User Manual

Copyright

Trademarks

Aprisa and the Aviat logo are trademarks of Aviat Networks.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries. All other marks are the property of their respective owners.

Disclaimer

Although every precaution has been taken when preparing this information, Aviat Networks assumes no liability for errors and omissions, or any damages resulting from use of this information. This document or the equipment may change, without notice, in the interest of improving the product.

RoHS and WEEE Compliance

The Aprisa LTE 5G is fully compliant with the European Commission's RoHS (Restriction of Certain Hazardous Substances in Electrical and Electronic Equipment) and WEEE (Waste Electrical and Electronic Equipment) environmental directives.

Restriction of hazardous substances (RoHS)

The RoHS Directive prohibits the sale in the European Union of electronic equipment containing these hazardous substances: lead, cadmium, mercury, hexavalent chromium, polybrominated biphenyls (PBBs), and polybrominated diphenyl ethers (PBDEs).

Aviat Networks has worked with its component suppliers to ensure compliance with the RoHS Directive which came into effect on the 1st July 2006.

End-of-life recycling programme (WEEE)

The WEEE Directive concerns the recovery, reuse, and recycling of electronic and electrical equipment. Under the Directive, used equipment must be marked, collected separately, and disposed of properly.

Aviat Networks has instigated a programme to manage the reuse, recycling, and recovery of waste in an environmentally safe manner using processes that comply with the WEEE Directive (EU Waste Electrical and Electronic Equipment 2002/96/EC).

Aviat Networks invites questions from customers and partners on its environmental programmes and compliance with the European Commission's Directives.

Compliance General

The Aprisa LTE 5G router operates within frequency bands that are controlled through spectrum license managed by the carriers[1] . Devices using these frequencies must meet the regional regulatory requirements in addition to any requirements put in place by the carriers.

It is the responsibility of the user, before operating the equipment, to ensure that where required the appropriate regulatory and regional carrier requirements have been met.

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

Equipment authorizations sought by Aviat Networks are based on the Aprisa LTE 5G router being installed at a fixed restricted access location and operated within the environmental profiles defined in Table 1; operation outside these criteria may invalidate the authorizations and / or license conditions.

Table 1 General Compliance

Environmental	Storage: EN 300 019-1-1 Class 1.2
	Transportation: EN 300 019-1-2 Class 2.3
	Stationary use: EN 300 019-1-3 Class 3.3
	Mobile use: EN 300 019-1-5 Class 5.1
Vehicle	ISO 7637-2, ISO 16750-2 (12V Code D 24V Code E)
	Shock & Vibration: SAE J1455
Safety	UL 62368-1, Class 1 division 2, Groups ABCD for hazardous locations

---

[1] The carriers are the mobile phone carriers such as Verizon, AT&T, Vodafone etc.

Compliance Radio Equipment Directive

The Aprisa LTE 5G router complies with the Radio Equipment Directive (RED) 2014/53/EU European Telecommunications Standards Institute (ETSI) specifications defined in Table 2:

Table 2 RED Compliance

Aprisa LTE 5G	GCF certified
EMC	EN 301 489-1 EN 301 489-52
WWAN (LTE)	This product may contain a LTE Module EN 301 908-1 and EN 301 908
WLAN (Network)	This product may contain a Network Module of type: 　　　Wi-Fi Module EN 300 328 and EN 301 893
Environmental	Storage: EN 300 019-1-1 Class 1.2 Transportation: EN 300 019-1-2 Class 2.3 Stationary use: EN 300 019-1-3 Class 3.3 Mobile use: EN 300 019-1-5 Class 5.1
Vehicle	ISO 7637-2, ISO 16750-2 (12V Code D 24V Code E) Shock & Vibration: SAE J1455
Safety	EN 62368-1:2014, Class 1 division 2, Groups ABCD for hazardous locations

Compliance United States of America FCC

The Aprisa LTE 5G router may contain an LTE module and/or a WLAN Network module certified to Federal Communications Commission (FCC) specifications defined in Table 3:

Table 3 USA Compliance

HOST ONLY (Aprisa LTE 5G without modules)	This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
	This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
	—Reorient or relocate the receiving antenna.
	—Increase the separation between the equipment and receiver.
	—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
	—Consult the dealer or an experienced radio/TV technician for help.
WWAN (LTE)	This product may contain a LTE Module.
	This device complies with part 15 of the FCC Rules. Operation is subject to the condition that this device does not cause harmful interference.
WLAN (Network)	This product may contain a Network Module of type: Wi-Fi Module FCC ID: SQG-60SIPT
	47 CFR Parts 15C and 15E
	This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
EMC	47 CFR Part 15B
Aprisa LTE 5G	PTCRB, CBRS End Device, AT&T, Verizon Wireless, Anterix

Compliance Canada ISED

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Compliance Brazil Anatel

This equipment is not entitled to protection against harmful interference and may not cause interference to duly authorized systems. For more information, consult the ANATEL website www.gov.br/anatel/pt-br/.

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados. Para maiores informações, consulte o site da ANATEL www.gov.br/anatel/pt-br/.

Wi-Fi

For the 5150-5350 MHz band, emissions must be confined to the internal environments of buildings. If the product is to be installed outdoors, the 5.1 GHz frequency cannot be used.

Para a faixa de 5150-5350 MHz, as emissões devem ser confinadas aos ambientes internos dos edifícios. Se o produto for instalado ao ar livre, a frequência de 5,1 GHz não pode ser usada.

Compliance Hazardous Locations Notice

This product is suitable for use in Class 1, Division 2, Groups ABCD hazardous locations or non-hazardous locations. A Nationally Recognized Testing Laboratory (NRTL) listed Safety Extra Low Voltage / Limited Power Source (SELV/LPS) power supply with a maximum rating of 32V d.c., 100W is required to power the equipment.

The following text is printed on the Aprisa LTE 5G:

WARNING: EXPLOSION HAZARD - Do not connect or disconnect while circuits are live unless area is known to be non-hazardous.

The following text is printed on the Aprisa LTE 5G where the end user is in Canada:

AVERTISSEMENT: RISQUE D'EXPLOSION - Ne pas brancher ou débrancher tant que le circuit est sous tension, à moins qu'il ne s'agisse d'un emplacement non dangereux.

Symbols

	ISO 7000-0434B	Exposure Warning Avertissement d'exposition
	IEC 60417-5041	Potential hot surface hazard Risque potentiel de surface chaude
	ISO 7000-0434B	Read the instructions Lis les instructions

Cooling

If the Aprisa LTE 5G is operated in an environment where the ambient temperature exceeds 50°C, the convection air flow over the heat sink must be considered.

The environmental operating conditions are as follows:

Operating temperature	-30 to +70° C (-22 to +158° F)
Storage temperature	-40 to +85° C (-40 to +185° F)
Humidity	Maximum 95% non-condensing

WARNING:

If the Aprisa LTE 5G is operated in an environment where the ambient temperature exceeds 50°C, the Aprisa LTE 5G must be installed within a restricted access location to prevent human contact with the enclosure heat sink.

ATTENTION:

Si l'Aprisa LTE 5G fonctionne dans un environnement où la température ambiante dépasse 50 ° C, l'Aprisa LTE 5G doit être installé dans un endroit à accès restreint de manière à éviter tout contact humain avec le dissipateur de chaleur du boîtier.

WARNING:

The Aprisa LTE 5G can be operated in an environment where the ambient temperature exceeds 50°C. The heat sink will be a hot surface - do not touch.

ATTENTION:

L'Aprisa LTE 5G peut fonctionner dans un environnement où la température ambiante dépasse 50 ° C. Le dissipateur de chaleur sera une surface chaude - ne le touchez pas.

Earthing

The Aprisa LTE 5G has an earth connection point on the top left of the enclosure. A M4 8mm pan pozi machine screw and M4 lock washer is supplied fitted to the router. This screw is used to earth the enclosure to a protection earth. A minimum of 0.8 mm² (18 AWG) wire shall be used and it shall not contain switches or protective devices.

![Aviat Networks logo]

RF Exposure Warning

WARNING:

To comply with FCC/ISED regulations limiting maximum RF output power, human exposure to RF radiation, and possible antenna co-location interaction, the antenna gains and resulting EIRP must not exceed those stipulated in Table 4.

At least 20 cm (8 inches) separation distance between any antenna used with this device and the general public must be maintained at all times when using antennas with gain up to the Maximum MPE Antenna Gain values shown below.

Where the Aprisa LTE 5G and Wi-Fi antennas are co-located or combined, the lower co-located antenna gain figure must be used.

In the USA, the radiated power of the Aprisa LTE 5G system (the Maximum Time Averaged Conducted Power plus the user supplied antenna gain less any cable losses) must not exceed the EIRP limit stipulated in Table 4. Not all bands shown are available in all Aprisa LTE 5G devices nor are they all available for use in the USA.

For example, in the case of Aprisa LTE 5G Band 8 in the USA the antenna gain for uncontrolled exposure of the general public is limited to 6 dBi (4 dBi if co-located with Wi-Fi) but the antenna gain may be increased to 12 dBi if the installation prevents occupational/controlled exposure closer than 50 cm (20 inches) to the antenna. Refer FCC OET Bulletin 65 "Evaluating Compliance with FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields".

In other regulatory regions, the safe compliance distance from the antenna can be determined from the local regulatory limiting power density, and the formula and example provided in the section titled 'Antenna Selection' from page 83 of this manual.

ATTENTION:

Pour se conformer aux réglementations FCC / ISED limitant la puissance de sortie RF maximale, l'exposition humaine au rayonnement RF et l'interaction possible de co-emplacement d'antenne, les gains d'antenne et la PIRE résultante ne doivent pas dépasser ceux stipulés dans le Tableau 4.

Une distance de séparation d'au moins 20 cm (8 pouces) entre toute antenne utilisée avec cet appareil et le grand public doit être maintenue à tout moment lorsque vous utilisez des antennes avec un gain allant jusqu'aux valeurs de gain d'antenne MPE maximum indiquées ci-dessous.

Lorsque les antennes Aprisa LTE 5G et Wi-Fi sont co-localisées ou combinées, le chiffre de gain d'antenne co-localisé inférieur doit être utilisé.

Aux États-Unis, la puissance rayonnée du système Aprisa LTE 5G (la puissance conductrice moyenne dans le temps maximum plus le gain d'antenne fourni par l'utilisateur moins les pertes de câble) ne doit pas dépasser la limite de PIRE stipulée dans le tableau 4. Toutes les bandes indiquées ne sont pas disponibles dans tous les Aprisa Les appareils Aprisa LTE 5G ne sont pas non plus tous disponibles pour une utilisation aux États-Unis.

Par exemple, dans le cas de la bande Aprisa LTE 5G 8 aux États-Unis, le gain d'antenne pour une exposition incontrôlée du grand public est limité à 6 dBi (4 dBi si co-localisé avec Wi-Fi) mais le gain d'antenne peut être augmenté à 12 dBi si l'installation empêche une exposition professionnelle / contrôlée à moins de 50 cm (20 pouces) de l'antenne. Reportez-vous au Bulletin 65 de la FCC OET «Évaluation de la conformité aux directives de la FCC pour l'exposition humaine aux champs électromagnétiques de radiofréquence».

Dans d'autres régions réglementaires, la distance de conformité de sécurité par rapport à l'antenne peut être déterminée à partir de la densité de puissance limite réglementaire locale, et de la formule et de l'exemple fournis dans la section intitulée « Sélection de l'antenne » de la page 83 de ce manuel.

Table 4 Antenna Compliance Requirements

Operating Mode	Tx Freq Range (MHz)	Max Time-Avg Cond. Power (dBm)	Maximum MPE Antenna Gain [c]		FCC EIRP Limits (dBm)
			Standalone (dBi)	Co-located (dBi)	
LTE B1	1920 – 1980	24	N/A	4	N/A
LTE B2	1850 - 1910	24	8	6	33
LTE B3	1710 – 1785	24	N/A	4	N/A
LTE B4	1710 – 1755	24	6	4	30
LTE B5	824 – 849	24	6	4	40.6
LTE B7	2500 – 2570	23.8 [a]	9	4	32.8
LTE B8 (USA)	880 – 915 (897.5 – 900.5)	24	6 [e]	6	42
LTE B9	1750 – 1785	24	N/A	6	N/A
LTE B12	699 – 716	24	6	4	30
LTE B13	777 – 787	24	6	4	30
LTE B14	788 - 798	24	8	4	32
LTE B17	704 – 716	24	6	4	30
LTE B18	815 - 830	24	N/A	6	N/A
LTE B19	830 - 854	24	N/A	6	N/A
LTE B20	832 - 862	24	N/A	6	N/A
LTE B21	1448 - 1463	24	N/A	6	N/A
LTE B25	1850 - 1915	24	6	4	33
LTE B26	814 – 849	24	6	4	40.6
LTE B28	703 - 748	24	N/A	6	N/A
LTE B30	2305 – 2315	24	1 [d]	1 [d]	25
LTE B38	2570 - 2620	24	N/A	6	N/A
LTE B39	1880 - 1920	24	N/A	6	N/A
LTE B41	2496 – 2690	23.8 [a]	9	4	32.8
LTE B48 [b]	3550 – 3700	23	0	0	23
LTE B66	1710 – 1780	24	6	4	30
LTE B71	663 - 698	24	6	4	30
Co-located antennas with standalone FCC EIRP and co-located (EIRP) limits					
WLAN 2.4 GHz	2400 - 2500	21.4	14	3	36 (25)
WLAN 5 GHz	5150 - 5850	21.6	14	5	36 (27)

Note a   Includes 0.8 dB offset from single-cell tolerance for UL CA.

Note b   Important: Airborne operations in LTE Band 48 are prohibited.

Note c   Antenna gain above the co-located maximum gain value must not be used when the Wi-Fi module is fitted unless the Wi-Fi and cellular antennas are separated by more than 20 cm.

Note d   Important: The FCC and IC have a strict EIRP limit in Band 30 for mobile and portable stations in order to protect adjacent satellite radio, aeronautical mobile telemetry, and deep space network operations. Mobile and portable stations must not have antenna gain exceeding 1 dBi in Band 30. Additionally, both the FCC and IC prohibit the use of external vehicle-mounted antennas for mobile and portable stations in this band. Fixed stations may use antennas with higher gain in Band 30 due to relaxed EIRP limits. UIP4RF55 modules used as fixed subscriber stations in Canada or fixed customer premises equipment (CPE) stations in the United States may have an antenna

gain up to 10 dBi in Band 30, however, the use of outdoor antennas or outdoor station installations are prohibited except if professionally installed in locations that are at least 20 meters from roadways or in locations where it can be shown that the ground power level of -44 dBm per 5 MHz in the bands 2305–2315 MHz and 2350–2360 MHz or -55 dBm per 5 MHz in the bands 2315-2320 MHz and 2345–2350 MHz will not be exceeded at the nearest roadway. For the purposes of this notice, a roadway includes a highway, street, avenue, parkway, driveway, square, place, bridge, viaduct or trestle, any part of which is intended for use by the general public for the passage of vehicles.

Mobile carriers often have limits on total radiated power (TRP), which requires an efficient antenna. The end product with an embedded module must output sufficient power to meet the TRP requirement but not too much to exceed FCC/IC's EIRP limit. If you need assistance in meeting this requirement, please contact Aviat Networks.

Note e   In the case of Anterix Band 8 (B106) in the USA, the antenna gain for uncontrolled exposure of the general public is limited to 6 dBi (4 dBi if co-located with Wi-Fi) but the antenna gain may be increased to 12 dBi if the installation prevents occupational / controlled exposure closer than 50 cm (20 inches) to the antenna. Refer FCC OET Bulletin 65 "Evaluating Compliance with FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields".

Contents

1.   Introduction

About This Manual

What It Covers

This user manual describes how to install and configure an Aprisa LTE 5G router.

It specifically documents an Aprisa LTE 5G router running system software version 3.6.

It is recommended that you read the relevant sections of this manual before installing or operating the Aprisa LTE 5G router.

Who Should Read It

This manual has been written for professional field technicians and engineers who have an appropriate level of training and experience. Only such people shall install and service the Aprisa LTE 5G.

Contact Us

If you experience any difficulty installing or using Aprisa LTE 5G after reading this manual, please contact Customer Support or your local Aviat Networks representative.

The Aviat Networks United States head office is:

Aviat Networks

5250 Prue Road

San Antonio, Texas 78240

United States of America

E-mail	tacsupport@aviatnet.com
Website	aviatnetworks.com
Telephone	+1 (210) 526 6345

The Aviat Networks New Zealand sales office is:

Aviat Networks (NZ) Limited

110 Jackson Street, Petone

Lower Hutt 5012

New Zealand

Aviat Networks (NZ) Limited

PO Box 30248

Lower Hutt 5040

New Zealand

What's in the Box

Inside the box you will find:

- One Aprisa LTE 5G router
- One power cable one metre fitted with 4 pin Molex Micro-Fit 3.0 female connector and wire ended see 'Power Supply' on page 77.
- One power connector, power retention clip and screw

The Aprisa LTE 5G Quick Start Guide is available on the Aviat Networks ARC at the URL Aprisa LTE Quick Start Guide
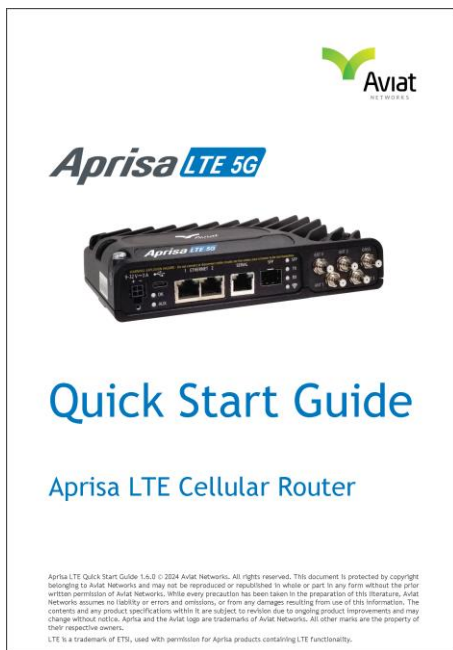
Product Overview

The Aviat Networks Aprisa LTE 5G is a 3GPP LTE router for critical infrastructure monitoring and control for smart SCADA (e.g. electricity, water, oil and gas industries), transportation, smart city, backhaul, and industrial communication hardened for both mission and business critical applications.
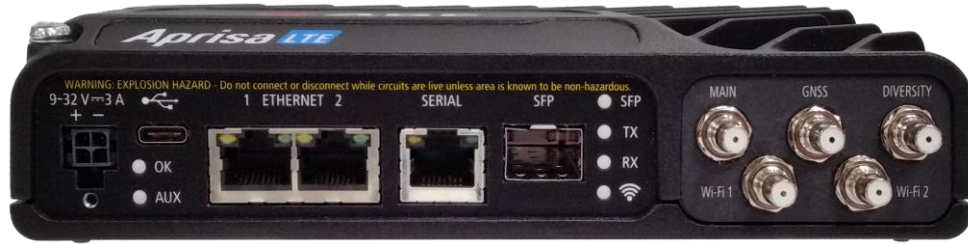
Key Features

- All in one: cellular, Ethernet and fiber, serial, WiFi, GPS, anti-tamper, and 2xSIM switch/router device
- Gigabit LTE / Advanced-LTE wireless data services providing broadband enhanced LTE data rates and latency
- Versatile support of applications such as SCADA, public transportation, public safety, smart city, leased line replacement, industrial VPN router, fleet management, workforce mobility, backhauling, and more
- Provide dynamic routing protocol of IGP (OSPF, EIGRP, RIPv2) and EGP (MP-BGP/BGP) protocol
- Secure and auto DMVPN hub-spoke or full mesh (spoke-to-spoke) services over public internet/WAN network
- GRE VPN, and IPsec support, the Aprisa LTE 5G protects against vulnerabilities and malicious attacks
- Flexible Bridge / Router – allow any switching and routing combination to fit your network needs
- Multi VSI (Virtual Switch/Bridge Instance) allows group / service isolation each with its own MAC switching table
- Multi VRF (Virtual Routing and Forwarding) allows group / service segregation and isolation each with its own routing table instance
- Service segregation using VLANs with manipulation of add / remove / swap VLANs options
- Advanced QoS for dedicated bandwidth per service and support of Cellular QoS profile
- Advanced networking capabilities and protocols such as DNS, DHCP, DDNS, NTP, HTTP/S, SSH, SNMPv2c/3, ARP, VLAN/double VLANs, QoS, NAT, IPv4, and IPv6
- Failover protection using Aprisa LTE 5G router switch over with redundant public and private carrier connection (dual SIM, multi-APN) and interface failover to provide alternate path routing on WAN or FAN failure
- Serial and Ethernet ports with an SFP port for additional electrical / optical connection
- USB host and device mode for local CLI and optional future extention of USB/serial or USB/Eth ports
- Aprisa smart sleep and low power control for off-grid endurance, network recovery, and resilience
- 360^0 layered security, protecting device, access and network levels for privacy, integrity, and authenticity communications
- Complies with LTE 3GPP standards for secure data / control plan over the Aprisa LTE 5G air interface
- Secure device level via anti tamper, secure boot, signed firmware, and enabling / disabling interfaces
- Secure management access and protocols via SSH / HTTPS / SNMPv3, RADIUS, complex password, user privilege, HTTPS certificates, secure firmware upgrade via web/HTTPS or CLI/SFTP, and security auditing
- Secure network via firewall and VPN / IPsecl for privacy, integrity, and authenticity communications
- Detect physical intrusion and secure key storage using anti-tamper module and Trusted Platform Module
- Secure firmware upgrade using web manager via HTTPS and CLI via SFTP protocols
- Supports strong CSNA complaint encryption, authentication and hashing algorithms (e.g. RSA4096 and SHA384).

- 2FA (Two Factor Authentication) via SMS and Account lockout / slowdown user account lockout mechanisms to mitigate brute force password guessing attacks
- Random and unique Admin user password for any new shipped device
- Support secure remote or auto event-based reboot in any case of losing remote connectivity to save truck roll
- Mobility and Wi-Fi supporting advanced remote visibility in vehicle networks with GNSS location (Wi-Fi currently only on the 4G models)
- GNSS navigation and 2x2 MIMO Wi-Fi access point/client for robust workforce mobility and communication
- Transition support to maximize performance and prioritize mission critical traffic while meeting tough security and IP network policy imperatives
- Ruggedized LTE router solution in hardened cast aluminum enclosure for protection from electromagnetic transients and hazardous environments
- Design for electric power substation harsh environment
- Supports the IEEE 1613 environmental standard for electric substation
- Supports the IEC 61850-3 communication protocol standard for electric substation
- Hazard places (fire or explosion), supporting HazLoc Class 1 Div 2 and IEC 62368-1 for safety
- Electrostatics discharge (ESD) protection to IEEE C37 series
- Supports Ingress Protection IP41 for vertically falling drops
- A wide temperature operating range –30 to +70 ˚C (–22 to +158 ˚F) using full specification industrially rated components for hostile environments, extended service life and shared Aprisa family heritage
- Certified to meet tough vehicle electrical and vibration standards
- FCAPS model management options such as web manager, CLI, and variety of 3rd party SNMP manager
- Easily managed with SuperVisor GUI local element management via HTTPS
- Element management over the air via SNMP to allow network-wide monitoring
- Local CLI via USB and remote CLI via Ethernet / IP. Easy to use and intuitive CLI with help and auto complete
- Aprisa Configurator – an application designed to simplify the deployment, configuration, and management of Aprisa LTE 5G cellular routers by providing a low-touch, QR code-based provisioning system
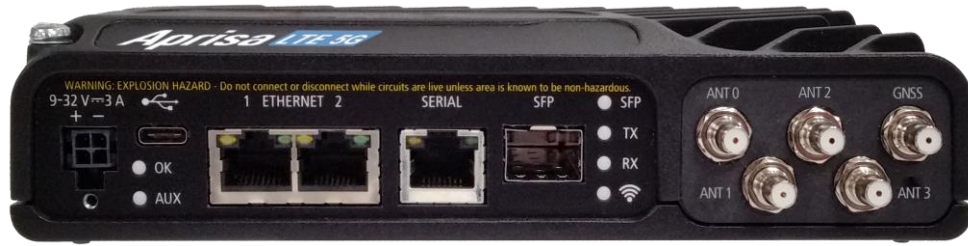
Front Panel Connections

4G Modules

The front panel connections to the Aprisa LTE 4G are:

Designator	Description
9 - 32 VDC---3A	+9 to +32 VDC (negative ground) DC power input using pins 1 & 2 of the 4 pin Molex Micro-Fit 3.0 connector. See 'Power Supply' on page 77.
GPIO pins	General Purpose I/O with one input and one output using the power connector pins 3 & 4 of the 4 pin Molex Micro-Fit 3.0 connector. See 'GPIO' on page 91.
	USB Host Port using a USB type C connector. Used for software upgrade. See 'Software Upgrade' on page 72.
ETHERNET 1 & 2	Integrated 10/100/1000BASE-T layer-3 Ethernet switch / router using RJ45 connectors. Used for Ethernet user traffic and product management. See 'Ethernet Interface Connections' on page 88.
SERIAL	One port of RS-232 / RS-422 / RS-485 serial using RJ45 connector. See 'Serial RS-232 Interface Connections' on page 89 and 'Serial RS-422 / RS-485 Interface Connections' on page 90.
SFP 100/1000Base-X	SFP module socket see 'SFP Modules' on page 64. The Aprisa LTE router supplied with dust plug fitted to SFP socket.
MAIN	Main cellular Aprisa LTE MIMO antenna using 50 ohm QMA female connector.
GNSS	GNSS (Global Navigation Satellite System) antenna using 50 ohm QMA female connector.
DIVERSITY	Diversity cellular Aprisa LTE MIMO antenna using 50 ohm QMA female connector.
Wi-Fi 1 & Wi-Fi 2 (when Wi-Fi fitted)	For connection of Wi-Fi MU-MIMO antennas, see 'Wi-Fi Antenna Requirements' on page 86.

4G / 5G Modules

The front panel connections to the Aprisa LTE 5G are:

Designator	Description
9 - 32 VDC---3A	+9 to +32 VDC (negative ground) DC power input using pins 1 & 2 of the 4 pin Molex Micro-Fit 3.0 connector. See 'Power Supply' on page 77.
GPIO pins	General Purpose I/O with one input and one output using the power connector pins 3 & 4 of the 4 pin Molex Micro-Fit 3.0 connector. See 'GPIO' on page 91.
⊷	USB Host Port using a USB type C connector. Used for software upgrade. See 'Software Upgrade' on page 72.
ETHERNET 1 & 2	Integrated 10/100/1000BASE-T layer-3 Ethernet switch / router using RJ45 connectors. Used for Ethernet user traffic and product management. See 'Ethernet Interface Connections' on page 88.
SERIAL	One port of RS-232 / RS-422 / RS-485 serial using RJ45 connector. See 'Serial RS-232 Interface Connections' on page 89 and 'Serial RS-422 / RS-485 Interface Connections' on page 90.
SFP 100/1000Base-X	SFP module socket see 'SFP Modules' on page 64. The Aprisa LTE router is supplied with dust plug fitted to SFP socket.
ANT 0 to ANT 3	Antenna connections using 50 ohm QMA female connectors. See '5G Antenna Ports' on page 59.
GNSS	GNSS (Global Navigation Satellite System) antenna using 50 ohm QMA female connector.

Rear Panel Connections

The rear panel connections to the Aprisa LTE 5G are:

Designator	Description
SIM cards 1 & 2	Removable plate for fitting of SIM cards. See 'Installing a SIM' on page 69

LED Indicators

The Aprisa LTE 5G LEDs indicate the following conditions:

	OK	AUX	SFP	TX (LTE)	RX (LTE)	Wi-Fi
Off	No input power detected	USB disabled or no USB device detected and GNSS disabled or not present	Disabled, SFP not fitted, no link or link failed	No LTE TX link	No LTE RX link	Wi-Fi not enabled, Wifi not linked (in client mode only) or no module fitted
Solid Green	All OK no alarms	USB device is detected OK or last GPS position valid	SFP fitted, and link detected OK	LTE TX link OK	LTE RX link OK	Wi-Fi enabled (access point mode) Wi-Fi linked with AP (client mode)
Flashing Green	Flashing between orange and green during bootup	Continuous slow flash - Waiting to provision from configurator Momentary – QR scan OK Flashing green / orange QR Scan being processed	SFP TX or RX traffic detected	LTE TX traffic detected	LTE RX traffic detected	Wi-Fi RX or TX traffic detected
Solid Orange	Warning & minor alarm	Device detect on the USB host port (momentary) and GPS position of poor quality (hdop > 5) when GNSS receiver enabled	SFP LOS (loss of signal) detected	LTE TX link in fallback to secondary SIM	LTE RX link in fallback to secondary SIM	Wi-Fi in client mode and connected OK
Flashing Orange	Flashing between orange and green during bootup	Management traffic on the USB port or receive invalid position from GNSS Flashing green / orange QR Scan being processed		LTE TX traffic when link in fallback	LTE RX traffic when link in fallback	Wi-Fi RX or TX traffic detected (client mode)
Solid Red	Critical & major alarm active, HW fail	GNSS is enabled but last known position is invalid Connected USB device is not functioning	SFP module reports an error	LTE TX link fail	LTE RX link fail	Wi-Fi not connected (client mode)
Flashing Red		GNSS Hardware Failure Momentary – QR scan failed	SFP module HW failure	LTE module HW failure	LTE module HW failure	Wi-Fi module HW failure

LED Colour	Severity
Green	No alarm (all OK) or Wi-Fi in AP mode
Orange	Warning alarm or LTE in fallback or Wi-Fi in client mode
Red	Critical, major or minor alarm

Ethernet / Serial Port LED Indicators

Ethernet / Serial (RS-232/482/422) RJ45 LED Indicators

LED Position (front facing)	LED Name	LED Color	Explanation
Right	Link LED	Off	Port is disabled, or not connected, or link failed.
		Solid Green	Port link detected and connected.
Left	Activity LED	Off	No data traffic detected on port.
		Flashing Orange	Data traffic detected on port.

