then click "Properties".

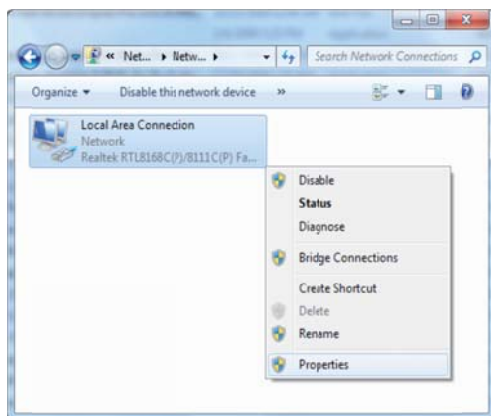


Figure 13: Windows 7 - Selecting Local Area Connection Properties

- Double click on "Internet Protocol Version 4 (TCP/IPv4)".

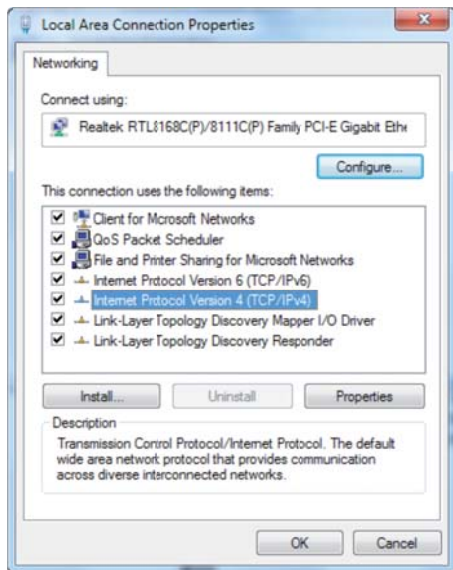


Figure 14: Double Click Internet Protocol Version 4 (TCP/IPv4)

- Click on "Obtain an IP address automatically" and "Obtain DNS server address automatically" then click on "OK" to continue.

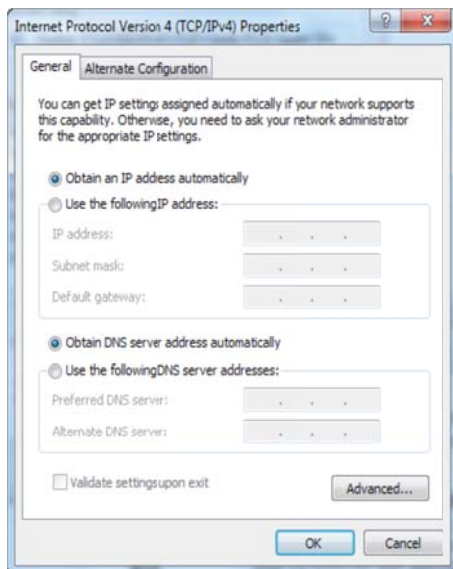


Figure 15: Set Properties to Automatic Settings







- Click on "OK" to complete the computer preparation for the router.

Accessing the Router Web User Interface

There are two system management accounts for maintaining the system, root and admin, which both have slightly different router management capabilities.

The root manager account is has full permission privileges and can use every command option that the router is configured with.

The admin manager (administrator) account has access to the majority of router settings available except the router's system options that can alter or copy the router's firmware (software). The system options not available to an admin user are:

-  Firmware Upgrade – The ability to install an upgraded version of the router's software.
-  Device Configuration Backup – the option of saving the router's current settings, useful for configuring multiple NTC-6000 routers.
-  Upload - Uploading previously saved settings to the router.
-  Restore Factory Defaults - Setting the router to factory default settings, essential after a firmware upgrade.
-  System Configuration settings – The TCP Keepalive function can be used to ensure the current live mobile broadband connection is still alive even when no data packet traffic is being transmitted. It does this by periodically sending a ping (ICMP) request message to a WAN IP address or a well-known internet domain host such as www.google.com. Once the internet connection is deemed to be down the router will attempt to reconnect to the WWAN mobile broadband provider.
-  TR-069 settings - Remote management function allowing the auto-configuration of end-user device.

To login to the router in root manager mode, please use the following login details:

http://192.168.20.1	
User Name	root
Password	admin

Table 4: Root Access Details

To login to the router in admin manager mode, please use the following default login details.

http://192.168.20.1	
User Name	admin
Password	admin

Table 5: Admin Access Details



NOTE – Whenever you make changes, please refresh your web page (press the F5 key) to prevent errors occurring due to caching.

The steps required to access the router's web browser configuration is illustrated below:

1. Open your web browser (e.g. Internet Explorer/Firefox/Safari) and navigate to <http://192.168.20.1/>.
2. Click Login and type "admin" (without quotes) in the Username and Password fields. Then click on the Submit button.

Login	
User Name:	<input type="text"/>
Password:	<input type="password"/>
<input type="button" value="Clear"/> <input type="button" value="Submit"/>	

NTC-6000 Series Login at <http://192.168.20.1>

Unlocking the SIM Card

If the SIM card is locked it can only be unlocked using a PIN that was assigned to your SIM card by your mobile broadband provider. To check if the SIM card is locked view the SIM Status on the router Status page:

Connection Status	
Provider	Telstra
Service Type	Invalid service
Coverage	WCDMA 850
IMEI	355310030024784
Frequency	WCDMA 850
Signal Strength (dBm)	-67 dBm (strong) 
SIM Status	SIM locked - remaining count : 3

Figure 19: SIM Status Locked

If the SIM Status shows the SIM is locked as shown above, you should be automatically redirected to the SIM unlock page. If not, then select the following:

- Click on the "Internet Settings" menu and select "Mobile Broadband" followed by "SIM Security".
- When you click on the 'SIM Security' menu item you should see the following message:-

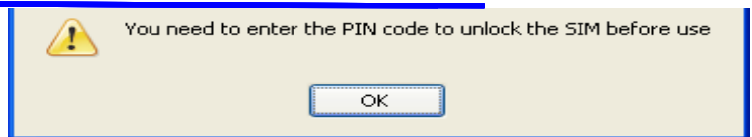


Figure 21: PIN Code Unlock Message

- Click OK
- Enter the PIN code in the PIN and Confirm PIN fields. Then click the Save button.

PIN Settings	
SIM Status	SIM locked - remaining count : 3
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>
Remember PIN	<input type="radio"/> Yes <input checked="" type="radio"/> No
Disable PIN	<input type="radio"/> Yes <input checked="" type="radio"/> No
<input type="button" value="Save"/> <input type="button" value="Help"/>	

Figure 22: PIN Settings

- Click on the Status link and the Home Status page should look as below with SIM Status 'SIM OK':

System Information					
System Up time	00 : 08 : 55				
Router Version	Hardware: 1.3 Software: V1.6.0				
Phone Module	Model: MC8790v Hardware: 1.0 Firmware: K2_0_7_30AP Temp: 31 °C				
Serial Number	02.00.53.CC.B6.63				
Ethernet Port Status					
Lan:	 Up / 100Mb / HDX				
WWAN Show Data Usage					
Profile Name	Interface	Status	APN	Local	Remote
Telstra Internet		Waiting			
Connection Status					
Provider	Telstra				
Service Type	Invalid service				
Coverage	None				
IMEI	354123030124350				
Frequency	WCDMA 850				
Signal Strength (dBm)	-66 dBm (strong) 				
SIM Status	SIM OK				

Figure 23: Status Page - SIM Card Unlocked

Enter PUK Code

If after three incorrect attempts at entering the PIN code, you will be requested to enter a PUK code.



Figure 24: Enter Correct PIN and PUK Message

The PUK code is sometimes referred to as a PIN Unlocked Key (PUK) code. You will need to contact your mobile broadband provider to obtain this number. Your mobile broadband provider will issue you a PUK code which will enable you to unlock the SIM card and enter a new PIN code.

- 1. Enter the new PIN and PUK codes as shown below and click Save.

PIN Settings

PIN Settings	
SIM Status	ENTER PUK
PIN	••••
Confirm PIN	••••
PUK	••••••
Confirm PUK	••••••
Remember PIN	<input checked="" type="radio"/> Yes <input type="radio"/> No
Disable PIN	<input type="radio"/> Yes <input checked="" type="radio"/> No

- 2. If you have entered the PUK correctly you should see the following message:

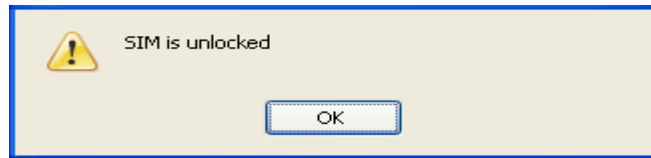


Figure 27: PUK Code Correctly Entered Response

Now click on the "Status" menu item at the top left-hand side of the page. It should reflect the screenshot below and show a SIM Status of 'SIM OK':

All Status LAN PPPoE PPTP					
System Information					
System Up time	00:08:55				
Router Version	Hardware: 1.3 Software: V1.6.0				
Phone Module	Model: MC0790V Hardware: 1.0 Firmware: K2_0_7_30AP Temp: 31 °C				
Serial Number	020053CCB663				
Ethernet Port Status					
Lan	Up / 100Mb / HDX				
WWAN Show Data Usage					
Profile Name	Interface	Status	API	Local	Remote
Telstra Internet		Waiting			
Connection Status					
Provider	Telstra				
Service Type	Invalid service				
Coverage	None				
IMEI	354123030124350				
Frequency	WCDMA 850				
Signal Strength (dBm)	-66 dBm (strong)				
SIM Status	SIM OK				

Figure 28: Status - PIN Unlocked

The 'Remember PIN' Feature

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 unauthorized use of the SIM card elsewhere), while still allowing the router to connect to the cellular service.

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

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

Cellular Band and MBB Provider Selection

Locking To a Specific Band

You may want to lock the router to a specific band. To do this, click on the "Internet Settings" menu and select "Mobile Broadband" followed by the "Band / Provider" menu item on the right.

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



Figure 29: Band/Provider Menu Option

- Make your selection from the "Change Band:" drop down list.

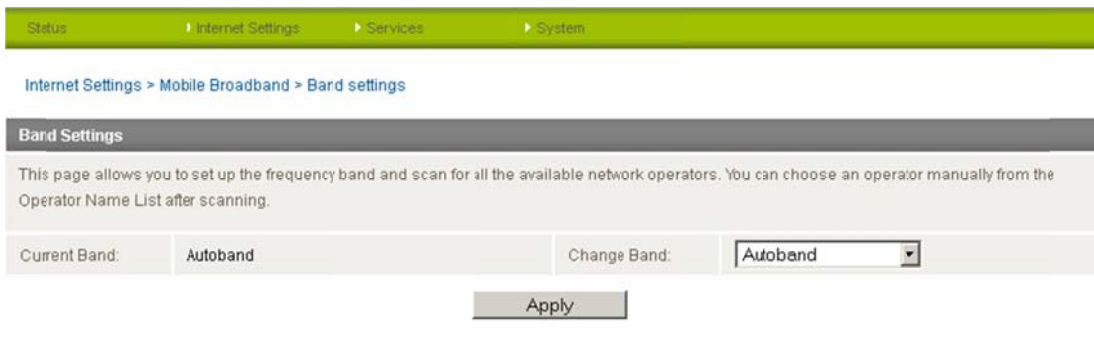


Figure 30: Band Settings


- The following band settings options are applicable.

BAND SELECTION OPTIONS – NTC-6908	
UMTS 850MHz, 2G	UMTS 850 MHz GSM/EDGE/GPRS 900/1800/1900MHz
UMTS 850MHZ ONLY	UMTS 850 MHz Only
2G	GSM/EDGE/GPRS 900/1800/1900MHz
WCDMA All	UMTS 850/2100/1900MHz
ALL BANDS (AUTOBAND)	UMTS 850/2100/1900MHz GSM/EDGE/GPRS

Table 6: NTC-6908 Band Selection Options

BAND SELECTION OPTIONS – NTC-6909	
UMTS 900MHz Only	UMTS 900 MHz Only
WCDMA All	UMTS 900/2100/1900MHz
UMTS 900MHz, 2G	UMTS 900 MHz GSM/EDGE/GPRS 850/900/1800/1900MHz
2G	GSM/EDGE/GPRS 850/900/1800/1900MHz
ALL BANDS (AUTOBAND)	UMTS 850/900/2100/1900MHz GSM/EDGE/GPRS

Table 7: NTC-6909 Band Selection Options

 Click Save to confirm the new band settings.



NOTE: After changing the band, if the change is not reflected on the frequency field on the "Status" page then you may need to reboot the router.

