



NTC-550 Series User Guide

NTC-551
NTC-552

Part Number PMD-00305
Revision A July 2025

Trademark Notice

This product may reference NetComm. On December 26, 2024, Lantronix, Inc. acquired the Industrial Internet of Things (IIoT) product portfolio from NetComm Wireless Pty Ltd and is authorized to use the NetComm trademark in association with this product.

Intellectual Property

© 2025 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

Lantronix is a registered trademark of Lantronix, Inc. in the United States and other countries.

Patented: <https://www.lantronix.com/legal/patents/>. Additional patents pending.

Warranty

For details on the Lantronix warranty policy, please go to our web site at <https://www.lantronix.com/support/warranty/>.

Contacts

Lantronix, Inc.
48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support

Online: www.lantronix.com/technical-support/

Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix website at <https://www.lantronix.com/about-us/contact/>.

Disclaimer

All information contained herein is provided “AS IS.” Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user’s access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

Important Notice

This device, like any wireless device, operates using radio signals which cannot guarantee the transmission and reception of data in all conditions. While the delay or loss of signal is rare, you should not rely solely on any wireless device for emergency communications or otherwise use the device in situations where the interruption of data connectivity could lead to death, personal injury, property damage, data loss, or other loss. Lantronix accepts no responsibility for any loss or damage resulting from errors or delays in transmission or reception, or the failure of the Lantronix NTC-550 Series to transmit or receive such data.

Safety and Hazards



Warning: Do not connect or disconnect cables or devices to or from the USB port, SIM card tray, Ethernet port or the terminals of the power connector in hazardous locations such as those in which flammable gases or vapours may be present, but normally are confined within closed systems; are prevented from accumulating by adequate ventilation; or the location is adjacent to a location from which ignitable concentrations might occasionally be communicated.

Revision History

Date	Rev.	Comments
July 2025	A	Initial document

For the latest revision of this product document, please check our online documentation at <https://www.lantronix.com/support/documentation/>.

Contents

1. Overview	10
Introduction	10
Target audience	10
Prerequisites	10
Notation	10
2. Product introduction	11
Product overview	11
Product features	11
Package contents	11
Ordering Information	11
Product Label	12
3. Physical dimensions and indicators	13
Physical dimension	13
Interfaces	14
LED indicators	16
Signal strength LEDs	17
LED update interval	17
Ethernet port LED indicators	18
4. Placement of the router	19
Antenna Installation	19
Mounting Options	20
Wall Mount	20
Ceiling Mount	20
Desk Mount	21
Mounting Using DIN Rail Mounting Kit	21
5. Installation and configuration of the NTC-550 Series router	23
Powering the router	23
DC power via 6-way connector	23
DC power via field terminated power source	23
Installing the router	24
6. Advanced configuration	25
Initialization	25
Configure as a new device (create new passwords)	25

Logging In.....	27
7. Status	28
System Information.....	30
Cellular Connection Status	30
WWAN Connection Status	31
Ethernet WAN Connection Status	32
Wi-Fi Status	32
Advanced Status	33
4G LTE Neighboring Cell Information.....	35
5G NR Neighboring Cell Information.....	35
2.5GE LAN/WAN	36
1GE LAN	36
WAN	36
8. Networking	37
Cellular settings	37
SIM security	37
SIM switching.....	37
Network bands	39
Operator selection	40
Cell lock list	41
WAN profiles	42
5G Network Slicing	47
Service assurance	51
LAN Settings	52
LAN	52
DHCP	53
VLAN	56
Wi-Fi Settings.....	58
Wi-Fi mode	58
Access Point configuration.....	59
Wi-Fi client	61
WAN Settings.....	63
Interface assignment	63
WAN configuration.....	64
Failover	65

Routing settings	69
Static routes	69
Firewall.....	70
DMZ	72
Port forwarding.....	73
Filtering	74
Redundancy (VRRP).....	77
RIP	80
VPN.....	81
IPSec	81
OpenVPN	84
GRE Tunnelling.....	91
Server Certificate	92
9. Services.....	95
Network time (NTP)	95
SMS messaging	96
Setup.....	96
Diagnostics	98
Inbox	111
Compose Message	111
Outbox	112
Dynamic DNS	113
DNS server.....	113
GPS	115
GPS Configuration	115
Assisted GPS	116
GPS Odometer	117
GPS Geofence	118
Remote management.....	121
OMA-LWM2M	121
SNMP	124
Configuring SNMP	124
Configuring SNMP traps.....	124
TR-069.....	125
Internet of Things	127

MQTT	127
Cumulocity agent	132
Serial data status	134
Data stream manager.....	134
Endpoints	134
Data stream	146
Event Configuration	148
Event Notification Configuration	149
Destination configuration	149
Event notification log.....	151
Email Settings	152
Low power mode	154
IO configuration.....	156
10. System	159
Log.....	159
System log	159
System log settings.....	159
Diagnostic log	161
IPSec log	163
Watchdog.....	164
Periodic ping	164
Periodic reboot	166
System configuration	167
LDAP Settings.....	167
Restore factory defaults	168
Web server setting	169
Administration settings.....	170
Settings backup/restore.....	171
Site and location settings.....	172
Runtime configuration.....	173
SSH key management	173
LED operation mode	176
A/B system configuration.....	177
Firmware upgrade.....	178
Updating the router firmware	178

SD Card	179
Access control.....	179
Reboot	181
Field test	182
Encrypted debuginfo	183
USB-OTG	184
Storage.....	184
Voltage Monitor.....	186
11. Help	187
Appendix A. Configuring Radio Access Technologies	188
Appendix B. Inputs / Outputs	189
Hardware Interface	189
Wiring examples	190
Open Collector Output driving a relay	190
Logic level output.....	190
LED output	190
Digital inputs	191
NAMUR sensor	192
Analogue Sensor with Voltage output	192
Analogue Sensor with 4 to 20mA output	193
Analogue Sensor with Thermistor	193
System Example – Solar powered router with battery backup.....	194
Power detection (ignition) input	195
Appendix C. Compliance Information	196
EU Declaration of Conformity	197
EU Statements	198
UK Declaration of Conformity	203

1. Overview

Introduction

This document provides you all the information you need to set up, configure and use the Lantronix NTC-550 Series router.

Target audience

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

Prerequisites

Before continuing with the installation of your NTC-550 Series router, please confirm that you have the following:

- An electronic computing device with a working Ethernet network adapter
- A web browser such as Mozilla Firefox® or Google Chrome™

Notation

The following symbols may be used in this document:



Note: *This note contains useful information.*



Important: *This is important information that may require your attention.*



Warning: *This is a warning that may require immediate action to avoid damage or injury.*

2. Product introduction

Product overview

The NTC-550 Series routers are high-end, high-speed industrial-grade 5G routers. Designed with critical and complex applications in mind, it provides ultra-reliable, high bandwidth throughput even in extremely demanding environments.

The NTC-550 Series features support the latest wireless technologies including Release 16 5G and Wi-Fi 6 to ensure access to the latest innovations and the best possible throughput at a world-leading price point.

Ideal for use in emergency vehicles, trucks, and buses, or as the core of complex systems to monitor and control critical infrastructure in remote, unmanned locations.

Product features

- 5G with failover to 4G
- Wi-Fi 6 and Bluetooth support (Bluetooth support not available in current firmware.)
- Multiple gigabits per second ports
- Built-in GPS
- Serial port, I/Os and Ignition sensing
- Robust, ruggedized industrial-grade metal housing and a wide operating temperature range
- Designed, assembled, and tested for unmanned locations in extreme environments

Package contents

The Lantronix NTC-550 Series router package contains:

- 1 x NTC-550 Series router
- 1 x Six-way terminal block
- 1 x 1 m Ethernet cable
- 1 x DIN rail mounting kit
- 1 x Welcome Card
- 1 x Compliance sheet

If any of these items are missing or damaged, please contact your sales representative or the support team.

Ordering Information

Model	Lantronix Part Number	Description
NTC-551	NTC-551-01-01	5G Release 16 Sub 6 Industrial Grade 5 Port Router with Wi-Fi for North America
NTC-552	NTC-552-01-01	5G Release 16 Sub 6 Industrial Grade 5 Port Router with Wi-Fi, Global

Product Label

Figure 2-1 NTC-552 Product Label



3. Physical dimensions and indicators

Physical dimension

Figure 3-1 NTC-550 Series top and side views

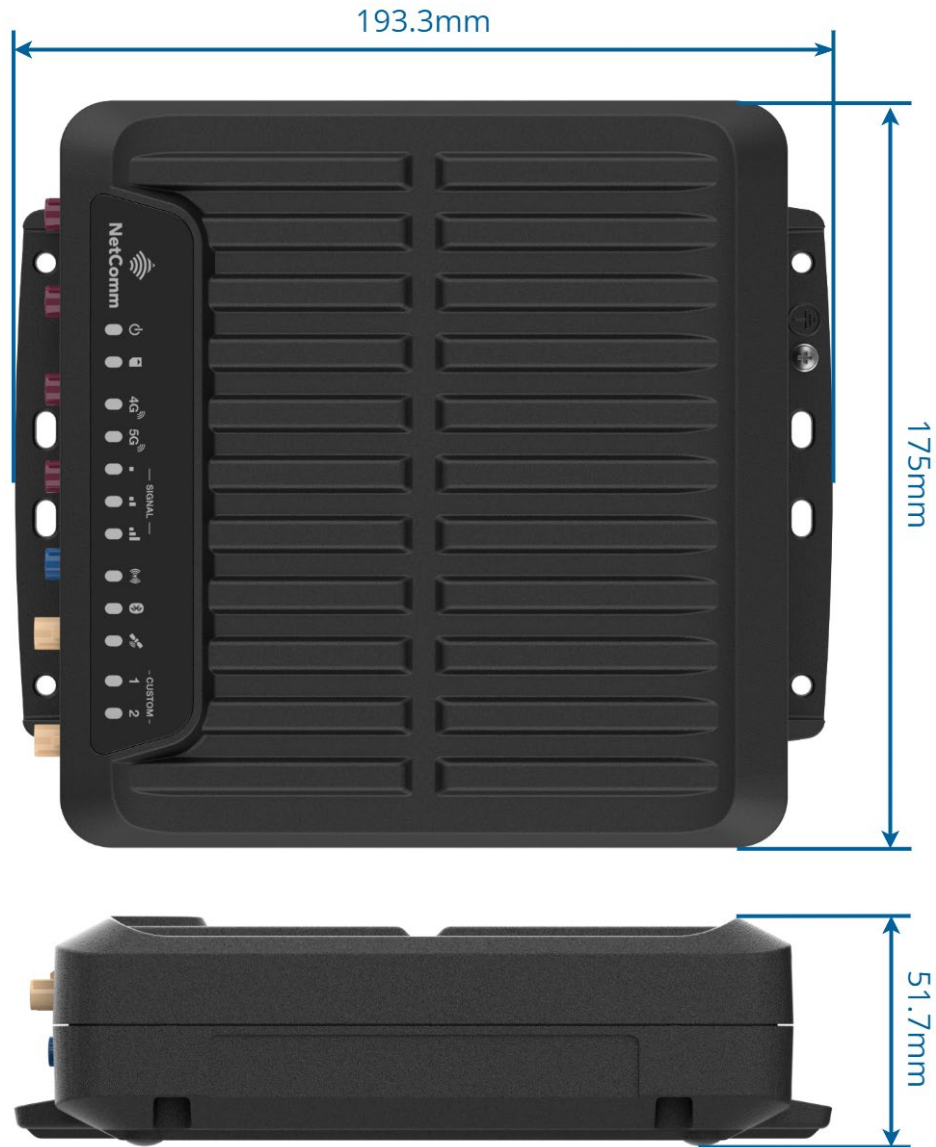


Table 3-1 NTC-550 Series Router Dimensions

NTC-550 Series Router Dimensions	
Length	175 mm
Depth	193.3 mm
Height	51.7 mm
Weight	1.050 kg

Interfaces

The following interfaces are available on the NTC-550 Series router:

Figure 3-2 Interfaces



Table 3-2 Interfaces

No.	ITEM	DESCRIPTION
1	2.5Gbps WAN Ethernet Port	Connect a wired WAN connection here.
2	Gigabit LAN Ethernet ports	Connect local Ethernet compatible devices here.
3	Serial Port	Configurable RS232 DE-9 serial port used to connect serial devices to the router.
4	Factory reset button	Press and hold for less than 5 seconds to reboot to normal mode. The LEDs are green and extinguish in sequence to indicate that the router will reboot normally if the button is released during this period. Press and hold for 5 to 10 seconds to reboot to another partition for recovery purpose. The LEDs are amber and extinguish in sequence to indicate that the router will load the recovery image. Press and hold for 10 to 15 seconds to reset the router to factory default settings. The LEDs are red and extinguish in sequence to indicate that the router will reset to factory default settings if the button is released during this period.
5	Bluetooth pairing button	Press for one second then release to initiate Bluetooth pairing.
6	Six-way terminal block connector	Connect power source wires here. Power wires may be terminated on optional terminal block and connected to DC input jack. Refer to Powering the Router section for further information.
7	Cellular antenna connectors (claret violet)	FAKRA connectors for cellular antennas.
8	GNSS antenna connector (signal blue)	FAKRA connector for GNSS antenna.
9	Wi-Fi antenna connectors (beige)	FAKRA connectors for Wi-Fi antennas.
10	SIM card tray	Insert SIM card (2FF size) here.
11	SIM eject button	Press to eject the SIM card tray.
12	microSD card slot	Insert microSD card here. Remove the cover using a Phillips head screwdriver to access the slot.
13	USB-C port	Provides USB connectivity for debugging. Remove the cover using a Phillips head screwdriver to access the slot.

LED indicators

The NTC-550 Series router uses LEDs to display the current system and connection status.

Figure 3-3 LED Indicators



Table 3-3 LED Indicators

LED	NAME	COLOUR	STATE	DESCRIPTION
	Power		Off	Power off
			Blinking	Router starting up
			On	Power on
	SIM		Off	No SIM detected
			Blinking	SIM error
			On	SIM installed and working
	4G Network		Off	No 4G connection
			Blinking	Connecting to 4G network
			On	4G connected
	5G Network		Off	No 5G connection
			Blinking	Connecting to 5G network
			On	5G connected
SIGNAL	Signal Strength		Off	No signal
			One Lit	Poor signal
			Two Lit	Fair signal
			Three Lit	Good signal
	Wireless		Off	Wireless off

LED	NAME	COLOUR	STATE	DESCRIPTION
			Blinking	Client mode enabled
			On (Amber)	Connected to Wi-Fi network as client device
			On	Wireless Access Point enabled
	Bluetooth		Off	Bluetooth off
			Blinking	Bluetooth pairing mode
			On	Bluetooth on
	GPS		Off	GPS off
			Blinking	Acquiring GPS location
			On	GPS on
CUSTOM	Custom 1	Customizable		Programmable LED for custom use
CUSTOM	Custom 2	Customizable		Programmable LED for custom use

Signal strength LEDs

The following table lists the signal strength range corresponding to the number of lit signal strength LEDs.

Table 3-4 Signal strength LED indicators

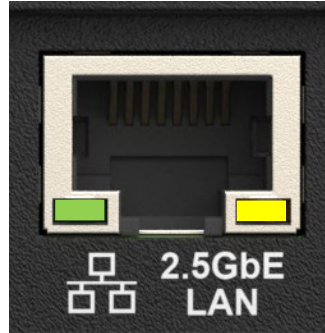
NUMBER OF LIT LEDS	SIGNAL STRENGTH
All LEDs unlit	No signal
1	> -120 dBm
2	> -105 dBm
3	> -90 dBm

LED update interval

The signal strength LEDs update within a few seconds with a rolling average signal strength reading. When selecting a location for the router or connecting and positioning an external antenna, please allow up to 20 seconds for the signal strength LEDs to update before repositioning.

Ethernet port LED indicators

Figure 3-4 NTC-550 Series Ethernet port LED indicators



The table below describes the status of each light and their meanings.

Table 3-5 Ethernet port LED indicators

LED	STATUS	DESCRIPTION
Green	On	Valid network link.
	Blinking	Activity on the network link.
	Off	No valid network detected.
Amber	On	Ethernet port is operating at a speed of 100 Mbps or 1000 Mbps or 2500 Mbps.
	Off	Ethernet port is operating at a speed of 10 Mbps or no ethernet cable is connected

4. Placement of the router

Antenna Installation

The NTC-550 Series router is fitted with multiple FAKRA antenna connectors to connect cellular, Wi-Fi, and GNSS antennas. Attach antennas fitted with FAKRA connectors to the corresponding antenna connectors on your router. Refer to the [Interfaces](#) section for the antenna connector layout.

Figure 4-1 Connecting Antenna



Note: The antennas are not shipped with the device and have to be ordered separately.

If you find the signal strength is weak, try adjusting the orientation of the antennas. If you are unable to get an acceptable signal, try moving the router to a different place or mounting it differently.

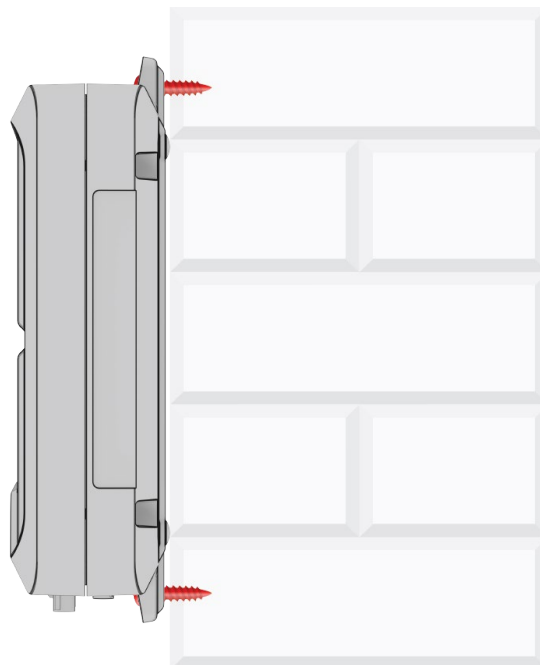
Note: When selecting a location for the router, allow at least 20 seconds for the signal strength LEDs to update before trying a different location.

Mounting Options

You have multiple options to mount the NTC-550 Series router.