Interfaces

Antenna Interfaces

Aprisa LTE 5G Front

- MAIN - Main cellular QMA 50 ohm female connector
- GNSS - Global Navigation Satellite System QMA 50 ohm female connector
- DIVERSITY – Diversity Cellular QMA 50 ohm female connector

    Used for receiver diversity and downlink MIMO operation.

- Wi-Fi 1 and Wi-Fi 2 antenna QMA 50 ohm female connectors

Aprisa LTE 5G Rear

- Dual SIM socket – a dual socket for fitting 2 x 3FF (micro SIM) cards

Ethernet Interface

- 2 port 10/100/1000 base-T Ethernet layer 2 switch using RJ45 female connector

    Used for Ethernet user traffic and modem network management.

RS-232 / RS-422 / RS-485 Interface

- 1 port RS-232 / RS-422 / RS-485 asynchronous port using RJ45 female connector

USB Interface

- 1 x USB port using USB standard type C female connector

    Used for software upgrade, QR code scanner, diagnostic reporting and configuration save / restore.

SFP Module Socket

- 1 x SFP Module Socket for fitting of optional SFP modules see 'SFP Modules' on page 64

Default Services

The following outbound services are enabled by default:

Interface	Protocol	IP Protocol	Port Number	Service	Purpose
sfp1	IPv4	UDP	67	DHCP Client	Provides IPv4 Autoconfiguration on WAN port
sfp1	IPv6	UDP	547	DHCPv6 Client	Provides IPv6 Autoconfiguration on WAN port
any	IPv4 or IPv6	UDP	123	NTP Client	Provides time autoconfiguration
any	IPv4 or IPv6	UDP	53	DNS Client	Provides Domain Name resolution

The following inbound services are enabled by default:

Interface	Protocol	IP Protocol	Port Number	Service	Purpose
sfp1	IPv4	UDP	68	DHCP Client	Provides IPv4 Autoconfiguration on WAN port
sfp1	IPv6	UDP	548	DHCPv6 Client	Provides IPv6 Autoconfiguration on WAN port
eth1, eth2	IPv4 or IPv6	UDP	53	DNS Server	Provides Domain Name resolution
any	IPv4 or IPv6	ICMP		ICMP Echo	Provide responses to ICMP Echo requests
eth1, eth2	IPv4 or IPv6	TCP	443	HTTPS	Provides Web interface for configuration and monitoring
eth1, eth2	IPv4 or IPv6	TCP	22	SSH	Provides CLI interface for configuration and monitoring

Network Architecture Overview

The following describes the Aprisa LTE 5G Architecture and its components. Figure 1 shows an Aprisa LTE 5G network reference model, consisting of LTE/E-UTRAN entities and EPC entities connected to PDN network.
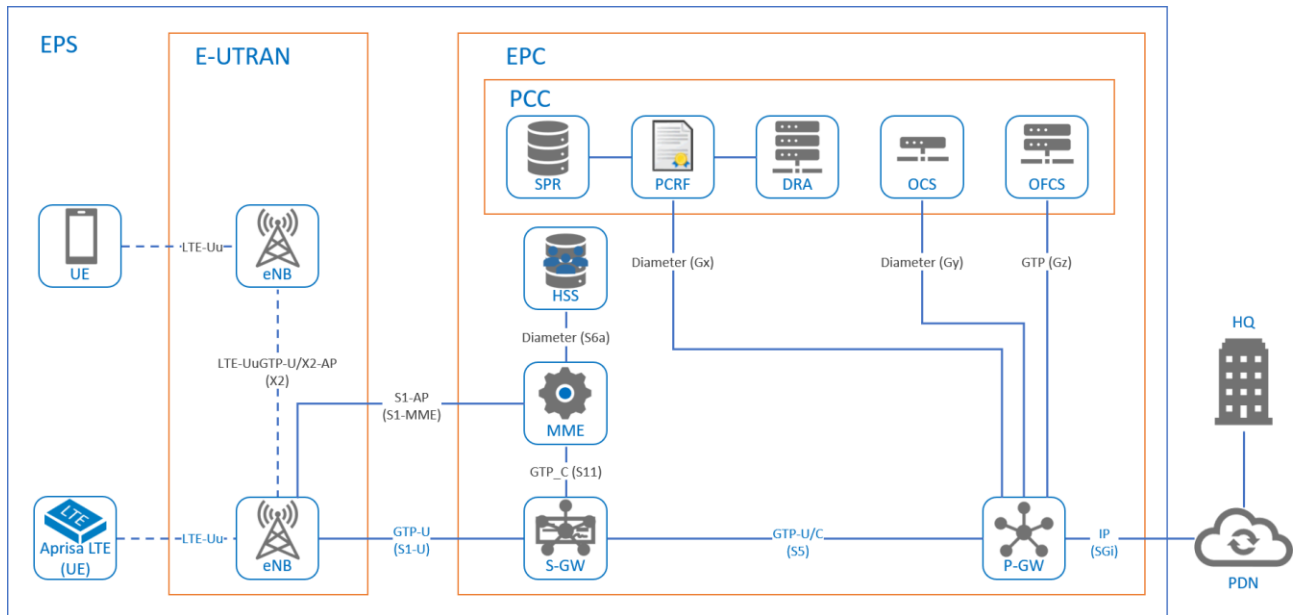

Figure 1 Network Reference Model

Entity	Description
EPS	The Aprisa LTE 5G network called EPS (Evolved Packet System) is an end-to-end (E2E) all IP network; EPS is divided into two main parts E-UTRAN and EPC. An E2E all IP network means that all traffic flows from a UE all the way to a PDN which connects to a service entity are transferred based on IP protocol within EPS.
E-UTRAN	The E-UTRAN (Evolved-Universal Terrestrial Radio Access Network) is the LTE part which deals with the technology related to a radio access network
EPC	The EPC (Evolved Packet Core) deals with the technology related to a core network. The EPC is based on IP as the transport technology for data and control plane (including for instance voice service).
PCC	The PCC (Policy and Charging Control) framework allows operators to control the service a customer receives over the network and its billing services (based on time or data volume or event occurring) based on the network state and SDF (Service Data Flow) IP flow QoS enforcement, i.e. the way traffic flows.
PDN	A PDN (Packet Data Network) is a generic term for the network that LTE subscriber would connect for mobile/fix data services. i.e. an internal or external IP domain of the operator and provides the UE with services such as the Internet, data services or IP Multimedia Subsystem (IMS). APN (Access Point Name) identifies a PDN Gateway (P-GW). It includes an APN network identifier which defines the PDN to which the UE requests connectivity and may also include an APN operator identifier which defines in which Public Land Mobile Network (PLMN) the P-GW is located.

The following describes the LTE/E-UTRAN components / entities.

Component	Description
UE	A UE (User Equipment) mobile device connects to an eNB. It is uniquely identified by their IMEI/IMSI (International Mobile Equipment/subscriber Identity). UE contain a SIM (Subscriber Identity Module) or USIM (Universal SIM) that holds the subscriber credentials associated with accessing services (IMSI, keys, ect).
eNB	An eNB serve as the base station within the E-UTRAN and provides users with the radio interfaces and performs Radio Resource Management (RRM) functions such as dynamic resource allocation, radio admission control, connection mobility control and Radio Bearer (RB) control and Inter-Cell Interference Coordination (ICIC), security and conducting inter eNB handover via X2 interface.

The following describes the EPC components / entities.

Component	Description
MME	An MME is the main control entity for the E-UTRAN. It communicates with an HSS for user authentication and user profile download and provides UEs with EPS Mobility Management (EMM) and EPS Session Management (ESM) functions using NAS signaling and it support the following main functions:
	NAS (Non-Access Stratum) signaling manage the establishment and continues communication sessions with the UE as it moves (EMM, ESM and NAS Security)
	User authentication and roaming with HSS
	Mobility management (Tracking Area (TAI) and handover management)
	EPS bearer management
S-GW	An S-GW terminates the interface towards an E-UTRAN. It serves as the local mobility anchor point of data connections for inter-eNB and inter-3GPP handover.
P-GW	A P-GW provides a UE with access to a PDN by assigning an IP address from the address space of the PDN. The P-GW serves as the mobility anchor point for handover between 3GPP and non-3GPP. It also performs policy enforcement, packet filtering and charging based on the PCC rules provided by a PCRF and it support the following main functions:
	IP routing and forwarding
	Per-SDF (Service Data Flow i.e. QoS)/Per-User based packet filtering
	UE IP address allocation
	Mobility anchoring between 3GPP and non-3GPP
	PCEF (Policy and Charging Enforcement Function) functions
	Charging per-SDF/per-User
HSS	An HSS is the central DB where user profiles are stored. It provides user authentication information and user profiles to the MME.
PCRF	A PCRF is the policy and charging control entity. It makes policy decisions for SDFs and provides the PCC rules (QoS and charging rules) to the PCEF (P-GW).
SPR	A SPR provides subscription information (access profile per subscriber) to the PCRF. Receiving the information, the PCRF performs subscriber-based policy and creates PCC rules.
DRA	A DRA (Diameter Routing Agent) enables the appropriate PCRF discovery and selections associate with subscriber.
OCS	An OCS provides a real-time credit control and a charging functions based on volume, time and event.
OFCS	An OFCS provides CDR (Charging Data Record) based charging information.

Applications

Cellular technology and in specific 4G Long-Term Evolution LTE have proliferated to almost all corners of the globe and continue to evolve toward full mobile broadband capability.

LTE technology allows an easy deployment of a Private LTE broadband network. It offers end-to-end IP centric and quality of service (QoS) with application delivery prioritization within LTE that extends from user equipment networks through LTE and backhaul transport and into the packet data network.

Aprisa LTE 5G has the required level of IP centric, security, ruggedized design, manageability, agility, flexibility, intelligence and customization within LTE broadband network to support variety of industries, market segments and applications.

Aprisa LTE 5G is very flexible network device and can combine a router and a switch / bridge function, where each interface can be configured to be used as part of the router or the switch / bridge ports (with internal connectivity between the switch and router functions).

The Aprisa LTE 5G supports the following market segments:

- ✓ Smart SCADA
- ✓ Transportation
- ✓ Smart City
- ✓ Backhaul
- ✓ Industrial Communication

Smart SCADA Applications

The Aprisa LTE 5G supports the following smart SCADA applications:

- ✓ Smart Grid – communication platform for self-healing / management power outage, resiliency (for security / physical attack), supply / demand-side management (SSM/DSM) and balancing of power load, power quality and capacitor bank control, and maintenance workforce mobility.

- ✓ Electric grid - communication platform for distribution automation, control and protection, monitoring transformers, and maintenance workforce mobility

- ✓ Water & wastewater - communication platform for pressure monitoring, pipeline monitoring and control, and maintenance workforce mobility

- ✓ Oil & Gas - communication platform for well head automation, pressure monitoring, pipeline monitoring and control

- ✓ Renewable – communication platform for control monitoring and manage wind power, photovoltaic (PV), water dam and sea wave power generation.

- ✓ Workforce mobility connectivity – communication platform providing smart SCADA workforce connectivity to the HQ with corporate ability to track workforce vehicles

- ✓ Train control – communication platform for train signaling

With the Aprisa LTE 5G, smart SCADA can be supported with single or dual SIM / operator LTE connectivity using a routed active / standby protection for high availability as shown in Figure 2 and Figure 3. In both cases, the user can exploit the option to use wireless LAN (WLAN) for local office connectivity or for local secure device management.

The Aprisa LTE 5G supports Ethernet / serial (using the embedded terminal server) / fiber optic (SFP) / Wi-Fi connection with RTU/PLC, supporting all IP / serial SCADA protocols. The user can disable or create local LAN switch / bridge with all, or part of the remaining interfaces not used at / or toward the WAN side of the network.
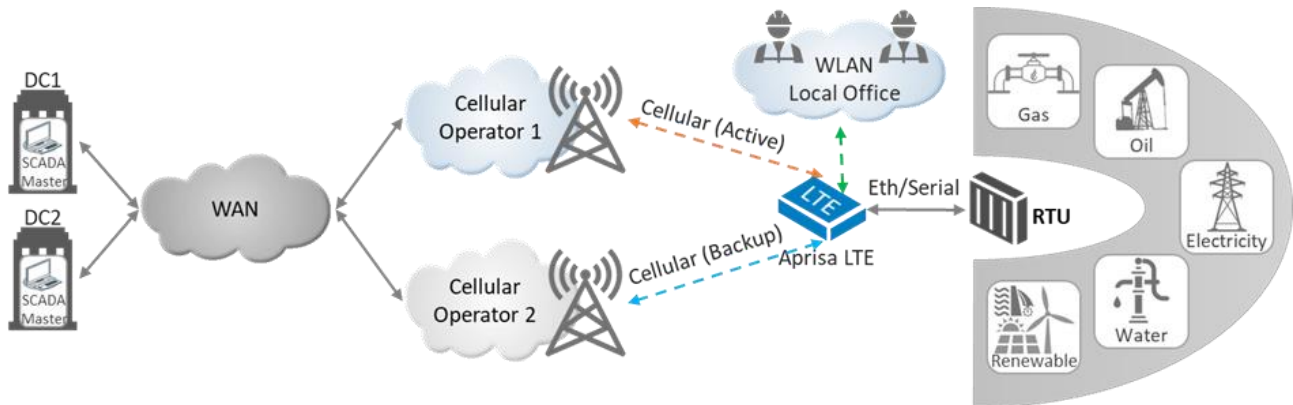
Figure 2 Smart SCADA Dual SIM / Operator for High Availability Solution
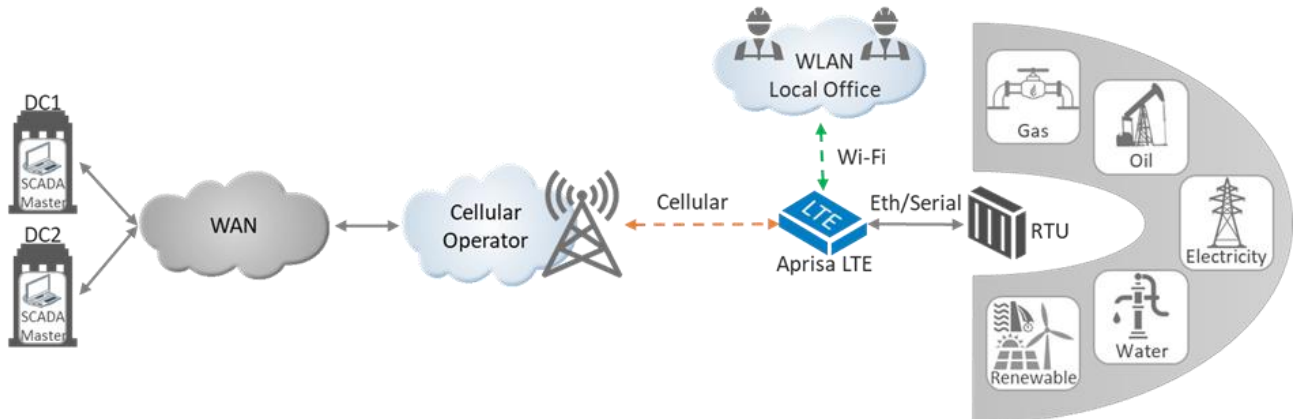
Figure 3 Smart SCADA Single SIM / Operator Solution

Smart SCADA high availability can be achieved by using any of the Aprisa LTE 5G interfaces as an alternate / protected path to the LTE cellular path as shown in Figure 4 (and as alternative to dual SIM/operator high availability solution). The Ethernet / Fiber optic / Wi-Fi interfaces can be used as a protected routing path to the LTE cellular path. The Aprisa LTE 5G router supports alternate routing and routing path metric priority.
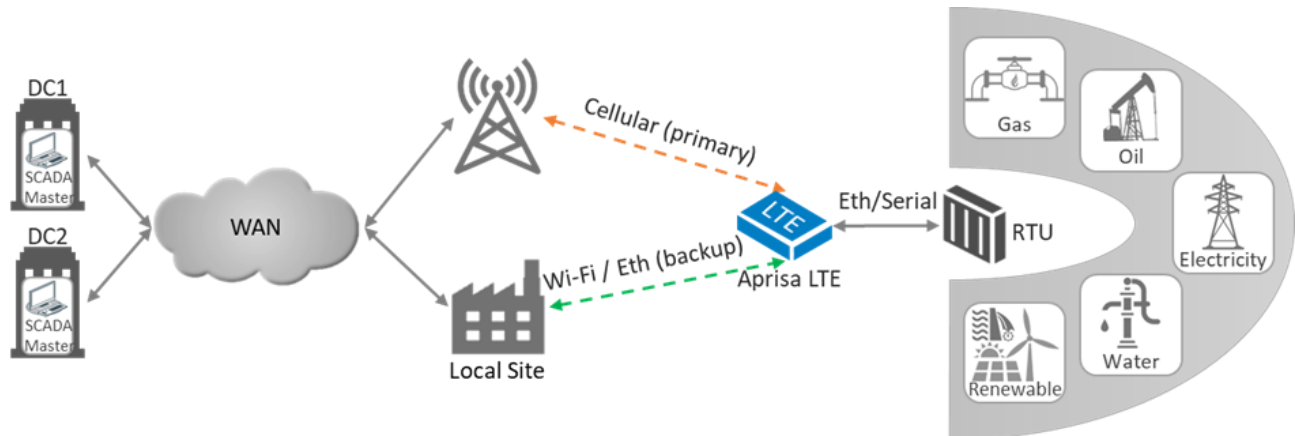
Figure 4 Smart SCADA LTE path and Any Interface Alternate Path Application

The Aprisa LTE 5G can be used in harsh environments like electrical substations, supporting IEEE 1613 (requirements for communications networking devices installed in electric power substations) and IEC 61850-3 (general requirements for communication networks and systems for power utility automation) standards. In addition, the Aprisa LTE 5G can be fitted with an optical fiber interface SFP which is particularly immune to noise generated in a substation environment as shown in Figure 5.
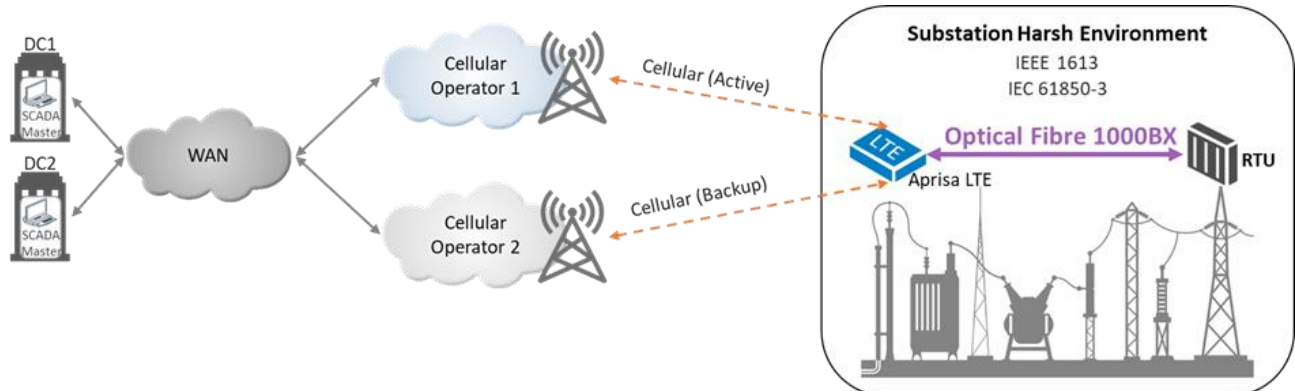
Figure 5 Smart SCADA in Substation Harsh Environment Application

In a smart SCADA AMI (Advanced metering infrastructure) / AMR (Automatic meter reading) application, the Aprisa LTE 5G can be used as a backhaul network, collecting the meter information directly from Wi-Fi meters or indirectly from an AMI collector that supports meters with a proprietary RF technology shown in Figure 6.
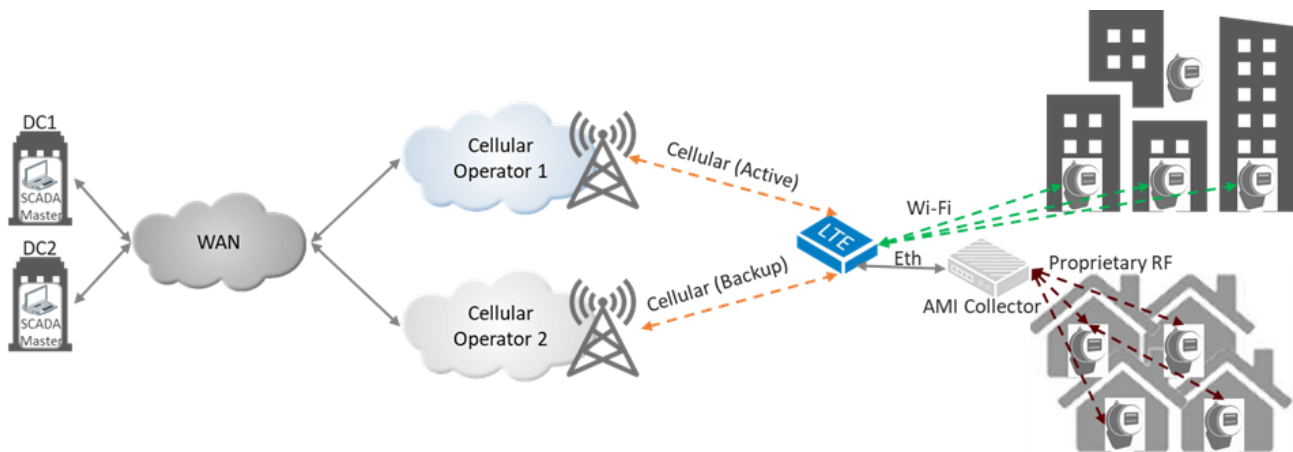
Figure 6 Smart SCADA AMI/AMR with Aprisa LTE 5G Backhauling Application

In a smart SCADA workforce (vehicle) mobility application, the Aprisa LTE 5G provides the field technician onsite Wi-Fi WLAN local connectivity and communication path to the HQ control center. The control center can track the vehicle on a map for security (e.g. theft) / auditing (including GNSS location, speed, and heading) and read online self-diagnostics and reporting / alerts state of the vehicle when the vehicle OBD II (On-Board Diagnostics II) interface is connected via an adapter (e.g. USB, Wi-Fi) to the Aprisa LTE 5G as shown in Figure 7.
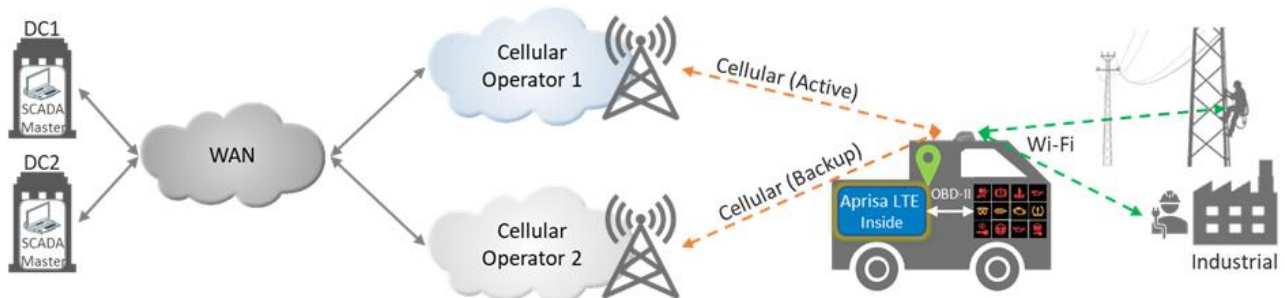
Figure 7 Smart SCADA Workforce Mobility Connectivity Application

Transportation Applications

The Aprisa LTE 5G support the following transportation applications:

- ✓ Public transportation - communication platform for train and buses comms, video surveillance and tracking
- ✓ Fleet management - communication platform for vehicle tracking and diagnostics.
- ✓ Public safety - communication platform for public safety ambulance, police and firefighter forces.

The Aprisa LTE 5G in a public transportation application provides the commuters a local Wi-Fi WLAN communication to connect to the public internet and provide the public management center the ability to track the train / bus location on a map, view the security cameras and read the bus diagnostic and alerts status as shown in Figure 8.
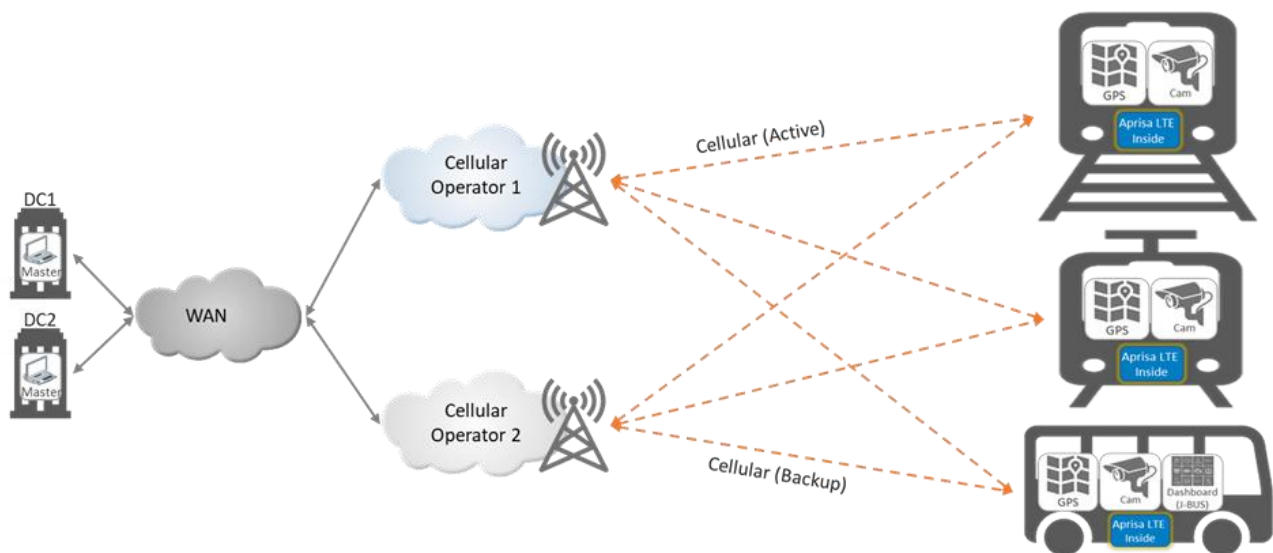
Figure 8 Public Transportation Application

The Aprisa LTE 5G in a fleet management application provides the corporate fleet management center the ability to track on a map (including GNSS location, speed, and heading) and read online self-diagnostics and reporting / alerts state (when OBD II interface is connected via an adapter (e.g. USB, Wi-Fi) to the Aprisa LTE 5G) of its fleet vehicles as shown in Figure 9.
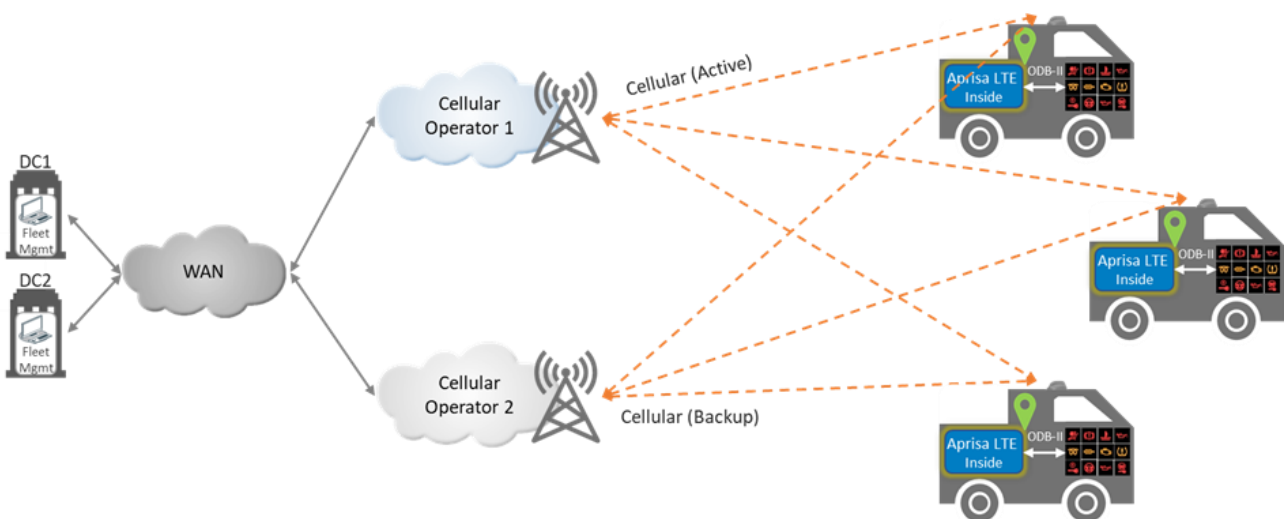
Figure 9 Fleet Management Application

The Aprisa LTE 5G in a public safety application provides the ambulance, police and firefighter forces the ability to track their vehicles on a map (including GNSS location, speed, and heading), read online vehicles self-diagnostics and reporting / alerts state (when OBD II interface is connected via an adapter (e.g. USB, Wi-Fi) to the Aprisa LTE 5G). The Aprisa LTE 5G also provides communication to the vehicle built-in computer and Wi-Fi connectivity to bodycams on ambulance doctors / police / firefighters as shown in Figure 10.
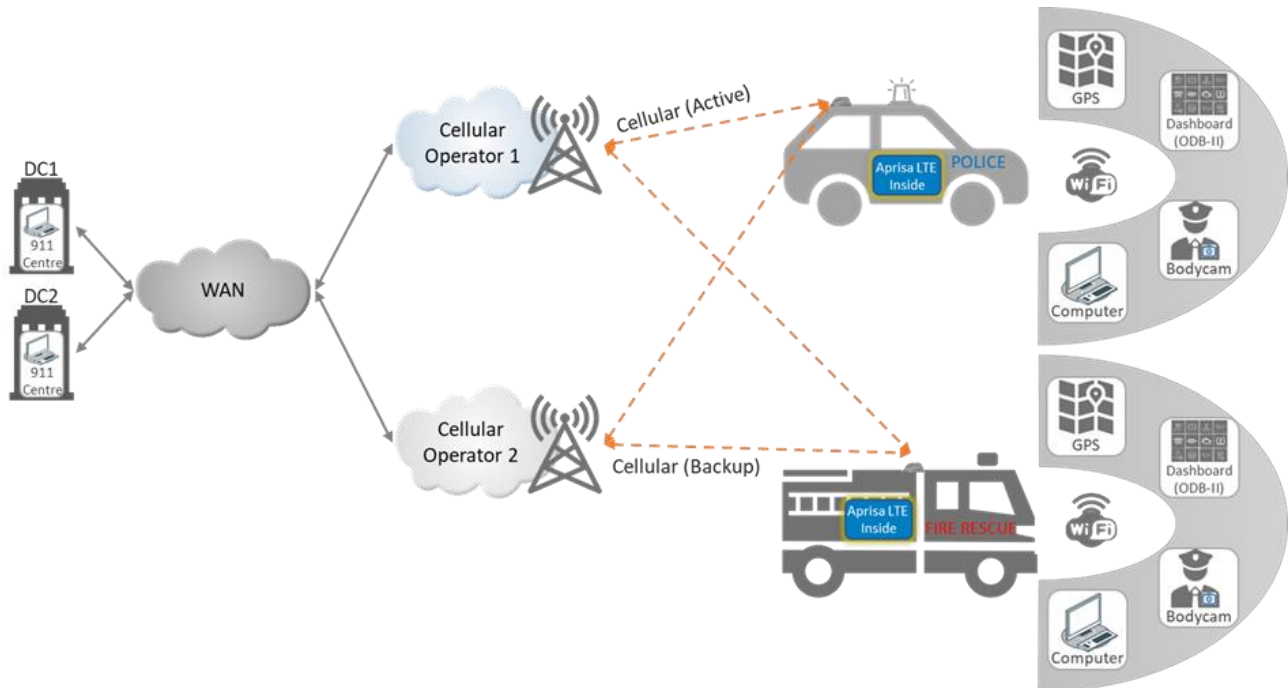
Figure 10 Public Safety Application

Smart City Applications

The Aprisa LTE 5G support the following smart city applications:

- ✓ A communication platform for city service, streetlight, traffic light, and video security.