Choosing Your Mobile Broadband Provider Manually

The default setting is "Automatic".

To scan manually for available cellular network operators (providers) follow the steps below:

1. If you are currently connected to the internet, disconnect your session and ensure "Auto Connect" is disabled in the current cellular connection profile you are using (You can check this by clicking on the "Internet Settings" menu and selecting "mobile broadband" followed by the "Connection" menu item).
2. Set the operator mode to Manual
3. Click on the Scan button. A list of cellular operators in the vicinity of your router should appear under the "Operator Name List" heading.
4. Select your chosen provider from the list of detected operators and click the Apply button

The router will then use the chosen operator to attempt to connect to the cellular service profile you have elected to use.

Provider				
Current Operator Selection Mode: Automatic		Select Operator Mode: <input checked="" type="radio"/> Automatic <input type="radio"/> Manual		
Current Operator Registration: voda AU		MCC	MNC	Operator Status
-- Operator Name List --				Network Type
		<input type="button" value="Scan"/> <input type="button" value="Apply"/>		

Figure 31: Selecting a Band Manually

Establishing a Connection to a Cellular Network

This section describes how to configure the router to initiate a Mobile Broadband connection. There are 2 possible methods that can be used to set up a Mobile Broadband connection via PPP:

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

Initiating a PPP Connection Directly from the Router

The status page of the router should be displayed as below. Please ensure that the SIM Status is 'SIM OK' before you initiate a Mobile Broadband connection.

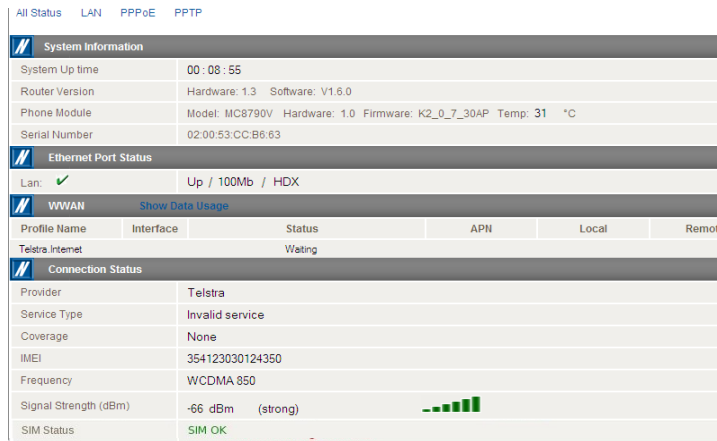


Figure 32: Status Page - Sim Ok

- ➋ Click on the "Internet Settings" menu and select "Mobile Broadband" followed by the "Connection" option on the right as shown in [Figure 33](#) below.



Figure 33: Mobile Broadband - Connection Option

Connecting to the Internet using a Connection Profile

The router supports multiple APN profiles; that allow you the router settings to be configured to connect to different cellular networks

Internet Settings > Mobile Broadband > Connection

Mobile Broadband Profile Settings

Profile Name: Automatically configure my mobile broadband

Profile Name:

APN Name:

Mobile Broadband Connection: Enable Disable

Username:

Password:

Authentication Type: CHAP PAP

Reconnect Delay: (30-65535) secs

Reconnect Retries: (1-65535, 0=Unlimited)

Metric: (1-65535)

MTU: (1-1500)

NAT Masquerading: Enable Disable

PAD Mode

Remote Host:

Port: (1-65535)

Local Encoding: Enable Disable

PAD Mode:

PAD Auto Answer: Enable Disable

Profile Name	Enabled	APN	User
Telstra.Internet	Yes	telstra.internet	
Telstra.Dataack	No	telstra.datapack	
TNZ	No	direct.telecom.co.nz	
Profile4	No		
Profile5	No		
Profile6	No		

Figure 34: Mobile Broadband - Connection Page

- First examine the list of configured profiles
- Select the profile that you wish to connect with and make sure that the APN name field is correct. This is very important
- Select "Enable" for the Auto Connect option and click Save.

From now on, Auto Connect will remain enabled and the router will automatically connect unless you return to this page and disable it.

To Confirm a Successful Connection

Select the Status link to return to the status page. Pay close attention to WWAN section on the page. The WWAN status should be "up". The Local field will show the current IP address that the network has allocated to the router.

Status > Internet Settings > Services > System

All Status LAN PPPoE PPTP

System Information

System Up time: 00:06:02

Router Version: Hardware: 1.3 Software: V1.6.0

Phone Module: Model: MC8790V Hardware: 1.0 Firmware: K2_0_7_30AP Temp: 36 °C

Serial Number: 02.00.53.CC.B6.63

Ethernet Port Status

Lan: Up / 100Mb / HCX

WWAN [Show Data Usage](#)

Profile Name	Interface	Status	APN	Local	Remote
Telstra.Internet	ppp0	wwan0 up	telstra.internet	10.204.88.123	10.64.64.64

Connection Status

Provider: Telstra

Service Type: Combined service

Coverage: HSPA

IMEI: 354123030124350

Frequency: WCDMA 850

Signal Strength (dBm): -66 dBm (strong)

SIM Status: SIM OK

Copyright © 2009 NetComm Limited. All Rights Reserved.

Figure 35: Status Page - WWAN Status Up

Congratulations, the router is now ready to use!

Initiating a Connection using the Router in Transparent PPPoE mode

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

Then select the PPPoE page by clicking on the "Internet Settings" menu, then select "Mobile Broadband" followed by the "PPPoE" option.



The screenshot shows a web interface for configuring PPPoE. At the top, there is a navigation bar with "Status", "Internet Settings", "Services", and "System". Below this, the breadcrumb path "Internet Settings > Mobile Broadband > PPPoE" is displayed. The main section is titled "PPPoE Setup" and contains a form with the following fields:

PPPoE	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
APN Name	<input type="text"/>
Service Name	<input type="text"/>

Below the form is a "Save" button.

Figure 36: Mobile Broadband - PPPoE

- 1 Select "Enable" to enable PPPoE mode.
- 2 Specify the APN you wish to use to suit your carrier. In addition you may specify an optional "Service Name". When a "Service Name" is specified the connected device must use the same service name when connecting. This facility is particularly useful if you have more than one PPPoE router or modem on a single Ethernet network.
- 3 Finally click "Save" to save your settings and enable PPPoE.

Ethernet Related Commands

How to configure the Ethernet IP address

The IP settings can be configured by clicking on the "Internet Settings" menu followed by "LAN" and then "IP Setup"

The default IP of the Ethernet port is 192.168.20.1 with the subnet mask 255.255.255.0.

If you wish to change this then simply enter the new IP address and click on the Save button at the bottom of the page.

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

LAN Configuration				
Ethernet IP Address	192	168	20	1
Ethernet Subnet Mask	255	255	255	0

Figure 37: LAN - IP Settings

How to Configure DNS Masquerading

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

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

DNS Masquerade	
DNS Masquerade	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Figure 38: DNS Masquerading Setting

How to Configure the DHCP Server

Use the following procedure to change the router's DHCP server default settings. Ensure your PC's Ethernet connector is configured to automatically obtain an IP and DNS server address.

When you plug in the Ethernet cable to your PC, the router should automatically assign it an IP address within 10-15 seconds. Please be aware that you will be sharing the bandwidth of the router between all connected devices. You can manually set DNS1 and DNS2 or if DNS Masquerade is enabled the DHCP DNS1 address will automatically be set to the router's LAN address.

DHCP Configuration			
DHCP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
DHCP Start Range	192	168	20
DHCP End Range	192	168	199
DHCP Lease Time	86400 (seconds)		
Default Domain Name Suffix			
DNS Server 1 IP Address	0	0	0
DNS Server 2 IP Address	0	0	0
WINS Server 1 IP Address	0	0	0
WINS Server 2 IP Address	0	0	0
NTP Server (Option 42)	10.100.100.1		
TFTP Server (Option 65)	10.100.100.100		
Option 150			
Option 160			
Address Reservation List			
Computer Name	MAC Address	IP Address	<input type="button" value="Add"/>
Dynamic DHCP Client List			
Computer Name	MAC Address	IP Address	Expire Time
<input type="button" value="Refresh"/> <input type="button" value="Save"/>			

Figure 39: DHCP

This example has a start address of 100, an end address of 199, lease time of 86,400 seconds, and uses the DNS servers that are auto-assigned by the network upon connection.

If you do not enter the DNS1 and DNS2 addresses manually, then to browse the Internet from your Ethernet connected device you must enable DNS Masquerade (see above).

Upon enabling DNS Masquerade, you will notice that the DNS1 address is automatically set to the IP address of the Ethernet port. DNS addresses are then automatically assigned by the connection to the network.

How to Configure Static DHCP Assignments

This facility is available by clicking on the "Internet Settings" menu followed by "LAN" and then the "DHCP" menu item on the right.

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

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

Figure 40: Static IP Assignment

- 1 Click the Add button.

Address Reservation List			
Computer Name	MAC Address	IP Address	
<input type="text" value="Someone"/>	<input type="text" value="00:0c:29:dd:a0:b0"/>	<input type="text" value="192.168.20.100"/>	<input type="button" value="Add"/>
			<input checked="" type="checkbox"/> Enable <input type="button" value="Remove"/>

Dynamic DHCP Client List			
Computer Name	MAC Address	IP Address	Expire Time

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

How to configure your device's IP address manually (no DHCP)

If your device has a static IP address set, you can configure your device to work with the router by manually configuring your device to the following settings:





- 1 Set your device's IP address to any valid IP address between 192.168.20.2 and 192.168.20.99 or disable the DHCP server and use any address. Do not use the IP address assigned to the router's Ethernet interface.
- 2 Set your device's subnet to: 255.255.255.0.
- 3 Set your Gateway to the IP address of the router's Ethernet interface: 192.168.20.1
- 4 Set DNS (if required) to 192.168.20.1 or configure manually to your mobile broadband provider's DNS Servers.

Virtual Private Networks

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

PPTP and GRE are common encapsulation methods used to create a virtual private network (VPN) over public networks. OpenVPN and IPSec can also be configured on the NTC-6000 series routers.

The advantages of the VPN feature include:

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

Configuring a PPTP / GRE connection

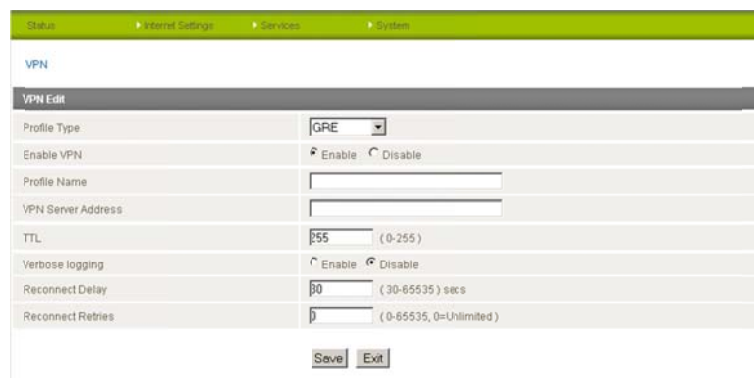
This facility is available by clicking on the "Internet Settings" menu followed by the "VPN" menu item.



The screenshot shows the "VPN Edit" configuration page for a PPTP profile. The breadcrumb trail is "Status > Internet Settings > Services > System". The "Profile Type" is set to "PPTP". The "Enable VPN" option is checked. The "Authentication Type" is set to "Any". The "Metric" is set to 0. The "Use peer DNS" option is checked. "NAT Masquerading" and "Set Default Route to PPTP" are both unchecked. "Verbose logging" is unchecked. The "Reconnect Delay" is set to 0 seconds. The "Reconnect Retries" is set to 0. "Save" and "Exit" buttons are at the bottom.

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

Figure 41: Internet Settings - VPN - PPTP






The screenshot shows the "VPN Edit" configuration page for a GRE profile. The breadcrumb trail is "Status > Internet Settings > Services > System". The "Profile Type" is set to "GRE". The "Enable VPN" option is checked. The "TTL" is set to 55. "Verbose logging" is unchecked. The "Reconnect Delay" is set to 0 seconds. The "Reconnect Retries" is set to 0. "Save" and "Exit" buttons are at the bottom.

