TELiG

User Guide

Firmware Rev 2.5.1

NOTICE

Due to the nature of wireless communications, data delivery cannot be guaranteed. Data transmission or reception may be corrupted, delayed, or lost. The E1500 product should not be used in situations where failure of communications could result in damage of any kind to the user or any other party. Council Rock assumes no liability for damages resulting from delays or errors in data transmitted or received using the E1500 product, or for failure of the product to transmit or receive data.

SAFETY AND HAZARDS

This product is classified for Class I Div 2 locations. See also Certifications.

LIMITATION OF LIABILITY

The information in this manual is subject to change without notice by Council Rock. Council Rock and its affiliates specifically disclaim liability for any and all direct, indirect, special, general, incidental, consequential, punitive or exemplary damages including, but not limited to, loss of profits or revenue or anticipated profits or revenue arising out of the use or inability to use any Council Rock product, even if Council Rock and/or its affiliates have been advised of the possibility of such damages or they are foreseeable, or for claims by any third party.

Notwithstanding the foregoing, in no event shall Council Rock and/or its affiliates aggregate liability arising under or in connection with the E1500 product, regardless of the number of events, occurrences, or claims giving rise to liability in excess of the purchase price of the E1500 product.

CONTACT INFO

Sales	sales@councilrock.com
Technical Support	techsupport@councilrock.com
Corporate Info	https://councilrock.com

Contents

Overview 5
E1500 5
Product Description 5
Product Features 5
Product Details 7
Description 7
Front Panel 8
Top Row 8
Bottom Row 9
Rear Panel 10
Hardware 11
Software 11
Accessories 12
Model Options 12
Initial Setup 13
Unpacking 13
Connect 13
Web Admin 14
Troubleshooting 16
Settings and Web Admin Interface 17
STATUS 17
SYSTEM 31
VPN 45
SERVICES 53
NETWORK 58
Radio Specifications 87
Ordering Information 87
Model Options 87

Hardware Summary 88
RF Specifications 89
Regulatory Info 90
Certifications 90
Hazardous Locations 90
FCC Notice 90
Important Information on Radio Exposure 90
Warranty 91
Appendix A: 93
CONFIGURATION FUNDAMENTALS 93
Fundamentals A: SIM card installation 93
Fundamentals B: LAN Interface config 95
Fundamentals C: WAN Interface config 98
Fundamentals D: System Administration 101
Appendix B: 105
USE CASES 105
Use Case A: Serial Connection via WAN 105
Use Case B: LAN to WAN traffic 107
Use Case C: SIM Failover 114
Use Case D: Radio Module Failover 116
Use Case E: Interface Bridging 124
Use Case F: SNMPD Trap Alerts 126
Appendix C: 127
List of Acronyms 127
Appendix D: 130
List of Tables / List of Figures 130

Overview

E1500

Product Description

The Council Rock E1500 is a rugged edge computing device with LTE communications capability and Remote Terminal Unit (RTU) protocol bridging features. It provides wireless connectivity for a wide range of critical infrastructure applications including Industrial IoT, Distribution Automation (DA), Distributed Intelligence, and Smart Cities.

Product Features

The E1500 is a Linux-based networking device featuring:

Hardware

- Ruggedized carrier grade design
- Dual-Core ARM Cortex-A9 32-bit microprocessor
- 1 GB DDR3 High Performance Random Access Memory (RAM)
- 8 GB High Performance Flash Memory
- 2 10/100/1000 Ethernet RJ45 Interface ports
- 1 RS232/RS422/RS 485 auto-sensing serial port for RTU device communications
- 1 RS232 serial port for RTU device communications
- 1 RJ45 console port for direct console communications with a PC
- 3 radio expansion slots

Software

- Open Source Linux Operating System
- Edge Intelligence Framework
- Networking & Security
- Embedded Wireless & Wired Communications
- Device Management Support
- Over-the-Air update capability

The E1500 can be configured with private/public carrier LTE, Cat-M/NB IoT, and Wi-Fi radios for local and wide area network connectivity. The unit also has an embedded GPS receiver to obtain precision timestamps and location data.

The E1500 leverages OpenWRT Linux and includes several sophisticated software packages tailored to Distribution Automation solutions, including:

- Automatic Network Routing software that ensures connectivity of RTU devices to connected networks through the serial and Ethernet ports.
- IP Router/Firewall/VPN capabilities including BGP, MPLS, RIPv2, EIGRP, LDP, IS-IS, OSPF, DMVPN, RPL, GRE, etc.
- RTU command, control, and monitoring protocol translation software for standard RTU communications protocols including DNP3 and MODBUS that intelligently bridge legacy serial communications to the radio network.
- Device management via SNMP and COAP
- Device settings configured via a web browser based graphical user interface. For advanced users, the admin interface is accessible through a secure shell (SSH) console over Ethernet or Wi-Fi (optional), enabling complete control of the unit if necessary.

Product Details

Description

The E1500 is an edge computing WLAN device that connects end devices to the enterprise network with multiple interface options.

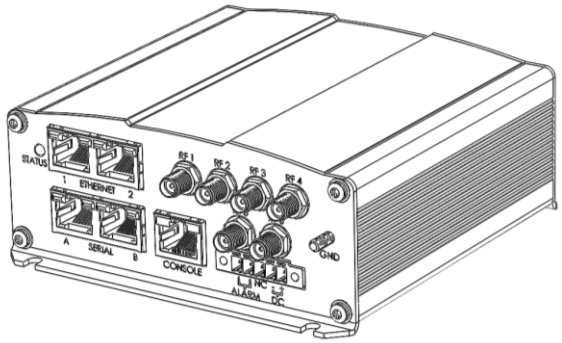

Figure 1: Models E1500-L8N, E1500-8NW

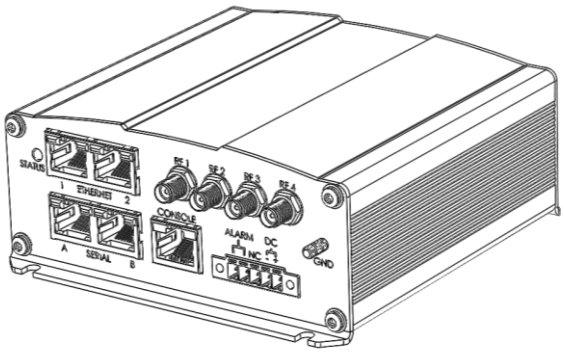

Figure 2: Models E1500-LW, E1500-8W

Front Panel

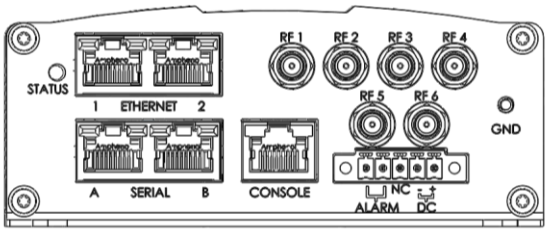

Figure 3: Models E1500-L8N, E1500-8NW

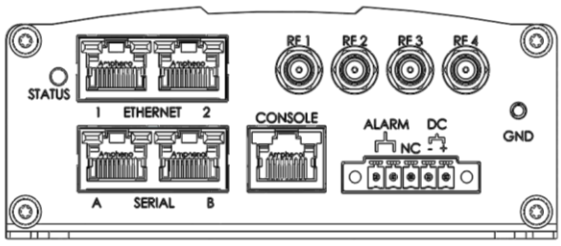

Figure 4: Models E1500-LW, E1500-8W

Top Row

(1) Status LED – System status indicator for LTE models. (LEDs are configurable for non-LTE models - see *System > LED Configuration*)

Appearance	Status
Red Blinking	System Active, Not joined to radio network
Green Blinking	System Active, Joining radio network
Green Solid	System Active, Joined radio network

Table 1*: LED Status List*

(2) Ethernet 1 / Ethernet 2 Connectors - 10/100/1000 Mbps, Ethernet autodetection

(4) RF Connectors #1-#4

(2) RF Connectors #5-#6 (on some models)

(1) GND Connector

Models	RF Connectors
E1500-LW E1500-8W	4
E1500-L8N E1500-8NW	6

Table 2: RF Connectors by Model

RF Ports map to wan interfaces as shown in the table below, where “Main” indicates the primary radio antenna connector, while “Aux” indicates the secondary radio antenna.

RF Port	L8N	LW	8NW	8W
1	wan_a Main	wan_a Main	wan_b Main	wan_b Main
2	wan_a Aux	wan_a Aux	wan_b Aux	wan_b Aux
3	wan_c	WiFi CH1	wan_c LTE	WiFi CH1
4	GPS	GPS	GPS	GPS
5	wan_b Main		WiFi CH1	
6	wan_b Aux		WiFi CH2	

Table 3: RF Port to WAN mapping

Bottom Row

(1) SERIAL A Port – RS 232 / RS 485, serial comms, software configurable
(1) SERIAL B Port – RJ45 – RS 232 serial comms
(1) Console Port – TTL-level system console serial interface

Serial pinouts are given below, and in the table that follows.

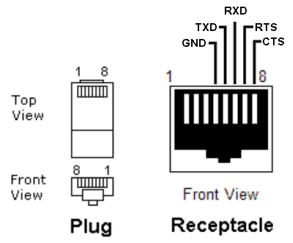

Figure 5: Serial Port Pinout - RS232 (Serial)

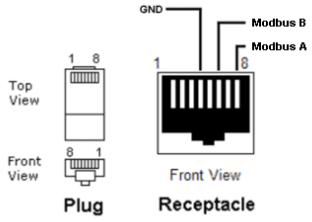

Figure 6: Serial Port Pinout – RS485 (Modbus)

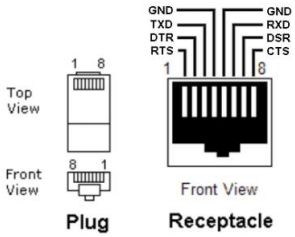

Figure 7: Serial Port Pinout – RS232 (Console)

NOTE: The pin-outs shown may not match all devices as there is no standard for pin connections or levels for RS232 on RJ458-pin modular connectors. RS422 serial over RJ45 requires a separate converter.

See Also: Serial Configuration

Pin	RS232 (serial)	RS485 (ModBus)	RS232 (console)
1	-	-	RTS
2	-	-	DTR
3	-	-	TXD
4	GND	GND	GND
5	TXD	-	GND
6	RXD	Modbus B	RXD
7	RTS	-	DSR
8	CTS	Modbus A	CTS

Table 4: Common Serial pinouts

(1) Alarm / Power Connector – Door alarm / tamper sensor inputs and DC power. Alarm connection is a dry contact.

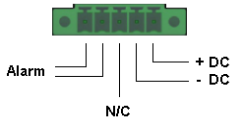

Figure 8: Alarm / Power Connections

Rear Panel

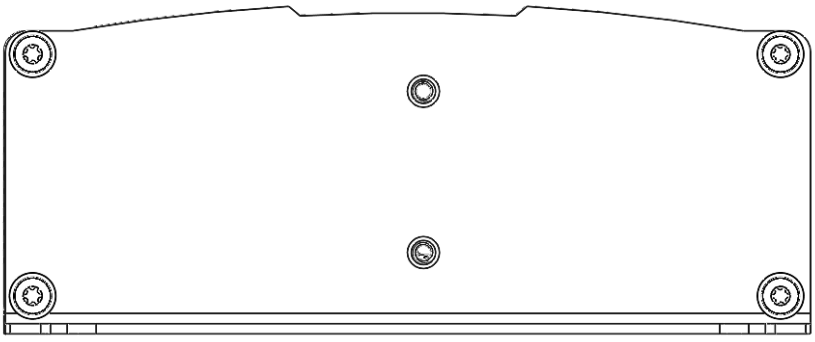

Figure 9: Rear Panel - Note center screw holes for DIN-rail mount accessory

Hardware

The E1500 unit consists of two primary circuit boards: a Gateway processor card and a power/interface card. The Power/Interface card includes a wideband DC power supply that converts primary input power to the voltages required for the processor and peripherals. The Power/Interface card also includes circuitry to convert serial data signals into EIA-561 compatible serial via an RJ-45 connector. The unit can be powered through the front panel terminal block connector (9-60VDC) or through 802.3af PoE via Ethernet1.

The E1500 leverages a dual core ARM Coretex-A9 processor to control all peripherals and run edge intelligence applications. The unit comes standard with 1 GB RAM and 8 GB eMMC flash storage. There are two 10/100/1000 Ethernet ports, two serial, and three peripheral expansion slots.

Three peripheral expansion slots include two mini-PCI express (mPCIe) and one m.2 form factor. A variety of cards are commercially available to enable communications over a wide range of interfaces.

The i.MX6 ARM Cortex-A9 processor is used to connect the serial and Ethernet ports to peripherals placed in these expansion slots. The Gateway processor card also includes onboard GPS, a gyro, and encryption co-processor.

Software

The E1500 unit is based on the OpenWRT Linux operating system. The operating system runs on top of a secure file system that includes secure boot and encryption.

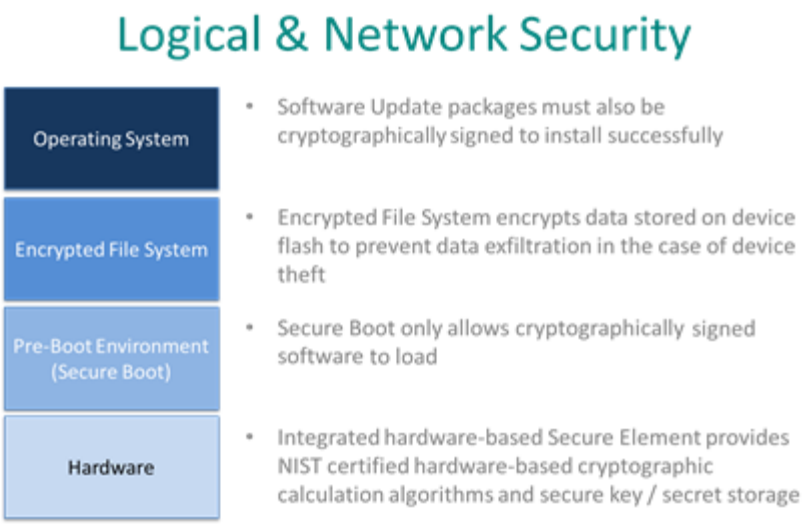

Figure 10: Software Architecture

The device comes configured with a suite of tools and services to enable Distribution Automation (DA), Smart Networking, and Network Function Virtualization.

The software supports an edge intelligence framework that can run 3rd party applications. The Linux operating system is customized with advanced features to enable secure resource allocation and isolation, which provide the foundation for containerizing these applications.

Accessories

A range of accessories are available including connectors, mounting, antennas, and more. Contact your sales representative at sales@councilrock.com for more information.

Model Options

All E1500s include Public/Private LTE.

Optional communications include LTE-CBRS, LTE Cat-M/NB-IoT, Private Enterprise Broadband 900MHz 3+3MHz FDD, and 2.5/5 GHz WiFi. See **Radio Specifications** for details.

Configuration

Initial Setup

Unpacking

Check the contents against the packing list secured to the outside of the box when unpacking. Council Rock recommends saving all shipping materials in case the unit needs to be returned. Contact Council Rock Support for assistance or notification of any issues.

Connect

1. Connect RF Antenna(s) and GPS antenna to the unit
2. Insert SIM card(s) - see Appendix A for details
3. Connect DC power to the power block
4. (Optional) Attach Alarm sensors to the power block
5. Attach the power block to the front panel
6. Plug in the power supply. The E1500 will boot
7. Front panel LED changes state based on network connection status

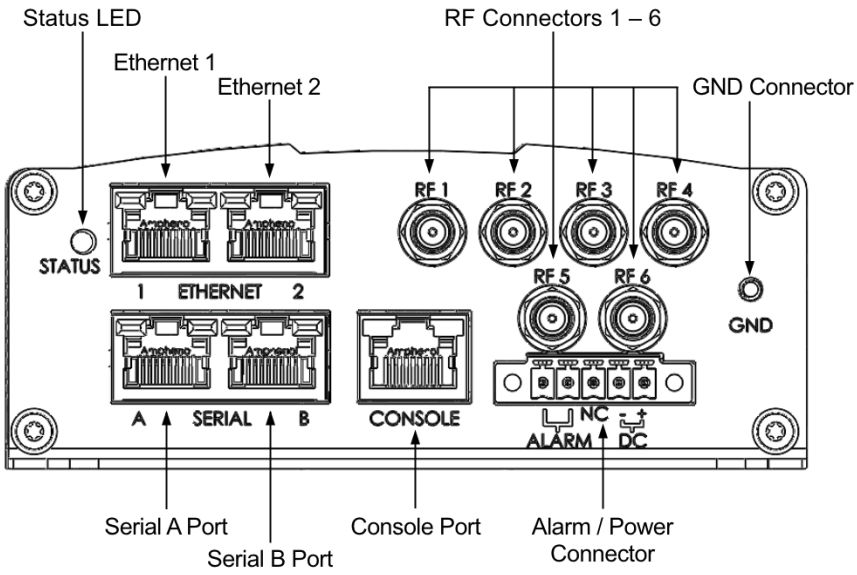

Figure 11: Unit Connections

Note that front panels differ across models. Panel shown is an example.

Web Admin

1. Connect a standard Ethernet cable from your PC to Ethernet 1 on the front panel.
2. The unit should receive an IP address in the 10.0.0.0/24 range from the DHCP server. If not, configure the PC interface with a static IP in the 10.0.0.0/24 subnet, except 10.0.0.1 which is used by the Ethernet 1 interface.
3. Using a web browser, navigate to https://10.0.0.1. Confirm the security exception when it appears in the browser -- the E1500 is factory-configured with a self-signed certificate for its web server.
4. At the login screen, access the Web Admin Interface with the username and password provided. *Note: after three failed logins, the root user is blocked for 300 seconds between successive login attempts. All other users are blocked for 30 seconds between successive login attempts.*

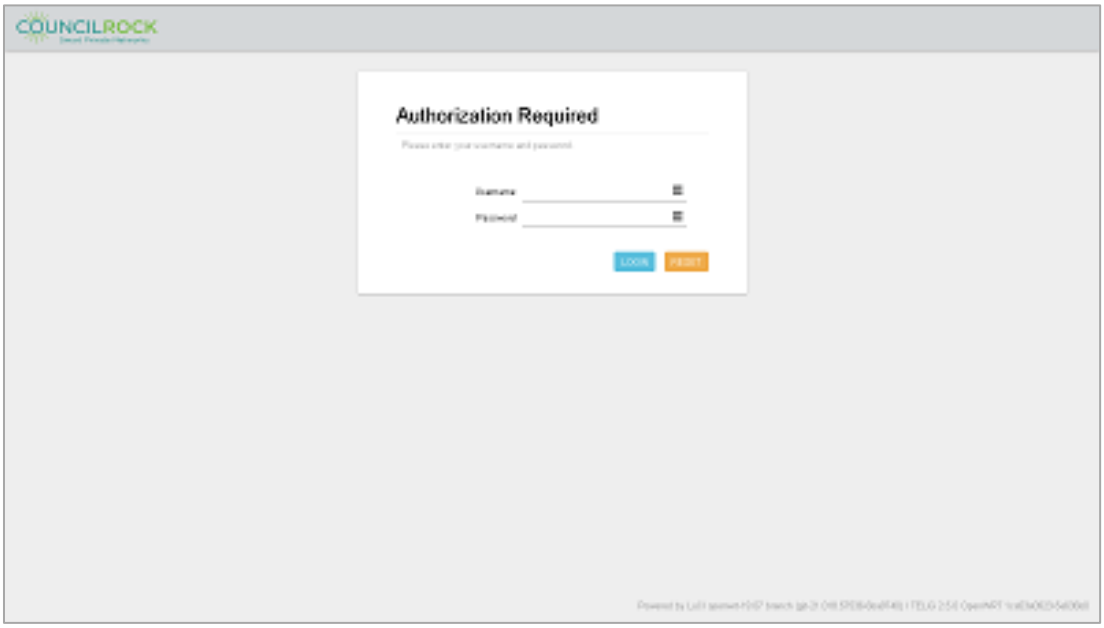

Figure 12: Login Screen

5. For each SIM card installed, an Access Point Name (APN) must be configured.
    a. Navigate to *Network* > *SIMs*
    b. Note the interface for each SIM in the General Info Section
    c. In the APNs section, use the text boxes listed under the appropriate interface to enter each SIMs APN
    d. Click SAVE & APPLY

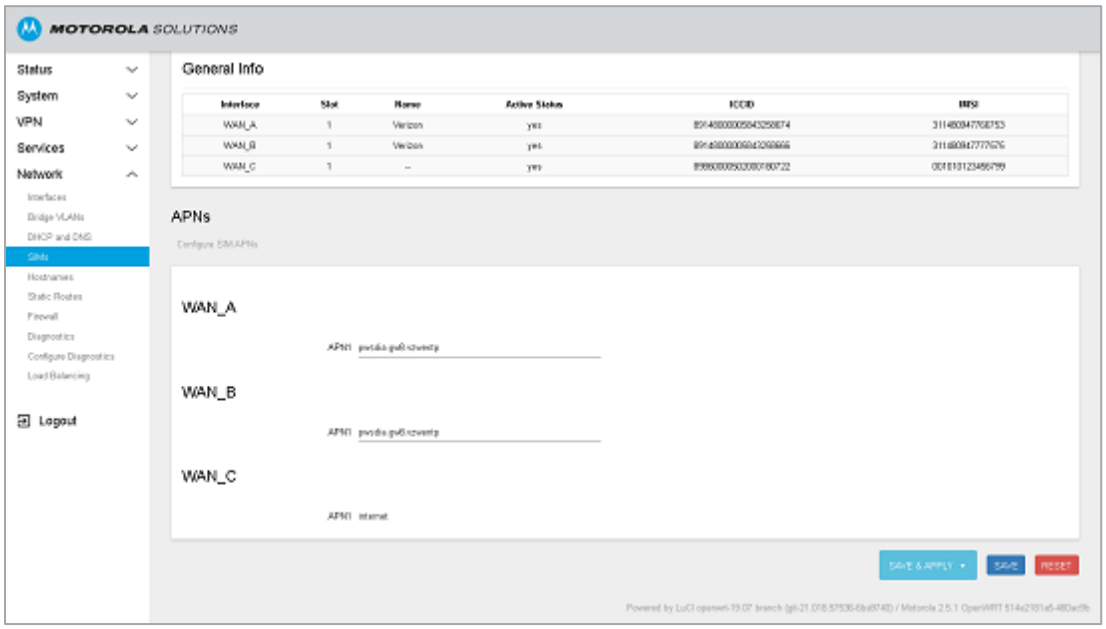

Figure 13: SIM Card APN Entry

Troubleshooting

After completing the procedure in “Connect” above, the E1500 should display a solid green light and be ready to use. If it is not, connect to the web admin using the procedure in “Web Admin” above, and review these troubleshooting steps:

1. Navigate to ***Status > LTE > Overview*** and review the information displayed. Identify the WAN interface you expect to use.
2. Confirm that the connection state is “connected”, and the operator is the expected provider. If not, verify the device information. If you do not see an ICCID or IMSI, there may be an issue with your SIM card or with the APN configuration which is associated with your SIM card.
3. If your device information appears correct, but you are not connected to your expected operator, navigate to the **Scan** tab. Run a cellular network scan for the interface through which you are expecting to connect, and verify that the modem is able to see the network to which you are expecting to connect.
4. If your connection state, operator, and signal quality all check out, double-check the **Bearers** tab to verify the unit has received an IP address.
5. Navigate to ***Network > SIMs*** and review the interface through which you are attempting to connect. Under APNs for the interface, verify that the correct APN has been entered.
6. Navigate to ***Network > Interfaces*** and select **Edit** on the interface through which you are attempting to connect.
7. On the **General Settings** tab check whether the interface IP Type is set to IPv4-only, IPv6-only, or both. IPv4-only setting is recommended unless IPv6 is required.
8. On the **Firewall Settings** tab, verify that the firewall zone assigned to the interface is set to “wan.” See *Network > Firewall*.

Settings and Web Admin Interface

The unit settings are managed through the Web Admin Interface, accessible through a web browser as described in Initial Setup. The unit settings are grouped by function as follows:

- STATUS
- SYSTEM
- VPN
- SERVICES
- NETWORK

Menus are organized by function in the left sidebar. Submenus for each function are accessible via Tab headings in the main window.

STATUS

The Status menus display current System Status Overview and status details of Firewall / LTE / GPS / Routing / Logging / Processes / Load Balancing. Real-time graphs of system performance are available here as well. Status menus are useful for gathering system info and/or troubleshooting. User input is generally not expected on the Status menus. Each menu is summarized in the following subsections.

Overview

The System Status Overview is displayed, including system information regarding hardware including serial number, model, and software version as well as memory utilization, network connections including IP/DHCP info for the active network, active DHCP leases, and Multi-Wide Area Network (MWAN) interfaces.

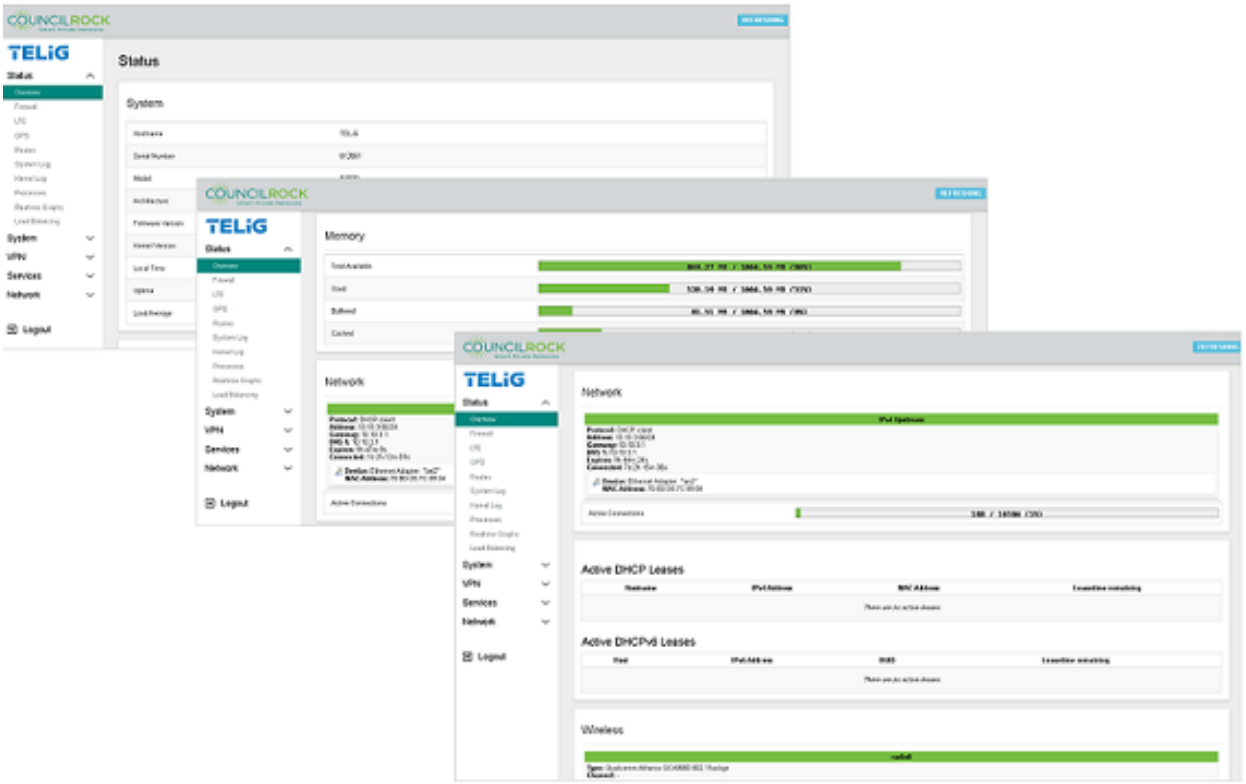

Figure 14: Status > Overview

Firewall

A complete list of active Firewall rules is displayed in this menu, with real time data regarding network traffic handled by these rules.

IPV4 and IPV6 are separately displayed by selecting the Tab at the top of the main window.

Firewall rules are shown at the WAN and LAN level for Inputs, Outputs, Forwarding, Rejection, and Quality of Service (QoS). Rules are sorted into Tables by FILTER / NAT / MANGLE / RAW. Firewall NAT tables apply to IPv4 only.

Each rule entry describes the rule via the target, protocol, input interface, output interface, source IP address or IP address range, and destination IP address or IP address range. Each rule entry also displays options and comments, if any. Finally, each rule entry displays the number of packets and amount of traffic handled by the rule.

Buttons at the top right of the screen allow the user to

- **Hide empty chains:** removes chains with no firewall rules from the display
- **Reset Counters:** to set all traffic counters to zero
- **Restart Firewall:** restarts all firewall rule chains

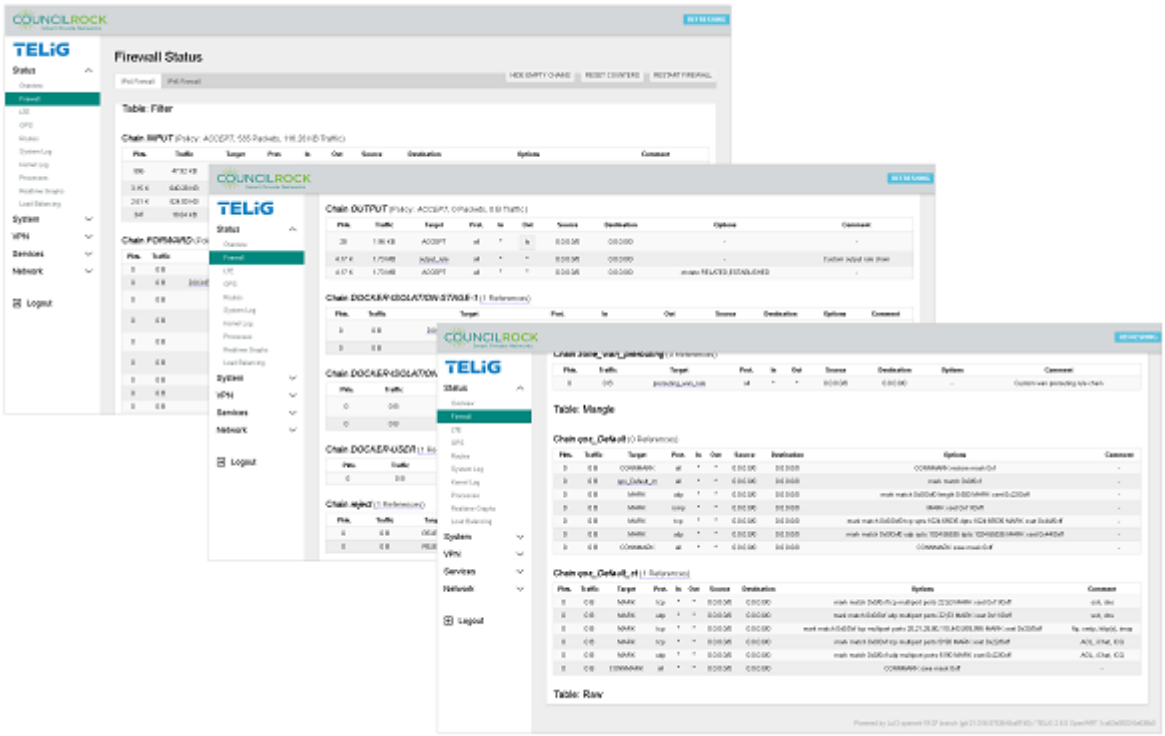

Figure 15: Firewall Menus

LTE

Displays information on the state of LTE modems and connections.

Submenus are accessible at the top of the LTE menu for displaying an overview of LTE WAN connections, LTE Bearers, LTE Signal indicators, and a Scan tool for troubleshooting.

The **Overview** tab provides connection status for each modem present, including connection state, registration state, operator information, and signal quality as a percentage, as well as device information for each modem present, including Integrated Circuit Card Identifier (ICCID), International Mobile Subscriber Identity (IMSI), and International Mobile Equipment Identity (IMEI).

Connection States - LTE modem is:

1. **Enabled:** not connected to the cellular network
2. **Connected**: connected the network provider
3. **Connecting**: attempting to activate the connection to the network provider
4. **Disconnecting**: deactivating the connection to the network provider
5. **Disabled**: not enabled and is powered down

Registration States - LTE modem is:

1. **Registered**: registered with network provider; data connections may be available for use
2. **Idle**: not registered, not searching for a new network provider to register with
3. **Searching**: not registered, searching for a new network provider to register with.

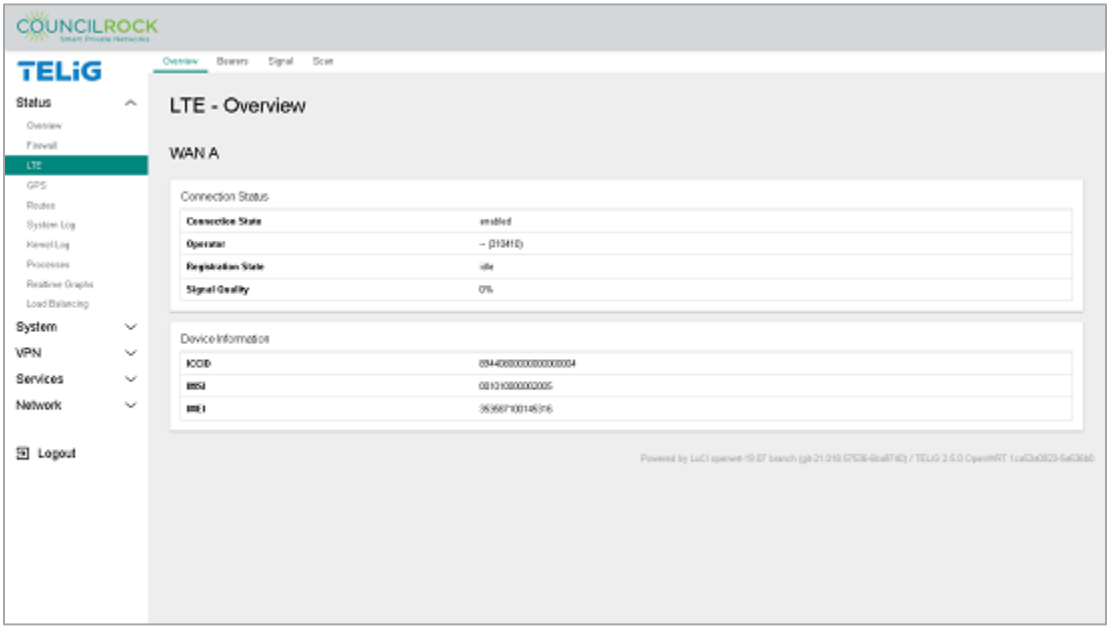

Figure 16: Status > LTE > Overview

Signal Quality is shown as a percentage in the range from 0-100%, where higher percentage indicates better signal quality. Signal quality is based on the LTE radio's RSSI level. In general, signal quality above 40% is usable.

The **Bearers** tab provides information on each LTE bearer network established for each modem present, including interface status, IPv4 and/or IPv6 network information, and data transmission statistics.

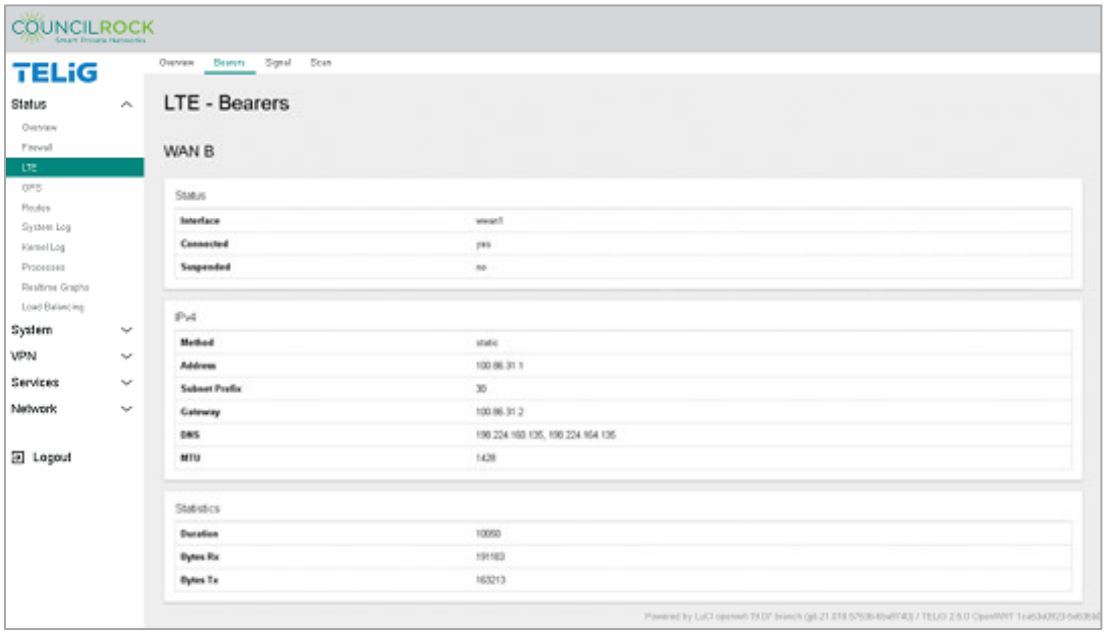

Figure 17: Status > LTE > Bearers

The **Signal** tab provides information for each modem present for the active band, channel, and cell, as well as quality information for the RF signal.

- **RSSI**: Received Signal Strength Indicator. Provides measurement of power received by the radio modem in the frequency band, including noise.
- **RSRP**: Reference Signal Received Power. Provides measurement of power of the LTE Reference signals spread over the full bandwidth and narrowband.
- **RSRQ**: Reference Signal Received Quality. Provides measurement of the quality of the signal considering not only RSSI but also the number of used Resource Blocks
- **SNR**: Signal to noise ratio. Provides measurement of the ratio of the power of the signal of interest to the average noise power within a specified bandwidth.

Signal quality level with respect to RSRQ thresholds (Referenced from TIA TSB-88.4 standards)

Signal Quality Level	RSRQ
Excellent	≥ -10
Good	-10 to -15
Fair	-15 to -20
Poor	< -20

Table 5: Signal Quality categories by RSRQ

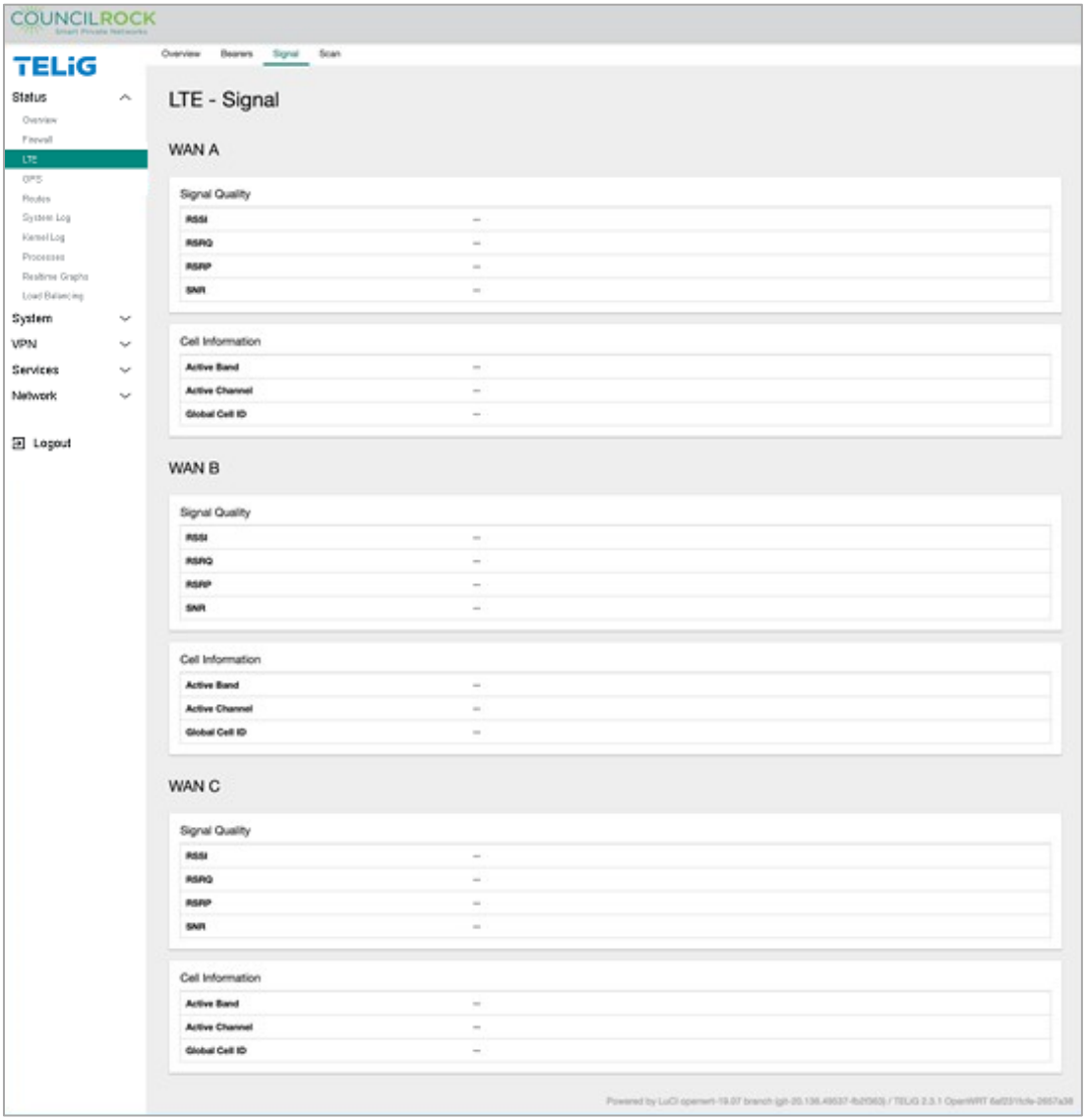

Figure 18: Status > LTE > Signal

Finally, the **Scan** tab provides a tool for the user to perform a network scan for time intervals from 30 to 90 seconds using any system modems, listing carriers detected. Details are given for Operator Code, Operator Name, Access Technology, and Availability.

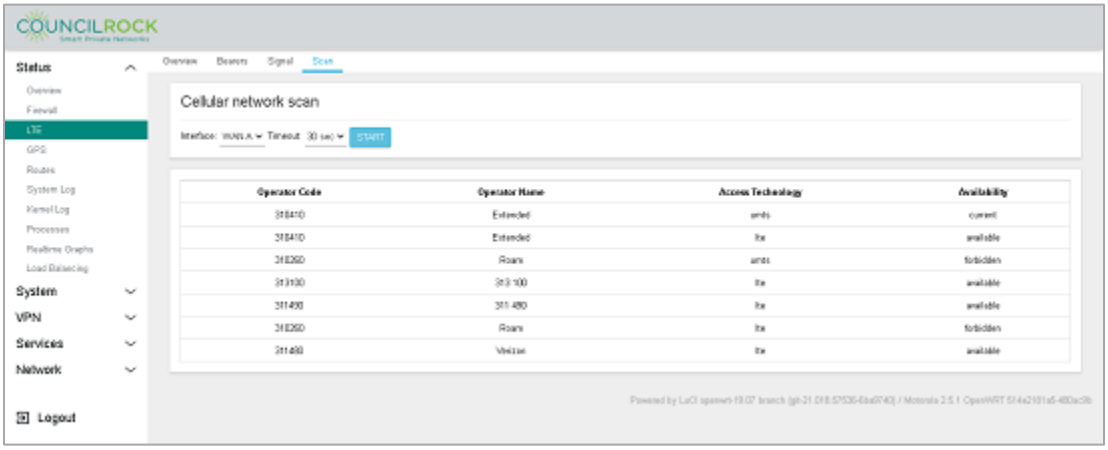

Figure 19: Status > LTE Scan: Cellular Network Scanning Tool

GPS

Information retrieved from the E1500's GPS connection is displayed. This includes the last known GPS location and time.