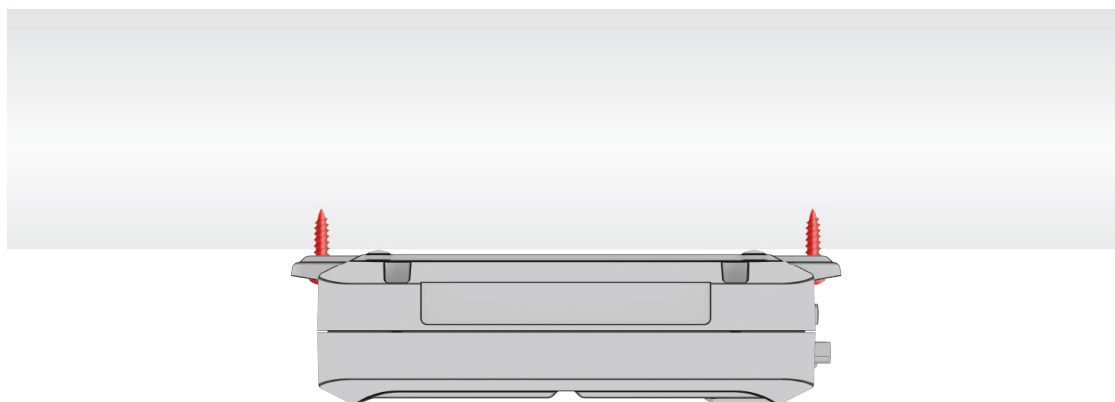
Wall Mount

Figure 4-2 NTC-550 Series Router Wall Mount



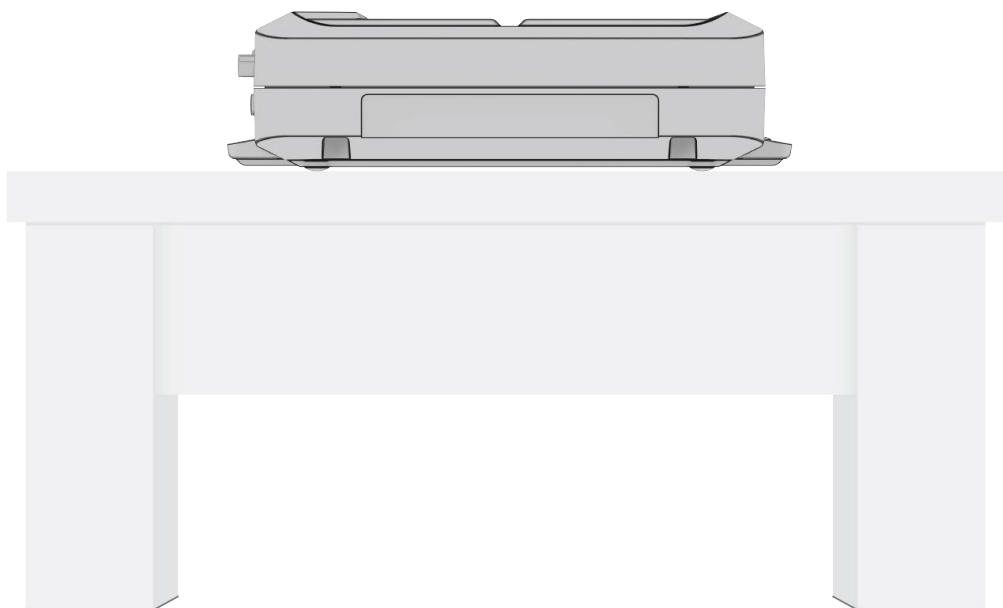
Ceiling Mount

Figure 4-3 NTC-550 Series Router Ceiling Mount



Desk Mount

Figure 4-4 NTC-550 Series Router Desk Mount



Mounting Using DIN Rail Mounting Kit

The DIN rail mounting kit allows you to install the device in two orientations. Install the DIN rail mounting kit by screwing the DIN rail mounts into the locations as shown below.

Figure 4-5 Installing DIN Rail Mounts



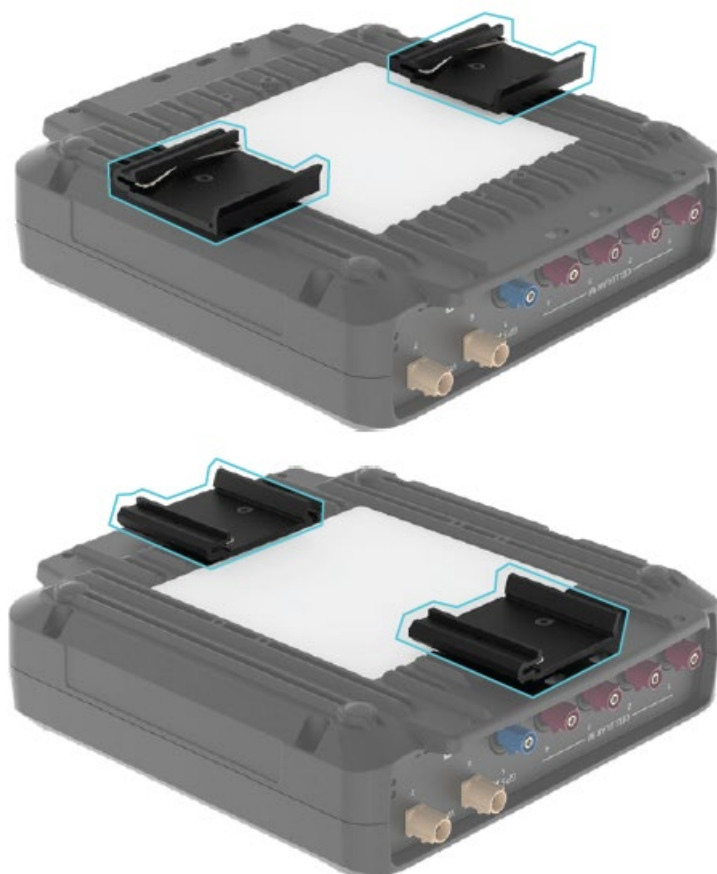
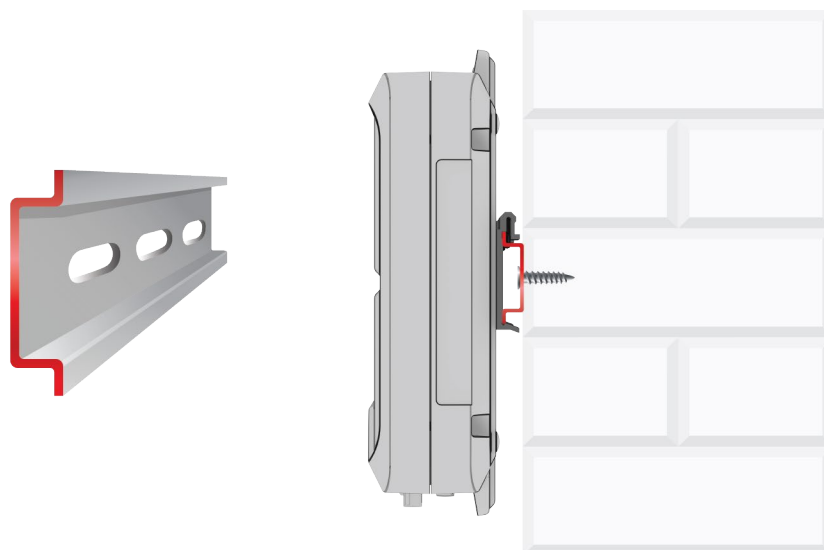


Figure 4-6 Mounting Using DIN Rail Kit



5. Installation and configuration of the NTC-550 Series router

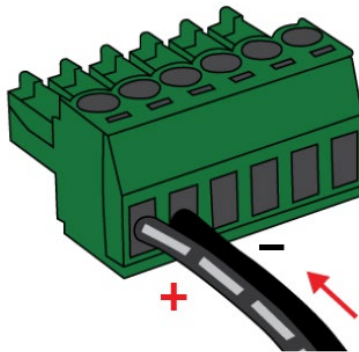
Powering the router

DC power via 6-way connector

The positive and ground terminals on the 6-pin connector can accept power from a separately sold DC power supply. Both a standard temperature range DC power supply and an extended temperature range DC power supply are available to purchase as accessories.

If you have purchased an optional DC power supply, first remove the terminal block from the connector. The terminal block connector uses rising cage clamps to secure the wires and ships with the cages lowered and ready for wire insertion. Inspect the cage clamps and use a flathead screwdriver to lower the cage clamps if they have moved during transportation. Insert the wires into the terminal block as shown below, noting the polarity of the wires, then use a flathead screwdriver to raise the cage clamp to secure the wires in the terminal block. Insert the wired terminal block into the terminal block connector of the router and then connect the adapter to a wall socket.

Figure 5-1 Terminal block wiring diagram



DC power via field terminated power source

If an existing 8-40V DC power supply is available, you can insert the wires into the supplied terminal block to power your router. Use a flathead screwdriver to tighten the terminal block screws and secure the power wires, making sure the polarity of the wires is correctly matched, as illustrated below. You should avoid using DC cables greater than 2 metres in length.

Figure 5-2 Locking Power Terminal block pinout

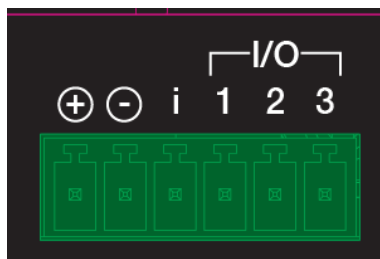


Table 5-1 Locking Power Terminal Block Pinout Description

Terminal	Description
+	Positive wire for power
–	Ground wire
i	Dedicated terminal for ignition detection
I/O	Used for general purpose input/output (refer to IO configuration section for more information)

Installing the router

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

1. Connect equipment that requires network access to the Ethernet port of your router. This may be your computer for advanced configuration purposes, or your end equipment which requires data access via the NTC-550 Series router. You can connect one device directly, or several devices using a network switch.
2. Connect the antennas, if required.
3. If your router does not come with a SIM pre-installed, insert a SIM card into the SIM card slot by pressing the SIM Eject button to eject the SIM card tray. Place the SIM card in the tray and then insert the loaded tray into the SIM slot with the gold side facing up.
4. Ensure the external power source is switched on and wait 2 minutes for your NTC-550 Series router to start up and connect to the mobile network. Your router arrives with preconfigured settings that should suit most customers. Your router is now connected. To check the status of your router, compare the LED indicators on the device with those listed in the LED indicators table.

6. Advanced configuration

To access the web-based user interface, open a web browser (e.g., Mozilla Firefox or Google Chrome), type `https://192.168.1.1` into the address bar and press Enter.

The router's web user interface is displayed.



Important: The HTTP protocol is disabled by default, secure HTTP (HTTPS) is the default protocol. HTTP access is available but must be manually enabled.

Initialization

The first time the device is booted (or booted after a factory reset), the device enters configuration mode. In configuration mode, the router runs a setup wizard which must be completed before the device boots into live mode. This is a security feature which enables you to set strong passwords for the web UI users root, admin, and user, and Telnet/SSH access or restore a previous configuration from a file.

To complete the setup:

1. Click **Next** on the first dialogue box.

Welcome to your new router. The router is now in configuration mode and must be either configured with secure passwords or restored to a previous configuration before it is operational.

Next

2. Enter the factory default password which is printed on the device label, then click **Next**.

To begin using your device, please enter the factory default password. The factory default password is printed on the device label.

Next

3. Select whether to configure the router as a new device or restore a previous configuration backup.

Configure as a new device (create new passwords)

Select **I want to configure this as a new device**, then click **OK**.

In the **NEW PASSWORDS** section, enter a strong password in each field. You may configure the same password for all three accounts, but it must meet the following security requirements:

- The password must be a minimum of eight characters and no more than 128 characters in length.
- The password must contain at least one upper case, one lower case character, and one number.
- The password must contain at least one special character, such as: ` ~ ! @ # \$ % ^ & * () - _ = + [{] \ | ; : ' " , < > / ?

- Additionally, the password must satisfy an algorithm which analyses the characters as you type them, searching for commonly used patterns, passwords, names, and surnames according to US census data, popular English words from Wikipedia, US television, movies, and other common patterns such as dates, repeated characters (aaa), sequences (abcd), keyboard patterns (qwertyuiop), and substitution of numbers for letters.

Figure 6-1 New device configuration dialog page

NEW DEVICE CONFIGURATION

NEW PASSWORDS

Please enter a root, admin, user and SSH password in the respective fields below. For details on password complexity criteria, select the information link next to each field.

New root password

[i](#)

Strong password

Confirm root password

New admin password

[i](#)

☐ Same as the above

Confirm admin password

New user password

[i](#)

☐ Same as the above

Confirm user password

New SSH password

[i](#)

☐ Same as the above

Confirm SSH password

New Wi-Fi password

[i](#)

☐ Same as the above

Confirm Wi-Fi password

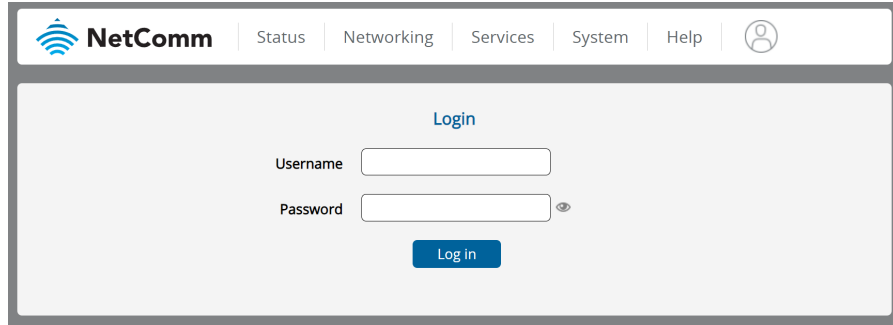
Save

When you have entered values for all password fields, Click **Save** button. If the passwords meet the security requirements, they are saved and the router reboots to Live mode automatically. See below for further instructions on logging in.

Logging In

To login into the router, enter the login username (root, admin or user) and the password that you configured for that user during the initialisation process.

Figure 6-2 Log in prompt for web-based user interface

The image shows a web browser window displaying the NetComm user interface. At the top, there is a navigation bar with the NetComm logo and several menu items: Status, Networking, Services, System, and Help. To the right of the menu is a user profile icon. Below the navigation bar is a large, light gray rectangular area containing the login form. The form has a title 'Login' in blue text. It includes two input fields: 'Username' and 'Password'. The 'Password' field has a small eye icon to its right, indicating a toggle for password visibility. Below the input fields is a blue button labeled 'Log In'.

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



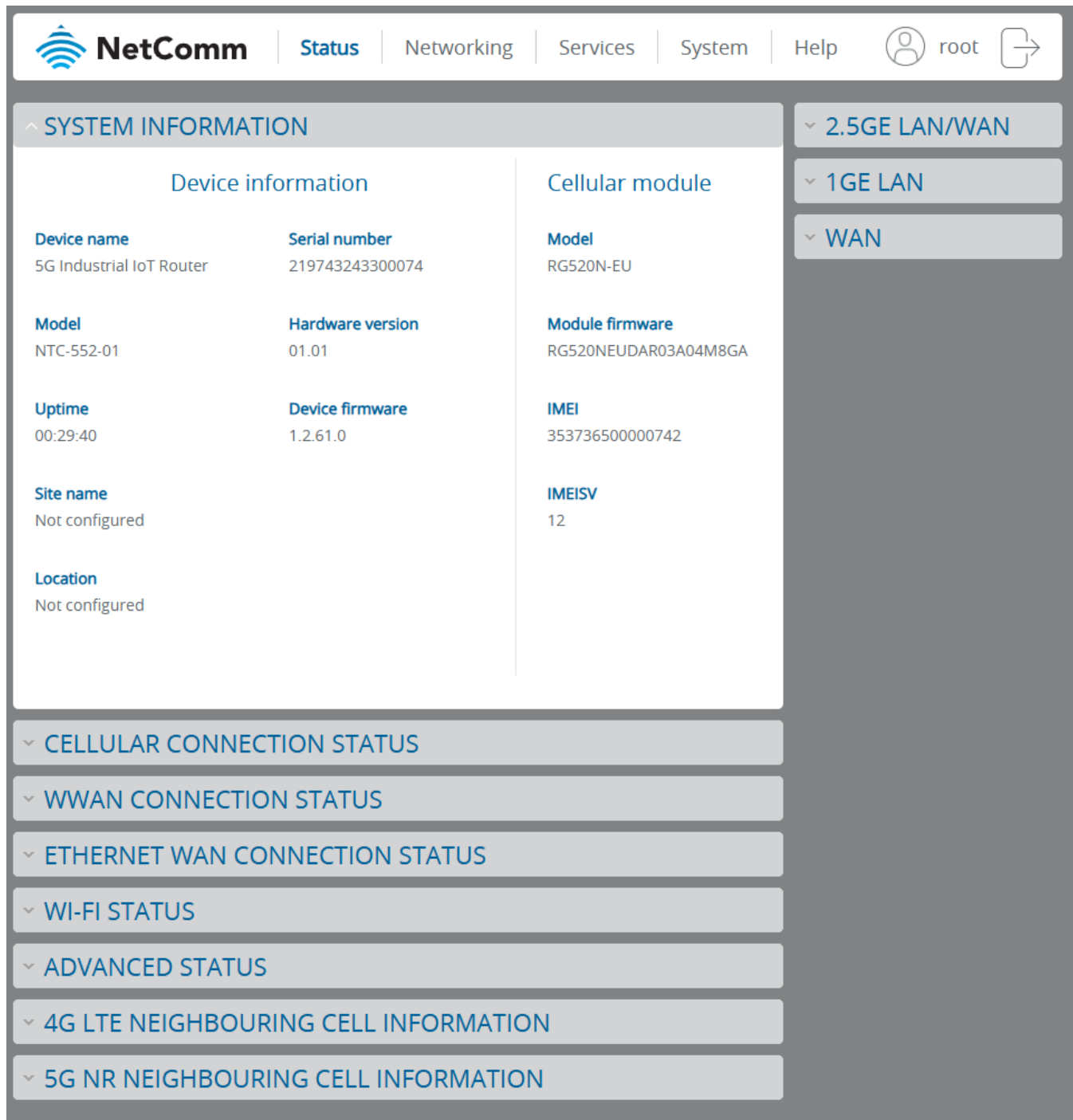
7. Status

The Status page displays once you login into the NTC-550 Series router web interface. The Status page displays the following details:

- System Information
- Cellular Connection Status
- WWAN Connection Status
- Ethernet WAN Connection Status
- Wi-Fi Status
- Advanced Status
- 4G LTE Neighboring Cell Information
- 5G NR Neighboring Cell Information
- 2.5GE LAN/WAN
- 1GE LAN
- WAN

Click  or  buttons in each section tab to show or hide the details in that section. Extra sections will appear as additional software features are enabled.

Figure 7-1 NTC-550 Series router status page



The screenshot displays the NetComm router status page. At the top is a navigation bar with the NetComm logo and tabs for Status, Networking, Services, System, and Help. A user profile icon labeled 'root' and a refresh icon are on the right. The main content area is divided into two columns. The left column contains a 'SYSTEM INFORMATION' section with a table of device and cellular module details. The right column features expandable sections for network interfaces: '2.5GE LAN/WAN', '1GE LAN', and 'WAN'. Below these are several status sections, each with a dropdown arrow: 'CELLULAR CONNECTION STATUS', 'WWAN CONNECTION STATUS', 'ETHERNET WAN CONNECTION STATUS', 'WI-FI STATUS', 'ADVANCED STATUS', '4G LTE NEIGHBOURING CELL INFORMATION', and '5G NR NEIGHBOURING CELL INFORMATION'.

NetComm | **Status** | Networking | Services | System | Help | root

^ SYSTEM INFORMATION

Device information		Cellular module
Device name 5G Industrial IoT Router	Serial number 219743243300074	Model RG520N-EU
Model NTC-552-01	Hardware version 01.01	Module firmware RG520NEUDAR03A04M8GA
Uptime 00:29:40	Device firmware 1.2.61.0	IMEI 353736500000742
Site name Not configured		IMEISV 12
Location Not configured		

2.5GE LAN/WAN

1GE LAN

WAN

CELLULAR CONNECTION STATUS

WWAN CONNECTION STATUS

ETHERNET WAN CONNECTION STATUS

WI-FI STATUS

ADVANCED STATUS

4G LTE NEIGHBOURING CELL INFORMATION

5G NR NEIGHBOURING CELL INFORMATION

System Information

The table below lists the System Information details:

Table 7-1 System Information details

Item	Definition
Device Information	
Device name	The device name of the NTC-550 Series router
Model	The commercial product name which helps to identify the available features of the router.
Uptime	The current up time (the time since the router was last turned on) of the router.
Site name	The configured site name.
Location	The configured location.
Serial number	The serial number of the router.
Hardware version	The hardware version of the router.
Device Firmware	The firmware version of the router
Cellular Module	
Model	The type of cellular module
Module firmware	The firmware revision of the cellular module.
IMEI	The International Mobile Station Equipment Identity number used to uniquely identify a mobile device.
IMEISV	International Mobile Equipment Identity and Software Version. It is a 16-digit code that uniquely identifies a mobile device and its software version.