Profile Type	GRE
Enable VPN	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable
Profile Name	<input type="text"/>
VPN Server Address	<input type="text"/>
TTL	55 (0-255)
Verbose logging	<input type="checkbox"/> Enable <input checked="" type="checkbox"/> Disable
Reconnect Delay	0 (30-65535) secs
Reconnect Retries	0 (0-65535, 0=Unlimited)







Figure 42: Internet Settings - VPN - GRE

There are a few configuration steps you will need to complete before obtaining a PPTP/GRE connection:

Step 1: Connect to the Cellular Broadband Network:

-  Click on the "Internet Settings" menu followed by "Mobile Broadband" and then the "Connection" menu item on the right and in the Mobile Broadband Profile Settings section, click 'enable' for the appropriate profile.
-  To check that the PPP interface is connected, click on the Status menu at the top of the page and check the WWAN status. The status should be shown as "UP".
-  For more details on enabling a data connection refer to the [Connection configuration](#) section of this guide.

Step 2: Enabling PPTP:





-  Click on the VPN menu item (By clicking on the "Internet Settings" menu followed by the "VPN" menu item).
-  Press the Add button and select PPTP as the profile type.
-  Set the "Enable VPN" option to "Enable".
-  Enter the PPTP/GRE server IP address and user name and passwords in the appropriate boxes.
-  Press the "Save" button.
-  To check that the PPTP/GRE interface is up, click on the Status menu and in the PPTP/GRE section, the status should be shown as "UP".



NOTE – It may be necessary to add a static route. The Gateway IP address is the same as the PPTP/GRE server address. Enter the PPTP/GRE server IP address in the Gateway IP address box.

Example:

If the PPTP/GRE server address is 203.44.251.100 and the IP address of the local PPTP/GRE interface is 10.1.3.42 (i.e. a 10.0.0.0 address) then in the static routes section (Internet Settings > Routing > Static), you would need to enter the following:

-  10.0.0.0 in the Destination IP address box
-  255.0.0.0 in the IP subnet mask box
-  203.44.251.100 in the Gateway IP address box.
-  1 in the metric box.

Editing the PPTP/GRE credentials:

If you need to edit the PPTP/GRE credentials you need to disable the existing PPTP/GRE connection and then enter the new credentials and re-enable the connection.

Disabling PPTP/GRE:

If you want to completely disconnect both the PPP and PPTP/GRE interface from the network then it is best to first disable the PPTP/GRE interface simply by clicking "Disable" and hitting "Save" and then disabling the PPP connection by clicking "Disable" for the appropriate profile number on the "Connection" configuration page.




However, if you want to leave the PPTP/GRE enabled for future use then just disable the PPP connection on the "Connection" configuration page. The next time a PPP connection is enabled the PPTP/GRE interface will also come up.

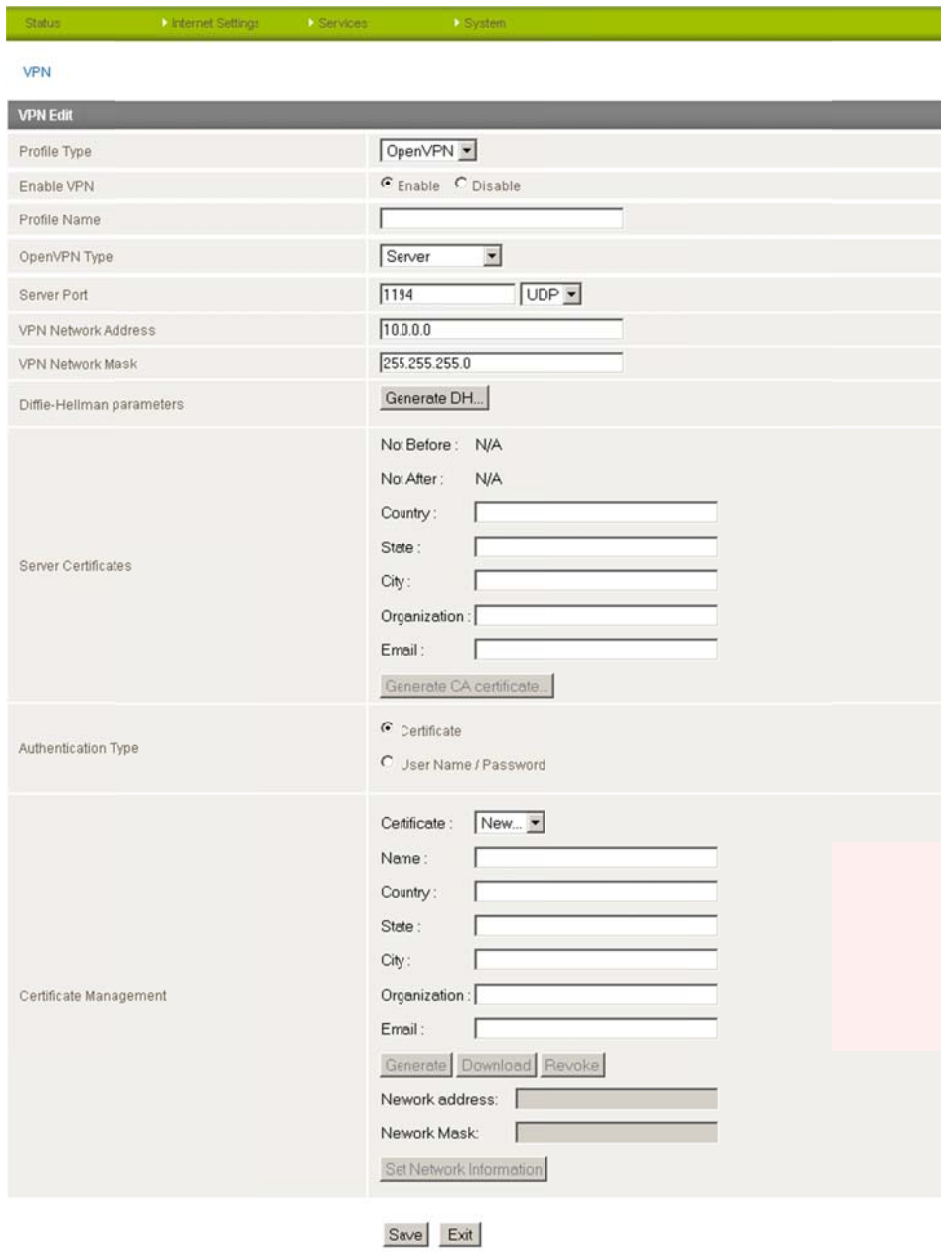


Note: GRE TTL (Time to Live) limit is 255 on the period of transmissions.

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. The NTC-6000 supports three different OpenVPN modes:

-  OpenVPN Server
-  OpenVPN Client
-  OpenVPN Peer-to-Peer VPN connection.



The screenshot shows the 'VPN Edit' configuration page. The breadcrumb trail at the top reads: Status > Internet Settings > Services > System > VPN. The main content area is titled 'VPN Edit' and contains the following fields and controls:

- Profile Type:** OpenVPN (dropdown)
- Enable VPN:** Enable Disable
- Profile Name:** (empty text input)
- OpenVPN Type:** Server (dropdown)
- Server Port:** 1114 (text input), UDP (dropdown)
- VPN Network Address:** 10.0.0.0 (text input)
- VPN Network Mask:** 255.255.255.0 (text input)
- Diffie-Hellman parameters:** Generate DH... (button)
- Server Certificates:**
 - No Before: N/A
 - No After: N/A
 - Country: (text input)
 - State: (text input)
 - City: (text input)
 - Organization: (text input)
 - Email: (text input)
 - Generate CA certificate... (button)
- Authentication Type:** Certificate User Name / Password
- Certificate Management:**
 - Certificate: New... (dropdown)
 - Name: (text input)
 - Country: (text input)
 - State: (text input)
 - City: (text input)
 - Organization: (text input)
 - Email: (text input)
 - Generate (button), Download (button), Revoke (button)
 - Network address: (text input)
 - Network Mask: (text input)
 - Set Network Information (button)

At the bottom of the form are 'Save' and 'Exit' buttons.

Figure 43: Internet Settings - OpenVPN

ITEM	DEFINITION
Profile Type	Set this option to OpenVPN to create an OpenVPN VPN tunnel.
Enable VPN	Enable or Disable the VPN connection.
Profile Name	A name that can be used to identify the VPN connection.
OpenVPN Type	Select the type of OpenVPN session to use. Options include Server, Client or Peer-to-Peer
Server Port	Enter the port number the OpenVPN connection is to run on.
VPN Network Address	Enter the network address for use on the VPN connection.
VPN Network Mask	Enter the network mask for use on the VPN connection.
Diffie-Hellman parameters	Generate the server and client keys used by the VPN connection.
Server Certificates	Enter the applicable details to identify the OpenVPN server and create a CA certificate based on this information.
Authentication Type	Select the type of authentication in use for the VPN connection. You can select from a Certificate or Username and Password combination.

Table 8: Internet Settings - VPN – OpenVPN Fields

IPSec

IPSec operates on Layer 3 of the OSI model and as such can protect higher layer protocols. IPSec is used for both Site to Site VPN and Remote Access VPN. The NTC-6000 Series Cellular routers support IPSec end points and can be configured with Site to Site VPN tunnels with other NTC-6000s or third party VPN routers.

A White Paper with full Instructions on configuring an IPSec VPN tunnel is available at <http://support.netcommwireless.com/product/m2m/ntc-6000>

The screenshot shows a web-based configuration interface for a VPN tunnel. The breadcrumb navigation at the top indicates the path: Status > Internet Settings > Services > System. The main heading is 'VPN'. Below this is a 'VPN Edit' section with the following fields:

- Profile Type: **IPSEC** (dropdown)
- Enable VPN: Enable Disable
- Profile Name: [Empty text box]

The next section is 'Remote Gateway' with the following fields:

- Remote IPsec Gateway: [Empty text box] **Road Warrior** (button)
- Remote Address/Net to Join: [IP address input fields]
- Remote Address/Net Mask: **255 . 255 . 255 . 0**

The 'Local LAN' section has the following fields:

- Local Address/Net to Join: [IP address input fields]
- Local Address/Net Mask: **255 . 255 . 255 . 0**

The 'Negotiation' section contains the following fields:

- Encap Protocol: **ESP** (dropdown)
- IKE Mode: **Main** (dropdown)
- Pfs: **On** (dropdown)
- IKE Encryption: **Any** (dropdown)
- IKE Hash: **Any** (dropdown)
- IPsec Encryption: **Any** (dropdown)
- IPsec Hash: **Any** (dropdown)
- DH Group: **Any** (dropdown)
- DPD Action: **Hold** (dropdown)
- DPD Keep Alive Time: **10** secs
- DPD Timeout: **60** secs
- Ike Rekey Time: **3600** (0-71400, 0=Unlimited) secs
- SALife Time: **28800** (0-71400, 0=Unlimited) secs
- Key Mode: **Pre Shared Key** (dropdown)
- Pre Shared Key: [Empty text box]
- Remote Id: [Empty text box] (xy.sample.com or blank)
- Local Id: [Empty text box] (xy.sample.com or blank)

At the bottom of the form are 'Save' and 'Exit' buttons.

Figure 44: VPN - IPSec Configuration Settings

Please see the table on the following page for details of the IPSec fields shown above.

ITEM	DEFINITION
Profile Type	Set this option to IPSec.
Enable VPN	Enable or Disable the VPN connection.
Profile Name	A name that can be used to identify the VPN connection.
Remote IPSec Gateway	The IP address that the IPSec server is running on.
Road Warrior	Click this to configure the VPN connection for Road Warrior (connection from a dynamic IP Address) use.
Remote Address/Net to Join	Enter the Remote IP address or Network for use on the VPN connection.
Remote Address/Net Mask	Enter the subnet mask in use on the remote network.
Local Address/Net to Join	Enter the Local IP address or Network for use on the VPN connection.
Local Address/Net Mask	Enter the subnet mask in use on the local network.
Encap Protocol	Select the encapsulation protocol to use with the VPN connection.
IKE Mode	Select the IKE mode to use with the VPN connection.
PFS	Select whether or not to use PFS (Perfect Forward Secrecy) for the VPN connection. This feature will make sure the same key is not generated twice and forces a new diffie-hellman key exchange. Both VPN endpoints must support this function in order for it to work.
IKE Encryption	Select the IKE (IPSec Key Exchange) encryption type to use with the VPN connection.
IKE Hash	Select the IKE Hash type to use for the VPN connection.
IPSec Encryption	Select the IPSec encryption type to use with the VPN connection.
IPSec Hash	Select the IKE Hash type to use for the VPN connection.
DH Group	Select the Diffie-Hellman group the VPN tunnel will use.
DPD Action	Select the appropriate DPD (Dead Peer Detection) Action to use when the VPN tunnel detects a peer dropping the VPN tunnel connection.
DPD Keep Alive Time	Enter the time in seconds for DPD to keep alive.
DPD Timeout	Enter the time in seconds for DPD to timeout.
IKE Rekey Time	Enter the appropriate IKE Rekey time for the VPN connection.
SA Life Time	Enter the appropriate SA (Security Association) Life time for the VPN connection.
Key Mode	Select the type of key mode in use for the VPN connection. You can select from: Pre Shared Key, RSA Keys or Certificates

Table 9: Internet Settings - VPN – IPSec Details

Routing Configuration

Configuring Static Routes

This facility is available by clicking on the "Internet Settings" before selecting "Routing" followed by the "Static" menu item on the right.