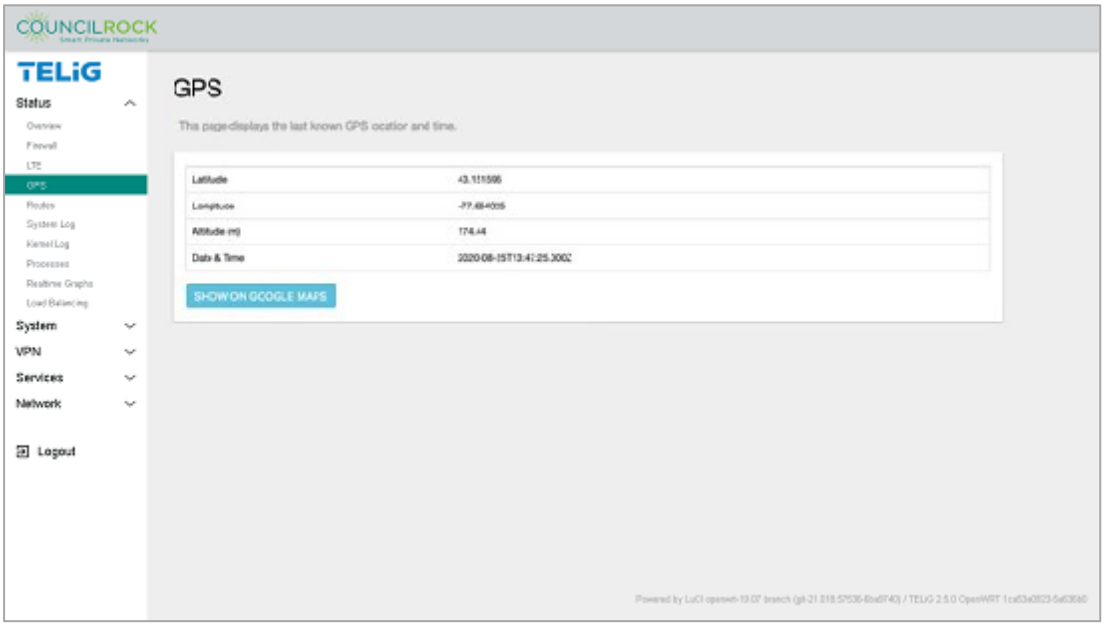

Figure 20: Status> GPS

Routes

Displays information on currently configured routing rules. The rules are divided into IPv4 and IPv6. An ARP table and an IPv6 neighbors table are also provided.

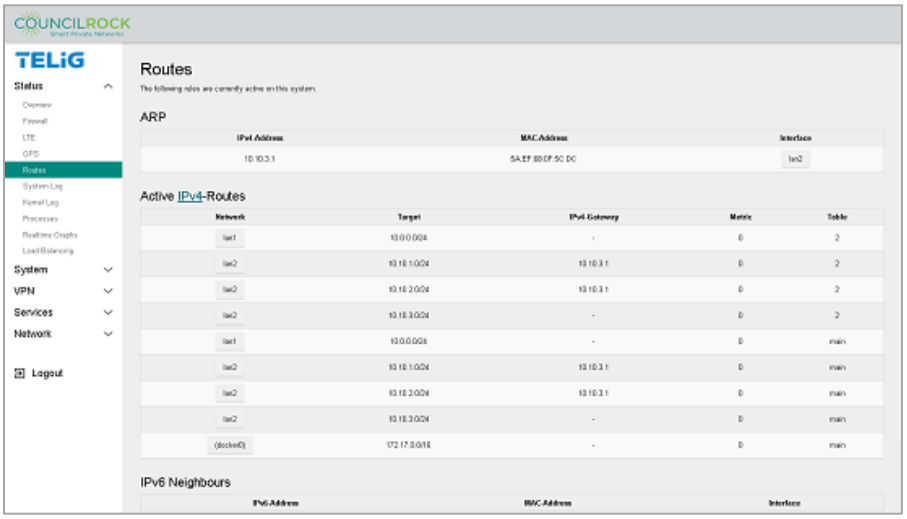

Figure 21: Status > Routes

System Log

The operating system log output is displayed.

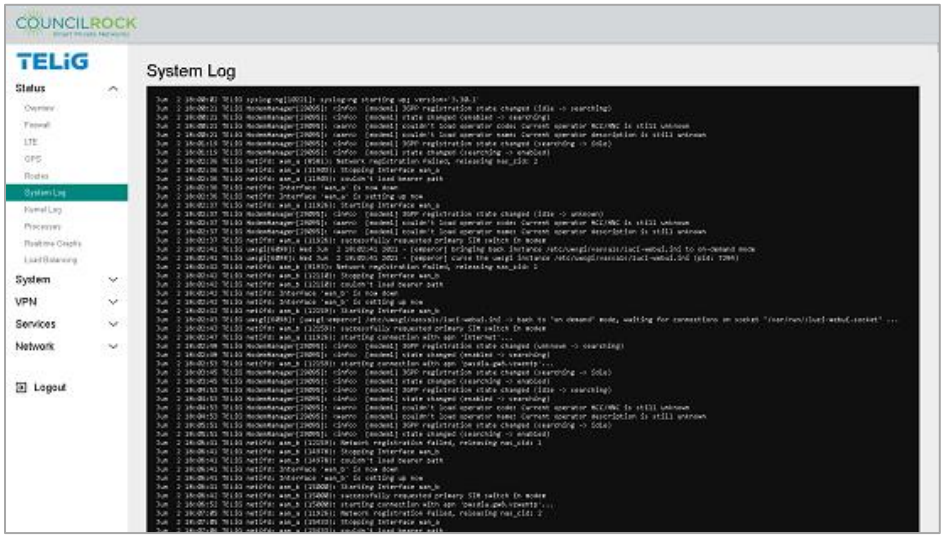

Figure 22: Status > System Log

Kernel Log

The operating system kernel log is displayed.

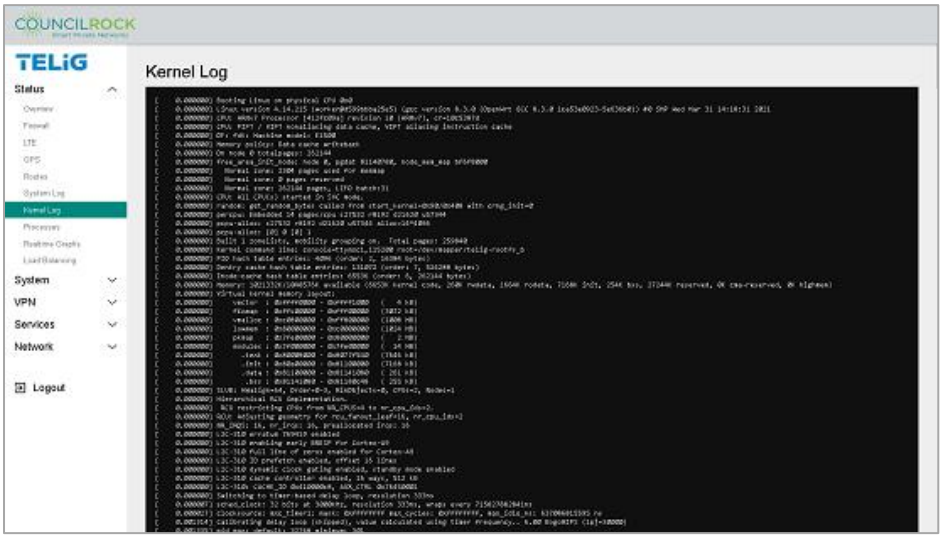

Figure 23: Status > Kernel Log

Processes

A list of currently running system processes is displayed, including process ID (PID), owner, command, and CPU / memory usage. To quit a process, action buttons are given for "Hang Up" and to forcibly quit an unresponsive process, the more aggressive "Terminate" and "Kill".

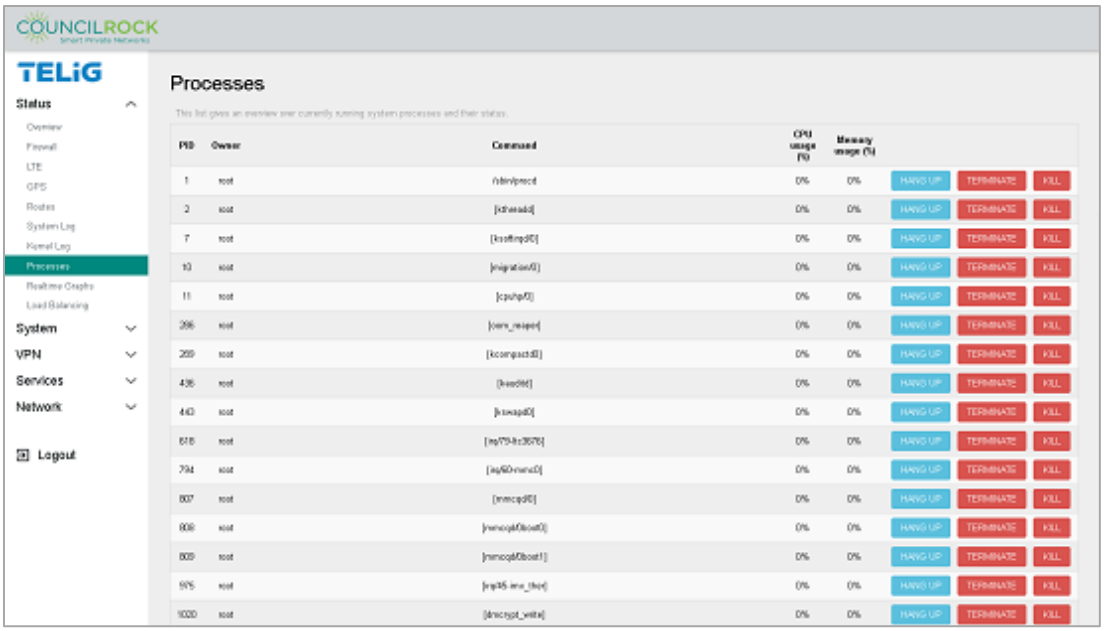

Figure 24: Status > Processes

Realtime Graphs

Displays live graphs of system performance.

The **Load** tab displays a live graph of the queue of processes handled by the CPU, as well as average and peak loads for the past 1, 5, and 15 minutes. Note that in a single core CPU, a load of 1.0 is considered fully loaded.

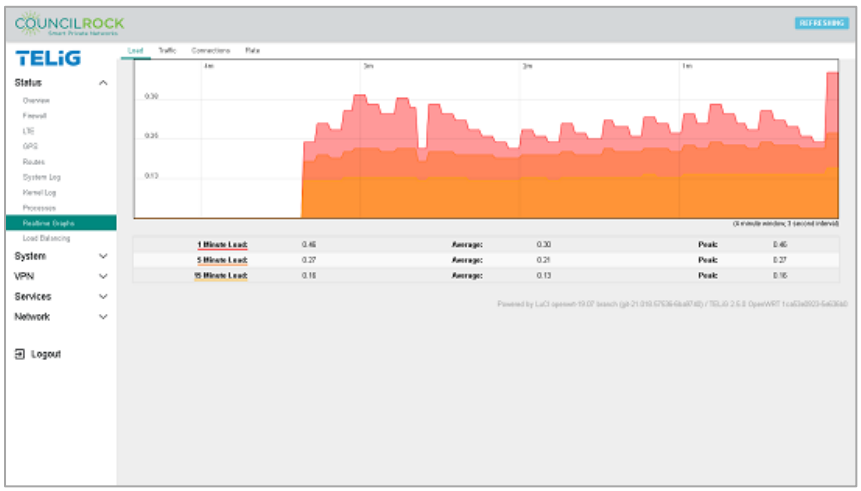

Figure 25: Status > Realtime Graphs > Load

The **Traffic** tab shows a live graph of inbound and outbound traffic as well as a table of average and peak inbound and outbound traffic. At the top of the graph is a selectable list of interfaces that the user can select.

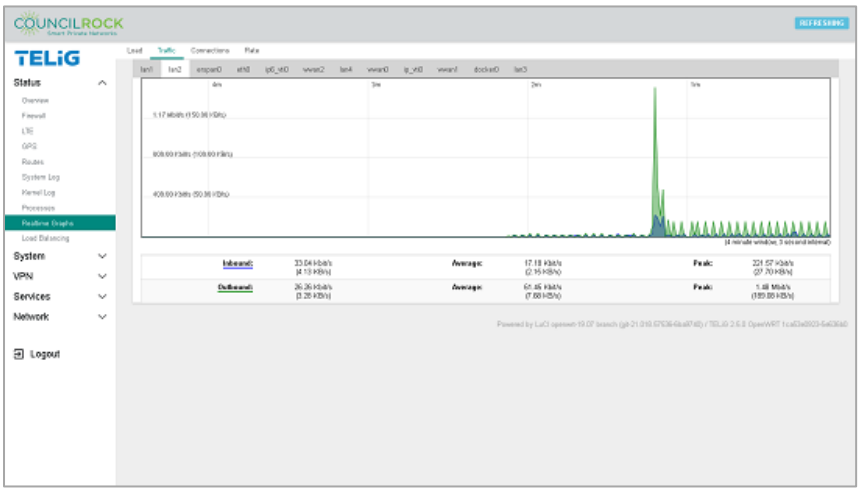

Figure 26: Status > Realtime Graphs > Traffic

The **Connections** tab provides a live graph of network connections, divided into TCP, UDP, and others, including averages and peaks. A table lists each active connection, its protocol, source, destination, and amount of data transferred.

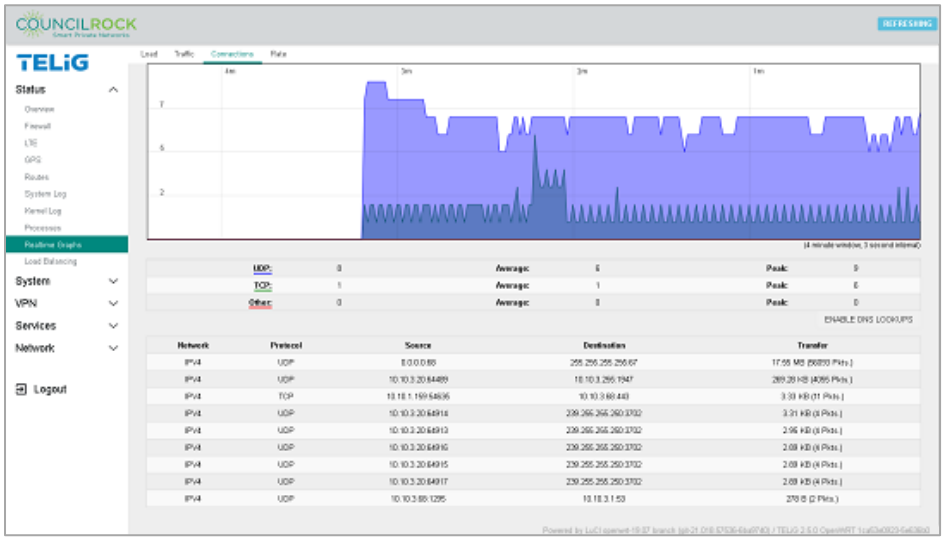

Figure 27: Status > Realtime Graphs > Connections

Finally, the **Rate** tab shows the real time download and upload rates by IP address, as well as total bytes and total packets over which the rate is calculated.

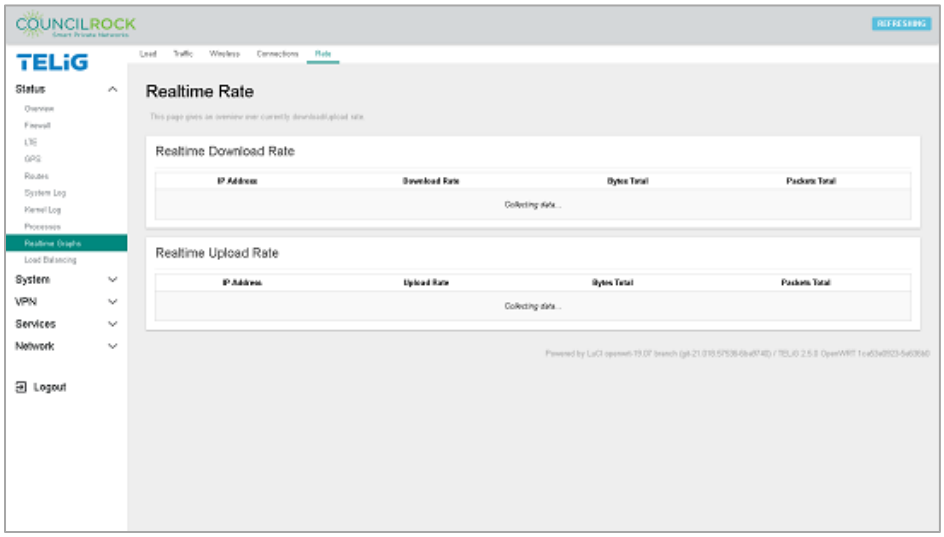

Figure 28: Status > Realtime Graphs > Rate

Load Balancing

Provides information on MWAN interfaces. The **Interface** tab lists all available MWAN interfaces and their status.

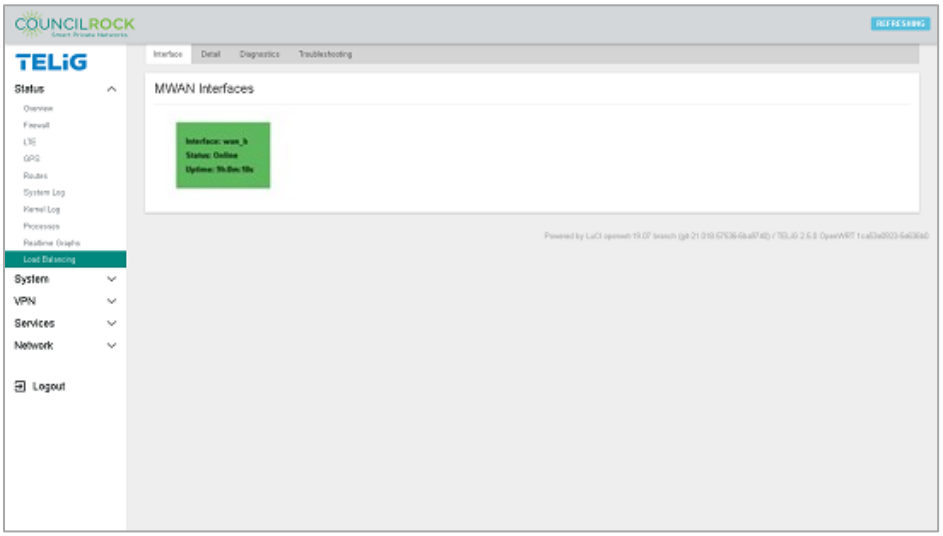

Figure 29: Status > Load Balancing > Interface

MWAN interfaces are the interfaces participating in a configured load balancing process. See **LAN to WAN Traffic** or **Radio Module Failover** use cases for details on how to configure these interfaces.

The **Detail** tab provides information from the operating system on interface status, IPv4 and IPv6 policies, and connected IPv4 and IPv6 networks.

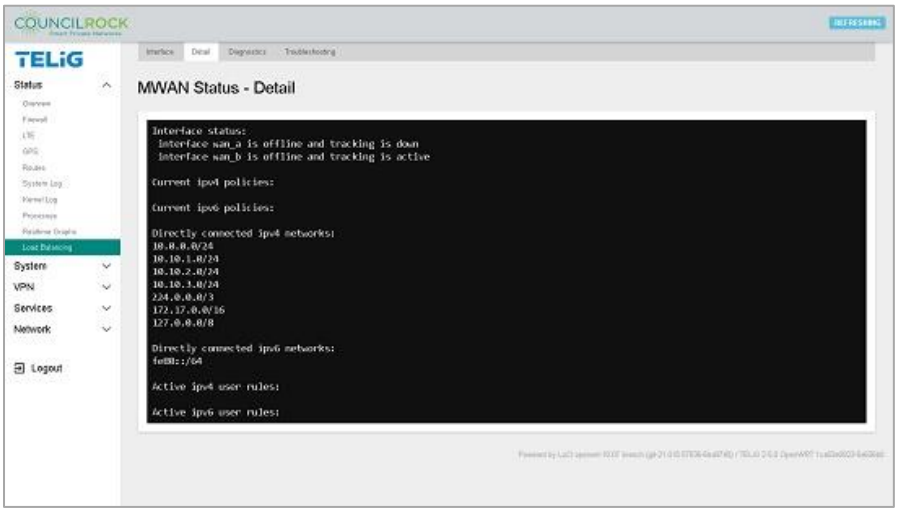

Figure 30: Status > Load Balancing > Detail

The **Diagnostics** tab includes basic tools for testing MWAN interfaces (Gateway ping, Ping tracking IP, Check IP rules, Check routing table, Hotplug ifup, Hotplug ifdown).

- **Gateway Ping:** Pings the interface gateway IP address defined for the WAN interface associated with the MWAN interface
- **Ping tracking IP**: Pings the "Tracking hostname or IP address" defined on *Network > Load Balancing > Interfaces*
- **Check IP rules:** Displays which routing table the MWAN interface will use to route traffic
- **Check routing table:** Displays the routing table defined for the WAN interface associated with the MWAN interface
- **Hotplug ifup:** Enables the specified MWAN interface
- **Hotplug ifdown:** Disables the specified MWAN interface

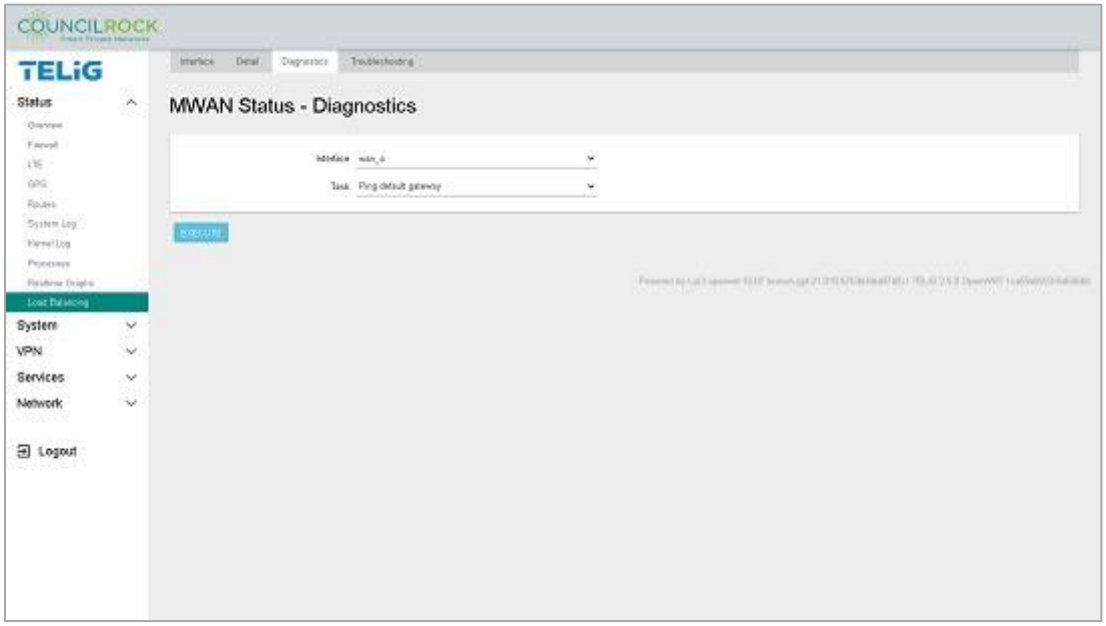

Figure 31: Status > Load Balancing > Diagnostics

The **Troubleshooting** tab shows the operating system's output after running diagnostic commands. Information on network interfaces, active routes, routing, and firewall rules can be inspected on the output display.

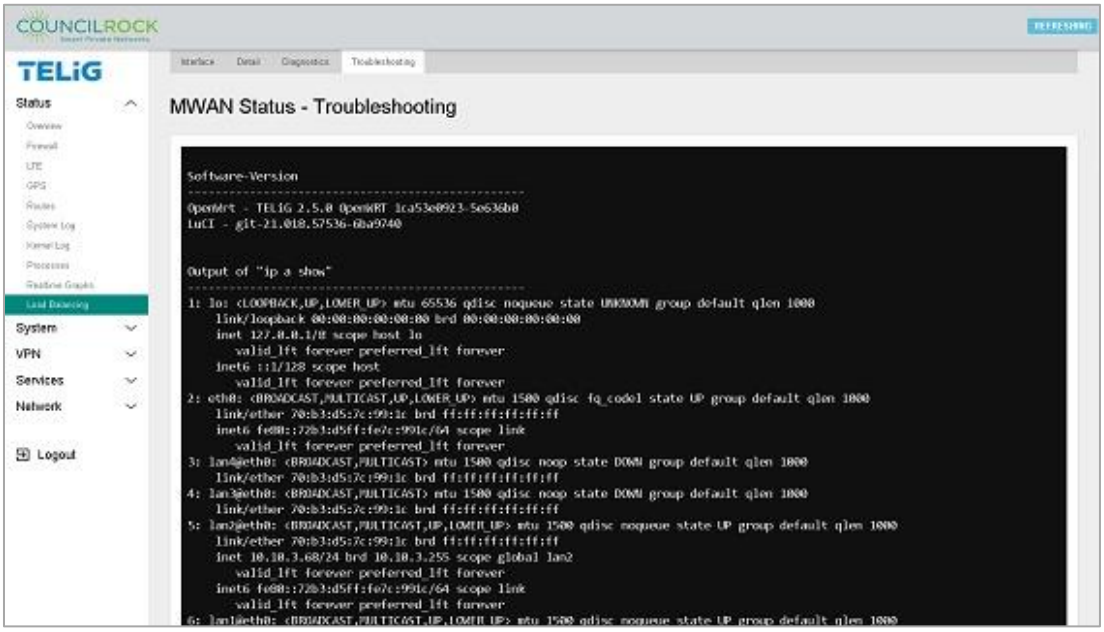

Figure 32: Status > Load Balancing > Troubleshooting

SYSTEM

System menus provide access to the unit's settings. Here the user can rename the unit and set the administrator password and time settings. Firmware backups/updates are handled here as well as installation and removal of software packages, system startup tasks and recurring tasks. LED status indicators can be configured, and serial port protocols can be set. Advanced users can configure and execute custom commands (shell commands) defined by an admin user. Finally, from the System menu the user can perform a soft reboot on the unit.

System

The **System** submenu provides access to overall unit settings. The **General Settings** tab lets the user set time, hostname, and time zone. The **Logging** tab has settings for the log buffer size, log output level, and log file save location. The **Language and Style** tab lets the user set the GUI theme and language.

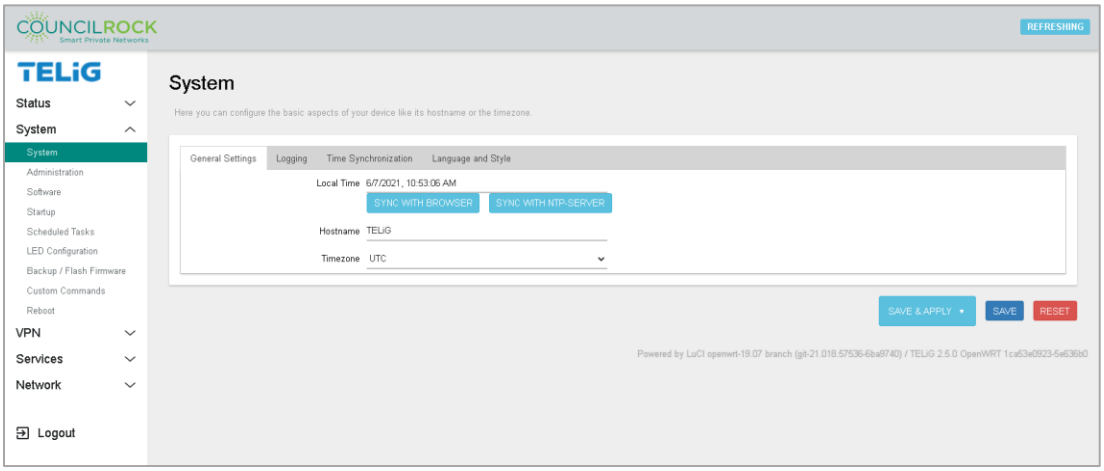

Figure 33: System > System > General Settings

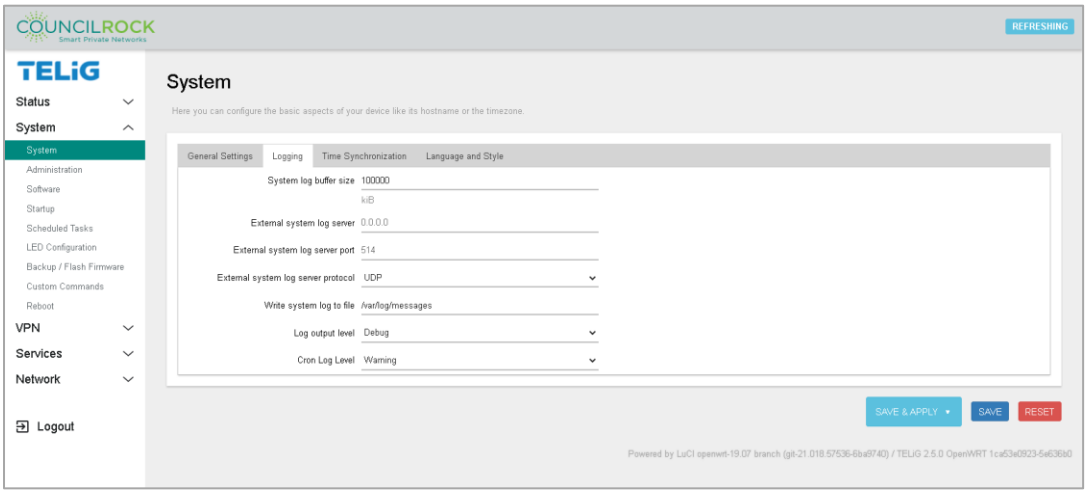

Figure 34: System > System > Logging

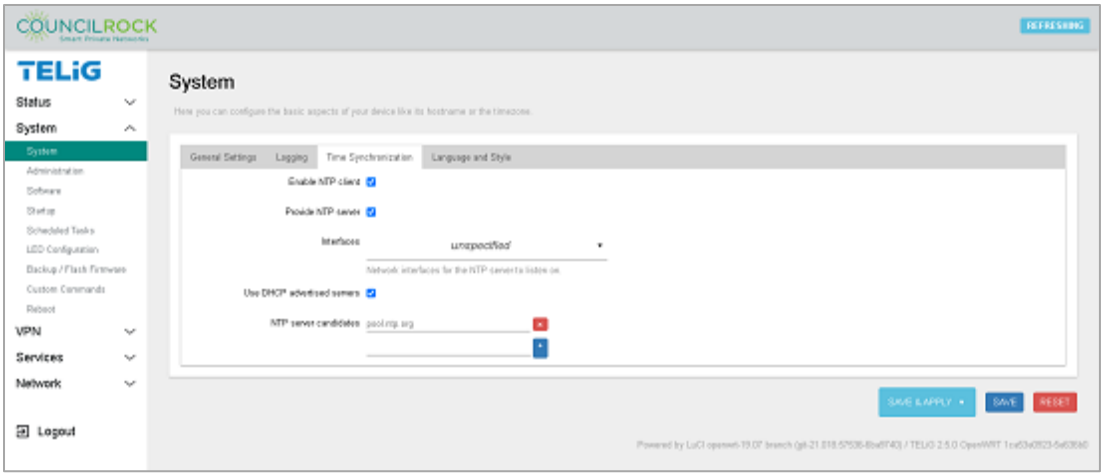

Figure 35: System > System > Time Synchronization

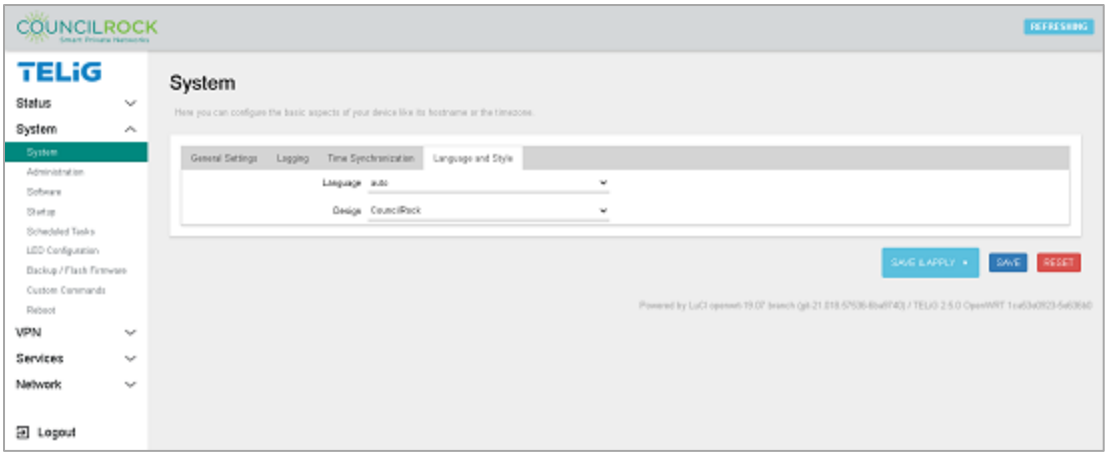

Figure 36: System > System > Language and Style

Usernames and passwords are configured in the **Administration** submenu.

The **Router Password** tab lets the user change the device's root password. The root user is currently the only user who can access the GUI. Future firmware revisions will allow other users to access the GUI.

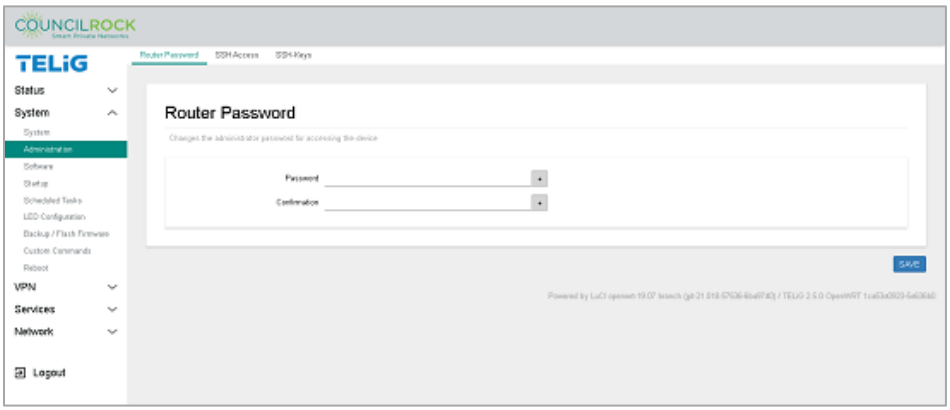

Figure 37: System > Administration > Router Password

The **SSH Access** tab lets the user enable or disable general users and/or the root user over SSH with password authentication. SSH can also be restricted via access to a specified interface & port.

When the "Password authentication" box is checked, *all users except 'root'* will have password authenticated access to the unit via SSH.
When the "Allow root login with password' box is checked, *only the 'root' user* will have password authenticated access via SSH.

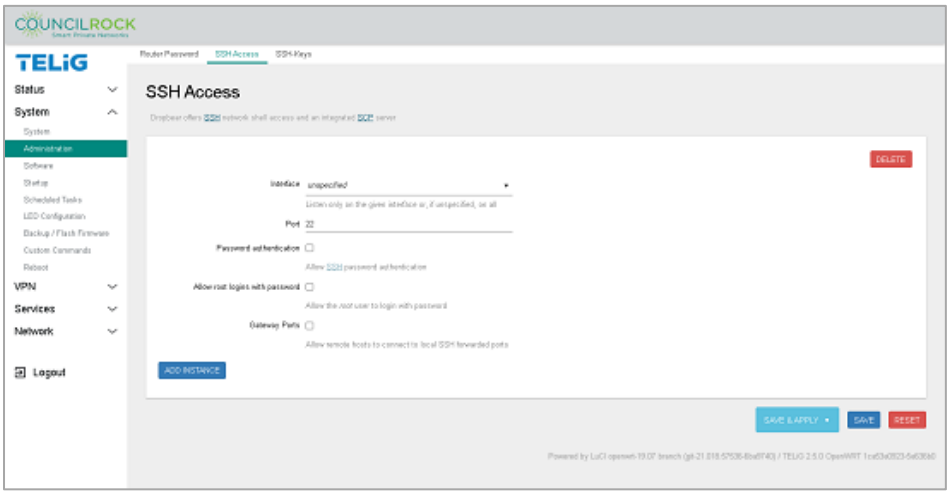

Figure 38: System > Administration > SSH Access

The **SSH-Keys** tab displays uploaded SSH public keys, and lets you upload an SSH public key to access SSH using public-private keypair authentication.

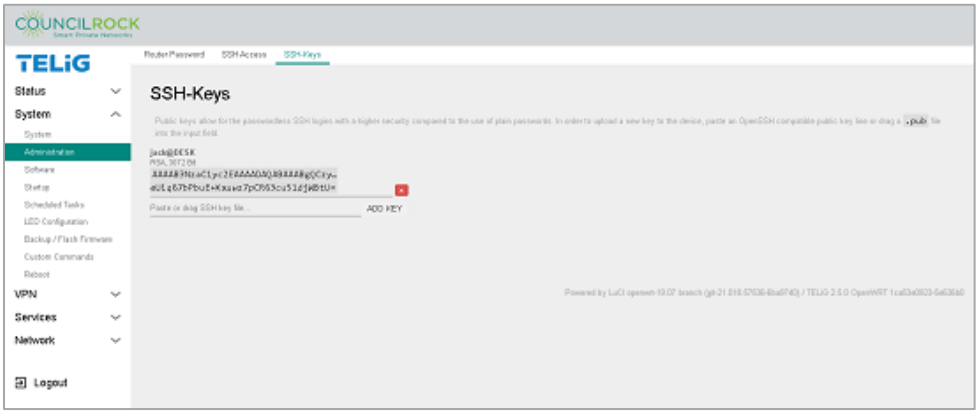

Figure 39: System > Administration > SSH-Keys

Software

Displays free space on the device, and allows the installation, removal, and updating of software packages. The **Available** tab shows packages available through the configured package manager. The **Installed** tab shows currently installed packages and allows for their removal. The **Updates** tab shows installed packages with available updates and lets the user update to the latest version.

> **Important:** Installing new packages is intended only for Advanced Users.

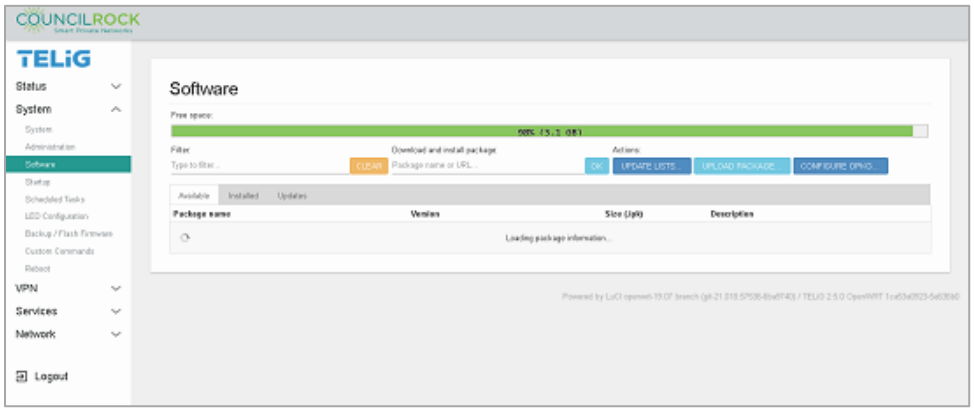

Figure 40: System > Software

To configure OPKG, click on the “Configure OPKG” option. The OPKG Configuration screen will pop up.

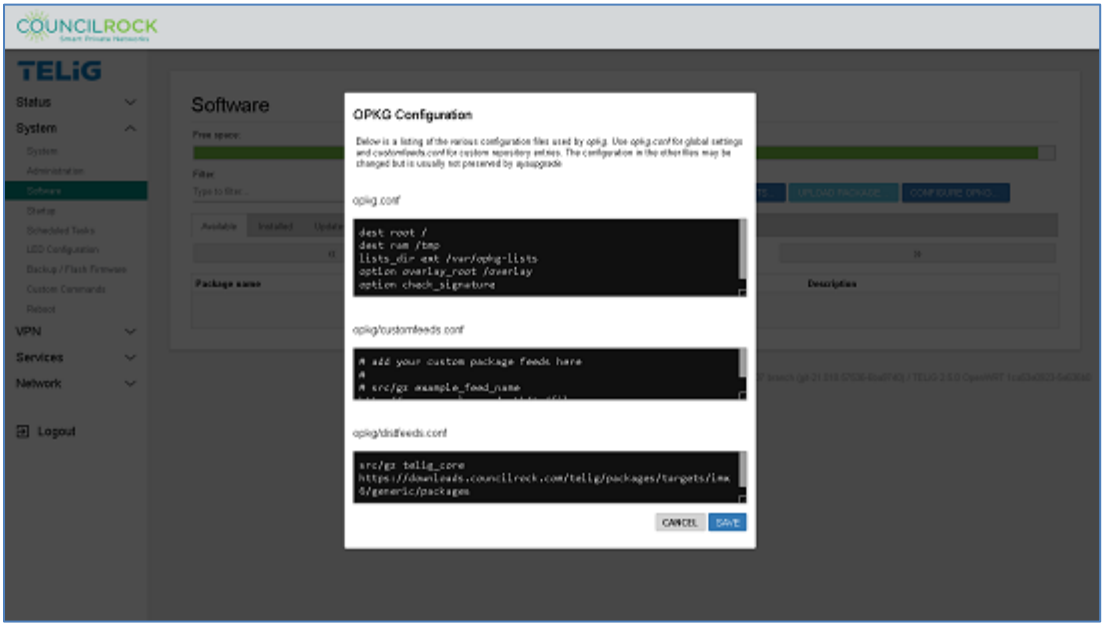

Figure 41: OPKG Configuration

On the OPKG configuration screen, go to the last section “opkg/disfeed.conf” and change the default repository to the desired repository where you are hosting the packages you would like to install. Click save after you are done.

Click the UPDATE LISTS button to show the available packages in the newly configured repository. After that point you can install new packages from the list by clicking the INSTALL... button and then clicking on INSTALL in the pop up window.

> ⚠ **Important:** *UPDATE LISTS triggers the unit to connect to a remote server to query availability of software packages. The unit must be configured with network visibility to this server prior to performing this action.*

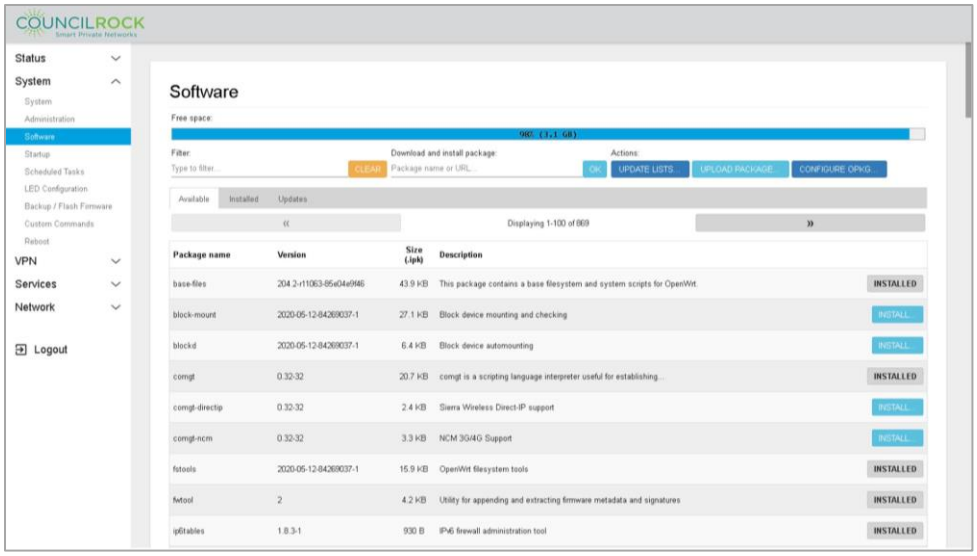

Figure 42: Install new packages.

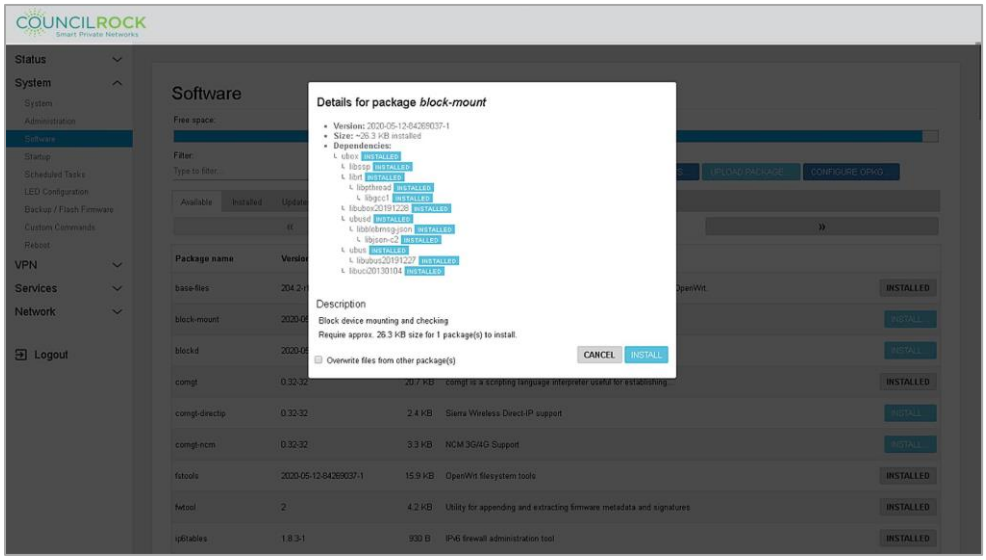

Figure 43: Detailed list of packages (example: block-mount)

Clicking INSTALL will show software details as in the example ‘block-mount’ package shown above. Software details including Version, Size, and Dependencies are displayed. A description of the software package is shown at the bottom. The option to overwrite files from other package(s) is selectable by a check box. From this dialog, the user can select CANCEL to go back or INSTALL to install the software package.