Cellular Connection Status

The table below lists the Cellular Connection Status details.

Table 7-2 Cellular Connection Status Items

Item	Definition
SIM status	Displays the SIM status of the NTC-550 Series router. This includes information about whether there is a SIM inserted or if the SIM card has an error.
Signal strength	The current signal strength measured in dBm.
Network registration status	The status of the NTC-550 Series router registration for the current network.
Operator selection	The mode used to select an operator network.

Item	Definition
Provider	The current operator network in use.
Roaming status	The roaming status of the NTC-550 Series router.
Enabled bands	The bands to which the NTC-550 Series may connect.
Current band	The current band being used by the NTC-550 Series.
Connection (RAT)	The radio access technology in use.
Coverage	The type of mobile coverage being received by the NTC-550 Series router.
Service options	The network options provided by the current service in use.

WWAN Connection Status

The table below lists the WWAN Connection Status details.

Table 7-3 WWAN Connection Status Items

Item	Definition
Profile	The name of the active profile.
APN	The Access Point name currently in use, If the APN has been manually entered by you. Auto-assigned is displayed if the APN is assigned by the network.
Connection uptime	The duration of the current mobile connection session.
Default profile	Indicates whether the current profile in use is the default profile.
IPv4 status	The IPv4 connection status of the active profile.
IPv4 WWAN	The IPv4 address assigned by the mobile broadband carrier network.
IPv4 DNS server	The primary and secondary IPv4 DNS servers for the WWAN connection.
IPv4 MTU	The current IPv4 Maximum Transmission Unit (MTU) of the WWAN connection.
IPv6 status	The IPv6 connection status of the active profile.
IPv6 WWAN	The IPv6 address assigned by the mobile broadband carrier network.
IPv6 DNS server	The primary and secondary IPv4 DNS servers for the WWAN connection.
IPv6 MTU	The current IPv6 Maximum Transmission Unit of the WWAN connection.

Ethernet WAN Connection Status

The table below lists the Ethernet WAN Connection Status details.

Table 7-4 Ethernet WAN Connection Status Items

Item	Definition
#	Index number of the WAN interface.
Name	The interface name as it is shown on the system.
Status	Displays whether interface is up or down.
IP address	IP address assigned to the ethernet interface.
Gateway	Gateway address for the ethernet interface.

Wi-Fi Status

The table below lists Wi-Fi Status details.

Table 7-5 Wi-Fi Status Items

Item	Definition
Wi-Fi client	
Network name (SSID)	Network name (SSID) of the Wi-Fi access point.
Channel	The frequency band used for the Wi-Fi communication.
State	Status of the Wi-Fi network.
IP	IP address assigned to the Wi-Fi interface by the access point to which it is connected.
5GHz AP	
Network name (SSID)	Network name (SSID) of the router that is broadcasted in the network.
Channel	The frequency band used for the Wi-Fi communication.
State	Status of the Wi-Fi network.
Broadcast SSID	Status the SSID broadcast.
2.4GHz AP	
Network name (SSID)	Network name (SSID) of the router that is broadcasted in the network.
Channel	The frequency band used for the Wi-Fi communication.
State	Status of the Wi-Fi network.
Broadcast SSID	Status the SSID broadcast.

Advanced Status

The table below lists the Advanced Status details.

Table 7-6 Advanced Status Items

Item	Definition
Mobile country code	The Mobile Country Code (MCC) of the NTC-550 Series router.
Mobile network code	The Mobile Network Code (MNC) of the NTC-550 Series router.
SIM ICCID	The Integrated Circuit Card Identifier of the SIM card used with the NTC-550 Series router, a unique number up to 19 digits in length.
IMSI	The International Mobile Subscriber Identity is a unique identifier of the user of a cellular network.
Packet service status	Displays whether the packet service is attached or detached. When APN or username/password is changed, the device detaches and reattaches to the network.
4G LTE	
ECGI	E-UTRAN Cell Global Identifier. The globally unique identity of a cell in E-UTRA. The ECGI concatenates the PLMN-Id and the ECI (E-UTRAN Cell Identifier). The ECI concatenates the eNodeB ID and the Cell ID
eNodeB	Also known as the Evolved Node B, 5G this is the hardware element in the LTE network that communicates directly with mobile devices.
Cell ID	A unique code that identifies the base station from within the location area of the current mobile LTE network signal.
PCI	Physical Cell ID of the LTE Cell.
Channel number (EARFCN)	The channel number of the current cellular connection.
Reference Signal Received Power (RSRP)	Average power received from a single reference signal within a specific bandwidth.
Reference Signal Received Quality (RSRQ)	RSRQ calculates signal quality taking into consideration the RSSI. It is calculated by $N \times \text{RSRP} / \text{RSSI}$ where N is the number of Physical Resources Blocks (PRBs) over which the RSSI is measured.
Signal to Interference plus Noise Ratio (SINR)	The power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.
CQI	Channel Quality Indicator. This is a value between 1 and 15 with 15 being the highest rating.

Item	Definition
5G NR	
NCGI	NR Cell Global Identifier. This concatenates the PLMN-Id (PLMN Identifier) and the 36bit NCI (NR Cell Identity). This information is not available when the device is operating in LTE or 5G non-standalone mode.
gNodeB	The gNodeB (gNB) is the term given to network equipment that transmits and receives wireless communications between UE and a mobile network
gNB Cell ID	A unique code that identifies the base station from within the location area of the current mobile 5G network signal. This is not available when the device is operating in LTE or 5G non-standalone mode.
gNB PCI	Physical Cell ID of the 5G NR Cell.
Channel number (NR ARFCN)	The channel number of the current 5G cellular connection.
SSB Channel number (SSB ARFCN)	The Synchronization Signal Block (SSB) channel number of the current 5G cellular connection.
SCS	The size of the current Subcarrier Spacing (SCS) expressed in KHz.
Reference Signal Received Power (SS-RSRP)	Synchronization Signal Reference Signal Received Power (SS-RSRP). The linear average over the power contributions (in Watts) of the resource elements that carry Secondary Synchronization Signal (SSS).
Reference Signal Received Quality (SS-RSRQ)	Secondary Synchronization Signal Reference Signal Received Quality (SS-RSRQ). It calculates signal quality taking into consideration the RSSI. It is calculated by $N \times \text{SS-RSRP} / \text{NR carrier RSSI}$ where N is the number of Physical Resources Blocks (PRBs) over which the NR RSSI is measured.
Signal to Interference plus Noise Ratio (SS-SINR)	Synchronization Signal – Signal to interference plus noise ratio. The power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.
NR CQI	The 5G NR Channel Quality Indicator (CQI).
Synchronisation Signal Block (SSB) Index	This is a key part of beam management. It is a value comprised of Primary Synchronization Signal (PSS), Secondary Synchronization Signal (SSS) and the Physical Broadcast Channel (PBCH).

4G LTE Neighboring Cell Information

The table below lists the 4G LTE Neighboring Cell Information details.

Table 7-7 4G LTE Neighboring Cell Information Items

Item	Definition
PCI	The Physical Cell ID.
EARFCN	E-UTRA Absolute Radio Frequency Channel Number. Uniquely identifies the LTE Band and carrier frequency.
RSRP	Reference Signal Received Power.
RSRQ	Reference Signal Received Quality.
RAT	The radio signal being served e.g., 5G NR, LTE.

5G NR Neighboring Cell Information

The table below lists the 5G NR Neighboring Cell Information details.

Table 7-8 5G NR Neighboring Cell Information Items

Item	Definition
PCI	The Physical Cell ID.
NR ARFCN	Absolute radio-frequency channel number
SS-RSRP	Synchronization Signal Reference Signal Received Power.
SS-RSRQ	Secondary Synchronization Signal Reference Signal Received Quality.
Type	Serving or neighbor
Role	
SSB ARFCN	The Synchronization Signal Block (SSB) channel number of the current 5G cellular connection.
RAT	The radio signal being served e.g., 5G NR, LTE.

2.5GE LAN/WAN

The table below lists the 2.5GE LAN/WAN details.

Table 7-9 2.5GE LAN/WAN Items

Item	Definition
Interface assignment	Displays the current interface assignment, whether LAN or WAN.
IP	The IP address and subnet mask assigned to the interface.
MAC address	The MAC address of the interface.
Ethernet port status	The status of the port and its current operating speed.

1GE LAN

The table below lists the 1GE LAN details.

Table 7-10 1GE LAN Items

Item	Definition
IP	The IP address and subnet mask assigned to the interface.
MAC address	The MAC address of the interface.
Ethernet port status #1	The status of the port and its current operating speed.
Ethernet port status #2	The status of the port and its current operating speed.
Ethernet port status #3	The status of the port and its current operating speed.
Ethernet port status #4	The status of the port and its current operating speed.

WAN

WAN section displays the priority and status of the available WAN connections.

8. Networking

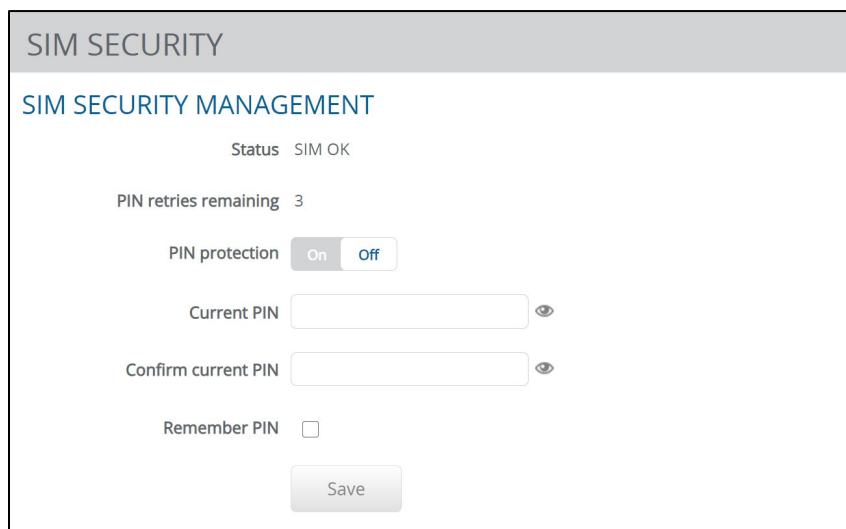
The Networking page provides configuration options for Cellular Settings, LAN Settings, Wi-Fi settings, WAN settings, Routing Settings, and VPN Settings

Cellular settings

SIM security

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

Figure 8-1 SIM security settings

The screenshot shows the 'SIM SECURITY' settings page. At the top, there's a header 'SIM SECURITY' and a sub-header 'SIM SECURITY MANAGEMENT'. Below this, the status is 'SIM OK'. The 'PIN retries remaining' is set to 3. The 'PIN protection' toggle is currently set to 'Off'. There are two input fields: 'Current PIN' and 'Confirm current PIN', both with eye icons for toggling visibility. Below these is a 'Remember PIN' checkbox, which is unchecked. At the bottom, there is a 'Save' button.

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

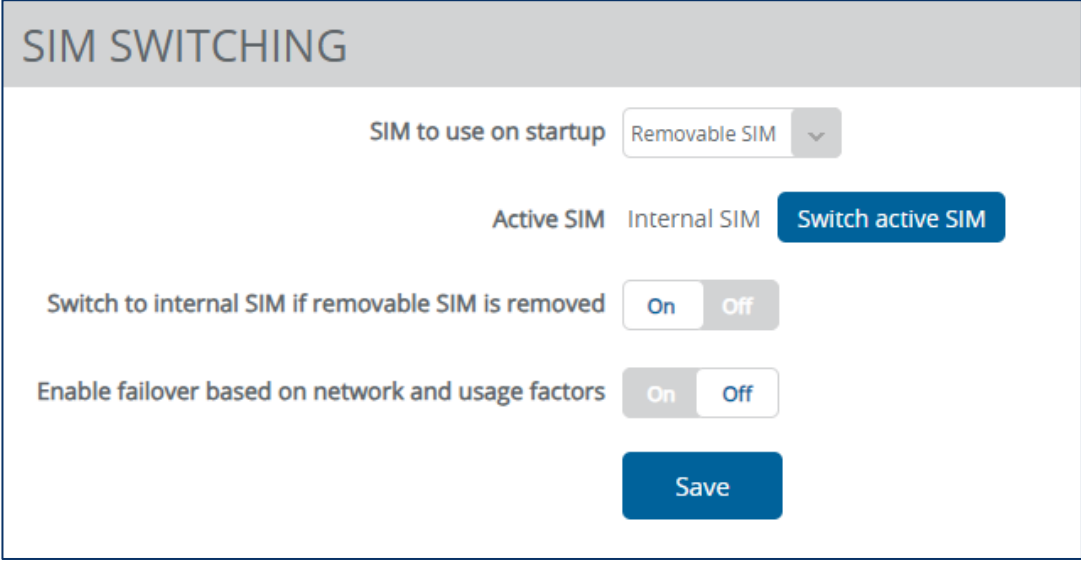
If you are not redirected to the PIN settings page, to unlock the SIM:

1. Click **Networking** tab on the top menu bar, and then click **SIM security**.
2. Enter the PIN in the **Current PIN** field (enter numbers only).
3. Click **Save** to save the PIN and unlock access.
4. Once unlocked, you may toggle the **PIN protection** switch to the **Off** position if you do not wish to have access locked by a PIN.

SIM switching

The NTC-550 Series router is equipped with both a removable and an internal SIM. To configure and switch between the two SIMs, the SIM switching page is used. The SIM switching page also provides several failover options to switch between the SIM cards.

Figure 8-2 SIM management

The image shows a web-based configuration interface titled "SIM SWITCHING". It contains several settings: a dropdown menu for "SIM to use on startup" currently set to "Removable SIM"; a section for "Active SIM" showing "Internal SIM" as the current state and a blue "Switch active SIM" button; a toggle for "Switch to internal SIM if removable SIM is removed" currently set to "On"; a toggle for "Enable failover based on network and usage factors" currently set to "Off"; and a blue "Save" button at the bottom.

SIM SWITCHING

SIM to use on startup Removable SIM ▼

Active SIM Internal SIM **Switch active SIM**

Switch to internal SIM if removable SIM is removed **On** Off

Enable failover based on network and usage factors **On** Off

Save

To select the SIM which should be used on startup, set the **SIM to use on startup** field to either **Internal SIM** or **Removable SIM**.

Active SIM displays the SIM that is currently in use. Click **Switch active SIM** to use the other SIM.

To automatically switch to the internal SIM if the removable SIM card is removed, set the **Switch to internal SIM if removable SIM is removed** toggle to **On**.

To configure **Failover** options, set the **Enable failover based on network and usage factors** to **On**, then set the relevant toggles for each condition that you would like to meet.

Click **Save** to apply any changes to this page.

Network bands

This page allows you to select individual bands from the following band groupings: **LTE, NR5G NSA, NR5G SA**.

Figure 8-3 NTC-550 Series band selection

NETWORK BANDS

4G LTE BANDS On Off

☒ B1	☒ B3	☒ B5	☒ B7	☒ B8
☒ B20	☒ B28	☒ B32	☒ B38	☒ B40
☒ B41	☒ B42	☒ B43		

Select all Unselect all Reset all

5G NR NSA BANDS On Off

☒ n1	☒ n3	☒ n5	☒ n7	☒ n8
☒ n20	☒ n28	☒ n38	☒ n40	☒ n41
☒ n75	☒ n76	☒ n77	☒ n78	

Select all Unselect all Reset all

5G NR SA BANDS On Off

☒ n1	☒ n3	☒ n5	☒ n7	☒ n8
☒ n20	☒ n28	☒ n38	☒ n40	☒ n41
☒ n75	☒ n76	☒ n77	☒ n78	

Select all Unselect all Reset all

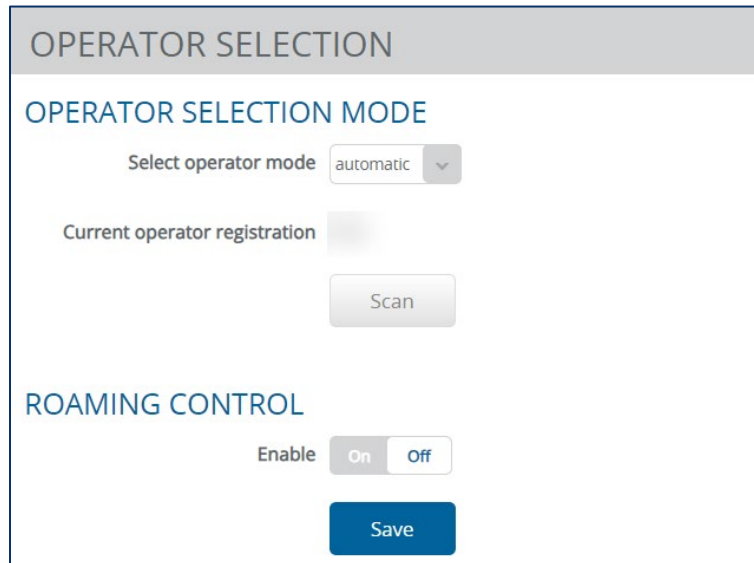
Save

To setup a device for different LTE, 5G non-standalone (NR5G NSA) and 5G Standalone (NR5G SA) modes, refer to [Appendix A – Configuring Radio Access Technologies](#)

Operator selection

The Operator selection page allows you to set how the NTC-550 Series router selects the operator, whether automatically or manually. If you set it to manual, you can override and lock it to a particular carrier or access technology. The operator setting page also contains roaming controls.

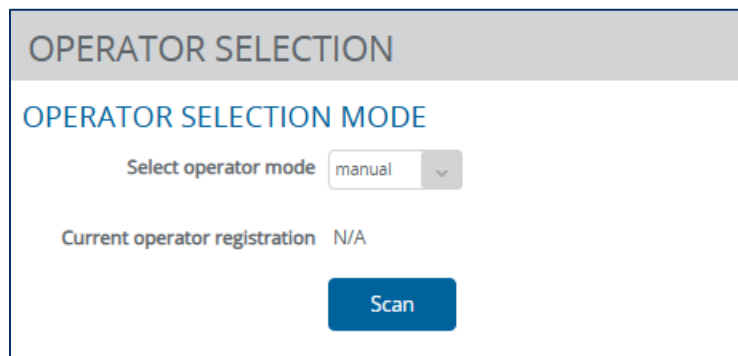
Figure 8-4 Operator setting



The screenshot shows the 'OPERATOR SELECTION' page. Under the 'OPERATOR SELECTION MODE' section, the 'Select operator mode' dropdown is set to 'automatic'. Below it, the 'Current operator registration' field is empty, and a 'Scan' button is visible. In the 'ROAMING CONTROL' section, the 'Enable' toggle is set to 'Off'. A 'Save' button is at the bottom.

Operator selection mode

Figure 8-5 Operator selection mode



The screenshot shows the 'OPERATOR SELECTION' page with 'manual' selected in the 'Select operator mode' dropdown. The 'Current operator registration' field now displays 'N/A'. The 'Scan' button is highlighted in blue.

To scan for available networks, set the **Select operator mode** to manual and click **Scan** button. This operation can take a few minutes and requires that the packet data session be disconnected prior to scanning. A list of the detected service carriers in your area is displayed.

Figure 8-6 Operator list

OPERATOR LIST					
	Operator name	MCC	MNC	Operator status	Network type
☐	Optus	505	02	forbidden	5G NR
☒	Boost	505	01	current	4G LTE
☐	voda AU	505	03	forbidden	4G LTE
☐	Optus	505	02	forbidden	4G LTE

Select the required service from the list and click **Apply**.

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

Roaming control

The roaming control function allows roaming to be enabled or disabled on the NTC-550 Series router. Enable roaming by setting the **Enable** toggle to On, then click **Save**.