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

However, if you have other routers (hence networks) on the Ethernet subnet for example, you may want to add some more static routes.

Adding Static Routes

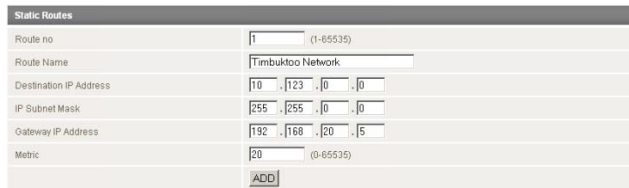


Figure 45: Adding Static Routes

- Enter the values in the fields as above.
- Click the ADD button.



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

The Active Routing table at the bottom of the screen will show the new route added as shown at the bottom of the screenshot below:



Example:

If you have another router on the Ethernet side of the router with a gateway of 192.168.20.5 that interfaces to network 10.123.0.0/16 and you want to get to a device on that network then you enter:

- 10.123.0.0 in the Destination IP address field.
- 255.255.0.0 in the IP Subnet Mask field.
- 192.168.20.5 in the Gateway IP address field.

The lower the metric value the higher the priority this route has over other routes.

Deleting Static Routes

Static Routes						
Route no	<input type="text"/> (1-65535)					
Route Name	<input type="text" value="Timbuktoo Network"/>					
Destination IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>					
IP Subnet Mask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>					
Gateway IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>					
Metric	<input type="text" value="20"/> (0-65535)					
<input type="button" value="ADD"/>						
Item	Route Name	Dest IP	Subnet Mask	Gateway IP	Metric	
0	Timbuktoo Network	10.123.0.0	255.255.0.0	192.168.20.5	20	<input type="button" value="Delete Entry"/>

Figure 47: Deleting a Static Route Entry

Select the "Delete Entry" text (in blue) for the route as shown in the figure above.

How to Configure RIP

RIP (Routing Information Protocol) is used for advertising routes to other routers. Thus all the routes in the router's routing table will be advertised to other nearby routers.

For example, the route for the router's Ethernet subnet could be advertised to a Router on the PPP interface side so that a Router on this network will know how to route to a device on the router's Ethernet subnet.

You will have to add the routes appropriately in the Static Routes section – see [Adding Static Routes](#).



NOTE: it is possible that some routers will ignore RIP.

To enable RIP click on the "Internet Settings" menu followed by "Routing" and then the "RIP" menu item on the right.

- Set the Enable RIP option to Enable.
- Select the RIP version you wish to use.
- Click Save RIP

Routing > RIP

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

Figure 48: Internet Settings - Routing – RIP

How to Configure VRRP






The Virtual Router Redundancy Protocol (VRRP) is a non-proprietary redundancy protocol designed to increase the availability and reliability of the default gateway servicing hosts on the same subnet. This increased reliability is achieved by advertising a "virtual router" (an abstract representation of master and backup routers acting as a group) as a default gateway to the host(s) instead of one physical router.

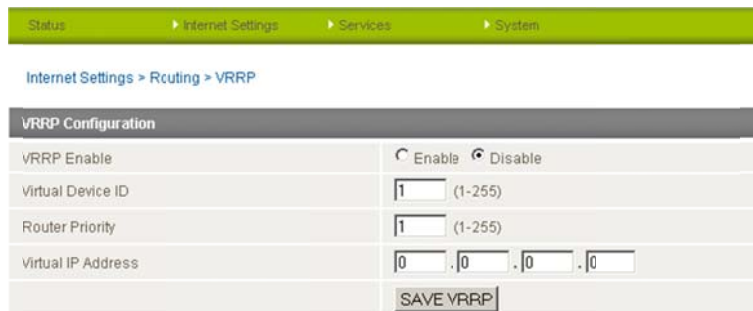
Two or more physical routers are then configured to stand for the virtual router, with only one doing the actual routing at any given time. If the current physical router that is routing the data on behalf of the virtual router fails, an arrangement is made for another physical router to automatically replace it. The physical router that is currently forwarding data on behalf of the virtual router is called the master router.

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

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

To enable VRRP click on the "Internet Settings" menu followed by "Routing" and then the "VRRP" menu item on the right.

-  Click Enable to activate VRRP.
-  Enter an ID – this is the VRRP ID which is different for each virtual router on the network
-  Enter a priority – a higher value is a higher priority.
-  Enter the VRRP IP address – this is the virtual IP address that both virtual routers share.
-  Click Save VRRP



VRRP Configuration	
VRRP Enable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Virtual Device ID	<input type="text" value="1"/> (1-255)
Router Priority	<input type="text" value="1"/> (1-255)
Virtual IP Address	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
<input type="button" value="SAVE VRRP"/>	

Figure 49: Internet Settings - Routing – VRRP





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

NAT configuration

This facility is available by clicking on the "Internet Settings" menu followed by "Routing" and then the "NAT" menu item on the right. The router is set to use NAT mode by default. With NAT enabled by default port forwarding may be necessary to use some applications and devices over the internet. Port forwarding allows remote computers or hosts to connect to a specific computer or service within a private local-area network (LAN).

How to Configure Port Forwarding

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

-  Enter the information as appropriate according to the guidelines below.
-  Click Save

ITEM	DEFINITION
Item No.	1 to as many as needed. Increment by one for each port forwarding rule.
Protocol	Options include TCP, UDP, or All protocols
Source IP Address	Specifies either a "Friendly" IP address that is allowed to access the router or a wildcard IP address of 0.0.0.0 that allows all IP addresses to access the router.
Incoming Port Range	Enter the External port(s) to listen to.
Destination IP Address	Enter the Local Area Network Address of device to forward inbound requests to.
Destination Port Range	Enter the Local Area Network Port(s) to forward connections to

Table 10: Internet Settings - Routing - NAT Options

Example:

IP Mapping Settings

Mapping no:

Protocol:

Source IP Address: . . .

Incoming Port Range: to (1-65535)

Destination IP Address: . . .

Destination Port Range: to (1-65535)

Figure 50: Internet Settings - Routing - NAT Example



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

Configured mappings are displayed shown in the screenshot below:

Item	Protocol	Incoming Address	Incoming Port	Destination Address	Destination Port	
0	tcp	0.0.0.0 (anywhere)	400 - 400	192.168.20.20	400 - 400	Delete Entry
1	tcp	10.1.2.3	500 - 550	192.168.20.60	500 - 550	Delete Entry

Figure 51: Configured NAT Mappings

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

How to Configure DMZ

The Demilitarized Zone (DMZ) enables a device to utilize a direct connection to the WAN. This means any incoming connections are forwarded directly to this device with all ports open.

This facility is available by clicking on the "Internet Settings" menu followed by "Routing" and then the "DMZ" menu item on the right.

The screenshot shows a web interface for configuring DMZ settings. At the top, there is a navigation bar with the following items: Status, Internet Settings, Services, and System. Below this, the breadcrumb path is "Firewall > DMZ". The main content area is titled "DMZ Settings" and contains two rows of configuration options:

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

At the bottom of the form, there are two buttons: "Save" and "Reset".




Figure 52: Internet Settings - Routing - NAT

Services Features

How to Configure the Dynamic DNS Client

This facility is available by clicking on the "Services" menu followed by the "DDNS" menu item on the right.

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

-  To configure dynamic DNS set the DDNS Configuration option to Enable.
-  Select the Dynamic DNS service that you wish to use. Enter your dynamic DNS account credentials.
-  Click Save



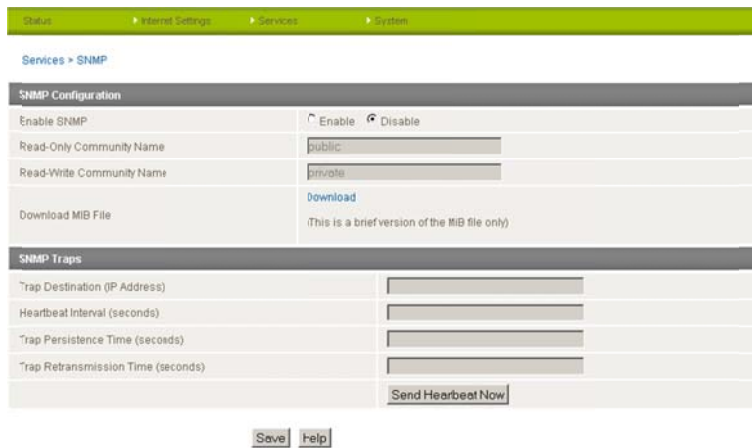
The screenshot shows the "DDNS Configuration" web interface. At the top, there is a "DDNS Configuration" section with radio buttons for "Enable" (selected) and "Disable". Below this is the "DDNS Settings" section, which includes a dropdown menu for "Server Address" set to "www.dyndns.org", a text input for "Host Name" with "myhost.dyndns.org", a text input for "User Name" with "user", a password input for "Password" with "****", and a password input for "Verify Password" with "****". At the bottom of the form are "Save" and "Help" buttons.

Figure 53: Services - Dynamic DNS

How to configure SNMP

This facility is available by clicking on the "Services" menu followed by the "SNMP" menu item on the right.




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



The screenshot shows the "Services > SNMP" web interface. It has a breadcrumb trail: "Status > Internet Settings > Services > System". The "SNMP Configuration" section includes radio buttons for "Enable" (selected) and "Disable". Below are text inputs for "Read-Only Community Name" (public) and "Read-Write Community Name" (private). There is a "Download MIB File" button with a note: "(This is a brief version of the MIB file only)". The "SNMP Traps" section includes text inputs for "Trap Destination (IP Address)", "Heartbeat Interval (seconds)", "Trap Persistence Time (seconds)", and "Trap Retransmission Time (seconds)". A "Send Heartbeat Now" button is located at the bottom of the traps section. At the very bottom of the form are "Save" and "Help" buttons.

Figure 54: Services - SNMP

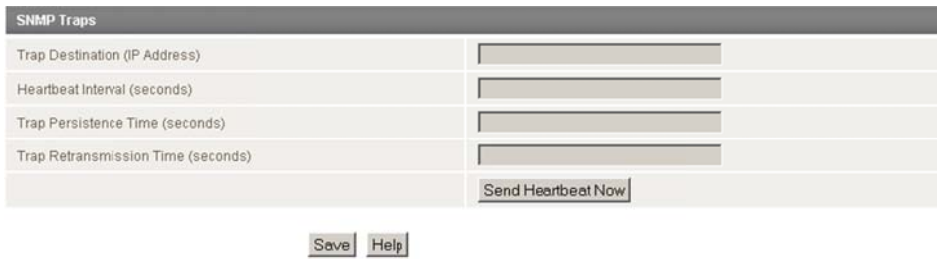
To configure SNMP:

-  Click Enable
-  Enter Community Names or leave them as default
-  Click Save.

SNMP mandates that the SNMP agents should accept request messages only if the community string in the message matches its community name. Therefore, the management application should always communicate with the agents along with the associated community name. The default SNMP community names are "public" for read-only (GET) operations and "private" for read-write (SET) operations.

SNMP Traps

The SNMP Trap functions to provide system event notifications to a SNMP server without solicitation so that the SNMP server does not have to request information from each and every device connected on the network. This helps to reduce the number of unnecessary SNMP requests across a network and reduces network traffic and resources



The image shows a configuration form for SNMP Traps. It has a title bar 'SNMP Traps' and four input fields: 'Trap Destination (IP Address)', 'Heartbeat Interval (seconds)', 'Trap Persistence Time (seconds)', and 'Trap Retransmission Time (seconds)'. Below these fields is a 'Send Heartbeat Now' button. At the bottom of the form are 'Save' and 'Help' buttons.

Figure 55: Services - SNMP Traps

Configuring the SNMP Traps settings

- Enter the Trap Destination IP Address – the address of the object that generates the trap.
- Heartbeat Interval – Enter the time in seconds between which a multicast Heartbeat notification message is generated.
- Trap Persistence Time. – Enter the time in seconds that the trap will persist before timing out
- Trap Retransmission Time – Enter the time to resend notifications on a retransmission queue.

How to Configure NTP

This facility is available by clicking on the "Services" menu followed by the "NTP" menu item on the right.