Startup

The **Startup** submenu lets the user configure startup and initialization programs.

The **Initscripts** tab displays a list of the available initialization scripts, their priorities, and whether they are enabled or disabled (for run on startup). You can also toggle the scripts between enabled and disabled, and manually start, restart, or stop a script.

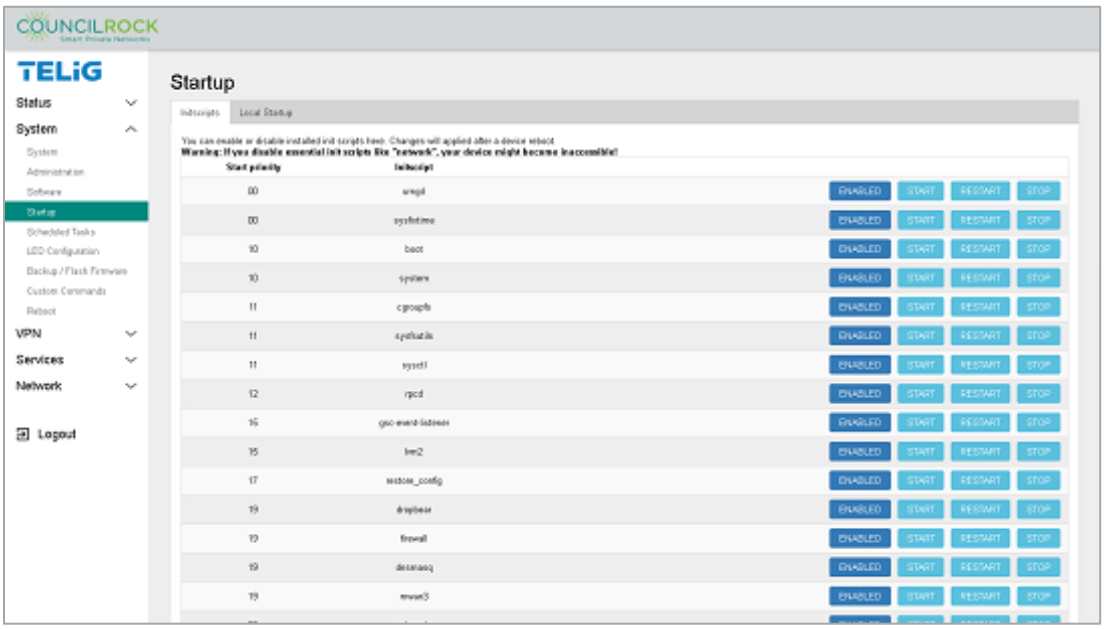

Figure 44: System > Startup > Initscripts

The **Local Startup** tab lets the user enter a custom shell script, to be executed after the enabled system initialization scripts listed on the **Initscripts** tab.

Figure 45: System > Startup > Local Startup

Important: *Custom Shell Scripting is intended only for Advanced Users.*

Scheduled Tasks

Here the user can set up "cron jobs" - recurring tasks which are configured to run on a set schedule.

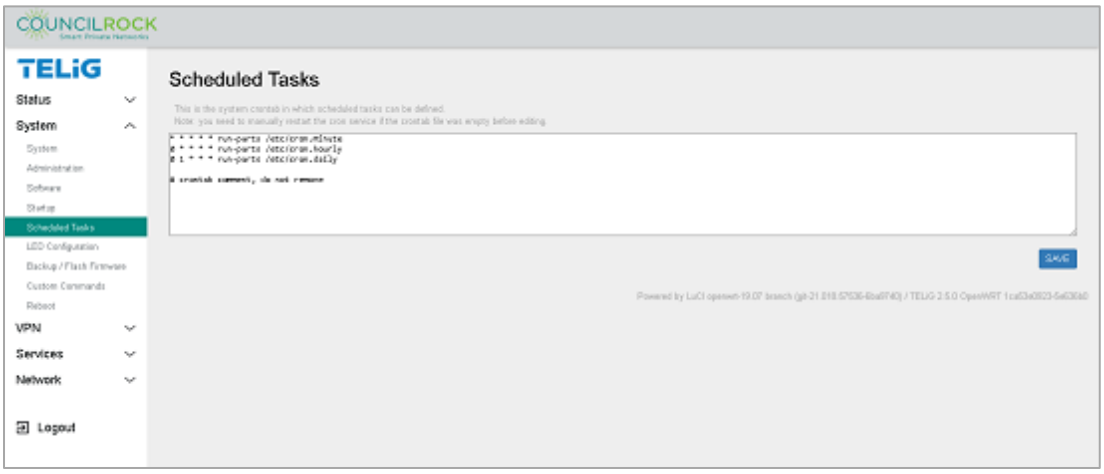

Figure 46: System > Scheduled Tasks

Important: *Cron Jobs are intended only for Advanced Users.*

LED Configuration

The status LED is a red/green LED that can be customized to the user's preferences.
The LED Configuration screen lists LED behaviors (actions) and lets the user edit, delete, and reorder them.

Important: LED configurations are overridden by LTE status indicators. If the E1500 unit has an active LTE interface, the LED actions shown on this screen will not apply. See Table 1 for LTE status indicators.

Since the status LED contains a green and a red LED, each color can be configured to its own action. For maximum clarity, a simple green 'always on' power indicator is typical. Multiple actions can be configured but for simplicity we recommend no more than a one-to-one mapping of a color to an action (maximum of two actions in the list).

A new LED action can be added by clicking "**Add LED Action** ". To edit an existing action, click "**EDIT**." Whether adding a new action or editing an existing action, the input fields are the same:

Name: Label the action. For clarity, we suggest *"LED Color - action name"*
LED Name: select "user1" for Green, "user2" for Red.
Default state: check = on, no check = off
Trigger: selected from the dropdown list

LED triggers are selected from the following options:

defaulton - Always ON
Heartbeat - Flash to simulate a heartbeat
mmc0 - ON when SD card is accessed.
netdev - Flash with link status / send & receive activity
requires additional selections for **device** (from a dropdown list) and **Trigger Mode** (Link / Transmit / Receive - multiple selections allowed)
none - Always OFF
timer - Blinks at a specified rate
Specify On-State Delay and Off-State delay in milliseconds. For example, to turn the LED on for one second and blink off for a half-second, On-State Delay = 1000 and Off-State Delay = 500
usbdev / usbport - ON when a specified USB device or port is connected
usbdev / usbport requires selecting a USB device or port from the dropdown

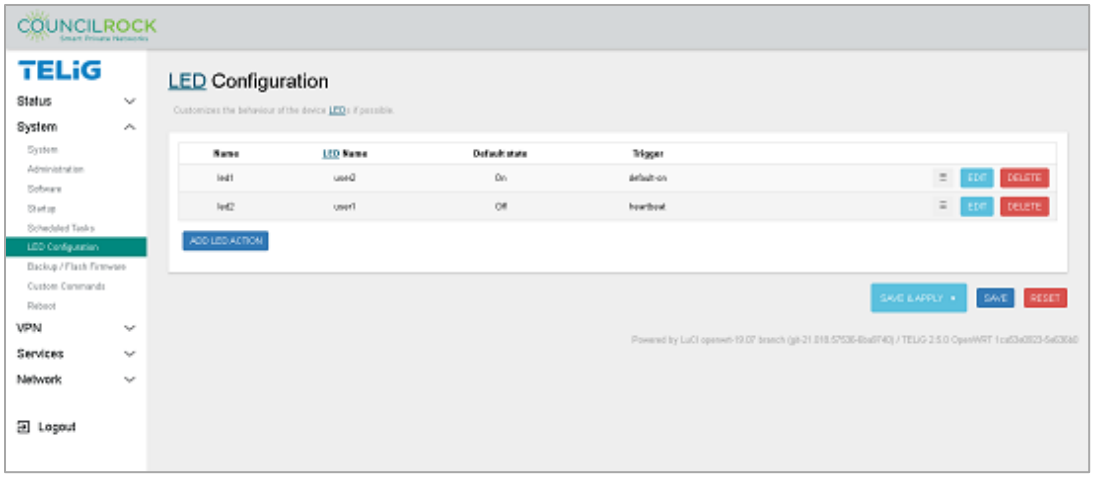

Figure 47: System > LED Configuration

The example configuration shown above is set up for a green 'always on' power indicator with a simultaneous red LAN1 send/receive indicator. Note that the red LED in this example will act the same as the existing ethernet port LED - and therefore is not a recommended LED action based on the rule of thumb of simplicity.

"Netdev" trigger settings for the red LED action are seen below.

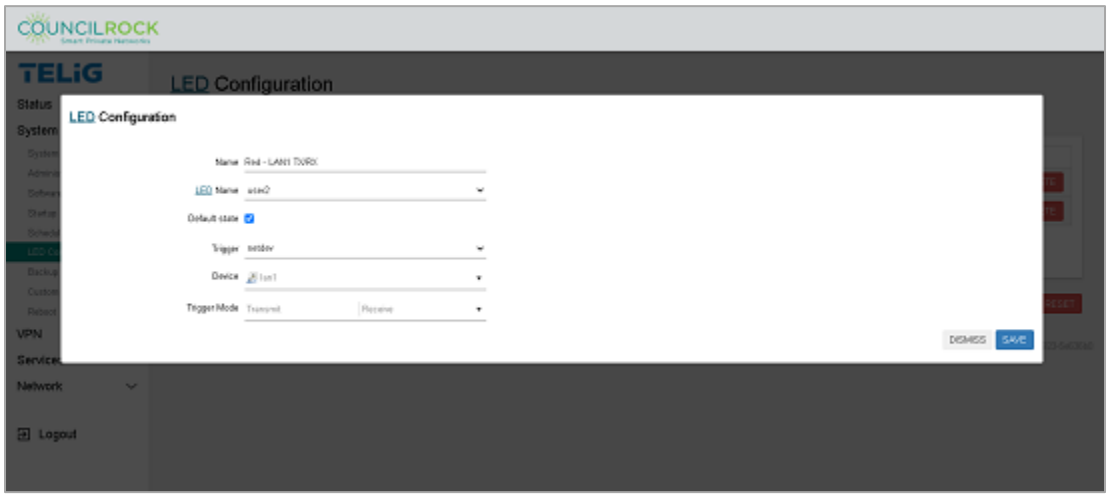

Figure 48: System > LED Configuration: netdev example

Backup / Flash Firmware

This menu gives access to the unit firmware.

The **Action** tab lets the user backup and restore firmware.

- GENERATE ARCHIVE: download a backup archive to your computer
- PERFORM RESET: reset the unit back to default settings (factory reset)
- UPLOAD ARCHIVE: upload a backup saved on your computer to the unit
- Choose mtdblock / SAVE MTDBLOCK: download backup partition info (do not use unless you are familiar with mtdblocks)
- FLASH IMAGE: manually flash a firmware update

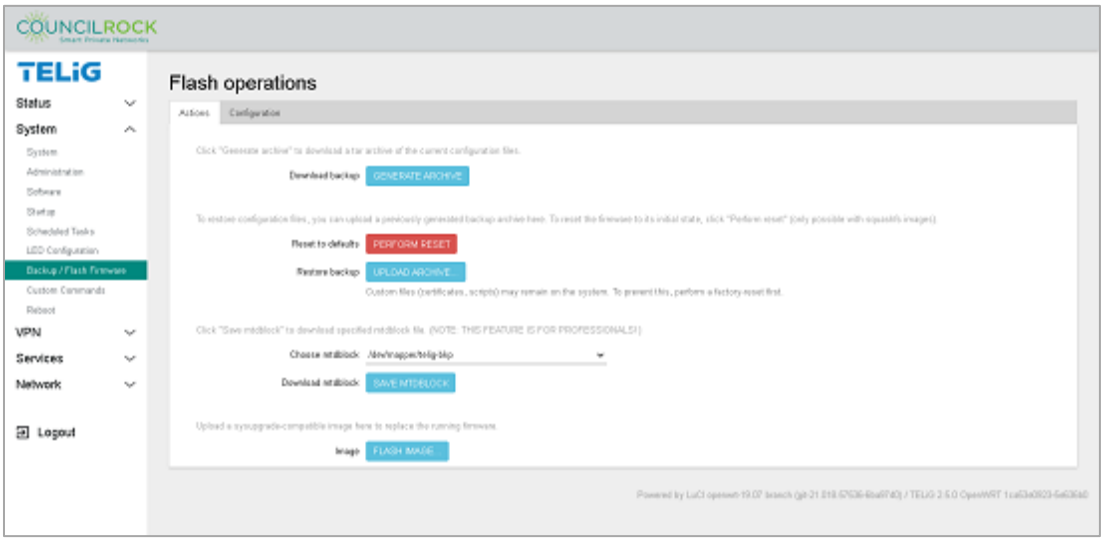

Figure 49: System > Backup/Flash Firmware: Actions

> ⚠ **Warning:** mtdblocks (discussed above) is a Linux method of interacting with Flash memory via a simple Flash Transition Layer (FTL) within a Linux Memory Technology Device (MTD) subsystem. Use of mtdblocks is recommended only for advanced users familiar with this Linux concept.

The **Configuration** tab gives the user the option to specify files and directories to be preserved when flashing new firmware.

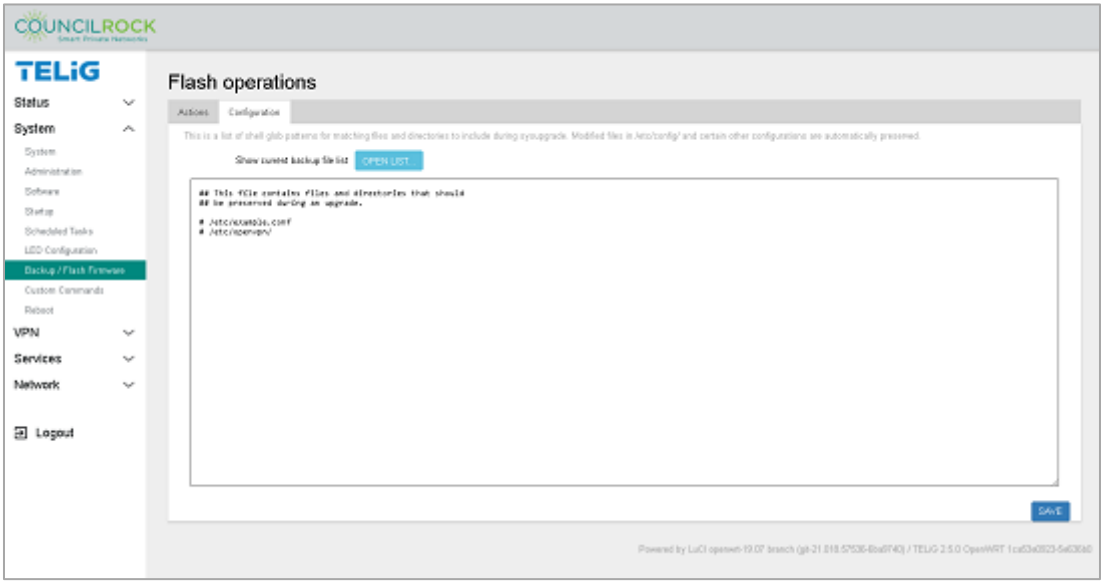

Figure 50: System > Backup/Flash Firmware: Configuration

Custom Commands

Allows for setup and execution of custom commands. These can be any applicable Linux command typically run from a command line interface. As such, these commands should only be performed by an advanced user.

The **Dashboard** tab displays currently configured custom commands and provides a button to run the command. Clicking RUN will display the command output at the bottom of the page when the command has completed.

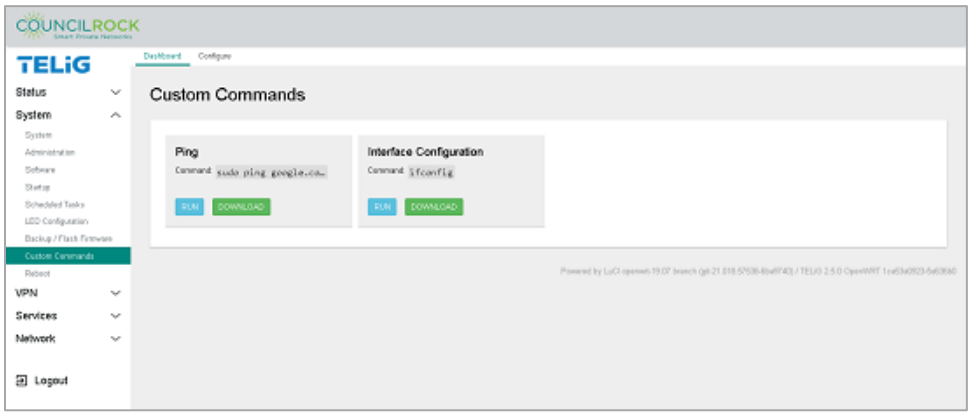

Figure 51: System > Custom Commands > Dashboard

NOTE: commands shown are provided as examples. A new unit will not have custom commands set up.

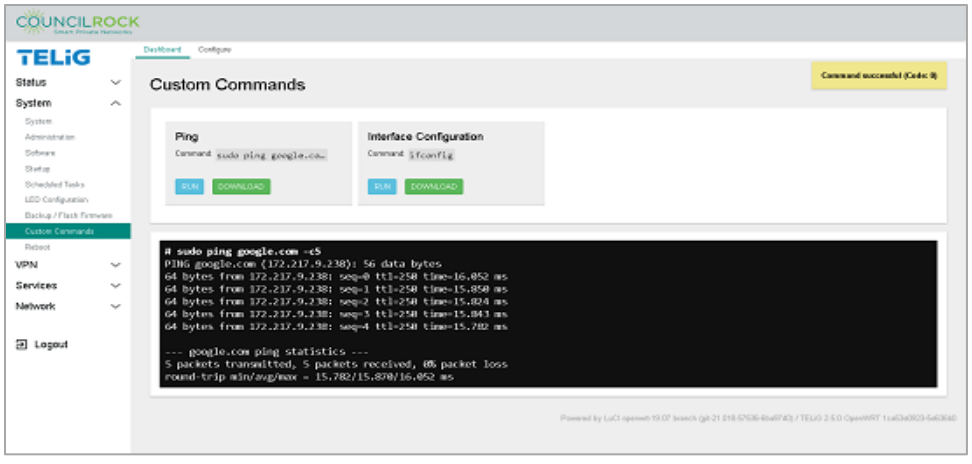

Figure 52: System > Custom Commands > Dashboard
Showing results of 'sudo ping google.com -c5' command

The **Configure** tab lets the user add new custom commands and edit and delete existing ones.

> **Warning:** *Custom Commands are intended only for Advanced Users.*

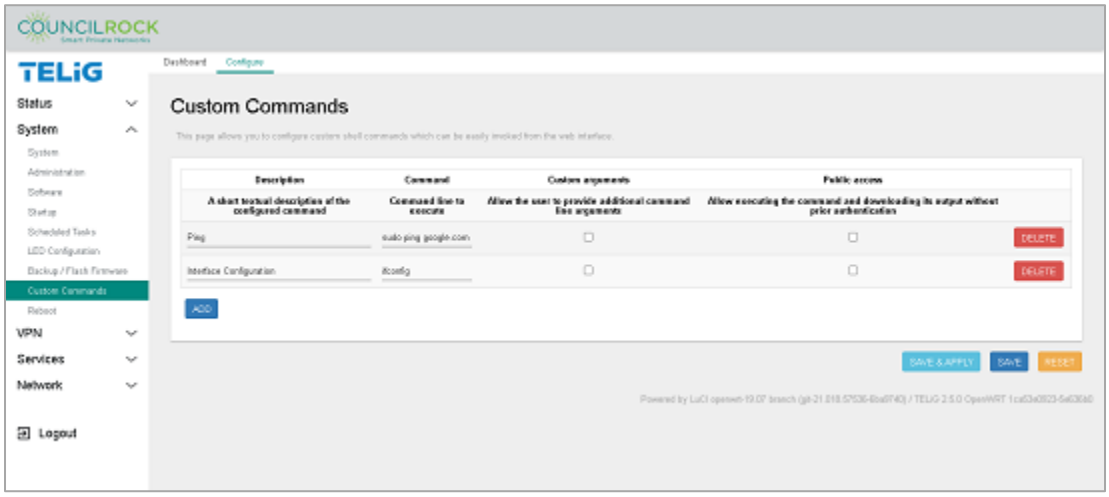

Figure 53: System > Custom Commands > Configure

Reboot

Lets the user perform a Reboot. This is a soft reboot, which restarts the unit and all components without removing power.

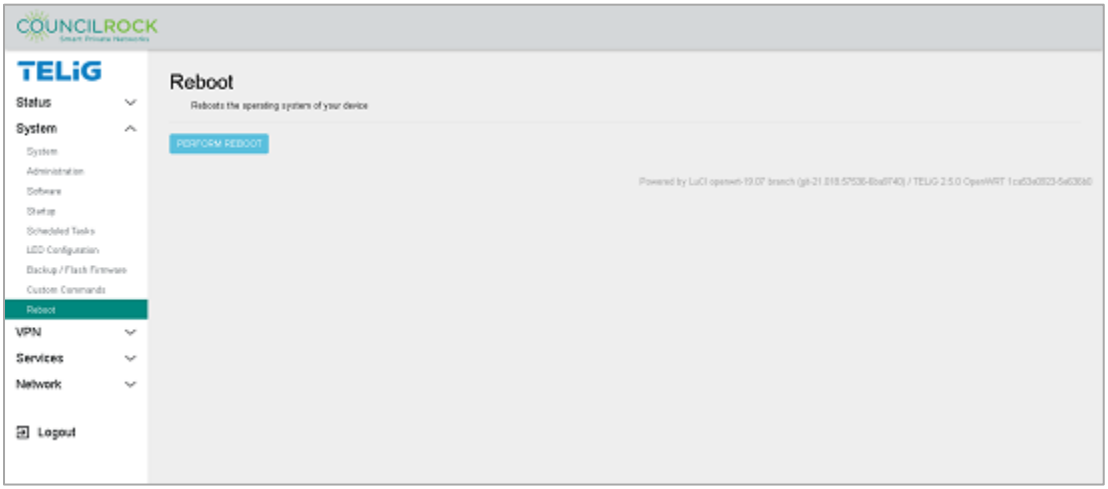

Figure 54: System > Reboot

VPN

The VPN menu lets the user configure Virtual Private Network (VPN) settings using IPSec and OpenVPN. For details on these see two VPN options see https://openvpn.net/ and https://www.strongswan.org/.

IPSec

Under IPSec there are two main tabs. **Status** shows the status of all active IPSec configurations, and **Config** lets the user configure IPSec Connections, Tunnels, and Ciphers.

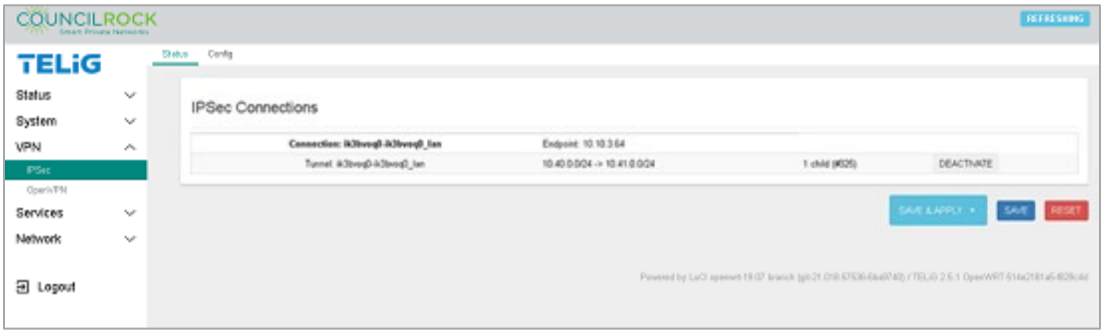

Figure 55: VPN > IPSec: Status

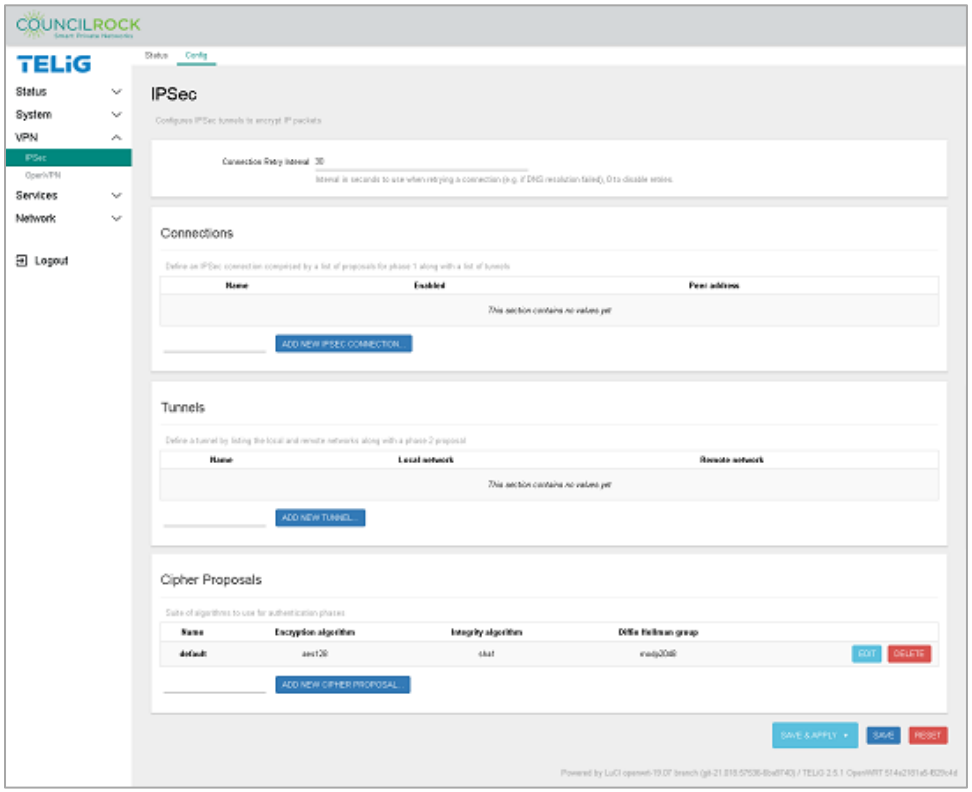

Figure 56: VPN > IPSec: Config

NOTE: *VPN > IPSec: Configure* window is the same as the main IPSec window

IPSec is a secure network protocol for encrypting communications between two points, the client and server. To create a configuration there are three steps:

1. define the cipher proposal for authentication (ADD NEW CIPHER PROPOSAL)
2. define the tunnel parameters for encryption (ADD NEW TUNNEL)
3. create the vpn session (ADD NEW IPSEC CONNECTION)

In the cipher proposal window, the suite of algorithms to use for authentication phases parameters are defined: the encryption algorithm, the integrity algorithm and the Diffie Hellman group. Supported options are listed in the drop-down menus.

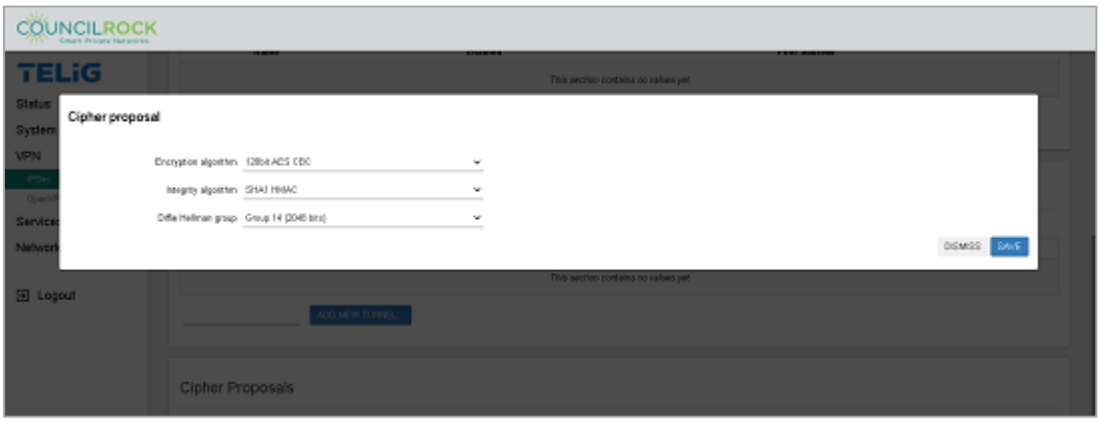

Figure 57: IPSec Cipher proposal

In the Tunnels configuration window, the next set of parameters define the local and remote networks along with a phase 2 proposal. These settings define the networks of the two ends of the tunnel, and the authentication method is selected (pre-shared key or X.509 certificates).

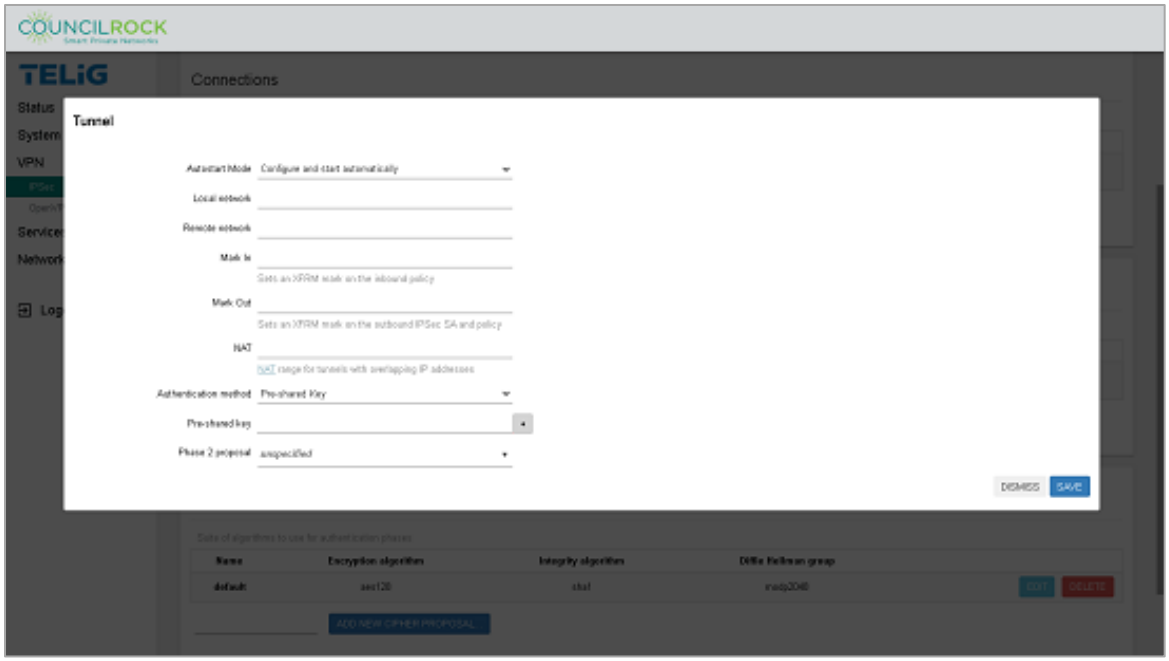

Figure 58: IPSec Tunnel configuration

The last step in setting up a VPN with IPSec encryption is defined in the Connections window. Here, peer network information (detailing the other end of the VPN tunnel) is entered, and the Cipher (Phase 1) Proposal and Tunnel are selected.

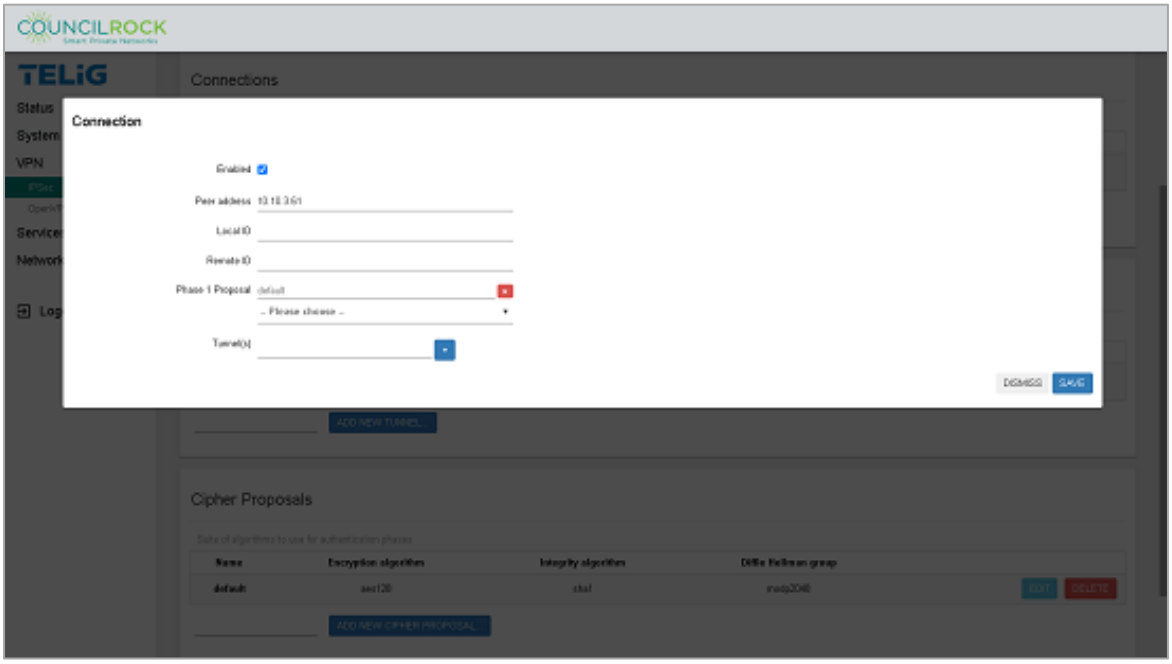

Figure 59: IPSec Connection configuration

OpenVPN

OpenVPN is an open-source VPN protocol that executes virtual private network (VPN) techniques for producing safe site-to-site or point-to-point connections in remote access facilities and bridged or routed configurations.

The OpenVPN menu displays a list of configured VPNs and their current states and allows the user to enable, start/stop, add, edit, or delete VPNs.

Create a new configuration with the *Template-based configuration* dialog by giving the new configuration a name, selecting a template, and clicking **ADD.** The new configuration appears in the *OpenVPN Instances* list and can be edited by clicking **EDIT.**

OpenVPN Templates provided are:

- **Client configuration for an ethernet bridge VPN** populates basic settings for a client VPN session where the IP network of the server will be extended to the tunnel interface assigned to this VPN session. The kernel virtual network device is set to TAP which is an Ethernet level (layer 2) and acts like a switch.
- **Client configuration for a routed multi-client VPN** populates basic settings for a client VPN session where the kernel virtual network device is set to TUN, which works at network level (layer 3) and routes packets on the VPN
- **Simple client configuration for a routed point-to-point VPN** populates basic settings to set a TUN kernel network device to create a client VPN connection to connect to a server in a point to point configuration. Traffic needs to be routed by the server and the client independently.
- **Server configuration for an ethernet bridge VPN** populates basic configuration to setup a server to allow clients to connect setting the kernel network device to TAP.
- **Server configuration for a routed multi-client VPN** populates basic configuration to setup a server to allow clients to connect setting the kernel network device to TUN. The clients get network configuration settings and routes from the server
- **Simple server configuration for a routed point-to-point VPN** populates basic configuration settings to set the E1500 as a server VPN configuration to connect to only one client. The kernel network device is set to TUN.

Configuration files for these templates are shown below:

```
#
# Ethernet bridge client
#
config openvpn_recipe client_tun
	option _description	"Client configuration for an ethernet bridge VPN"
	option _role		"client"
	option client		"1"
	option dev		"tap"
	option remote		"vpnserver.example.org 1194"
	option ca			"ca.crt"
	option cert		"my_client.crt"
	option key		"my_client.key"
	option dh			"dh1024.pem"
	option ns_cert_type	"server"
	option keepalive		"10 120"
	option comp_lzo		"1"
	option nobind		"1"
```

```
#
# Routed client
#
config openvpn_recipe client_tun
	option _description	"Client configuration for a routed multi-client VPN"
	option _role		"client"
	option client		"1"
	option dev		"tun"
	option remote		"vpnserver.example.org 1194"
	option ca			"ca.crt"
	option cert		"my_client.crt"
	option key		"my_client.key"
	option dh			"dh1024.pem"
	option ns_cert_type	"server"
	option keepalive		"10 120"
	option comp_lzo		"1"
	option nobind		"1"
```

```
#
# Routed point-to-point client
#
config openvpn_recipe client_tun_ptp
	option _description	"Simple client configuration for a routed point-to-point VPN"
	option _role		"client"
	option dev			"tun"
	option remote		"mypeer.dyndns.org"
	option port		"1194"
	option ifconfig		"10.0.0.2 10.0.0.1"
	option secret		"shared-secret.key"
	option nobind		"1"
```

```
#
# Multi-client ethernet bridge server
#
config openvpn_recipe server_tun
	option _description		"Server configuration for an ethernet bridge VPN"
	option _role			"server"
	option dev				"tap"
	option port			"1194"
	option server_bridge		"192.168.1.1 255.255.255.0 192.168.1.128
192.168.1.254"
	option ca				"ca.crt"
	option cert			"server.crt"
	option key			"server.key"
	option dh				"dh1024.pem"
	option client_to_client	"1"
	option keepalive			"10 120"
	option comp_lzo			"1"
```

```
#
# Routed multi-client server
#
config openvpn_recipe server_tun
	option _description			"Server configuration for a routed multi-client VPN"
	option _role				"server"
	option dev					"tun"
	option port				"1194"
	option server				"10.0.100.0 255.255.255.0"
	option ca					"ca.crt"
	option cert				"server.crt"
	option key				"server.key"
	option dh					"dh1024.pem"
	option client_to_client	"1"
	option keepalive				"10 120"
	option comp_lzo			"1"
```

```
#
# Routed point-to-point server
#
config openvpn_recipe server_tun_ptp
	option _description		"Simple server configuration for a routed point-to-point VPN"
	option _role			"server"
	option dev				"tun"
	option port			"1194"
	option ifconfig			"10.0.0.1 10.0.0.2"
	option secret			"shared-secret.key"
```

New VPNs can be uploaded from an OpenVPN configuration file, or by using one of the provided VPN templates. Note that when using template configuration, the user must edit the VPN after creation to provide the required information. However, this option is only for client configurations.

Use the “OVPN configuration file upload” dialog to name the new configuration and click **UPLOAD**. The new configuration appears in the table.

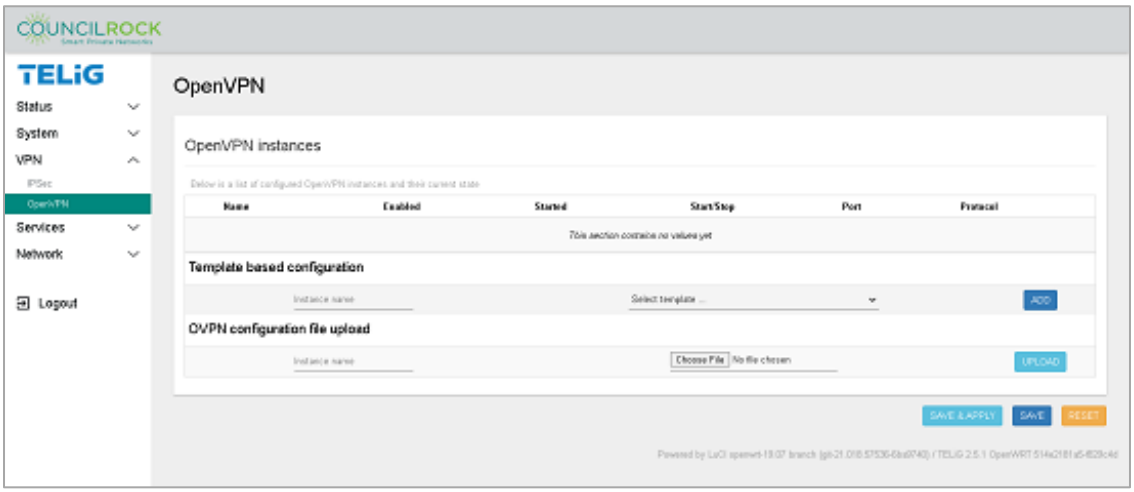

Figure 60: VPN > OpenVPN

SERVICES

The Services submenus give access to the following settings:

- Serial Gateway - Includes drop down options for Gateway types:
    - Distributed Network Protocol (DNP3) Gateways
    - Modbus Gateways - Modbus is a standard industrial Programmable Logic Controller (PLC) communication protocol over a serial interface.
- SNMPD - Simple Network Management Protocol (SNMP) is an Internet Standard protocol for device management over IP networks. SNMPD is the Linux-based SNMP agent that binds to a port and listens for requests from SNMP management software.

Serial Gateways

Allows the user to set the serial communication protocol for the Serial A interface. The protocols supported by this interface are RS232, RS485 Half Duplex, and RS422/RS485 Full Duplex. The table below shows a basic comparison between these three protocols.

	RS232	RS485	RS422
Max number of devices	1	32	10
Modes of operation	half duplex	half duplex	full duplex
	full duplex		
Network topology	point-to-point	multipoint	multipoint
Max distance (acc. standard)	50ft	4000ft	4000ft
Max speed at 50 ft	20 kbs	35 Mbs	10 Mbs
Max speed at 4000 ft	(1 kbs)	100 kbs	100 kbs

Table 6: Serial Configuration

The Serial B interface only supports the RS232 protocol.

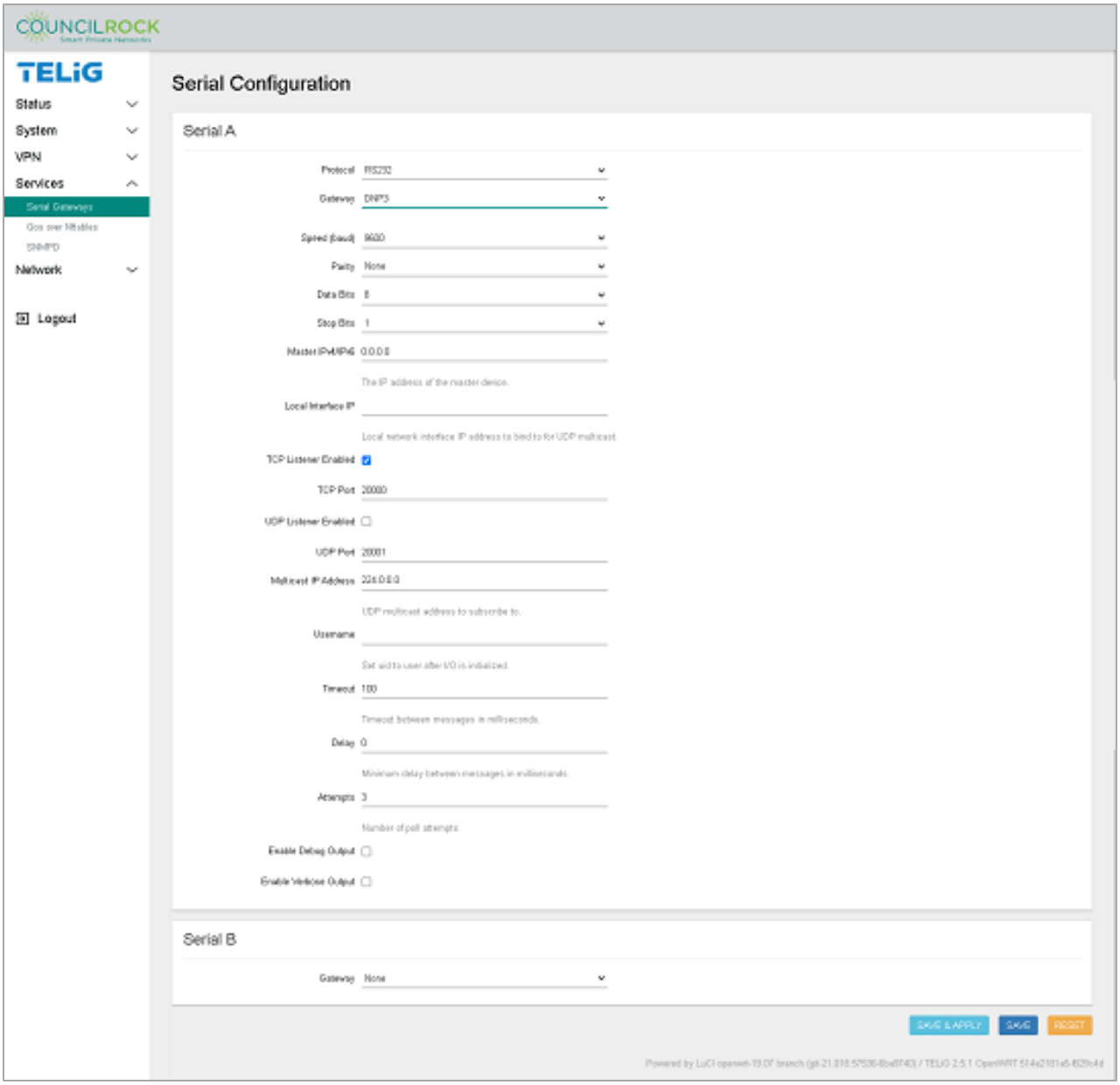

Figure 61: Services > Serial Configuration

QoS over Nftables (Quality of Service)

This menu controls QoS at the packet level. It lets the user set Upload and Download Rate Limits to prioritize network traffic for each system interface. Rate Limits can be created to match traffic based on source IP address. Existing classification rules can be edited or deleted.