Figure 8-7 Roaming control toggle

ROAMING CONTROL

Enable
☒ On
☐ Off

Save

Cell lock list

The Cell lock function allows you to specify a list of cells that the NTC-550 Series router will not deviate from. The cells are separated on the basis of LTE and NR5G networks.

Figure 8-8 Cell lock

CELL LOCK LIST

LTE CELL LOCK LIST

+ Add

PCI	EARFCN
-----	--------

5G NR CELL LOCK LIST

+ Add

gNB PCI	SSB ARFCN	SCS	NR SA band
---------	-----------	-----	------------

Adding to LTE cell lock list

To add a cell to the LTE cell lock list:

1. Click **Add**, next to **LTE Cell Lock List**.
2. Enter the **PCI** and **EARFCN** values of the cell that you want to lock.

Figure 8-9 Cell lock – Adding cell to LTE cell lock list

The screenshot shows a dialog box titled "CELL LOCK LIST" with a sub-header "LTE CELL LOCK SETTINGS". It contains two input fields: "PCI" and "EARFCN". Below these fields are two buttons: "Save" and "Cancel".

3. Click **Save** button. Repeat steps 1 to 3 for all the LTE cells that you wish to add.

Adding to NR cell lock list

To add a cell to NR cell lock list:

1. Click **Add**, next to **NR5G Cell Lock List**.
2. Enter the **gNB PCI**, **SSB ARFCN** values, select SCS value, and enter **NR SA band** value for the NR5G cell that you want to lock to.

Figure 8-10 Cell lock – Add NR5G cell lock

The screenshot shows a dialog box titled "CELL LOCK LIST" with a sub-header "NR5G CELL LOCK SETTINGS". It contains four input fields: "gNB PCI", "SSB ARFCN", "SCS" (with a dropdown menu showing "15 KHz"), and "NR SA band". Below these fields are two buttons: "Save" and "Cancel".

3. Click **Save** button. Repeat steps 1 to 3 for all the NR5G cells that you wish to add.

WAN profiles

The WAN profiles page allows you to configure and enable or disable connection profiles.

Each profile refers to a set of configuration items which are used by the router to activate a Packet Data Protocol (PDP) context. Under normal scenarios, you may have a single profile enabled. Multiple profiles can be used for simple fast switching of PDP settings such as APN or advanced networking configuration where multiple simultaneous PDP contexts may be required.

Figure 8-11 WAN profiles

WAN PROFILES						
Profile no.	Profile name	Status	APN	IP passthrough	Map to LAN/VLAN	Default route
1		☐ On ☒ Off	blank	☐ On ☒ Off	bridge0 v	☒ edit
2		☐ On ☒ Off	blank	☐ On ☒ Off	None v	☐ edit
3		☐ On ☒ Off	blank	☐ On ☒ Off	None v	☐ edit
4		☐ On ☒ Off	blank	☐ On ☒ Off	None v	☐ edit
5		☐ On ☒ Off	blank	☐ On ☒ Off	None v	☐ edit
6		☐ On ☒ Off	blank	☐ On ☒ Off	None v	☐ edit
Save						

Table 8-1 WAN profile item details

ITEM	DEFINITION
Profile no.	Number of the profile.
Profile name	Name of the profile.
Status	Toggles the corresponding profile on or off. Only one profile may be turned on at any time.
APN	The APN configured for the corresponding profile.
IP passthrough	Allows a downstream device, such as a router, to manage the connection. The downstream device connects to the Internet and receives a WAN IP address so that all Internet traffic is passed to the downstream device. Internet traffic is still terminated at the gateway (NTC-550 Series router) and passed through to a downstream device, so the carrier is still able to connect to the gateway.
Map to LAN/VLAN	The LAN or VLAN that the profile is assigned to.

ITEM	DEFINITION
Default Route	Sets the profile as the default route for traffic.

Connecting to the mobile broadband network

The NTC-550 Series router supports the configuration of up to six APN profiles. These profiles allow you to configure the settings that the router will use to connect to the 5G/4G network and switch easily between different connection settings.

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

Manually configuring a connection profile

To manually configure a connection profile:

1. Click  button corresponding the profile that you wish to modify.
2. The **Wireless WAN Profile Settings** page is displayed.

Figure 8-12 WWAN profiles – WWAN profile settings

WIRELESS WAN PROFILE SETTINGS

PROFILE SETTINGS

Enable

Name

APN

Username

Password 

Authentication type None

PDP type IPv4v6

MTU size 576-1500

Metric number 0-65535

IP passthrough

Allow admin access

Modem profile 1 modem profile changes require a reboot to take effect

PROFILE ROUTING

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

Network address

Network mask

Table 8-2 WWAN profiles – WWAN profile settings details

Item	Definition
Enable	Toggle the enable button to On or Off , as desired.
Name	The name of the profile for easy identification on the Wireless WAN profile page. This name is only used to identify the profile on the NTC-550 Series.
APN	Enter the APN (Access Point Name) configured for the corresponding profile.
Username	The username used to log on to the corresponding APN (if required).
Password	The password used to log on to the corresponding APN (if required).

Item	Definition
Authentication type	The authentication type required by your provider. This can be set to: None , PAP or CHAP
PDP Type	Select the PDP type (IP protocol) to use for the connection. • IPv4 – Sets a single stack IPv4 connection through which the NTC-550 Series router receives only IPV4 network and DNS addresses. • IPv6 – Sets a single stack IPv6 connection through which the NTC-550 Series router receives only IPV6 network and DNS addresses.  Note: Before selecting this PDP type, check with your carrier to confirm that single stack IPV6 connectivity is supported. • IPv4v6 – Sets a dual stack connection allowing simultaneous IPV4 and IPV6 network connectivity. The NTC-550 Series router receives both IPv4 and IPV6 network and DNS addresses. This is the default PDP type
MTU size	Enter the Maximum Transmission Unit size. This may be from 1 to 1500 bytes.
IP passthrough	Allows a downstream device, such as a router, to manage the connection. The downstream device connects to the Internet and receives a WAN IP address so that all Internet traffic is passed to the downstream device. Internet traffic is still terminated at the gateway (NTC-550 Series) and passed through to a downstream device, so the carrier is still able to connect to the gateway.
Allow Admin Access	Set to on, if you want to allow remote SSH, TR-069, and WebGUI access to the device via this Wireless WAN profile.  Note: SSH/HTTP/HTTPS can be individually restricted in the Access Control menu. Note also that this will automatically be enabled if the profile is selected in the TR-069 settings menu.
Modem profile	Assigns the WWAN profile to a specific modem profile, which may be required by your carrier.
Profile Routing (See the Profile Routing section below)	
Network address	Enter network address of the remote network.
Network mask	Enter the network mask of the remote network.

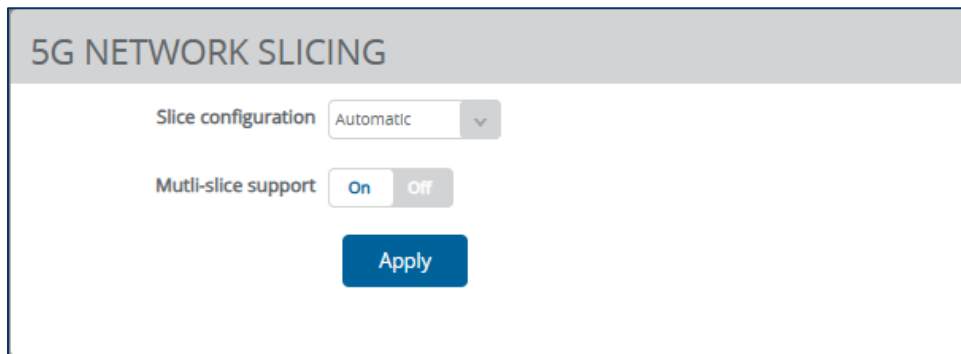
Profile routing

For advanced networking such as using dual simultaneous PDP contexts, you can configure a particular profile to route only certain traffic via that profile by with a custom address and mask of traffic to send via that profile. To do this, in the **Profile Routing** section, enter the **Network address** and **Network mask** of the remote network. If you do not want to use this feature, or are unsure, please leave these fields blank. This will not designate any particular traffic to be routed via this profile.

5G Network Slicing

The 5G Network Slicing page allows to perform network slice configuration.

Figure 8-13 Network slice configuration



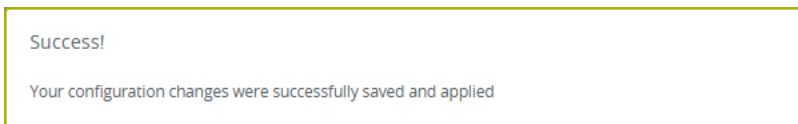
You can perform automatic or manual network slice configuration.

Automatic Network Slice Configuration

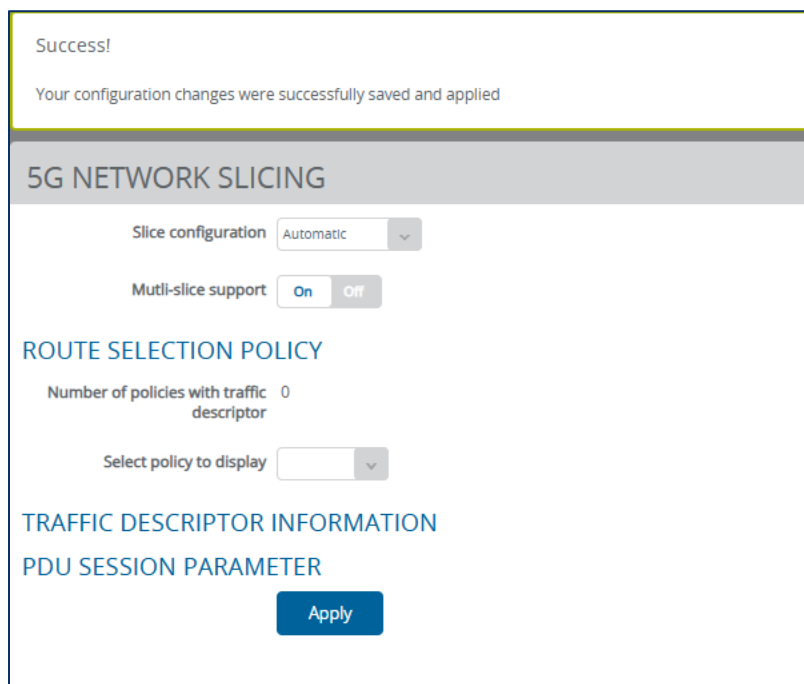
To perform automatic network slice configuration:

1. Select option Automatic for **Slice configuration** in the 5G Network Slicing page.
2. Set Multi-slice support to On or Off.
3. Click **Apply**

In the case **Multi-slice support** is set to **Off**, the below success message displays.



In the case **Multi-slice support** is set to **On**, the below success message and settings display.



Manual Network Slice configuration

To perform manual network slice configuration:

1. Select option Manual for **Slice configuration** in the 5G Network Slicing page. The below page displays.

Figure 8-14 Manual Network Slicing

The screenshot shows the '5G NETWORK SLICING' interface. At the top, 'Slice configuration' is set to 'Manual'. Below this is the 'URSP CONFIGURATION' section, which includes a table with headers: 'Rule DNN', 'Rule priority', and 'No. of route selection descriptors'. There are 'Clear' and 'Apply' buttons at the bottom of the table. A '+ Add' button is located to the right of the table header.

2. Click **Add** for **URSP Configuration**, then click **Add** for **Route Selection Descriptor**. The below settings display.

Figure 8-15 Manual Network Slicing Configuration

The screenshot shows the '5G NETWORK SLICING' interface with the 'TRAFFIC DESCRIPTOR' section. It includes input fields for 'Rule DNN' and 'Rule priority' (with a range of 1-255). Below this is the 'ROUTE SELECTION DESCRIPTOR' section, which includes input fields for 'S-NSSAI SST' (with a range of 0-255), 'S-NSSAI SD' (optional), 'SSC mode' (set to URSP_SSC_MODE_1), 'PDU session type' (set to PDU_IPV4), and 'RSD priority' (with a range of 0-255). There are 'Save' and 'Cancel' buttons at the bottom.

The table below lists the manual network slicing configuration details.

Table 8-3 Manual Network Slicing Configuration Items

Item	Definition
Traffic Descriptor	
Rule DNN	Enter the Data Network Name. It identifies the external data network (e.g., "internet" or an enterprise APN) that a PDU session should connect to.

Item	Definition
Rule priority	Enter a number from 1 to 255. It Determines the order in which URSP rules are evaluated (lower number = higher priority)
Route Selection Descriptor	
S-NSSAI SST	Enter the required value. Single-Network Slice Selection Assistance Information SST (Slice/Service Type) indicates the category or type of service the slice is intended to provide.
S-NSSAI SD	Enter the required value. Single-Network Slice Selection Assistance Information SD (Slice Differentiator) complements the mandatory SST (Slice/Service Type) to further differentiate between multiple network slices that share the same SST value.
SSC mode	Select a mode. Options are: • URSP_SSC_MODE_1: The network preserves the UE's connectivity and retains the same IP address throughout the session. • URSP_SSC_MODE_2: The network may release the PDU session and re-establish a new session, possibly assigning a new IP address. • URSP_SSC_MODE_3: The network allows the PDU Session Anchor (PSA) to be relocated while the session remains active, which can result in the IP address being changed.
PDU session type	Select an option. It specifies the kind of data connectivity established between a user device (UE) and the data network (DN) for a given PDU (Packet Data Unit) session. Options are: • PDU_IPV4 • PDU_IPV6 • PDU_IPV4V6
RSD priority	Enter a number from 0 to 255. It refers to the order in which Route Selection Descriptors (RSDs) are evaluated within a UE Route Selection Policy (URSP) rule.

3. Click **Save** to save the settings. The above configuration is added to Route Selection Descriptor.

Figure 8-16 Manual Network Slicing – Route Selection Descriptor

Success!
Your configuration changes were successfully saved and applied

5G NETWORK SLICING

TRAFFIC DESCRIPTOR

Rule DNN

Rule priority (1-255)

ROUTE SELECTION DESCRIPTOR

[+ Add](#)

S-NSSAI	SSC mode	PDU session type	RSD priority		
EMBBFFFFF	URSP_SSC_MODE_1	PDU_IPV4	1		

[Save](#) [Cancel](#)

- Click to edit the Route Selection Descriptor, click to delete it.
- Click **Save** to save the configuration. The configuration displays in the URSP Configuration.

Figure 8-17 Manual Network Slicing – URSP Configuration

5G NETWORK SLICING

Slice configuration

URSP CONFIGURATION

[+ Add](#)

Rule DNN	Rule priority	No. of route selection descriptors		
MyDNN	1	1		

[Clear](#) [Apply](#)

- Click to edit that URSP configuration, click to delete it.

Service assurance

The service assurance page allows you to run a number of tests to confirm connectivity on different WWAN profiles.

Figure 8-18 Service assurance

SERVICE ASSURANCE

Here you can perform a network connectivity status check. Select the WWAN profile below to check.

WWAN profile(s)

Enter the addresses and parameters in the fields below to perform the test. Fields left empty will result in the respective tests being skipped.

Domain name for DNS test

Destination for ping test

URL for web test

Request method in web test

Start

RESULT

Status

Progress stage

Error

To run a service assurance test:

1. In the **WWAN profiles** field select the WWAN profile you wish to test.
2. In the **Domain name for DNS test** field enter a Domain name to check the DNS connectivity.
3. In the **Destination for ping test** field enter an IPv4 IP address to test the ping.
4. In the **URL for web test** field enter a full URL to test a web page download.
5. In the **Request method in web test** dropdown, select either GET or PUT as the request method.
6. Press the **Start** button to run the test.

In the **Results** section, a successful test will show a **Passed** whilst a failed test will show **Failed** and which of the tests did not pass.

LAN Settings

LAN

The **LAN Configuration** page allows you to configure the LAN settings of the NTC-550 Series router. To access the LAN configuration page, go to **Networking > LAN settings > LAN**

The default IP of the LAN port is 192.168.1.1 with subnet mask 255.255.255.0. To change the IP address, Subnet mask or Hostname enter the appropriate value into the respective field and select the **Save** button.

Note: If you change the IP address, remember to refresh the Ethernet interface of your device, or set an appropriate IP address range, then enter the new IP address into your browser address bar to access the NTC-550 Series router.



Figure 8-19 LAN configuration

The screenshot shows the 'LAN CONFIGURATION' page. It has a title bar 'LAN' and a subtitle 'LAN CONFIGURATION'. Below the subtitle are four configuration fields: 'IP address' with a numeric keypad showing 192, 168, 1, 1; 'Subnet mask' with a numeric keypad showing 255, 255, 255, 0; 'Hostname' with a text input field containing 'my.router'; and 'DNS masquerading' with a toggle switch currently set to 'Off'. At the bottom is a 'Save' button.

DNS masquerading

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

The DNS masquerading toggle key is OFF by default.

With DNS masquerading OFF, the DHCP server hands out the upstream cellular DNS server IP addresses to downstream clients directly, so that downstream clients can send DNS requests directly to the upstream DNS servers without being proxied by the NTC-550 Series router.

With DNS masquerading ON, the DHCP server embedded in the NTC-550 Series router hands out its own IP address (e.g., 192.168.1.1) as the DNS server address to LAN clients. The downstream clients then send DNS requests to the NTC-550 Series router, which proxies them to the upstream DNS servers.

You may also override the DNS Masquerading option by specifying custom DNS Server IP addresses in the DNS server configuration, detailed in [DNS server section](#). In this case the DHCP server assigns downstream devices the manually configured addresses and the DNS Masquerading option is ignored.

The DNS masquerading toggle key is OFF by default.

DHCP

The **DHCP configuration** page is used to configure the DHCP settings of the NTC-550 Series router. You can manually set the IP address range, the lease time of the assigned address, the default domain name suffix, primary and secondary DNS server, the primary and secondary WINS server, as well as the advanced DHCP settings such as NTP, TFTP and Option 150/Option 160 (VoIP options).

Figure 8-20 DHCP configuration

DHCP

DHCP CONFIGURATION

DHCP

On

Off

DHCP start range

192

168

1

100

DHCP end range

192

168

1

199

DHCP lease time (seconds)

86400

(120~86400)

Default domain name suffix

DNS server 1 IP address

DNS server 2 IP address

WINS server 1 IP address

WINS server 2 IP address

NTP server (option 42)

TFTP server (option 66)

DHCP option 150

DHCP option 160

Save

DYNAMIC DHCP CLIENT LIST

Computer name	MAC address	IP address	Expiry time

ADDRESS RESERVATION LIST

+ Add

Computer name	MAC address	IP address	Enable

Table 8-4 DHCP configuration items

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

Enter required values for DHCP items and click **Save** button.

Dynamic DHCP client list

The **Dynamic DHCP Client List** displays a list of the DHCP clients that have been allocated IP addresses. If you want to reserve the current IP address for a particular device, click **Clone**  button corresponding to the device details. The device details are added to the Address Reservation List.

Figure 8-21 Dynamic DHCP client list

DYNAMIC DHCP CLIENT LIST			
Computer name	MAC address	IP address	Expiry time
		192.168.1.124	Tue Feb 13 08:03:47 AEDT 2024 

Address Reservation List

The Address Reservation List displays the list of DHCP clients whose IP address has been reserved and add devices to the list by reserving their IP address.

Figure 8-22 Address reservation list

ADDRESS RESERVATION LIST				+ Add	
Computer name	MAC address	IP address	Enable		
		192.168.1.191	1		

To add a device to the address reservation list:

1. Select the **+Add** button. The Static DHCP page appears.

Figure 8-23 Address reservation list – Add Static DHCP settings

DHCP

STATIC DHCP

Computer name

MAC address

IP address

Enable

On

Off

Save

Cancel

2. In the **Computer name** field enter a name for the device.
3. In the **MAC address** field, enter the device's MAC address.
4. In the **IP address** field, enter the IP address that you wish to reserve for the device.
5. Set the **Enable** toggle to **On** to enable the setting.
6. Select the **Save** button to save the settings.