The NTP (Network Time Protocol) settings allow your router to synchronize the NTC-6000 router's internal clock with a global Internet Time server. This setting will affect functions such as System Log entries and Firewall settings.



The image shows the NTP Configuration form. It has a breadcrumb trail: 'Status > Internet Settings > Services > System'. Below this is 'Services > NTP'. The form has a title bar 'NTP Configuration' and two fields: 'Enable NTP Synchronization' with radio buttons for 'Enable' (selected) and 'Disable', and 'NTP Server Address' with a text box containing '0.netcomm.pool.ntp.org'. At the bottom are 'Save' and 'Help' buttons.

Figure 56: Services - NTP

How to Configure the Periodic Ping Reset Monitor

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

The Periodic Ping Reset Monitor configures the router to transmit controlled ping packets to 1 or 2 user specified IP addresses. Should the router not receive responses to the pings, the router will reboot.

This works as follows:

The screenshot shows a web interface for configuring the System Monitor. At the top, there is a navigation bar with 'Status', 'Internet Settings', 'Services', and 'System'. Below this, the breadcrumb 'Services > System Monitor' is displayed. The main configuration area is titled 'Periodic PING Settings' and contains the following fields:

Destination Address	<input type="text"/>
Redundant Address	<input type="text"/>
Retry Period	<input type="text"/> (0:disable, 120-65535) secs
Failure Retry Period	<input type="text"/> (0:disable, 1-65535) secs
Failures Before Reset	<input type="text"/> (0:disable, 1-65535)

Below these fields is a section titled 'Periodic Reset' with one field:

Force reset every	<input type="text"/> (0:disable, 2-65535) mins
-------------------	--

At the bottom of the configuration area, there are two buttons: 'Save' and 'Help'.

Figure 57: Services - System Monitor

1. After every "Periodic Ping Timer" configured interval, the router sends 3 consecutive pings to the "Destination Address".
2. If all 3 pings fail the router sends 3 consecutive pings to the "Second Address".
3. The router then sends 3 consecutive pings to the "Destination Address" and 3 consecutive pings to the "Second Address" every "Periodic Ping Accelerated Timer" configured interval.
4. If all accelerated pings in step C above fail the number of times configured in "Fail Count", the router reboots.
5. If any ping succeeds the router returns to step 1 and does not reboot.



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

Periodic Ping Disabled

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



The screenshot shows the 'Services > System Monitor' configuration page. It features a breadcrumb trail at the top: 'Status > Internet Settings > Services > System'. Below this, the 'Periodic PING Settings' section includes fields for 'Destination Address', 'Redundant Address', 'Retry Period' (0: disable, 120-65535 secs), 'Failure Retry Period' (0: disable, 1-65535 secs), and 'Failures Before Reset' (0: disable, 1-65535). The 'Periodic Reset' section includes a 'Force reset every' field (0: disable, 2-65535 mins). At the bottom are 'Save' and 'Help' buttons.

Figure 58: Services - System Monitor

Periodic Ping Enabled

An Example Setup:

The setup below will ping 10.1.2.3 every 10 minutes, if it fails it then tries to ping 10.1.2.4, if that also fails it then accelerates the ping attempts to once every 60 seconds and if 3 successive ping attempts at the one minute interval fails, the router will reboot.



The screenshot shows the 'Services > System Monitor' configuration page with example values. The 'Destination Address' is '10.1.2.3' and the 'Redundant Address' is '10.1.2.4'. The 'Retry Period' is '600' (0: disable, 120-65535 secs), the 'Failure Retry Period' is '60' (0: disable, 1-65535 secs), and the 'Failures Before Reset' is '3' (0: disable, 1-65535). The 'Force reset every' field is empty (0: disable, 2-65535 mins). 'Save' and 'Help' buttons are at the bottom.

Figure 59: Example Periodic Ping Setup



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

How to Configure a Periodic Reset Timer

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

The router can be configured to automatically reboot after a periodic interval 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. The default value is 0 which disables the Periodic Reset Timer. The maximum value is 65535 minutes.



Periodic PING Settings	
Destination Address	10.1.2.3
Redundant Address	10.1.2.4
Retry Period	600 (0: disable, 120-65535) secs
Failure Retry Period	60 (0: disable, 1-65535) secs
Failures Before Reset	3 (0: disable, 1-65535)

Periodic Reset	
Force reset every	0 (0: disable, 2-65535) mins

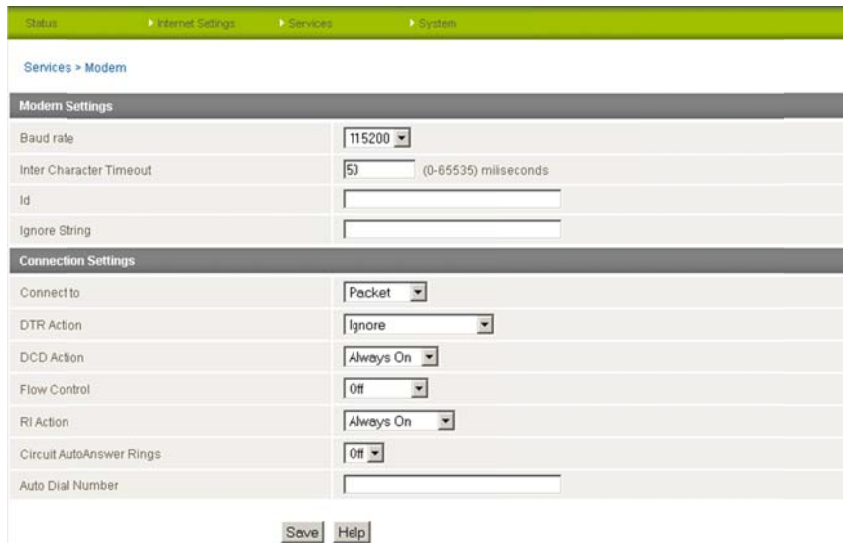
Figure 60: Services - System Monitor

How to Configure the Modem Settings

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

The modem can be utilized to communicate with serial devices via the DE-9 connector on the router. This enables the router to communicate with remote monitoring systems, as well as a variety of embedded systems utilizing serial port connections.

The modem settings can be adjusted if required to match your serial device settings.



Modem Settings	
Baud rate	115200
Inter Character Timeout	5 (0-65535) milliseconds
Id	
Ignore String	

Connection Settings	
Connect to	Packet
DTR Action	Ignore
DCD Action	Always On
Flow Control	Off
RI Action	Always On
Circuit AutoAnswer Rings	Off
Auto Dial Number	

Figure 61: Services - Modem

GPS

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

The built-in GPS module enables you to utilize location based services, keep track of hardware out in the field 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.

Select to “Enable” GPS Operation and an appropriate update interval depending on how quickly you would like the current GPS position information updated.

Click “Save” to save your GPS settings.

Services > GPS

GPS Configuration

GPS Operation: Enable Disable AGPS Update Interval: (60 - 65534 seconds)

GPS Status

Positioning Data Source: MS Assisted GPS

Date & Time: 29.11.2010 03:32:26 UTC

Latitude & Longitude: XX° XX' XX.X" S XX° XX' XX.X" E

Altitude & GEOID Hight: N/A m N/A m

Ground Speed: N/A km/h N/A knots

PDOP & HDOP & VDOP: N/A N/A N/A

GPS Device Status: Standalone Invalid Mobile Assisted Normal

Number of Satellites: 07

Index	In Use	PRN	SNR	Elevation	Azimuth
1	X	02	N/A	07	255
2	X	03	N/A	10	102
3	X	04	N/A	14	284
4	X	23	N/A	40	098
5	X	19	N/A	07	070
6	X	16	N/A	04	143
7	X	28	N/A	16	340
8	X	08	N/A	41	272
9	X	06	N/A	04	112
10	X	13	N/A	55	147
11	X	10	N/A	37	227
12	X	07	N/A	60	222

User Name: root Copyright © 2009 NetComm Limited. | All Rights Reserved

Figure 62: Services – GPS

The “GoogleMap” button provides a quick short cut to show your routers current position on a map, while the “Clock Sync” button enables you to quickly synchronize the router time from the GPS service.

Because GPS positioning relies on accurate clock settings to obtain the correct information about your location, the “Clock Sync” button enables you to quickly set the router clock to the correct time. This ensures you will always have the correct GPS position information available.

MS Assisted GPS enables the router to quickly and efficiently obtain location information by querying the cellular network for current GPS satellite and location information.









Please note: The GPS functionality is available in the NTC-6908 and NTC-6908S only, from firmware version 1.6.0 onwards.

SMS Tools

The SMS tools application has been developed to include basic SMS functionality such as sending a message, receiving a message and redirecting an incoming message to another destination. You can also utilize this functionality to read and change run-time variables on the router.

Basic functionality supported:

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

SMS Tools Setup

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

Figure 63: Services - SMS - Setup

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

Figure 64: SMS Setup Configuration Items

SMS Configuration for Redirection

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

Redirect to Mobile

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

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

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

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

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

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

SMS Configuration for Remote Diagnostics

Enable Remote Diagnostics

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

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



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



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

SMS - New Message

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

Create New Message	
Destination Number 001	<input checked="" type="checkbox"/> 61412345678
Destination Number 002	<input checked="" type="checkbox"/> 6123456543
Destination Number 003	<input type="checkbox"/>
Destination Number 004	<input type="checkbox"/>
Destination Number 005	<input type="checkbox"/>
Destination Number 006	<input type="checkbox"/>
Destination Number 007	<input type="checkbox"/>
Destination Number 008	<input type="checkbox"/>
Destination Number 009	<input type="checkbox"/>
Destination Number 010	<input type="checkbox"/>

Message Body

SMS test message 22/06/2012 #1

30 / 160

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

Send Refresh Help

Figure 65: Services - SMS - New Message

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

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

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

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

Inbox/Outbox

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

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

NetComm
www.netcomm.com.au

NetComm NTC-6908 Cellular Router

Status | Internet Settings | Services | System

Services > SMS > Inbox

Received Messages - Total 5 Messages

<input type="checkbox"/>	From	Time	Message
<input type="checkbox"/>	61412345678	Fri Apr 1 14:28:21 2011	sms test #0010 Fri Apr 1 14:28:21 UTC 2011
<input type="checkbox"/>	61412987654	Fri Apr 1 14:28:20 2011	sms test #009 Fri Apr 1 14:28:20 UTC 2011
<input type="checkbox"/>	61412345678	Fri Apr 1 14:28:19 2011	sms test #008 Fri Apr 1 14:28:19 UTC 2011
<input type="checkbox"/>	61412987654	Fri Apr 1 14:28:18 2011	sms test #007 Fri Apr 1 14:28:18 UTC 2011
<input type="checkbox"/>	61412345678	Fri Apr 1 14:28:17 2011	sms test #006 Fri Apr 1 14:28:17 UTC 2011

1 / 1

Figure 66: Services - SMS - Inbox

NetComm
www.netcomm.com.au

NetComm NTC-6908 Cellular Router

Status | Internet Settings | Services | System

Services > SMS > Outbox

Sent Messages - Total 5 Messages

<input type="checkbox"/>	To	Time	Message
<input type="checkbox"/>	61412345678	Fri Apr 1 14:31:50 2011	SMS TX test #005 Fri Apr 1 14:31:50 UTC 2011
<input type="checkbox"/>	61412987654	Fri Apr 1 14:31:49 2011	SMS TX test #004 Fri Apr 1 14:31:49 UTC 2011
<input type="checkbox"/>	61412345678	Fri Apr 1 14:31:48 2011	SMS TX test #003 Fri Apr 1 14:31:48 UTC 2011
<input type="checkbox"/>	61412987654	Fri Apr 1 14:31:47 2011	SMS TX test #002 Fri Apr 1 14:31:47 UTC 2011
<input type="checkbox"/>	61412345678	Fri Apr 1 14:31:46 2011	SMS TX test #001 Fri Apr 1 14:31:46 UTC 2011

1 / 1

Figure 67: Services - SMS - Outbox

SMS Diagnostics and Command Execution Setup

The screenshot shows the configuration page for SMS Diagnostics & Command Execution Setup. The breadcrumb trail is: Status > Internet Settings > Services > System > Services > SMS > Diagnostics & Command Execution Setup.