NFT-QoS Settings > Limit Rate contains settings for Download and Upload rate limits. Select the *Limit Enable* checkbox. By selecting *Limit Type: Static*, the user can set default DL/UL limit rates in bytes/s, Kbytes/s, or Mbytes/s. By selecting *Limit Type: Dynamic*, the user can set default DL/UL bandwidth limits in Mbps across a specified target Network using IPv4 or IPv6 addresses in CIDR notation. Individual IP address(es) can be added to a whitelist to bypass default limit rates when using either Limit Type by entering a whitelisted address and clicking the '+' button.

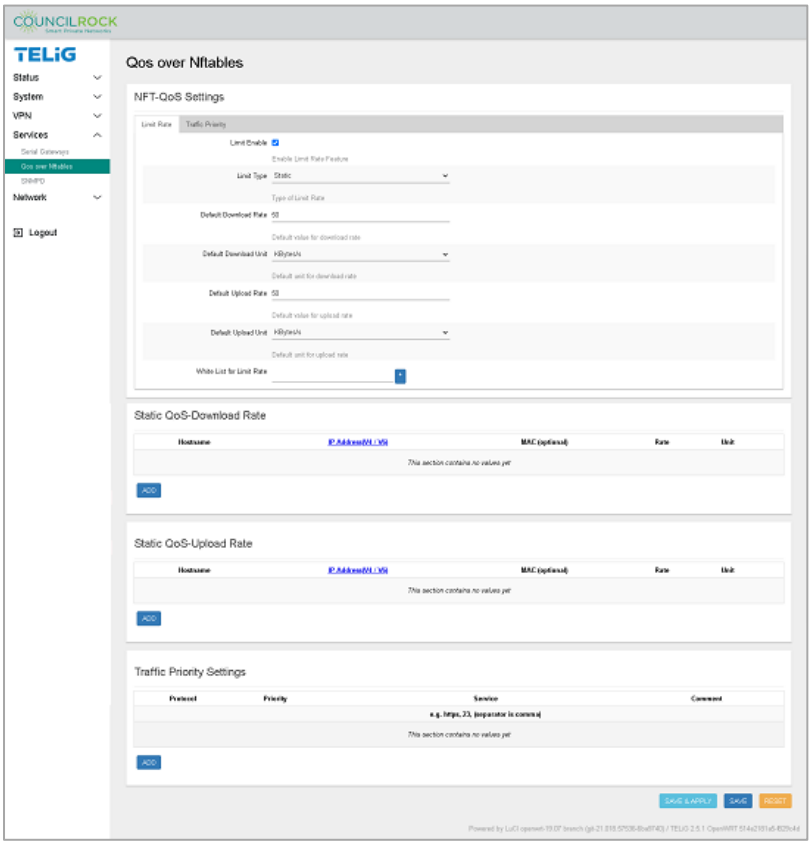

Figure 62: Services > QoS over Nftables > Limit Rate

NFT-QoS Settings > Traffic Priority contains the interface selector for which QoS Traffic Priorities can be configured. Select the *Enable Traffic Priority* checkbox. Select the *Default Network Interface* from the dropdown.
If the *Traffic Priority Settings* section is not visible, click *Save & Apply*. Continue to *Traffic Priority Settings*.

Static QoS-Download Rate / Static QoS-Upload Rate sections are configurable when the Limit Rate is enabled. These sections allow the user to set Download / Upload rates for specific IP address(es). Click the *ADD* button and enter each hostname, IP address, MAC (optional) and Limit Rates in bytes/sec, Kbytes/sec, or Mbytes/sec. These Static QoS Rates are configurable in either Limit Type: Static or Limit Type: Dynamic (described in the Limit Rate settings above).

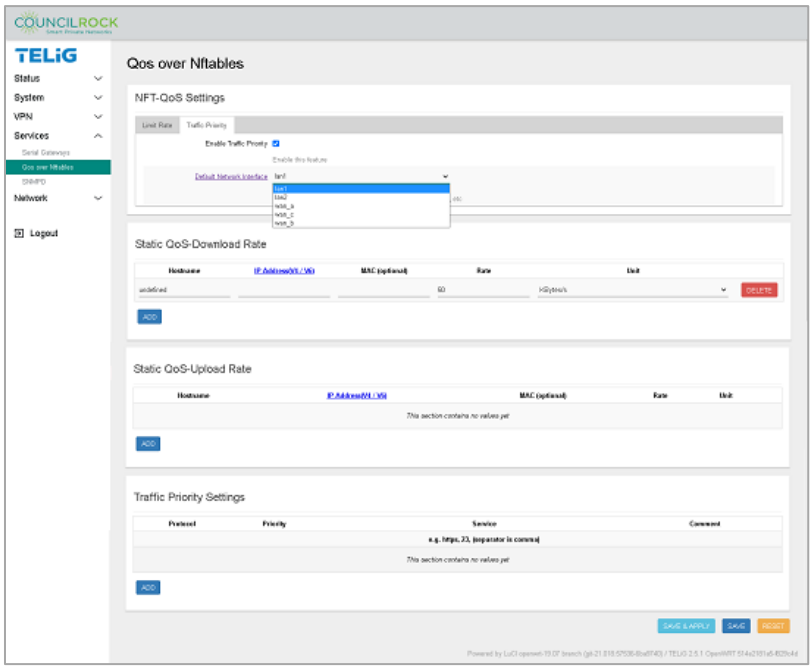

Figure 63: Services > QoS over Nftables > Traffic Priority

Traffic Priority Settings section lets the user configure traffic priority by protocol and service. Click the ADD button and select a protocol (TCP, UDP, UDP-Lite, SCTP, or DCCP), priority (1 is highest), service (telnet, http, https, or a port number – multiple entries are possible, separated by a comma), and an optional comment. For multiple protocols, click the ADD button and repeat as needed. Click *Save & Apply*.

NOTE: When *Limit Enable* and/or *Enable Traffic Priority* are disabled, the corresponding Static Rates and/or Traffic Priority settings are not displayed until after clicking *Save & Apply*. Likewise, if *Limit Enable* and/or *Enable Traffic Priority* are enabled, their corresponding settings will not appear in the display until after clicking *Save & Apply*. If either option is disabled and later re-enabled, any settings the user has previously configured will be available as previously configured.

SNMPD

This menu provides Simple Network Management Protocol (SNMP) configuration via SNMP agents, SNMP traps, and SNMP informs, to manage the device over the network. SNMP is implemented via the Linux daemon net-snmpd. For more information on configuring SNMPD, see http://net-snmp.sourceforge.net/wiki/index.php/Snmpd.

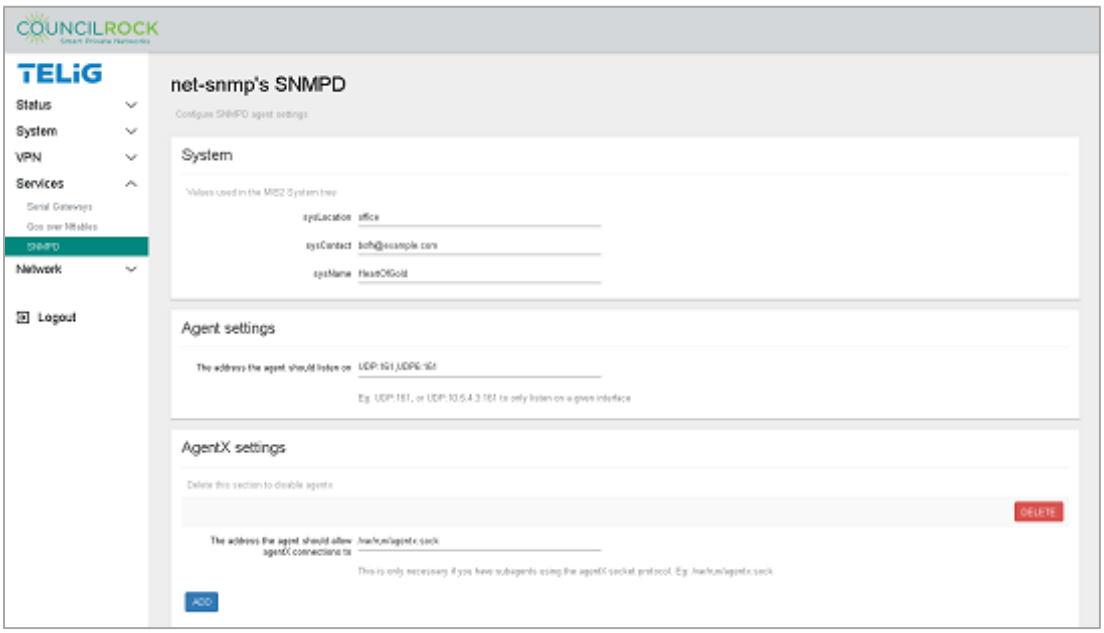

Figure 64: Services > SNMPD

NETWORK

Interfaces

Displays information on and allows the configuration of the unit's network interfaces. Each interface is listed with information including protocol, uptime, MAC address, transmitted and received data, and IPv4/IPV6 address and netmask (if applicable). The user can add / edit / delete interfaces and stop or restart active interfaces.

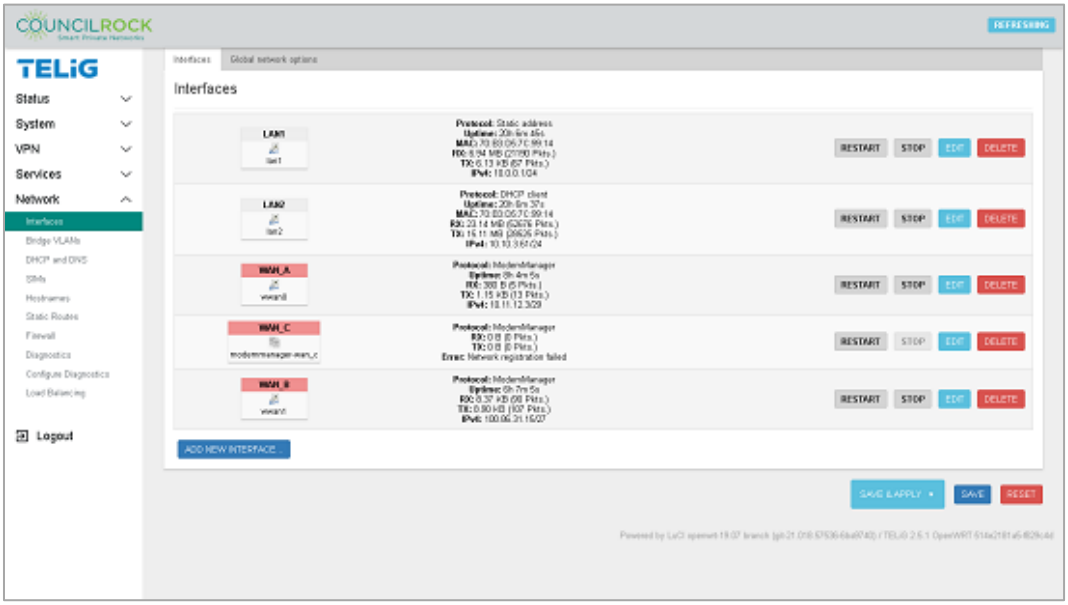

Figure 65: Network > Interfaces

To add interfaces, enter a name, select a protocol, and select the physical interface (multiple interfaces if bridging). Additional options can be accessed by editing the interface once created, such as the protocol to use and whether to bring up the interface automatically on boot.

Available Options on the Interface editing dialogue vary depending on the selected protocol.

Example 1:
Static Address protocol

In the General Settings tab:
- Set static IPv4 address, netmask, gateway, and broadcast address
- Add custom DNS servers
- Set static IPv6 address gateway, assignment length routed prefix, and suffix

In the Advanced Settings tab:
- Select builtin IPv6 management
- Select / deselect force the link
- Set MAC address / MTU overrides
- Set a custom gateway metric.

On the Physical Settings tab,
- Select physical interface bridging
- Select physical interface (or interfaces,
- If Bridging is enabled
  - enable/disable STP and IGMP snooping.

Static Access protocol gives access to *DHCP Server* menus

Example 1a: DHCP Server on Static Address

On the DHCP Server tab:
- Enable the wireless interface's DHCP server.

Once DHCP is enabled, additional options are displayed for General / Advanced settings / IPv6.

On the General Settings tab:
- Network address offset for start of leased addresses
- Maximum number of leases
- Lease time

On the Advanced Settings tab:
- Dynamic allocation of DHCP leases (as opposed to static leases),
- Force running the DHCP server, even if another server is detected on the network
- Override the IPv4 netmask
- Set DHCP options.

On the IPv6 tab:
- Router advertisement service mode
- DHCPv6 service
- NDP proxy
- DNS servers and DNS addresses to announce

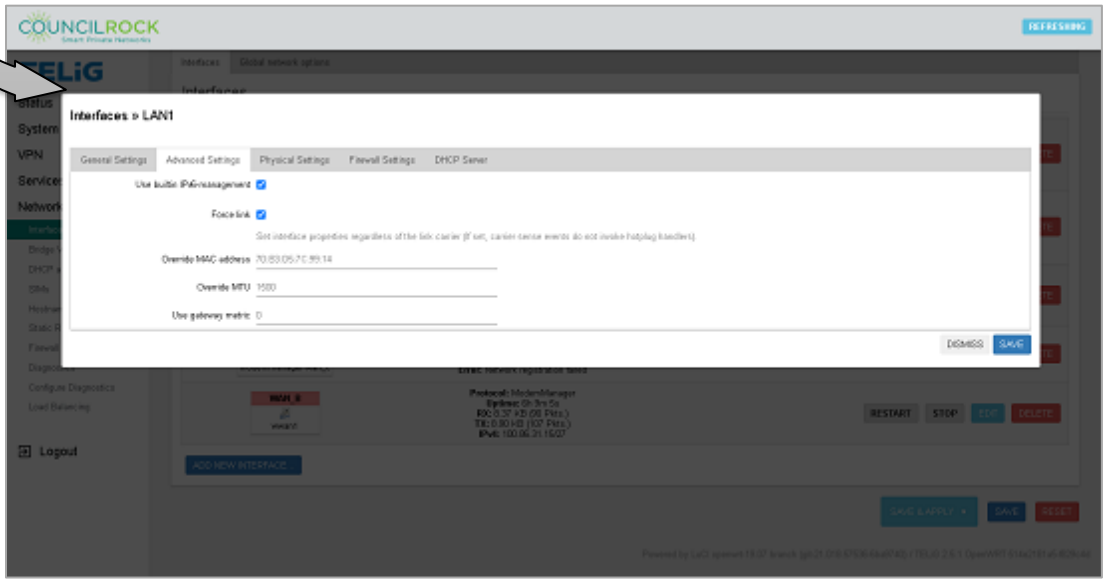

Figure 66: Interfaces > Advanced Settings

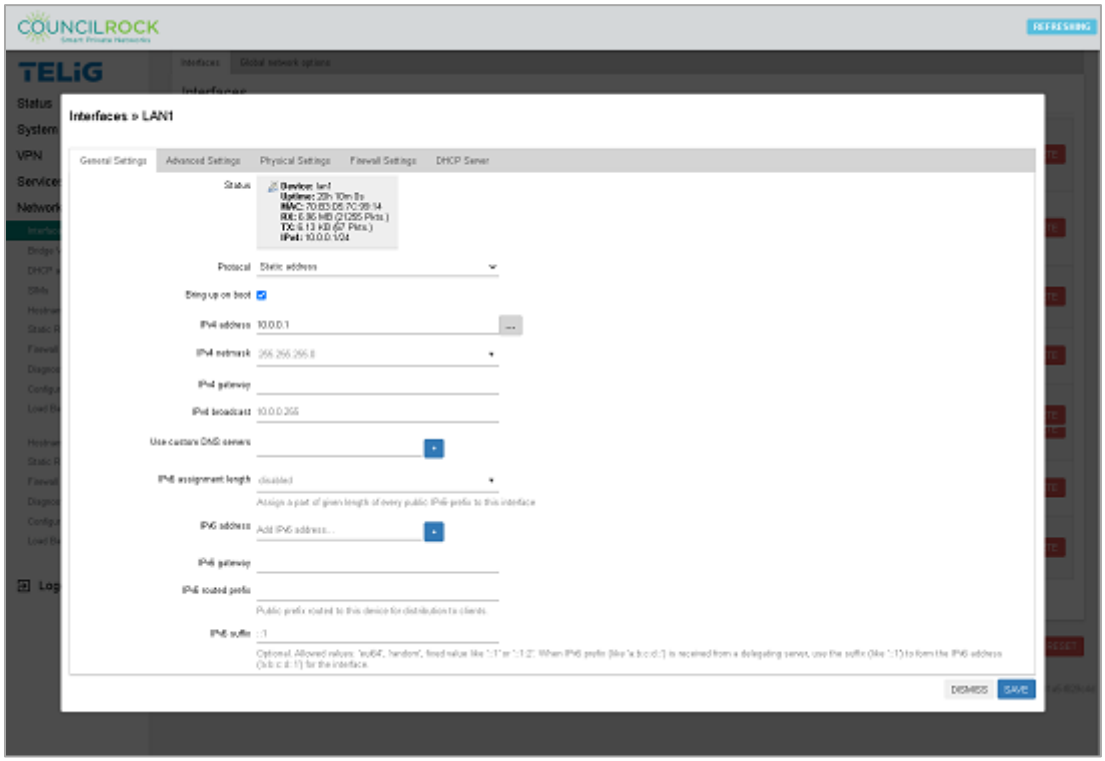

Figure 67: Interfaces > LANx > General Settings

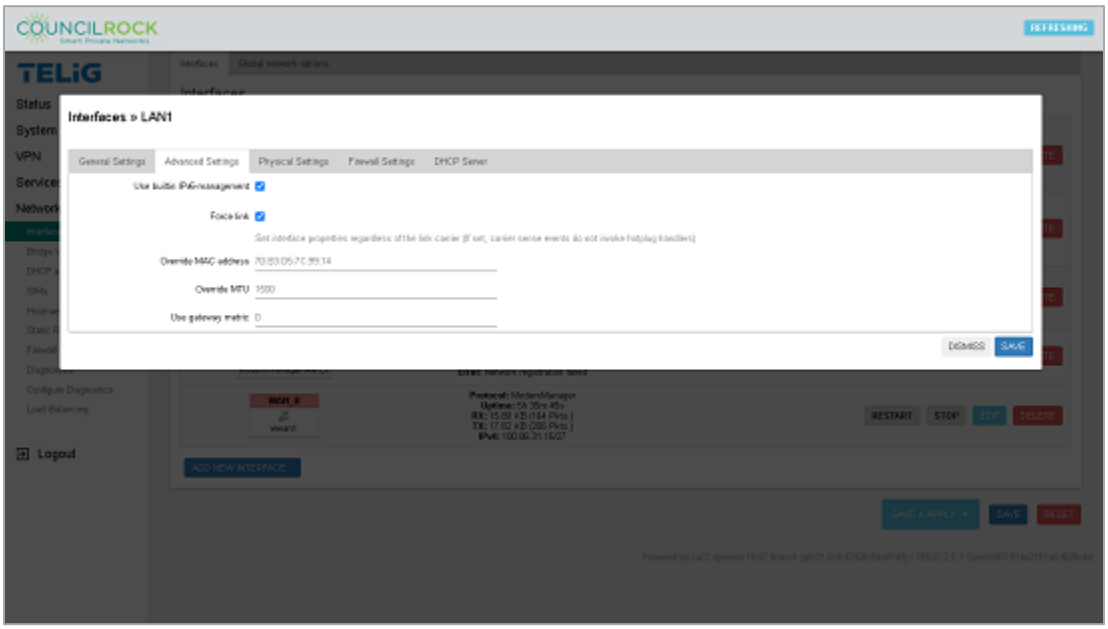

Figure 68: Interfaces > LANx > Advanced Settings

On the **Physical Settings** tab, the user can select whether to bridge physical interfaces, and select the physical interface (or interfaces, in the case of a bridge). If bridging is enabled, the user can enable/disable STP and IGMP snooping.

Bridging physical interfaces allows all ports in the bridge to act as a single network.
By enabling bridging, we can combine, for example, the WiFi (WLAN) interface(s) with the wired LAN ports to create a single logical network. We can also combine the two ethernet ports if desired.

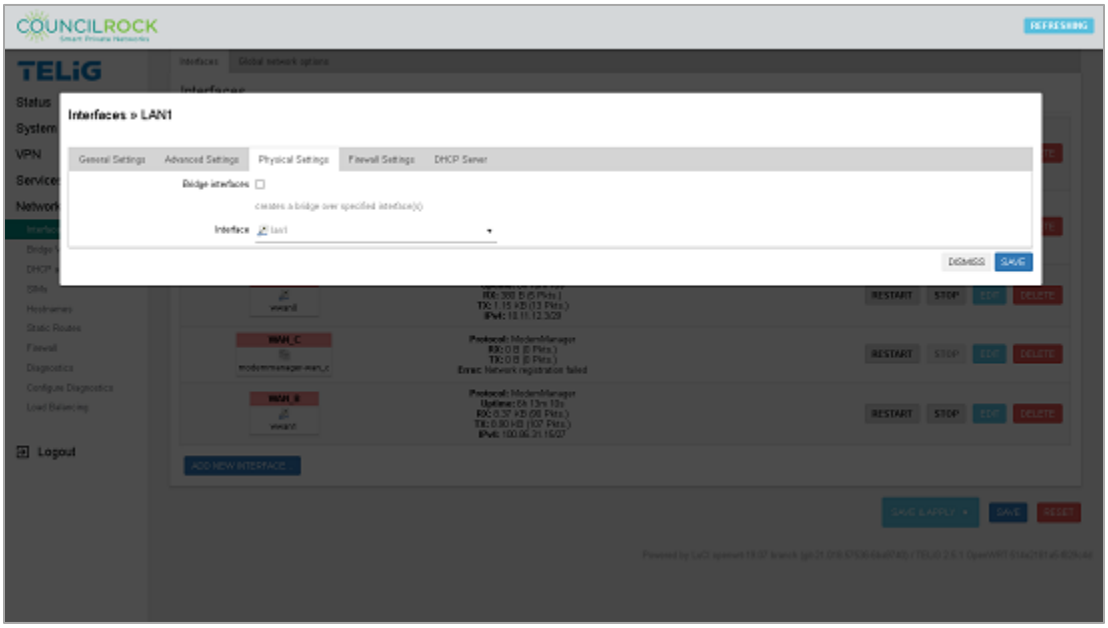

Figure 69: Interfaces > LANx > Physical Settings

On the **Firewall Settings** tab, the user can create / assign the interface's firewall- zone.

The router Firewall collects interfaces into 'firewall-zones' to filter traffic. A firewall-zone can be configured to any set of interfaces but generally there are at least two zones:

- lan - to collect LAN interfaces
- wan - to collect WAN interfaces

A minimal router firewall configuration typically consists of one section, at least two firewall-zones (lan and wan), and one forwarding to allow traffic from LAN to WAN.

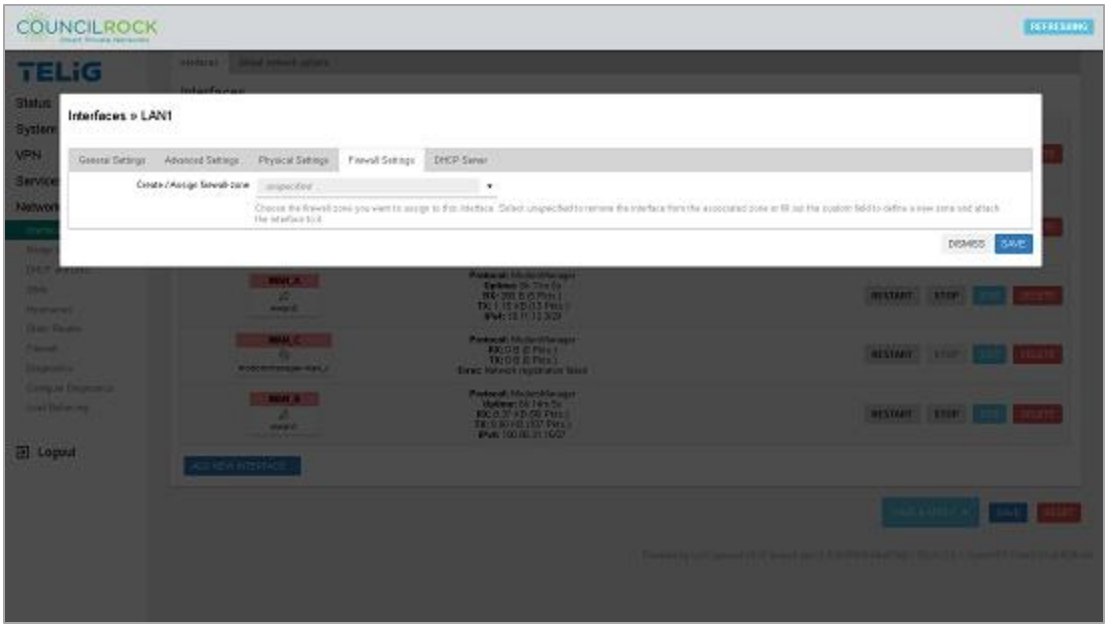

Figure 70: Interfaces > Firewall Settings

On the **DHCP Server** tab, the user can set up the interface as a DHCP (Dynamic Host Control Protocol) Server.

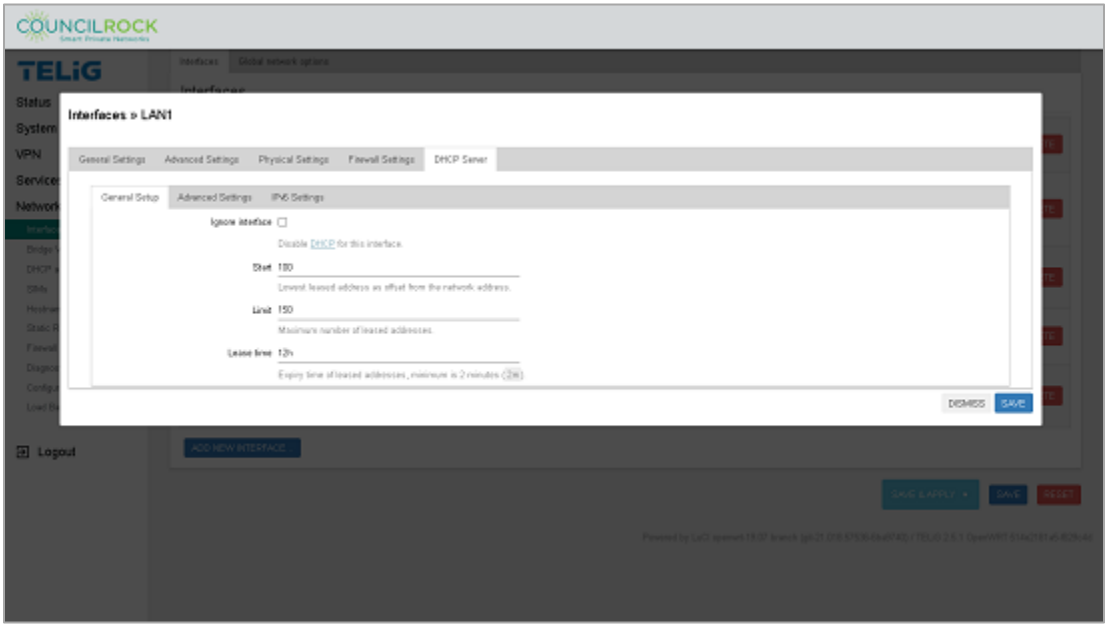

Figure 71: Interfaces > DHCP Server > General

General Settings – Here the user can set the following general options:

- Ignore interface – select the checkbox to bypass DHCP for this interface
- Start: the starting number for address leases (the "**N**" in the IP address x.x.x.**N)**
- Limit: the maximum number of addresses to lease

- Lease Time: the time before leased addresses expire (for hours use ‘h’, for minutes use ‘m’; the minimum allowable is 2m)

Advanced Settings – Here the user can set up the following Advanced DHCP options:

- Dynamic DHCP – select the checkbox to automatically manage DHCP addresses. Leaving the box unchecked will limit IP address leases to clients with static addresses.
- Force – select the checkbox to force DHCP on the interface even if another DHCP server is detected
- IPv4-Netmask – (default 255.255.255.0) enter an IPv4 netmask here to override the default netmask, normally calculated from the subnet it serves
- DHCP-Options – lets the user configure other advanced DHCP options, such as use of an alternate gateway, DNS server and NTP server, or disable WINS. For a complete list of options, refer to: http://www.networksorcery.com/enp/protocol/bootp/options.htm

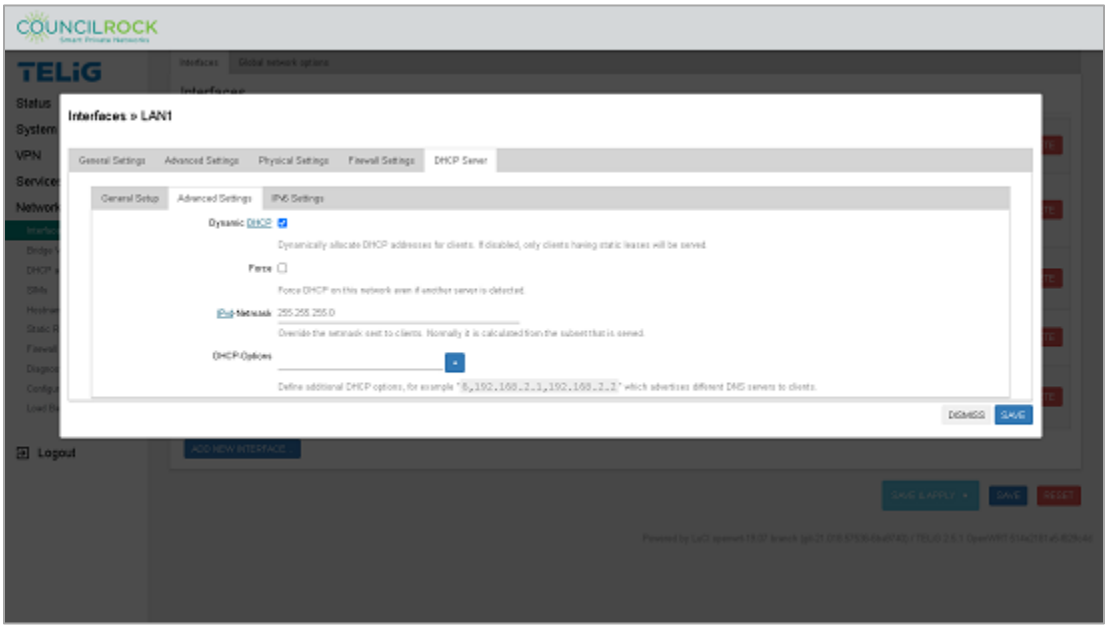

Figure 72: Interfaces > DHCP Server > Advanced

IPv6 Settings – Here the user can set the following IPv6 DHCP options:

- Router Advertisement-Service – from the dropdown list, select *disabled*, *server mode*, *relay mode*, or *hybrid mode*
- DHCPv6-Service – from the dropdown list, select *disabled*, *server mode*, *relay mode*, or *hybrid mode*
- NDP-Proxy – from the dropdown list, select *disabled*, *relay mode*, or *hybrid mode*

- Announced DNS servers – add an IP address to the text box and click the '+' button to set the DNS server to be announced
- Announced DNS domains – add an IP address to the text box and click the '+' button to set the DNS domain to be announced

From the OpenWRT manual:

> *OpenWrt features a versatile RA & DHCPv6 server and relay. Per default, SLAAC (Stateless Address Autoconfiguration) and both stateless and stateful DHCPv6 are enabled on an interface. If there are any prefixes of size /64 or shorter present, then addresses will be handed out from each prefix. If all addresses on an interface have prefixes shorter than /64 then DHCPv6 Prefix Delegation is enabled for downstream routers. If a default route is present the router advertises itself as default router on the interface.*
>
> *The system is also able to detect when there is no prefix available from an upstream interface and can switch into relaying mode automatically to extend the upstream interface configuration onto its downstream interfaces. This is useful for putting the target router behind another IPv6 router which doesn't offer prefixes via DHCPv6-PD.*

For more on IPv6 routing with OpenWRT, refer to:
https://openwrt.org/docs/guide-user/network/ipv6/start#router_advertisement_dhcpv6

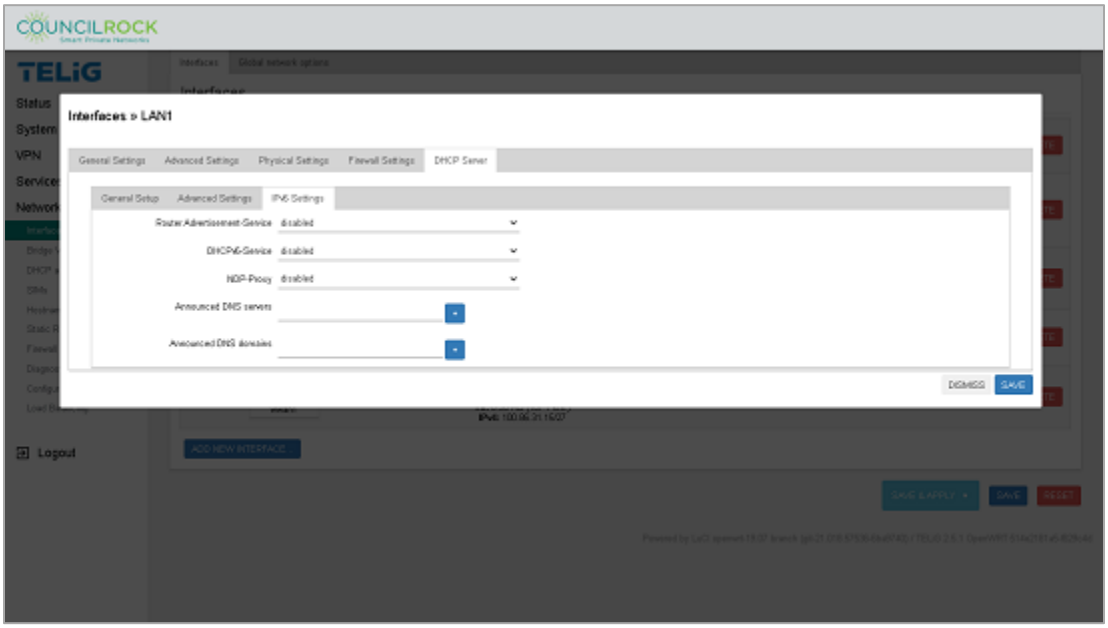

Figure 73: Interfaces > DHCP Server > IPv6 Settings

Wireless (Available on “W” models)

Displays active wireless networks and associated stations. Wireless network interfaces can be enabled / disabled / restarted / added / edited / removed.

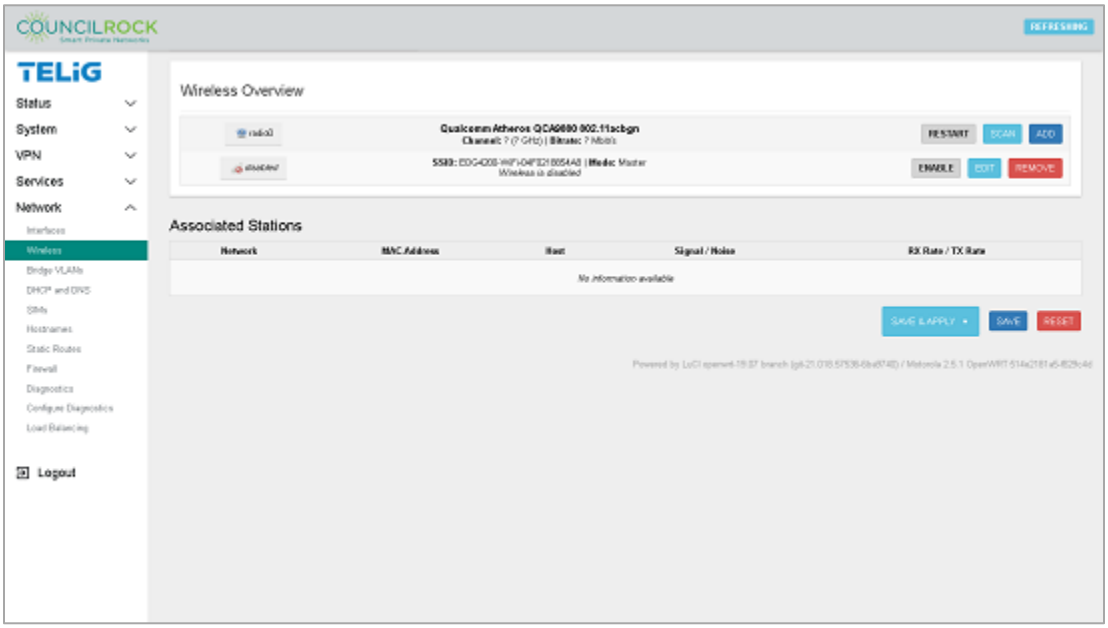

Figure 74: Wireless > Overview

A **Restart** button can be used to restart the wireless interface.

A **Scan** button starts a network scan for detectable wireless networks, displaying signal strength, SSID (network name), encryption type, and other network information.

The **Join Network** button opens a dialogue to connect to a network. If the network is encrypted, authentication credentials are required to join.

When adding / editing a wireless network, the Edit wireless network dialogue is displayed. The **General Setup** tab (located on the top card of the Edit wireless network dialogue) lets the user enable or disable the network, select the frequency band and channel, and set maximum transmit power.

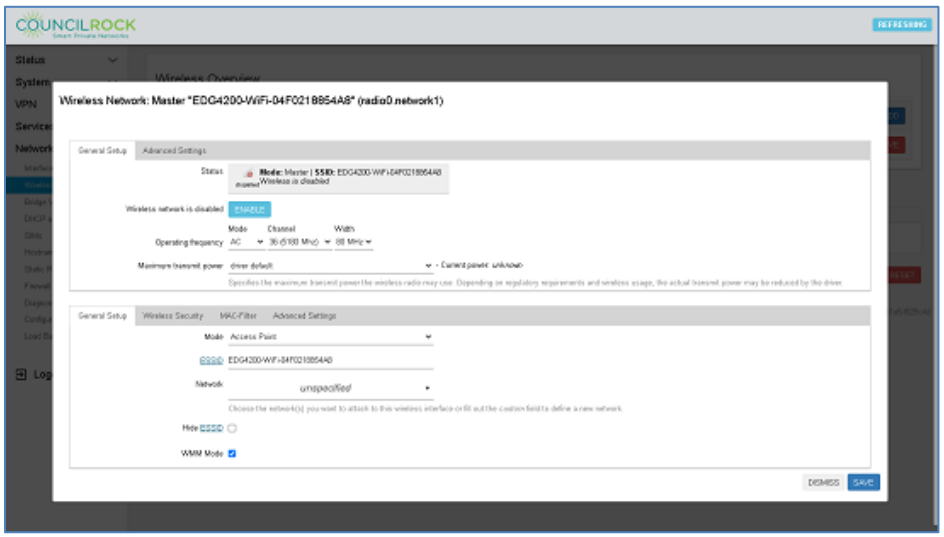

Figure 75: Wireless > Wireless Network > General [Top Card]

The **Advanced Settings** tab (located on the top card of the Edit wireless network dialogue) allows the user to set a non-default country code, toggle allowing legacy 802.11b rates, set up distance optimization, change fragmentation and RTS/CTS thresholds, and set the beacon interval. The user can force 40MHz channels, bearing in mind that this is non-compliant with IEEE 802.11n-2009.

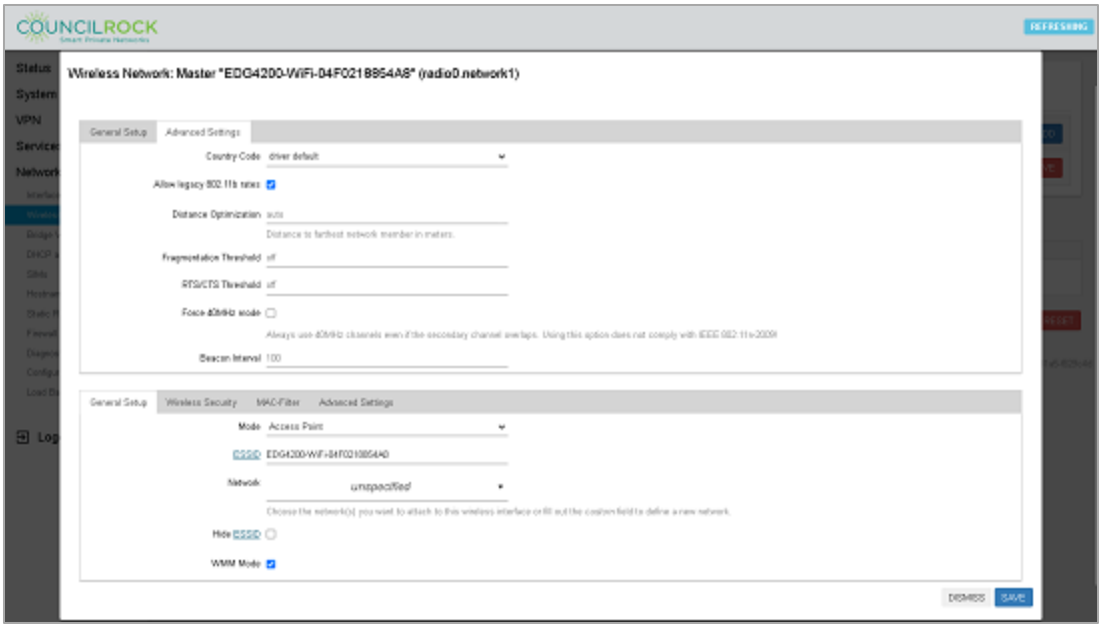

Figure 76: Wireless > Wireless Network > Advanced [Top Card] and General Setup [Bottom Card]

Configuration options available on the bottom card of the Edit wireless network dialogue vary depending on the wireless mode configuration.

A common configuration, for example, is to configure the unit as a wireless access point. To set this up, under the **General Setup** tab (located on the bottom card of the Edit wireless network dialog) use the following options:

Mode	Access Point
ESSID	Network name as it appears on client devices.
Network	The network(s) to attach to the wireless interface.
Hide ESSID	Check to hide the network (requiring manual SSID entry to connect)
WMM Mode	Check to enable WiFi Multimedia (WMM) mode (prioritizing multimedia packets for quality of service)

Table 7: Wireless Access Point Typical Setup Options

Under the **Wireless Security** tab (located on the bottom card of the Edit wireless network dialog), the user can configure network security settings. Configuration options vary based on encryption type selected. We recommend using a strong security WPA2 encryption.

The most common is WPA2-PSK password-based encryption. After selecting “WPA2-PSK (strong security)” from the dropdown, the user can enter the Key (password), and optionally enable WPS push button authentication.