The device is added to the Address Reservation List.

Click **Edit**  button to edit the details of that device and  button to delete that device from the Address Reservation List.

VLAN

A Virtual Local Area Network (VLAN) is a subnetwork used to group devices located on separate physical networks. This is useful since it allows you to partition your network without the need for additional cabling or wireless access.

Figure 8-24 VLAN

VLAN

Configuring VLAN rules may cause your device to reboot.

Device will reboot when going from zero to one or more enabled VLANs, and the reverse. The reboot will take a few minutes, during which you won't be able to access your device.

VLAN CONFIGURATION

Enable

VLAN RULES

Name	Interface	Address	Subnet mask	DHCP range	DHCP	Allow admin access	Enabled
------	-----------	---------	-------------	------------	------	--------------------	---------

VLAN Settings

To create a VLAN:

1. Click **+Add** button on the VLAN Configuration page. The **VLAN Settings** display.

Figure 8-25 VLAN Settings

VLAN

Configuring VLAN rules may cause your device to reboot.

Device will reboot when going from zero to one or more enabled VLANs, and the reverse. The reboot will take a few minutes, during which you won't be able to access your device.

VLAN SETTINGS

Rule name

Interface

VLAN ID 0~4094 (excl. 253, 254, 255)

IP address

Subnet mask

DHCP ☒ On ☐ Off

DHCP start range

DHCP end range

DHCP lease time (seconds) (120~86400)

Allow admin access ☒ On ☐ Off

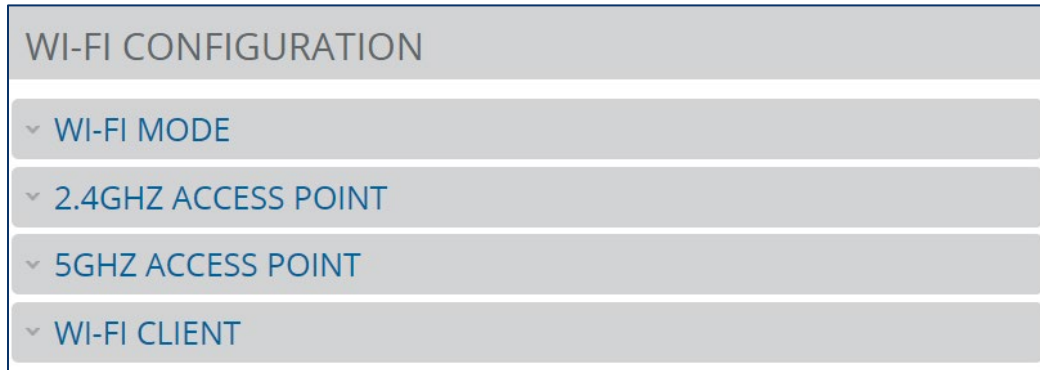
Enable ☒ On ☐ Off

2. In the **Rule name** field, enter a name for the VLAN rule. This is a name that allows you to easily identify the VLAN.
3. In the **VLAN ID** field, enter a number between 0 and 4094 which will be used by the network to identify the VLAN uniquely.
4. In the **IP address** field, enter the IP address for this device on the VLAN.
5. In the **Subnet mask** field, enter the Subnet mask for the device on the VLAN.
6. To use DHCP, set the **DHCP** to On position. Enter values for **DHCP start range** and **DHCP end range** fields. Addresses within this range will be assigned automatically to devices connecting to this VLAN.
7. In the **DHCP lease time (seconds)** field, enter the number of seconds for which the DHCP lease is valid. This value must be 120 or higher.
8. To allow access to the administration web interface, set the **Allow admin access** toggle to **On** position.
9. Set the **Enable** toggle to the **ON** position.
10. Select on the **Save** button to apply the settings.

Wi-Fi Settings

The Wi-Fi configuration allows you to configure settings for Wi-Fi functionality of the NTC-550 Series router. Click each section to display the fields and configure that section.

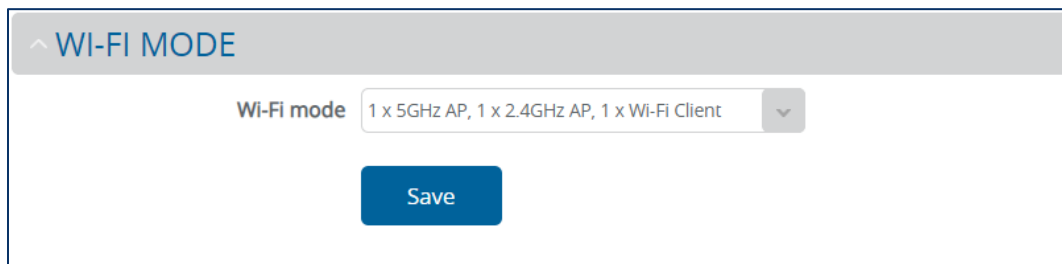
Figure 8-26 Wi-Fi configuration

A screenshot of the 'WI-FI CONFIGURATION' menu. The title 'WI-FI CONFIGURATION' is at the top. Below it are four expandable sections, each with a downward arrow icon: 'WI-FI MODE', '2.4GHZ ACCESS POINT', '5GHZ ACCESS POINT', and 'WI-FI CLIENT'.

Wi-Fi mode

The Wi-Fi mode allows you to configure the Wi-Fi mode that the NTC-550 Series router should operate in. To configure each of the modes once the selection has been made, click the required section in the **Wi-Fi configuration** page

Figure 8-27 Wi-Fi configuration – Wi-Fi mode

A screenshot of the 'WI-FI MODE' configuration screen. The title 'WI-FI MODE' is at the top with an upward arrow icon. Below the title, the text 'Wi-Fi mode' is followed by a dropdown menu showing '1 x 5GHz AP, 1 x 2.4GHz AP, 1 x Wi-Fi Client'. At the bottom center is a blue 'Save' button.

Two modes are available:

1 x 5GHz AP, 1 x 2.4GHz AP, 1 x Wi-Fi Client

In this mode, the NTC-550 Series router will broadcast one 5GHz Wi-Fi network, one 2.4GHz network and will be able to connect to another Wi-Fi network to act as a WAN connection for the gateway.

2 x 5GHz AP, 1 x 2.4GHz AP

In this mode, the NTC-550 Series router will broadcast two 5GHz Wi-Fi networks and one 2.4GHz Wi-Fi network.

Access Point configuration

Both the 2.4 GHz and 5GHz access points provide the same configuration settings for their relevant band.

Figure 8-28 Wi-Fi configuration – 2.4GHz access point

2.4GHZ ACCESS POINT

WIRELESS SETUP (2.4GHZ)

AP radio ☒ On ☐ Off

Country

Network mode

Frequency (channel) Current channel: **11**

Channel width selection

SSID AND SECURITY SETTINGS (2.4GHZ)

SSID

Activate this SSID ☒ On ☐ Off

Broadcast SSID ☒ On ☐ Off

Wireless client isolation ☒ On ☐ Off

Network authentication

WPA pre-shared key

WPA group rekey interval seconds

WPA encryption

Wireless Setup

To configure the Wireless Setup of the access point:

1. Set the **AP radio** toggle to **On** to enable the access point.
2. Set the **Country** field to the country where the NTC-550 Series router is located.
3. Set the **Network mode** to the Wi-Fi version which should be broadcast. The default is 802.11b/g/n/ax mixed mode, which covers most modern devices.
4. Set the **Frequency (channel)** to the appropriate channel. The default is **Auto**, for which the router will analyze the surrounding networks and choose the most appropriate channel.
5. Set the **Channel Width** to the most appropriate width. Lower channel widths will generally provide better stability in an environment with many other interfering Wi-Fi networks or with high levels of frequency interference.
6. Select the **Save** button at the bottom of the page to apply any changes.

SSID and security settings

To configure the SSID and security settings of the Wi-Fi access point:

1. Set the **SSID** (Wi-Fi name) of the network as required.
2. Set the **Activate SSID** toggle to **On** to enable the SSID. If the toggle is set to off, clients will be unable to connect to the access point.
3. Set the **Broadcast SSID** toggle to **On** to broadcast the SSID and allow it to be seen by clients. If the toggle is set to **Off** the SSID will not appear in the list of networks for clients to connect.
4. Set the **Wireless client isolation** toggle to **On** to only allow Wi-Fi clients to access the internet via the Wi-Fi network. They will not be able to access other devices on the network. Set the toggle to **Off** to allow clients to find and connect to network resources connected to the NTC-550 Series router.
5. Set the **Network authentication** field to the required level of security for the Wi-Fi network. Options are **Open**, **WPA2-PSK**, and **WPA3-SAE**. If you select **Open** any Wi-Fi device will be able to access the network, which may compromise the security of the router and any other connected devices.
6. Enter a value for **WPA shared key** field. This key should be used by Wi-Fi clients to connect to the network.
7. Enter a value for **WPA group rekey interval**. It is the number of seconds between WPA key rotations. The default is 600 seconds.
8. Set the **WPA encryption** type field to either **AES** or **None**. Selecting none may reduce the security of the network key.
9. Select the **Save** button to apply the changes.

Wi-Fi client

The Wi-Fi client section allows you to configure the NTC-550 Series router to connect an existing Wi-Fi network, allowing you to rebroadcast an internet connection via the NTC-550 Series router.

Figure 8-29 Wi-Fi configuration – Wi-Fi Client

^ WI-FI CLIENT

WIRELESS CLIENT CONFIGURATION

Client radio

OnOff

Status

State:Radio off

Auto roaming

OnOff

Short scan interval

30

seconds

Signal strength threshold

-45

(dBm)

Long scan interval

300

seconds

Metric

15

0-65535

SSID to connect to

REMOTE_AP_NAME

Scan

AP BSSID

Network authentication

WPA2-PSK

WPA pre-shared key

.....

WPA encryption

AES

Save

Table 8-5 Wireless Client Configuration Items

Item	Definition
Client radio	Set to On to enable.
Status	Displays the current channel and connection status of the wireless client.
Auto roaming	Set to On to enable. Auto roaming allows the router to scan for other access points with the same SSID at regular intervals to determine whether the signal strength is below the Signal strength threshold and switch to an access point with a stronger signal if it is below the threshold at the time of the scan.
Short Scan Interval	Enter the time in seconds. The interval at which the router will scan all access points with the same SSID when the signal strength is below the Signal strength threshold.
Signal strength threshold	Enter the value. The signal strength value in dBm that determines whether the router should use the Short scan interval or the Long scan interval
Long scan interval	Enter the time in seconds. The interval at which the router will scan all access points with the same SSID when the signal strength is above the Signal strength threshold.
Metric	Enter the metric value is used by the router to prioritise routes.
SSID to connect to	Enter the SSID of the network you wish to connect to. Click Scan to discover nearby networks.
AP BSSID	Enter the BSSID or MAC address of the access point to which you are connecting.
Network authentication	Select type of authentication in use on the network from the available options.
WPA pre-shared key	Enter the pre-shared key required to join the wireless network.
WPA encryption	Select the type of encryption in use on the network.

Click **Save** to save the settings.

Figure 8-30 Wi-Fi configuration – Wi-Fi Client - Connected

Status Channel: 4 State: Connected

WAN Settings

The WAN Settings section allows you to configure the WAN port on the NTC-550 Series router.

Interface assignment

The Interface assignment page allows you to configure the functionality of the WAN port or the virtual USB port.

Figure 8-31 WAN Settings – Interface assignment

INTERFACE ASSIGNMENT						
ETHERNET INTERFACE ASSIGNMENT						
No.	Description	Name	Link status	MAC	Port	Configuration
1	Ethernet	eth0	Down	ec:21:e5:10:4f:ea	platform	LAN v
2	USB	ecm0	Down	d0:db:b7:ba:8c:83	virtual	LAN v

Save

Use the dropdown under the **Configuration** column to set the function of the port. Set the field to **LAN** for the port to function as a **LAN** port. Set the field to **WAN** for the port to function as a WAN port, which allows you to configure it as an incoming connection. Set the field to **Disable** to disable the port. Select **Save** to apply the change.

WAN configuration

The **WAN configuration** allows you to configure the WAN connection.

Figure 8-32 WAN Settings – WAN configuration

The screenshot displays the 'WAN CONFIGURATION' window with the 'ETHERNET WAN CONFIGURATION' tab selected. The 'WAN connection' dropdown is set to 'eth0'. The 'Connection type' dropdown is set to 'Static'. Below these, there are input fields for 'IP address', 'Subnet mask', 'Gateway', 'DNS server 1 IP address', and 'DNS server 2 IP address', each represented by four individual boxes. All these fields currently contain the value '0'. At the bottom of the configuration area is a blue 'Save' button.

To configure the WAN connection:

1. Set the **WAN connection** field as the ethernet interface you want to use for WAN connection.
2. Set the **Connection type** field to match the requirements of the WAN connection, either **DHCP** or **Static**.
3. If using **Static**, enter required values for the following fields:
 - **IP address**
 - **Subnet mask**
 - **Gateway**
 - **DNS server 1 IP address**
 - **DNS server 2 IP address**
4. Select the **Save** button to apply the changes.

Failover

The WAN failover page allows you to configure the priority of failover for WAN connections on the NTC-550 Series router. When multiple connections are active, one can be prioritised over another. The method by which the connection can be monitored can also be configured.

Figure 8-33 WAN Settings – Failover

WAN FAILOVER

WAN INTERFACES

No.	WAN type	Interface	Monitor type	Host	Priority	
1	Ethernet	eth0	Link	N/A	^ v	
2	Cellular	N/A	Link	N/A	^ v	

WAN CONFIGURATIONS

WAN interfaces can be activated and configured on the following pages.

[WAN profiles](#)
[Ethernet WAN](#)
[Wi-Fi client configuration](#)

Save

Use the **Priority** arrows to move each connection to the appropriate position on the **Failover** table. The interface at the top will receive priority over the connections which follow it. When a connection becomes disconnected, the router will try to failover to the next connection.

Click  button to manage the connection monitoring method.

Figure 8-34 WAN Settings – Failover – Failover configuration

FAILOVER CONFIGURATION

Monitoring method

Verbose logging ☒ On ☐ Off

First destination address

Second destination address

Periodic Ping timer (3-65535) secs

Retry timer (2-65535) secs

CONSECUTIVE ERROR MONITOR

Consecutive error monitor ☒ On ☐ Off

Failover fail count (3-65535) times

Failback success count (3-65535) times

PERIODIC RATIO MONITOR

Periodic ratio monitor ☒ On ☐ Off

Monitor total count (3-65535) times

Failover fail count (3-65535) times

Failback success count (3-65535) times

Monitoring Methods

The following methods are available:

- Physical link:** If the monitoring method is set to Physical link, the failover mechanism is controlled by the physical detection of the link. When the physical link to eth.0 is broken (i.e. the cable is disconnected, or some other hardware fault causes the physical connection to fail), the router fails over to the WAN interface with the next highest priority.
- Ping:** If the monitoring method is set to Ping, controlled ping packets can be used to determine the status of the link. These are small packets of data that the router sends to a remote address and if the connection is up, a reply is received. They are sent indefinitely at regular intervals that you specify. At each interval, a set of 3 pings are sent to the first destination address and 3 pings are sent to the second destination address configured for each WAN interface to test the availability of the interface.

Methods of evaluating ping responses

The following methods are available:

- **Consecutive Error Monitor** - using this method, the router will determine the availability of an interface based on a set number of consecutive ping instance responses.
- **Periodic Ratio Monitor** - using this method, the router will determine the availability of an interface based on a set ratio of ping instance successes or failures to the number of attempts.

It should be noted that the Periodic ratio monitor evaluates an interface over a Series of ping instances (defined by the Total monitor count) and when the Series has completed, the success and fail counts are reset. For example, with the default Total monitor count value set to 10 and Failover fail count set to 5, the router sends 10 ping instances and if 4 of those instances fail and the first instance of the next Series of 10 fails, the router will not fail over because the 5 failed instances occurred across a different Series.

To simplify configuration, we recommend using only one of the monitor types at any point in time.

Table 8-6 Ping Monitoring Configuration Items

Item	Definition
Failover Configuration	
Monitoring method	Select Ping .
Verbose logging	When enabled, this logs verbose comments in the system log related to the failover monitoring.
First destination address	Enter the first address that the router should ping in order to confirm the connection is up. This may be an IP address or a domain name.
Second destination address	Enter the second address that the router should ping in order to confirm the connection is up. This may be an IP address or a domain name.
Periodic Ping timer	The time in seconds between ping attempts.
Retry timer	The time in seconds between attempts when a ping failure occurs.
Consecutive Error Monitor	
Consecutive error monitor	Set to On to enable.
Failover fail count	The number of failed pings that must occur before the monitor fails the connection over to the next interface.
Failback success count	The number of successful pings that must occur before the monitor fails the connection back to the higher priority interface.
Periodic Ratio Monitor	
Periodic ratio monitor	Set to On to enable.
Monitor total count	This field specifies a Series of pings to consider when calculating whether to fail over or fail back. When the Series is completed, the router repeats the ping test and resets the Failover fail count/Failback success count, therefore, in order for

Item	Definition
	the failover or failback ratio to be met, the number of Failover fail counts/Failback success counts must occur within a particular Series.
Failover fail count	This field specifies the number of failed ping results that must occur within a Series of pings configured in the Monitor total count before the router fails over to the next highest priority interface. For example, at the default setting of 5, the router fails over to the next interface when 5 out of 10 ping attempts in a particular Series have failed. The failures need not be consecutive to meet the failover criteria. If any 5 of the 10 pings in a Series have failed, the router deems the interface connection to be down and fails over.
Failback success count	Like the Failover fail count field, this field specifies the number of ping successes that must be registered on a higher priority interface within a Series of pings configured in the Monitor total count before the router fails back to that interface.

To configure Failover for Ping monitoring method:

1. In the **First destination address** field, enter a website address or IP address to which the router should send the first round of ping requests.
2. In the **Second destination address** field, enter a website address or IP address to which the router should send the second round of ping requests.
3. In the **Periodic Ping timer** field, enter an integer between 3 and 65535 for the number of seconds the router should wait between ping attempts.
4. In the **Retry timer** field, enter an integer between 2 and 65535 for the number of seconds the router should wait between retry ping attempts, i.e. pings to the second destination address.
5. Configure Consecutive Error Monitor.
 - a. Set the **Consecutive error monitor** toggle to **On** position.
 - b. In the **Failover fail count** field, enter an integer between 3 and 65535 for the number of times a retry ping should fail before the router fails over to the next WAN interface.
 - c. In the **Failback success count** field, enter an integer between 3 and 65535 for the number of times a periodic ping should succeed before the router fails back to the higher priority interface.
 - d. Click **Save** to Save the settings.
6. Configure Periodic ratio Monitor.
 - a. Set the **Periodic ratio monitor** toggle to **On**,
 - b. In the **Monitor total count** field, enter an integer between 3 and 65535 for the number of previous ping instances to consider for failover and failback.
 - c. In the **Failover fail count** field, enter the number of pings out of the total count that must fail before the router fails over to the next highest priority WAN interface.
 - d. In the **Failback success count** field, enter the number of pings out of the total count that must succeed before the router fails back to the higher priority WAN interface.
 - e. Click **Save** to save the settings.

To simplify configuration, we recommend using only one of the monitor types at any point in time i.e. either the **Consecutive error monitor** or the **Periodic ratio monitor**.

Routing settings

Static routes

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

To access the Static routing page, select on the **Networking** menu at the top of the screen, select on the **Routing** menu on the left, then select on the **Static** menu item.