SMS Diagnostics & Command Execution Configuration

- Enable Authentication: Enable Disable
- Send Ack. SMS for Set Command: Enable Disable
- Send Ack. SMS to: Fixed Number SMS Sender Number
- Fixed Ack. SMS Number:
- Send Error SMS for Get/Set/Exec Command: Enable Disable
- Send Error SMS to: Fixed Number SMS Sender Number
- Fixed Error SMS Number:
- Max. Diag. SMS Tx Limit: messages per 0 / 100 messages sent

Limit the maximum number of diagnostic text messages to be sent within a certain time period. The current "messages sent" count automatically resets at the beginning of the designated time unit. For example, the counter will reset to 0 at 1:00, 2:00... for "HOUR", 00:00 for "DAY", 00:00 Monday for "WEEK" and the 1st day of the month for "MONTH".

White List for Diagnostic or Execution SMS Messages

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

Index	Destination Number	Password	Control
01	<input type="text"/>	<input type="text"/>	<input type="button" value="Delete"/> <input type="button" value="+"/> <input type="button" value="-"/>

Figure 68: Services - SMS – Diagnostics and command Execution Setup

Enable Authentication

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

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

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

This is enabled by default.



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

Send Ack. SMS for Set Command

Enable or disable sending an acknowledgement message after execution of a "Set" command.

If disabled the router does not send any acknowledgement after execution of a "Set" command. This can be useful to determine if a command was received and executed by the router. This is disabled by default.

Send Ack. SMS to

Select the destination to send an acknowledgement message to after the execution of a "Set" command.

If "Fixed Ack. SMS Number" is selected, the acknowledgement message will be sent to the predefined number in the "Fixed Ack. SMS Number" field.

If the SMS Sender Number is selected, the acknowledgement message will be sent to sender directly. The default setting is to use "SMS Sender Number".

Fixed Ack. SMS Number

Acknowledgement messages sent after the execution of a "Set" command will be sent to this number.

Send Error SMS for Get/Set/Exec Command

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

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

This function is disabled by default.

Send Error SMS to

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

If the "Fixed Number" option is selected, any error messages will be sent to the predefined number in the "Fixed Error SMS Number" field.

If the "SMS Sender Number" option is selected, any error messages will be sent to the sender directly.

The default setting is to use "SMS Sender Number".

Fixed Error SMS Number

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

Max. Diag. SMS Tx Limit

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

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





You can check the current sent message count by looking next to the "Max. Diag. SMS Tx Limit" field. If the maximum number has been exceeded, you can also reset the sent message counter by pressing the "Reset" button.

The Total transmitted message count resets after a reboot or at the beginning of the time frame specified.



Please note: Times displayed are in UTC (Coordinated Universal Time) format.

For example:

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

White List

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

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

One blank entry is shown by default and you can add or delete an entry by pressing the "+" or "-" button. The White List numbers and passwords can be cleared by pressing the "Delete" button.

To add an entry, simply enter the appropriate phone number and password and click "Save".

Message Storage for Diagnostic Messages

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

Security

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

This prevents unauthorized or accidental execution of SMS commands.

SMS Command format

Generic Format for reading variables:

- get VARIABLENAME
- PASSWORD get VARIABLENAME

Generic Format for writing to variables:

- set VARIABLENAME=VALUE
- PASSWORD set VARIABLENAME=VALUE

Generic Format for executing a command:

- execute COMMAND
- PASSWORD execute COMMAND

Replies

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

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

Table 11: SMS Command Replies

- Where "VARIABLENAME" is the name of the value to be read
- Where "VARIABLENAME(x)" is the name of another value to be read
- Where "VALUE" is the content to be written to the "VARIABLENAME"
- Where "COMMAND" is a supported command to be executed by the device (e.g. reboot)
- Where "PASSWORD" is the password (if configured) for the corresponding sender number specified in the White List.
- Multiple commands can be sent in the same message, if separated by a semicolon.
- For Example:
 - i. get VARIABLENAME1; get VARIABLENAME2; get VARIABLENAME3
 - ii. PASSWORD get VARIABLENAME1; get VARIABLENAME2
 - iii. set VARIABLENAME=VALUE1 ; set VARIABLENAME2=VALUE2
 - iv. PASSWORD set VARIABLENAME1=VALUE1; set VARIABLENAME2=VALUE2; set VARIABLENAME3=VALUE3
- If required, values can also be bound by an apostrophe, double apostrophe or back tick.

For Example:

- v. "set VARIABLE="VALUE"
- vi. "set VARIABLE="VALUE"
- vii. "set VARIABLE=`VALUE`"
- viii. "get VARIABLE"
- A password (if required), only needs to be specified once per SMS, but can be prefixed to each command if desired.
 - ix. "PASSWORD get Variable1"; "get VARIABLE2"
 - x. "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:

- xi. "PASSWORD execute reboot; get Variable1"; "get VARIABLE2"
- xii. "PASSWORD execute reboot; PASSWORD get Variable1"; "get VARIABLE2"

- Commands are case insensitive; however variable names and values are case sensitive.

List of Valid Commands (which can be used in conjunction with the execute command)

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

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

Table 12: List of Valid SMS Commands

List of Valid Variables:

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

#	RDB VARIABLE NAME	SMS VARIABLE NAME	READ/WRITE	DESCRIPTION	EXAMPLE
0	link.profile.x.enable link.profile.x.apn link.profile.x.user link.profile.x.pass link.profile.x.auth_type link.profile.x.iplocal link.profile.x.status	profile or profilex	RW	Profile	Read: (profile no,apn,user,pass,auth,iplocal,status) 1,Telstra.internet,username,password,chap,202.44.185.111,up Write: (apn, user, pass,auth) Telstra.internet,username,password
1	link.profile.x.apn	apn or apnx	RW	APN	telstra.internet
2	link.profile.x.user	username or usemamex	RW	3G username	Guest, could also return "null"
3	link.profile.x.pass	password or password	RW	3G password	Guest, could also return "null"
4	link.profile.x.auth_type	authtype or authypex	RW	3G Authentication type	"pap" or"chap"
5	link.profile.x.iplocal	wanip or wanipx	R	WAN IP address	202.44.185.111
6	wwan.0.radio.information.signal_strength	rsi	R	3G signal strength	65 dBm
7	wwan.0.imei	imei	R	IMEI number	359102128941027512
8	statistics.usage_current	usage	R	3G data usage of current session	"Rx 500 bytes, Tx 1024 bytes, Total 1524 bytes" or "Rx 0 byte, Tx 0 byte, Total 0 byte" when wwan down
9	statistics.usage_current	wanuptime	R	Up time of current 3G session	1 days 02:30:12 or 0 days 00:00:00 when wwan down
10	/proc/uptime	deviceuptime	R	Device up time	1 days 02:30:12
11	wwan.0.system_network_status.current_band	band	R	Current 3G frequency	WCDMA 850

Table 13: SMS - Valid Variables

SMS Diagnostics Examples

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

DESCRIPTION	AUTHENTICATION	INPUT EXAMPLE
Send SMS to change APN	Not Required	set apn1=Telstra.internet set apn2="3netacccss"
	Required	Password1234 set apn1=Telstra.internet Password1234 set apn2=3netacccss
Send SMS to change the 3G username	Not Required	set username='NetComm'
	Required	Password1234 set username= "NetComm"
Send SMS to change the 3G password	Not required	set password= 'NetComm'
	Required	Password1234 set password= 'NetComm'
Send SMS to change the 3G authentication	Not required	set authtype= 'pap'
	Required	Password1234 set authtype = pap
Send SMS to reboot	Not Required	execute reboot
	Required	Password1234 execute reboot
Send SMS to check the WAN IP address	Not Required	get wanip
	Required	Password1234 get wanip
Send SMS to check the 3G signal strength	Not Required	get rssi
	Required	Password1234 get rssi
Send SMS to check the IMEI number	Not Required	get imei
	Required	Password1234 get imei
Send SMS to check the current band	Not Required	get band
	Required	Password1234 get band
Send SMS to Disconnect (if disconnected) and reconnect the 3G connection	Not Required	execute pdpcycle
	Required	Password1234 execute "pdpcycle1"
Send SMS to disconnect the 3G connection	Not Required	execute pdpdown1
	Required	Password1234 execute "pdpdown1"
Send SMS to connect the 3G connection	Not Required	execute pdpup
	Required	Password1234 execute pdpup 1
Send multiple get command	Not Required	get wanip; get rssi
	Required	Password1234 get wanip; get rssi
Send multiple set command	Not Required	set apn1="3netacccss"; set password1='NetComm'
	Required	Password1234 set apn="3netacccss"; set password=NetComm

Table 14: SMS Diagnostics Command Examples

NSUpdate

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

Figure 69: Services - NSUpdate

FIELD	DESCRIPTION
Server Address	The server address is the name server to which updates will be sent to.
Secondary Server Address	The secondary server address is a backup name server to which updates will be sent to.
DNS Zone	Specify the DNS domain to be updated.
Host Name	Specifies the changes to be made to one or more DNS records.
Expiry Time (in minutes)	The newly-added records' time to live.

Table 15: Services – NSUpdate

System Features

Viewing the system log

This facility is available by clicking on the "System" menu followed by "Log".

System > Log

Log File Display Level Page 1 of 29

Date & Time	Machine	Level	Process	Message
Sunday, 1 January 2012 1:01:17 p.m.	NTC-6000	user.err	modem_emulator	interrATCmd: AT+ICCID? does not respond
Sunday, 1 January 2012 1:01:09 p.m.	NTC-6000	user.err	modem_emulator	interrATCmd: AT+ICCID? does not respond
Sunday, 1 January 2012 1:01:07 p.m.	NTC-6000	daemon.info	dismasq-dhop[2118]	DHCPACK(bnd) 192.168.20.171 00:0f:b0:fa:92:57 techsupport-laptop
Sunday, 1 January 2012 1:01:07 p.m.	NTC-6000	daemon.info	dismasq-dhop[2118]	DHCPINFORM(bnd) 192.168.20.171 00:0f:b0:fa:92:57
Sunday, 1 January 2012 1:01:04 p.m.	NTC-6000	daemon.info	dhcp_lease_update[2288]	adding lease
Sunday, 1 January 2012 1:01:04 p.m.	NTC-6000	daemon.info	dhcp_lease_update[2288]	event = add, mac = 00:ff:b0:fa:92:57, ip = 192.168.20.171, host = techsupport-laptop, expiry = 86463
Sunday, 1 January 2012 1:01:03 p.m.	NTC-6000	daemon.info	dismasq-dhop[2118]	DHCPACK(bnd) 192.168.20.171 00:0f:b0:fa:92:57 techsupport-laptop
Sunday, 1 January 2012 1:01:03 p.m.	NTC-6000	daemon.info	dismasq-dhop[2118]	DHCPREQUEST(bnd) 192.168.20.171 00:0f:b0:fa:92:57
Sunday, 1 January 2012 1:01:03 p.m.	NTC-6000	daemon.info	dismasq-dhop[2118]	DHCPOFFER(bnd) 192.168.20.171 00:0f:b0:fa:92:57
Sunday, 1 January 2012 1:01:03 p.m.	NTC-6000	daemon.info	dismasq-dhop[2118]	DHCPDISCOVER(bnd) 192.168.20.171 00:0f:b0:fa:92:57
Sunday, 1 January 2012 1:01:01 p.m.	NTC-6000	user.err	modem_emulator	interrATCmd: AT+ICCID? does not respond
Sunday, 1 January 2012 1:00:57 p.m.	NTC-6000	user.notice	kimel	[57.940000] JFFS2 notbe: (415) check_node_data: wrong data CRC in data node at 0x01cb5354: read 0xfe0a0e64, calculated 0x181d301e.
Sunday, 1 January 2012 1:00:53 p.m.	NTC-6000	user.err	modem_emulator	interrATCmd: AT+ICCID? does not respond
Sunday, 1 January 2012 1:00:40 p.m.	NTC-6000	local5.err	cis-manager[2024]	sierracs_writeNotify Enable(18, 0xf0c) = 1
Sunday, 1 January 2012 1:00:40 p.m.	NTC-6000	local5.err	cis-manager[2024]	sierracs_writeNotify Enable(17, 0xf0b) = 1
Sunday, 1 January 2012 1:00:40 p.m.	NTC-6000	local5.err	cis-manager[2024]	sierracs_writeNotify Enable(16, 0xf0e) = 1
Sunday, 1 January 2012 1:00:40 p.m.	NTC-6000	local5.err	cis-manager[2024]	sierracs_writeNotify Enable(15, 0xf0a) = 1
Sunday, 1 January 2012 1:00:40 p.m.	NTC-6000	local5.err	cis-manager[2024]	sierracs_writeNotify Enable(14, 0x100f) = 1
Sunday, 1 January 2012 1:00:40 p.m.	NTC-6000	local5.err	cis-manager[2024]	sierracs_writeNotify Enable(13, 0x1042) = 1

[Download Log File](#)

Figure 70: System Log Page

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

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






Remote Administration

This facility is available by clicking on the "System" menu followed by "Administration".