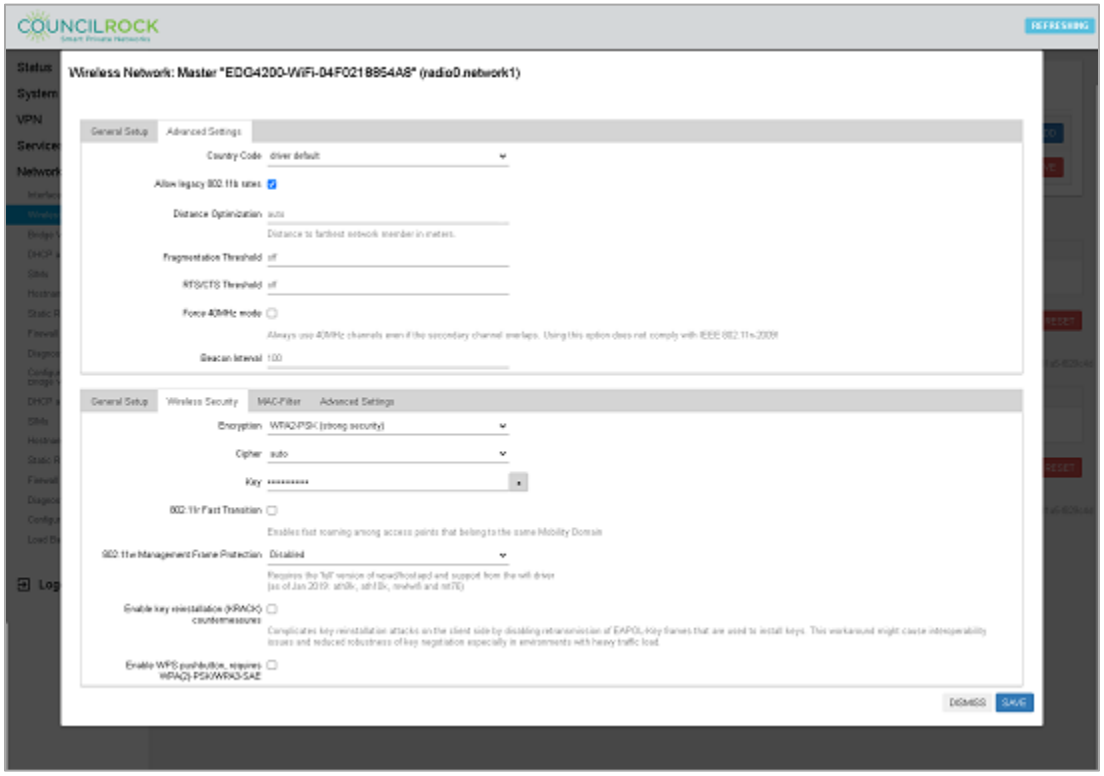

Figure 77: Wireless > Wireless Network > Wireless Security [Bottom Card]

Alternatively, if a RADIUS authentication server exists on the network, the user can select “WPA2-EAP (strong security)” from the dropdown to set up RADIUS authentication. Follow these steps to set up RADIUS:

1. Enter the RADIUS server’s IP address for Radius-Authentication-Server, and the port number for Radius-Authentication-Port, (if different from the default).
2. Add the pre-configured password to Radius-Authentication-Secret.
3. If the RADIUS authentication system uses a different server for accounting, enter the server’s IP address and port (if different from the default), as Radius-Accounting-Server and Radius-Accounting-Port.
4. Enter the accounting password as Radius-Accounting-Secret.
5. If the DAE client differs from your RADIUS server, enter the DAE client’s IP address and port (if different from the default) as DAE-Client and DAE-Port, and the DAE client’s password as DAE-Secret.
6. Optionally, set a NAS ID.

For both WPA2-PSK and WPA2-EAP encryption, the user has the option to select a cipher, and configure 802.11r fast translation, 802.11w management frame protection, and key reinstallation countermeasures.

Under the MAC-Filter tab (located on the bottom card of the Edit wireless network dialogue), the user can set up blacklist (do not allow) or whitelist (only allow) devices with specific MAC addresses.

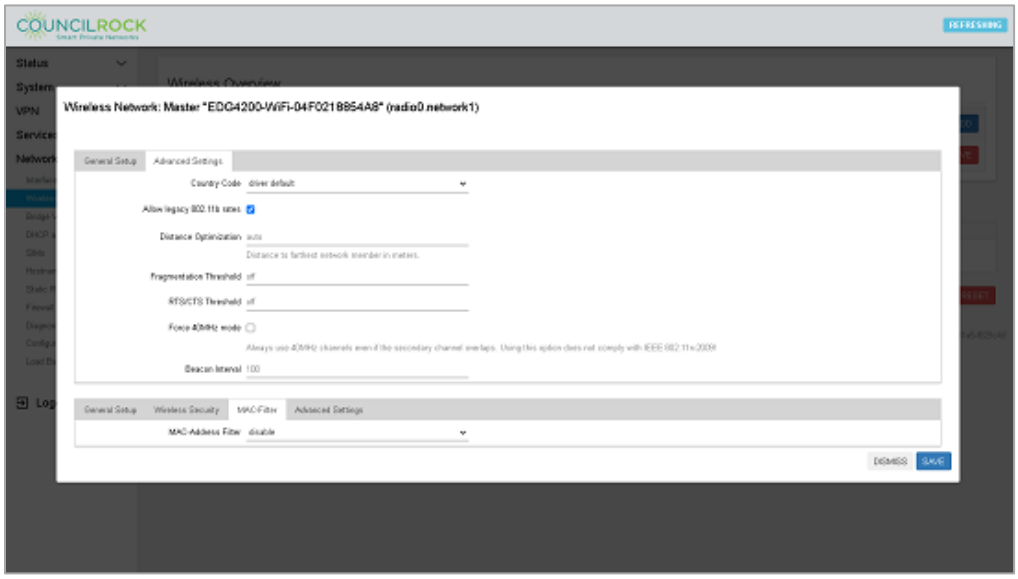

Figure 78: Wireless > Wireless Network > MAC-Filter [Bottom Card]

Under the **Advanced Settings** tab (located on the bottom card of the Edit wireless network dialogue), the user can configure advanced settings for the wireless network such as preventing client to client communication and overriding the default wireless interface name.

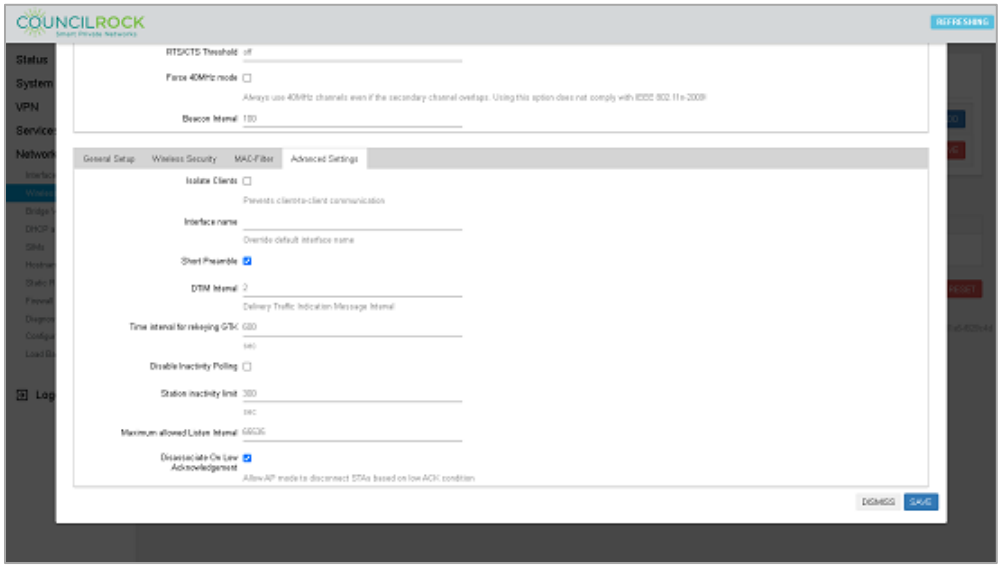

Figure 79: Wireless > Wireless Network > Advanced Settings [Bottom Card]

Bridge VLANs

Allows the user to configure groups of ports as 'virtual LANs'

The **Status** tab displays the status of the bridge interfaces and VLANs.

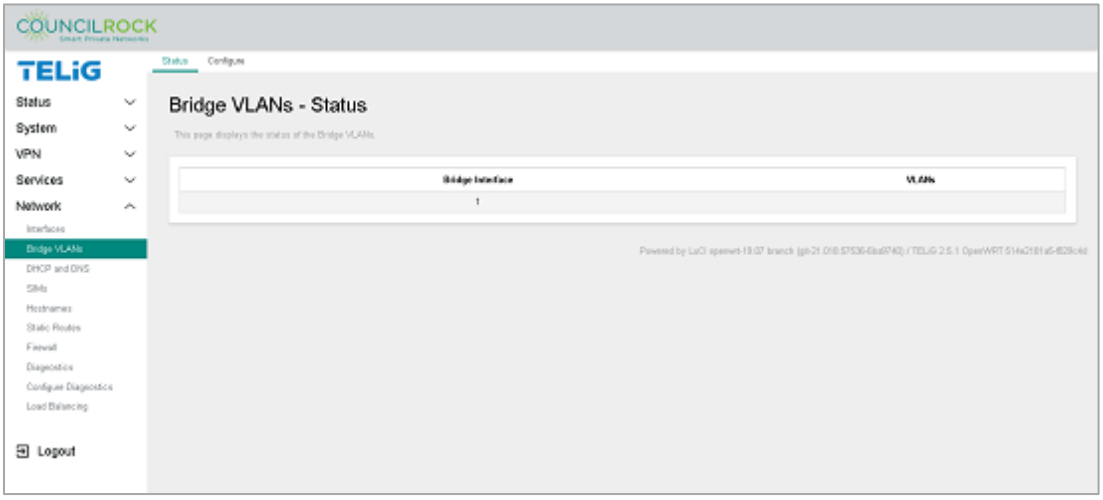

Figure 80: Network > Bridge VLANs > Status

The **Configure** tab lets the user enable bridge VLAN filtering and specify a bridge interface to use, and to add, edit, and delete bridge VLAN assignments.

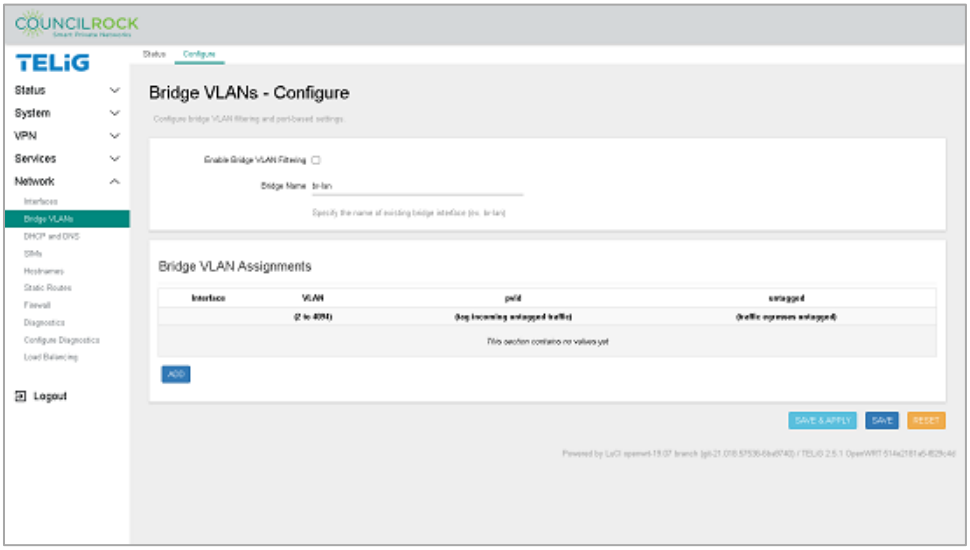

Figure 81: Network > Bridge VLANs > Configure

DHCP and DNS

The DHCP and DNS menu lets the user configure Dynamic Host Configuration Protocol (DHCP) server and Domain Name System (DNS) forwarder options for local Network Address Translation (NAT) networks.

The **General Settings** tab allows the user to set the general behavior for the DHCP server and DNS forwarder.

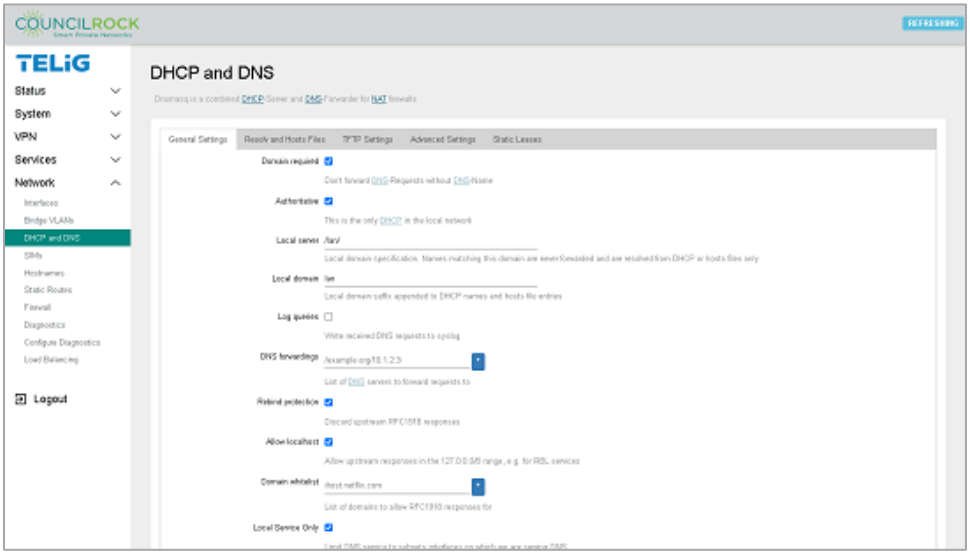

Figure 82: Network > DHCP and DNS > General Settings

The **Resolv** and **Hosts Files** tab lets the user specify configuration files for the DHCP server, specify a DHCP lease file, specify a DNS resolve file, and specify additional hosts files (in addition to the default /etc/hosts).

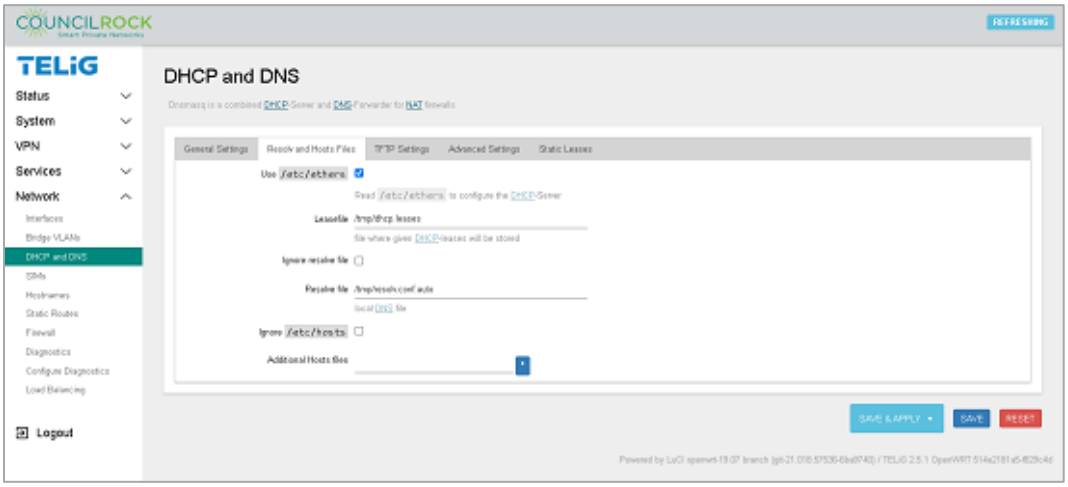

Figure 83: DHCP and DNS > Resolv and Hosts Files

The **TFTP Settings** tab is to enable and configure the root directory for a TFTP server.

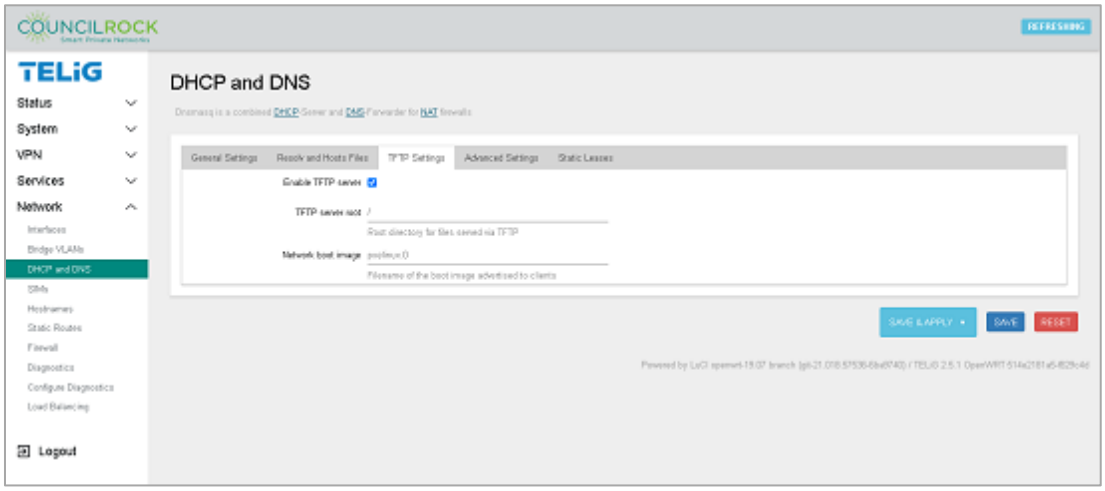

Figure 84: DHCP and DNS > TFTP Settings

The **Advanced Settings** tab allows the configuration of advanced behavior settings for the DHCP server and DNS forwarder.

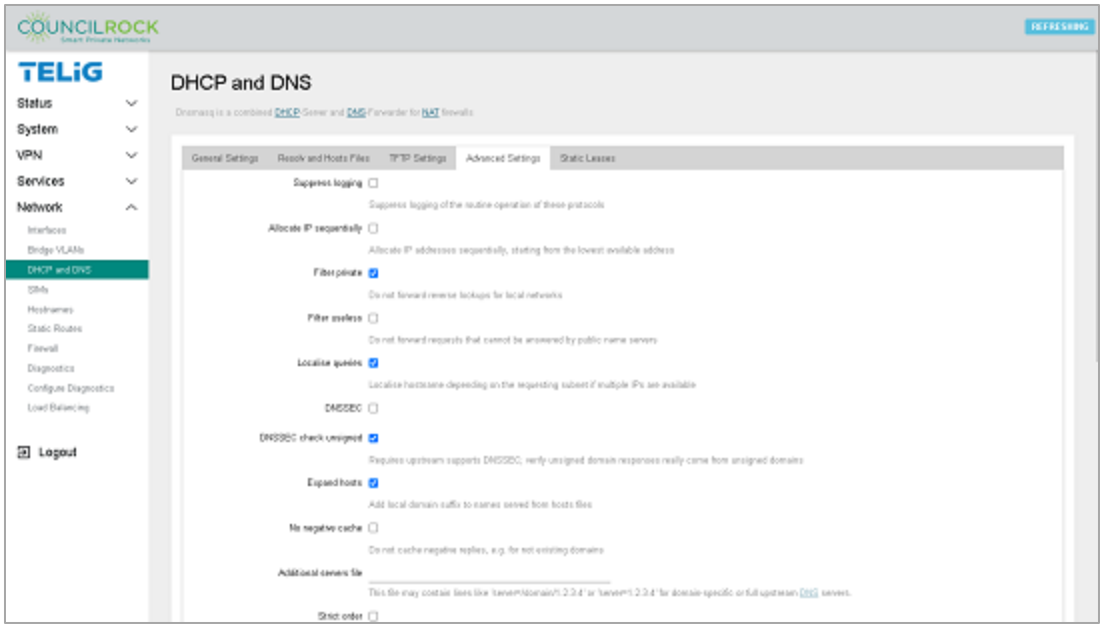

Figure 85: DHCP and DNS > Advanced Settings

Finally, the **Static Leases tab** lets the user view, add, and edit static leases for DHCP clients as well as view active DHCP leases for IPv4 and IPv6 clients. Static DHCP leases can be configured with optional symbolic hostnames and custom lease times.

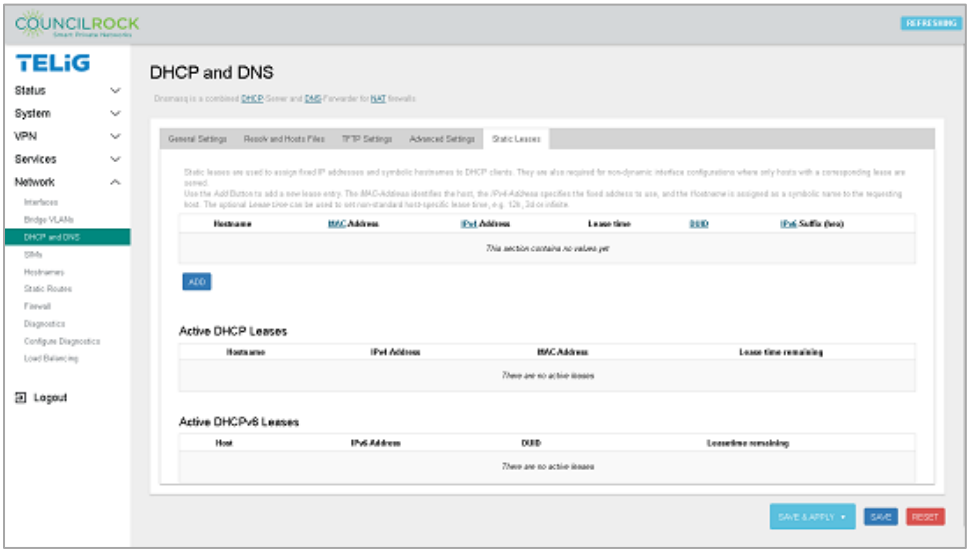

Figure 86: DHCP and DNS > Static Leases

SIMs

The SIMs menu lets the user displays current SIM card info in the *General Info* section. In the *APNs* section, users can set identifying APN numbers on installed SIM card(s) by entering the APN number in the applicable interface text box and clicking *Save & Apply*.

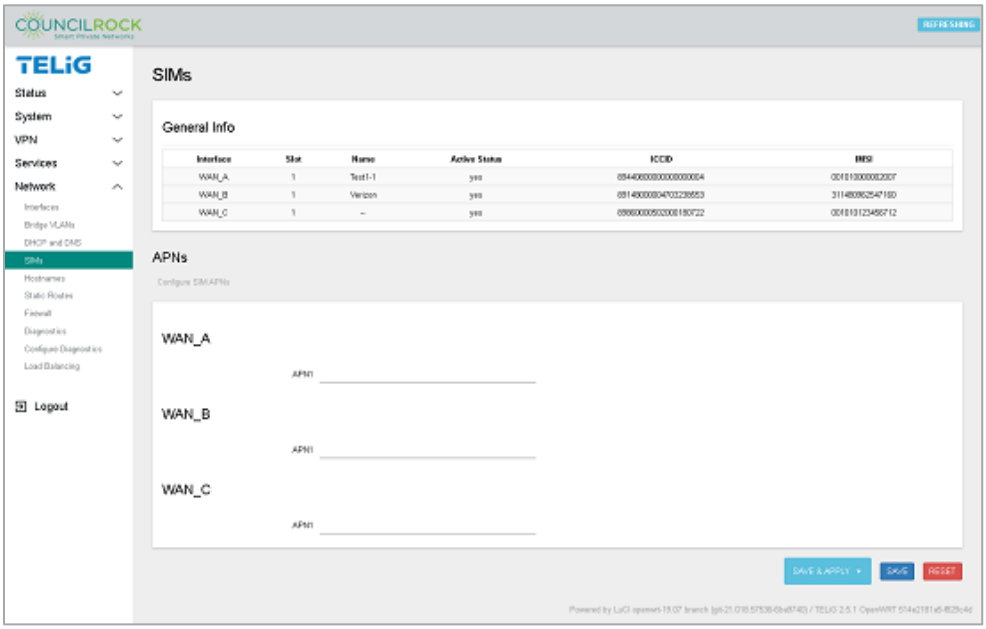

Figure 87: SIMs

Hostnames

The **Hostnames** menu lets the user set up custom hostnames for IP addresses.
You can add a new hostname entry by clicking the ADD button and entering a hostname then selecting an IP address from the dropdown menu or
You can edit or delete existing entries, and reorder entries by dragging them to another location in the list with the ‘ ☰ ’ icon.

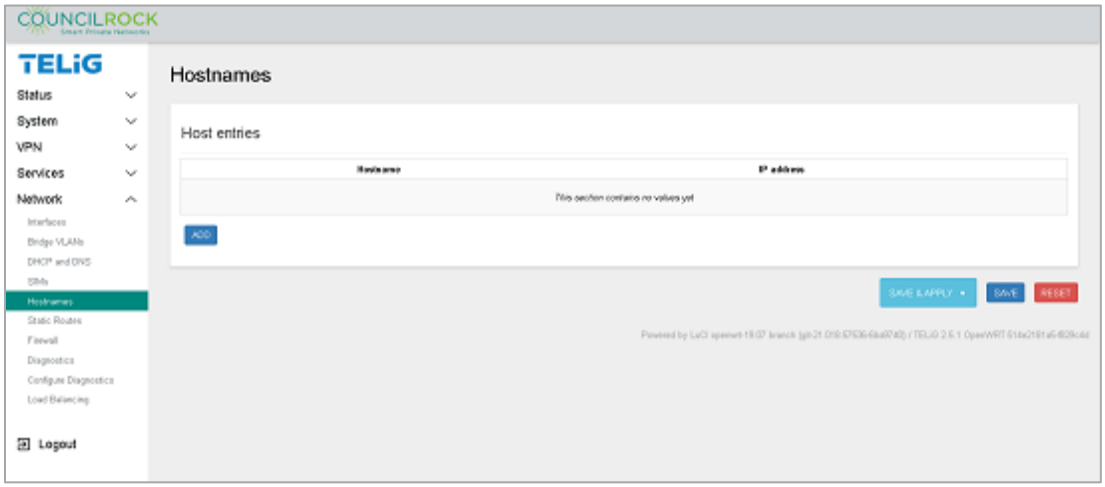

Figure 88: Network > Hostnames

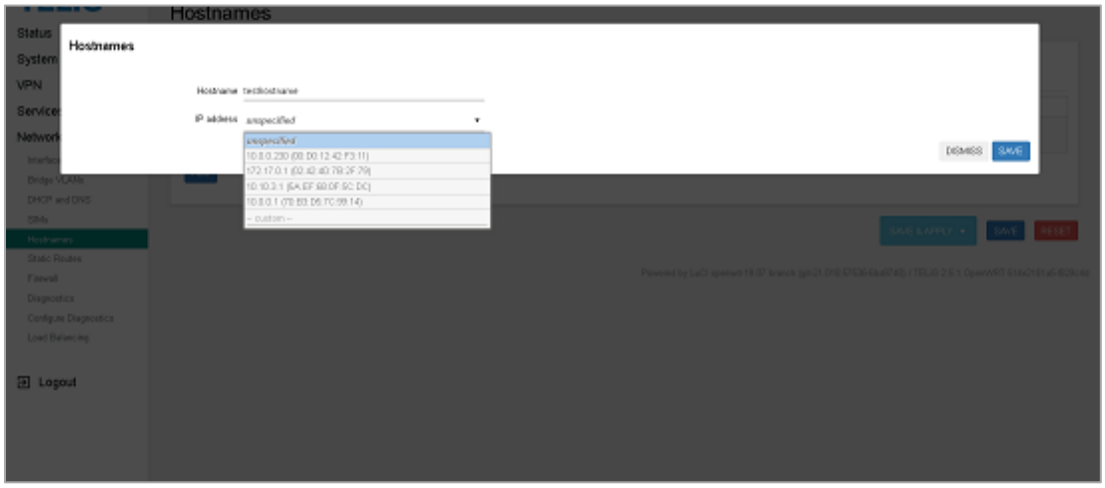

Figure 89: Network > Hostnames > Adding a hostname

Static Routes

Static routes provide one of the safest methods of Layer 3 connectivity. These are secure from route spoofing attacks because your router does not rely on routing information being sent and received from other routers. All the routing information is user controlled and locally configured.

Static routes are typically used where:

- There are only a small number of destinations to configure
- One or two paths exist to each destination

With static routes, the following is true:

- A default route is used on the perimeter router to reach external resources
- Specific internal routes are used to reach internal resources

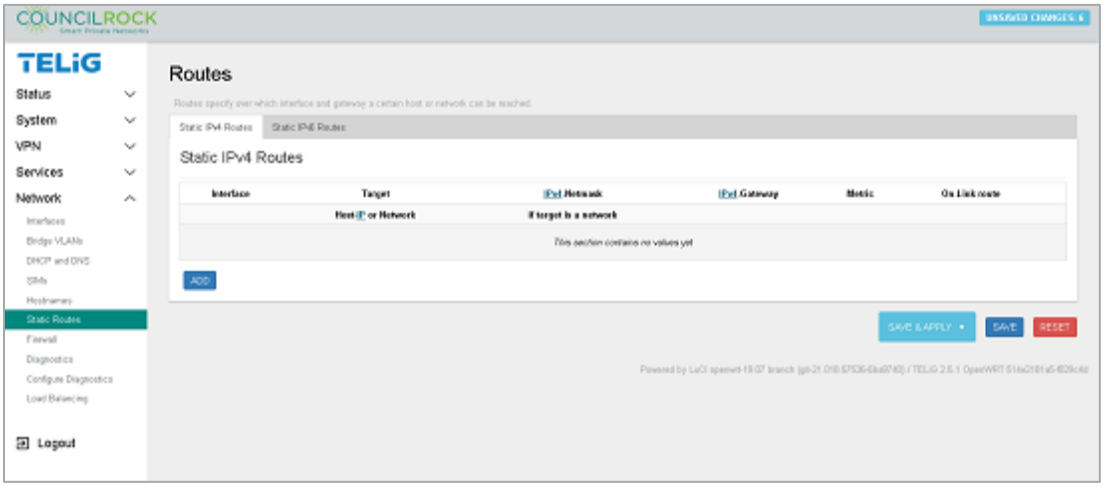

Figure 90: Network > Static Routes

To add a route, click the ADD button. On new routes or when editing existing routes, the following settings are available:

- GENERAL SETTINGS
    - Interface: Select the interface where the target network resides; defined interfaces will be selectable from the dropdown list.
    - Target IP: The address of the destination network
    - Netmask: A mask that is applied to the Target IP to determine to what actual IP addresses the route applies. If omitted, 255.255.255.255 is assumed, which makes Target IP a host address.

- Gateway: Defines where the router should send traffic. If omitted, the gateway from the parent interface is taken if any, otherwise creates a link scope route. If set to 0.0.0.0 no gateway will be specified for the route.

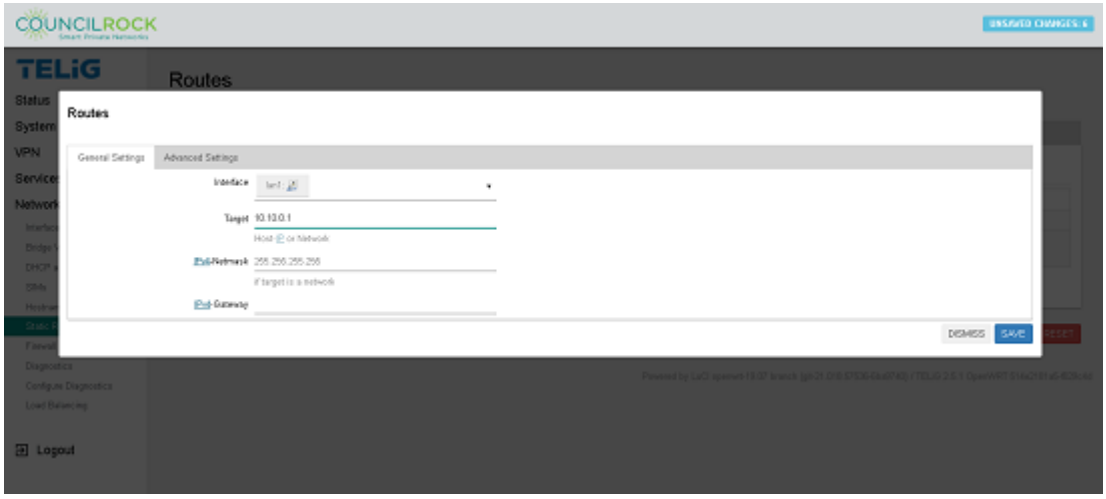

Figure 91: Network > Static Routes > General Settings

- ADVANCED SETTINGS
  - Metric: (default: 0) Metric is used as a sorting measure. If a packet that is about to be routed fits two rules, the one with the lower metric is applied.
  - MTU: (default: 1500) Specify the Maximum Transmission Unit (MTU) in Kb for this route.
  - Route Type: (default: unicast) Each route type specifies a different behavior for the route:
    - *unicast:* the route entry is for a path to a single destination IP
    - *local:* the destination is assigned to this host. Packets are looped back and delivered locally.
    - *broadcast:* the destination is a broadcast address. Packets are sent as link broadcasts
    - *multicast*: a special type used for multicast routing. It is not present in normal routing tables
    - *unreachable:* these destinations are unreachable. Packets are discarded and the ICMP message 'host unreachable' is generated
    - *prohibit:* these destinations are unreachable. Packets are discarded and the ICMP message 'communication administratively prohibited' is generated
    - *blackhole:* these destinations are unreachable. Packets are discarded without a response.

        - *anycast:* these destinations are anycast: equivalent to local with one difference - such addresses are invalid when used as the source address of any packet
    - Route Table: (default: main (254)) Defines the table ID to use for the route. The special aliases local (255), main (254) and default (253) as well as 'custom' are selectable from the dropdown list. If 'custom' is used, enter a number ranging from 0 to 65535 directly in the dropdown.
    - Source Address: (default: automatic) The preferred source address when sending to destinations covered by the target. Local IP addresses are selectable from a dropdown list, as well as a 'custom' field for entering IP addresses directly.
    - On-Link route: (default: off) When enabled, gateway is on link even if the gateway does not match any interface prefix

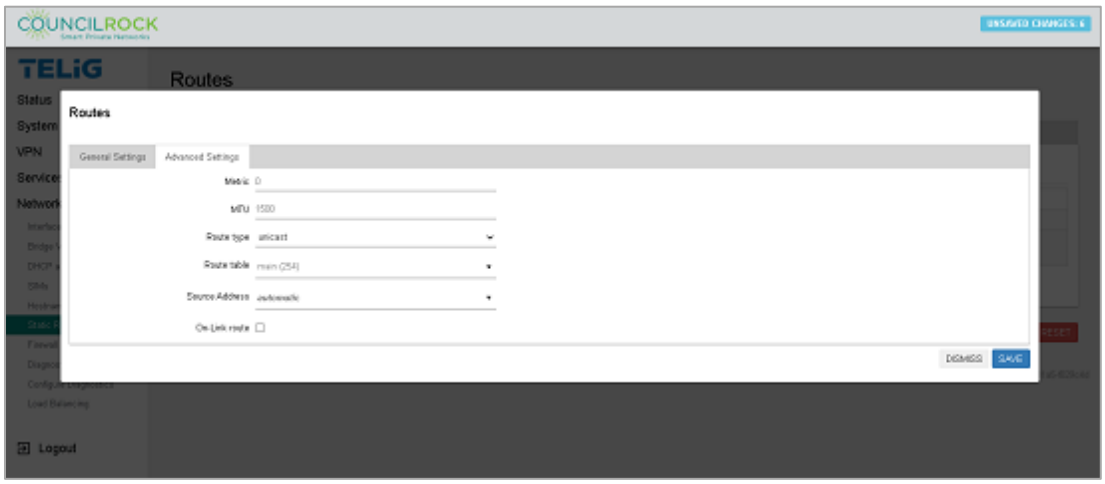

Figure 92: Network > Static Routes > Advanced

Firewall

The **Firewall** menu is for setting up Firewall Zones, Rules, and Port Forwarding.

The **General Settings** tab contains default Firewall settings and provides add / edit / delete functions for the listed Firewall Zones.

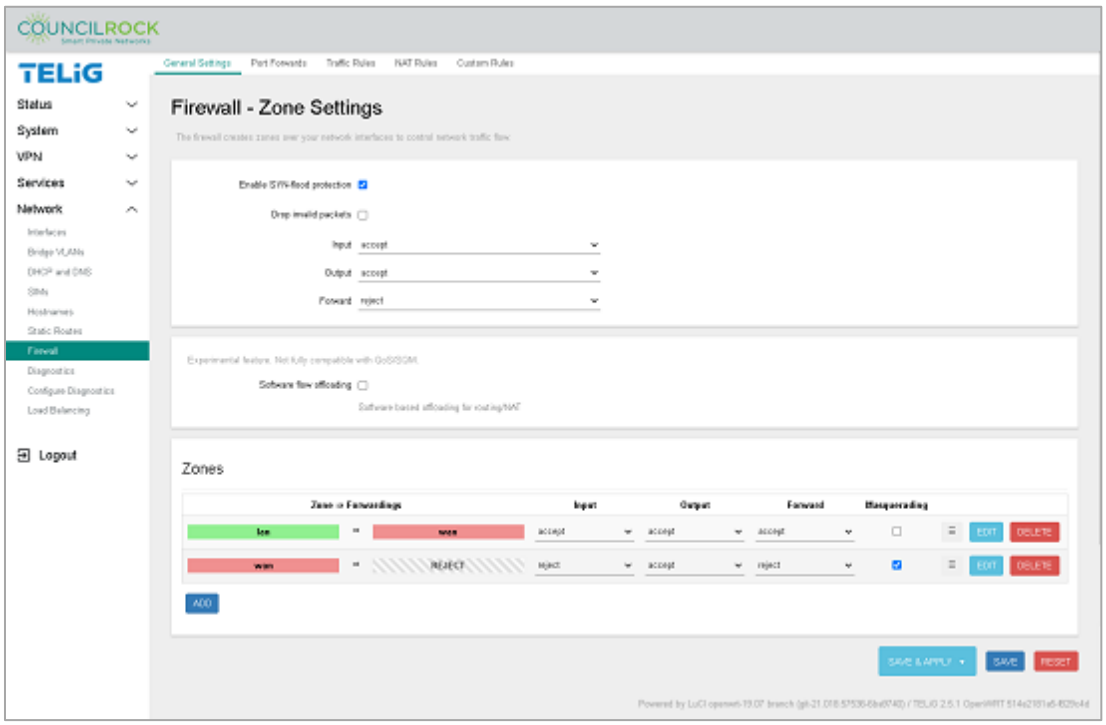

Figure 93: Network > Firewall > General

> NOTE: "Software flow offloading"
> This is a Linux kernel- based routing process using netfilter allowing specific kernel modules to register callback functions to the networking stack. When a packet is received and its flow is not known, it is forwarded to the networking stack. If its flow is known, NAT translation (if any) is applied, and it is forwarded to the appropriate port. As an experimental Linux feature, we do not recommend activating software flow offloading.

When creating a new firewall zone or editing an existing one, the **Firewall - Zone Settings** dialogue appears with the following submenus:

Firewall - Zone Settings > General Settings contains settings for:

- Zone name
- Zone input, output, and traffic forwarding behavior
- Networks covered by the zone
- Forwarding policy to and from the zone
- Masquerading and MSS clamping.

Firewall - Zone Settings > Advanced Settings contains the settings to:

- Restrict zone coverage
    - By device
    - By subnet
    - By IP family
- Set Masquerading by source and/or destination subnets
- Enable / disable logging.

Firewall - Zone Settings > Conntrack Settings contains settings for:

- Toggling automatic conntrack helper assignment
- Allowing “invalid” traffic for the zone.

Conntrack is a userspace command line program targeted at system administrators. It enables them to view and manage the in-kernel connection tracking state table.

Firewall - Zone Settings > Extra Iptables Arguments allows the user to set up raw source and destination arguments to the iptables command allowing finer control of firewall rules.

Important: *Firewall Zone Extra IPTables Arguments are intended only for Advanced Users.*

The **Port Forwards** tab displays existing port forwarding rules, and lets the user add / edit / delete Port Forwarding Rules. This configures the unit to forward traffic directed to a port on the device to another IP address and port.

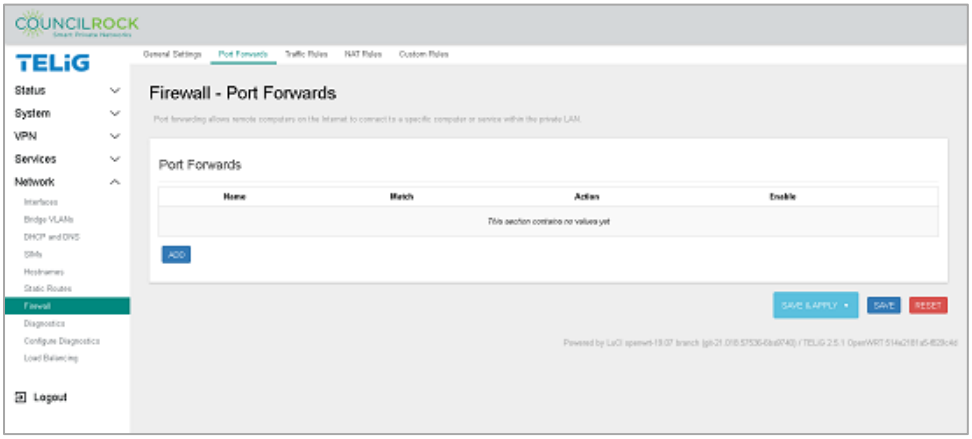

Figure 94: Network > Firewall > Port Forwards

> **Important:** *Firewall Port Forwarding is intended only for Advanced Users.*

When creating / editing a port forward, the Firewall - Port Forwards dialogue is displayed with the following submenus:

Firewall - Port Forwards > General Settings contains settings for:

- Protocol
- Source zone
- External destination port
- Destination zone
- Internal destination IP address and port

Firewall - Port Forwards > Advanced Settings provides for further traffic restrictions by matching the forwarding rule to

- Source MAC address
- Source IP address
- Source port
- External destination IP address

Advanced Settings are also provided for these cases (intended only for Advanced users):

- Whether to use an internal or external IP address for reflected traffic
- To specify additional matching configurations

- To pass raw arguments to the underlying iptables command

The **Traffic Rules** tab displays existing traffic rules and provides add / edit / delete functionality.

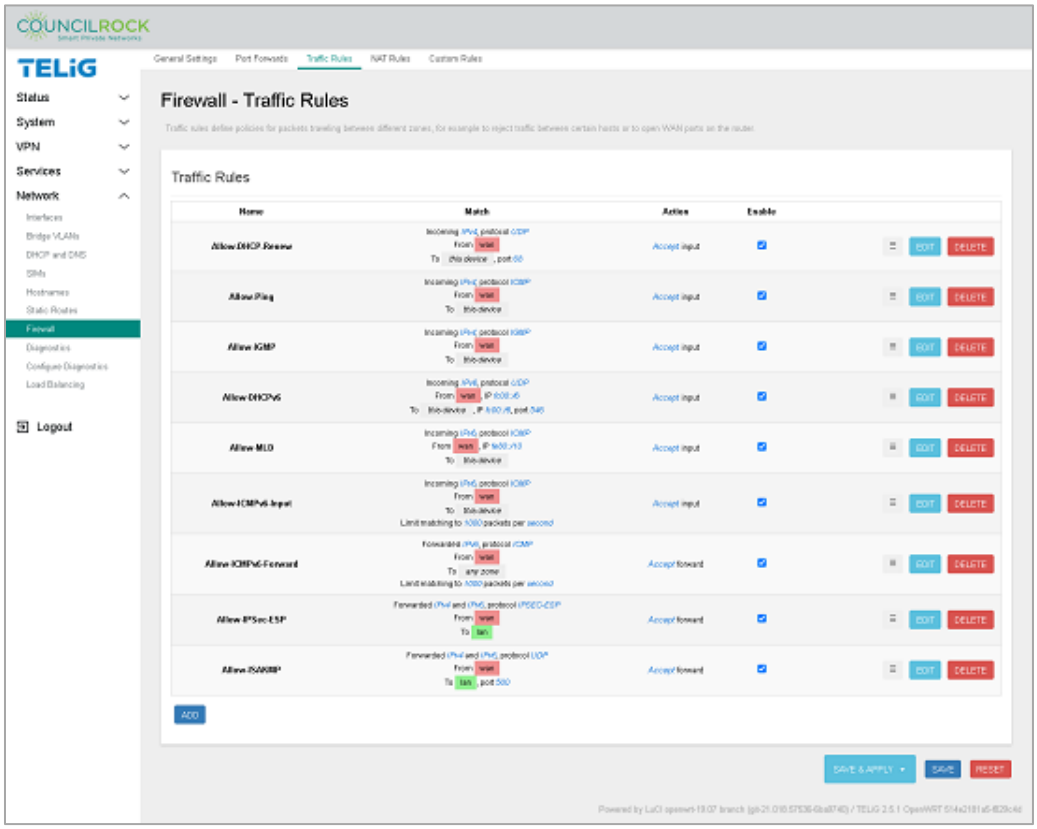

Figure 95: Network > Firewall > Traffic Rules

When adding / editing an existing Rule, the Firewall - Traffic Rules dialogue is displayed.

Firewall - Traffic Rules > General Settings is provided to configure the Traffic Rule matching criteria:

- Protocol
- Source zone
- Destination zone
- IP address and port

And to set the action to take for packets matching the rule.

Available actions are summarized below:

Accept - Allow the traffic to pass the firewall
Reject - Drop the traffic
Don't Track - Do not keep track of traffic

Assign Conntrack Helper - These are modules that can assist the firewall in tracking protocols, intended only for Advanced users

Apply Firewall / XOR Firewall Mark - Firewall marks provide a powerful mechanism to group services together, intended only for Advanced users

DSCP classification - DSCP Marking is used to determine traffic classification for network data. This can be used to determine which network traffic requires higher bandwidth, has a higher priority, and more likely to drop packets. This functionality is intended only for Advanced users.

Firewall - Traffic Rules > Advanced Settings provides further restrictions when the traffic rule matches

- Device - select from inbound, outbound, or unspecified
- IP address family - restrict to IPv4, IPv6, or both
- Source MAC address - select from dropdown list of available MAC addresses
- Additional matching configurations for advanced users

And to pass raw arguments (Firewall Zone Extra IPTables Arguments) to the underlying iptables command.