Figure 8-35 Static routing

STATIC ROUTES

STATIC ROUTING LIST

+ Add

Route name	Destination	Netmask	Gateway	Interface	Metric
------------	-------------	---------	---------	-----------	--------

ACTIVE ROUTING LIST

Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Interface
0.0.0.0	10.141.177.204	0.0.0.0	UG	25	0	0	rmnet_data0
10.3.8.2	0.0.0.0	255.255.255.255	UH	10	0	0	rmnet_data0
10.3.56.162	0.0.0.0	255.255.255.255	UH	10	0	0	rmnet_data0
10.141.177.200	0.0.0.0	255.255.255.248	U	0	0	0	rmnet_data0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	bridge0

Adding Static Routes

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

Figure 8-36 Static routing – Route configuration

STATIC ROUTES	
ROUTE CONFIGURATION	
Route name	
Destination IP address	· · ·
Netmask	· · ·
Gateway IP address	· · ·
Network interface	auto v
Metric	0-32766
Save	Cancel

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

Active Routing List

Static routes are displayed in the **Active routing list**.

Figure 8-37 Static routing – Active routing list

ACTIVE ROUTING LIST							
Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Interface
0.0.0.0	10.141.177.204	0.0.0.0	UG	25	0	0	rmnet_data0

Static Routing List

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

Figure 8-38 Static routing – Static routing list

STATIC ROUTING LIST						+ Add	
Route name	Destination	Netmask	Gateway	Interface	Metric		
MyRoute	192.168.1.20	255.255.255.0	192.168.1.101	auto	0		

Firewall

The Firewall on the NTC-550 Series router implements an Intrusion Prevention System (IPS). The IPS works together with system firewalls, but in a different manner, to prevent unauthorised access to your network and potentially malicious attacks. It provides a few more levels of security protection for your system from external threats.

Firewalls are rules-based and allow or exclude broad ranges of traffic that do not meet the criteria. IPS monitors and analyses individual inbound data packets to identify threats. Be aware that an IPS should not be considered a replacement for a well-defined firewall but should be seen as one more defensive weapon in your network security arsenal: firewalls, anti-virus software, etc.

IPS filters are interposed between the firewall and the other NTC-550 Series router functionality. It uses a variety of sophisticated techniques to monitor traffic flows and analyse inbound packets to determine whether they constitute network threats and, if so, deny them access. The IPS firewall allows different levels of protection to be selectively applied, to thwart a specifically identified threat.

IPS Firewall Settings

Figure 8-39 IPS router firewall

FIREWALL

IPS FIREWALL SETTINGS

Enable IPS firewall ☒ On ☐ Off

Logging ☒ On ☐ Off

SYN flood defence ☒ On ☐ Off

Packets/Second (10-10000)

Ping flood defence ☒ On ☐ Off

Packets/Second (10-10000)

UDP flood defence ☒ On ☐ Off

Packets/Second (10-10000)

IPV4 Ping Max Size (bytes) ☒ On ☐ Off

Packets Size (0-65535)

The table below lists the IPS Firewall Settings configuration details

Table 8-7 IPS Firewall Settings Configuration Items

Item	Description
Enable IPS Firewall	Enables or disables IPS Firewall
Logging	Enables or disables logging of network activity.
SYN flood defense	Enables or disables SYN flood defense which restricts the number of SYN requests processed by the router during a given time frame. When enabled enter the number of packets/second. Default value is 10, range (10-10000)
Ping flood defense	Enables or disables Ping flood defense. When enabled enter the number of packets/second accepted. Default value is 10, range (10-10000)
UDP flood defense	Enables or disables UDP flood defense. When enabled enter the number of packets/second allowed from a single source. Default value is 10, range (10-10000)

Item	Description
IPv4 Ping Max Size (bytes)	Enables or disables IPv4 Ping Max Size which allows you set maximum size for an IPv4 packet. When enabled enter the maximum packet size. Default value is 512, range (0-65535)

Click **Save** to save the settings.

DMZ

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

To access the DMZ page, select on the **Networking** menu at the top of the screen, select on the **Routing** menu on the left, then select on the **DMZ** menu item.

Figure 8-40 DMZ configuration

To configure DMZ:

1. Set **Enable** to On.
2. Enter the WWAN profile number with which you want to associate the DMZ configuration.
3. Enter the IP Address of the device to be the DMZ host in the **DMZ IP Address** field.
4. Select the **Save** button to save your settings.

Port forwarding

The Port forwarding list is used to configure the Network Address Translation (NAT) rules currently in effect on the NTC-550 Series router. To access the Port forwarding page, select on the **Networking** menu at the top of the screen, select on the **Firewall** menu on the left.

Figure 8-41 NAT

Name	Profile no.	Protocol	Public port	Local IP address	Local port	Enable

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

Note: Some carriers block inbound connections or require a public IP address to get inbound requests.

Adding a port forwarding rule

To create a new port forwarding rule:

1. Click **+Add** button in the Port Forwarding List page. The Port Forwarding Settings page displays.

Figure 8-42 IPv4 Port Forwarding Settings

PORT FORWARDING

PORT FORWARDING SETTINGS

Rule name: DemoRule

Profile no.: 1 (range 1-6)

Protocol: TCP

Public port: 443 (range 1-65535)

Local IP address: 192.168.1.5

Local port: 10000 (range 1-65535)

Enable: On

Save Cancel

2. In the **Rule name** field, enter a name for the rule so that it can be easily identified.
3. In the **Profile no.** field, enter the of the Wireless WAN Profile that you want to use for the rule.
4. Use the **Protocol** drop-down list to select the type of protocol you want to use for the rule. The protocols selections available are **TCP**, **UDP** and **TCP/UDP**.
5. In the **Public port** field, enter port number to use for the communication between the NTC-550 Series and the mobile network, range (1-65535)
6. In the **Local IP Address** field, enter the IP address of LAN equipment to which traffic should be routed or a wildcard IP address (0.0.0.0) that allows all IP addresses to access the traffic.

7. In the **Local port** field, enter the port number to use for traffic to the local device, range (1-65535).
8. Set the **Enable** toggle to **On** position.
9. Click **Save** to save your settings.

To delete a port forwarding rule, click the  button in the **Port forwarding list** for the rule that you want to delete. To edit an existing rule, select on the  button for that rule.

Filtering

The Filtering feature allows you to restrict devices that are allowed to connect to the NTC-550 Series router bases on their MAC address.

Figure 8-43 Filtering

FILTERING

MAC FILTERING

Enable ☒ On ☐ Off

MAC WHITELIST

[+ Add](#)

Name	MAC address	Enable		
DemoDevice	3e:00:00:00:00:00	1		

MAC / IP / PORT FILTERING

Enable ☒ On ☐ Off

Default rule (inbound/forward) Accepted

MAC / IP / PORT FILTERING RULES IN EFFECT

[+ Add](#)

Index	Protocol	Action	Comment		
0	ALL	Drop	DemoRule		

[Save](#)

To enable MAC filtering, set the **Enable** toggle to **On**, then click **Save**.

MAC whitelist

To add a device to the MAC whitelist:

1. Click **+Add** button in MAC Whitelist. The **MAC whitelist settings** page displays.

Figure 8-44 MAC - MAC filtering whitelist settings

The screenshot shows the 'MAC WHITELIST SETTINGS' page. At the top is a grey header with the word 'FILTERING'. Below it, the title 'MAC WHITELIST SETTINGS' is displayed in blue. The form contains two input fields: 'Name' with the value 'DemoDevice' and 'MAC address' with the value '3e:00:00:00:00:00'. Below these is an 'Enable' toggle switch currently set to 'On'. At the bottom are two buttons: 'Save' (grey) and 'Cancel' (blue).

2. In the **Name** field, enter a name for the device.
1. In the **MAC address** field, enter the MAC address of the device.
2. Set the Enable toggle to **On**.
3. Click **Save** button.
4. The device displays in the **MAC Whitelist** section.

To remove a device, select the  button for that device. To edit the device, including temporarily disabling it, Click the  button.

MAC / IP / Port filtering

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

Figure 8-45 Firewall Filtering

The screenshot shows the 'MAC / IP / PORT FILTERING' settings page. It has a title 'MAC / IP / PORT FILTERING' in blue. Below the title is an 'Enable' toggle switch set to 'On'. Underneath is a 'Default rule (inbound/forward)' dropdown menu currently set to 'Accepted'. Below this is a section titled 'MAC / IP / PORT FILTERING RULES IN EFFECT' with a '+ Add' button. A table lists the current rules in effect:

Index	Protocol	Action	Comment		
0	ALL	Drop	DemoRule		

At the bottom of the page is a 'Save' button.



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

Creating a MAC / IP / Port filtering rule

To create a filtering rule:

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

Figure 8-46 MAC/IP/Port Filter Settings

Table 8-8 MAC/IP/Port Filter Settings Configuration Details

Item	Description
Bound	Select the direction of traffic. The options available are: • Inbound • Outbound • Forward
Protocol	Select the protocol of the traffic. The options available are: • All • UDP/TCP • UDP • TCP

Item	Description
	• ICMP
MAC Address	Enter MAC Address of the source device.
Source IP address	Enter IP address of the source device.
Action	Select the action to be taken. The options available are: • Drop • Accept
Comment	Add comments for the rule

Enter, select the required values for all the fields and click **Save**.

- The new rule is displayed in the filtering rules list. To edit the rule click the  Edit button and to delete the rule click the  button.

Redundancy (VRRP)

Virtual Router Redundancy Protocol (VRRP) is a non-proprietary redundancy protocol designed to increase the availability of the default gateway servicing hosts on the same subnet. This increased reliability is achieved by advertising a “virtual router” (an abstract representation of master and backup routers acting as a group) as a default gateway to the host(s) instead of one physical router. Two or more physical routers are then configured to stand for the virtual router, with only one doing the actual routing at any given time. If the current physical router that is routing the data on behalf of the virtual router fails, an arrangement is made for another physical router to automatically replace it. The physical router that is currently forwarding data on behalf of the virtual router is called the master router. Routers are given a priority of between 1 and 255 and the router with the highest priority is assigned as the master.

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

Figure 8-47 Redundancy

REDUNDANCY (VRRP)

REDUNDANCY (VRRP) CONFIGURATION

Redundancy (VRRP)

On Off

Virtual ID

1

(1-255)

Router priority

1

(1-255)

Virtual IP address

.

.

.

VRRP WAN WATCHDOG

VRRP WAN watchdog

On Off

Save

Configuring VRRP

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

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

Note: Configuring VRRP changes the MAC address of the Ethernet port which may interrupt the connection to the router. If you want to resume with the web configuration you must use the new IP address (VRRP IP) or clear the arp cache (old MAC address). On Windows, run the following command in command prompt:



```
arp -d <ip address> (i.e. arp -d 192.168.1.1)
```

Configuring the VRRP WAN watchdog

The VRRP WAN watchdog is disabled by default. When it is enabled, VRRP monitors the status of the primary and secondary by the physical link. When enabled, the VRRP WAN watchdog feature monitors the status of the connection by both the physical link and controlled ping packets.

Figure 8-48 Redundancy – VRRP WAN Watchdog

VRRP WAN WATCHDOG

VRRP WAN watchdog ☒ On ☐ Off

Verbose logging ☐ On ☒ Off

First destination address

Second destination address

Periodic Ping timer (3-65535) secs

Retry timer (2-65535) secs

CONSECUTIVE ERROR MONITOR

Consecutive error monitor ☒ On ☐ Off

Failover fail count (3-65535) times

Failback success count (3-65535) times

PERIODIC RATIO MONITOR

Periodic ratio monitor ☒ On ☐ Off

Monitor total count (3-65535) times

Failover fail count (3-65535) times

Failback success count (3-65535) times

The following table details each field on the VRRP WAN Watchdog page.

Table 8-9 VRRP WAN Configuration Items

Parameter	Description
VRRP WAN Watchdog	Set to On to enable the watchdog.
Verbose logging	When enabled verbose comments are logged in the system log related to the failover monitoring.
First destination address	The first address the router that the router should ping to confirm the connection is up. This may be an IP address or a domain name.
Second destination address	The second address the router that the router should ping to confirm the connection is up. This may be an IP address or a domain name.
Periodic Ping timer	The time in seconds between ping attempts.
Retry timer	The time in seconds between attempts when a ping failure occurs.
Consecutive error monitor	
Consecutive Error Monitor	Set to On to enable the consecutive error monitor. Using this method, the router will determine the availability of an interface based on a set number of consecutive ping instance responses.
Failover fail count	The number of failed pings that must occur before the monitor fails the connection over to the next interface.
Failback success count	The number of successful pings that must occur before the monitor fails the connection back to the higher priority interface.
Periodic ratio monitor	
Periodic ratio monitor	Set to On to enable the Periodic ratio monitor. Using this method, the router will determine the availability of an interface based on a set ratio of ping instance successes or failures to the number of attempts.
Monitor total count	This field specifies a series of pings to consider when calculating whether to fail over or fail back. When the series is completed, the router repeats the ping test and resets the Failover fail count/Failback success count. Therefore, for the failover or failback ratio to be met, the number of Failover fail counts/Failback success counts must occur within a particular Series.
Failover fail count	This field specifies the number of failed ping results that must occur within a series of pings configured in the Monitor total count before the router fails over to the next highest priority interface. For example, at the default setting of 5, the router fails over to the next interface when 5 out of 10 ping attempts in a particular Series have failed. The failures need not be consecutive to meet the failover criteria. If any 5 of the 10 pings in a Series have failed, the router deems the interface connection to be down and fails over.

Parameter	Description
Failback success count	Like the Failover fail count field, this field specifies the number of ping successes that must be registered on a higher priority interface within a Series of pings configured in the Monitor total count before the router fails back to that interface.

RIP

RIP (Routing Information Protocol) is used for advertising routes to other routers. By enabling RIP all the routes in the router's routing table will be advertised to other nearby routers. For example, the route for the router's Ethernet subnet could be advertised to a router on the PPP interface side so that a router on this network will know how to route to a device on the router's Ethernet subnet. Static routes must be added manually according to your requirements. See Adding Static Routes for more information.

Figure 8-49 RIP configuration



Note: Other routers may ignore RIP.

To enable Routing Information Protocol (RIP)

1. Set the **RIP** toggle to **On** to enable RIP.
2. Using the **Version** drop-down list, select the version of RIP to use.
3. Select the **Interface** that RIP should apply on. Options are **LAN**, **WWAN** or **Both**.
4. If you want to turn on authentication, toggle the **Authentication** toggle key to the **ON** position. Use the Authentication type drop-down list to select the method of authentication then enter password in the Password field.
5. Click **Save** button to save your settings.

VPN

IPSec

IPSec operates on Layer 3 of the OSI model and can protect higher layered protocols. IPSec is used for both Site-to-Site VPN and Remote Access VPN. The NTC-550 Series router supports IPSec end points and can be configured with Site-to-Site VPN tunnels for third party VPN routers.

Figure 8-50 VPN – IPSec

IPSEC					
IPSEC TUNNEL LIST					
+ Add					
#	Name	Remote LAN address/mask	Remote gateway	Local LAN address/mask	Enable

Configuring an IPSec VPN

From the menu at the top of the screen, click **Networking** and under the VPN section, click **IPSec**. A list of configured IPSec VPN connections is displayed. Click the **+Add** button to begin configuring an IPSec VPN connection.

Figure 8-51 VPN – IPsec Profile Edit

IPSEC

IPSEC PROFILE EDIT

IPSec profile

Profile name

PHASE 1 PARAMETERS

Remote IPSec address

Key mode

Pre-shared key

Remote ID (xy.sample.com or blank)

Local ID (xy.sample.com or blank)

IKE version

IKE mode

IKE encryption

IKE hash

DH group

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

DPD action

DPD keep alive time secs

DPD timeout secs

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

PHASE 2 PARAMETERS

Remote LAN address

Remote LAN subnet mask

Local LAN address

Local LAN subnet mask

Encapsulation type

IPSec encryption

IPSec hash

The following table describes each of the fields of the IPsec VPN configuration page.

Table 8-10 IPsec configuration items

Parameter	Description
IPsec profile	Enables or disables the VPN profile.
Profile name	A name used to identify the VPN connection profile.
Phase 1 parameters	
Remote IPsec address	The IP address or domain name of the IPsec server.
Key mode	Select the type of key mode in use for the VPN connection. You can select from: • Pre-Shared Keys • RSA keys • Certificates • SCEP client
Pre-shared key	The pre-shared key is the key that peers use to authenticate each other for Internet Key Exchange. The pre-shared key must meet the requirements for a strong password. See the Configuring a strong password section. This field appears if Pre-shared keys is used as the key mode.
Remote ID	Remote ID of the connection. Refer to the documentation of the remote IPsec server for further details. This field may be left blank.
Local ID	Local ID of the connection. Refer to the documentation of the remote IPsec server for further details. This field may be left blank.
Local RSA key upload	Upload the Local RSA key if RSA Keys is used as the Key mode.
Remote RSA key upload	Upload the Remote RSA key if RSA Keys is used as the Key mode.
Private key passphrase	The Private key passphrase is required if Certificates is used as the Key mode.
Key / Certificate	Select the Key / Certificate type for the IPsec connection if Certificates is used as the Key mode.
IPsec certificate upload	Upload the IPsec certificate if Certificates is used as the Key mode.
SCEP remote id	Enter the SCEP remote ID if SCEP client is used as the Key mode.
IKE version	Set the IKE version for the connection. There are two options available IKE V1 and IKE V2 .
IKE mode	Set the IKE mode for the connection. There are three options Any , Main and Aggressive .
IKE encryption	Select the cipher type to use for the Internet Key Exchange.
IKE hash	Select the IKE Hash type to use for the VPN connection. The hash is used for authentication of packets for the key exchange.

Parameter	Description
DH group	Select the desired Diffie-Hellman group to use. Higher groups are more secure but also require longer to generate a key.
IKE re-key time	Enter the time in seconds between changes of the encryption key. To disable changing the key, set this to 0.
DPD action	Select the required Dead Peer Detection action. This is the action to take when a dead Internet Key Exchange Peer is detected.
DPD keep alive time	Enter the time in seconds for the interval between Dead Peer Detection keep alive messages.
DPD timeout	Enter the time in seconds of no response from a peer before Dead Peer Detection times out.
SA life time	Enter the time in seconds for the security association lifetime.
Phase 2 parameters	
Remote LAN address	Enter the IP address of the remote network for use on the VPN connection.
Remote LAN subnet mask	Enter the subnet mask in use on the remote network.
Local LAN address	Enter the IP address of the local network for use on the VPN connection.
Local LAN subnet mask	Enter the subnet mask in use on the local network.
Encapsulation type	Select the encapsulation protocol to use with the VPN connection. You can choose ESP , AH or Any .
IPSec encryption	Select the IPSec encryption type to use with the VPN connection.
IPSec hash	Select the IPSec hash type to use for the VPN connection. The hash is used for authentication of packets for the VPN connection.

OpenVPN

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

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

Figure 8-52 VPN - OpenVPN

The screenshot shows the OpenVPN configuration page with three main sections:

- OPENVPN SERVER LIST**: Includes a table with columns: Profile Name, VPN Network Address, Authentication type, Username, Status, and Edit. A blue '+ Add' button is to the right.
- OPENVPN CLIENT LIST**: Includes a table with columns: Profile Name, Server IP address, Authentication type, Username, Status, and Edit. A blue '+ Add' button is to the right.
- OPENVPN P2P LIST**: Includes a table with columns: Profile Name, Server IP address, Local IP Address, Remote IP Address, Remote Subnet Mask, Status, and Edit. A blue '+ Add' button is to the right.

Configuring an OpenVPN Server

To add an OpenVPN server, select the **+Add** button to the right of the OpenVPN Server List heading. Each time the **+Add** button is selected, the router checks if there are existing server certificates. If no server certificate is found, you are prompted to generate a certificate before configuring the OpenVPN server.