The Aprisa LTE 5G in a smart city application provides communication to city security video cameras (connected via Ethernet or Wi-Fi), traffic lights and streetlight for city control center.
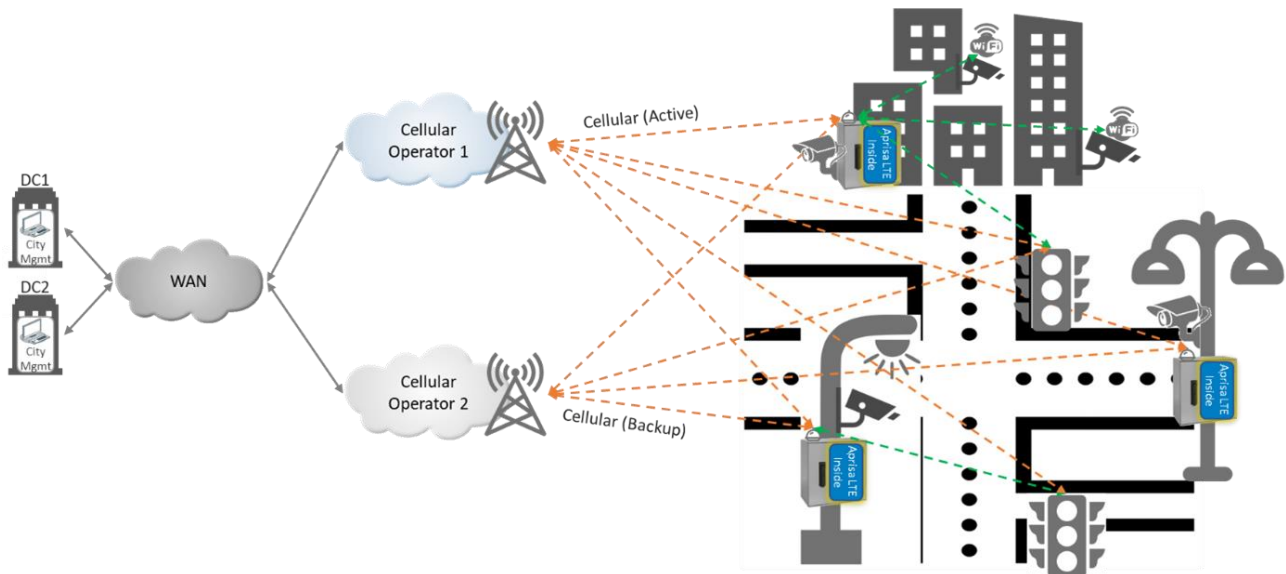
Figure 11 Smart City Application

Network Backhaul Applications

The Aprisa LTE 5G support the following network backhaul applications:

- ✓ SCADA backhauling
- ✓ AMI/AMR backhauling
- ✓ DMR backhauling

The Aprisa LTE 5G in a network backhauling application provides LTE backhauling communication network to smart SCADA licensed / unlicensed radio network and to AMI/AMR network as shown in Figure 12.
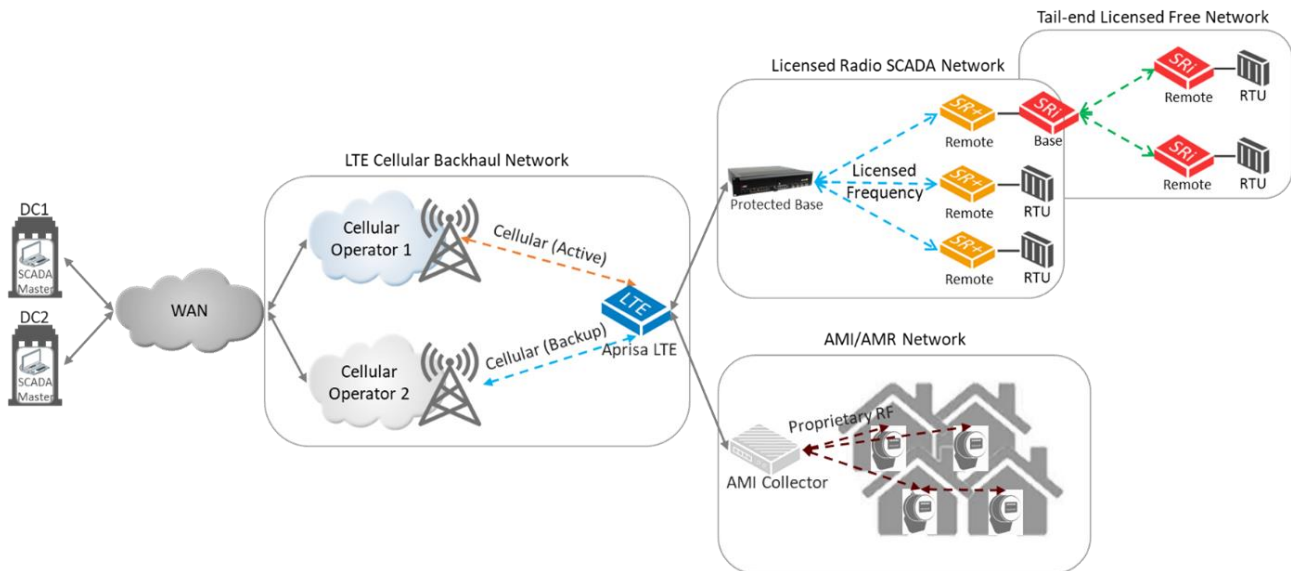
Figure 12 Network Backhauling Application

Industrial Communication Applications

The Aprisa LTE 5G support the following industrial communication applications:

- ✓ Industrial terminal server communication platform
- ✓ Substation / industrial switch/router communication platform
- ✓ Underground / sewerage Wi-Fi communication platform

The Aprisa LTE 5G in an industrial communication application provides a networking switch / router device functionality in a substation or industrial site and / or a terminal server device to connect a legacy serial device (e.g. serial RTU) to an IP network without the need to use the LTE network as shown in Figure 13.
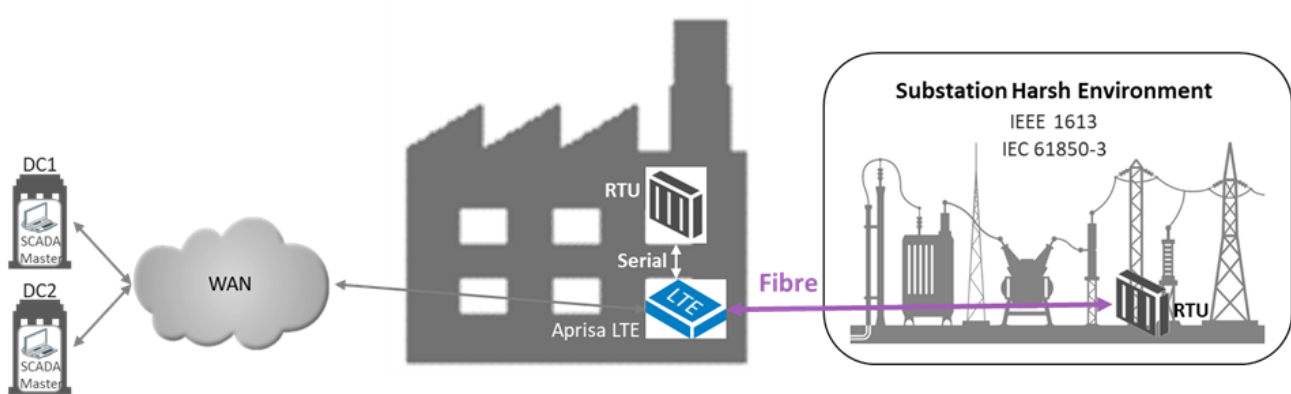
Figure 13 Industrial Communication Application

Leased Line Applications

The Aprisa LTE 5G supports the following leased line applications:

- ✓ Replace legacy TDM leased line that are dismantle by the operators with Ethernet/serial interface.

- ✓ Leased line via LTE network as alternative to wired WAN leased line.

- ✓ Any leased line topology supported: point-to-point (PTP), point to multipoint (PMP) and multipoint/mesh (MPMP).

- ✓ Supports any endpoint interface to any endpoint interface (e.g. Ethernet (fiber/copper) ←→ Serial)

The Aprisa LTE 5G in a leased line application, provides the required connectivity between endpoints with different interfaces across the LTE network with the ability to control the bandwidth and enforce QoS on this service as shown in Figure 14.
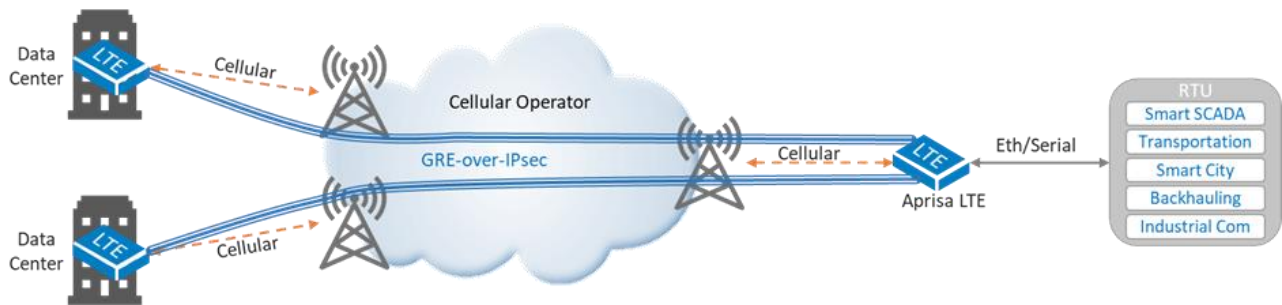
Figure 14 Leased Line Application

DMVPN Service Applications

The Aprisa LTE 5G supports the DMVPN service application. DMVPN is a service connectivity solution for organizations requiring secure full mesh/PMP VPNs between main corporate site/s (Hub) and remote sites (Spoke) over the internet with full networking and failover capabilities as shown in Figure 15.

The DMVPN service application supports the following options:

✓   Hub and spoke (PMP) - where multiple hubs and multiple spokes are supported.

✓   Spoke to Spoke (mesh) – a full mesh connectivity is supported between the hubs and spokes.

✓   NAT with DMVPN - NATed hub and/or spokes are supported.

✓   Uses multipoint GRE (mGRE) Tunnel, IPsec and NHRP (Next Hop Resolution Protocol) for a flexible virtual point to multipoint or full mesh secure VPN network.

✓   Can be used over dynamic routing protocols such as BGP and OSPF, BGP and EIGRP, OSPF and EIGRP, or static routes.

The Aprisa LTE 5G DMVPN service application supports the following benefits:

✓   Secure full mesh connectivity built for any service/s over the internet/private network.

✓   Replace or used as a backup service over the internet for leased line/private network.

✓   Uses mGRE, dynamic IPsec and NHRP for autoconfiguration of secure VPNs and full mesh creation.

✓   Zero touch configuration when adding/removing spoke sites (no hub nor spoke configuration is required).

✓   Full mesh reduce latency, bandwidth and eliminating hubs loads.
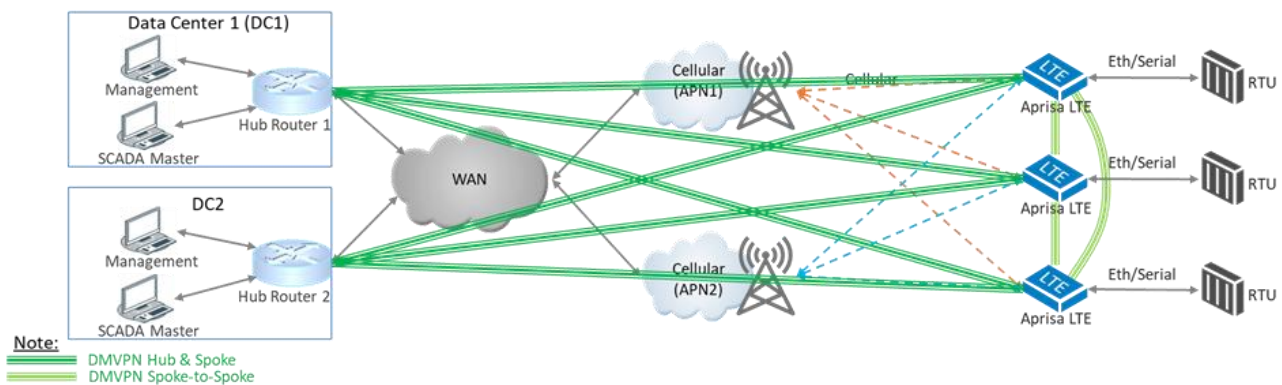
Figure 15 PMP and/or Mesh DMVPN Service Application
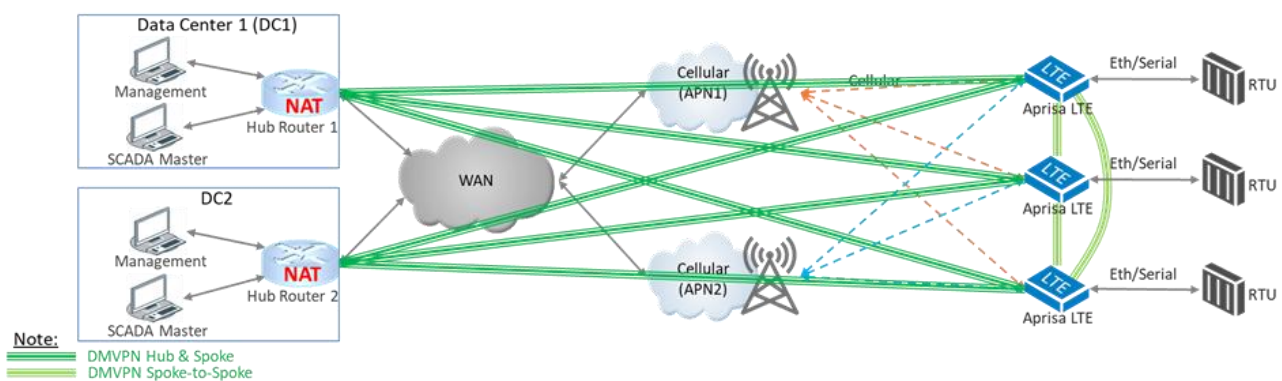
Figure 16 PMP and/or Mesh DMVPN Service with NATed Hubs Application

Dynamic Routing Applications

The Aprisa LTE 5G supports dynamic routing application over MP-BGP/BGP, OSPF and EIGRP or as interoperable routing domain between BGP and OSPF, BGP and EIGRP, and/or OSPF and EIGRP. The routing table can support more than 100k dynamic and static routes.

MP/BGP

MP / BGP is an EGP (Exterior Gateway Protocol) routing protocol designed for scale and used to connect different routing domains. BGP design to interwork with any IGP (Interior Gateway Protocol) routing protocol (OSPF, EIGRP, etc) and thus useful in organization with multiple IGP routing domains or with multiple ISP/Cell Operator connections.
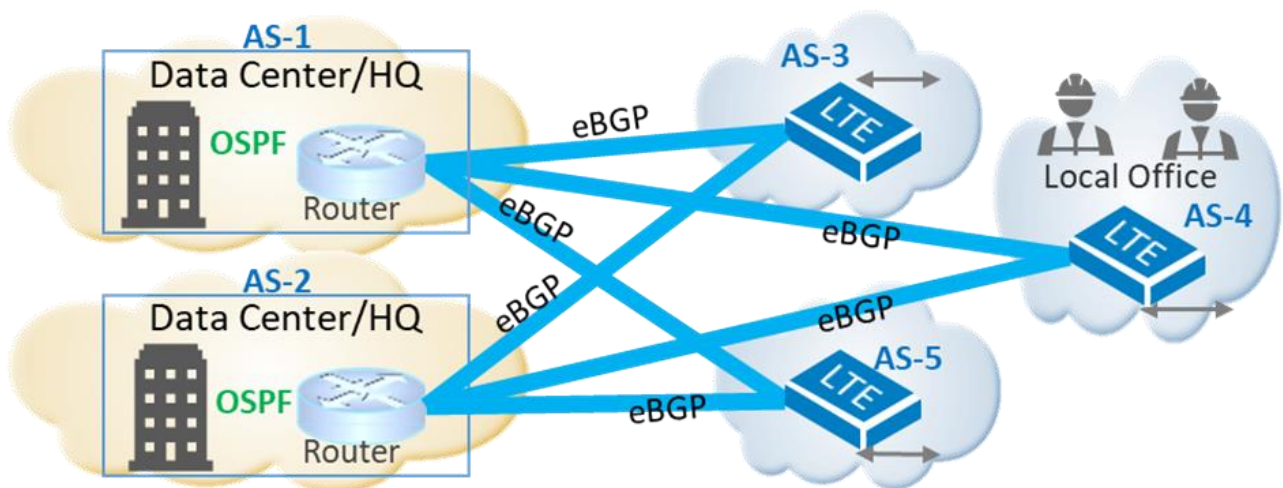
MP / BGP introduce the following benefits:

- ✓ When BGP is running inside routing domain/AS (Autonomous System), used as (internal) iBGP and between AS used as (external) eBGP.

- ✓ Interworks with all IGP protocols (OSPF, EIGRP, etc) and IPv4/v6 multicast/unicast (MP-BGP).

- ✓ Supports Loop prevention, redundancy, load sharing/balancing and use attributes as metrics (for routes).

- ✓ Manipulating routing policy and route selection for traffic in/out the AS (avoid full internet neighbours).

OSPF

OSPF (Open Shortest Path First) is a standardize Interior Gateway Protocol (IGP) and commonly used in large enterprise networks. OSPF is a link-state routing protocol providing fast convergence and excellent scalability. As a link-state protocols, OSPF is very efficient in its use of network bandwidth. It realizes the Link State routes and distribute routing information in an area.

OSPF introduce the following benefits:

- ✓ OSPF is loop free (derived by its own algorithm) and scalable supporting high number of routers in an AS.
- ✓ OSPF protocol design to minimize the traffic overhead and ensures a better use of bandwidth by sending updates only in case routing changes occur instead of periodically, uses short multicast hello message (for discovery and neighbours' maintenance), multicast instead of broadcast, minimize route exchange, NSSA (not-so-stubby area) concept to reduce route injection into extension of stub area, and ABRs (Area Border Routers) route aggregation to reduce route info.
- ✓ OSPF providing fast convergence time since routing changes are propagated instantaneously in short time and not periodically.
- ✓ OSPF allows load balancing.
- ✓ OSPF allows the concept of logical area division of networks where routers can be divided into areas in an Autonomous System (AS) to limit link state advertise updates over the whole network/AS. This also provides a mechanism for aggregating routes and summary of routing information between regions and cutting down on the unnecessary propagation of subnet information.
- ✓ OSPF supports routing authentication by using password and MD5 authentication.
- ✓ OSPF interoperable with BGP and IGP routing protocols, allowing external routes injection and keeps their tracks.

EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is an interior gateway protocol (IGP) suited for many different topologies and media. It is highly valued for its simplicity, ease of deployment, fast convergence, and commonly used in Enterprise networks. It maintains all the advantages of distance-vector protocols, while avoiding the concurrent disadvantages.

EIGRP introduces the following benefits:

- ✓ IPv4 / IPv6 network support
- ✓ For an IGP, it scales effectively on large DMVPN deployments in a well-designed network
- ✓ Very fast convergence times at network topology changes
- ✓ Only routing table changes are propagated to other routers (not all tables)
- ✓ Efficient links usage, through equal cost multipath (ECMP) and unequal cost load sharing
- ✓ Use of multicast and unicast communication
- ✓ Variable-length subnet masking (VLSM) support
- ✓ Seamless connectivity across all data link layer protocols and topologies

VRF (Virtual Routing and Forwarding) and VSI (Virtual Switch Instance)

Multi VSI is a virtual switch instance that allows almost the same capability as the VRF. Multi VSI allows group and/or service segregation and isolation each with its own MAC forwarding table (L2) on the same Aprisa LTE 5G platform. This allows any interface and virtual interface in Aprisa LTE 5G to be associated (enslaved) with a specific VSI that the user can create.

Multi VRF is a virtual routing instances that allows group and/or service segregation and isolation each with its own routing table (L3) on the same Aprisa LTE 5G platform to increases security. This allows any interface, virtual interface, and/or some protocol functions in Aprisa LTE 5G to be associated (enslaved) with a specific VRF that the user can create.

The following figures are two different examples using the VSI and VRF internally in the Aprisa LTE 5G. Multiple configurations can be formed to create Layer-2 and layer-3 segmentation / segregation and isolation between different groups or services on the Aprisa LTE 5G platform.
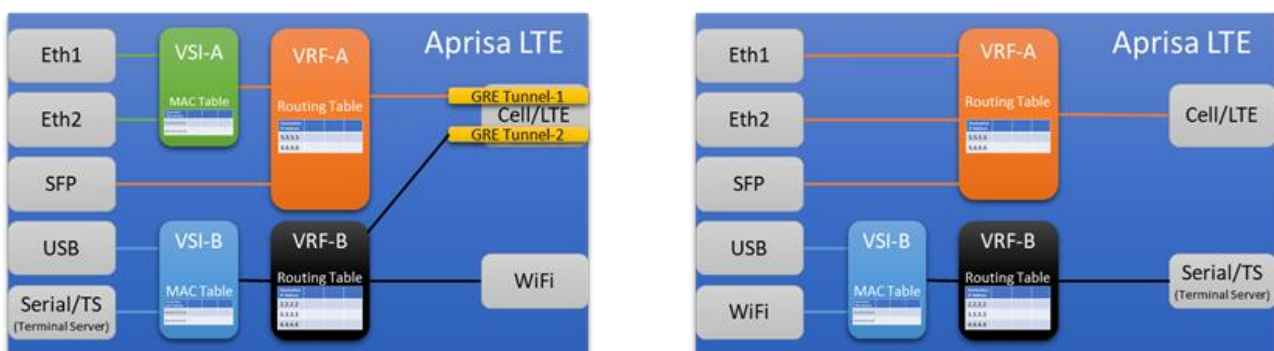
Aprisa LTE 5G physical interfaces (such as Ethernet, SFP, Cellular, Wi-Fi, Serial/Terminal Server), logical interfaces (such as VLAN, GRE tunnel, IPsec tunnel and child, VSI, Loopback, etc) and protocols (such as SSH, DHCP, and DNS) can be associated with a VRF or operate within a VRF.

All dynamic routing protocol (such as BGP/BGP-MP, OSPF, EIGRP, RIPv2) as well static routes and IPSLA can operate within a VRF.

Both SuperVisor web manager and CLI management interfaces are VRF aware and support the FCAPS management of VRF through these interfaces.

Maintenance / debug (such as ping, advance ping, traceroute, and nslookup), performance monitoring, events and alarms are all VRF aware.

The following figure describes a network using VRF to segregate and isolate three services and departments (video surveillance, management, and SCADA) in a company, each with its own routing table.

A DMVPN service can operate within a VRF and multiple DMVPN services can each work within its own VRF creating multiple segregated and isolated DMVPN services across the network and Aprisa LTE 5G.
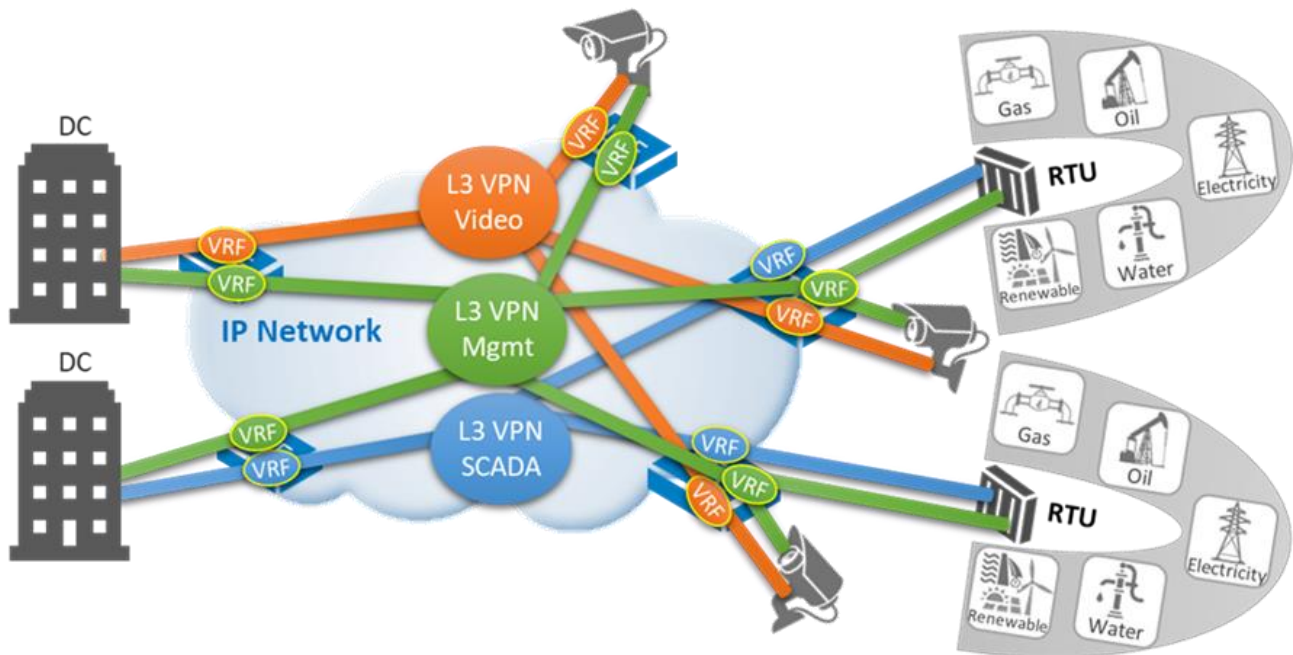
VSI and VRF introduces the following benefits:

- ✓ IPv4 / IPv6 network support
- ✓ Allow multiple virtual switch instances and virtual routing instances on the same Aprisa LTE 5G platform
- ✓ Allows multiple VSI and VRF to secure and isolate group/user/services
- ✓ Unlimited VRF and VSI supported
- ✓ Physical interfaces, logical interfaces, protocols, routing protocols, static routes, DMVPN, and management are all VRF aware and can operate within a VRF

Aprisa LTE 5G Multi-VRF also supports FVRF / IVRF which denotes for Front Door VRF / Inside VRF. IVRF/FVRF allow to build multiple isolated services or groups and isolate between inside VRF (IVRF) to outside (front door) VRF (FVRF) as shown in the following diagram
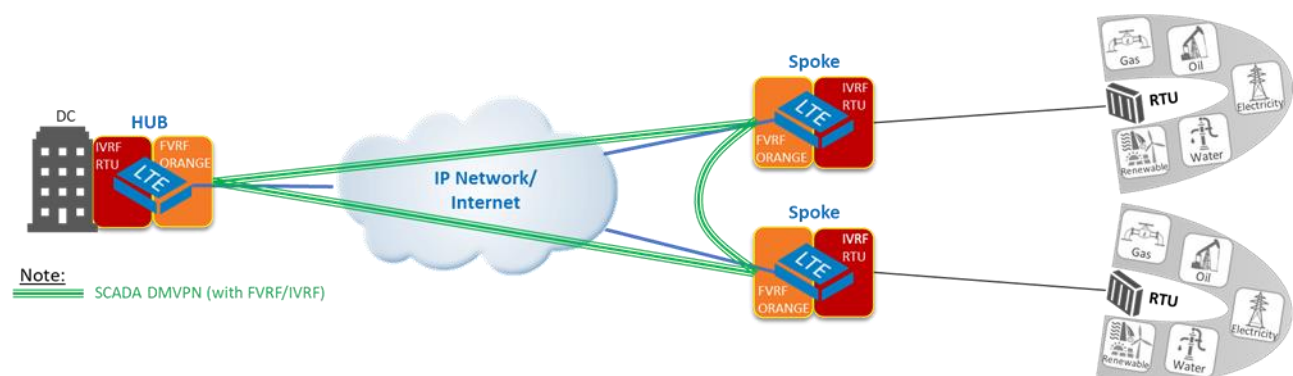
As shown in the diagram above, each GRE and IPsec tunnel is associated with two VRF domains, the FVRF and IVRF.