Important: *Firewall Zone Extra IPTables Arguments are intended only for Advanced Users.*

Firewall - Traffic Rules > Time Restrictions lets the user specify a date and/or time range during which the Traffic Rule will be enforced.

The **NAT Rules** tab displays existing NAT rules. Here the user can add / delete / edit NAT rules, fine-tuning control over the source IP address(es) used for outbound and forwarded traffic.

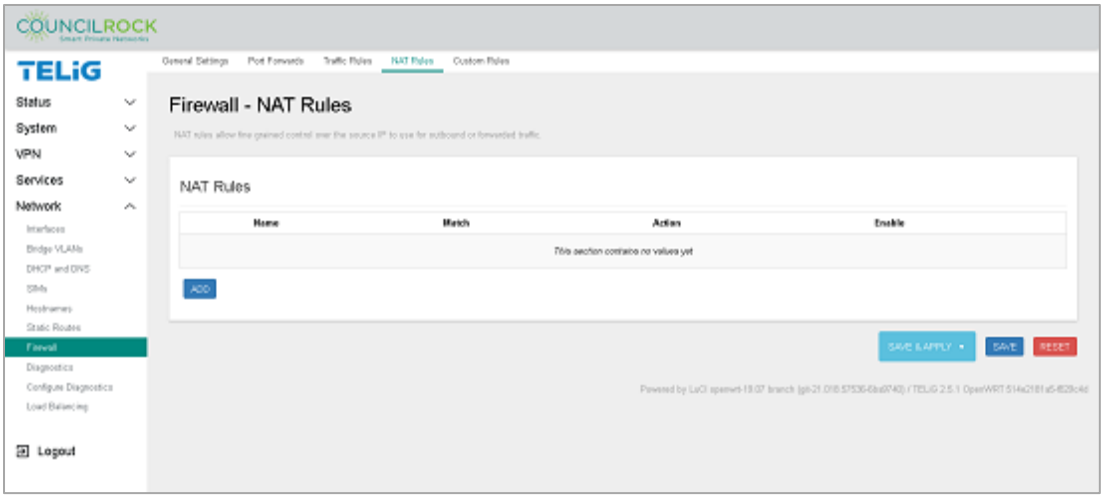

Figure 96: Network > Firewall > NAT Rules

When adding a new NAT rule or editing an existing one, the Firewall - NAT Rules dialogue is displayed.

Firewall - NAT Rules > General Settings lets the user set

- Protocol
- Outbound zone
- Source address
- Destination address

And the action to take for packets matching the rule. In the case of the SNAT action, you must specify a rewrite IP address.

Firewall - NAT Rules > Advanced Settings lets the user further restrict when the NAT rule is matched by

- Outbound device
- Additional matching configurations

And to pass raw arguments to the underlying iptables command.

Firewall - NAT Rules > Time Restrictions lets the user specify a date and/or time range during which the Traffic Rule will be enforced.

> ⚠ **Important:** *Firewall NAT Rules are intended only for Advanced Users.*

The **Custom Rules** tab lets the user specify a custom shell script to be executed after the default ruleset has been loaded, allowing advanced users direct control to execute arbitrary iptables commands.

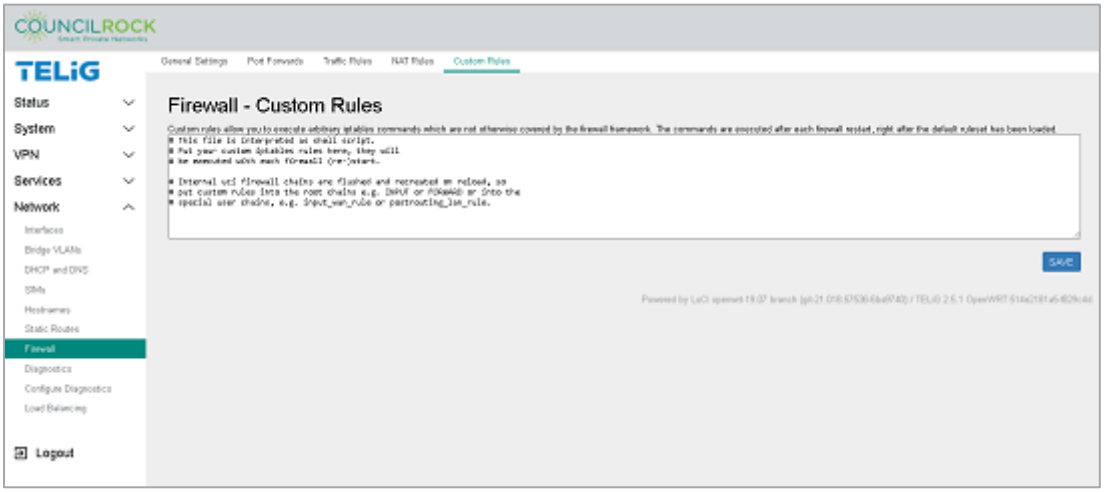

Figure 97: Network > Firewall > Custom Rules

> ⚠ **Warning:** *Custom Rules are intended only for Advanced Users.*

Diagnostics

The **Diagnostics** menu provides basic tools to verify network state and troubleshoot network issues. Ping, traceroute, or nslookup can be performed on any specified hostname or IP address.

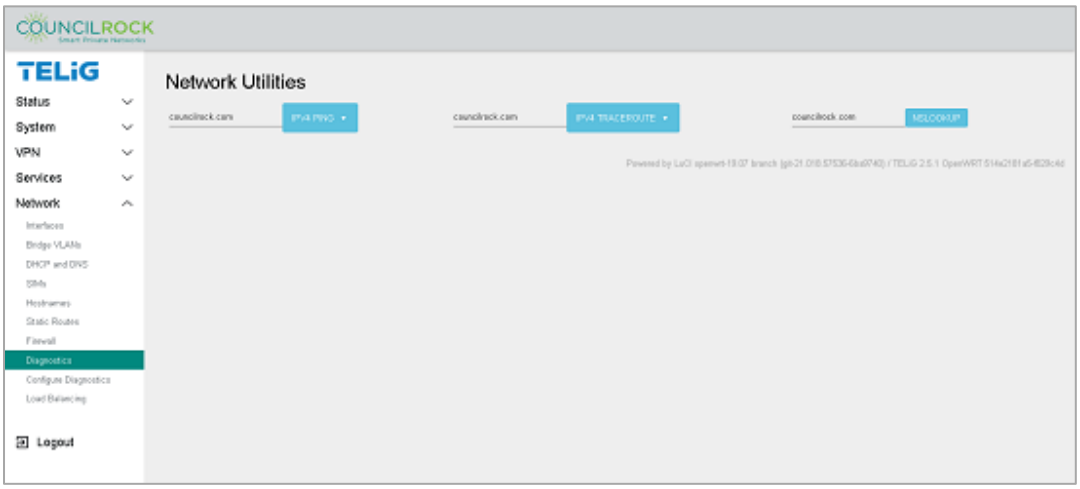

Figure 98: Network > Diagnostics

Configure Diagnostics

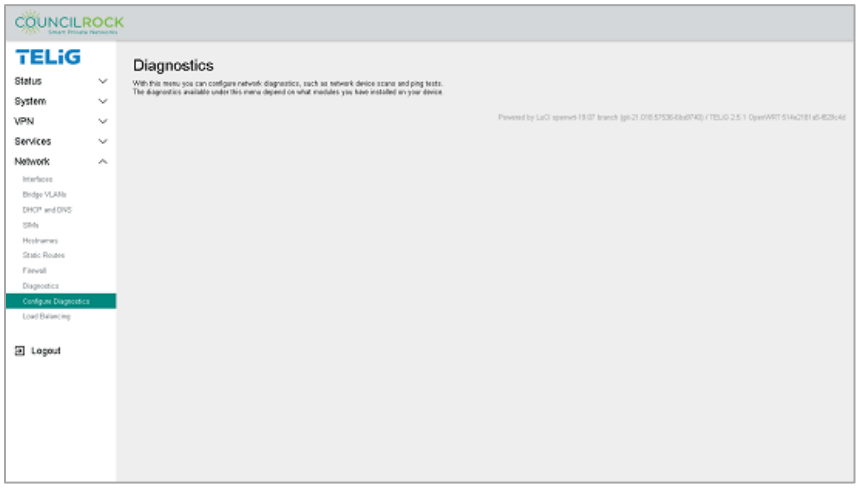

Figure 99: Network > Configure Diagnostics

NOTE: Out-of-the-box, the E1500 has no modules installed to display in *Configure Diagnostics*. See *Network > Diagnostics* for default tools – *ping*, *traceroute*, and *nslookup*. Use of other diagnostic tools are intended for advanced users only.

Load Balancing

See Use Case D: Radio Module Failover

Radio Specifications

Ordering Information

To order, contact sales@council-rock.com

Model Options

Model	Public LTE	Private LTE	LTE - CBRS	LTE Cat-M/NB-IoT	Private Enterprise Broadband 900MHz	2.5 / 5 GHz WiFi
E1500-L8N	X	X	X	X	X	
E1500-LW	X	X	X			X
E1500-8NW	X	X		X	X	X
E1500-8W	X	X			X	X

Table 8: Model Options

Hardware Summary

	E1500-L8N	E1500-LW	E1500-8NW	E1500-8W
Processor	ARM Cortex A9 Dual Core	ARM Cortex A9 Dual Core	ARM Cortex A9 Dual Core	ARM Cortex A9 Dual Core
Memory	1GB	1GB	1GB	1GB
Storage	8GB eMMC	8GB eMMC	8GB eMMC	8GB eMMC
DC Voltage	9-60VDC	9-60VDC	9-60VDC	9-60VDC
Ethernet Ports (10/100)	2	2	2	2
Serial Ports	1xRS-232 & 1xRS-232/485/422, RJ45 Connectors	1xRS-232 & 1xRS-232/485/422, RJ45 Connectors	1xRS-232 & 1xRS-232/485/422, RJ45 Connectors	1xRS-232 & 1xRS-232/485/422, RJ45 Connectors
GPS	Yes w/ Precision Time	Yes w/ Precision Time	Yes w/ Precision Time	Yes w/ Precision Time
Radio Slot 1 (m.2)	Radio A w/ 2x2 MIMO	Radio A w/ 2x2 MIMO	Radio B2 w/ 2x2 MIMO	Radio B2 w/ 2x2 MIMO
Radio Slot 2 (mPCIe center)	Radio B1 w/ 2x2 MIMO	none	Radio C w/ 1x1 SISO	none
Radio Slot 3 (mPCIe outside)	Radio C w/ 1x1 SISO	Radio F w/ 1x1 SISO	Radio F w/ 2x2 MIMO	Radio F w/ 1x1 SISO
RF Connector	6x SMA	4x SMA	6x SMA	4x SMA
Networks Supported	Private Enterprise Broadband 900MHz, FNN, CBRS, Verizon, AT&T, T-Mobile, Sprint	Verizon, AT&T, T-Mobile, Sprint	Private Enterprise Broadband 900MHz, Verizon, AT&T, T-Mobile, Sprint	Private Enterprise Broadband 900MHz, Verizon, AT&T, T-Mobile, Sprint
Waveforms	LTE, CAT-M/ NB IoT	LTE	LTE, CAT-M/NB IoT	LTE
Indicators	Red/Green LED for device status	Red/Green LED for device status	Red/Green LED for device status	Red/Green LED for device status
Size	4.8"W x 4.9"D x 1.9"H	4.8"W x 4.9"D x 1.9"H	4.8"W x 4.9"D x 1.9"H	4.8"W x 4.9"D x 1.9"H

Table 9: Hardware Summary

RF Specifications

[see also Model Options]

E1500 Model	Radio	Networks	Bands	Category
L8N LW	A	First Net, CBRS, Verizon, AT&T, T-Mobile, Sprint	1-5, 7-9, 12-14 18-20, 26, 28-30 32 41, 42, 43, 46 48, 66	Cat 12 DL Cat 13 UL
L8N	B1	Private Enterprise Broadband 900MHz, Verizon, AT&T, T-Mobile, Sprint	1-5, 7, 8, 12, 13 20, 25, 26, 29, 30 41	Cat 6 DL Cat 6 UL
8NW 8W	B2			
L8N 8NW	C	Private Enterprise Broadband 900MHz, Verizon, AT&T, T-Mobile	2, 4, 5, 8, 12, 13	Cat M/NB-IoT
LW 8NW 8W	F	Wifi	ISM	-

Table 10: RF Specifications

To order, contact sales@councilrock.com

Regulatory Info

Certifications

This device is certified under FCC Part 15b as an unintentional radiator. It has also been tested to IEEE1613 for use in electrical substations and conforms to UL standard #121201 and CSA Standard C22.2#213 for operation in Class I Division 2 Groups A-D, T4 hazardous locations.

Finally, this device is authorized for use on CBRS, Verizon, AT&T, and FirstNET.

Hazardous Locations

This device is approved:
Class I Division 2 Groups A-D.
T4, -40°C ≤ Tamb ≤ +62°C

Do not disconnect equipment unless power has been switched off or the area is known to be non-hazardous. Refer to Articles 500 through 502 of the National Electrical Code (NFPA 70) for further information on hazardous locations and approved Division 2 wiring methods.

FCC Notice

This device complies with part 15 of the FCC rules. Operation is subject to the condition that it does not cause harmful interference.

This device must be installed such that there is cabling of at least 20cm to the antennas. Additionally, the transmitters should be spaced 20cm apart.

The radios installed in the E1500 unit comply with Title 47 CFR Parts 15b of the Federal Communications Commission (FCC)

Important Information on Radio Exposure

The radio equipment described in this guide emits radio frequency (RF) energy. Professional installation is recommended. Although power levels are low, concentrated energy from directional antennas may pose a health hazard. More information is available online at https://www.fcc.gov/general/radio-frequency-safety-0.

Warranty

Council Rock warrants that under normal use and service each Product will conform in all material respects to Council Rock's specifications therefore and the hardware will be free from defects in materials and faulty workmanship. The warranty period ("Warranty Period") for new ordered Product is three (3) years from its original date of Delivery. The Warranty Period for repaired or replacement Product is ninety (90) days from its date of delivery to Purchaser or until the end of its original Warranty Period, whichever is longer.

If an item of hardware is or becomes defective during its Warranty Period, Council Rock will at its option either repair or replace the item. Purchaser must return each defective item to Council Rock, CIP, as defined in Incoterms 2000, destination airport advised by Council Rock, no later than thirty (30) days after the end of its Warranty Period. In making such a return, Purchaser will comply with Council Rock's Return Material Authorization (RMA) procedures. Council Rock will repair or replace such defective items at no additional charge to Purchaser and return the repaired or replacement item CIP, destination airport in the country stated in Purchaser's address in the Purchase Order. Title to each replacement item will pass to the receiving party on payment in full for the replacement item or, if no payment is due, on receipt by Purchaser.

During the Warranty Period, Council Rock will provide to the Purchaser Software maintenance releases that Council Rock makes generally available for the Software feature release licensed to Purchaser as part of the warranty program purchased by Purchaser.

Council Rock will have no obligation to replace or repair any Product or Software that is or becomes defective if such defects were the result of: (a) the Product or Software being altered, repaired or reworked by any party other than Council Rock without Council Rock's prior written consent; (b) Purchaser's or a third party's improper installation, maintenance or storage, mishandling, abuse or misuse of the Product or Software; (c) Purchaser's or a third party's use of the Product or Software in conjunction with equipment electronically or mechanically incompatible or of an inferior quality; (d) damage by fire, explosion, lightning, power failure, accident, any act of nature or other such event beyond Council Rock's control; (e) failure to implement a Software release or patch or other such solution provided or recommended by Council Rock; or (f) failure of consumable parts which includes, but is not limited to, fuses, bulbs and batteries. Council Rock will have no obligation to replace or repair any Product or Software that is received by Council Rock later than thirty (30) days after the end of its Warranty Period. Council Rock does not warrant that use of the Software will be uninterrupted or error free or that

all reported Software errors will be corrected. If on inspection by Council Rock of a returned item there is no fault found (NFF), Purchaser will pay Council Rock's then prevailing NFF charge and its transportation and insurance costs. Council Rock will charge Purchaser for any maintenance carried out which is not covered by the warranties contained in this Section at Council Rock's then prevailing standard rates for such Services.

The warranties set forth in this Section are in lieu of, and Council Rock hereby disclaims, all other warranty conditions, whether express or implied, including without limitation the implied terms of satisfactory quality and fitness for a particular purpose. The provisions of this Section set forth Council Rock's entire obligation and Purchaser's sole remedy under the warranties set forth in this Section

Customer Support Services. During the Warranty period, Purchaser shall obtain support services for the Products by electing to receive Warranty Plus services as offered by Council Rock, if Purchaser has paid to Council Rock the support fee for such services.

Appendix A:

CONFIGURATION FUNDAMENTALS

The basic setups in this section can be thought of as the building blocks of an E1500 system configuration. More complicated system setups generally depend upon these fundamental configurations.

Fundamentals A: SIM card installation

Initial setup of the unit requires SIM card installation prior to powering up. This section describes SIM card installation. SIM cards slots are a nano SIM 4FF form factor.

Tools Needed

- T10 Torx bit
- Tweezers

OPENING THE UNIT

1. Unscrew the four (4) corner screws and lock washers from the unit's rear panel
2. Remove the rear panel and Locate the SIM slots on the left side of the upper circuit board. When viewed from the back slot 1 is on the left, slot 2 is on the right

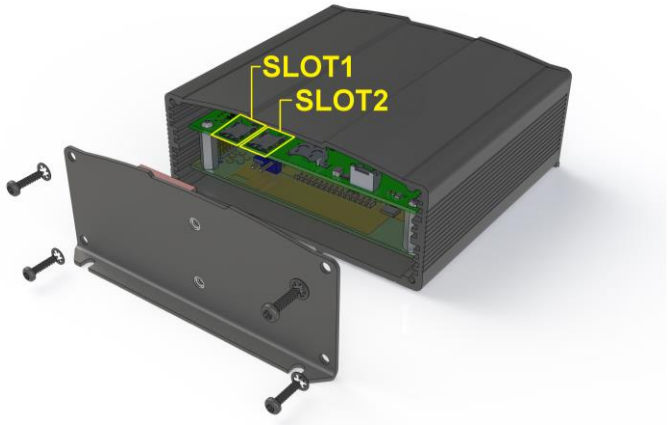

Figure A.A.1: Rear Panel removal

INSTALLING SIM CARDS

3. Using tweezers, insert the SIM cards in slots 1 and 2.

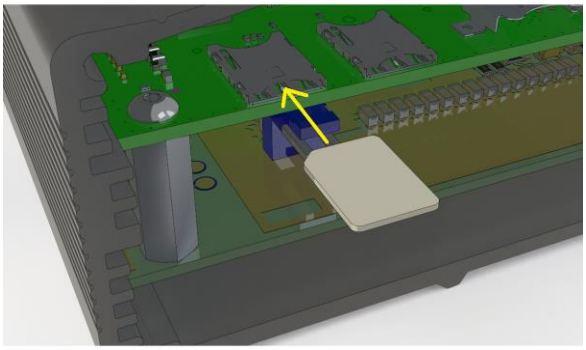

Figure A.A.2: SIM card insertion

CLOSING THE UNIT

4. Replace the rear panel and reattach corner screws and lock washers

> NOTE: See "Initial Setup: Web Admin - step 5" for details on SIM card interface configuration.

REMOVING SIM CARDS

A 'pick' of sorts is needed to remove SIM cards that have previously been installed. Any type of pick with a 90-degree bend at one end should suffice. Gently hook the pick onto the back edge of the SIM card and pull the card out enough to remove it with tweezers.

Fundamentals B: LAN Interface config

To set up the E1500 LAN interface according to your network plan,

Interface settings are defined via the *Network* > *Interfaces* menu, by clicking on the EDIT button on a LAN interface and selecting the *General* tab. The LAN interface status is displayed in a highlighted box, showing the Device name, Uptime, MAC address, Total received / transmitted packets (RX/TX), and the IP Address in CIDR notation.

- Static / Dynamic Protocol
- Bring up on Boot
- IP address and Subnet Mask (IPV4 and IPV6)
- Gateway address (IPV4 and IPV6)
- IPV4 broadcast address
- Custom DNS server settings
- IPV6 Assignment length, address, gateway, routed prefix, and suffix

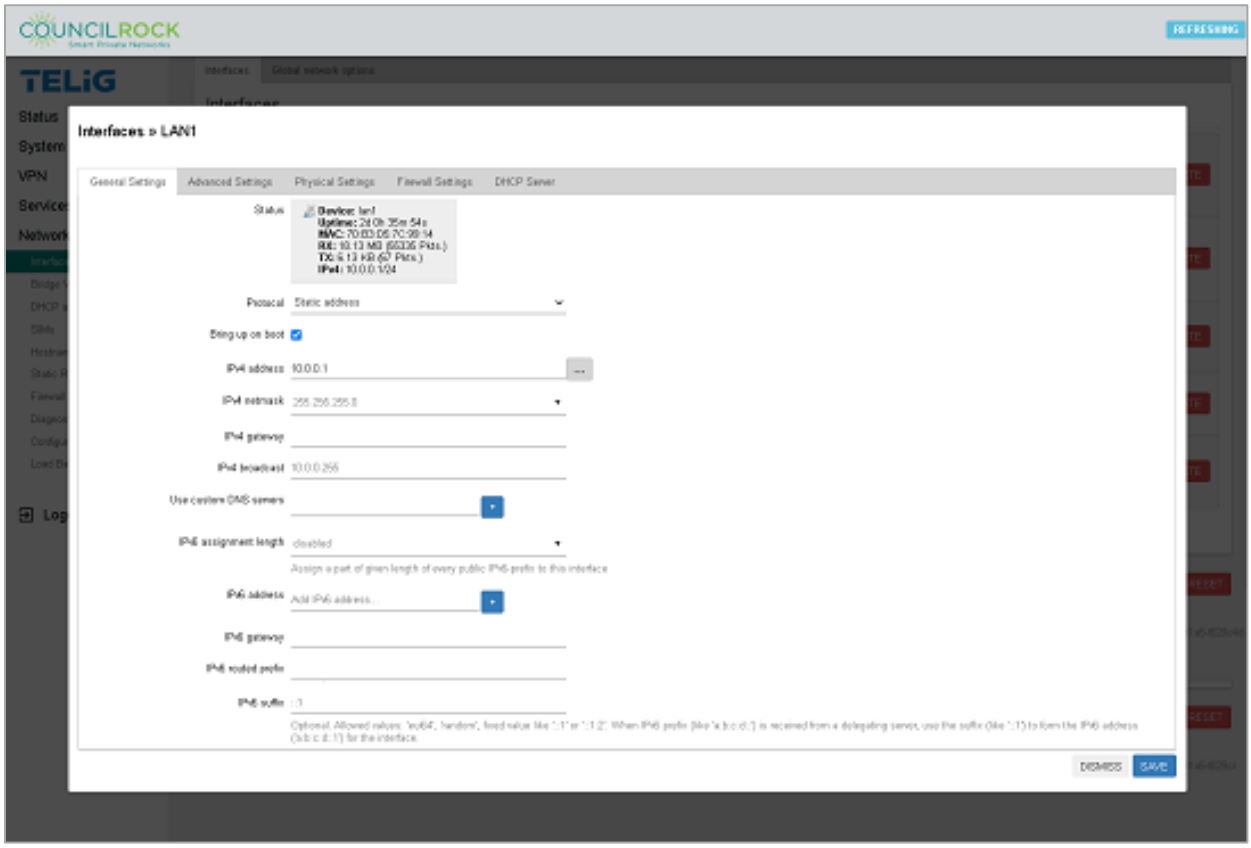

Fig. A.B.1: LAN Interface General Settings

The *Advanced Settings* tab has settings for:

- [Checkbox] – Use built-in IPv6 Management
- [Checkbox] – Force link (to ignore carrier sense events)
- Overriding the unit's MAC address
- Overriding the default Maximum Transmission Unit (MTU) - packet size (for advanced users only - we recommend the default MTU setting)
- Using a gateway metric - Gateway metric defines the value that is assigned to an IP route for a network interface that identifies the cost that is associated with using that route. If the device has two routes to the same destination, the route with the lower metric will be preferred. The default value of 0 is usually the recommended setting for the LAN interfaces as the routes advertised by the LAN are usually "connected" routes.

NOTE: Built-in IPv6 management enables IPv6 prefix delegation for cases of IPv6 traffic tunneling over IPv4 networks.

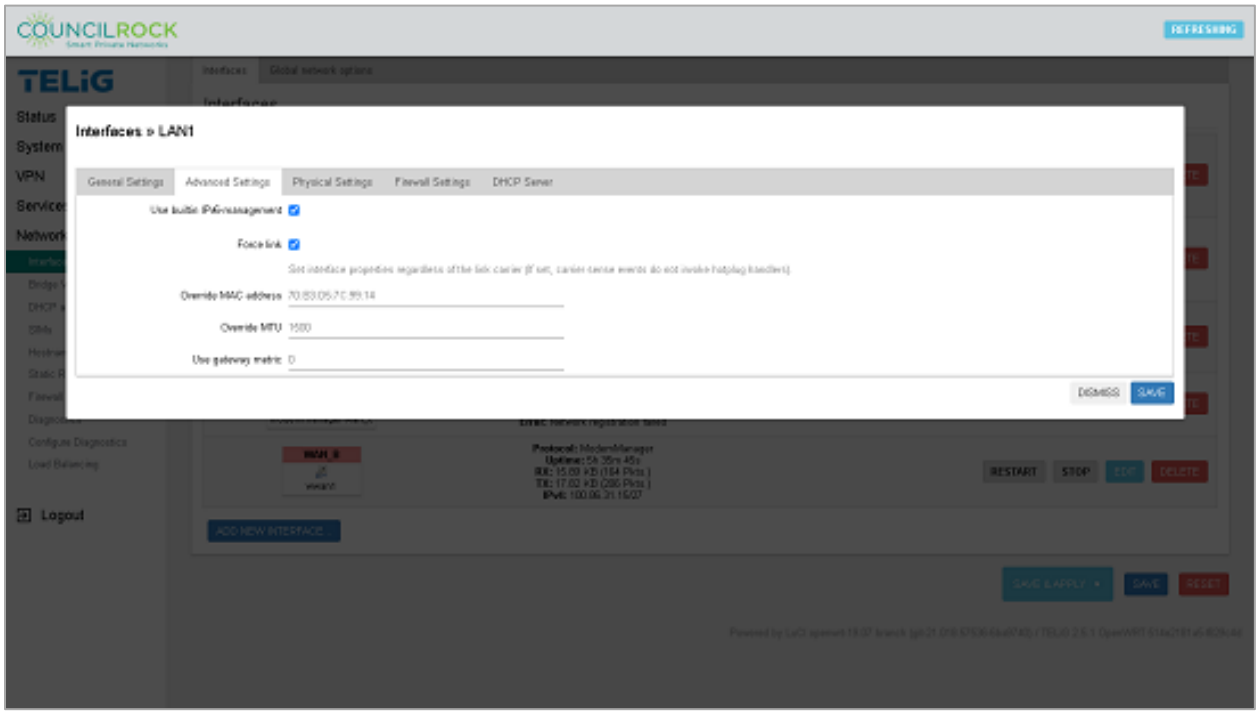

Fig. A.B.2: LAN Interface Advanced Settings

Verify the LAN is always in the LAN firewall zone on the *Firewall Settings* tab. For more, see [Fundamentals C: WAN Interface config]

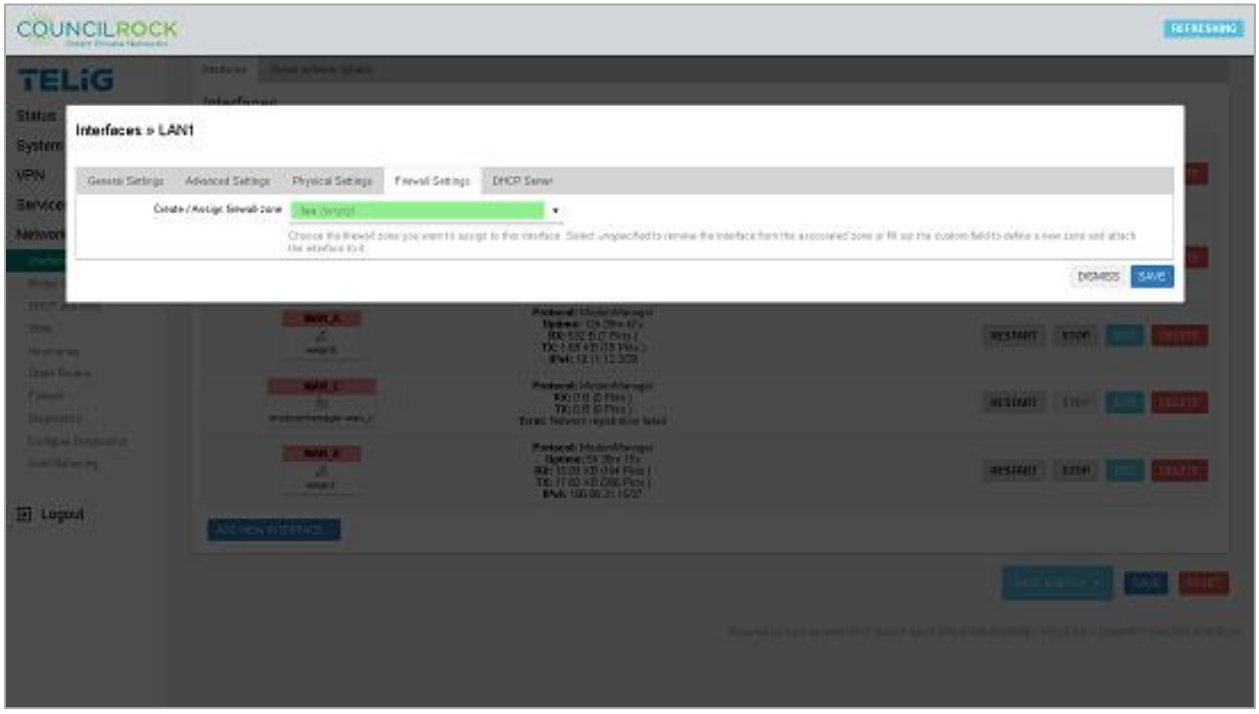

Fig. A.B.3: LAN Interface Firewall Settings

Your network deployment settings will vary from the example screenshots shown here (mainly IP addressing schemes / netmasks / gateways, but may also include settings such as bridging, firewalls, and DHCP servers). Enter your specific network details on each applicable menu tab and click Save.

Fundamentals C: WAN Interface config

To set up the E1500 WAN interface according to your network plan,

Interface settings are defined via the *Network* > *Interfaces* menu, by clicking on the EDIT button on a WAN interface and selecting the *General* tab. The WAN interface status is displayed in a highlighted box, showing the Device name, Uptime, Total received / transmitted packets (RX/TX), and the IP Address in CIDR notation.

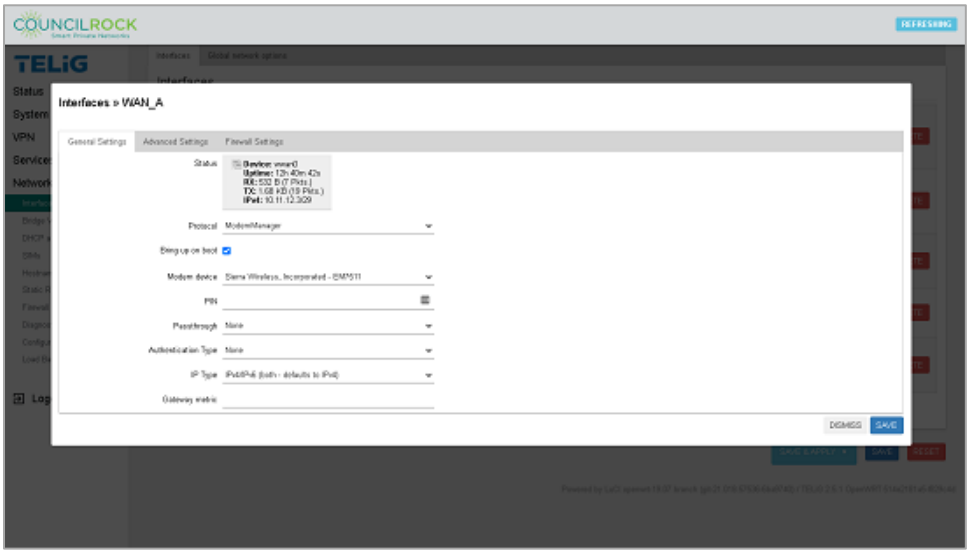

Fig. A.C.1: WAN Interface General Settings

- **Protocol** - Defines how the device communicates with the LTE modem. *Modem Manager* is the recommended protocol option for all modems
- **Bring up on boot** – Checkbox option to start the interface when the unit boots up
- **Modem device** - Defines which LTE modem is associated with the interface. Default selection is the recommended setting for general use
- **PIN** - for PIN protected SIM cards
- **Passthrough** - Shares WAN IP address with a single device on the LAN
- **Authentication Type** - Defines authentication methods with the WAN network provider (if required)
- **IP Type -** (IPv4 / IPv6)
- **Gateway metric** - In networks where multiple WAN interfaces are configured as default gateways, the Gateway metric determines which default gateway will be utilized. In these multiple default gateway networks, the default gateway with the lowest Gateway metric is used

The *Advanced Settings* tab has settings for:

- Using built-in IPv6 management
- Force link (to ignore carrier sense events)
- Overriding the default Maximum Transmission Unit (MTU) - packet size (for advanced users only - we recommend the default MTU setting)
- Using the unit as a default gateway.

> NOTE: "USE AS DEFAULT GATEWAY"
> Checking this box sets the interface as the outgoing node for any packet whose destination IP is not on the routing table. A user may configure multiple default gateways. However, be sure to give them different metrics using the Advanced Setting "Gateway metric". The device will use the default gateway with the lowest metric.

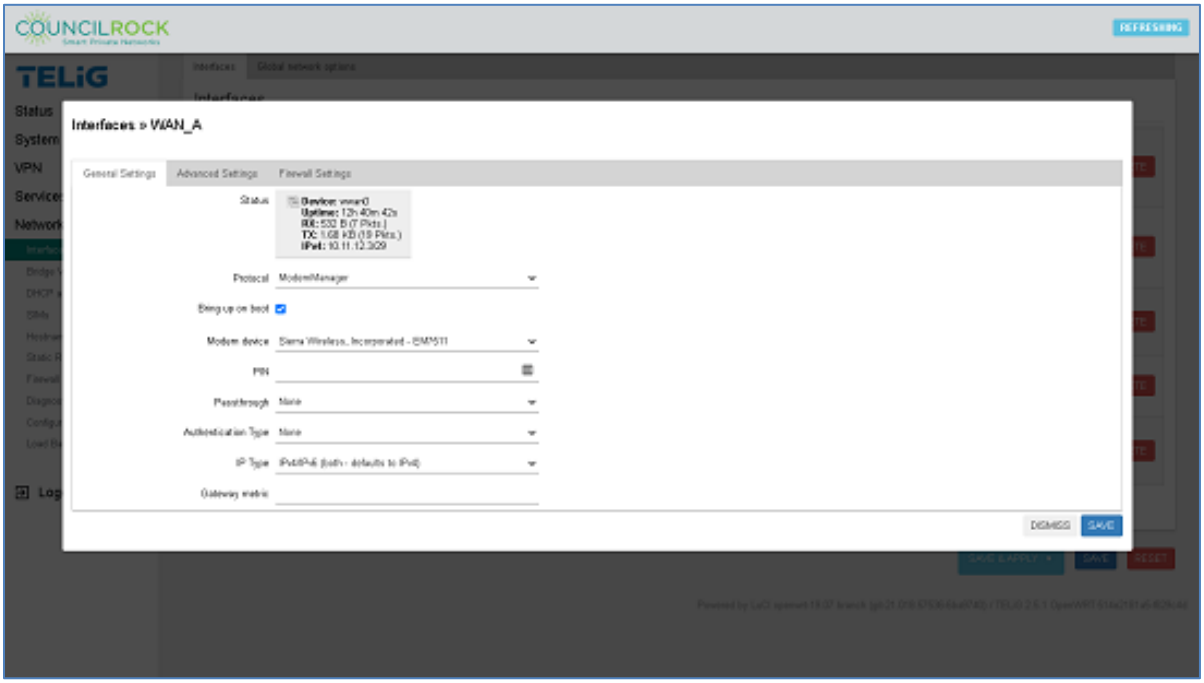

Fig. A.C.2: - WAN Interface Advanced Settings

Verify the WAN is always in the WAN firewall zone on the *Interfaces >> WAN_x > Firewall Settings* menu.

NOTE: A zone can be configured to any set of interfaces but generally there are at least two zones for the sake of simplicity: lan for the collection of LAN interfaces and wan for the WAN interfaces. In most cases users generally want to allow/prevent the same type of traffic in & out of the LAN/WAN interfaces therefore it makes sense to group interfaces of the same type in the same zone.

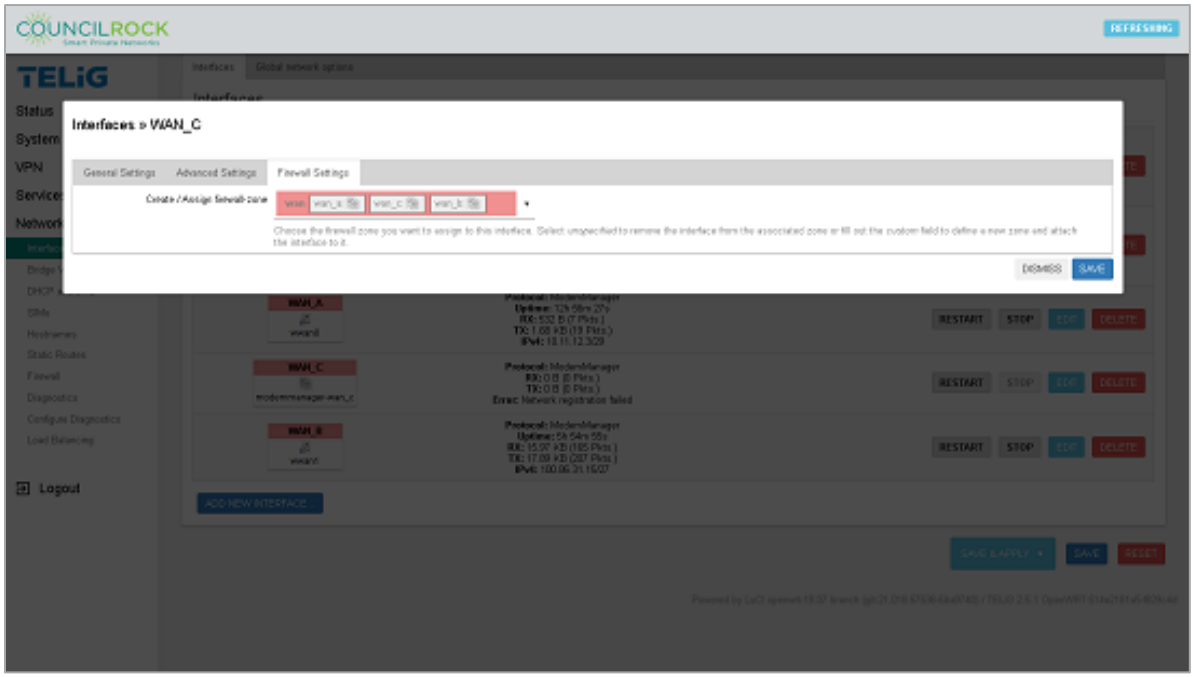

Fig. A.C.3: WAN Interface Settings

Your network deployment settings will vary from the example screenshots shown here (mainly IP addressing schemes / netmasks / gateways, but may also include settings such as bridging, firewalls, and DHCP servers). Enter your specific network details on each applicable menu tab and click Save.

Fundamentals D: System Administration

This section covers basic and advanced system administration topics.

Changing User / Passwords
The password for the device can be changed by navigating to *System* > *Administration* > *Router Password*.

The password policy is:

Length: minimum 18 characters
Requirements:

- 1 lower case letter
- 1 upper case letter
- 1 number
- 1 special character

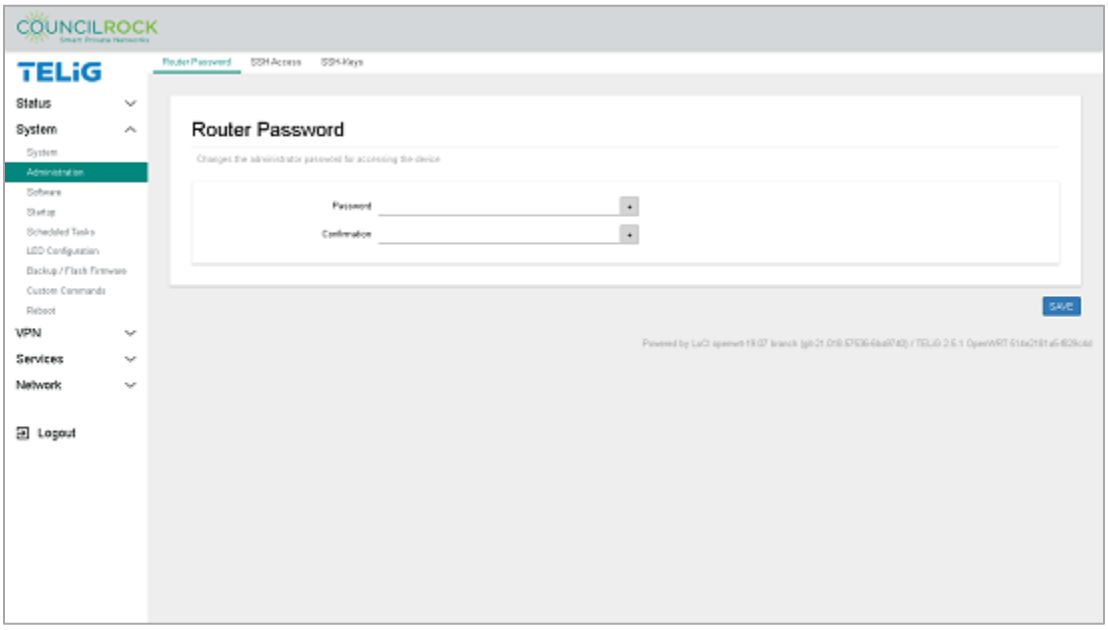

Fig. A.D.1: System > Administration > Router Password

> **Warning:** *The following topics are intended only for Advanced Users.*

Remote System Logging Configuration:
Allows the user to configure the unit to send logs to an external syslog server.

By default, system logs are stored locally as a text file continually updated during system events. The *System > System: Logging* page allows the user to specify logging parameters, detailed below. The amount of system log entries, and therefore the rate at which the log is updated is determined by the log output level, which is selected on this screen under *Log output level*. For external log servers, setting up the server's config files to receive logging data (passed by TCP/UDP) is an advanced user topic.

For more information, see https://openwrt.org/docs/guide-user/base-system/log.essentials

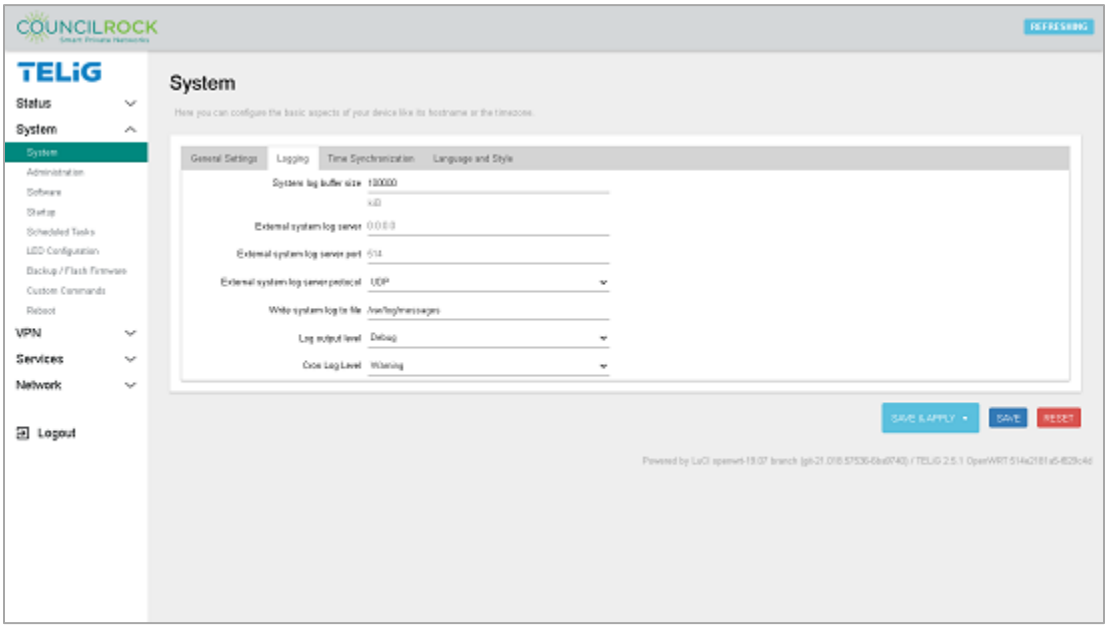

Fig. A.D.2: System > System: Logging

System log buffer size: Specifies how much memory to allocate for saving logs in the unit. When allocated memory is used up, the system will overwrite old messages.