Figure 8-53 VPN – OpenVPN – Generate server certificate prompt

The dialog box contains the following text:

You must generate a certificate before configuring an OpenVPN server. Select OK to proceed to the OpenVPN server certificate configuration page.

At the bottom are two buttons: **OK** (grey) and **Cancel** (blue).

Select the **OK** button, the Server Certificate page displays. For more information on generating server certificates, refer to the [Server Certificate](#) section of this guide. When you have created the certificate, return to the OpenVPN server configuration page to continue the setup.

To configure an OpenVPN server:

1. Set the **OpenVPN profile** toggle key to **ON** position.
2. In the **Profile name** field, enter a name for the OpenVPN server profile you are creating.
3. In the **Type** field, select the OpenVPN connection type (**TUN/TAP**). Default is **TUN**.
4. In the **Port type** field, select a packet type to use for your OpenVPN Server and in the **Server port** field, enter a port number. The default OpenVPN port is 1194 and default packet type is UDP.
5. In the **Encryption cipher** field, select the encryption type for the connection. The default is **AES-256** as this is the strongest encryption level.
6. Enter a maximum transmission unit value into the **MTU** field. The default is 1500.

7. In the **VPN network address** and **VPN network subnet mask** fields, enter the IP address and network subnet mask to assign to your VPN. This is ideally an internal IP address which differs from your existing address scheme.
8. The Server certificates section displays the details of the certificate. If you wish to change the certificate, click the **Change** button.
9. HMAC or Hash-based Message Authentication Code is a means for calculating a message authentication code using a cryptographic hash function and a cryptographic key. If you wish to use the HMAC signature as an additional key and level of security, under the SSL/TLS handshake section, set the **Use HMAC Signature** toggle key to **On** position, then click the **Generate** button so that the router can randomly generate the key. The **Server key timestamp** field is updated with the time that the key was generated. Click the **Download** button to download the key file so that it can be uploaded on the client.
10. Select an **Authentication type**. Authentication may be done using a Certificate or Username / Password. See the below sections for information on each of the certificate types.

Certificate authentication

In the Authentication Type section select **Authentication type** as **Certificate**. Enter the required details to create a client certificate. All fields are required. After filling out the required fields, click **Generate** button.

Figure 8-54 VPN – OpenVPN – Certificate Authentication type

AUTHENTICATION TYPE

Authentication type

Certificate

Name

Country

State

City

Organisation

Email

Once the certificate is generated, click **Download P12 button** or **Download TGZ button** to save the certificate file, depending on which format you would like. If for some reason the integrity of your network has been

compromised, return to this screen, use the Certificate drop-down list to select the certificate and then select the Revoke button to make the certificate invalid.

Username / Password Authentication

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



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

Figure 8-55 VPN – OpenVPN – Username / Password Authentication type

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

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

Configuring an OpenVPN client

To configure and Open VPN client:

1. In the OpenVPN page click the **+Add** button in the **OpenVPN Client List** section. The OpenVPN Client Edit page displays

Figure 8-56 VPN – OpenVPN – Configure OpenVPN client

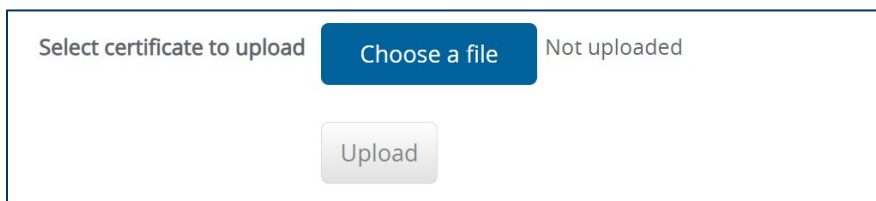
2. Set the **OpenVPN profile** toggle key to the **On** position.
3. In the **Profile name** field, enter a name for the OpenVPN client profile you are creating.
4. In the **VPN network address** field, enter the WAN IP address / host domain name of the OpenVPN server.
5. Select **Type (TUN/TAP)**. Default is **TUN**.
6. In the **Server port** field enter a port number and for **Encryption cipher** select a packet type to use for the OpenVPN server. The default OpenVPN port is 1194 and default packet type is UDP.
7. Enter a maximum transmission unit value in the **MTU** field
8. If the **Default gateway** option is applied on the OpenVPN client page, the OpenVPN server will enable connections to be made to other client networks connected to it. If it is not selected, the OpenVPN connection allows for secure communication links between this router and the remote OpenVPN server only.
9. Select the **Authentication type** to use for the OpenVPN client. The available options are **Certificate**, **Username and Password**, or **Combination Certificate and Username / Password**. See the below sections to understand the different authentication types.

Certificate Authentication

To use Certificate Authentication:

1. Set the **Authentication Type** field to **Certificate**.
2. Scroll down to the **Select certificate to upload** field and click **Choose a file** button.

Figure 8-57 OpenVPN – Certificate upload



Select certificate to upload **Choose a file** Not uploaded

Upload

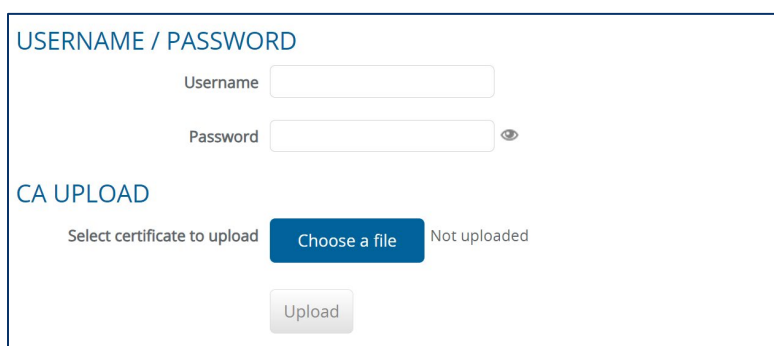
3. Locate the certificate on your computer, click **Open**, then click **Upload**.
4. Once the certificate is uploaded, click the **Save** button to confirm the connection.

Username / Password Authentication

To use Username / Password Authentication:

1. Set the **Authentication Type** field to **Username / Password**.

Figure 8-58 OpenVPN – Username / Password Authentication



USERNAME / PASSWORD

Username

Password 

CA UPLOAD

Select certificate to upload **Choose a file** Not uploaded

Upload

2. In the **Username** field, enter the username of the OpenVPN server.
3. In the **Password** field, enter the password of the OpenVPN server.
4. Click **Choose a file** button to locate the CA certificate file you saved from the OpenVPN Server and then click the **Upload** button.
5. If you have an additional SSL/TLS key created on the server, set the **Use HMAC Signature** toggle key to **ON** position. Click **Choose a file** button then locate the key file on your computer. Click the **Upload** button to upload it to the router.
6. Click **Save** button to confirm the connection.

Certificate and Username / Password authentication

The Certificate and Username / Password Authentication option is a combination of both the Certificate and Username / Password authentication methods. This provides additional levels of security since the client must know the username / password combination and be in possession of the certificate. Set the **Authentication type** to **Certificate and Username / Password Authentication**, then follow the instructions in both the above sections to complete the configuration.

Configuring an OpenVPN P2P Connection

The OpenVPN P2P connection allows you to create a Peer-to-peer VPN connection with another router. One router should be the primary router, and the other router should be a secondary router.

1. In the OpenVPN page click the **+Add** button in the OpenVPN P2P List section . The OpenVPN Peer Edit page displays.

Figure 8-59 OpenVPN – P2P Peer Edit Page

The screenshot shows the 'OPENVPN PEER EDIT' configuration page. It includes a toggle for 'OpenVPN profile' (set to 'On'), a 'Profile name' text field, a 'Server IP address' text field with a note 'leave empty if peer-to-peer server', a 'Port type' dropdown (set to 'TCP'), a 'Server port' text field (set to '1194') with a range '1-65535', an 'Encryption cipher' dropdown (set to 'AES-256'), an 'MTU' text field (set to '1500') with a range '(576-1600)', 'Local IP address' and 'Remote IP address' four-part text boxes, a 'REMOTE NETWORK' section with 'Remote Network LAN address' and 'Remote Network LAN mask' four-part text boxes, a 'SERVER SECRET KEY' section with an 'Update time' label and 'Generate' and 'Download' buttons, a 'CLIENT SECRET KEY' section with an 'Update time' label and a 'Delete' button, a 'Client secret key upload' section with a 'Choose a file' button and 'Not uploaded' text, and 'Save' and 'Cancel' buttons at the bottom.

2. Set the **OpenVPN profile** toggle key to **ON** position.
3. In the **Profile** name field, enter a name for the OpenVPN P2P profile you are creating.
4. In the router designated as the server, leave the **Server IP address** field empty. In the router designated as the client, enter the WAN IP address/host domain name of the server.
5. In **Port type** and **Server port** fields enter port number and select a packet type to use for the OpenVPN server. The default OpenVPN port is 1194 and default packet type is UDP.
6. In the **Local IP Address** and **Remote IP Address** fields, enter the respective local and remote IP addresses to use for the OpenVPN tunnel. The secondary router should have the reverse settings of the primary router.

7. In the **Remote network** section, in the **Local IP Address** and **Remote IP Address** fields, enter the respective local and remote IP addresses to use for the OpenVPN tunnel. The secondary router should have the reverse settings of the primary router.
8. Click **Generate** button to create a secret key to be shared with the other router. When the timestamp displays, you can click the **Download** button to save the file to exchange with the other router.
9. When you have saved the secret key file on each router, click the **Choose a file** button to locate the secret key file for the master and then click the **Upload** button to send it to the secondary router. Perform the same for the other router, uploading the secondary secret key file to the primary router.
10. Click **Save** button to confirm the Peer-to-peer VPN connection.

GRE Tunnelling

The Generic Route Encapsulation (GRE) protocol creates a point-to-point connection similar to a VPN between clients and servers or between clients only. GRE is used to encapsulate the data or payload.

Figure 8-60 VPN – GRE Tunnelling

GRE TUNNELLING				
GRE CLIENT LIST				
+ Add				
Name	GRE server address	Local tunnel address	Remote tunnel address	Status
DemoClient	10.10.10.100	10.20.30.40	20.30.30.1	disabled  

To configure GRE tunnelling:

1. In the GRE client list section, click the **+Add** button. The **GRE Client Edit** screen displays.

Figure 8-61 VPN – GRE Tunnelling – GRE Client Edit

GRE TUNNELLING

GRE CLIENT EDIT

Enable VPN ☒ On ☐ Off

Profile name

GRE server address

Local tunnel address

Remote tunnel address

Remote network address

Remote network subnetmask

TTL 255 (0-255)

Reconnect delay 30 (30-65535) seconds

Reconnect retries 0 (0-65535, 0=Unlimited)

2. Set the **Enable VPN** toggle to **On**.
3. In the **Profile name** field, enter a profile name for the tunnel. This name is used to identify the tunnel on the router.
4. In the **GRE server address** field, enter the IP address or domain name of the GRE server.
5. In the **Local tunnel address** field, enter the IP address you want to assign the tunnel locally.
6. In the **Remote tunnel address** field, enter the IP address you want to assign to the remote tunnel.
7. In the **Remote network address** field, enter the IP address scheme of the remote network.
8. In the **Remote network subnetmask** field, enter the subnet mask of the remote network.
9. The **TTL** (Time To Live) field is an 8-bit field used to remove an undeliverable data packet from a network to avoid unnecessary network traffic across the internet. The default value of 255 is the upper limit on the time that an IP datagram can exist. The value is reduced by at least one for each hop the data packet takes to the next router on route the datagram's destination. If the TTL field reaches zero before the datagram arrives at its destination the data packet is discarded and an error message is sent back to the sender.
10. The **Reconnect delay** is the time in seconds that the router will wait before attempting to connect to the GRE server if the connection is broken. The minimum time to wait is 30 seconds so as to not flood the GRE server with connection requests, while the maximum time to wait is 65335 seconds.
11. The **Reconnect retries** is the number of connection attempts that the router will make if the GRE connection goes down. If set to 0, the router will retry the connection indefinitely, otherwise the maximum number of times to retry cannot be greater than 65335.
12. Click the **Save** button to save the changes. The VPN will attempt to connect after your click Save. Select the Status button at the top left of the interface to return to the status window and monitor the VPN's connection state.

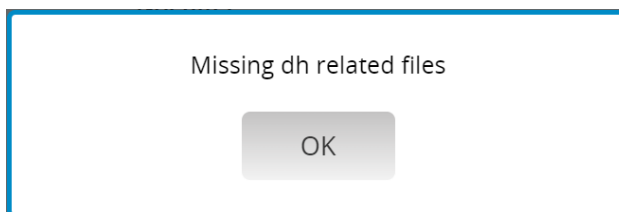
Server Certificate

The Server Certificate page is used to generate a certificate for use with OpenVPN.

Generating Diffie-Helman files

On first use of the certificate page, you will see the following prompt, where **dh** refers to **Diffie-Hellman**.

Figure 8-62 VPN – Server Certificate – Missing dh related files



To proceed with generating the certificate, the Diffie-Hellman parameters must first be generated. Click **OK** on the prompt to close it. The OpenVPN Server Certificate page is shown.

Figure 8-63 VPN – Server Certificate – Missing dh related files

Click **Generate** for the **Diffie-Hellman parameters** field. The following prompt displays.

Figure 8-64 VPN – Server Certificate – Generate Diffie-Hellman prompt

Selecting the **OK** button will delete and invalidate all previous server and client keys, if they exist, and generates new parameters. This process will take up to five minutes to complete. Once the files are generated, the Success prompt is shown.

Figure 8-65 VPN – Server Certificate – Missing dh related files

The Server Certificate can now be generated.

Generating the OpenVPN Server Certificate

To generate an OpenVPN Server Certificate:

1. In the **Country** field, enter the SSL Country code for the country the certificate is issued for.
2. In the **State** field, enter the state the certificate is issued for.

3. In the **City** field, enter the city the certificate is issued for.
4. In the **Organization** field, enter the name of the organization for the certificate.
5. In the **Email** field, enter a contact email for the certificate.
6. For the **Generate Server Certificate** field click **Generate** to generate the certificate. A success prompt is shown, and the certificate serial number and validity dates are shown in **Certificate serial number, Not before** and **Not after** fields.

Figure 8-66 VPN – Server Certificate – Generate certificate

OPENVPN

OPENVPN SERVER CERTIFICATE

Server key size 2048

Diffie-Hellman parameters

Generate

Certificate serial number 72A7D54CE506F92C80D96F3311F34FA1

Not before Feb 15 01:01:23 2024 GMT

Not after Feb 12 01:01:23 2034 GMT

Country AU

State NSW

City Sydney

Organization NetComm Wireless

Email example@casa-systems.com

Generate server certificate

Generate

9. Services

Network time (NTP)

The NTP Network (NTP) page allows you to configure the NTC-550 Series router to synchronize its internal clock with a global Internet Time server and specify the time zone for the location of the router. This provides an accurate timekeeping function for features such as System Log entries and Firewall settings where the current system time is displayed and recorded. Any Network Time Protocol (NTP) server available publicly on the internet may be used.

To access the Network time (NTP) page, click the **Services** tab at the top of the screen then click **Network time (NTP)** tab on the left.

Figure 9-1 NTP

The screenshot shows the NTP configuration page. At the top, the title 'NTP' is displayed. Below it, the 'TIMEZONE SETTINGS' section includes a 'Current time' field showing 'Fri Feb 16 09:59:44 AEDT 2024' and a 'Timezone' dropdown menu set to '(GMT+10:00) Australia/Sydney'. A 'Daylight savings time schedule' button is located below the dropdown. The 'NTP SETTINGS' section features an 'NTP' toggle switch set to 'On', an 'NTP service' text field containing '0.netcomm.pool.ntp.org', a 'Synchronisation on WWAN connection' toggle switch set to 'On', and a 'Daily synchronisation' toggle switch set to 'On'. A 'Save' button is at the bottom of the settings section.

Timezone Settings

The **Current time** field shows the time and date configured on the router. If this is not accurate, use the Timezone drop-down list to select the correct time zone for the router.

If the selected zone observes daylight savings time, a **Daylight savings time schedule** button displays below the drop-down list. Click **Daylight savings time schedule**, a window displays the start and end times for daylight savings. Click **OK** and click **Save** to save the settings.

Configuring NTP settings

To configure NTP settings:

1. Set the **Network time (NTP)** toggle key to switch it to the **On** position.
2. In the **NTP service** field, enter the address of the NTP server you want to use.
3. Set the **Synchronization on WWAN connection** toggle key to **On** or **Off** as required. It enables or disables the router to perform time synchronization, each time a mobile broadband connection is established.
4. Set the **Daily synchronization** toggle key to **On** or **Off** as required. It enables or disables the router to perform time synchronization each day.
5. Click **Save** to save the settings.

SMS messaging

The NTC-550 Series router offers an advanced SMS feature set, including sending messages, receiving messages, redirecting incoming messages to another destination, and supporting remote commands and diagnostics messages.

Some of the functions supported are:

- Ability to send a text message via a cellular network and store it in permanent storage.
- Ability to receive a text message via a cellular network and store it in permanent storage.
- Ability to forward incoming text messages via a cellular network to another remote destination which may be a TCP/UDP server or other mobile devices.
- Ability to receive run-time variables from the device (e.g. uptime) on request via SMS.
- Ability to change live configuration on the device (e.g. network username) via SMS.
- Ability to execute supported commands (e.g. reboot) via SMS.
- Ability to trigger the NTC-550 Series router to download and install a firmware upgrade.
- Ability to trigger the NTC-550 Series router to download and apply a configuration file.

To access the SMS messaging functions of the NTC-550 Series router, click the **Services** tab on the top menu bar, and then click an option under the **SMS messaging** section.

Setup

The **SMS Setup** page allows you to perform SMS and SMS forwarding configurations of the router. SMS messaging is enabled by default.

Figure 9-2 SMS - SMS setup configuration

SMS SETUP

GENERAL SMS CONFIGURATION

Messages per page 10-50

Encoding scheme ▼

SMSC address

SMS FORWARDING CONFIGURATION

Forwarding ☒ On ☐ Off

Redirect to mobile

TCP server address

TCP port

UDP server address

UDP port

Table 9-1 SMS - SMS setup configuration items

Option	Definition
General SMS configuration	
Messages per page	Enter the number of SMS messages to display per page. Must be a value between 10 and 50.
Encoding scheme	Enter the encoding method used for outbound SMS messages. GSM 7-bit mode permits up to 160 characters per message but drops to 50 characters if the message includes special characters. UCS-2 mode allows to send Unicode characters and permits a message to be up to 50 characters in length.
SMS forwarding configuration	
Forwarding	Set to On , to enable forwarding. Incoming text messages can be redirected to another mobile device and/or a TCP/UDP message server.
Redirect to mobile	Enter a mobile number as the destination for forwarded SMS messages. You can forward incoming text messages to a different destination number. This destination number can be another mobile phone or a router phone number. The text message is stored on the router and forwarded to the mobile number at the same time.
TCP server address	Enter an IP address or domain name as the destination for forwarded SMS messages using TCP. You can also forward incoming text messages to a TCP based destination. The TCP server can be any kind of public or private server if the server accepts incoming text-based messages. The TCP address can be an IP address or domain name. The text message is stored on the router and forwarded to the TCP server at the same time.
TCP port	The TCP port on which to connect to the remote destination. The port number range is from 1 to 65535. Please refer to your TCP based SMS server configuration for which port to use.
UDP server address	Enter an IP address or domain name as the destination for forwarded SMS messages using UDP. You can also forward incoming text messages to a UDP based destination. The UDP server can be any kind of public or private server if the server accepts incoming text-based messages. The UDP address can be an IP address or domain name. The text message is stored on the router and forwarded to the UDP server at the same time.
UDP port	The UDP port on which to connect to the remote destination. The port number range is from 1 to 65535. Please refer to your UDP based SMS server configuration for which port to use.