The outer encapsulated packet or local endpoint of the IPsec tunnel belongs to the FVRF domain, while the inner, protected IP packet or the source and destination addresses of the inside packet belongs to the IVRF.

FVRF/IVRFs provides the following benefits:

- ✓ Default route separation between traffic in IP/WAN/Internet network and the DMVPN tunnel network
- ✓ Control and data plane separation between inside (IVRF) and outside (FVRF) networks for security purposes
- ✓ Network segmentation of user traffic across an IP/WAN/internet network

More Information on DMVPN, BGP, OSPF, EIGRP, VRF / IVRF / FVRF Setup Applications

For more information on setting up basic BGP network, DMVPN network, DMVPN behind NAT network, DMVPN over BGP network, basic OSPF network, DMVPN over OSPF network, basic EIGRP network, DMVPN over EIGRP network, VRF aware DMVPN, and VRF aware dynamic and static routing. See the 'Aprisa LTE User Manual 3.6 Appendix 1 - DMVPN and Dynamic Routing Protocols Configuration Guide'.

Product options

The Aprisa LTE 5G provides the following LTE product options:

Network Module	Function	Part Number Option
AP	Standard Aprisa LTE 5G product	APLT-Mxxx-Nxx-Px-vx-TxAx
FN	Enhanced security features Band 14 first responder network use	FNLT-M002-Nxx-Px-vx-TxAx

Modules

The Aprisa LTE 5G provides the following LTE module options:

Code	Downlink Cat/CA**	Downlink Peak Mbit/s	Uplink Cat/CA**	Uplink Peak Mbit/s	Bands
M000					None
M001	Cat 12 / 3CA & Cat 9 / 3CA	600 / 450	Cat 13 / 2CA contig	150	B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B18, B19, B20, B26, B28, B29*, B30***, B32*, B41^T, B42^T, B43^T, B46*^{T}, B48^T, B66
M002	Cat 12 / 3CA & Cat 9 / 3CA	600 / 450	Cat 13 / 2CA contig	150	B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B14, B18, B19, B20, B26, B29*, B30***, B32*, B41^T, B42^T, B43^T, B46*^{T}, B48^T, B66
M003	Cat 6 / 2CA	FDD 300 TDD 222	Cat 6 / 2CA	FDD 50 TDD 26	B1, B2, B3, B4, B5, B7, B8, US B8A, B12, B13, B20, B25, B26, B29*, B30, B41^T
M005	Cat 7 / 2CA	300	Cat 13 / 2CA contig	150	B2, B4, B5, B7, B12, B13, B14, B25, B26, B41^T, B42^T, B43^T, B48^T, B66, B71
M006	Cat 7 / 2CA	300	Cat 13 / 2CA contig	150	B1, B3, B7, B8, B20, B28, B32, B38^T, B40^T, B41^T, B42^T, B43^T
M031	LTE: Cat 19 / 5CA	LTE/4G: 1600 5G NSA: 3400 5G SA: 2500	LTE: Cat 18 / 2CA contig	LTE/4G: 211 5G NSA: 460 5G SA: 900	4G bands: B1^{M4}, B2(B25)^{M4}, B3^{M4}, B4(B66)^{M4}, B26(B5, B18, B19), B7^{M4}, B8, B12(B17), B13, B14, B20, B28, B29, B30^{M4}, B32, B34, B38^{M4}, B39^{M4}, B40^{M4}, B41^{M4}, B42^{M4}, B43^{M4}, B46, B48(CBRS)^{M4}, B66^{M4}, B71 5G bands: n1^{M4}, n2^{M4}, n3^{M4}, n5, n7^{M4}, n8, n12, n13, n14, n18, n20, n25 M4, n26, n28, n29, n30^{M4}, n38$^{M4/M2}$, n40^{M4}, n41$^{T/M4/M2}$, n48$^{M4/M2}$, n66^{M4}, n71, n75^{M4}, n76, n77$^{T/M4/M2}$, n78$^{T/M4/M2}$, n79$^{T/M4/M2}$
M041	Cat 4	FDD 150 TDD 100	Cat 4	FDD 50 TDD 15	B2, B4, B5, US B8^A, B12, B13, B14, B26, B48^T, B66, B106^A

Note: The specifications and bands of these modules are updated over time.

Keys:

*	Downlink only
**	Carrier Aggregation
***	Uplink not supported for AT&T
T	TDD
A	Anterix B8, B106
M4	4x4 MIMO downlink support
M2	2x2 MIMO uplink support

Module Regional Deployment

The following are <u>typical</u> Aprisa LTE 5G Module deployments by region.

The deployment of Aprisa LTE 5G Module options may be dependent on regulatory requirements, and current availability. Please contact Aviat Networks for availability.

LTE Module	Part Number Option	USA	Canada	Asia / Pacific	Europe
M000	APLT-<u>M000</u>-Nxx-Px-xx-TxAx	✓	✓	✓	✓
M001	APLT-<u>M001</u>-Nxx-Px-xx-TxAx	✓	✓	✓	✓
M002	APLT-<u>M002</u>-Nxx-Px-xx-TxAx	✓	✓		
M003	APLT-<u>M003</u>-Nxx-Px-xx-TxAx	✓			
M005	APLT-<u>M005</u>-Nxx-Px-xx-TxAx	✓	✓		
M006	APLT-<u>M006</u>-Nxx-Px-xx-TxAx			✓	✓
M031	APLT-<u>M031</u>-Nxx-Px-xx-TxAx	✓	✓		
M041	APLT-<u>M041</u>-Nxx-Px-xx-TxAx	✓	✓		

Frequency Bands

Aprisa LTE Module LM001

Band	Frequency MHz (Tx)	Frequency MHz (Rx)	Standard
B1	1920-1980	2110-2170	LTE
B2	1850-1910	1930-1990	LTE
B3	1710-1785	1805-1880	LTE
B4	1710-1755	2110-2155	LTE
B5	824-849	869-894	LTE
B7	2500-2570	2620-2690	LTE
B8	880-915	925-960	LTE
B9	1749.9-1784.9	1844.9-1879.9	LTE
B12	699-716	729-746	LTE
B13	777-787	746-756	LTE
B17	704-716	734-746	LTE
B18	815-830	860-875	LTE
B19	830-845	875-890	LTE
B20	832-862	791-821	LTE
B26	814-849	859-894	LTE
B28	703-748	758-803	LTE
B29	n/a	717-728	LTE
B30	2305-2315	2350-2360	LTE
B32	n/a	1452-1496	LTE
B41	2496-2690 (TDD)		LTE
B42	3400-3600 (TDD)		LTE
B43	3600-3800 (TDD)		LTE
B46	n/a	5150-5925 (TDD)	LTE
B48	3550-3700 (TDD)		LTE
B66	1710-1780	2110-2200	LTE

Aprisa LTE Module LM002

Band	Frequency MHz (Tx)	Frequency MHz (Rx)	Standard
B1	1920-1980	2110-2170	LTE
B2	1850-1910	1930-1990	LTE
B3	1710-1785	1805-1880	LTE
B4	1710-1755	2110-2155	LTE
B5	824-849	869-894	LTE
B7	2500-2570	2620-2690	LTE
B8	880-915	925-960	LTE
B9	1749.9-1784.9	1844.9-1879.9	LTE
B12	699-716	729-746	LTE
B13	777-787	746-756	LTE
B14	788-798	758-768	LTE
B17	704-716	734-746	LTE
B18	815-830	860-875	LTE
B19	830-845	875-890	LTE
B20	832-862	791-821	LTE
B26	814-849	859-894	LTE
B29	n/a	717-728	LTE
B30	2305-2315	2350-2360	LTE
B32	n/a	1452-1496	LTE
B41	2496-2690 (TDD)		LTE
B42a	3400-3600 (TDD)		LTE
B43a	3600-3800 (TDD)		LTE
B46	n/a	5150-5925 (TDD)	LTE
B48a	3550-3700 (TDD)		LTE
B66	1710-1780	2110-2200	LTE

Aprisa LTE Module LM003

Band	Frequency MHz (Tx)	Frequency MHz (Rx)	Standard
B1	1920-1980	2110-2170	LTE
B2	1850-1910	1930-1990	LTE
B3	1710-1785	1805-1880	LTE
B4	1710-1755	2110-2155	LTE
B5	824-849	869-894	LTE
B7	2500-2570	2620-2690	LTE
B8	880-915	925-960	LTE
B12	699-716	729-746	LTE
B13	777-787	746-756	LTE
B17	704-716	734-746	LTE
B20	832-862	791-821	LTE
B25	1850-1915	1930-1995	LTE
B26	814-849	859-894	LTE
B29	n/a	717-728	LTE
B30	2305-2315	2350-2360	LTE
B41	2496-2690 (TDD)		LTE

Aprisa LTE Module LM005

Band	Frequency MHz (Tx)	Frequency MHz (Rx)	Standard
B2	1850-1910	1930-1990	LTE
B4	1710-1755	2110-2155	LTE
B5	824-849	869-894	LTE
B7	2500-2570	2620-2690	LTE
B12	699-716	729-746	LTE
B13	777-787	746-756	LTE
B14	788-798	758-768	LTE
B17	704-716	734-746	LTE
B25	1850-1915	1930-1995	LTE
B26	814-849	859-894	LTE
B41	2496-2690 (TDD)		LTE
B42	3400-3600 (TDD)		LTE
B43	3600-3800 (TDD)		LTE
B48	3550-3700 (TDD)		LTE
B66	1710-1780	2110-2200	LTE
B71	663-698	617-652	LTE

Aprisa LTE Module LM006

Band	Frequency MHz (Tx)	Frequency MHz (Rx)	Standard
B1	1920-1980	2110-2170	LTE
B3	1710-1785	1805-1880	LTE
B7	2500-2570	2620-2690	LTE
B8	880-915	925-960	LTE
B20	832-862	791-821	LTE
B28	703-748	758-803	LTE
B32	n/a	1452-1496	LTE
B38	2570-2620 (TDD)		LTE
B40	2300-2400 (TDD)		LTE
B41	2496-2690 (TDD)		LTE
B42	3400-3600 (TDD)		LTE
B43	3600-3800 (TDD)		LTE

Aprisa LTE 5G Module LM031 - 4G bands

Band	Frequency MHz (Tx)	Frequency MHz (Rx)	Standard
B1	1920-1980	2110-2170	LTE
B2	1850-1910	1930-1990	LTE
B3	1710-1785	1805-1880	LTE
B4	1710-1755	2110-2155	LTE
B7	2500-2570	2620-2690	LTE
B8	880-915	925-960	LTE
B12	699-716	729-746	LTE
B13	777-787	746-756	LTE
B14	788-798	758-768	LTE
B17	704-716	734-746	LTE
B20	832-862	791-821	LTE
B28	703-748	758-803	LTE
B29	n/a	717-728	LTE
B30	2305-2315	2350-2360	LTE
B32	n/a	1452-1496	LTE
B34	2010-2025 (TDD)		LTE
B38	2570-2620 (TDD)		LTE
B39	1880-1920 (TDD)		LTE
B40	2300-2400 (TDD)		LTE
B41	2496-2690 (TDD)		LTE
B42	3400-3600 (TDD)		LTE
B43	3600-3800 (TDD)		LTE
B46	n/a	5150-5925 (TDD)	LTE
B48	3550-3700 (TDD)		LTE
B66	1710-1780	2110-2200	LTE
B71	663-698	617-652	LTE

Aprisa LTE 5G Module LM031 - 5G bands

Band	Frequency MHz (Tx)	Frequency MHz (Rx)	Standard
n2	699-716	729-746	5G
n3	777-787	746-756	5G
n5	788-798	758-768	5G
n7	815-830	860-875	5G
n8	832-862	791-821	5G
n12	1850-1915	1930-1995	5G
n13	814-849	859-894	5G
n14	703-748	758-803	5G
n18	699-716	729-746	5G
n20	777-787	746-756	5G
n25	788-798	758-768	5G
n28	815-830	860-875	5G
n30	2570-2620		5G
n38	2300-2400		5G
n40	2496-2690		5G
n41	3550-3700		5G
n48	2570-2620		5G
n66	1710-1780	2110-2200	5G
n71	663-698	617-652	5G
n75	-	1432-1517	5G
n76	-	1427-1432	5G
n77	3300-4200 (TDD)		5G
n78	3300-3800 (TDD)		5G
n79	4400-5000 (TDD)		5G

Aprisa LTE Module LM041

Band	Frequency MHz (Tx)	Frequency MHz (Rx)	Standard
B2	1850-1910	1930-1990	LTE
B4	1710-1755	2110-2155	LTE
B5	824-849	869-894	LTE
B8	880-915	925-960	LTE
B12	699-716	729-746	LTE
B13	777-787	746-756	LTE
B14	788-798	758-768	LTE
B26	814-849	859-894	LTE
B48	3550-3700 (TDD)		LTE
B66	1710-1780	2110-2200	LTE

5G Antenna Ports

Aprisa LTE 5G Module LM031

Antenna Port	Technology	Tx	Rx
ANT 0	LTE	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B30, B34, B38, B39, B40, B41, B66, B71	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29(SDL), B30, B32(SDL), B34, B38, B39, B40, B41, B42, B43, B46(SDL), B48, B66, B71
	5G NR FR1	n1, n2, n3, n5, n7, n8, n20, n25, n28, n30, n38, n40, n41, n66, n71	n1, n2, n3, n5, n7, n8, n20, n25, n28, n30, n38, n40, n41, n48, n66, n71, n75(SDL), n77, n78, n79
ANT 1	LTE	-	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B30, B34, B38, B39, B40, B41, B66, B71
	5G NR FR1	n48, n77, n78, n79	n1, n2, n3, n5, n7, n8, n20, n25, n28, n30, n38, n40, n41, n66, n71
ANT 2	LTE	-	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29(SDL), B30, B32(SDL), B34, B38, B39, B40, B41, B42, B43, B46(SDL), B48, B66, B71
	5G NR FR1	n38, n41	n1, n2, n3, n5, n7, n8, n20, n25, n28, n30, n38, n40, n41, n48, n66, n71, n75(SDL), n77, n78, n79
ANT 3	LTE	B42, B43, B48	B1, B2, B3, B4, B7, B25, B30, B32(SDL), B34, B38, B39, B40, B41, B42, B43, B48, B66
	5G NR FR1	n48, n77, n78, n79	n1, n2, n3, n7, n25, n30, n38, n40, n41, n48, n66, n75(SDL), n77, n78, n79

Network Modules

The Aprisa LTE 5G provides the following Network Module options:

Network Module	Function	Part Number Example
N00	No network module fitted to the LTE	APLT-M001-N00-P0-V0-T0A0
N01	Wi-Fi IEEE 802.11ac (Wave 2), 2x2 receive Multi-User MIMO	APLT-M001-N01-P0-V0-T0A1

Processor Options

The Aprisa LTE 5G provides processor options:

Processor	Function	Part Number Example
P0	SOM A388	APLT-M001-N00-P0-V0-T0A0
P1	(future processor option)	APLT-M001-N00-P1-V0-T0A0

Power Supply Options

The Aprisa LTE 5G provides power supply options:

Power Supply	Function	Part Number Example
V	9–32 VDC neg earth input power	APLT-M001-N00-P0-V0-T0A0
W	(future power option)	APLT-M001-N00-P0-W0-T0A0

Tamper Protection Option

The Aprisa LTE 5G provides a tamper protection option:

Option	Function	Part Number Example
0	No tamper protection fitted to the Aprisa LTE 5G	APLT-M001-N01-P0-V0-T0A0
1	Tamper Protection fitted to the Aprisa LTE 5G	APLT-M001-N01-P0-V1-T0A0

The Aprisa LTE 5G tamper protection provides electronic and physical tamper detection to prevent unauthorized LTE movement and access to sensitive stored information. It uses a Trusted Platform Module (TPM) to provide secure storage of key material.

If a tamper is detected, this device will immediately erase any encryption keys in the battery backed tamper protected memory. Factory default settings are immediately loaded, and a tamper event will be flagged at the next boot.

The tamper module uses a replaceable 3V lithium battery to operate the tamper circuits even if the router is disconnected from power.

CAUTION:

- There is a risk of fire or explosion if the lithium battery is replaced by an incorrect type.
- Disposal of a lithium battery into fire or a hot oven, or mechanically crushing or cutting of the battery can result in an explosion.
- Leaving a lithium battery in an extremely high temperature surrounding environment that can result in an explosion or the leakage of flammable liquid or gas.
- A lithium battery subjected to extremely low air pressure that may result in an explosion or the leakage of flammable liquid or gas.

Tethered Options

The Aprisa LTE 5G tethered options:

Option	Function	Part Number Example
T0	Not tethered to any carrier	APLT-M001-N01-P0-V0-T0A0
T1	Tethered to AT&T	APLT-M001-N01-P0-V0-T1A0
T2	Tethered to Verizon	APLT-M001-N01-P0-V0-T2A0

Wi-Fi Region

The Aprisa LTE 5G Wi-Fi region options:

Option	Function	Part Number Example
A0	Wi-Fi Region 00 Not region specific, all regionally restricted bands are excluded	APLT-M001-N01-P0-V0-T0A0
A1	Wi-Fi Region 01 USA FCC Brazil Anatel	APLT-M001-N01-P0-V0-T0A1
A2	Wi-Fi Region 02 Canada ICES	APLT-M001-N01-P0-V0-T0A2
A3	Wi-Fi Region 03 Europe ETSI	APLT-M001-N01-P0-V0-T0A3
A4	Wi-Fi Region 04 Australia ACMA New Zealand RSM	APLT-M001-N01-P0-V0-T0A4

Hardware Types

Currently there are two hardware type variants of the Aprisa LTE 5G.

Option	Function
HW Type A	Standard Aprisa LTE 5G
HW Type B	USB CLI mode option
HW Type C	5G options

The Aprisa LTE 5G hardware type can be identified from SuperVisor (see 'Terminal > Details' on page 103) or from the Compliance label on the enclosure bottom.

Accessories

SFP Modules

The following Small Form-factor Pluggable (SFP) Modules are available from Aviat Networks as accessories:

Part Number	Description
APLB-MSFP-ETH	Aprisa LTE 5G SFP Module Ethernet 1000BASE-T Connector RJ45
APLB-MSFP-085-MM-SW-P5IT	Aprisa LTE 5G SFP Module Data Rate 1.25 Gbit/s Fibre Optic 850nm, multi-mode, single wavelength Connector LC Duplex Distance up to 0.55 km Operating temperature range -40 to +85C
APLB-MSFP-085-MM-SW-P5ST	Aprisa LTE 5G SFP Module Data Rate 1.25 Gbit/s Fibre Optic 850nm, multi-mode, single wavelength Connector LC Duplex Distance up to 0.55 km Operating temperature range -10 to +70C
APLB-MSFP-131-SM-SW-02IT	Aprisa LTE 5G SFP Module Data Rate 1.25 Gbit/s Fibre Optic 1310nm, single-mode, single wavelength Connector LC Duplex Distance up to 2 km on 9/125µm SMF Operating temperature range -40 to +85C
APLB-MSFP-131-SM-SW-10ST	Aprisa LTE 5G SFP Module Up to 1.25 Gbit/s bi-directional data links Fibre Optic 1310nm, single-mode, single wavelength Connector LC Duplex Distance up to 10 km on 9/125µm SMF Operating temperature range 0 to +70C
APLB-MSFP-131-SM-SW-40ST	Aprisa LTE 5G SFP Module Up to 1.25 Gbit/s bi-directional data links Fibre Optic 1310nm, single-mode, single wavelength Connector LC Duplex Distance up to 40 km on 9/125µm SMF Operating temperature range 0 to +70C

Part Number	Description
APLB-MSFP-155-SM-SW-80ST	Aprisa LTE 5G SFP Module Up to 1.25 Gbit/s bi-directional data links Fibre Optic 1550nm, single-mode, single wavelength Connector LC Duplex Distance up to 80 km on 9/125µm SMF Operating temperature range 0 to +70C

Antennas

The following antennas are available from Aviat Networks as accessories:

Part Number	Description
APLB-ACEL-MTB-DM-B5-BK	Aprisa LTE 5G cellular multiband antenna GNSS x1 / LTE x2 / WiFi x2 Dimensions - (LxWxH) 202.3mm x 88.5mm x 45mm (7.96 in x 3.48 in x 1.77 in) Mount - Direct Mount Connectors - 5x QMA straight Cables - 5.2m black WiFi / LTE cable LMR-195 GNSS cable LMR-100
APLB-APNL-3GH-DP-NF	Aprisa LTE 5G 3.3-4.01 GHz dual polarization / dual slant panel antenna Dimensions – 305 x 305 x 25 mm Polarization - Dual Linear Vertical Beamwidth - 17deg Horizontal Beamwidth - 17deg Connectors - 2x N type Female Gain - 19.5 dBi Includes mount MNT-22
APLB-AONI-CBL-GH-QM	Aprisa LTE 5G 600 MHz - 6 GHz wideband ground / vault mount omni antenna Suitable for LTE, 5G, IOT, WiFi, Bluetooth, LoRa, Cat-M Connectors - Antenna is fitted with a 6 ft cable terminated with a QMA male connector Gain - 2.0 dBi Dimensions: diameter x height – mm (inches) 78.4 x 104.7 (3.1 x 4.1) Requires a 2" mounting hole
APLB-AONI-CBL-AH-QM	Aprisa LTE 5G 600 MHz - 6 GHz Ultra-Wide Band AirHog omni antenna Ground Plane Independent, Dynamic Tuning Suitable for LTE, 5G, IOT, WiFi, Bluetooth, LoRa, Cat-M Connectors - Antenna is fitted with a 6 ft cable terminated with a QMA male connector Gain (typical) 2.5 dBi Mounting Height: 100.7mm Dimensions 100.7mm tall x 35mm wide
APLB-AONI-CBR-NF	Aprisa LTE 5G omnidirectional low PIM collinear antenna operates over the CBRS band 3550-3700 MHz Dimensions – diameter x height – mm (inches) 25.4 x 257 (1.0 x 10.0) Polarization - Vertical, Linear Connectors - N type Female Gain - 6.8 dBi

Part Number	Description
APLB-AONI-GNS-QM-01	GNSS antenna indoor / outdoor Bands – BEIDOU, GPS, GLONASS, no Wi-Fi, no LTE Suitable for most GNSS or asset tracking applications 2.1m (7ft) LMR195 cable terminated with a QMA male connector Gain: 2.6 dBi (GPS) and >4.4 dBi (GLONAS and BEIDOU) Dimensions: 48mm round, 14.9mm high Requires a 12mm mounting hole
APLB-APNL-3GH-DP-NF	Aprisa LTE 5G 3.3-4.01 GHz dual polarization / dual slant panel antenna Dimensions – 305 x 305 x 25 mm Polarization - Dual Linear Vertical Beamwidth - 17deg Horizontal Beamwidth - 17deg Connectors - 2x N type Female Gain - 19.5dBi
LRD GNS1559MPF-213QMAM	GNSS antenna indoor / outdoor Bands – BEIDOU, GPS, GLONASS, no Wi-Fi, no LTE Suitable for most GNSS or asset tracking applications 2.1m (7ft) LMR195 cable terminated with a QMA male connector Gain: 2.6 dBi (GPS) and >4.4 dBi (GLONAS and BEIDOU) Dimensions: 48mm round, 14.9mm high Requires a 12mm mounting hole
LRD GNS1559MPF-518QMAM	GNSS antenna indoor / outdoor Bands – BEIDOU, GPS, GLONASS, no Wi-Fi, no LTE Suitable for most GNSS or asset tracking applications 5.1m (17ft) LMR195 cable terminated with a QMA male connector Gain: 2.6 dBi (GPS) and >4.4 dBi (GLONAS and BEIDOU) Dimensions: 48mm round, 14.9mm high Requires a 12mm mounting hole
LRD VFP69383B22JN-213YMO	Aprisa LTE 5G 600 MHz - 6 GHz wideband omni-directional vehicular antenna 5 ports with 2.1m (7ft) LMR195 cable terminated with QMA male connectors Dimensions: 179 x 63 x 48mm (7.04 x 2.48 x 1669 in)
LRD VFP69383B22JN-518YMO	Aprisa LTE 5G 600 MHz - 6 GHz wideband omni-directional vehicular antenna 5 ports with 5.1m (17ft) LMR195 cable terminated with QMA male connectors Dimensions: 179 x 63 x 48mm (7.04 x 2.48 x 1669 in)
LRD PAS69278P-91NF	The PAS69278 antenna is a wide-band dual-port directional panel antenna with slant 45 polarization that covers the domestic LTE700/Cellular/PCS/AWS/MDS and global GSM900/GSM1800 / UMTS/LTE2600 bands. The antenna is ideal for both indoor and outdoor applications - UV-stable radome enclosure. 2 port 91cm (36") LMR195 cable with dual N type female connectors Dimensions: 295 x 295 x 82mm

Mounting

Part Number	Description
APGA-MBRK-DIN	DIN rail mounting bracket for mounting of the Aprisa LTE 5G. Steel bracket Width= 178 mm, Depth= 116 mm, Height= 52 mm

Cables

Part Number	Description
APLB-PPWR-X01	Aprisa LTE 5G power cable fitted with 4 pin Molex Micro-Fit 3.0 female connector and wire ended Cable length 1m Pin 1 Red +ve Power Input Pin 2 Black -ve Power Input Pin 3 Green Digital Input Pin 4 White Digital Output
APLB-PPWR-X10	Aprisa LTE 5G power cable fitted with 4 pin Molex Micro-Fit 3.0 female connector and wire ended Cable length 10m Pin 1 Red +ve Power Input Pin 2 Black -ve Power Input Pin 3 Green Digital Input Pin 4 White Digital Output
VEN TRFC-8311-19	RF Cable Asm, QMA M straight to N type M straight, LMR-195, 0.5m
VEN TRFC-8311-24	RF Cable Asm, QMA M straight to N type M straight, LMR-195, 0.6m
VEN TRFC-8311-36	RF Cable Asm, QMA M straight to N type M straight, LMR-195, 0.9m
VEN TRFC-8311-120	RF Cable Asm, QMA M straight to N type M straight, LMR-195, 3m
VEN TRFC-8311-204	RF Cable Asm, QMA M straight to N type M straight, LMR-195, 5m

Adapters

Part Number	Description
APLB-AQMM-SMF	QMA Male to SMA Female Adapter
APLB-AQMM-SMP	QMA Male to SMA Male Adapter - reverse outer conductor (RPSMA jack male pin)

2. Aprisa LTE 5G Router Installation

Basic Hardware Setup

Installing a SIM

A wireless broadband data plan must be added to your Aprisa LTE 5G, which are available from cellular operators such as Verizon, and AT&T and come with SIM card(s).