External system log server: The IP address of the syslog server that the logs will be sent to.

External system log server port: The transport layer port of the syslog server that the logs will be sent to.

External system log server protocol: The transport layer protocol that will be used to send syslog messages to the external server.

Write system log to file: local directory in the device where the syslog messages will be stored. Leave default value

Log output level: Syslog logging level. Levels are shown in the dropdown list in order from least to most important. Thus, for a minimal log, select "Error" level or higher. For a more verbose log, select "Warning" or lower.

Cron Log Level: Logging level for Cron jobs. Selections are "Debug", "Normal" and "Warning". For a verbose Cron log, select "Debug". For a minimal Cron log, select "Warning"

Disabling Unused Services:

To disable scripts for services that are executed automatically when the unit powers up, navigate to *System > Startup*. Here you can disable the desired scripts. This feature is intended only for advanced users.

Uninstalling Unused Packages:

To uninstall packages from the unit, navigate to *System > Software*. Click on "update list" to fetch the packages installed in the unit and then go click the "Installed" tab. Here you can remove unwanted packages. This feature is intended only for advanced users.

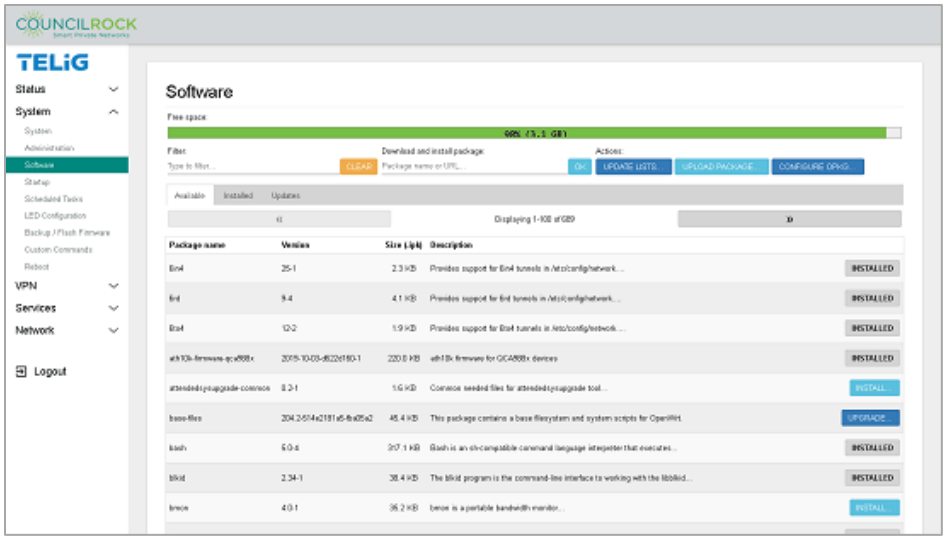

Fig. A.D.3: System > Software > Installed

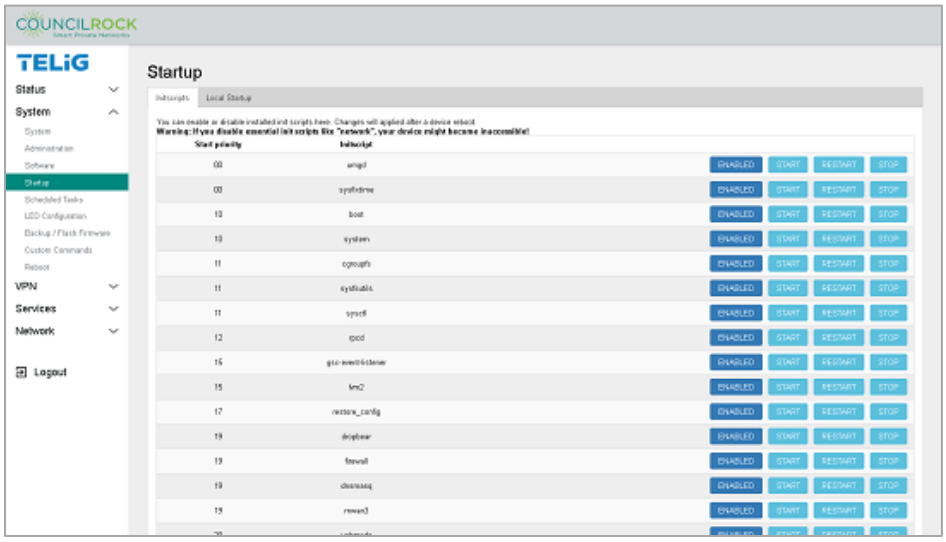

Fig. A.D.4: System > Startup > Initscripts

Appendix B:

USE CASES

Use Case A: Serial Connection via WAN

Example: Connect the E1500 to a device via serial / RS232 with DNP and send device traffic to the Enterprise Network through WAN A

Requirements**:**

Fundamentals C: WAN interface config

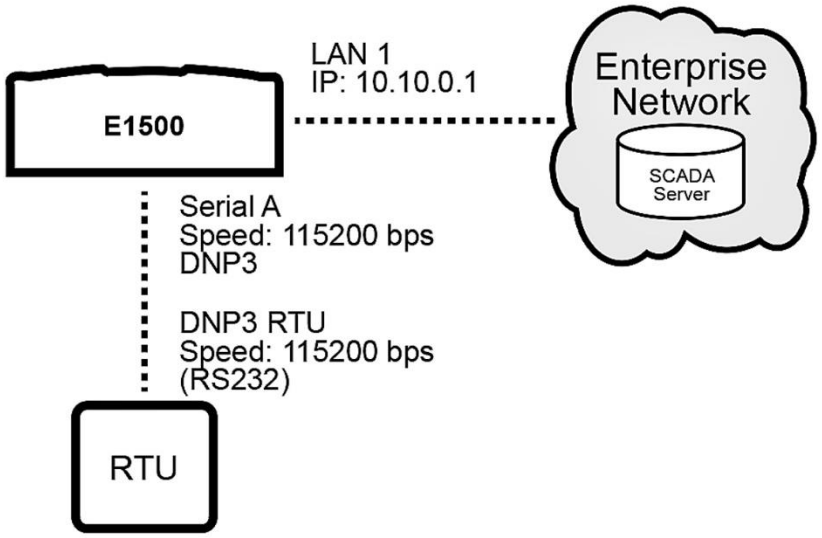

Figure B.A.1 – Serial to WAN concept diagram

Steps**:**

1. Navigate to *Services > Serial Gateways* and set configuration for Serial A
    a. Protocol: RS232
    b. Gateway: DNP3
    c. Baud Rate: 115200
    d. Parity: None
    e. Data Bits: 8
    f. Stop Bits: 1
    g. TCP Port: 20000
    h. TCP Listener Enabled: check

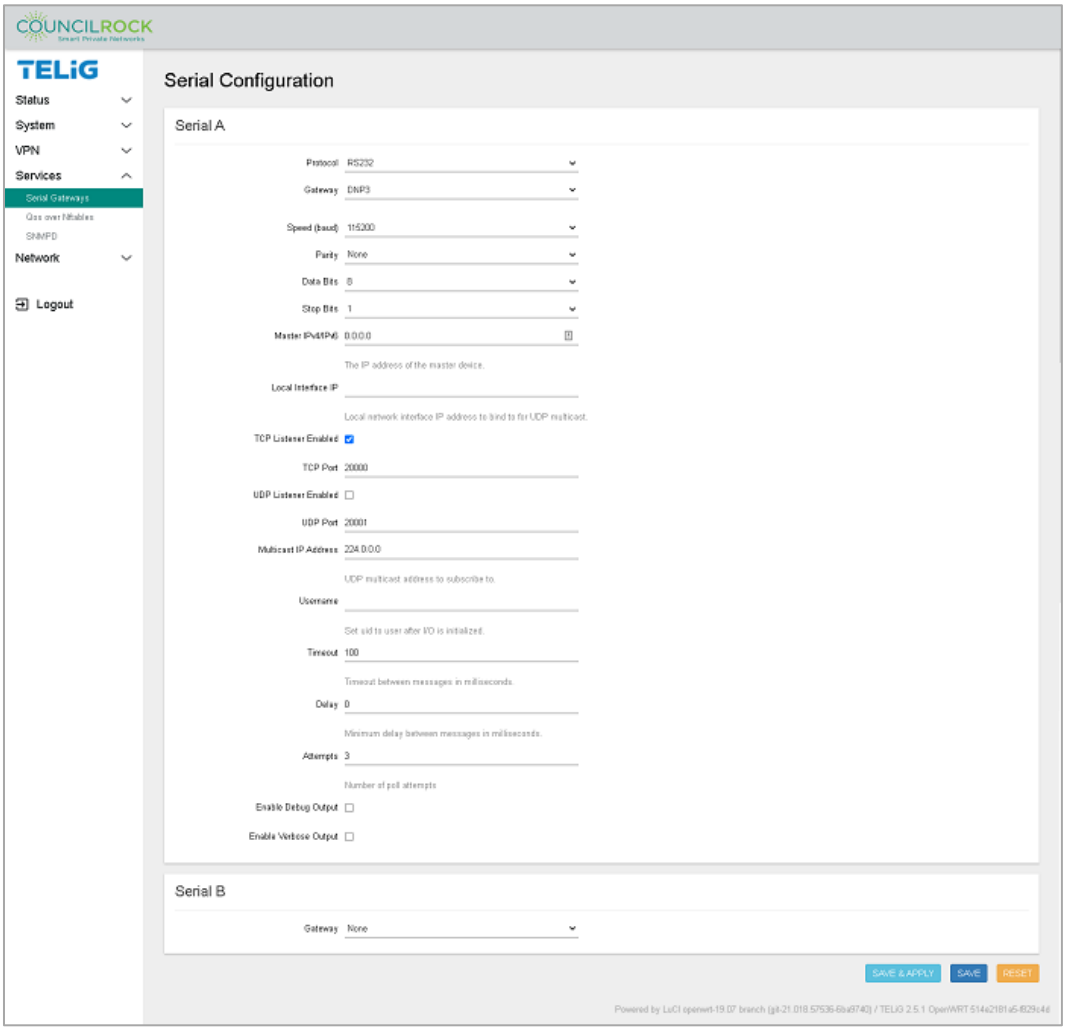

Figure B.A.2 - Services > Serial Gateways

- **Master IPV4/IPV6**: IP address of the master device. The master device is the device that polls the end devices or "slaves"
- **TCP Listener Disabled**: If checked, the device does not open the defined TCP port to listen for connections
- **UDP Listener Disabled**: If checked, the device does not open the defined UDP port to listen for connections
- **Multicast IP address**: Enter here the multicast IP address to subscribe to in case the DNP master is configured to send UDP multicast messages to a group of slave devices
- **Local Interface IP**: Local network Interface for sending multicast messages
- **Username**: The user to execute the application in the OS of the device. Be sure the username entered has administrative privileges; "root" for example.

Use Case B: LAN to WAN traffic

Example: Configure the E1500 to route traffic between radio ports (WAN A / WAN B) and ethernet port (LAN 1) as shown in Figure 2.1. Set WAN load balancing to WAN A 60% / WAN B 40%.

Requirements:

Fundamentals B: LAN interface config
Fundamentals C: WAN interface config

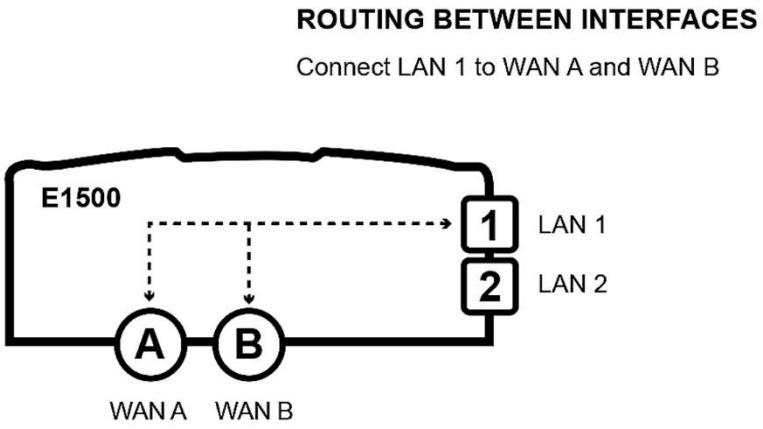

Figure B.B.1- LAN to WAN concept diagram

Steps:

1. Set up the LAN to WAN firewall zone:
    - Navigate to *Network > Firewall > General Settings*
    - Under Zones, click ADD and set the following (See Fig. B.B.2)
        - Name: lan
        - Input / Output / Forward: accept
        - Covered Networks: select available lan(s) to include in this zone

      (Input / output / forward fields set the default policies for traffic entering and leaving the firewall zone)
    - Click SAVE

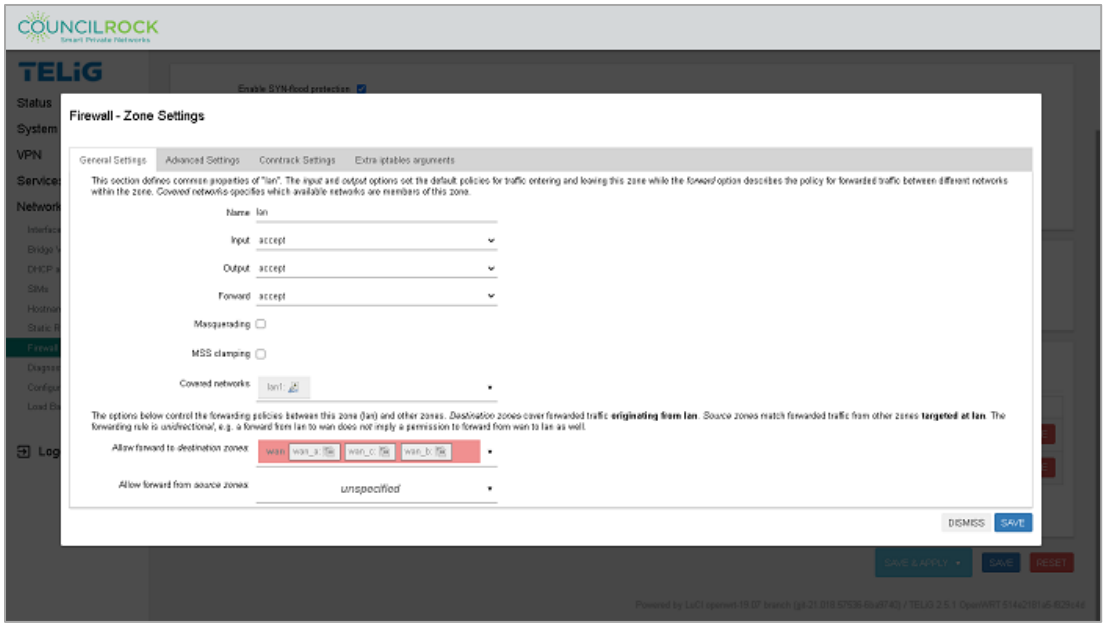

Figure B.B.2 - Firewall Zone Settings: lan

2. Set up Load Balancing
    A. Configure interfaces
    - Navigate to *Network > Load Balancing: Interfaces*
    - Add/Select the MWAN Interface for wan_a and set up as shown in Figure B.B.3.
        - Enabled: checked
        - Initial State: Online
        - Internet Protocol: IPv4
        - Tracking method: ping
        - Tracking hostname or IP address:
            - Enter the hostname or IP address of the node to ping to determine if the link is up or down
            - Leaving this blank assumes the interface always online
            - For demo purposes, you can use 8.8.8.8 (Google's DNS server)
        - Tracking reliability: 1
        - Ping count: 1
        - Ping size: 56
        - Max TTL: 60
        - Check link quality: unchecked
        - Ping timeout: 2 sec
        - Ping interval: 5 sec
        - Failure interval: 5 sec
        - Keep failure interval: unchecked
        - Recovery interval: 5 sec

- Interface down: 3
- Interface up: 3
- Flush conntrack table: all unchecked
- Metric: this is not an input, just for display

- Click SAVE & APPLY
- Click the *Interfaces* Tab to return to the MWAN - Interfaces view and repeat the setup for wan_b

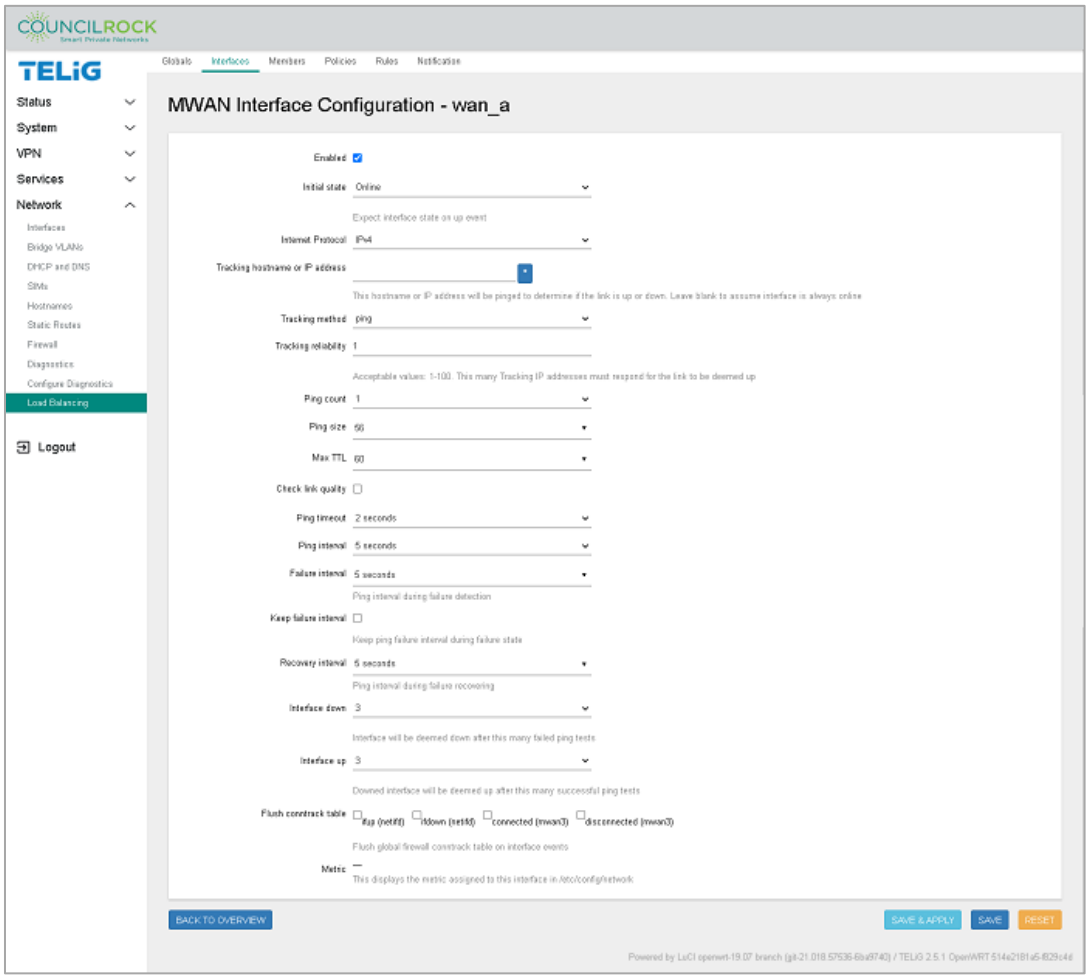

Figure B.B.3 - MWAN Interface wan_a Load Balancing configuration

B. Configure MWAN Members with Load Balancing settings

- Navigate to the *Members* Tab
- On the text input line next to the ADD button enter “wan_a_main” (In this example we use *wan_a_main* to indicate the high priority member for load

balancing and *wan_a_secondary* to indicate the low priority member for load balancing)

- Click ADD to open the *MWAN Member Configuration* window for wan_a_main. Enter the following settings (See Fig. B.B.4)
  - Next to “Interface” click on - - Please choose - -
  - Select wan_a
  - Metric = 1 (Metric is used as a sorting measure. If a packet that is about to be routed fits two rules, the one with the lower metric is applied)
  - Weight = 60 (load balance percent)
  - Click SAVE & APPLY, then BACK TO OVERVIEW
- Repeat the step above, adding a new member “wan_b_secondary” (See Fig. B.B.5)
  - Interface: wan_b
  - Metric = 1
  - Weight = 40
- Click SAVE & APPLY followed by BACK TO OVERVIEW
- *MWAN Members* window displays the load balancing scheme (See Fig. B.B.6)

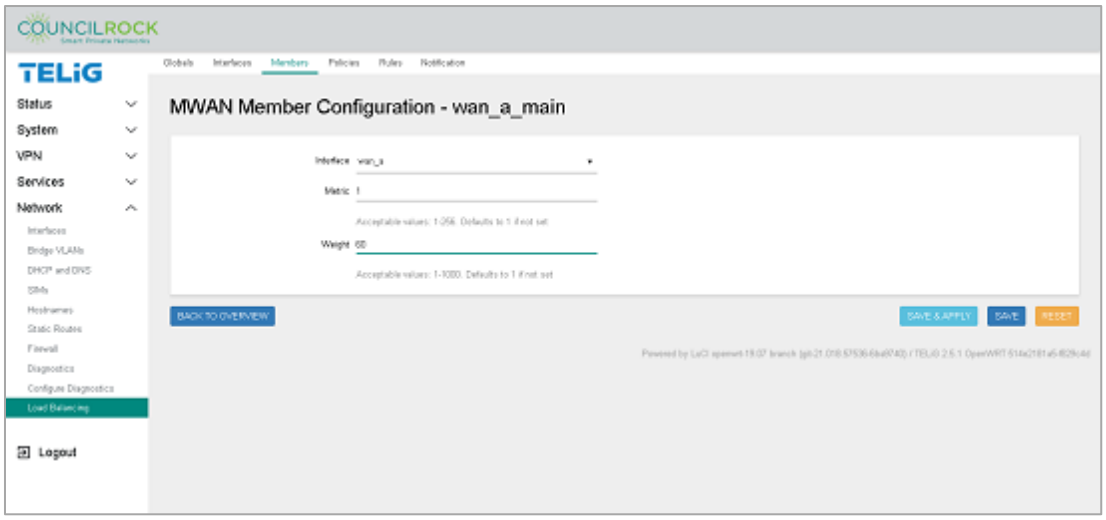

Figure B.B.4 - Member Configuration to set Load Balancing (Weight) on wan_a

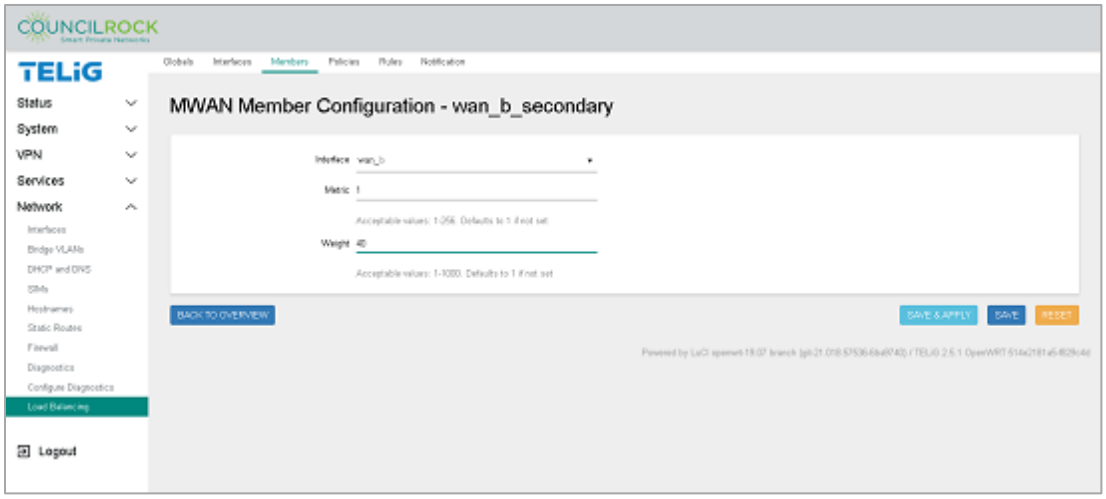

Figure B.B.5 - Member Configuration to set Load Balancing (Weight) on wan_b

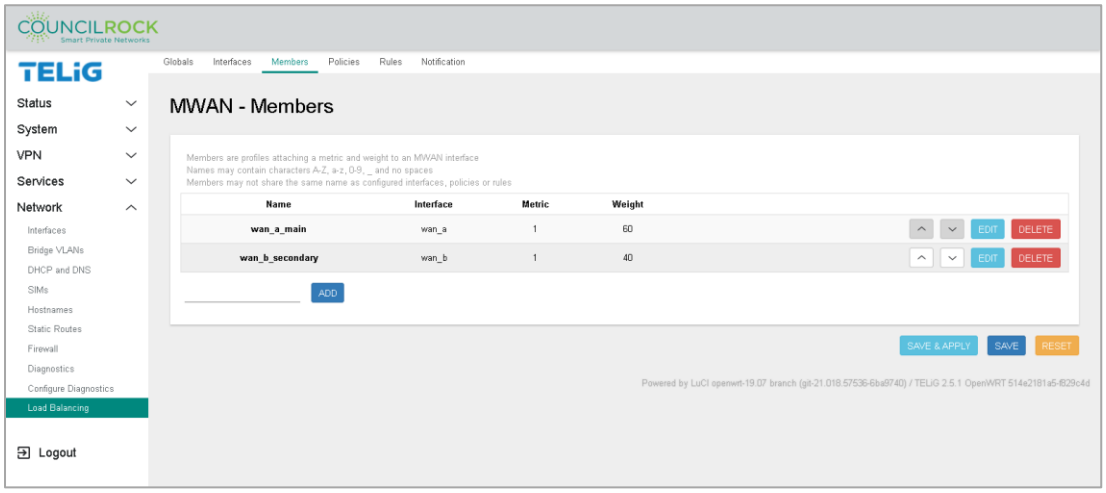

Figure B.B.6 - Member Configuration summarizing Members Load Balancing

C. Add a Load Balancing Policy

- Navigate to the *Policies* Tab
- On the text input line next to the ADD button enter “main_policy”
- Click ADD to open the *MWAN Policy Configuration* window for main_policy
  - Next to “Member used” click on - - Please choose - -
  - Select wan_a_main (See Fig. B.B.7)
  - Repeat to select wan_b_secondary
  - Last resort: unreachable (reject) – this is the default setting
  - Click SAVE & APPLY then BACK TO OVERVIEW
- MWAN Policy displays the Policy (Fig. B.B. 8)

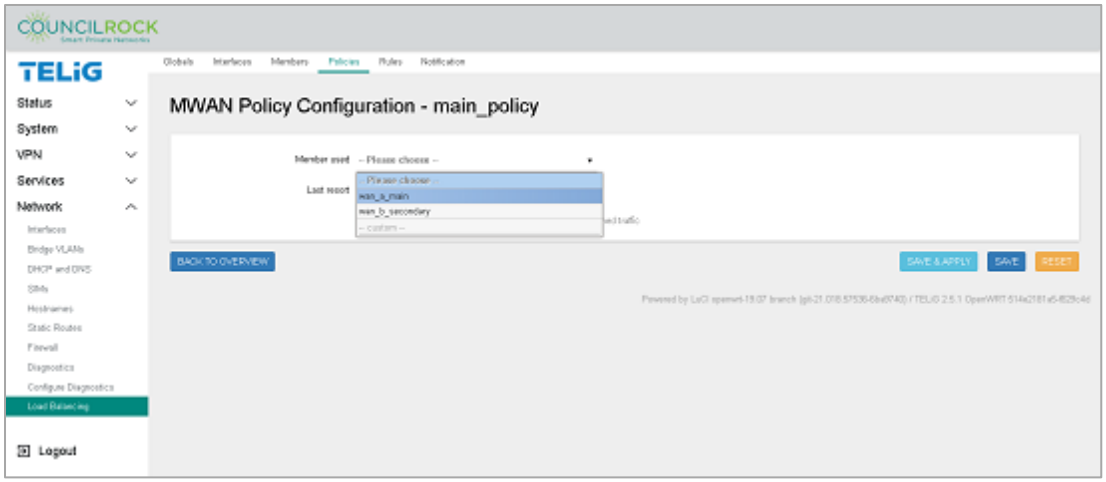

Figure B.B.7 - Load Balancing Policy Configuration: Member selection

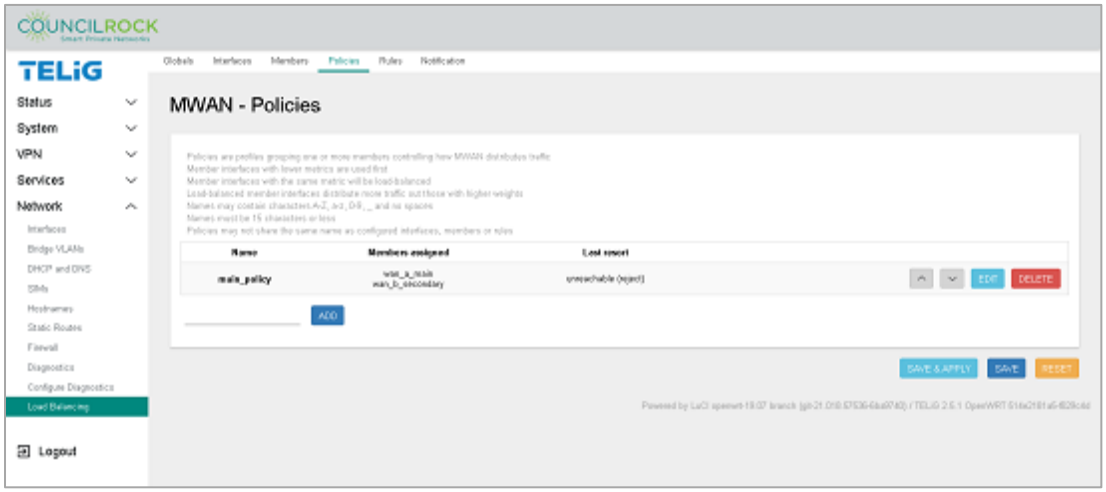

Figure B.B.8 - Load Balancing Policy Configuration: Policy settings

D. Add a Load Balancing Rule to the Load Balancing Policy
   - Navigate to the *Rules* Tab
   - On the text input line next to the ADD button enter “wan_a_rule”
   - Click ADD to open the *MWAN Rule Configuration* window for wan_a_rule
     - Source address: 10.0.0.1/24
     - Policy assigned: main_policy
     - All other fields use the default settings for this example
     - Click SAVE & APPLY then BACK TO OVERVIEW
   - MWAN - Rules displays the Policy

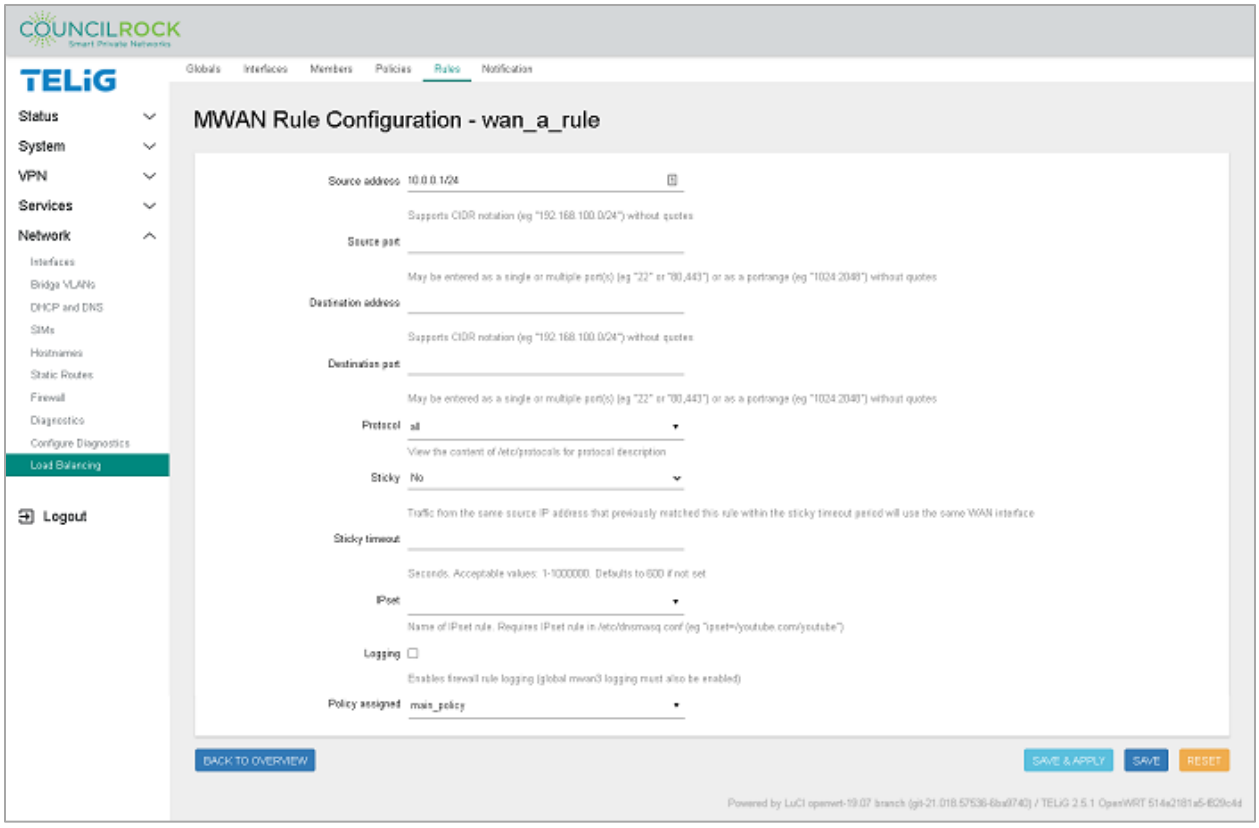

Figure B.B.9 - Load Balancing Rule Configuration using Load Balancing Policy

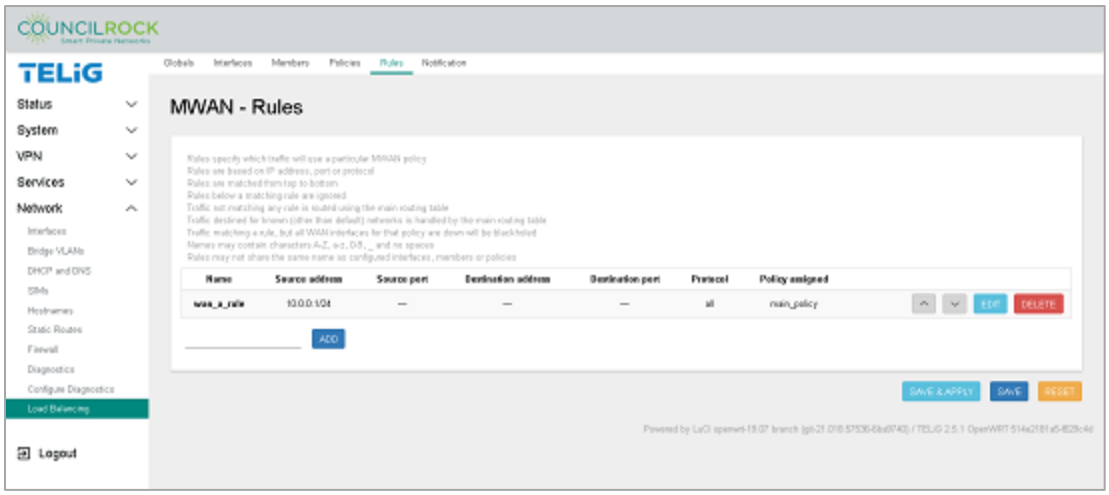

Figure B.B.10 - Load Balancing Rule Summary using Load Balancing Policy

Use Case C: SIM Failover

Example**:** Configure the E1500 to switch between SIM cards based on signal quality or network connectivity. Check connectivity every 5 minutes.

> NOTE: SIM failover is only available on dual-SIM units. The menu options shown in this section are not available on single-SIM units.

When the primary SIM card's network fails, the interface switches to the secondary SIM card. Network failure is tested against criteria of any of the following conditions:

- Network connectivity
- RSSI threshold criteria (-90dBm in the example)
- IP ping tests to a device

Criteria are tested at regular intervals (5 min in the example). Note that different intervals can be set for different criteria depending on user needs & preferences.

Requirements: Fundamentals B: WAN interface config

Steps**:**

1. Navigate to *Network* > *SIMs* and note the interface name, slot numbers, and Names of SIM cards in the unit.
2. In the *SIM Failover* section, check "*Enable SIM Failover*" to show failover options
    - Current SIM: The SIM that is currently active. With or without a failover configuration, the user can set the active SIM here.
    - Primary SIM: The SIM that is primary for failover purposes
    - In the dropdown next to *Failover based on*, select all three options
        i. Connection Availability
        ii. Signal Strength
        iii. Network Availability
3. Set Connection Availability criteria
    - Connection Availability Timeout [min]: 5
4. Set Signal Strength criteria
    - Signal Strength Timeout [min]: 5
    - Minimum RSSI [dBm]: -90
5. Set Network Availability criteria
    - Network Availability Timeout [min]: 5
    - Network Ping Address: 8.8.8.8

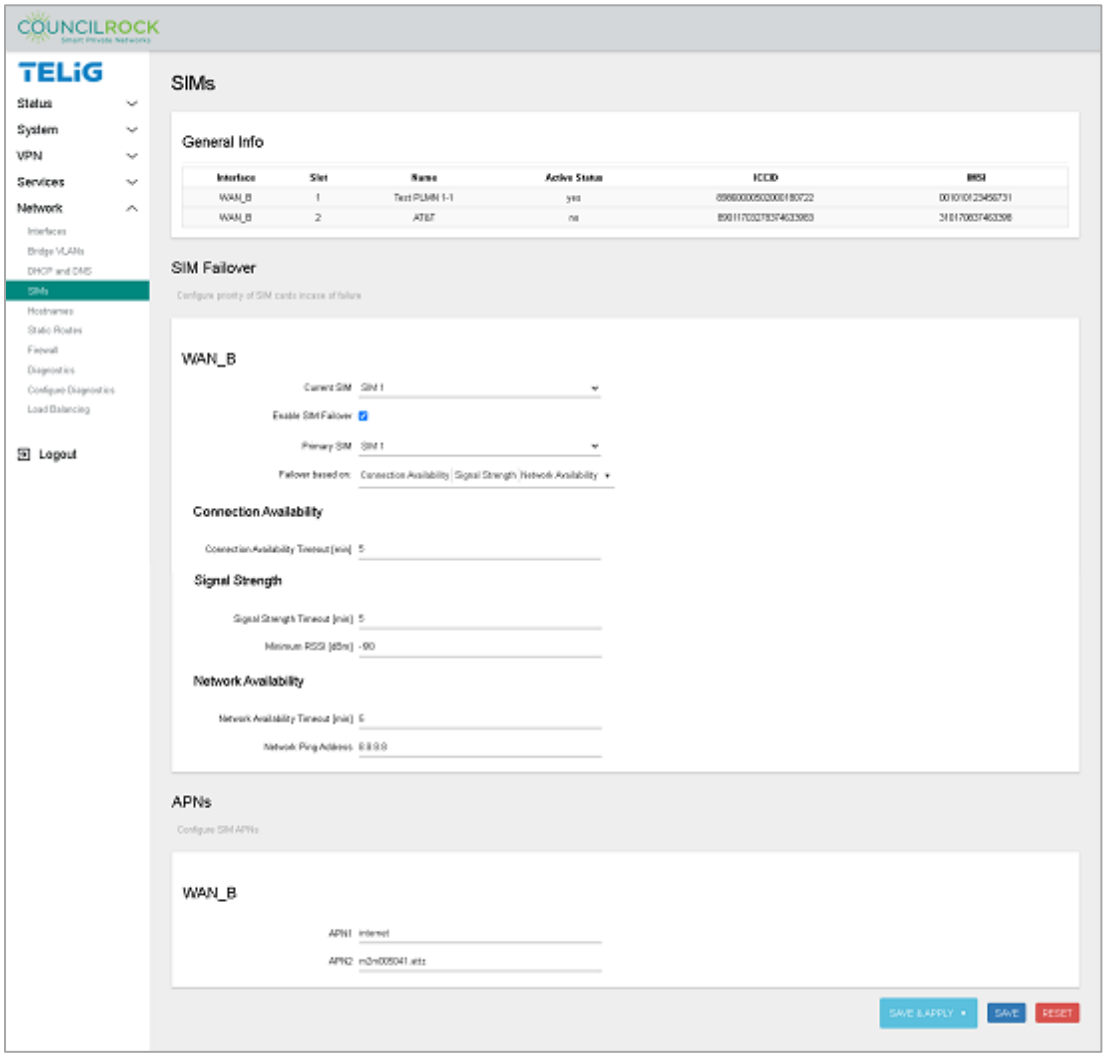

Figure B.C.1 - Network > SIMs: SIM Failover

NOTE: Network Ping Address shown here is for example only. An appropriate Ping Address for your network deployment should be entered here.

NOTE: After a primary SIM failover event, the 'non-primary' SIM becomes the Current SIM. The user can reset the failover by manually switching the Current SIM back to primary.

Use Case D: Radio Module Failover

The network balancing feature of the E1500 allows outbound WAN interface traffic to be load balanced over multiple WAN interfaces based on a numeric weight assignment. The user can also configure interfaces as main/backup WANs.

The user can configure the device to monitor each WAN connection using repeated ping tests thus allowing the device to automatically route traffic to another WAN interface if the main WAN interface loses connectivity.