Diagnostics

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

Figure 9-3 SMS – SMS diagnostics configuration

SMS MESSAGING

SMS DIAGNOSTICS AND COMMAND EXECUTION CONFIGURATION

Enable remote diagnostics and command execution ☐ On ☒ Off

Only accept authenticated SMS messages ☐ On ☒ Off

Send Set command acknowledgement replies ☐ On ☒ Off

Access advanced RDB variables ☐ On ☒ Off

Allow execution of advanced commands ☐ On ☒ Off

Send acknowledgement replies to The sender's number

Send command error replies ☐ On ☒ Off

Send error replies to The sender's number

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

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

WHITE LIST FOR DIAGNOSTIC OR EXECUTION SMS

#	Destination number	Password
Save Cancel		

The table below lists the SMS Diagnostics Configuration details.

Table 9-2 SMS – SMS Diagnostics and Command Execution Configuration Items

Item	Description
SMS Diagnostics and Command Execution Configuration	
Enable remote diagnostics and command execution	Enables or disables the remote diagnostics feature. If this setting is enabled all incoming text messages are parsed and tested for remote diagnostics commands. If remote diagnostics commands are found, the router executes those commands. This feature is enabled by default. All remote diagnostic commands that are received are stored in the Inbox.  Note: It is possible to adjust settings and prevent your router from functioning correctly using remote diagnostics. If this occurs, you will need to perform a factory reset to restore normal operation.
Only accept authenticated SMS messages	Enables or disables checking the sender's phone number against the allowed sender white list for incoming diagnostics and command execution SMS messages. If authentication is enabled, the router will check if the sender's number exists in the white list. If it exists, the router then checks the password (if configured) in the incoming message against the password in the white list for the corresponding sending number. If they match, the diagnostic or command is executed. If the number does not exist in the white list or the password does not match, the router does not execute the incoming diagnostic or command in the SMS message. This is enabled by default and it is strongly advised that you leave this feature enabled to maintain security.  Important: We highly recommended that you use the white list and a password when utilising this feature to prevent unauthorised access. See the White list description for more information.
Send Set command acknowledgement replies	The NTC-550 Series router will automatically reply to certain types of commands received, such as get commands, or execute commands. However, acknowledgement replies from the NTC-550 Series router are optional with set commands and the Wakeup command. This option enables or disables sending an acknowledgment message after execution of a set command or SMS Wakeup command. If disabled, the router does not send any acknowledgement after execution of a set command or SMS Wakeup command. All acknowledgment replies are stored in the Outbox after they

Item	Description
	have been sent. This can be useful to determine if a command was received and executed by the router. This option is disabled by default.
Access advanced RDB variables	This option allows access to the full list of RDB variables via SMS. When it is turned off, you are only allowed access to the basic RDB variables listed later in this guide.
Allow execution of advanced commands	This option allows execution of advanced commands such as those which are common to the Linux command line. For example: "execute ls /usr/bin/sms*" to list the contents of the /etc folder on the router. When it is turned off you are only allowed to execute the basic commands listed later in this guide.
Send acknowledgement replies to	Select A fixed number or The sender's number. This option allows you to specify where to send acknowledgment messages after the execution of a set, get, or exec command. If a fixed number is selected, the acknowledgement message will be sent to the number defined in the Fixed number to send replies to field. If the sender's number is selected, the acknowledgement message will be sent to the number that the SMS diagnostic or command message originated from. The default setting is to use the sender's number.
Send command error replies	Allows to enable or disable the option to send replies to error messages.
Send error replies to	Select A fixed number or The senders's number . This is the destination number to which error messages are sent after the execution of a get, set, or exec command whether a fixed number or the sender's number. This field is only displayed when it set to Fixed Number.
Send a maximum number of, replies per	Allows you to set the maximum number of acknowledgement and error messages sent when an SMS diagnostic or command is executed. The maximum limit can be set per hour, day, week or month. The router will send a maximum of 100 replies per day by default.

Click **Save** to save the settings.

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

The Whitelist For Diagnostic Or Execution SMS displays the list of mobile numbers added to white list and their details.

The table below lists the details of the Whitelist For Diagnostic Or Execution SMS

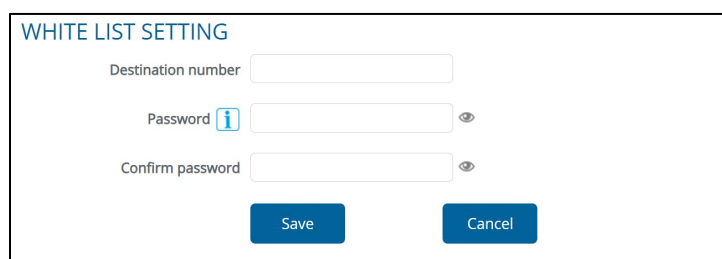
Table 9-3 Whitelist For Diagnostic Or Execution SMS Items

Item	Description
#	Serial number
Destination number	Mobile number added to white list
Password	Password associated with mobile number
	Click to edit the details of the white list number
	Click to delete the number from the white list

To configure a White List for Diagnostic or Execution SMS:

1. Click **+Add** button, the **Whitelist Setting** page displays.

Figure 9-4 SMS - SMS diagnostics configuration – White list settings



2. Enter a number in the **Destination number** field to add it to the White List.
3. In the Password field, enter a password. The password must meet the following requirements:
 - Must contain a minimum of eight characters and no more than 128 characters in length.
 - Must contain at least one upper case character, one lower case character and one number.
 - Must contain least one of the following special characters: !*()?/
4. In the Confirm password field, re-enter the password.
5. Click **Save** to save the settings.

Sending an SMS diagnostic command

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

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

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



You will then need to set a Password in the White list for diagnostic execution SMS list.

5. Select the **Save** button.

Types of SMS diagnostic commands

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

- execute COMMAND
- get VARIABLE
- set VARIABLE=VALUE

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

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

The following are some examples of SMS diagnostic commands:

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

SMS acknowledgement replies

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

SMS command format

Generic Format for reading variables:

```
get VARIABLE
PASSWORD get VARIABLE
```

Generic Format for writing to variables:

```
set VARIABLE=VALUE
PASSWORD set VARIABLE=VALUE
```

Generic Format for executing a command:

```
Execute COMMAND
PASSWORD execute COMMAND
```

Replies

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

Table 9-4 SMS – SMS diagnostics command syntax

Type	SMS Contents	Notes
get command	"VARIABLE=VALUE"	
set command	"Successfully set VARIABLE to VALUE"	Only sent if the acknowledgment message function is enabled
execute command	"Successfully executed command COMMAND"	

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

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

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

Where "COMMAND" is a supported command to be executed by the device (e.g. reboot)

Where "PASSWORD" is the password (if configured) for the corresponding sender number specified in the White List

Multiple commands can be sent in the same message, if separated by a semicolon.

For Example:

```
get VARIABLE1; get VARIABLE2; get VARIABLE3
PASSWORD get VARIABLE1; get VARIABLE2
set VARIABLE=VALUE1 ; set VARIABLE2=VALUE2
PASSWORD set VARIABLE1=VALUE1; set VARIABLE2=VALUE2; set VARIABLE3=VALUE3
```

If required, values can also be bound by an apostrophe, double apostrophe, or back tick.

For Example:

```
"set VARIABLE='VALUE'"
"set VARIABLE=""VALUE""
"set VARIABLE=`VALUE`"
"get VARIABLE"
```

A password (if required), only needs to be specified once per SMS, but can be prefixed to each command if desired.

```
"PASSWORD get Variable1"; "get VARIABLE2"
"PASSWORD set VARIABLE1=VALUE1"; "set VARIABLE2=VALUE2"
```

If the command sent includes the "reboot" command and has already passed the white list password check, the device keeps this password and executes the remaining command line after the reboot with this same password.

For Example:

```
"PASSWORD execute reboot; getVariable1"; "get VARIABLE2"
"PASSWORD execute reboot; PASSWORD get Variable1"; "get VARIABLE2"
```



Important: Commands, variables and values are case sensitive.

List of basic commands

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

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

Table 9-5 List of basic SMS diagnostic commands

Item	Command	Definition
1	reboot	Immediately performs a soft reboot.
2	pdpcycle	Disconnects (if connected) and reconnects the data connection. If a profile number is selected in the command, try to disconnect/reconnect the specified profile in case the profile is active. If no profile number is selected, try to disconnect/reconnect the current active profile. Reports an error if no profile number is selected and there is no currently activated profile.
3	pdpdown	Disconnects the PDP. If a profile number is selected in the command, the router tries to disconnect the specified profile in case the profile is active. If no profile number is selected, try to disconnect the current active profile. Reports an error if no profile number is selected and there is no currently activated profile.
4	pdpup	Reconnects the PDP. If a profile number is selected in the command, the router tries to connect with the specified profile. If no profile number is selected, the router tries to connect to the last active profile. The gateway will check the currently activated profile and disconnect this profile before executing the command. The router reports an error if no profile number is selected and there is no stored last active profile number.
5	factorydefaults	Performs a factory reset on the router. Be aware that this command also clears the SMS white list on the router.
6	download	Performs a download and install of a Firmware Upgrade (.cdi), Config File (.tar.gz) or a help document (.pdf) file. If the file is a firmware image as in the case of a .cdi file, the router will apply the recovery image first and then the main firmware image. The download location is specified immediately after the command and may be from an HTTP or FTP source URL. If the file is a .cdi file, the router will apply the file as a configuration file update for the device and reboot afterwards. If the file is a .pdf, the router will assume this is a user guide document and save it to the router and make the file available for viewing via the help menu on the Web-UI. Note: If your download URL includes any space characters, please encode these prior to transmission according to RFC1738, for example:

Item	Command	Definition
		ftp://username:password@serveraddress/directory%20with%20spaces/filename.cdi Note: Authenticated FTP addresses may be used following the format as defined in RFC1738, for example: ftp://username:password@serveraddress/directory/filename.cdi
10	ssh.genkeys	Instructs the router to generate new public SSH keys.
11	ssh.clearkeys	Instructs the router to clear the client public SSH key files.

List of get/set commands

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

Table 9-6 SMS - List of get/set commands

Command name	Example	Description
get status	get status	Returns the Module firmware version, LAN IP Address, Network State, Network operator and Signal strength.
get sessionhistory	get sessionhistory	Returns the time and date of recent sessions along with the total amount of data sent and received for each session.
set syslogserver	set syslogserver=123.45.67.89:514	Sets a remote syslog server IP or hostname and port.
get plmnscan	get plmnscan	Instructs the router to perform a network scan and returns the results by SMS.
set forceplmn	set forceplmn=505,3	Sets the operator to a manual selection made by the user where “505” is the Mobile Country Code for Australia. As no network type (e.g.. LTE/5G) is specified, it is selected automatically.
get forceplmn	get forceplmn	Returns the operator and network type selection mode (Automatic/Manual), in addition to the MCC and MNC values
get ledmode	get ledmode	Returns the status of the LED operation mode.
set ledmode	set ledmode=10	Sets the LED operation mode to be always on or to turn off after the specified number of minutes.
get ssh.proto	get ssh.proto	Returns the SSH protocol in use.
set ssh.proto	set ssh.proto=1,2	Sets the SSH Protocol to protocol 1, 2 or both (1,2).

Command name	Example	Description
get ssh.passauth	get ssh.passauth	Returns the status of the SSH Enable password authentication option.
set ssh.passauth	set ssh.passauth=1	Sets the SSH Enable password authentication option on or off.
get ssh.keyauth	get ssh.keyauth	Returns the status of the SSH Enable key authentication option.
set ssh.keyauth	Set ssh.keyauth=1	Sets the SSH Enable key authentication option on or off.
get download.timeout	get download.timeout	Returns the time in minutes that the router waits before a download times out.
set download.timeout	set download.timeout=20	Sets the time in minutes that the router waits before a download times out. This is set to 10 minutes by default. Supported range is 10 – 1440 minutes.
get install.timeout	get install.timeout	Returns the time in minutes that the router waits before a file that is being installed times out.
set install.timeout	set install.timeout=5	Sets the time in minutes that the router waits before a file that is being installed times out. This is set to 3 minutes by default. Supported range is 3 – 300 minutes.
get sw.version	get sw.version	Returns the software version of the router.

List of basic RDB variables

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

Table 9-7 SMS - List of basic SMS diagnostics RDB variables

#	RDB variable name	SMS variable name	Read/Write	Description	Example VALUE
0	link.profile.1.enable link.profile.1.apn link.profile.1.user link.profile.1.pass link.profile.1.auth_type	profile	RW	Profile	Read: (profile no,apn,user,pass,auth,iplocal,status) 1,apn,username,password, chap,202.44.185.111,up

#	RDB variable name	SMS variable name	Read/Write	Description	Example VALUE
	link.profile.1.iplocal link.profile.1.status				Write: (apn, user, pass,auth) apn,username,password
2	link.profile.1.user	username	RW	Cellular broadband username	Guest, could also return "null"
3	link.profile.1.pass	password	RW	Cellular broadband password	Guest, could also return "null"
4	link.profile.1.auth_type	authtype	RW	Cellular broadband Authentication type	"pap" or"chap"
5	link.profile.1.iplocal	wanip	R	WAN IP address	202.44.185.111
6	wwan.0.radio.information.signal_strength	rsssi	R	Cellular signal strength	-65 dBm
7	wwan.0.imei	imei	R	IMEI number	3.57347E+14
8	statistics.usage_current	usage	R	Cellular broadband 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 cellular broadband session	1 days 02:30:12 or 0 days 00:00:00 when wwan down
10	/proc/uptime	deviceuptime	R	Device up time	1 days 02:30:12
11	wwan.0.system_network_status.current_band	band	R	Current band	NR5G BAND 78

Network scan and manual network selection by SMS

Performing a network scan:

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

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

- MCC
- MNC
- Network Type (LTE, 5G)

- Provider's Name
- Operator Status (available, forbidden, current)

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

```
plmnscan=505,03,7,vodafone AU,1;505,03,1,vodafone AU,1;505,03,9,vodafone AU,4;505,01,7,Telstra
Mobile,1;505,01,1,Telstra Mobile,1;505,02,9,YES OPTUS,1;505,02,1,YES OPTUS,1;505,01,9,Telstra
```

Table 9-8 Operator status codes returned by get plmnscan SMS command

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

Note:

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

Setting the router to connect to a network

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

The command format for the **set forceplmn** command is:

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

For example:

```
set forceplmn=0
```

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

```
set forceplmn=505,9
```

Sets the operator to a manual selection made by the user where “505” is the Mobile Country Code for Australia and “1” is the Mobile Network Code for Telstra. As no network type (e.g. LTE/5G) is specified, it is selected automatically.

```
set forceplmn=505,1,9
```

Sets the operator and network type to a manual selection made by the user where “505” is the Mobile Country Code for Australia, “1” is the Mobile Network Code for Telstra and “9” is the LTE network type.

Table 9-9 SMS - Mobile Network Provider codes (Australia)

Mobile Network Code	Mobile Network Provider
1	Telstra
2	Optus
3	Vodafone

Confirming the currently configured operator and network type

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

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

```
Automatic, 505, 1
```

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

SMS diagnostics examples

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

If the default setting of **Only accept authenticated SMS messages** is enabled then password authentication is required. Add your password followed by a space as a prefix to the command, for example

If authentication required:

```
PASSWORD set username= "<username>"
```

If authentication not required:

```
set username='<username>'
```



Note: The authentication setting is located in the user interface at Services > SMS messages > Diagnostics.

Table 9-10 SMS – SMS diagnostics example commands

Description	Input Command (without PASSWORD prefix)
Send SMS to change the data connection username	<code>set username='<username>'</code>
Send SMS to change the data connection password	<code>set password= `<password>`</code>
Send SMS to change the data connection authentication	<code>set authtype= 'pap'</code>
Send SMS to reboot	<code>execute reboot</code>

Description	Input Command (without PASSWORD prefix)
Send SMS to check the WAN IP address	get wanip
Send SMS to check the mobile signal strength	get rssi
Send SMS to check the IMEI number	get imei
Send SMS to check the current band	get band
Send SMS to Disconnect (if connected) and reconnect the data connection	execute pdpcycle
Send SMS to disconnect the data connection	execute pdpdown
Send SMS to connect the data connection	execute pdpup
Send multiple get command	get wanip; get rssi
Send multiple set command	set ssh.genkeys=1; set username=test; set auth=pap
Send SMS to reset to factory default settings	execute factorydefaults
Send SMS to retrieve status of router	get status
Send SMS to retrieve the history of the session, including start time, end time and total data usage	get sessionhistory
Send SMS to configure the router to send syslog to a remote syslog server	set syslogserver=123.209.56.78
Send SMS to perform firmware upgrade when firmware is located on HTTP server	execute download http://download.com:8080/firmware_image.cdi execute download http://download.com:8080/firmware_image_r.cdi
Send SMS to perform firmware upgrade when firmware is located on FTP server	execute download ftp://username:password@download.com/firmware_image.cdi execute download ftp://username:password@ download.com/firmware_image_r.cdi
Send SMS to download and install IPK package located on HTTP server	execute download http://download.com:8080/package.ipk
Send SMS to download and install IPK package located on FTP server	execute download ftp://username:password@ download.com:8080/package.ipk
Send SMS to set the LED mode timeout to 10 minutes	set ledmode=10
Send SMS to retrieve the current LED mode	get ledmode
Retrieve current SSH protocol	get ssh.proto
Select SSH protocol	set ssh.proto=1
Retrieve password authentication status	get ssh.passauth

Description	Input Command (without PASSWORD prefix)
Enable/disable password authentication on host	<code>set ssh.passauth=1</code> or <code>set ssh.passauth=0</code>
Generate set of public/private keys on the host	<code>execute ssh.genkeys</code>
Clear client public keys stored on host	<code>execute ssh.clearkeys</code>
Send SMS to initiate a Network Quality test	<code>get networkquality</code>

Inbox

The Inbox displays all received messages that are stored on the router.

Figure 9-5 SMS – Inbox

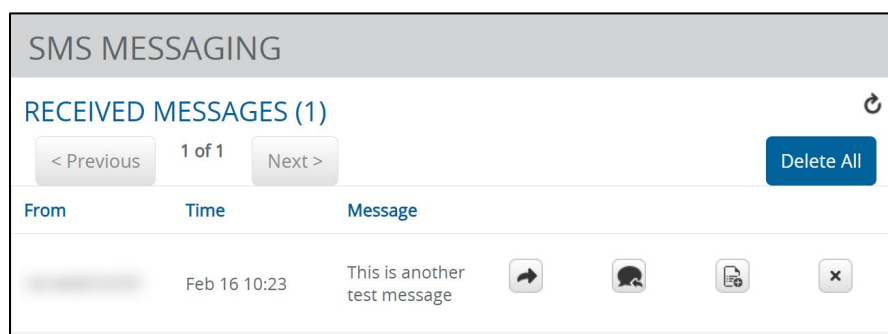


Table 9-11 SMS - Inbox

Icon	Name	Description
	Forward	Opens a new message window where you can forward the corresponding message to another recipient.
	Reply	Opens a new message window where you can reply to the sender.
	Add to White list	Add the sender's mobile number to the white list on the router.
	Delete	Delete the corresponding message.
	Refresh	Refresh the inbox to see new messages.

Compose Message

The Compose Message page can be used to send SMS text messages to a single or multiple recipients. To access the Compose message page, click **Services** tab on the menu bar, click **SMS messaging**, and in the dropdown click **Compose Message**.

A new SMS message can be sent to a maximum of 9 recipients at the same time. After sending the message, the result is displayed next to the destination number as "Success" or "Failure". By default, only one destination number field is displayed. Additional destination numbers may be added one at a time after entering a valid