The Aprisa LTE 5G can accommodate two standard 3FF (micro SIM) cards (12 x 15mm) which fit into the product rear under the SIM cards cover plate.
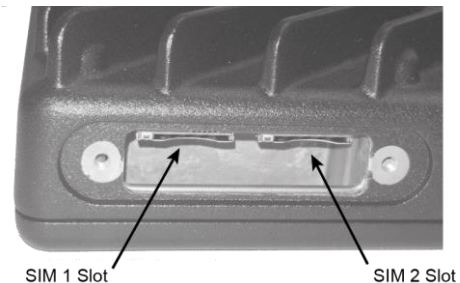
Once you have an activated SIM, insert it into the Aprisa LTE 5G SIM 1 Slot.

Use the SIM 2 slot for a backup SIM for an active/standby operation.

To install a SIM in the Aprisa LTE 5G router:

1. Turn the Aprisa LTE 5G power off (hot insertion or removal of SIMs is not supported).

2. Unscrew the two screws on the SIM cards cover plate.

3. Insert the SIM to the required slot notch-end first with metal contacts facing up.

4. Refit the SIM card cover plate and screw the two screws.

5. Turn the Aprisa LTE 5G power on.

6. Go to SuperVisor > Cellular > SIM 1 & 2 to view the SIM status.

7. Go to SuperVisor > Cellular > General to enable / assign the SIM to a PDN Profile (see 'Cellular > General' on page 115).

Attach the Cellular LTE, GNSS and Wi-Fi Antennas

Attach either separate antennas for LTE/GNSS and for Wi-Fi or a single combo antenna to the appropriate QMA connectors. See 'Antennas' on page 66 for antennas available from Aviat Networks.

NOTE: Ensure that the Aprisa LTE 5G router antennas are not near metal or other RF reflective surfaces.

Connect the Aprisa LTE 5G to the Power Source

Wire a power cable to your 9-32 VDC power source and connect the power connector (included) to the Aprisa LTE 5G. See 'Power Supply' on page 77 for the Aprisa LTE 5G power connector wiring diagram and pin functionality. Once power source is connected, the OK LED on the front panel will light solid green indicating correct operation.

For a VDC power source not within the specification of the Aprisa LTE 5G VDC input range, or the power source is AC, use an appropriate DC/DC or AC/DC converter power supply.

Installing an SFP Module

The Aprisa LTE 5G can accommodate one standard SFP module. See 'SFP Modules' on page 64 for SFP Module available from Aviat Networks.

To install an SFP in the Aprisa LTE 5G router:

1. Fit the SFP module in the Aprisa LTE 5G SFP socket (connector facing up).

   The Aprisa LTE 5G front panel SFP LED will light solid with the SFP installed and configured. If the SFP interface is not assigned in SFP settings, then the SFP LED will remain off.

   The Aprisa LTE 5G front panel SFP LED will flash green if TX or RX traffic is detected.

2. Go to SuperVisor > Interfaces/Networking > SFP for SFP settings.

Hardware Restoring of Factory Defaults

If you have lost or forgotten your username and/or password the following procedure will restore the Aprisa LTE 5G to factory defaults which will restore the username /password to defaults.

If you have lost or forgotten the IP address previously set on your LTE, use the procedure described in 'Login to SuperVisor' on page 95.

The Aprisa LTE 5G factory defaults can be restored via a 2 pin header on the board assembly.

To restore the Aprisa LTE 5G factory default configuration:

1. Power off the Aprisa LTE 5G

2. Open the Aprisa LTE 5G enclosure by unscrewing the securing screws (posi 2) (see enclosure picture on page 309)

3. Short the two pins of the RESET header as shown below

4. Power on the Aprisa LTE 5G and wait until the start-up is complete (OK LED turns green)

5. Power down the Aprisa LTE 5G

6. Remove the RESET header short

7. Close the Aprisa LTE 5G enclosure and tighten the screws

Note: Is it critical that the screws are re-tightened to 0.8 Nm. The regulatory compliance of the Aprisa LTE 5G router may be affected if the screws are not tightened correctly.

Basic Software Setup

For a basic setup, open the Aprisa LTE 5G SuperVisor web-based manager to make configuration changes to your router. See 'Connecting to SuperVisor' on page 94.

First Time Setup

When you log in for the first time to Aprisa LTE 5G router, configure any of the following:

- Time Zone – navigate to 'Services > Date & Time' and set the date, time, zone, and format.
- Admin Password – navigate to 'Security > Users > Accounts' and change the default password.
- Security Level - navigate to 'Security > Setup' and set the security level of the router. Strong security level will encrypt all files loaded from the Aprisa LTE 5G, such as configuration file, etc. User shall change the default security Encryption Key if Level 3 security level is selected.
- SIM pin – if required to enable the SIM(s), navigate to 'Cellular > SIM 1 & 2' and enter the SIM(s) pin code. Note: not all cellular operators use a pin to enable the SIM card.
- Access Point Name (APN) - navigate to 'Cellular > General' and set the active / backup APNs per your installed SIM(s).
- Wi-Fi Network Name and password – if router was ordered with Wi-Fi, navigate to 'Interfaces/Networking > WiFi', click the 'Edit' button and set under 'Interface Configuration' the ESSID WiFi network name and the password. If you are currently using the router's Wi-Fi network, you will need to reconnect your devices to the network using the newly established wireless network name (SSID) and password.
- Aprisa LTE 5G Link Check - navigate to 'Cellular > General > LINK HEALTH CHECK SETTINGS' and set the:
  - 'Health Check Test Type = Timed Ping or Ping Counts' – for short and temporary health test.
  - 'Ping Destination IP Address = valid IP address' - an IP address that can be reached through your PDN/WAN connection since some carriers block certain IP addresses.
  - Set the other parameters such as 'Inter-Ping Interval', 'Link Failure Ping Threshold', and 'test ping count / duration' to test the connection and verify the WAN/PDN device is connected. Click the 'Save' button and then click 'Start' to run the test. If the connection fails, the OK LED will light RED until the test finishes, or light green for a successful test.

Software Upgrade

This upgrade process is for upgrading the software on a single Aprisa LTE 5G.

SuperVisor Software Upgrade Method

The Aprisa LTE 5G software can be upgraded by loading the software file *.4nu from an external directory using the file transfer process (see 'Software > File Transfer' on page 268) and activated (see 'Software > Manager' on page 270).

To load and activate Aprisa LTE 5G software:

1. Download the software file *.4nu into your computer.

2. Login to SuperVisor and go to Software > File Transfer. The method is set to HTTPS.

3. Click Start Transfer.

4. Browse to the *.4nu software file stored on your computer.

FILE TRANSFER STATUS	
Transfer Activity	In Progress
Method	HTTP
File	Software Pack
Transfer Result	In Progress (46%)

The software release file will be transferred to the Aprisa LTE 5G Available Software Pack location and the file integrity verified.

If the file transfer fails, check the Events History Log page (see 'Events > History Log' on page 252) for more details of the transfer.

5. Activate the software on the Aprisa LTE 5G (see 'Software > Manager' on page 270). The router will reboot automatically.

USB Software Upgrade Method

The Aprisa LTE 5G software can be upgraded simply by plugging a USB flash drive containing the new software into the USB C host port ⟋ on the Aprisa LTE 5G front panel. A USB A to USB C convertor will be required for USB A flash drives.

To upgrade the Aprisa LTE 5G router software:

1. Copy the software file *.4nu into the root directory of a USB flash drive.

2. The SuperVisor USB Boot Upgrade setting allows for the new software to just be loaded into the LTE without affecting router operation or the new software to be loaded into the Aprisa LTE 5G with an automatic activate and reboot.

Option	Function
Load and Activate	New software will be uploaded from a USB flash drive in to the Aprisa LTE 5G and activated / rebooted automatically.
Load Only	New software will be uploaded from a USB flash drive in to the Aprisa LTE 5G. The software will need to be manually activated later (see 'Software > Manager' on page 270).

3. Insert the USB flash drive into the Aprisa LTE 5G host port ⟋. The AUX LED will light green indicating the presence of a USB flash drive. It does not indicate the presence of a software release file on the USB flash drive.

   If the software file *.4nu on the USB flash drive is not the same software version as the software version currently running the Aprisa LTE 5G, the software release file will be transferred to the Aprisa LTE 5G Available Software Pack location and the file integrity verified. The version of the uploaded software will be displayed in the Available Software Pack 'Version' field (see 'Software > Manager' on page 270).

4. Remove the USB flash drive from the Aprisa LTE 5G host port ⟋.

CLI Software Upgrade Method

The Aprisa LTE 5G software can be upgraded from the Command Line Interface.

To load and activate Aprisa LTE 5G software from a remote FTP server:

1. Open the CLI interface (see 'Command Line Interface' on page 291).
2. Type:

   copy ftp://username:password@server-ip-or-name/file-path-and-name flash:active-firmware

To load (and activate later) Aprisa LTE 5G software from a remote FTP server:

1. Open the CLI interface (see 'Command Line Interface' on page 291).
2. Type:

   copy ftp://username:password@server-ip-or-name/file-path-and-name flash:available-firmware

To activate already loaded Aprisa LTE 5G software:

1. Open the CLI interface (see 'Command Line Interface' on page 291).
2. Type:

   copy flash:available-firmware flash:active-firmware

Software Downgrade

Aprisa LTE 5G software can also be downgraded if required. The downgrade process is the same as the upgrade process.

Bench Setup

Before installing in the field, it is recommended that you bench-test the Aprisa LTE 5G. A suggested setup for basic bench testing is shown below:

DC power supply

PC running *SuperVisor*

Mobile Antenna
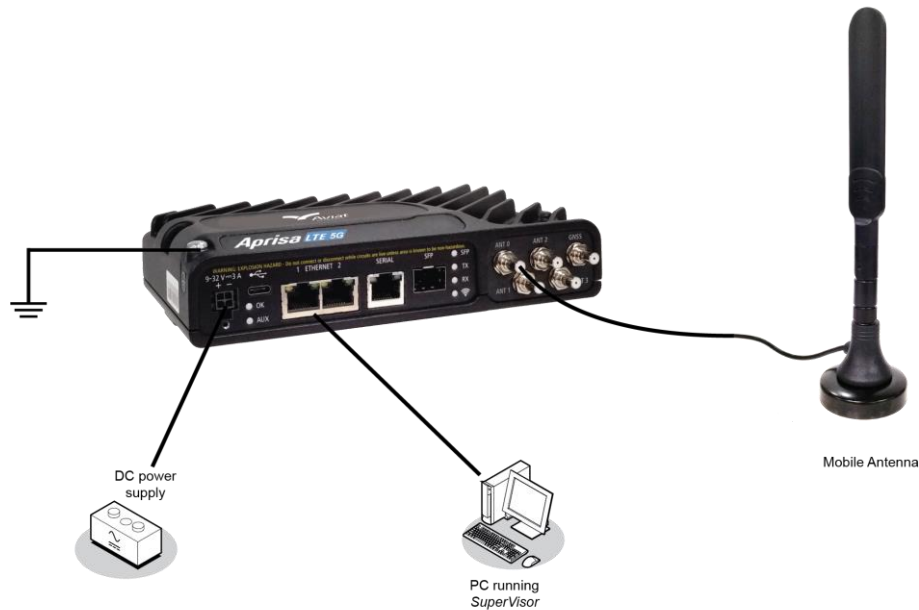
Set up the bench equipment as follows:

- Connect the Aprisa LTE 5G earth point to a protection earth
- Install an activated SIM in the Aprisa LTE 5G see 'Installing a SIM' on page 69
- Connect the DC power source to the Aprisa LTE 5G power input
- A wireless broadband data plan must be added to your Aprisa LTE 5G, which are available from cellular operators such as Verizon, and AT&T and come with SIM card(s). Once you have an activated SIM, insert it into the Aprisa LTE 5G SIM 1 Slot
- Connect either separate antennas for LTE/GNSS and for Wi-Fi or a single combo antenna to the appropriate QMA connectors on the Aprisa LTE 5G
- Turn the power source on
- Connect your PC to one of the Ethernet ports and login to SuperVisor with username: admin and password as shown on the Serial Number label on the left side of the enclosure.

S/N: R6510012014

User: admin
P/W: xxxxxxxxxx

Serial Number Label

If there is no password shown on the Serial Number label, your password will be 'admin'.

- Setup the correct SIM slot and APN name to use in SuperVisor > Cellular settings

Test the setup by verifying internet connectivity:

- Check the SuperVisor > Monitoring page that the Aprisa LTE 5G is connected
- Check the Aprisa LTE 5G internet connectivity by trying a ping using the SuperVisor heath test on 'Cellular > Carrier/Redundancy' on page 119.
- On PC that is connected to either Wi-Fi or wired Ethernet port, ping a well know internet addresses for example:
  - IPv4 connectivity, try ping to 8.8.8.8 (google DNS server)
  - IPv6 connectivity, try ping to 2001:4860:4860::8888 (google DNS server)
  - DNS connectivity, try to ping Aviat Networks.com
  - Try browsing the internet from the configuration PC

Power Supply

The input voltage for the Aprisa LTE 5G is +9 to +32 VDC. The maximum power input is 15 W.

The power connector required is a Molex Micro-Fit 3.0 4 pin female connector. The power supply input connects to pin 1 +ve and pin 2 -ve.

The Molex Micro-Fit 3.0 4 pin connector clips into the Aprisa LTE 5G socket. It also has a power retention clip and screw (supplied with the Aprisa LTE 5G) that enables the connector to be secured to the Aprisa LTE 5G with a screw. Do not use the product if the power retention clip is missing or loose.
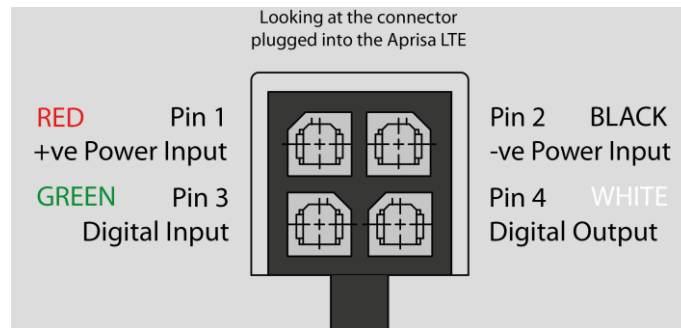
The negative supply of the Aprisa LTE 5G power connection is internally connected to the Aprisa LTE 5G enclosure. Power must be supplied from a negative earthed power supply.

A 1 metre power cable fitted with 4 pin Molex Micro-Fit 3.0 female connector and wire ended is supplied in the box with each Aprisa LTE 5G.

Additional power cables of the same type can be ordered from Aviat Networks as accessories:

Part Number	Part Description
APLB-PPWR-X01	4RF LTE Acc, Cable, Power, 1m
APLB-PPWR-X10	4RF LTE Acc, Cable, Power, 10m

Wire your power source to the power cable and plug the connector into the Aprisa LTE 5G.

Spare Molex Micro-Fit 3.0 connectors can be ordered from Aviat Networks:

Part Number	Part Description
APLS-CML4-FEM-01	4RF LTE Spare, Connector, Molex 4 Pin Micro-Fit 3.0, Female, 1 item

Turn your power source on:

- The OK and AUX LEDs will light orange while the Aprisa LTE 5G is booting up. The SFP, TX, RX and Wi-Fi LEDs will be off.
- When the Aprisa LTE 5G is ready to operate, the OK LED will light green.

If the LEDs fail to light, check the power supply polarity and voltage.

If a voltage greater than the specified voltage range of 9 to 32 VDC is applied to the Aprisa LTE 5G power supply input, or the polarity is reversed, the internal fuses may have blown to protect the unit. See 'Spare Fuses' on page 309 for instructions on how to replace the fuses.

Cooling

If the Aprisa LTE 5G is operated in an environment where the ambient temperature exceeds 50°C, the convection air flow over the heat sink must be considered.

The environmental operating conditions are as follows:

Operating temperature	-30 to +70˚ C (-22 to +158˚ F)
Storage temperature	-40 to +85˚ C (-40 to +185˚ F)
Humidity	Maximum 95% non-condensing

WARNING:

If the Aprisa LTE 5G is operated in an environment where the ambient temperature exceeds 50°C, the Aprisa LTE 5G must be installed within a restricted access location to prevent human contact with the enclosure heat sink.

ATTENTION:

Si l'Aprisa LTE 5G fonctionne dans un environnement où la température ambiante dépasse 50 ° C, l'Aprisa LTE 5G doit être installé dans un endroit à accès restreint de manière à éviter tout contact humain avec le dissipateur de chaleur du boîtier.

WARNING:

The Aprisa LTE 5G can be operated in an environment where the ambient temperature exceeds 50°C. The heat sink will be a hot surface - do not touch.

ATTENTION:

L'Aprisa LTE 5G peut fonctionner dans un environnement où la température ambiante dépasse 50 ° C. Le dissipateur de chaleur sera une surface chaude - ne le touchez pas.

Earthing

Earth Connection Point

The Aprisa LTE 5G has an earth connection point on the top left of the enclosure. A M4 8mm pan pozi machine screw and M4 lock washer is supplied fitted to the router. This screw is used to earth the enclosure to a protection earth. A minimum of 0.8 mm^2 (18 AWG) wire shall be used and it shall not contain switches or protective devices.

Mounting Options

The Aprisa LTE 5G has four threaded holes (M4) in the enclosure base and two holes (5.2 mm) through the enclosure for mounting.
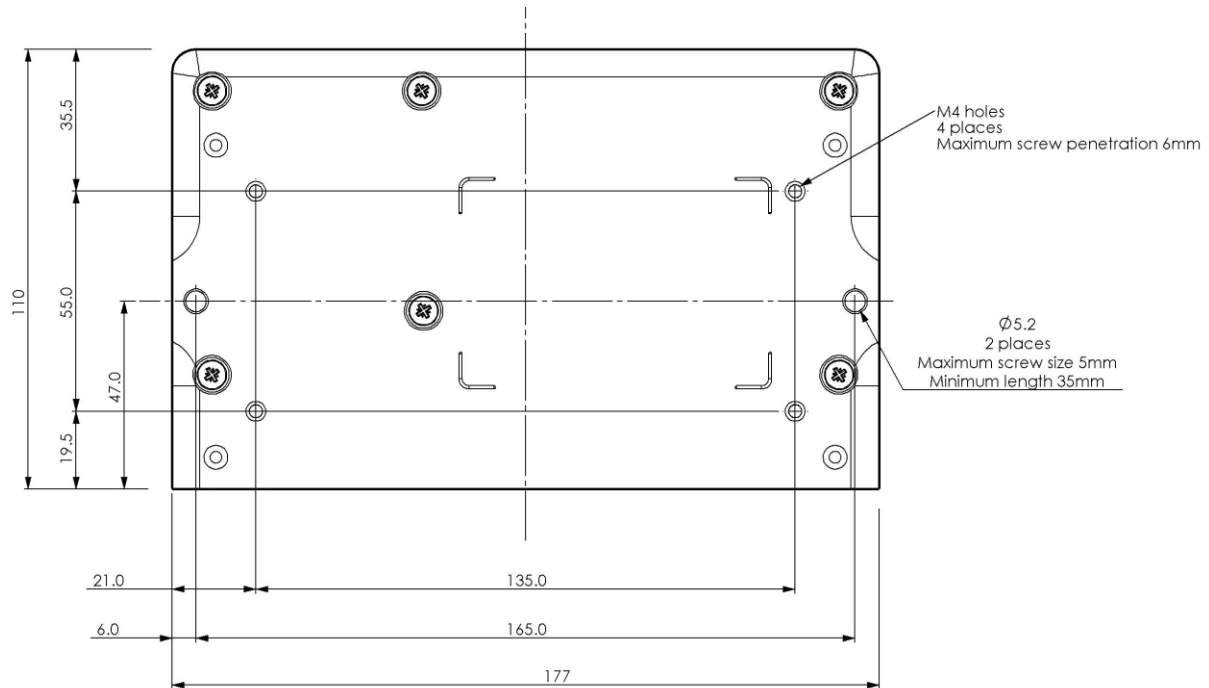
Mounting options include:

- DIN rail mounting with the DIN Rail Mounting Bracket
- Rack shelf mounting
- Wall mounting
- Outdoor enclosure mounting

DIN Rail Mounting

The Aprisa Family has an optional accessory part to enable the mounting on a standard DIN rail:

Part Number   **Part Description**

APGA-MBRK-DIN   4RF Acc, Mounting, Bracket, DIN Rail
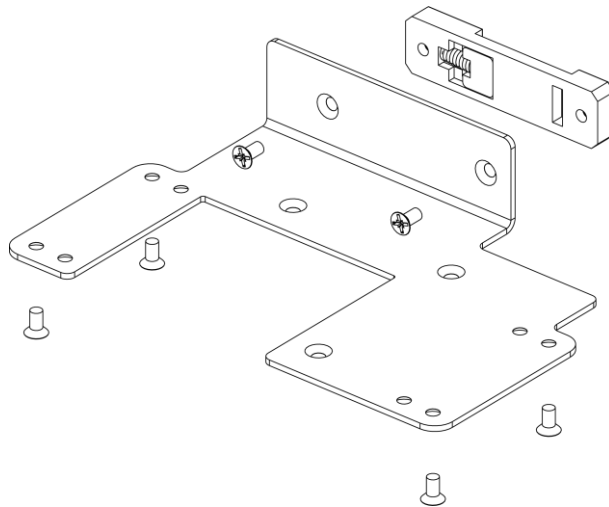
The Aprisa LTE 5G is mounted into the DIN rail mounting bracket using the four M4 threaded holes in the enclosure base. Four 8 mm M4 pan pozi machine screws are supplied with the bracket.
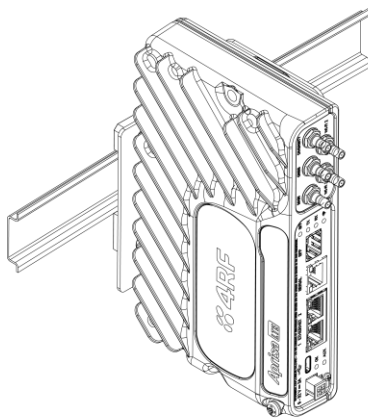
Vertical Mount
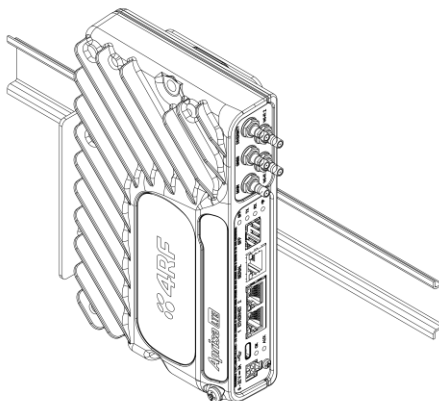
Flat Vertical Mount   Flat Horizontal Mount
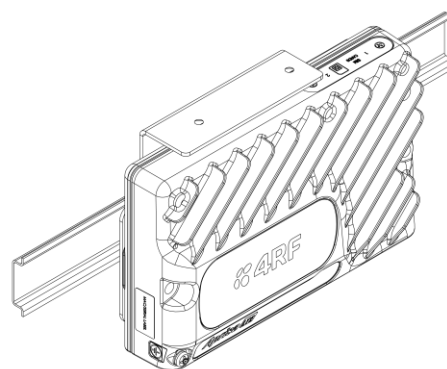
Rack Shelf Mounting

The Aprisa LTE 5G can be mounted on a rack mount shelf using the four M4 threaded holes in the Aprisa LTE 5G enclosure base. The following picture shows Aprisa LTE 5Gs mounted on 1 RU rack mounted shelves.

Part Number	Part Description
APGA-MR19-X1U	4RF Acc, Mounting, 19" Rack Mount Shelf, 1 Rack Unit
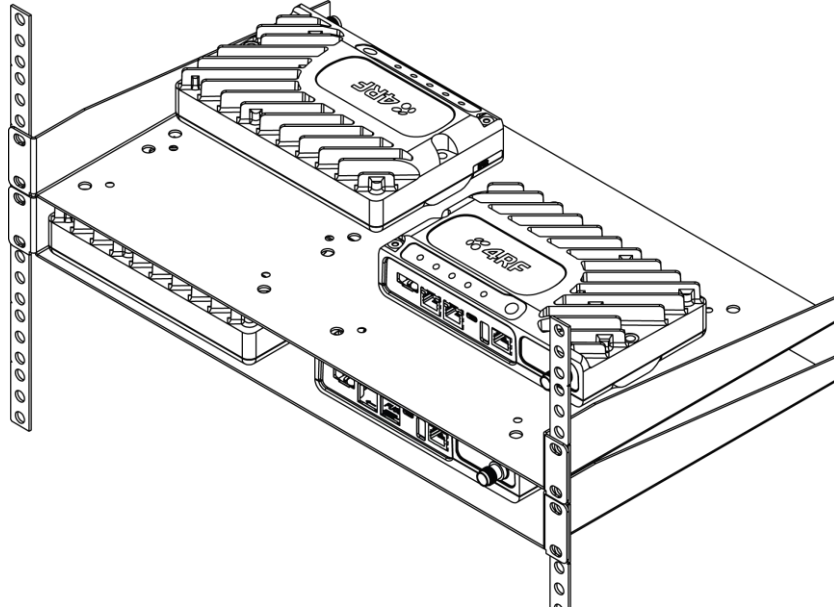
Wall Mounting

The Aprisa LTE 5G can be mounted on a wall using the two holes through the enclosure (5.2 mm diameter). Typically, M5 screws longer than 35 mm would be used.
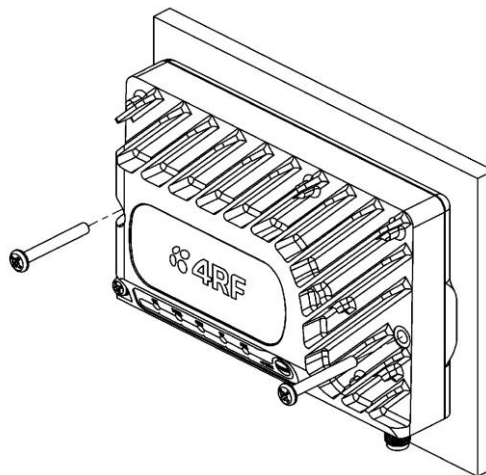
Antenna Selection

The performance specifications described in this section are valid with the antennas externally installed and antenna coaxial cables routed to their final locations.

Installation & Maintenance Training Requirements

The Aprisa LTE 5G may be used in fixed or mobile applications where the power density from the antenna exceeds National limits for uncontrolled exposure (i.e., the general public). Installation and maintenance of the Aprisa LTE 5G and associated accessories must only be performed by trained and qualified personnel who have received appropriate training regarding work practices relating to controlling or mitigating RF exposure.

The Installation and maintenance personnel must have knowledge of the regulatory requirements for maximum EIRP/ERP and RF Exposure limits and requirements within the region of deployment.

Determine Maximum Antenna Gain

To ensure that the maximum regulated EIRP or ERP is not exceeded, the maximum antenna gain must be determined, and the following installation parameters must be known:

1.	Antenna isotropic gain (specified in dBi)	G_{dBi}
2.	Aprisa LTE 5G maximum average power (specified in dBm)	P_{dBm}
3.	Regulatory isotropic power limit (EIRP specified in dBm)	R_{dBm}
4.	Feeder coax loss between Aprisa LTE 5G and Antenna (specified in dB/m)	$L_{dB/m}$
5.	Length of feeder coax between Aprisa LTE 5G and antenna (specified in metres)	d_m

The Aprisa LTE 5G has a maximum average output power of +24 dBm (includes positive tolerance).

Where the Regulatory power limit is expressed in Watts (R_W), this is converted to dBm from the formula:

$$R_{dBm} = 30 + 10 \times Log_{10}(R_W) \tag{1}$$

Where the Regulatory power limit (R_{dBm}) is expressed in terms of ERP, convert it to EIRP by adding 2.15 dB to the value, i.e.:

$$EIRP_{dBm} = ERP_{dBm} + 2.15_{dB} \tag{2}$$

To ensure operation within the regulatory requirements, the maximum Antenna isotropic gain G_{dBi} is calculated from the formula:

$$G_{dBi} = R_{dBm} + \left(d_m \times L_{dB/m}\right) - P_{dBm} \tag{3}$$

An antenna with an isotropic gain less than or equal to the maximum can then be selected for the installation. Antenna gain information can be obtained from the Antenna manufacturer and is either expressed in terms of dBi, referenced to an isotropic radiator, or dBd, referenced to a dipole. If the gain is expressed in dBd, it can be converted to dBi by adding 2.15 dB to the dBd gain value.

The transmitter $EIRP_{dBm}$ can now be calculated from the actual antenna gain and the Aprisa LTE 5G maximum output power, this value is used to derive the compliance distances:

$$EIRP_{dBm} = P_{dBm} - \left(d_m \times L_{dB/m}\right) + actual\ G_{dBi} \tag{4}$$

Determine Compliance Distance

The current limiting RF power density for uncontrolled (general public) and controlled (occupational) exposure must be obtained from the Regulatory Authority; for example, in Canada this information is contained in the latest version of ISED document RSS-102.

The limiting power density is usually expressed in W/m^2 or mW/cm^2, it is very important to use the correct units when performing the calculations; for this exercise W/m^2 will be used.

The $EIRP_{dBm}$ must be converted to linear power units (W):

$$EIRP_W = 0.001 \times 10^{(0.1 \times EIRP_{dBm})} \tag{5}$$

The limiting power density (S) is used to define the minimum compliance boundary from:

$$r = \sqrt{\frac{EIRP_W}{4\pi S}} \tag{6}$$

Where S is the limiting power density as defined in the applied standard in W/m^2, and r represents the compliance distance from the antenna in metres.