Example: Configure the device to perform automatic radio module failover from a main WAN interface to a backup WAN interface

Steps:

1. Navigate to *Network > Load Balancing > Interfaces*
2. Add wan interfaces. Be mindful that the names of WAN interfaces you are going to add must match the WAN interface names in the *Network > Interfaces* menu. Names are case sensitive. For this example, we use "wan_a" and "wan_b"
3. Configure wan_a as described below. Generally, the default values are used, only the Tracking hostname or IP address needs to be entered

> NOTE: in some scenarios the "Tracking hostname or IP address" may need to be changed. For example, if wan_a is connected to a network with no internet access, IP 8.8.8.8 might not be reachable, therefore a different IP address must be configured as the tracking IP.

wan_a configuration:

- Enabled: checked
- Initial State: Online
- Internet Protocol: IPv4
- **Tracking hostname or IP address: 8.8.8.8** (for demo purposes, we use Google's DNS server)
- Tracking method: ping
- Tracking reliability: 1
- Ping count: 1
- Ping size: 56
- Max TTL: 60
- Check link quality: uncheck
- Ping Timeout: 2

- Ping interval: 5
- Failure interval: 5
- Keep failure interval: uncheck
- Recovery interval: 5
- Interface down: 3
- Interface up: 3
- Flush conntrack table: uncheck all
    i. ifup
    ii. ifdown
    iii. connected
    iv. disconnected
- Metric: this value is for display only, no data to enter

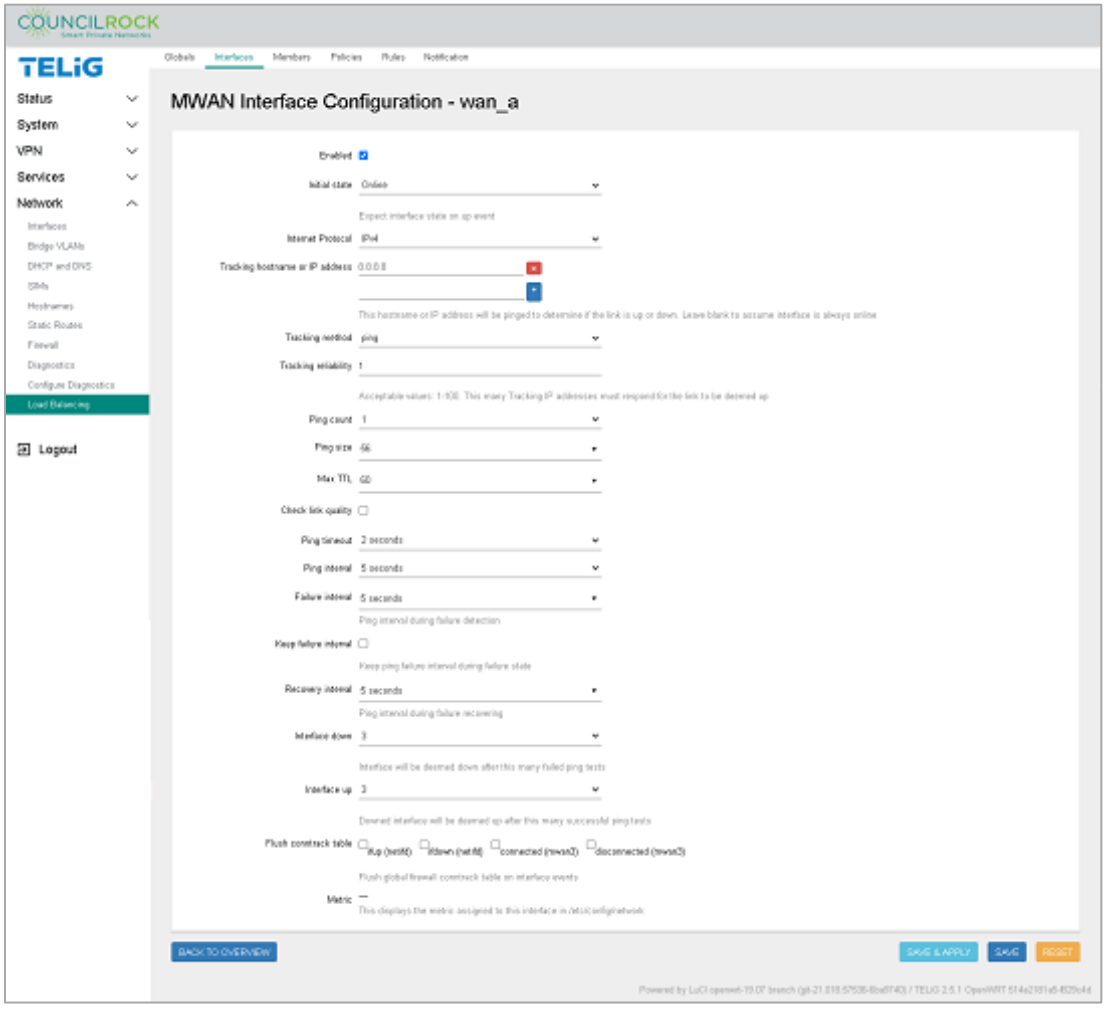

Figure B.D.1 - Network > Load Balancing > Interfaces (input screen)

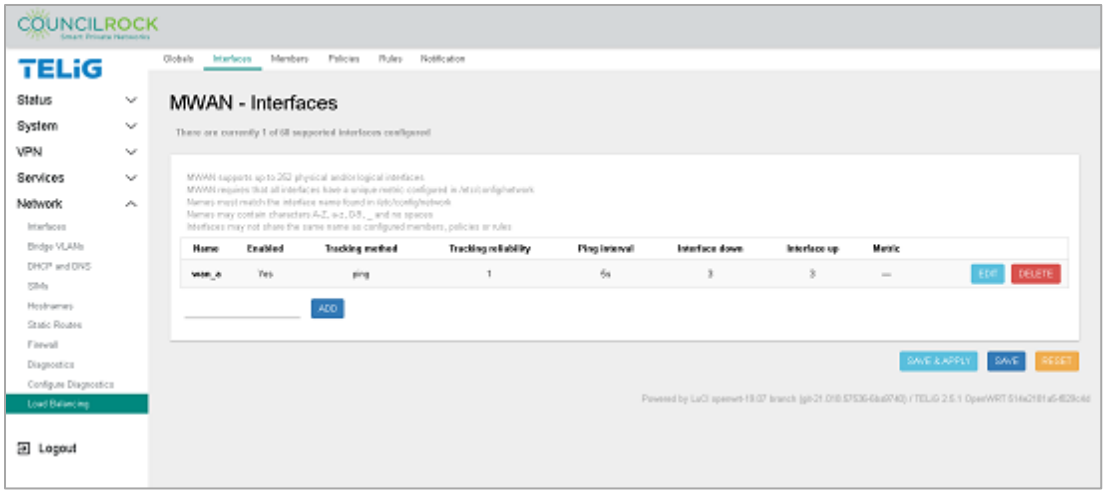

Figure B.D.2 - Network > Load Balancing > Interfaces (interface summary screen)

4. Click SAVE to create load balancing interface “wan_a”
5. Repeat steps 1 through 4 for interface wan_b

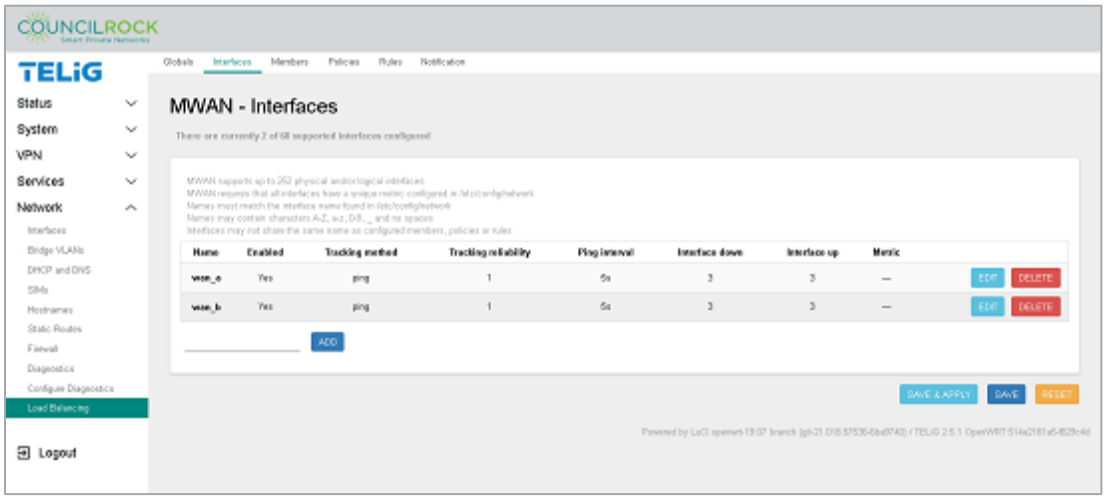

Figure B.D.3 - WAN Interfaces are set up

6. Navigate to Network > Load Balancing > Members.
7. Add a MWAN member for wan_a, the main interface in this example.
    a. On the text input line left of the ADD button, enter “failover_wan_a” and click ADD
    b. Click the *Interface* dropdown and select “wan_a”
    c. Enter *Metric* = 1
    d. Enter *Weight* = 1
    e. Click the SAVE & APPLY button, followed by the BACK TO OVERVIEW button.
8. Repeat steps 6-7 to create “failover_wan_b”, the backup interface in this example. Set *Metric* and *Weight* = 2.

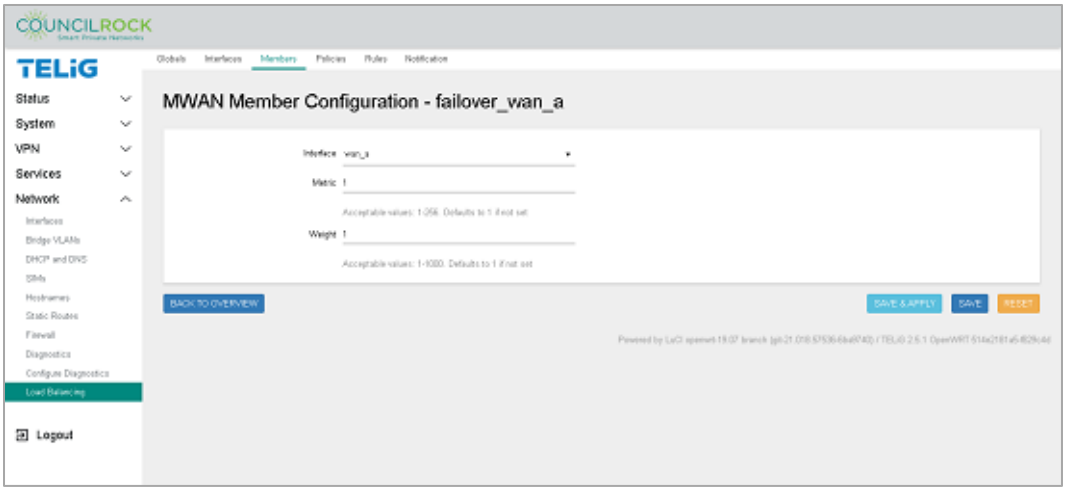

Figure B.D.4 - Member Configuration – failover_wan_a

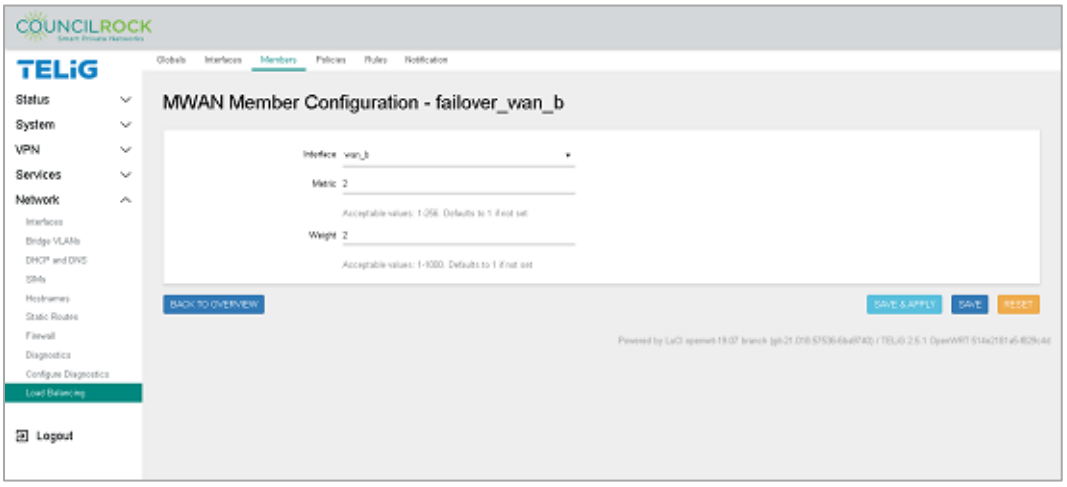

Figure B.D.5 - Member Configuration – failover_wan_b

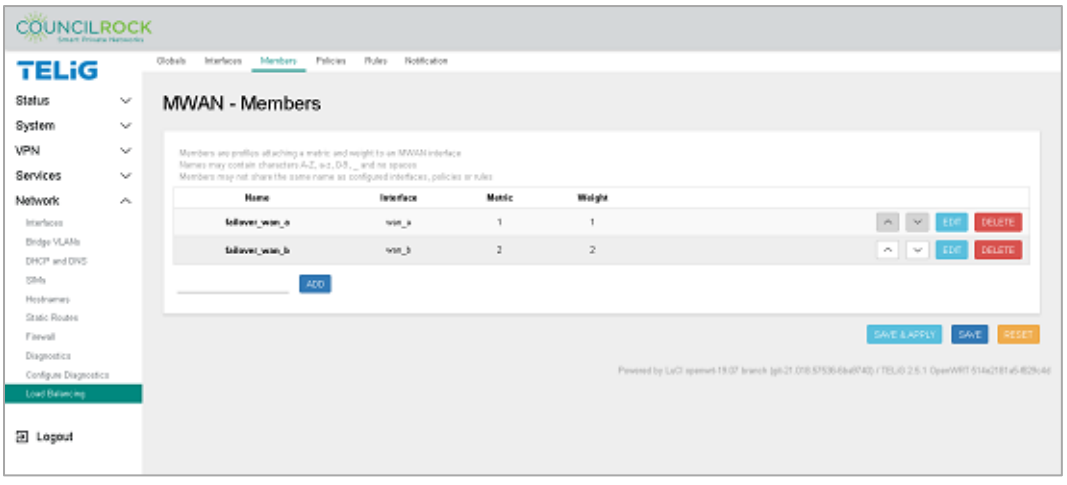

Figure B.D.6 – Load Balancing Members are set up

9. Create the Load Balancing Policy. The policy sets the unit to reject traffic across interfaces that are down.
    a. Navigate to the *Policies* tab
    b. On the text input line next to the ADD button, and enter “test_policy”
    c. From the *Member used* dropdown, select both ‘failover_wan_a’ and ‘failover_wan_b’
    d. Use the default setting for *Last Resort*: unreachable (reject)
    e. Click the SAVE & APPLY button, followed by the BACK TO OVERVIEW button.

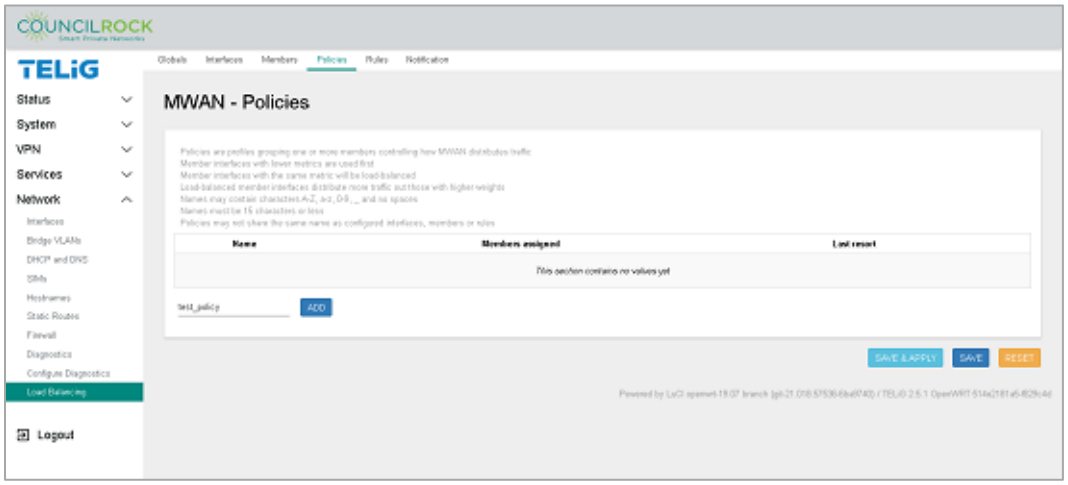

Figure B.D.7 - Network > Load Balancing > Policies (add a policy)

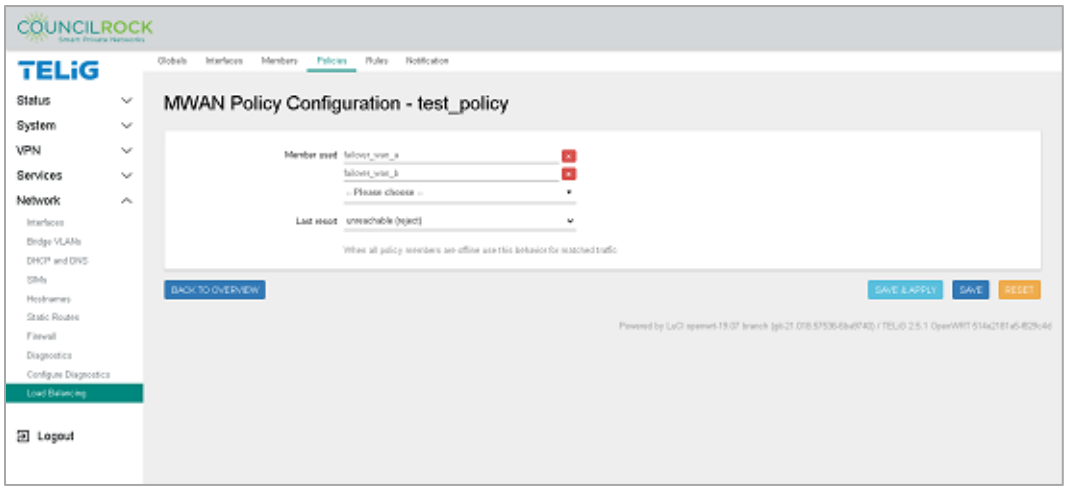

Figure B.D.8 - Network > Load Balancing > Policies (define a policy)

10. Create Load Balancing Rules. Rules determine what traffic uses the Load Balancing Policy defined in the previous step. In our example all traffic to the WAN will be part of the load balancing policy. Here we set up all incoming traffic (to the default route 0.0.0.0/0) to be our rule “classifier”.
    a. Navigate to *the Rules* tab.
    b. In the text input line next to the ADD button, enter “test_rule” and click the ADD button.

c. Configure test_rule as described below. Generally, the default values are used, only the *Destination address* and the *Policy assigned* needs to be entered.

test_rule configuration:

- Source address: blank
- Source port: blank
- **Destination address: 0.0.0.0/0**
- Destination port: blank
- Protocol: all
- Sticky: No
- Sticky timeout: blank
- IPset: blank
- Logging: unchecked
- Policy Assigned: test_policy (the policy from the previous step will be available in the dropdown list)

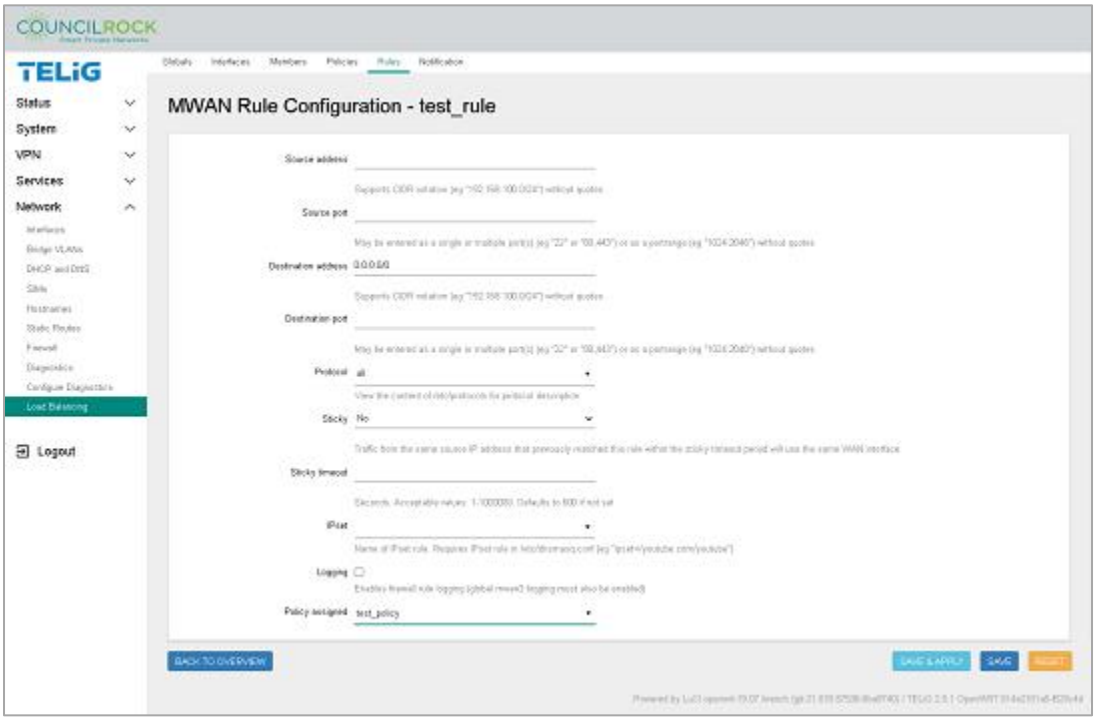

Figure B.D.9 - Network > Load Balancing > Rules (define a rule)

11. Click the SAVE & APPLY button

Creating the rule is the final step in this configuration. To verify the configuration is functioning, go to *Status > Load Balancing > Interface*. Verify that both MWAN interfaces (wan_a and wan_b) display "Status: Online". Note that interface uptime is provided here.

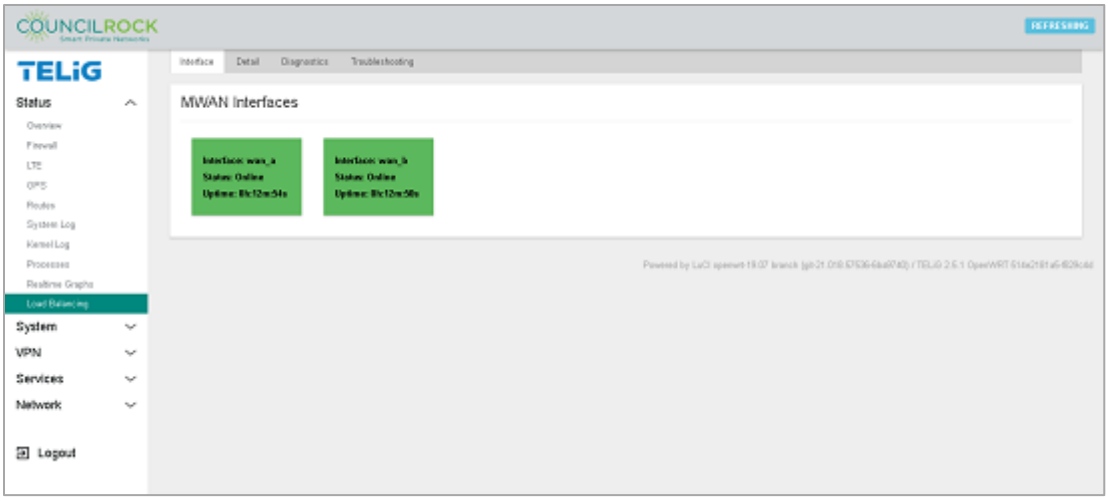

Figure B.D.10 - Status > Load Balancing > Interface (verify load balancing)

Additionally, on the *Detail* tab, we see the test_policy is directing 100% of traffic to wan_a, the interface we defined with the lowest metric.

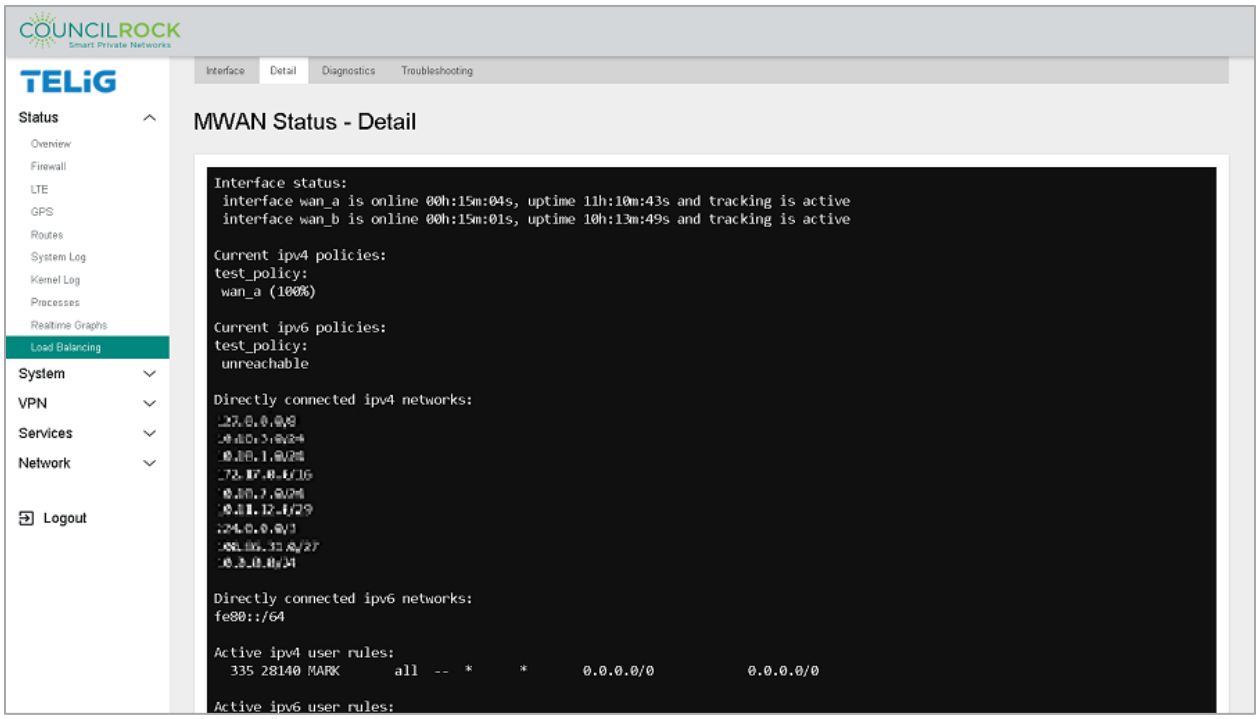

Figure B.D.11 - Status > Load Balancing > Detail (verify load balancing)

To verify failover is set up correctly, disable the main interface by navigating to *Network > Interfaces* and clicking the STOP button on wan_a. Navigate back to *Status > Load Balancing > Detail* to verify that traffic has switched to the backup interface “wan_b”.

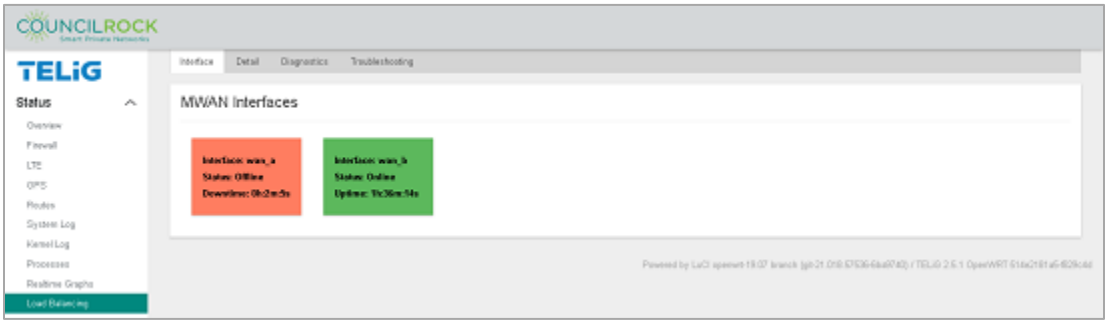

Figure B.D.12 - Status > Load Balancing > Detail (verify load balancing)

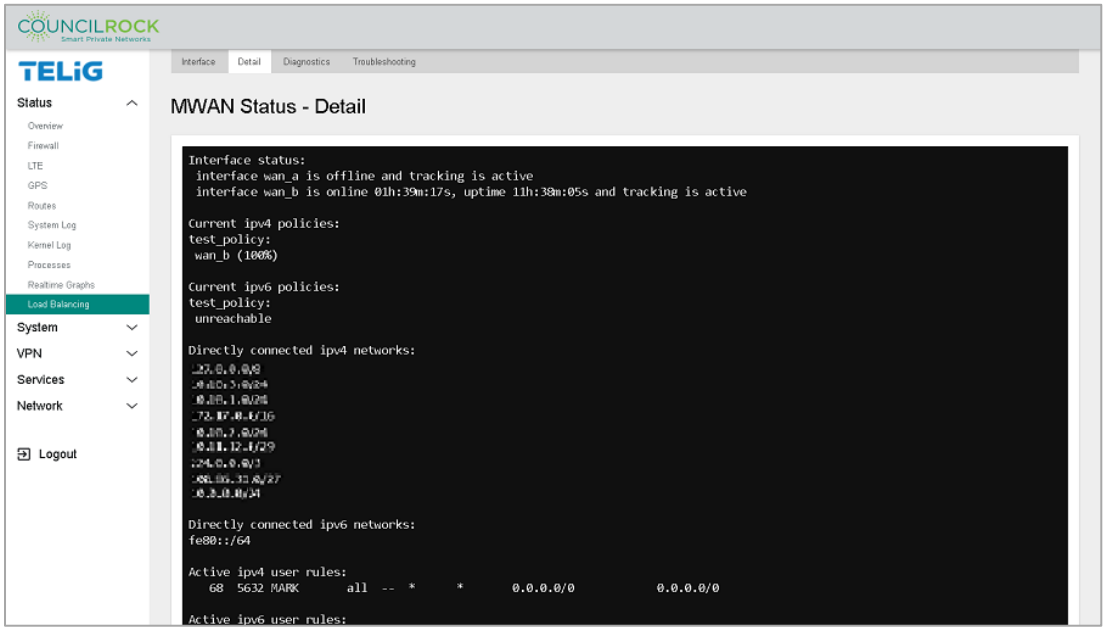

Figure B.D.13 - Status > Load Balancing > Detail (verify load balancing)

Use Case E: Interface Bridging

The LAN bridge combines the WLAN interface(s) with the wired LAN ports to create a single logical network.

Example: Configure a bridge between Ethernet ports lan1 and lan2.

Requirements:

Fundamentals B: LAN interface config
Fundamentals C: WAN interface config

Steps:

1. Navigate to *Network* > *Interfaces* and click the EDIT button on LAN1.

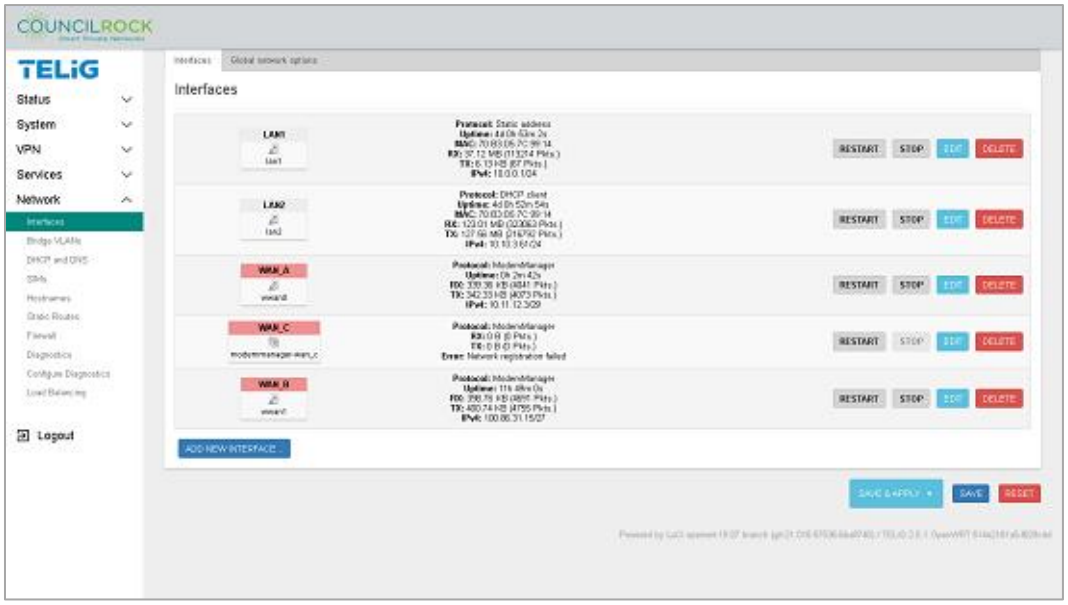

Figure B.E.1 - Network > Interfaces

2. Select the 'Physical Settings' tab and select the 'Bridge interface' checkbox. In the drop-down menu under Interfaces select lan1 and lan2.
3. Click the SAVE button to close the edit window
4. Click the SAVE & APPLY button to apply changes.

   All LAN physical ports in the bridge will act as a single network.

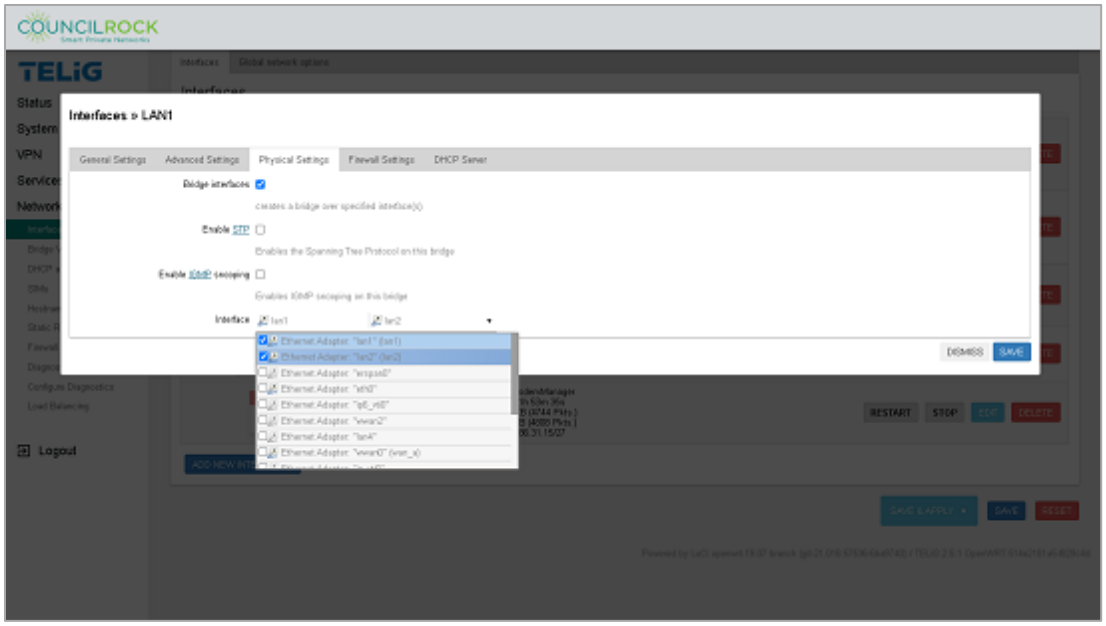

Figure B.E.2 - Interface EDIT > Physical Settings for LAN1

The new pseudo-interface has “br-“ prepended to the interface name (generally br-lan). This indicates the bridged LAN. The new interface will have a single IP address.

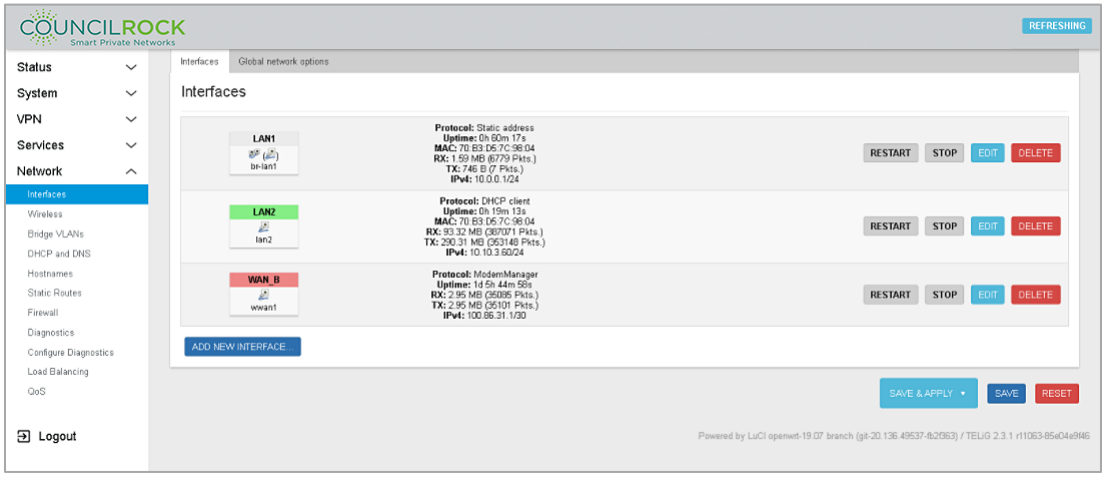

Figure B.E.3 - Network > Interfaces (showing bridged interfaces)

Use Case F: SNMPD Trap Alerts

Example: Send traps to a SNMP server using SNMPV2

Configure the unit to send trap alerts to an SNMP server hosted on the network using SNMP version 2.

Steps:

1. Navigate to *Services > SNMPD*

Figure B.F.1 - Services > SNMPD

2. Scroll down to the "v2c Traps" section, click the ADD button to open the lines for text input and enter the required information:
   - **Host:** IP address of the SNMP server
   - **Community:** SNMP community string to use when sending traps to the server. This community needs to match the community on the server side.
   - **Port:** Port on the SNMP server that will be receiving the traps

Figure B.F.2: Services > SNMPD: v2C Traps

3. Click the SAVE & APPLY button.

Appendix C:

List of Acronyms

	Definition
APN	Access Point Name
ARM	Advanced RISC machine
BGP	Border Gateway Protocol
br-lan	the pseudo LAN after being bridged
Cat-M/NB IoT	Category M / Narrowband for the Internet of Things - cellular data connectivity
CFR	Code of Federal Regulations
CIP	Common Industrial Protocol
COAP	Constrained Application Protocol
CPU	Central Processing Unit
cron	time based job scheduler in Linux
Cron log	the log output of a cron process
CSA	Canadian Standards Association
DA	Distributed Automation
DAE	Dynamic Authorization Extensions to RADIUS
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DL	Download

	Definition
DMVPN	Dynamic Multipoint VPN
DNP3	Distributed Network Protocol 3
DNS	Domain Name System
DSCP	Differentiated Services Code Point
EIGRP	Enhanced Interior Gateway Routing Protocol
eMMC	Embedded Multimedia Card
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
4FF	SIM card Form Factor
FTL	Flash Transition Layer
GB	Gigabytes
GHz	Gigahertz
GND	Ground
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
i.MX6 ARM	Advanced RISC Machine based Processor

	Definition
ICCID	A globally unique serial number for a SIM card
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IS-IS	Intermediate System - Intermediate System
ISM	Industrial, Scientific & Medical (frequency band)
Kbit/s	kilobits per second
LAN	Local Area Network
LDP	Label Distribution Protocol
LED	Light Emitting Diode
LTE	Long Term Evolution (4G mobile communications standard)
LTE-CBRS	Long Term Evolution - Citizens Broadband Radio Service
MAC	Media Access Control
Mbps	megabits per second

	Definition
MHz	Megahertz
MIMO	Multiple In Multiple Out
MODBUS	The de facto standard communications protocol for industrial electronic devices
mPCIe	Mini-PCI Express (expansion bus form factor)
MPLS	Multiprotocol Label Switching
MSS	Maximum Segment Size
MTD	Memory Technology Device (Linux device file for interacting with Flash technology)
mtdblocks	A Linux abstract layer to emulate block device data structures on flash technology
MTU	Maximum Transmission Unit
MWAN	Multi-Wide Area Network
NAS ID	Network Access Server Identifier
NAT	Network Address Translation
OpenVPN	An Open Source VPN (Virtual Private Networking) implementation
OpenWRT	An embedded Linux distribution installed on a router
OPKG	Open Package management - for installing, upgrading & managing software applications in an embedded Linux environment
OSPF	Open Shortest Path First
PC	Personal Computer
PID	Product ID

	Definition
PLC	Programmable Logic Controller
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RF	Radio Frequency
RIPv2	Routing Information Protocol Version 2
RPL	Routing Protocol for Low Power and Lossy Networks
RS	Recommended Standard
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indicator
RTS/CTS	Request to Send / Clear to Send
RTU	Remote Terminal Unit
SIM	Subscriber Identity Module
SINR	Signal to Interference plus Noise Ratio
SISO	Single Input Single Output
SLAAC	Stateless Address Autoconfiguration
SMA	Subminiature version A (connector)
SNMP	Simple Network Management Protocol
SNMPD	Linux SNMP agent (daemon)
SNR	Signal to Noise Ratio
SSH	Secure Shell

	Definition
STP	Spanning Tree Protocol
syslog	the system log
TAP	Kernel Virtual Network Device: “Network Tap”
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TIA TSB-88.4	Telecommunications Industry Association Telecommunications Service Bulletin 88.4
TUN	Kernel Virtual Network Device: “Network TUNnel”
UDP	User Datagram Protocol
UL	Underwriter's Laboratory
VLAN	Virtual LAN
VPN	Virtual Private Network
WAN	Wide Area Network
WiFi	Wireless networking protocol
WLAN	Wireless LAN
WMM	WiFi Multimedia
WPA2	Wireless Protected Access 2 (security)
WPA2-EAP	Wireless Protected Access 2 - Extensible Authentication Protocol (security)
WPA2-PSK	Wireless Protected Access 2 - Protected Shared Key (security)
WPS	WiFi Protected Setup
wwan	Wireless Wide Area Network
XOR	Exclusive OR (logic)

Appendix D:

List of Tables / List of Figures

Table 1*: LED Status List* 8
Table 2: RF Connectors by Model 8
Table 3: RF Port to WAN mapping 9
Table 4: Common Serial pinouts 10
Table 5: Signal Quality categories by RSRQ 22
Table 6: Serial Configuration 53
Table 7: Wireless Access Point Typical Setup Options 67
Table 8: Model Options 87
Table 9: Hardware Summary 88
Table 10: RF Specifications 89

Figure 1: Models E1500-L8N, E1500-8NW 7
Figure 2: Models E1500-LW, E1500-8W 7
Figure 3: Models E1500-L8N, E1500-8NW 8
Figure 4: Models E1500-LW, E1500-8W 8
Figure 5: Serial Port Pinout - RS232 (Serial) 9
Figure 6: Serial Port Pinout – RS485 (Modbus) 9
Figure 7: Serial Port Pinout – RS232 (Console) 9
Figure 8: Alarm / Power Connections 10
Figure 9: Rear Panel - Note center screw holes for DIN-rail mount accessory 10
Figure 10: Software Architecture 12
Figure 11: Unit Connections 13
Figure 12: Login Screen 14
Figure 13: SIM Card APN Entry 15
Figure 14: Status > Overview 18
Figure 15: Firewall Menus 19
Figure 16: Status > LTE > Overview 20
Figure 17: Status > LTE > Bearers 21
Figure 18: Status > LTE > Signal 22
Figure 19: Status > LTE Scan: Cellular Network Scanning Tool 23
Figure 20: Status> GPS 23
Figure 21: Status > Routes 24
Figure 22: Status > System Log 24
Figure 23: Status > Kernel Log 25

Figure 24: Status > Processes 25
Figure 25: Status > Realtime Graphs > Load 26
Figure 26: Status > Realtime Graphs > Traffic 26
Figure 27: Status > Realtime Graphs > Connections 27
Figure 28: Status > Realtime Graphs > Rate 27
Figure 29: Status > Load Balancing > Interface 28
Figure 30: Status > Load Balancing > Detail 28
Figure 31: Status > Load Balancing > Diagnostics 29
Figure 32: Status > Load Balancing > Troubleshooting 30
Figure 33: System > System > General Settings 31
Figure 34: System > System > Logging 31
Figure 35: System > System > Time Synchronization 32
Figure 36: System > System > Language and Style 32
Figure 37: System > Administration > Router Password 33
Figure 38: System > Administration > SSH Access 33
Figure 39: System > Administration > SSH-Keys 34
Figure 40: System > Software 34
Figure 41: OPKG Configuration 35
Figure 42: Install new packages 36
Figure 43: Detailed list of packages (example: block-mount) 36
Figure 44: System > Startup > Initscripts 37
Figure 45: System > Startup > Local Startup 37
Figure 46: System > Scheduled Tasks 38
Figure 47: System > LED Configuration 40
Figure 48: System > LED Configuration: netdev example 40
Figure 49: System > Backup/Flash Firmware: Actions 41
Figure 50: System > Backup/Flash Firmware: Configuration 42
Figure 51: System > Custom Commands > Dashboard 43
Figure 52: System > Custom Commands > Dashboard 43
Figure 53: System > Custom Commands > Configure 44
Figure 54: System > Reboot 44
Figure 55: VPN > IPSec: Status 45
Figure 56: VPN > IPSec: Config 45
Figure 57: IPSec Cipher proposal 46
Figure 58: IPSec Tunnel configuration 47
Figure 59: IPSec Connection configuration 47
Figure 60: VPN > OpenVPN 52
Figure 61: Services > Serial Configuration 54
Figure 62: Services > QoS over Nftables > Limit Rate 55

Figure 63: Services > QoS over Nftables > Traffic Priority 56
Figure 64: Services > SNMPD 57
Figure 65: Network > Interfaces 58
Figure 66: Interfaces > Advanced Settings 59
Figure 67: Interfaces > LANx > General Settings 60
Figure 68: Interfaces > LANx > Advanced Settings 60
Figure 69: Interfaces > LANx > Physical Settings 61
Figure 70: Interfaces > Firewall Settings 62
Figure 71: Interfaces > DHCP Server > General 62
Figure 72: Interfaces > DHCP Server > Advanced 63
Figure 73: Interfaces > DHCP Server > IPv6 Settings 64
Figure 74: Wireless > Overview 65
Figure 75: Wireless > Wireless Network > General [Top Card] 66
Figure 76: Wireless > Wireless Network > Advanced [Top Card] and General Setup [Bottom Card] 67
Figure 77: Wireless > Wireless Network > Wireless Security [Bottom Card] 68
Figure 78: Wireless > Wireless Network > MAC-Filter [Bottom Card] 69
Figure 79: Wireless > Wireless Network > Advanced Settings [Bottom Card] 70
Figure 80: Network > Bridge VLANs > Status 70
Figure 81: Network > Bridge VLANs > Configure 71
Figure 82: Network > DHCP and DNS > General Settings 72
Figure 83: DHCP and DNS > Resolv and Hosts Files 72
Figure 84: DHCP and DNS > TFTP Settings 73
Figure 85: DHCP and DNS > Advanced Settings 73
Figure 86: DHCP and DNS > Static Leases 74
Figure 87: SIMs 74
Figure 88: Network > Hostnames 75
Figure 89: Network > Hostnames > Adding a hostname 75
Figure 90: Network > Static Routes 76
Figure 91: Network > Static Routes > General Settings 77
Figure 92: Network > Static Routes > Advanced 78
Figure 93: Network > Firewall > General 79
Figure 94: Network > Firewall > Port Forwards 81
Figure 95: Network > Firewall > Traffic Rules 82
Figure 96: Network > Firewall > NAT Rules 84
Figure 97: Network > Firewall > Custom Rules 85
Figure 98: Network > Diagnostics 85
Figure 99: Network > Diagnostics 86