Once Remote administration is enabled, you are able to access the router's web-based configuration pages from a remote location to make configuration changes and to enable or disable features.

To get remote access, you have to connect to the WAN IP address of the router on the port assigned in the configuration page (e.g. 8080) after a connection to the cellular network via a data connection has been established.

To configure Remote Administration follow the steps below:

-  Click "Enable HTTP" to activate Remote Administration
-  Change the Remote Administration Port number if required; the factory default is 8080.
-  If you wish to use Telnet or ping the router select these options.
-  You may change the remote access password for enhanced security.
-  Click "Save"



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

Figure 71: System – Administration

The WAN IP address below is an example only, yours will be different.

http://10.10.0.10:8080	
Username	admin
Password	admin

Table 16: Remote Admin Login Details

http://10.10.0.10:8090	
Username	root
Password	admin

Table 17: Remote Root Login Details

The steps below illustrate how to access the router's configuration page remotely (from a remote computer):

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



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

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

The screenshot shows a web interface with a green header containing 'Status', 'Login', and 'Log' tabs. Below the header is a 'Login' section with a dark grey title bar. Underneath, there are two input fields: 'User Name:' with 'admin' entered and 'Password:' with masked characters. At the bottom of the form are 'Clear' and 'Submit' buttons.

Figure 72: Login Screen



Note: To perform functions like Firmware upgrade, device configuration backup and to restore and reset the router to factory defaults, you need to be logged in as the root user.

Saving a Copy of the Router's Configuration

This facility is available by clicking on the "System" menu followed by "Load / Save" and then the "Settings" menu item on the right.

To save a copy of the router configuration settings you need to login in the root manager mode.

To login to the router in root manager mode, please use the following login details:

http://192.168.20.1	
Username	root
Password	admin

Key in the root manager Password of "admin" and click Save.

The screenshot shows a breadcrumb trail: 'Status > Network Settings > Services > System'. Below this is 'System > Load/Save > Settings'. A dark grey bar contains the text 'Save a copy of current settings:'. Below that are two input fields: 'Password' (masked) and 'Confirm Password'. A 'Save' button is at the bottom.

Figure 73: System - Load/Save – Settings

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



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

Restoring a Copy of the Router's Configuration

This facility is available by clicking on the "System" menu followed by "Load / Save" and then the "Settings" menu item on the right.




-  Click Browse.
-  Select the configuration file you wish to restore.
-  Click Restore.



Figure 74: Restoring a Copy of the Router's Configuration

Restoring the Router's Configuration to the Factory Defaults

This facility is available by clicking on the "System" menu followed by "Load / Save" and then the "Settings" menu item on the right.



Figure 75: Restoring the Router Configuration to Factory Default Settings

Click Restore to restore the factory default configuration settings.

Upgrading the Router's System or Recovery Console Software Version

This facility is available by clicking on the "System" menu followed by "Load / Save" option and then the "Upload" option on the right.

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



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

Local Firmware Upgrade

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

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



Figure 76: System - Load/Save - Upload

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

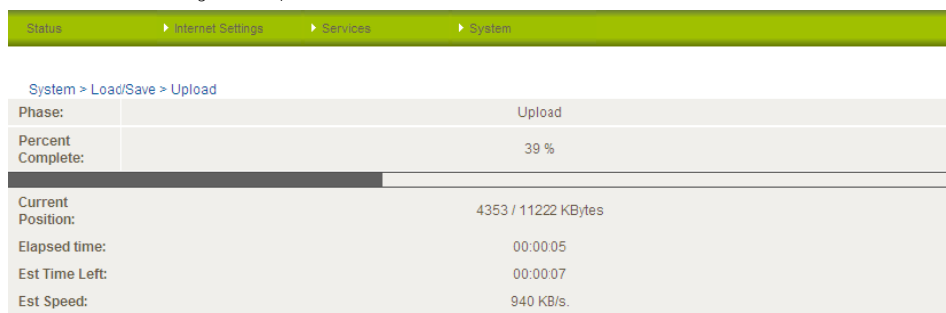


Figure 77: System - Load/Save - Firmware Upgrade Process

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



Figure 78: Firmware Install Link

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

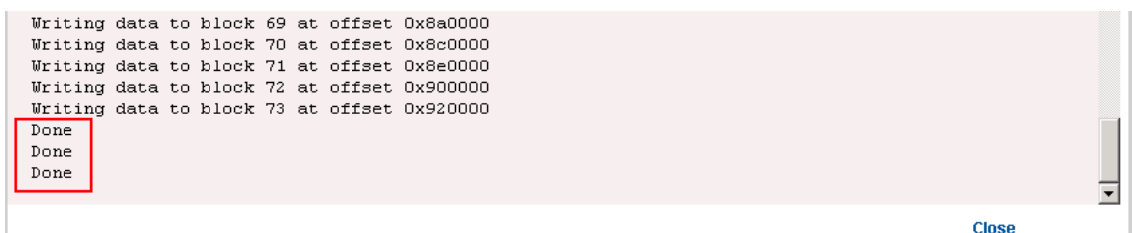


Figure 79: Firmware Upgrade Done Message

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

The second step is to upload and install the main system software image. To do this, open your web browser (e.g. Internet Explorer/Firefox/Safari) and navigate to <http://192.168.20.1/>

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

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



Figure 80: NTC-6908 Recovery Console Banner

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

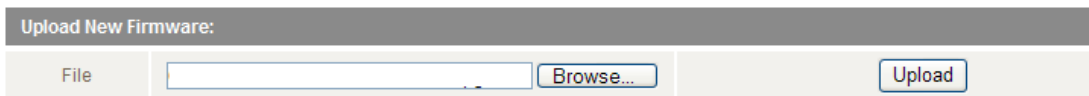


Figure 81: System - Load/Save - Upload Firmware

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

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

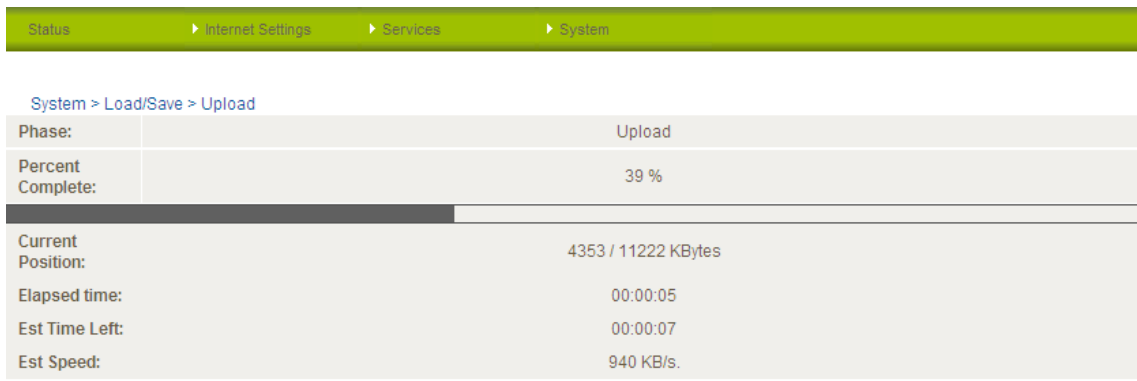


Figure 84: Recovery Console- Firmware Uploading Example

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

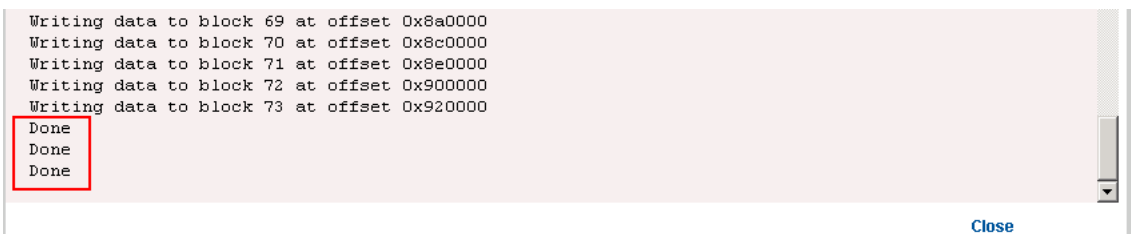


Figure 85: Main Firmware Image - Done Message

Remote Firmware Upgrade

The remote firmware update process has two steps:

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



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

The first step is to upload and install the system recovery image onto the router. You can do this by clicking on the browse button and then navigating to where the recovery image upgrade file is located on your computer.

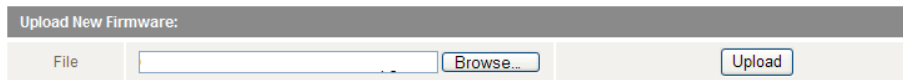


Figure 86: System - Load/Save - Upload Firmware

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

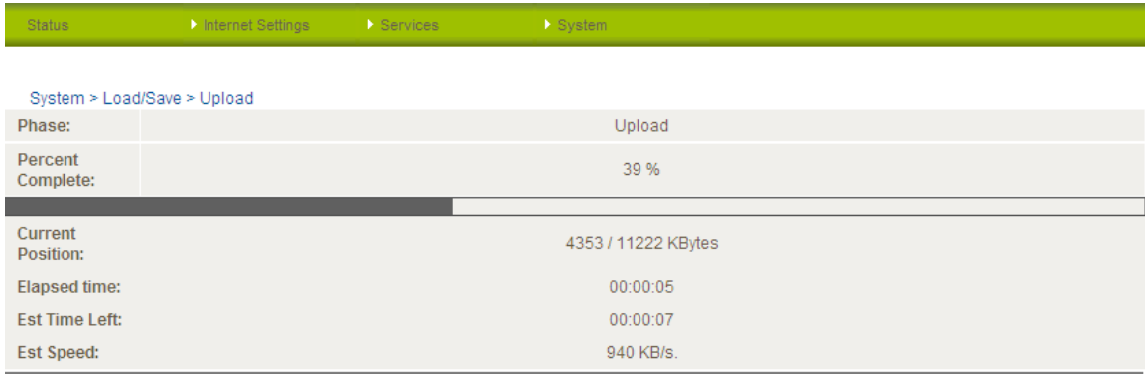


Figure 87: Uploading Firmware File

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



Figure 88: Firmware Install Link

Once you see "Done" shown as per the screenshot below,

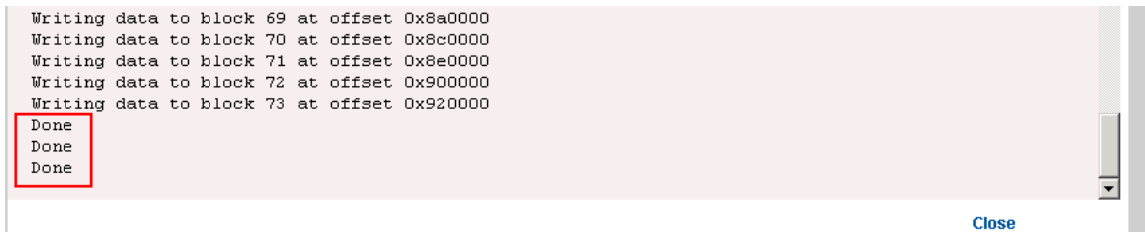


Figure 89: Firmware Upgrade Done Message

The second step is to upload and install the main system software image. Click on the browse button again and navigate to where the main system image upgrade file is located on your computer

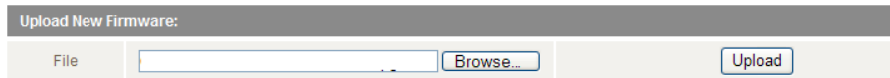
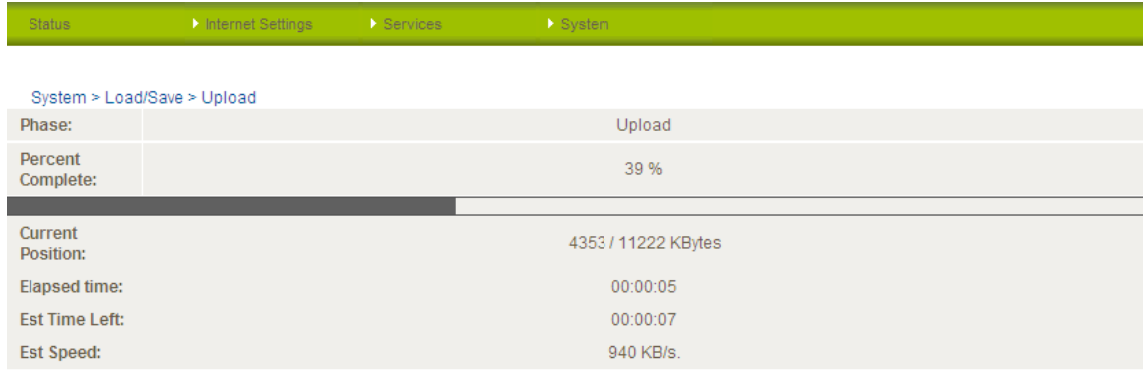


Figure 90: System - Load/Save - Upload Firmware

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



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

File	Action
9.2k	Install Delete

Once the install has completed, the router will automatically reboot, install the new main system image and then start up and reconnect to your selected Internet service.