The Installation and maintenance personnel must ensure that public access is restricted to an area outside the calculated compliance distance from the antenna.

Design Example

The following example should be used to verify the calculations performed.

Parameter	Notes	Value	Unit
LTE Band 2	Lower[2] Uplink frequency	2500	MHz
EIRP limit	RSS-199 section 4.4 for a fixed station	40.0	W EIRP
Power Density limit	RSS-102 Uncontrolled Environment: $0.02619 f^{06834}$ where f is the frequency in MHz	5.50	W/m^2
Aprisa LTE 5G TX power	Nominal power+1 dB tolerance	+24.00	dBm
$L_{dB/m}$	Feeder Loss RG214	0.40	dB/m
d_m	Feeder Length	4.00	m
R_{dBm}	EIRP limit from equation (1) in dBm	46.02	dBm
G_{dBi}	Maximum Antenna gain equation (3)	23.62	dBi
Actual G_{dBi}	Panel antenna with gain 12 dBd +2.15 dB	14.15	dBi
Actual $EIRP_{dBm}$	Equation (4)	36.55	dBm
Actual $EIRP_W$	Equation (5)	4.52	W
r	Compliance distance: Equation (6)	0.26	m

---

[2] The lower frequency of the band should be used as it may give in a higher power density.

Antenna Requirements

External multi-band 2x2 MIMO antenna systems (Main/Diversity).

Table 5 Antenna 1 and Antenna 2 requirements

Requirement	Main Antenna	Diversity Antenna
Operating Bands	All supporting Tx and Rx frequency bands.	All supporting Rx frequency bands.
VSWR	< 2:1 (recommended) < 3:1 (worst case) On all bands including band edges	
Total radiated efficiency	> 50% on all bands Measured at RF connector. Includes mismatch and antenna loss but excludes coaxial loss.	
Radiation pattern	Nominally omni-directional radiation pattern in azimuth plane	
Envelope correlation coefficient between Main and Diversity	< 0.5 on Rx bands below 960 MHz < 0.2 on Rx bands above 1.4 GHz	
Mean Effective Gain of Main and Diversity (MEG1, MEG2)	≥ -3 dBi	
Main and Diversity Mean Effective Gain Imbalance |MEG1 / MEG2|	< 2 dB for MIMO operation < 6 dB for diversity operation	
Maximum antenna gain	Must not exceed antenna gains due to RF exposure and ERP/EIRP limits, as listed in the module's FCC grant. See Table 4 Antenna Compliance Requirements.	
Isolation between Main and Diversity (S21)	> 10 dB	
Power handling	> 1 W (30 dBm)	

GNSS Antenna Requirements

Table 6 GNSS Antenna Requirements

Requirement	GNSS Antenna
Frequency Range	Wide-band GNSS: 1559–1606 MHz recommended Narrow-band GPS: 1575.42 MHz ±2 MHz minimum Narrow-band Galileo: 1575.42 MHz ±2 MHz minimum Narrow-band BeiDou: 1561.098 MHz ±2 MHz minimum Narrow-band GLONASS: 1601.72 MHz ±4.2 MHz minimum Narrow-band QZSS: 1575.42 MHz ±2 MHz minimum
Field of view (FOV)	Omni-directional in azimuth -45° to +90° in elevation
Polarization (average Gv/Gh)	> 0 dB (Vertical linear polarization is sufficient) Gv and Gh are measured and averaged over -45° to +90° in elevation, and ±180° in azimuth.
Free space average gain (Gv+Gh) over FOV	> -6 dBi (preferably > -3 dBi)
Gain	Maximum gain and uniform coverage in the high elevation angle and zenith. Gain in azimuth plane is not desired.
Average 3D gain	> 5 dBi
Isolation between GNSS and Ant1	> 10 dB in all uplink bands
Typical VSWR	< 2.5:1
Polarization	Any other than LHCP (left-hand circular polarized) is acceptable
Active GNSS Antenna	Where an active GNSS antenna is used, a +3.15 V d.c. supply at up to 100 mA is available at the GNSS antenna port. This feature is enabled/disabled through SuperVisor see 'Active Antenna' on page 126.

Wi-Fi Antenna Requirements

- Individual antenna gains must not exceed the values given for WLAN antennas in Table 4 Antenna Compliance Requirements.
- The Wi-Fi antenna must be installed such that at least 20 cm is maintained between the antenna and users.
- The required antenna impedance is 50 Ohms.
- To get maximum throughput when operating at MIMO 2x2, two antennas with at least 25 dB isolation are recommended.

RF Connector Adapters

Part Number	Description
APLB-AQMM-SMF	QMA Male to SMA Female Adapter
APLB-AQMM-SMP	QMA Male to SMA Male Adapter - reverse outer conductor

Interface Connection and Cabling

Ethernet Interface Connections
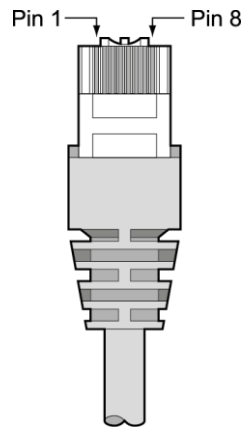
RJ45 pin numbering

Pin Number	Signal Name	Pin Function	Direction	TIA-568A Wire Colour	TIA-568B Wire Colour
1	TX+_D1	Transmit+	Output	Green/white	Orange/white
2	TX-_D1	Transmit-	Output	Green	Orange
3	RX+_D2	Receive+	Input	Orange/white	Green/white
4	BI+_D3	Bi-directional+	Bi-directional	Blue	Blue
5	BI-_D3	Bi-directional-	Bi-directional	Blue/white	Blue/white
6	RX-_D2	Receive-	Input	Orange	Green
7	BI+_D4	Bi-directional+	Bi-directional	Brown/white	Brown/white
8	BI-_D4	Bi-directional-	Bi-directional	Brown	Brown

Fibre Optic Connections

SFP modules are available as accessories from Aviat Networks with several different interface types (see 'SFP Modules' on page 64).

Serial RS-232 Interface Connections

The Aprisa LTE 5G RS-232 Serial Interface is always configured as a DCE:

RJ45 Pin Number	Pin Function	Direction	TIA-568A Wire Colour	TIA-568B Wire Colour
1	RTS	Input	Green / white	Orange/white
2	DTR	Input	Green	Orange
3	TXD	Input	Orange / white	Green/white
4	Ground		Blue	Blue
5	DCD	Output	Blue / white	Blue/white
6	RXD	Output	Orange	Green
7	DSR	Output	Brown / white	Brown/white
8	CTS	Output	Brown	Brown

Note: The TIA-568B wiring is the most commonly used and matches the cables we supply.

RS-232 Customer Cable Wiring

Aprisa LTE 5G RS-232 Interface - DCE			DTE Customer Interface		DCE Customer Interface	
RJ45 Pin Number	Pin Function	Direction	Pin Function	DB9 Male Pinout	Pin Function	DB9 Female Pinout
1	RTS	Input	RTS	7	CTS	8
2	DTR	Input	DTR	4	DSR	6
3	TXD	Input	TXD	3	RXD	2
4	Ground		Ground	5	Ground	5
5	DCD	Output	DCD	1		
6	RXD	Output	RXD	2	TXD	3
7	DSR	Output	DSR	6	DTR	4
8	CTS	Output	CTS	8	RTS	7

Serial RS-422 / RS-485 Interface Connections

RS-422 Serial Interface pinout

RJ45 Pin Number	Pin Function
1	TX-
2	
3	TX+
4	Ground
5	
6	RX+
7	
8	RX-

RS-485 Serial Interface pinout

RJ45 Pin Number	Pin Function	
	Full Duplex	Half Duplex
1	TX-	TX/RX-
2		
3	TX+	TX/RX+
4	Ground	Ground
5		
6	RX+	
7		
8	RX-	

USB

The Aprisa LTE 5G USB connector is a standard USB type C connector.

GPIO

The Aprisa LTE 5G has two I/O pins for connection to an Aprisa SRi/SR+ radio or as digital general-purpose input and output interface for any use e.g. door open/close or operating a camera remotely. See 'General Purpose I/O (GPIO) Pin Interface' on page 319 for the interface specification.

GPIO Digital Input

Pin3 of the Molex Micro-Fit connector used for the following functions:

- Programmable ignition turn on and turn off delays
- Programmable sleep modes
- Input sensing for protection systems

GPIO Digital Output

Pin 4 of the Molex Micro-Fit
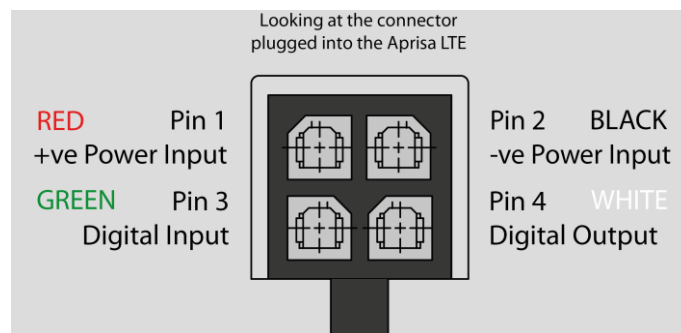
Spares

The following spare parts are available from Aviat Networks:

Spare Fuses

Part Number	Part Description
APGS-FNAN-453-05-02	4RF Spare, Fuse, Nano SMF, 453 Series, 5A, 2 Items
APGS-FNAN-453-05-10	4RF Spare, Fuse, Nano SMF, 453 Series, 5A, 10 Items
APGS-FNAN-453-05-50	4RF Spare, Fuse, Nano SMF, 453 Series, 5A, 50 items

Power Connectors

Part Number	Part Description
APLS-CML4-FEM-01	4RF LTE Spare, Connector, Molex 4 Pin Micro-Fit 3.0, Female, 1 item

3. Managing the Aprisa LTE 5G

SuperVisor

The Aprisa LTE 5G contains an embedded web server application (SuperVisor) to enable element management with any major web browser. The currently supported Browsers are:

- Mozilla Firefox
- Microsoft Edge
- Google Chrome

SuperVisor enables operators to configure and manage the Aprisa LTE 5G.

The key features of SuperVisor are:

- Full element management, configuration and diagnostics
- Performance and alarm monitoring, alarm states, time-stamped events, etc.
- View and set standard configuration parameters including Cellular settings see 'Cellular > General' on page 115
- Set and view security parameters
- User management
- Operates over a secure HTTPS session

SuperVisor Management Overview

Connecting to SuperVisor

The recommended management connection to the Aprisa LTE 5G router is with an Ethernet interface using standard IP networking.

The Aprisa LTE 5G has a factory default IP address of 192.168.4.1 with a subnet mask of 255.255.255.0.

To change the Aprisa LTE 5G IP address:

1. Set up your PC for a compatible IP address e.g. 192.168.4.100 with a subnet mask of 255.255.255.0.

2. Connect your PC network port to one of the Aprisa LTE 5G Ethernet ports.

3. Open a browser and enter 192.168.4.1.

4. Login to the Aprisa LTE 5G router with the default username 'admin' and password as shown on the Serial Number label on the left side of the enclosure. If there is no password shown on the Serial Number label, your password will be 'admin'.

5. Go to 'Interfaces/Networking > Logical Interfaces' on page 143, the LAN tab to change the IP address to conform to the network plan in use.

Login to SuperVisor

If SuperVisor is inactive for a period defined by the SuperVisor Inactivity Timeout option (see 'Services > SuperVisor' on page 195), the Aprisa LTE 5G router will automatically logout the user.

To login to SuperVisor:

1. Open your web browser and enter the IP address of the Aprisa LTE 5G router.

If you haven't assigned an IP address to the Aprisa LTE 5G router, use the factory default IP address of 192.168.4.1 with a subnet mask of 255.255.255.0.

If you have previously assigned an IP address to the Aprisa LTE 5G router but don't know what it is, you can either:

1   If your LTE device is hardware type B (or greater) (see 'Hardware Types' on page 63), the USB host port can also be used as a virtual serial device mode for CLI access. You can retrieve the IP address by opening the CLI via the USB-C port as access to the CLI via the USB option doesn't require an IP address, only username and password are required. A USB cable USB-C on one end and a USB to suit your PC on the other end will be required.

Login to the CLI (see 'Connecting to the CLI via the USB host port' on page 292) and type 'show ip' at the command prompt:

AprisaLTE> show ip

2   If your LTE device is hardware type A, you will need to open the enclosure and restore the factory defaults (see 'Hardware Restoring of Factory Defaults' on page 70).
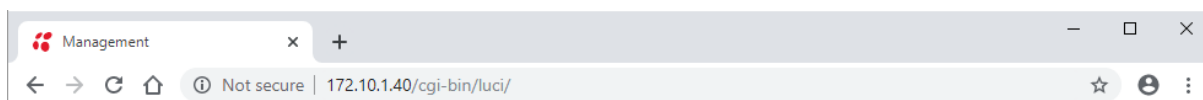
The Aprisa LTE 5G has a randomly generated unique self-signed ECC256 security certificate which may cause the browser to prompt a certificate warning. The valid certificate is 'Issued By: Aviat Networks' which can be viewed in the browser.

When connecting to a remote device for first time, you should manually load the certificate before connecting. Once you have added the exception to your browser, if a warning is shown again, it may indicate a 'man in the middle attack'.
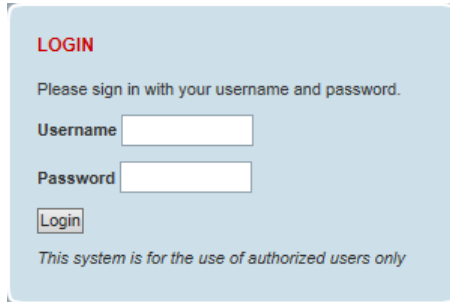
2. Login with the Username and Password.

If the Aprisa LTE 5G was purchased from Aviat Networks with Enhanced Security Features or has been supplied with a password shown on the Serial Number label on the left side of the enclosure, this is your Aprisa LTE 5G password.

Serial Number Label

If there is no password shown on the Serial Number label, your password will be 'admin'.
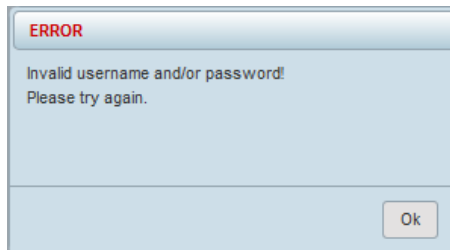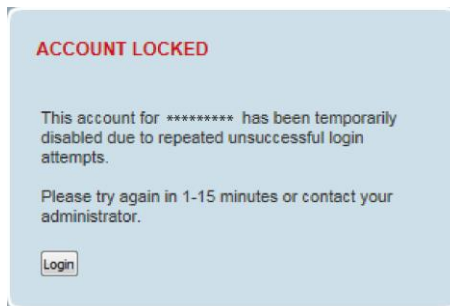
If the login fails, the pop-up will be displayed.

SuperVisor has login protection options which provide protection against unsuccessful login retries (see Security > Users 'Login Protection Mode' on page 210). If login protection is active and a login attempt failed due to temporary lockout of the account (Level 1 or Level 2 lockout), SuperVisor will display an 'Account Locked' message.
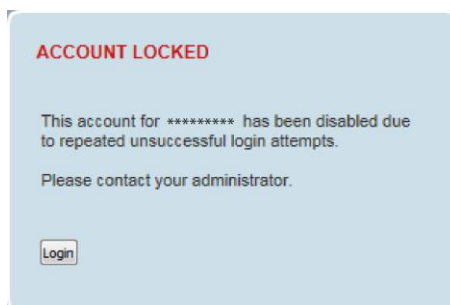
Login

If a login attempt failed due to permanent lockout of the account (continued failed login attempts even after levels 1 and 2 lockout periods), SuperVisor will display an 'Account Locked' message.

Two Factor Authentication
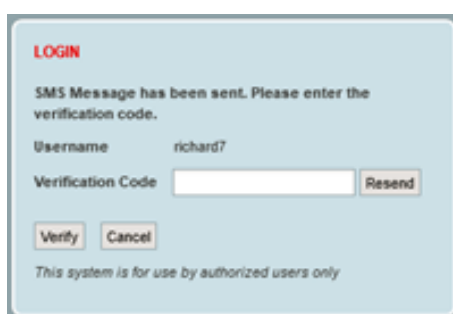
If a Two Factor Authentication SMS Number has been entered (see 'Security > Users > Accounts' on page 213), Two Factor Authentication login will be active.

If Two Factor Authentication is active, a user will not be able to login if there is no cellular network connectivity (because the SMS verification code will not be able to be sent).

The following is required for Two Factor Authentication:
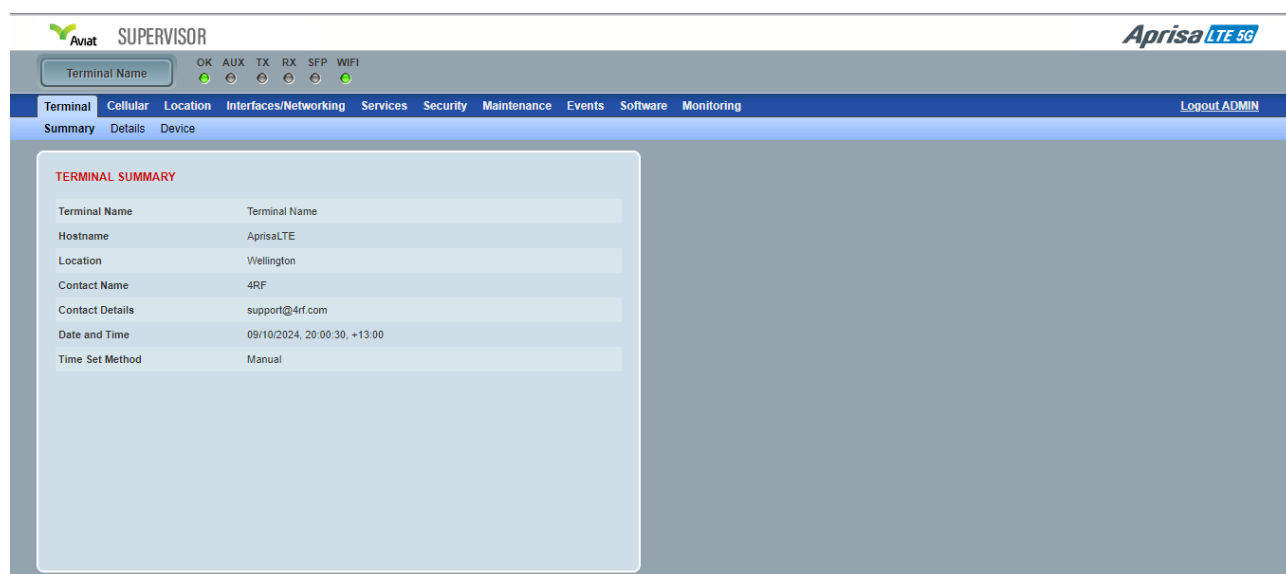
- a pre-programmed SIM card
- be within a cellular network coverage

When the Two Factor Authentication requirements are met, a SMS verification code will be sent to your cell phone, and a popup will request entry of the verification code.

If the login is successful, the opening Terminal > Summary page will be displayed.

Important: After you login for the very first time, it is recommended that you change the default admin password for security reasons (see 'Security > Users > Accounts' on page 213).

Logout of SuperVisor

As the maximum number of concurrent users that can be logged into an Aprisa LTE 5G router is 6, not logging out correctly can restrict access to the Aprisa LTE 5G router until after the timeout period (30 minutes).

If the SuperVisor window is closed without logging out, the Aprisa LTE 5G router will automatically log the user out after a timeout period of 3 minutes.

To logout of SuperVisor:

Click on the 'Logout' button on the Menu Bar.

SuperVisor Page Layout

The following shows the components of the SuperVisor page layout for the Aprisa LTE 5G router:

SuperVisor Branding Bar

The branding bar at the top of the SuperVisor frame shows the branding of SuperVisor on the left and the product branding on the right.

SuperVisor Alarm Bar

The alarm bar shows the name of the Aprisa LTE 5G router that SuperVisor is logged into on the left.

The LED alarm indicators reflect the status of the front panel LEDs on the Aprisa LTE 5G router.

SuperVisor Menu Access

The SuperVisor menu has varying access levels depending on the login User Privileges.

The following is a list of all possible SuperVisor menu items versus user privileges:

Menu Item	View	Technician	Engineer	Admin
Terminal > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Terminal > Details	Read-Only	Read-Only	Read-Only	Read-Only
Terminal > Device	No Access	Read-Write	Read-Write	Read-Write
Cellular > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Cellular > General	No Access	Read-Write	Read-Write	Read-Write
Cellular > Carrier/Redundancy	No Access	Read-Write	Read-Write	Read-Write
Cellular > SIM 1&2	No Access	No Access	Read-Write	Read-Write
Cellular > SMS	No Access	No Access	Read-Write	Read-Write
Location > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Location > General	No Access	Read-Write	Read-Write	Read-Write
Interfaces/Networking > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Interfaces/Networking > Ethernet	No Access	Read-Write	Read-Write	Read-Write
Interfaces/Networking > SFP	No Access	Read-Write	Read-Write	Read-Write
Interfaces/Networking > Serial	No Access	Read-Write	Read-Write	Read-Write
Interfaces/Networking > USB	No Access	Read-Write	Read-Write	Read-Write
Interfaces/Networking > WiFi	No Access	Read-Write	Read-Write	Read-Write
Interfaces/Networking > Logical Interfaces	No Access	No Access	Read-Write	Read-Write
Interfaces/Networking > DHCP and DNS	No Access	No Access	Read-Write	Read-Write
Interfaces/Networking > Firewall	No Access	No Access	Read-Write	Read-Write
Interfaces/Networking > QoS	No Access	No Access	Read-Write	Read-Write
Interfaces/Networking > Routing	No Access	No Access	Read-Write	Read-Write
Services > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Services > SuperVisor	No Access	Read-Write	Read-Write	Read-Write
Services > Configurator	No Access	Read-Write	Read-Write	Read-Write
Services > DDNS	No Access	No Access	Read-Write	Read-Write
Services > Date & Time	No Access	Read-Write	Read-Write	Read-Write
Services > Power Management	No Access	Read-Write	Read-Write	Read-Write
Security > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Security > Setup	No Access	No Access	Read-Write	Read-Write
Security > Users	No Access	No Access	No Access	Read-Write
Security > RADIUS	No Access	No Access	No Access	Read-Write
Security > VPN	No Access	No Access	Read-Write	Read-Write
Security > SSH	No Access	No Access	Read-Write	Read-Write
Security > HTTPS	No Access	No Access	Read-Write	Read-Write
Security > SNMPv2c/v3	No Access	No Access	No Access	Read-Write
Maintenance > General	No Access	Read-Write	Read-Write	Read-Write
Maintenance > Files	No Access	No Access	Read-Write	Read-Write

Menu Item	View	Technician	Engineer	Admin
Maintenance > Cellular	No Access	Read-Write	Read-Write	Read-Write
Maintenance > Networking	No Access	Read-Write	Read-Write	Read-Write
Events > Alarm Summary	Read-Only	Read-Only	Read-Only	Read-Only
Events > History Log	Read-Only	Read-Only	Read-Only	Read-Only
Events > Setup	No Access	No Access	Read-Write	Read-Write
Events > Action Setup	No Access	No Access	Read-Write	Read-Write
Events > Trap Setup	No Access	No Access	Read-Write	Read-Write
Events > Alarm I/O	No Access	No Access	Read-Write	Read-Write
Events > Syslog	No Access	No Access	No Access	Read-Write
Events > Defaults	No Access	No Access	Read-Write	Read-Write
Software > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Software > Setup	No Access	Read-Write	Read-Write	Read-Write
Software > File Transfer	No Access	Read-Write	Read-Write	Read-Write
Software > Manager	No Access	No Access	Read-Write	Read-Write
Monitoring > Terminal	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Cellular	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Ethernet	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Serial	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > WiFi	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Logical Interfaces	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > VPN	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > DHCP	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Firewall	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Routes	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > NAT	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Address Tables	Read-Only	Read-Only	Read-Only	Read-Only

SuperVisor Menu Items

All SuperVisor menu item descriptions assume full access 'admin' user privileges:
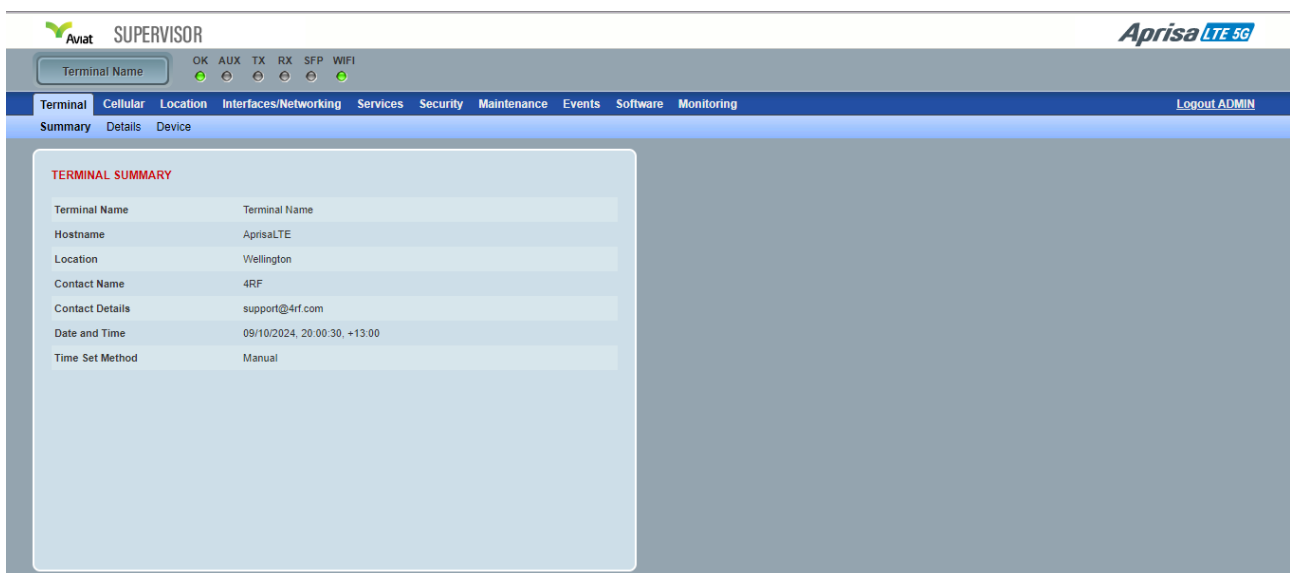
SuperVisor Parameter Settings

Changes to parameters settings have no effect until the 'Save' button is clicked.

Click the 'Save' button to apply the changes or 'Cancel' button to restore the current value.

Terminal

Terminal > Summary

TERMINAL SUMMARY

This page displays the current settings for the Terminal parameters Terminal > Details on page 103 and Terminal > Device on page 105 for setting details.

Terminal > Details

This page displays the current device hardware details.
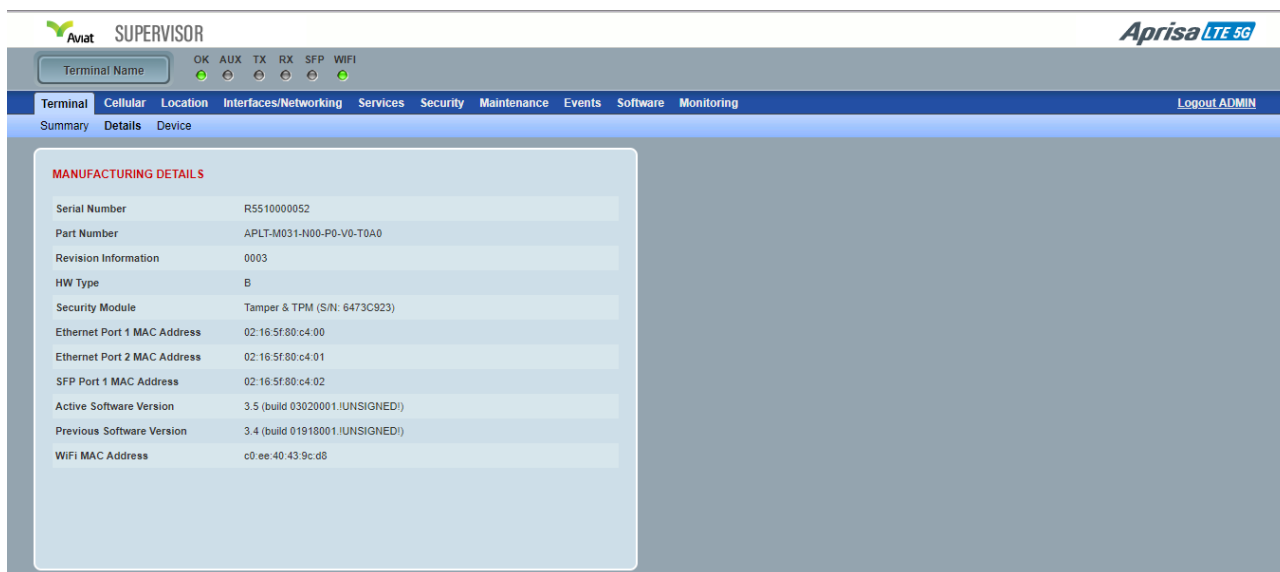
MANUFACTURING DETAILS

Serial Number

This parameter displays the Serial Number of the device (shown on the enclosure label).

Part Number

This parameter displays the Aprisa LTE 5G part number.

Revision Information

This parameter displays the Ethernet Port 1 MAC Address octet string.

Hardware Type

This parameter displays the Hardware Type.

Security Module

This parameter shows if a security module is fitted e.g. tamper Module.

Ethernet Port 1 MAC Address

This parameter displays the Ethernet Port 1 MAC Address octet string.

Ethernet Port 2 MAC Address

This parameter displays the Ethernet Port 2 MAC Address octet string.

SFP Device MAC Address

This parameter displays the SFP port MAC Address.

Active Software Version

This parameter displays the version of the software currently operating the device.

Previous Software Version

This parameter displays the software version that was running on the device prior to the current software being activated.
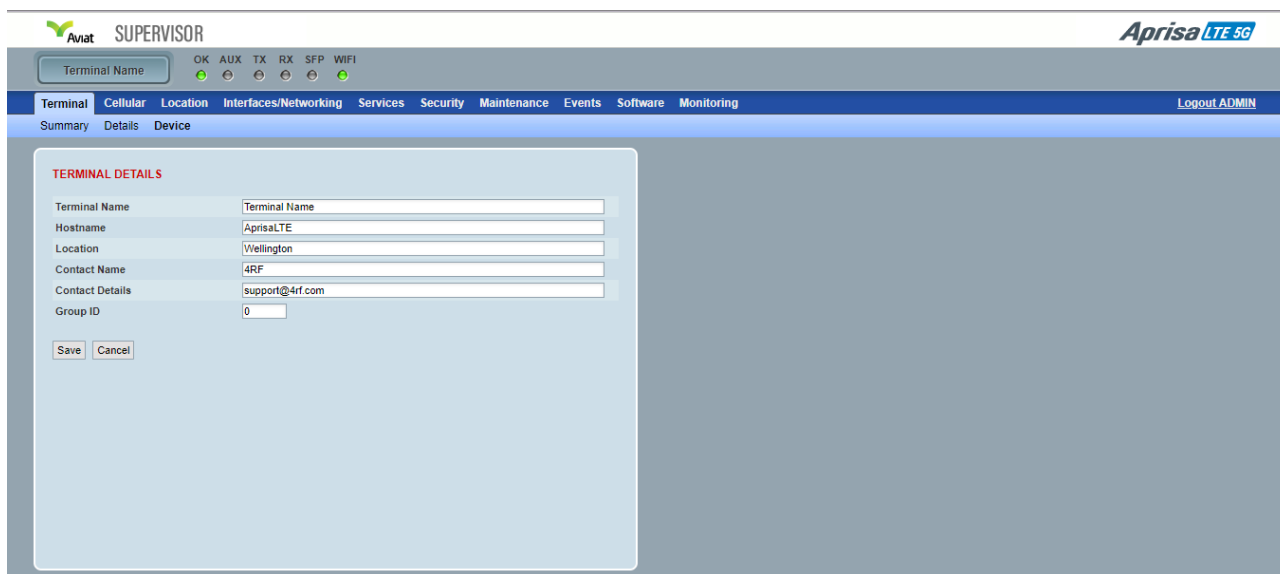
A new device from the factory will display 'None' for the Previous SW Version.

WiFi MAC Address

This parameter displays the WiFi MAC Address octet string if a WiFi network module is fitted to the Aprisa LTE 5G.

Terminal > Device

This page displays the current device terminal name settings.

TERMINAL DETAILS

The data entry in the next four fields can be up to 40 characters but cannot contain invalid characters. A popup warns of the invalid characters:

1. Enter the device Terminal Name.

2. Enter the device Host Name.

3. Enter the device Location of the router.

4. Enter a Contact Name.

5. Enter the Contact Details.

6. Enter the Group Id. This is the Aprisa LTE 5G router virtual group for NMS visual purpose or group operational purpose. The default value is '0'.

Cellular

See 'Network Architecture Overview' on page 30 for a general understanding of 4G LTE.

Single and Dual SIMs/Operators Connection

Connecting the Aprisa LTE 5G to the network requires the following setup options:

1. Install the SIM cards, following the steps outlined in 'Installing a SIM' on page 69. This is a prerequisite setup stage for any settings in this section.

2. Setup the APN for cellular connection and its APN backup connection if required. This is discussed in this section.

3. Setup of VPNs, for secure connection to the customer data center and/or to another Aprisa LTE 5G router over a public / private cellular network. This is discussed under the 'Security > VPN' section.

4. Checking and monitoring the cellular connections. This is discussed in this section.

The cellular menu allows you to configure and monitor a single, dual SIM / operator, backup connection.

Single SIM / Operator Connections and Backup

Figure 17 describes a single SIM / operator APN connection with a backup APN as an option withing the same operator.
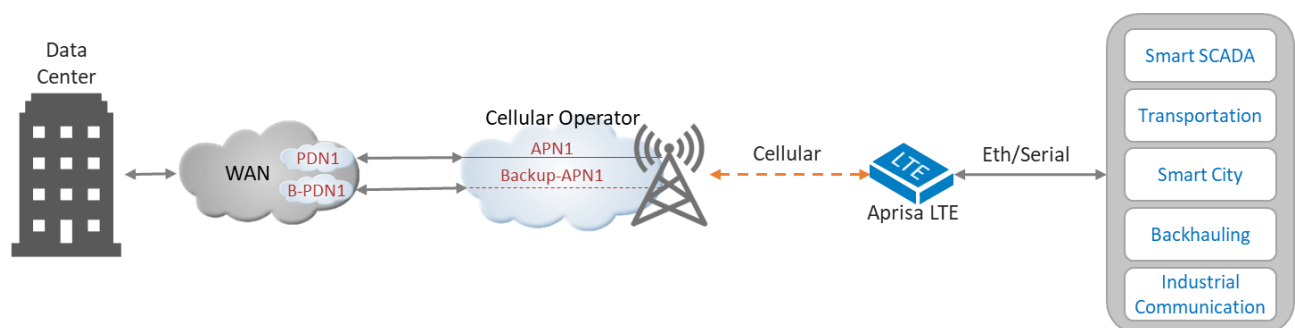
Figure 17 Single SIM / Operator Connections and Backup

To setup the cellular LTE connection, perform the following steps:

1. Navigate to SuperVisor 'Cellular > General' and select the required LTE bands supported by the SIM / operator in use. If you are not sure, use the 'Select All' to select all bands or select only the supported bands to minimize band search and connection time or restoration time.

2. On the same page, set the cellular operator APN name that identifies the PDN Gateway (P-GW) to create the connection to the PDN/WAN network. Setup the required active SIM, IP version and roaming and enable the service connection. Enabling roaming allows the Aprisa LTE 5G being used outside the range of its home network operator and connects to another available cellular network operator (high charges might apply).

3. In case of backup connection within the same cellular operator, setup a second APN name identifier for the backup connection withing the same cellular operator (same SIM). Note: The order of the APN settings is important, since the first APN is the highest priority followed by lower priority APNs and in this example the setting should be APN1, B-APN1, respectively).

4. Navigate to Cellular > Carrier/Redundancy and set the cellular redundancy parameters or keep the default settings. Note: in case of a backup APN connection, set the reverting mode and time as required.

5. On the same page and once the cellular connection is established, check the health of the connection. Set the ping test mode for one-time (time or count) or continuous health check and the rest of the parameters as required. Note: if the link health check fails for the duration of the 'Link Failure Timeout' parameter under the 'Redundancy Settings', the Aprisa LTE 5G will automatically switch to the next lower priority enabled PDN under the 'PDN Profile Settings' (see 'Cellular > General').

Dual SIM / Operator Connections and Backup

Figure 18 describes a dual SIM / operator APN connection with a backup APN as an option per each operator.
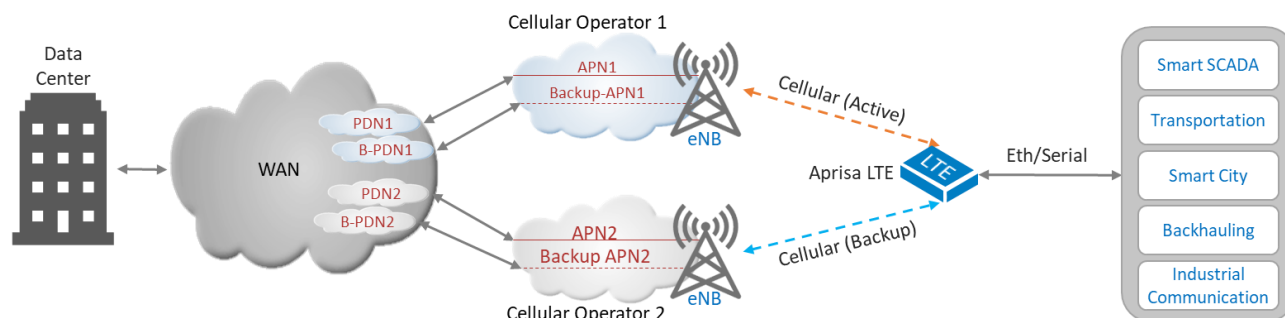
Figure 18 Dual SIM / Operator Connections and Backup
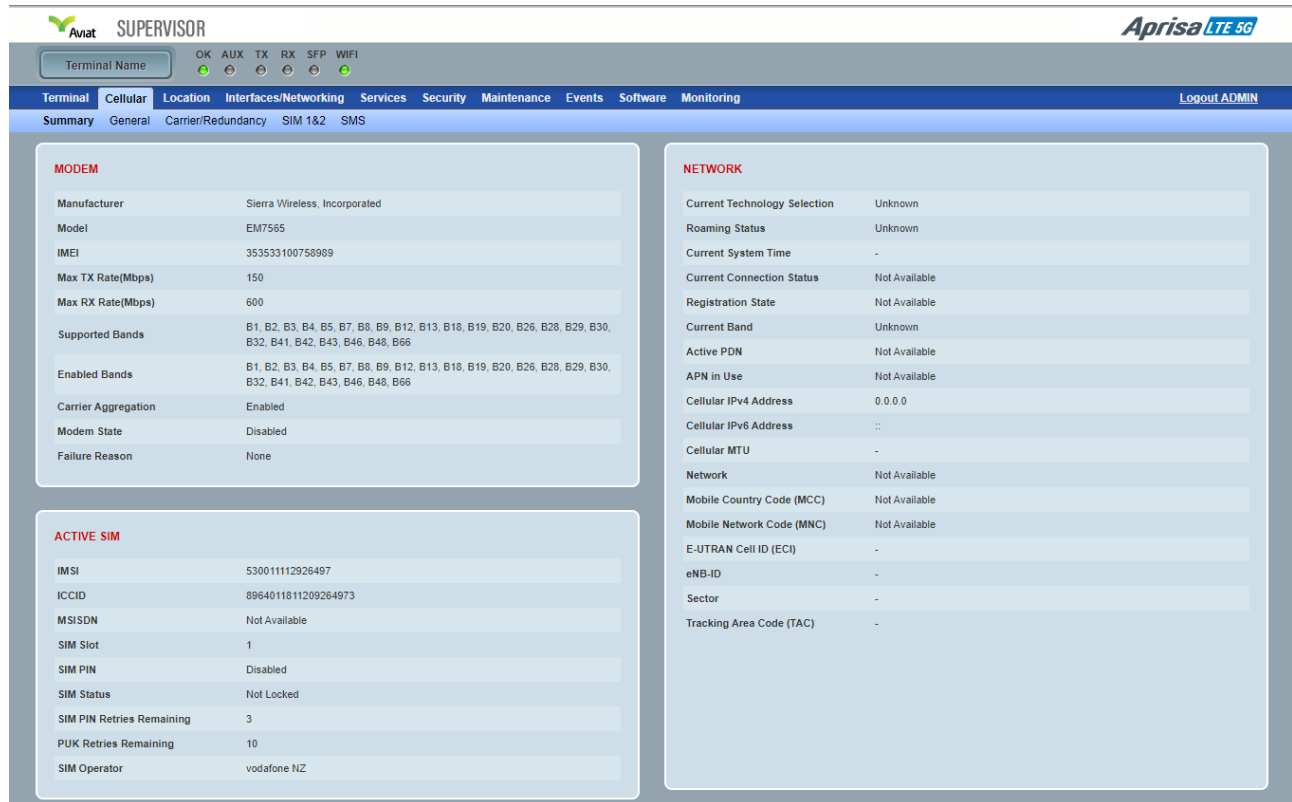
To setup the cellular LTE connection, perform the following steps:

1. Navigate to SuperVisor 'Cellular > General' and select the required LTE bands supported by the SIM / operator in use. If you are not sure, use the 'Select All' to select all bands or select only the supported bands to minimize band search and connection time or restoration time.

2. On the same page set the two different cellular operators APN names that identifies the PDN Gateway (P-GW) to create the connection to the PDN/WAN network. Set up the required active SIM per cellular operator, IP version and roaming and enable the service connection. Enabling roaming allows the Aprisa LTE 5G to be used outside the range of its home network operator and connects to another available cellular network operator (high charges might apply).

3. In case of APN backup connection requirements, setup a second APN name identifier a backup APN connection per each cellular operator (i.e. a total of four (4) APNs, two per each SIM/operator). Note: The order of the APN settings is important, since the first APN is the highest priority followed by lower priority APNs and in this example the setting should be APN1, B-APN1, APN2, B-APN2, respectively).

4. Navigate to Cellular > Carrier/Redundancy and set the cellular redundancy parameters or keep the default settings. Note: in case of a backup APN connection, set the reverting mode and time as required.

5. On the same page and once the cellular connection is established, check the health of the connection. Set the ping test mode for one-time (time or count) or continuous health check and the rest of the parameters as required. Note: if the link health check fails for the duration of the 'Link Failure Timeout' parameter under the 'Redundancy Settings', the Aprisa LTE 5G will automatically switch to the next lower priority enabled PDN under the 'PDN Profile Settings' (see 'Cellular > General').

Cellular > Summary

This page displays current Cellular settings.

4G Modules

MODEM

Manufacturer

Displays the modem manufacturer.

Model

Displays the modem model number.

IMEI

Displays the International Mobile Equipment Identifier (IMEI), a unique 15 or 17 digit code used to identify an individual mobile station to a GSM, UMTS or LTE network. This number is stored in the cellular modem.

Max TX Channel Rate

Displays the maximum transmit channel rate - 50 or 100 Mbit/s depending on the Aprisa LTE 5G module installed (see 'Modules' on page 50).

Max RX Channel Rate

Displays the maximum receive channel rate - 300 or 600 Mbit/s depending on the LTE module installed (see 'Modules' on page 50).

Supported Bands

Displays the list of bands supported by the installed LTE module and the carrier (see 'Modules' on page 50).

Enabled Bands

Displays the list of bands enabled in this LTE (see 'Cellular > General' on page 115).

Carrier Aggregation

When enabled, carrier aggregation is supported.

Modem State

Displays the cellular modem state. The values can be; Failed, Unknown, Initializing, Locked, Disabled, Disabling, Enabling, Enabled, Searching, Registered, Disconnecting, Connecting, Connected.

Fail Reason

Displays the reason for modem failure. If for some reason modem failed connection to network, then the reason is stated here.

ACTIVE SIM

IMSI

The International Mobile Subscriber Identifier (IMSI), a unique 15-digit code used to identify an individual user on a GSM / LTE network. This number is stored in SIM card.

ICCID

This object indicates the Integrated Circuit Card ID (ICCID). The ICCID is defined by the ITU-T recommendation E.118. ICCIDs are stored in the SIM cards and are also engraved or printed on the SIM card body during a process called personalization.

MSIISDN

This parameter indicates the Mobile Subscriber Integrated Services Digital Network Number (MSISDN). It is a number uniquely identifying a subscription in a GSM, UMTS or LTE mobile network. It represents the telephone number to the SIM card in a mobile/cellular phone.

SIM Slot

Indicates whether SIM is present or removed from the socket and its current status. It can take values: 1 or 2.

SIM PIN

Displays if this SIM requires a PIN or not. 'Enabled' indicates a PIN is required for this SIM. 'Disabled' indicates that no PIN is required for this SIM.

SIM Status

Displays the SIM status; Not locked, Locked (PIN), Locked (PUK), Present

Not locked / Present	SIM operating normally
Locked (PIN)	The SIM has been locked out due to the maximum number of SIM PIN retries being exceeded.
Locked (PUK)	The SIM has been locked out due to the maximum number of SIM PUK retries being exceeded.

SIM PIN retries remaining

Displays the number of SIM PIN number retries remaining.

PUK Lock retries remaining

Displays the number of SIM PIN Unlock Key (PUK) retries remaining.

SIM Operator

The network operator that this SIM is provisioned for.

NETWORK

Roaming Status

Displays the current cellular roaming status. Off = on home network, On = Roaming to other network

Current System Time

Displays the current cellular system time received from the base station.

Service Provider

Displays the cellular service provider (Vodafone, Sprint etc.)

Current Connection Status

Displays the current connection status: Connected since Date/Time or Not Connected since Date/Time.

Registration State

Displays the Registration state; Unknown, Registered, Home.

Current Band

Displays the band to which the modem is currently attached.

APN in Use

Displays the current Access Point Name (APN) in use. The APN is an identifier that lives in the LTE core network.

Cellular IPv4 Address

Displays the current Cellular IPv4 Address.

Cellular IPv6 Address

Displays the current Cellular IPv6 Address.

Network

Displays the current network name.

Mobile Country Code (MCC)

Displays the current Mobile Country Code (MCC) 3 digits e.g. 530 for New Zealand.

Mobile Network Code (MNC)

Displays the current Mobile Network Carrier (MNC) 2 or 3 digits. The MNC uniquely identifies a mobile network operator.

E-UTRAN Cell ID (ECI)

E-UTRAN Cell Identifier (ECI) is a decimal number used to identify a cell uniquely within an operator mobile network (or Public Land Mobile Network (PLMN)). The ECI has a length of 28 bits and contains the eNodeB-IDentifier (eNB-ID) and the cell sector (i.e. concatenating number of [eNB-ID | sector]). The ECI can address either 1 or up to 256 cell sectors per eNB, depending on the length of the eNB-ID which can be either 20 bits or 28 bits. A Macro eNB (MeNB) cell site provides coverage served by a high-power tower/antenna cell site, serving multiple UEs and contain the 20 bits option and thus the remaining 8 bits are used to represent the cell sectors (up to 256). A Home eNodeB (HeNB) is 3GPP term for an LTE femtocell or small cell, provides low coverage/power, serving very small number of UEs, optimized for deployment for smaller coverage than Macro eNB, such as indoor premises. HeNB contains the 28 bits option for eNB (i.e. ECI in this case represents the eNB or HeNB with a single sector).

The ECI, eNB-ID and cell sector are very important for RF path planning and installation. The user can use this information on the installation phase to validate it is connected to the appropriate eNB-ID and cell sector per the RF path planning.

eNB-ID

Evolved NodeB Identifier (eNB) is a decimal number used to identify an eNB uniquely within an operator mobile network (or Public Land Mobile Network (PLMN)). The eNB-ID can have either 20 bits or 28 bits. It is also comprised within the Global eNB-ID, which uniquely identifies an eNB globally. The Global eNB-ID is constructed from the Mobile Country Code (MCC), Mobile Network Code (MNC) and eNB-ID i.e. a concatenating number of [MCC | MNC | eNB-ID]. As explained in the ECI description, this eNB-ID value should be ignored when connecting to HeNB where ECI represents the eNB-ID in this case.

Sector
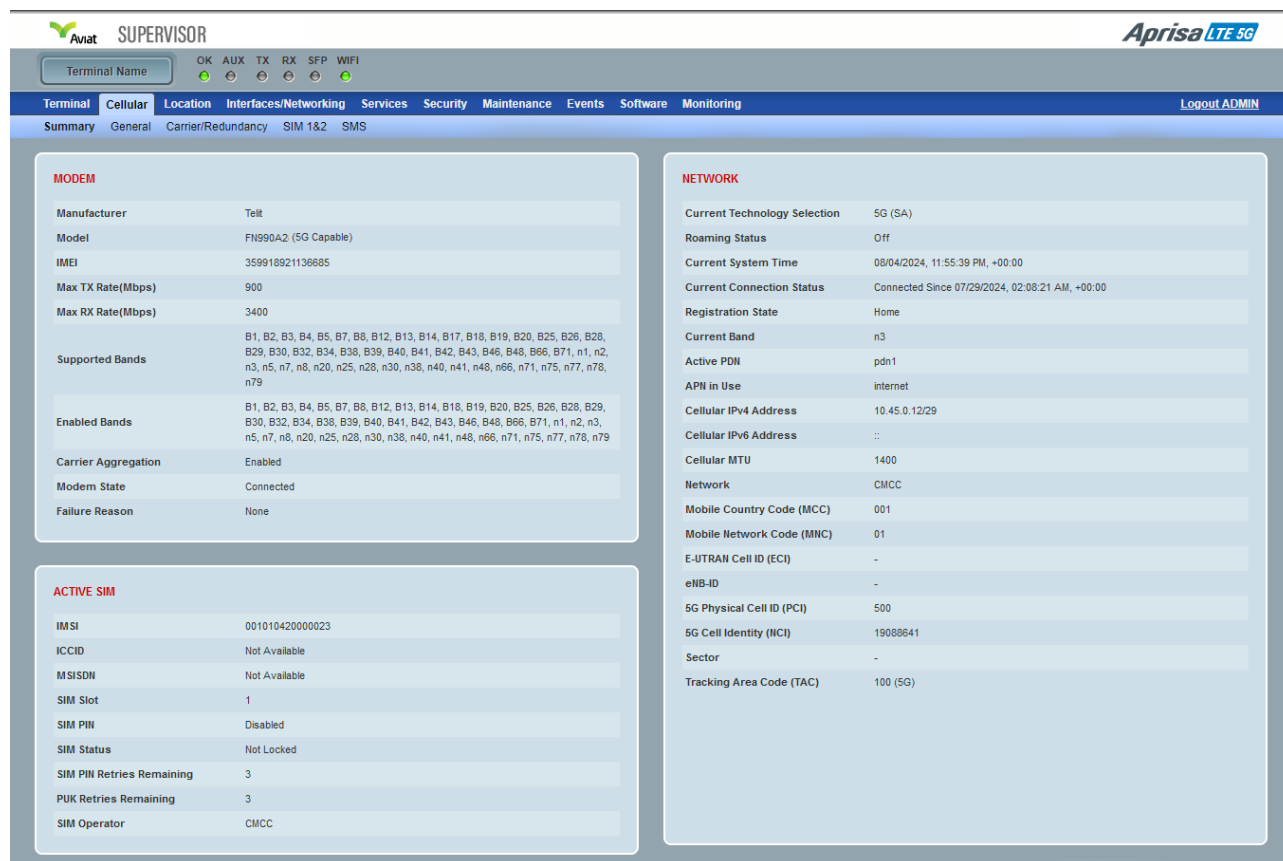
Cell sector represented is a decimal number used as an identifier of a particular sector within an eNB-ID. The cell sector can have either 0 bits or 8 bits. As explained in the ECI description, this cell sector value should be ignored when connecting to HeNB where ECI represents the eNB-ID in this case (i.e. a single sector).

Tracking Area Code (TAC)

Displays the current Tracking Area Code (4 digits). The TAC is used to identify a tracking area (TA) in the cellular network of an operator. The TAC is part of the Tracking Area Identity (TAI). The TAI is composed of a TAC, a Mobile Network Code (MNC) and a Mobile Country Code (MCC) (i.e. a concatenating number of [MCC | MNC | TAC]).

This page displays current Cellular settings.

4G / 5G Modules

NETWORK

Current Technology Selection

Displays the current cellular service selection e.g. LTE.

5G Physical Cell ID (PCI)

The Physical Cell Identity displays the current identifier used to identify a cell within a given frequency band. The network operator allocates the PCI during network planning, and it is unique within a specific coverage area.
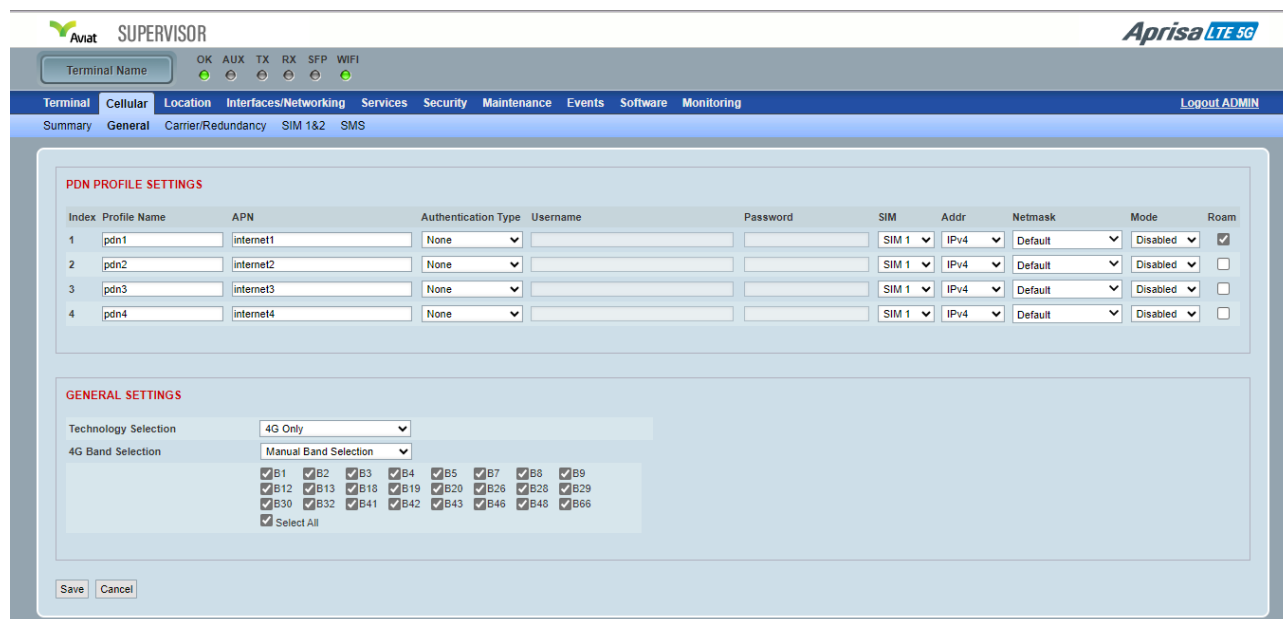
5G Cell Identity (NCI)

The New Cell Identity displays the current unique identifier assigned to each cell to distinguish and manage individual cells within a network.

Cellular > General

This page provides setup of the Cellular General settings.

4G Modules

PDN PROFILE SETTINGS

The four PDN profiles can be configured and the first PDN profile has highest priority followed by lower priority PDNs.

One or more PDNs can be associated / attached with a SIM card slots 1 or 2. One or more PDN profiles can be used as a backup PDN connection to another. The Aprisa LTE 5G will try first to connect to the highest priority PDN and switching between PDN due to connection failure is controlled by the 'Redundancy Settings' configuration parameters (see 'Cellular > Carrier/Redundancy' on page 119).

For example, the user may set four different PDN connections on a single cellular operator (i.e. using a single SIM1 card slot) where the first PDN will serve as the highest priority followed by lower priority PDNs. Another example, user may set first two PDN connections for cellular operator 1 (i.e. on SIM1) and set last two PDN connections for cellular operator 2 (i.e. on SIM2). This means that if the first PDN connection fails the Aprisa LTE 5G will automatically switch to the second PDN within the same cellular operator and only if the second PDN fails it will switch to the third PDN priority and to cell operator 2 and so on. If the last PDN fails to connect, the Aprisa LTE 5G will wrap around to PDN1.

Profile Name

This parameter sets the name of the Packet Data Network profile.

APN

This parameter sets the Access Point Name. The APN Identifies a PDN Gateway (P-GW) and is provided by the cellular operator.

Authentication Type

This parameter sets the authentication type of the Packet Data Network profile.

Option	Function
None	No authentication
PAP	Sets the authentication type to Password Authentication Protocol. PAP uses a two-way handshake to authenticate client sessions.
CHAP	Sets the authentication type to Challenge Handshake Authentication Protocol. CHAP uses a three-way handshake to authenticate client sessions. CHAP is a stronger authentication method than PAP, because the secret is not transmitted over the link, and because it provides protection against repeated attacks during the life of the link
PAP or CHAP	PAP and CHAP authentications are enabled. CHAP authentication is always performed first.

Username

This parameter sets the Packet Data Network profile username (optional).

A username can be up to 32 characters but cannot contain tabs. Usernames are case sensitive.

Password

This parameter sets the Packet Data Network profile password (optional).

A password can be between 8 and 64 characters.

SIM

This parameter selects SIM1 or SIM2.

Addr

This parameter sets the IP address type to request from the network operator.

Option	Function
IPv4	Request an IPv4 format IP address
IPv6	Request an IPv6 format IP address
IPv4v6	Request both IP version 4 and IP version 6
Any	Any IP protocol

Netmask

This parameter enters the Netmask required.

The default value of netmask is 0.0.0.0. With this default, the LTE modem will create a netmask as the smallest subnet that can contain the assigned IP address from the network operator.

Mode

This parameter sets the PDN mode.

Option	Function
Auto	The APN is automatically received from the network based on the SIM card's operator
Enabled	Enables the PDN profile
Disabled	Disables the PDN profile

Roam

This parameter enables the switching from the home network (i.e. the SIM operator network) to the roaming network when the Aprisa LTE 5G is being used outside the range of its home network and connects to another available cellular network (the roaming network). When on the roaming network, charges may be applied per customer contract.