Note: This process can take up to 10 minutes.

Package Manager

The package manager page lists additional software that has been installed to the router offering extra functionality to the router.



Figure 91: System - Load/Save - Package Manager

System Configuration

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

TCP Keepalive can be used to ensure the WWAN connection does not become disconnected due to inactivity by periodically sending a ping request message to a WAN IP address or domain to confirm the network connection is still valid.

Figure 93: System Configuration Page

OPTION	DEFINITION
IP / Hostname [PORT]	The IP address and port of the external syslog server you would like logging information sent to.
Keepalive	Select to enable or disable the TCP Keepalive function.
Keepalive Time	The interval between the last packet sent and the first TCP keepalive packet being sent.
Keepalive Interval	The time between subsequent TCP Keepalive packets.
Keepalive Probes	The number of TCP Keepalive packets to send.
Diagnostic Configuration	Select this option to enable diagnostic configuration mode.
Diagnostic TCP Port	Enter the port number you wish the diagnostic information sent to.

Table 18: System Configuration Settings

TR-069

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

TR-069 uses a bi-directional SOAP/HTTP-based protocol based on the application layer protocol. Some cellular specific vendor extensions are supported by the NTC-6000 series routers, with the data model available on request from NetComm.



Note: In order to access and configure the TR-069 settings you must be logged into the router as the root user.

Figure 94: System - TR-069

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

Table 19: System - TR-069 Options

Logoff

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

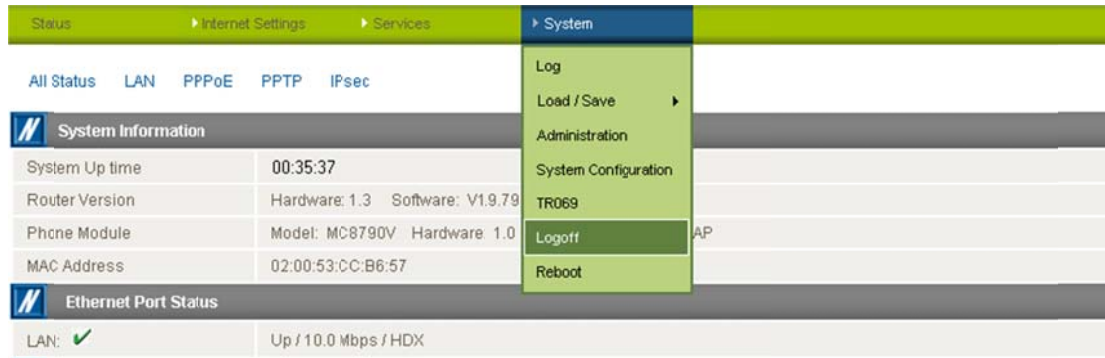


Figure 95: System - Logoff

Reboot

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

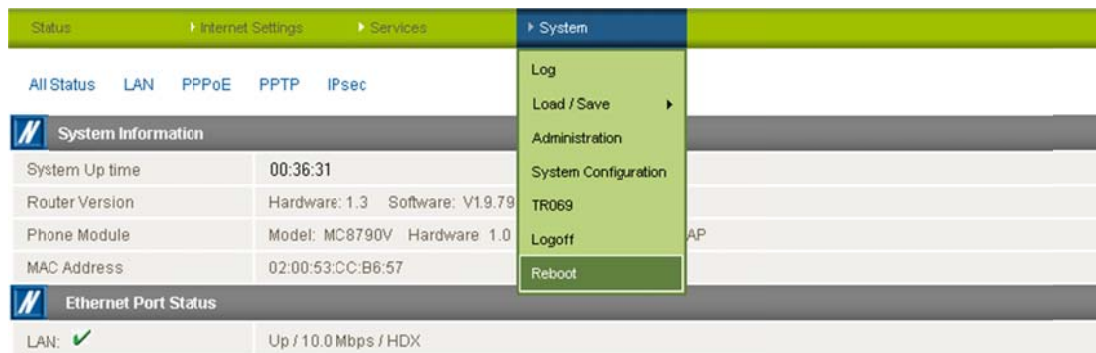


Figure 96: System - Reboot

Troubleshooting

Common problems and solutions.

1. I cannot seem to access the web page interface.

The default IP address of the router is 192.168.20.1, so first try to open a web browser to this address. Also check that your laptop/PC is on the same subnet as the router's Ethernet port if you are using a static IP address.

2. The router was connected but cannot get back online.

You may need to enable the periodic ping timer using the System Monitor (Click on the "Services" menu followed by "System Monitor"). This ensures that if the connection drops (i.e. outage on the network), the router will reboot after so many failed pings and then force a re-connect. Setting the timer to around 15 minutes should be sufficient.



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

3. The router is rebooting frequently.

Check the "System Monitor" configuration and see if the "force reset every" option is set to something other than 0. If it is set to 1 this means the unit will reboot every minute regardless of what happens. Reset it to 0 if you don't want this feature or something quite large if you don't want the router to reboot so often.

4. The router has a connection but cannot access the internet.

Check that DNS Masquerade is enabled by clicking on the "Internet Settings" menu followed by "LAN" and then the "IP Setup" menu item on the right. Make sure that the DHCP DNS server address is set to the same address as that of the Ethernet port.

5. I cannot seem to get a cellular WAN connection.

- i. Check the WWAN Status field on the router's Status page. If the modem is connected to your mobile broadband provider the Status field will report that it is "Up". There will also be a WAN IP address assigned to the router. If this is not the case check which profile and APN is in use and proceed to the next step.
- ii. Click on the "Internet Settings" menu followed by "Mobile Broadband" and then the "Connection" menu item on the right and check that the correct profile is enabled and the APN is correct.
- iii. Also check that the username and password credentials are correct if the APN in use requires these.
- iv. Make sure that Auto Connect is enabled.

6. I have set the Band but now it does not show the correct Frequency on the Status page and I cannot get a connection.

If this happens you must reboot the router.

7. The SIM status indicates "SIM removed" on the status page.

If a SIM was installed correctly this may indicate that the SIM has been removed or inserted whilst the unit is powered up. In this case you must reboot the unit. To reboot the router, click on the "System" menu followed by "Reboot". Clicking the reboot button on this page will reboot the router.

8. I am having problems getting a PPTP connection.

Check the routes on the "Routing" configuration page (This facility is available by clicking on the "Internet Settings" menu followed by "Routing" and then the "Static" menu item on the right.)

- i. There should be 5 routes shown.
- ii. One route for interface eth0.
- iii. Two routes for interface ppp0.
- iv. Two routes for interface ppp1.

If there are not 5 routes, it is possible the one of the following conditions exist:

- i. PPTP is not enabled.
- ii. The credentials on the PPTP Configuration page are incorrect (IP address / Username / Password).
- iii. If you see the message: "The synchronous PPTP option is not activated" or "CHAP Authentication Failure", then the credentials are incorrect.

Specifications

Hardware Specifications

	NTC-6908	NTC-6909	NTC-6900
MCU / Processor	Atmel AT91SAM9G20 Microcontroller / ARM9 based		
RAM	32MB DRAM		
Memory	256MB NAND Flash		
Wireless WAN Interface	Sierra Wireless MC8790V	Sierra Wireless MC8792V	Sierra Wireless MC8795V
Chipset	Qualcomm MSM6290		
3G UMTS Bands	850/ 1900/ 2100 MHz	900/ 1900/ 2100 MHz	850/ 900/ 1900/ 2100 MHz
2G GSM Bands	850/ 900/ 1800/ 1900 MHz		
Peak Data Speed	HSDPA Category 8 – Downlink up to 7.2 Mbps HSUPA Release 6 – Uplink up to 5.76 Mbps EDGE Multi Slot Class 12 – Downlink/Uplink up to 236 kbps		
SIM Card Reader	Locking Tray for SIM/SIM in Mini-SIM card format (25.00 x 15.00 x 0.76 mm)		
Antenna Interface	2x SMA (female), 50 Ohm		
Network Interfaces	1x Fast Ethernet 10/100Base-TX RJ-45 port with Auto MDI/MDIX 1x Serial RS-232 DE-9 female DCE port		
LED Indicators	5x LEDs: Power, Service, Tx/Rx, DCD, RSSI		
Power Input	Captive DECA® Euro Type Terminal Block MC100#50802 (DC Plug with Screw Terminal)		
Input Voltage Range	8 - 28 VDC		
Power Consumption	Idle: 1.32W (110 mA @ 12 V DC)		
	Active HSUPA connection: 3.6W (300 mA @ 12 V DC)		
	Maximum: 6.72W (560 mA @ 12 V DC)		
Dimensions	127 x 103 x 29 mm		
Weight	240g		
Temperature / Humidity	Operating: -30°C ~ 70°C (-22 ~ 140 F) / 0 ~ 85% (non-condensing) Storage: -55°C ~ 85°C (-67 ~ 185 F) /		
Regulatory Compliancy	A-Tick, RoHS		

Table 20: Hardware Specifications

RJ-45 Ethernet Port Integration Parameters

You can use the guide below to design Ethernet cables to integrate the router into your systems. Below you will find pin outs of the RJ-45 Ethernet Plug and Jack connectors:

PIN	FUNCTION	COLOUR
1	TX+	White/Orange
2	TX-	Orange/White
3	RX+	White/Green
4		Blue/White
5		White/Blue
6	RX-	Green/White
7		White/Brown
8		Brown/White

Table 21: Ethernet Port Integration Parameters



NOTE: The Ethernet port on the router supports Auto MDI/MDIX; you may use a straight through or cross-over Ethernet cable.

RS-232 Serial Port Integration Parameters

You can use the table below to design serial cables to integrate the router into your system.

Standard RS-232 DE-9 Pinout:

PIN	FUNCTION	DIRECTION	DESCRIPTION
1	CD	-->>	Carrier Detect
2	RX	-->>	Receive Data
3	TX	<<--	Transmit Data
4	DTR	<<--	Data Terminal Ready
5	GND		System Ground
6	DSR-	-->>	Data Set Ready
7	RTS	<<--	Request to Send
8	CTS	-->>	Clear to Send
9	RI	-->>	Ring Indicator

Table 22: RS-232 DB-9 Pin out

Note:

—>> Output from router

<<— Input to router



Shown below are the communications parameters of the RS-232 port:

OPTION	DEFINITION
Bits per Second	115200
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	Hardware

Table 23: RS-232 Communication Parameters

Custom Application and Scripting

The NTC series router covered in this manual offers the ability for the user to install custom application and firmware images via the application programming interface.

For further information, please contact the NetComm M2M support team.

CONTACT	DETAILS
Phone	+61 (02) 9424 2053
Fax	1800 063 962
Email	service@call-direct.com.au
Web	www.netcommwireless.com

Table 24: NetComm Contact Details

Legal & Regulatory Information

Intellectual Property Rights

All intellectual property rights (including copyright and trade mark rights) subsisting in, relating to or arising out of this Manual are owned by and vest in NetComm 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:
 - iv. Change the direction or relocate the receiving antenna.
 - v. Increase the separation between this equipment and the receiver.
 - vi. Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
 - vii. Consult an experienced radio/TV technician for help.
4. The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm Wireless. Failure to do so may cause damage to this product, fire or result in personal injury.

Consumer Protection Laws

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

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

Product Warranty

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

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

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

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

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

Limitation of Liability

This clause does not apply to New Zealand consumers. Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see the [Consumer Protection Laws](#) Section above), NetComm Wireless Limited accepts no liability or responsibility, for consequences arising from the use of this product. NetComm Wireless Limited reserves the right to change the specifications and operating details of this product without notice.

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

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

FCC Regulations:

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

● This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the

instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

▶ RF Exposure Information

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

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

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

IC Regulations:

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

- (1) this device may not cause interference, and
- (2) this device must accept any interference, including interference that may cause undesired operation of the device.

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

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

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

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

IMPORTANT NOTE:

IC Radiation Exposure Statement:

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

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