Note: This option is useful if the Aprisa LTE 5G frequently crosses between network operators or between borders. The Aprisa LTE 5G can be fitted with two SIM cards of two network operators that the user might frequently cross. The Aprisa LTE 5G then automatically switches to the SIM that is not roaming (after a configured roaming timeout delay) whenever it crosses between these two known network operators.
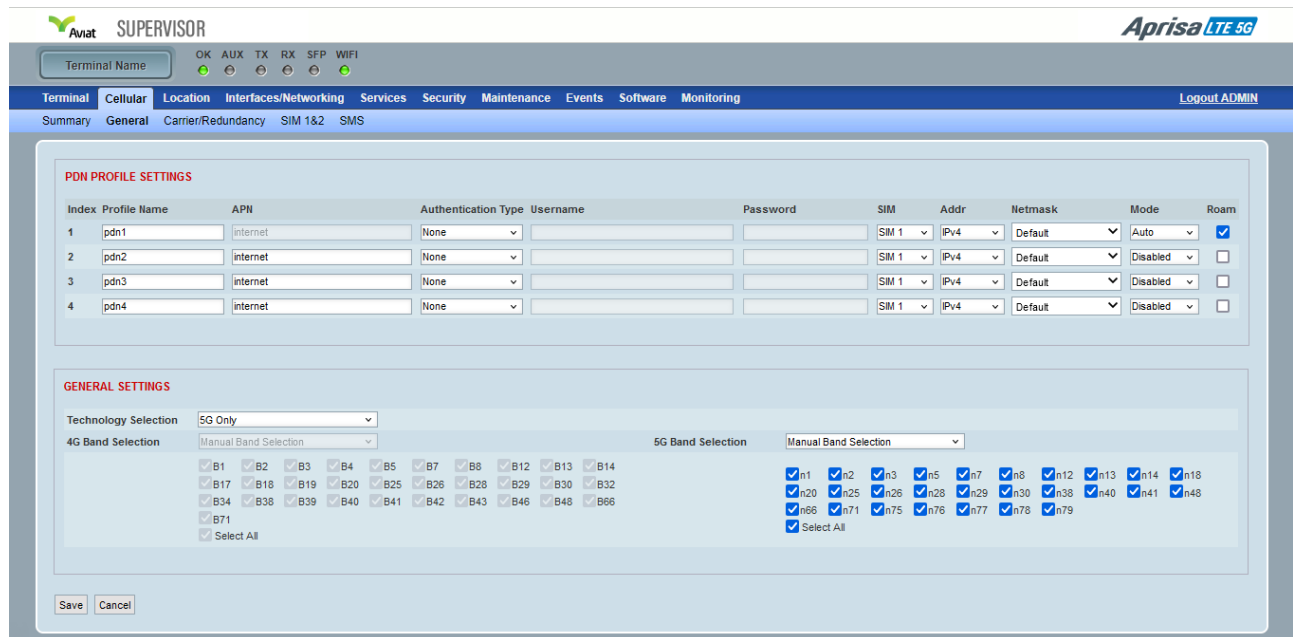
GENERAL SETTINGS

LTE Band Selection

This parameter selects the bands to be enabled from the bands available in the installed LTE Module and supported by the carrier (see 'Modules' on page 50 and 'Network Architecture Overview' on page 30). Tick 'Select All' for all bands.

This page provides setup of the Cellular General settings.

4G / 5G Modules

Technology Selection

This parameter sets the Technology Selection. The default value is 5G/4G Auto Select.

Option	Function
5G/4G Auto Select	The LTE will work in both 5G and 4G networks
4G only	The LTE will work in only a 4G network
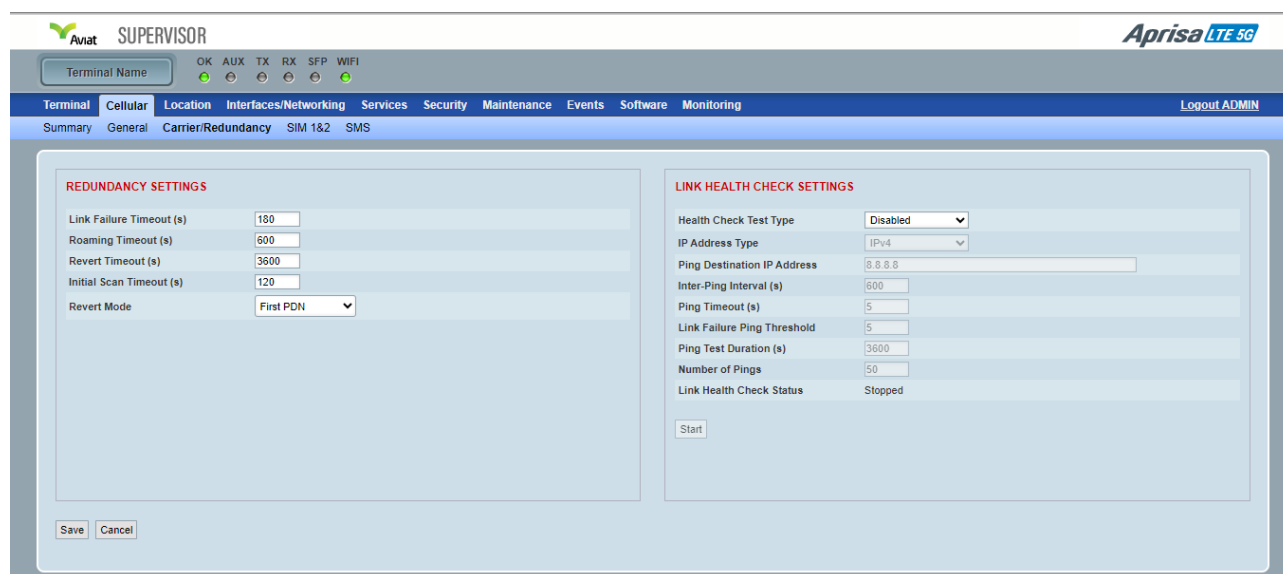
4G LTE Band Selection / 5G LTE Band Selection

This parameter selects the bands to be enabled from the bands available in the installed LTE Module and supported by the carrier (see 'Modules' on page 50 and 'Network Architecture Overview' on page 30). Tick 'Select All' for all bands.

Option	Function
Use Carrier Default Bands	The cellular carrier provides a predefined set of bands optimized for their network, referred to as 'Carrier Default Bands'. This option enables these bands to ensure optimal network performance and coverage, aligning with the carrier's infrastructure.
Manual Band Selection	Manually configure bands. 'Select All' enables all supported bands for a carrier.

Cellular > Carrier/Redundancy

This page provides setup of the Carrier Redundancy settings.

REDUNDANCY SETTINGS

Link Failure Timeout (s)

This parameter sets the duration time (in seconds) to switch to the next lower priority PDN if active PDN data connection is lost or link health check fails for the duration of this timeout. The first PDN in PDN profile settings (see Cellular > General) obtain the highest priority and subsequent are lower priority with the last one as the lowest priority PDN. If only a single PDN configured and fails, then connection to it shall be re-attempted after this timeout. The duration time is unlimited and 0 disables the switching option. The default value is 180 seconds (3 minutes)

Roaming Timeout (s)

This parameter sets the timeout that the connection can be on a roaming network before it automatically switches to a secondary (next lower priority) PDN. If after switching, the secondary PDN network is not available for the 'initial scan timeout' duration, then the connection return to the roaming service network for another roaming timeout time. The roaming timeout value is unlimited, but the recommended range is between 600 – 15,000 seconds. The default value is 600 seconds (10 minutes).

Revert Timeout (s)

This parameter sets the timeout that the connection can be on a secondary (next lower priority) PDN network profile before it automatically reverts to either the primary or next higher priority PDN network profile depending on Revert Mode option. If the timeout value is set to 0, then the revert function will be disabled. If after reverting, the primary PDN network is not available for the 'initial scan timeout' duration, then the connection return to the secondary PDN network for another revert timeout time. The revert timeout value is unlimited. The default value is 3,600 seconds (60 minutes).

Initial Scan Timeout (s)

This parameter sets the timeout to wait for a successful connection after switching to a new PDN network profile. If this times out with unsuccessful connection, then next lower priority PDN profile is used. If there are no lower priority PDNs, then first (highest priority) PDN profile is used. The idle scan timeout value is unlimited. The default value is 120 seconds (2 minutes).

Revert Mode

This parameter controls which PDN profile to select when attempting to revert to a PDN network profile: First PDN, or Previous PDN.

Controls

Start button – starts the heath check.

LINK HEALTH CHECK SETTINGS

Health Check Test Type

This parameter sets the Health Check Test Type ping mode.

Option	Function
Disabled	Health Check Test is disabled
Continuous Ping	The ping test runs continuously
Timed Ping	The ping test runs for the duration specified in 'Ping Test Duration' parameter
Ping Counts	The ping test runs for the number of times specified in 'Number of Pings' parameter

IP Address Type

This parameter sets the IP address type to IPv4 or IPv6.

Ping Destination IP Address

This parameter sets the destination IP address for the pings.

Inter-ping Interval (s)

This parameter sets the time in seconds between pings.

Ping Timeout (s)

This parameter sets the maximum amount of time in seconds to wait for a ping result.

Link Failure Ping Threshold (s)

This parameter sets the number of failed ping attempts to the destination address fails before an alarm is raised. This alarm may also be used for switching to the secondary link.

Ping Test Duration (s)

This parameter sets the time in seconds that a single health check test runs for.
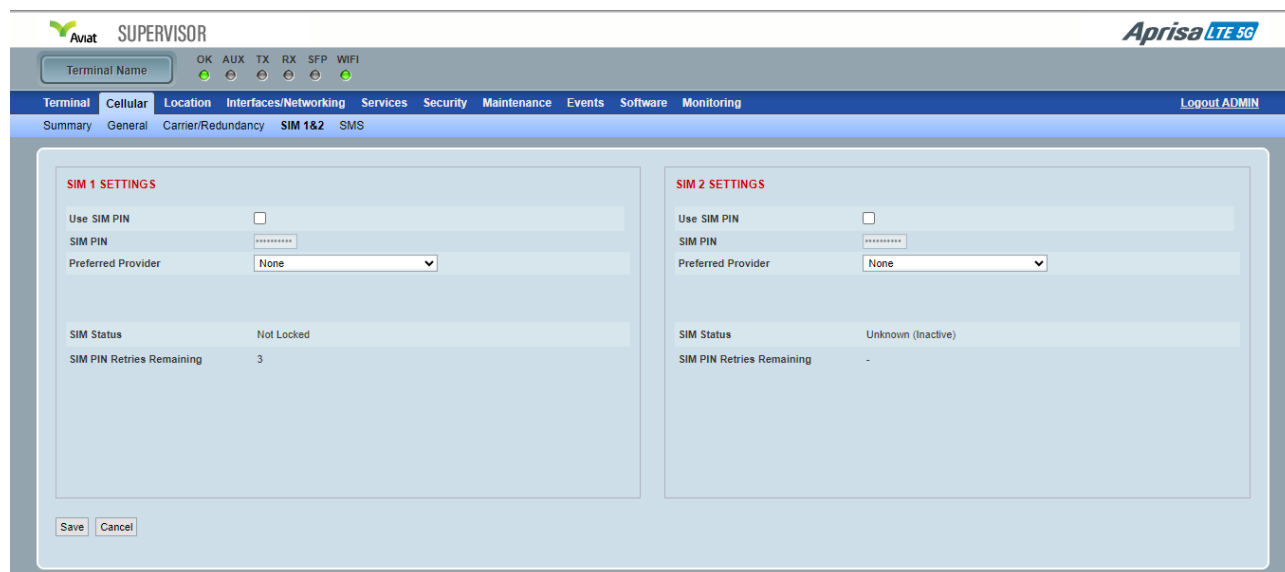
Number Of Pings (s)

This parameter sets the Number of Pings per health check test.

Cellular > SIM 1 & 2

This page provides setup of the SIM 1 & 2 settings.

The SIMs are installed via the rear panel on the LTE (see 'Installing a SIM' on page 69).

SIM 1 & 2 SETTINGS

Use SIM PIN

When selected, the SIM PIN can be entered to allow modem access a locked SIM.

SIM PIN

Enter a PIN number to allow modem access to a locked SIM. This only needs to be entered once, providing the SIM is not changed. The pin must be between 4 and 8 characters.

Preferred Provider

This parameter sets the Preferred Provider e.g. None, AT&T, Verizon Wireless, etc.

SIM Status

This parameter displays the SIM status; Not locked, Locked (PIN), Locked (PUK), Present.
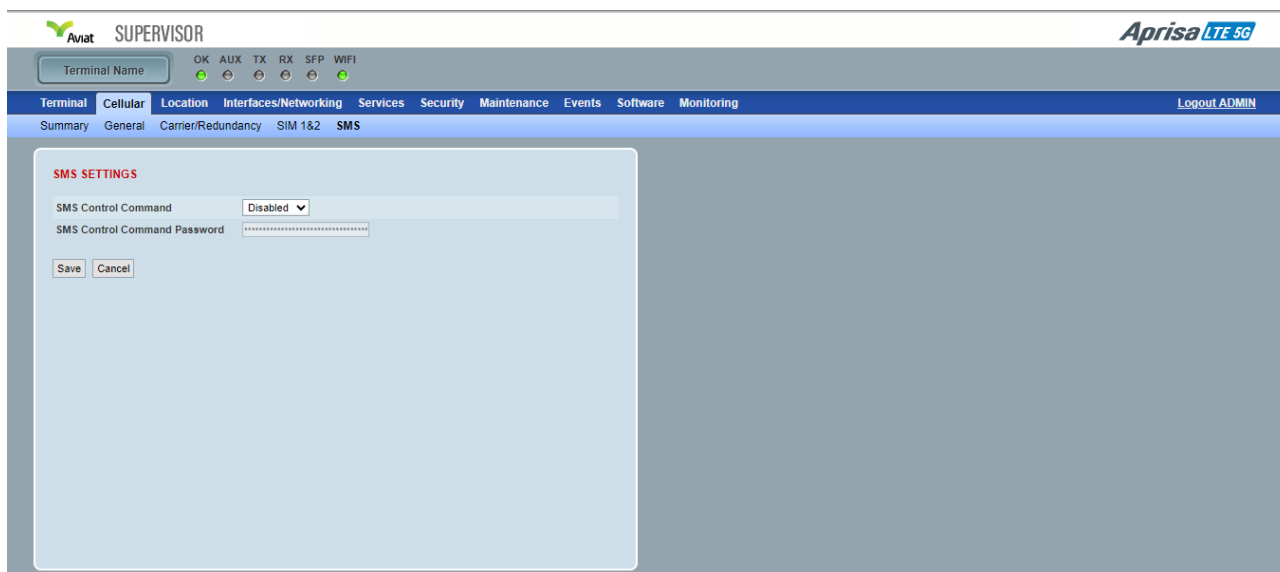
SIM PIN Retries Remaining

This parameter displays the number of SIM PIN retries remaining when entering the SIM PIN number.

Note: See 'Configure CLI Commands' on page 299 for more SIM commands

Cellular > SMS

This page provides setup of the SMS port parameters.

SMS SETTINGS

SMS Control Command

This parameter enables / disables the Short Message Service control command.

SMS Control Command Password

This parameter sets the Short Message Service control command password.

The password is used to verify commands sent to the Aprisa LTE 5G over SMS.
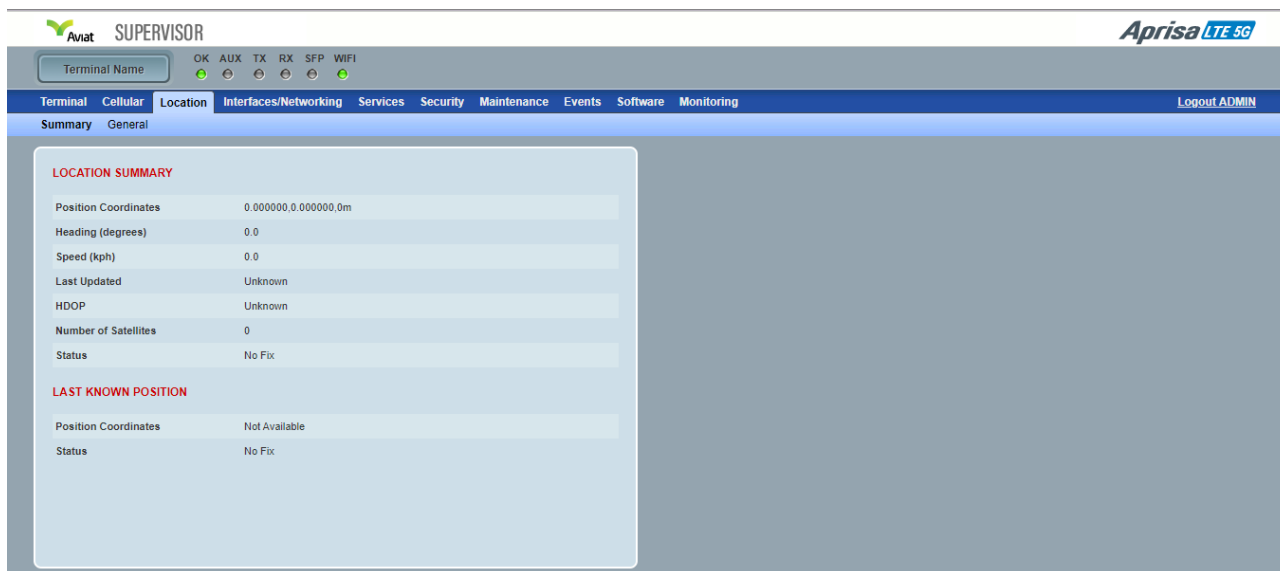
SMS messages must be sent in the format of <password> <space> <command>.

e.g. if password is 'passabc', then the command to reboot the Aprisa LTE 5G using SMS will be 'passabc reboot'.

Location

Location > Summary

This page displays the current GNSS values.

LOCATION SUMMARY

Position Coordinates

The current GNSS latitude, longitude and altitude.

Heading (degrees)

The current direction in degrees.

Speed (kph)

The current speed in kilometers per hour

Last Updated

The last time the GNSS data was updated.

HDOP

The GPS Horizontal Dilution Of Precision (HDOP) information provides a GPS signal quality rating;

DOP Value	Rating	Description
< 1	Ideal	Highest possible confidence level to be used for applications demanding the highest possible precision at all times.
1-2	Excellent	At this confidence level, positional measurements are considered accurate enough to meet all but the most sensitive applications.
2-5	Good	Represents a level that marks the minimum appropriate for making business decisions. Positional measurements could be used to make reliable in-route navigation suggestions to the user.
5-10	Moderate	Positional measurements could be used for calculations, but the fix quality could still be improved. A more open view of the sky is recommended.
10-20	Fair	Represents a low confidence level. Positional measurements should be discarded or used only to indicate a very rough estimate of the current location.
>20	Poor	At this level, measurements are inaccurate by as much as 300 meters with a 6-meter accurate device (50 DOP × 6 meters) and should be discarded.

Number of Satellites

The number of satellites reported as visible by the GNSS receiver.

Status

The status of the GNSS fix.

LAST KNOWN POSITION

Position Coordinates
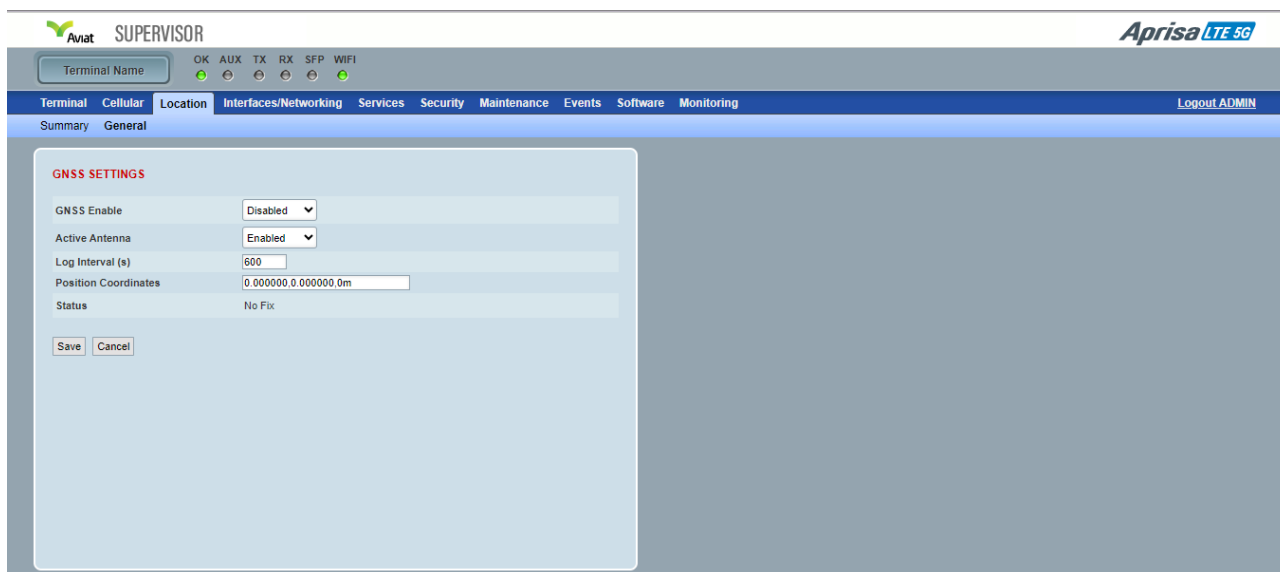
The last known GNSS latitude and longitude. If position coordinates are manually set in Location > General and auto fix is not available, then the manually configured position will be shown here.

Status

The last know GNSS status. This will show if last known position is an automatic fix or a manually configured position.

Location > General

This page provides setup of the GNSS port parameters.

GNSS SETTINGS

GNSS Enable
This parameter enables / disables GNSS.

Active Antenna
This parameter enables / disables the GNSS antenna power (3.3V).

Log Interval (min)
This parameter sets the interval in seconds between GNSS log entries. 0 disables GNSS logging. The default is 600 seconds.

Position Coordinates
This parameter manually sets the position latitude and longitude.
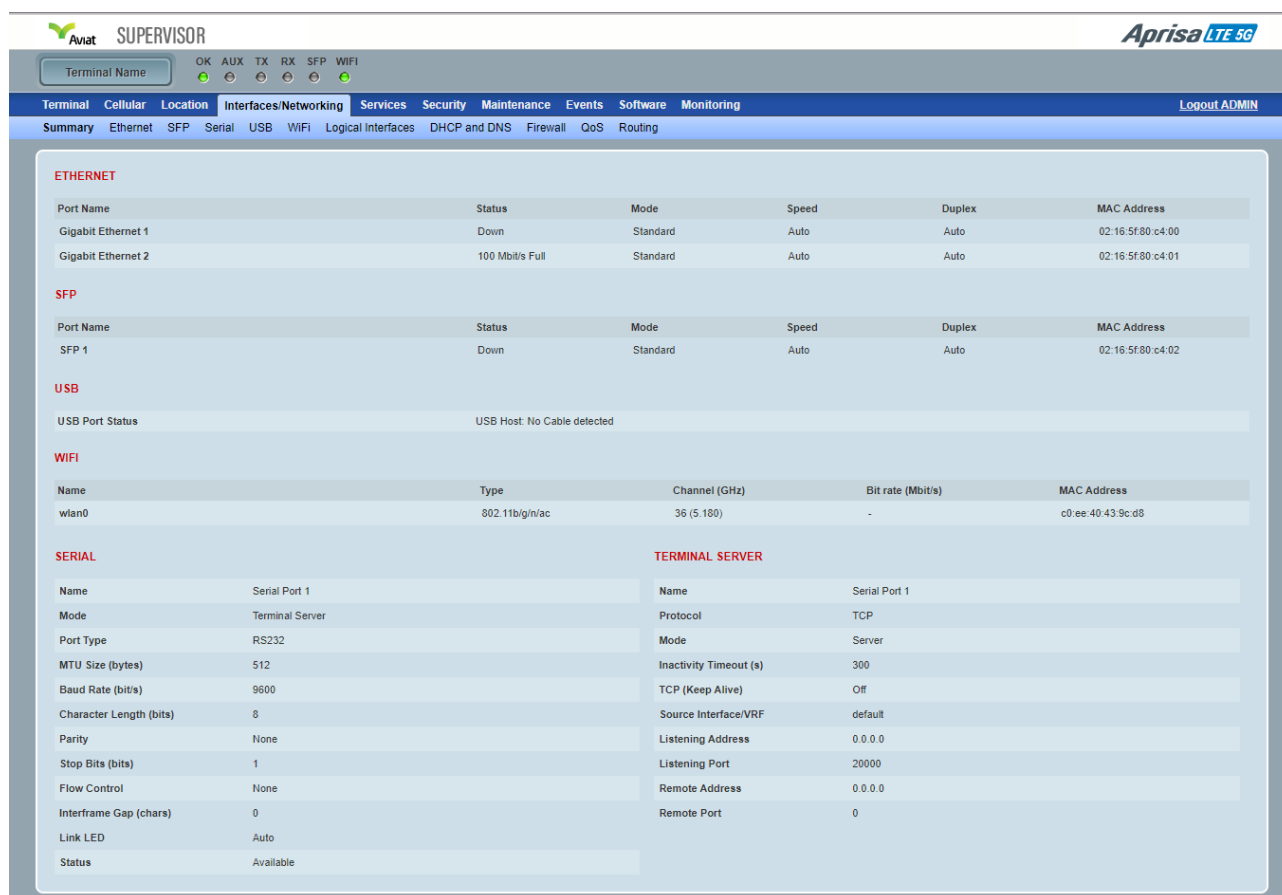
Status
The last know GNSS status.

Interfaces/Networking

Interfaces/Networking > Summary

This page displays the current settings for all interfaces and the status of the ports.

See the Interfaces/Networking pages for settings.

Interfaces/Networking > Ethernet

This page provides setup of the Ethernet port parameters.

ETHERNET PORT SETTINGS

Name

This parameter sets the port name which can be up to 32 characters. This name is only to aid customer and is not used by the LTE other than for display.

Mode

This parameter controls the enable/disable of the Ethernet port. The default setting is Standard.

Option	Function
Standard	Ethernet Port is in standard operation
Disabled	Ethernet port is disabled. Useful when the port is unused or when user would like to save in power consumption

Speed (Mbit/s)

This parameter controls the traffic rate of the Ethernet port. The default setting is Auto.

Option	Function
Auto	Provides auto selection of Ethernet Port Speed 10/100/1000 Mbit/s
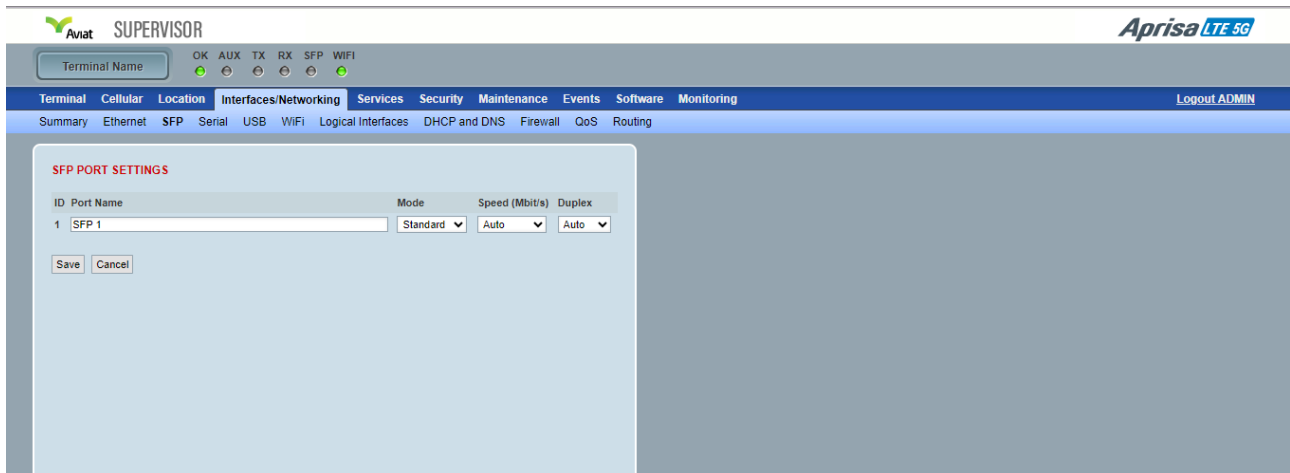
Duplex

This parameter controls the transmission mode of the Ethernet port. The default setting is Auto.

Option	Function
Auto	Provides auto selection of Ethernet Port duplex setting.

Interfaces/Networking > SFP

This page provides setup of the SFP module if fitted to the LTE.

SFP PORT SETTINGS

Name

This parameter sets the port name which can be up to 32 characters.

Mode

This parameter controls the enable/disable of the Ethernet port. The default setting is Standard.

Option	Function
Standard	SFP Port is in standard operation
Disabled	SFP port is disabled. Useful when the port is unused or when user would like to save in power consumption

Speed (Mbit/s)

This parameter controls the traffic rate of the Ethernet port. The default setting is Auto.

Option	Function
Auto	Provides auto selection of SFP Port Speed 10/100/1000 Mbit/s
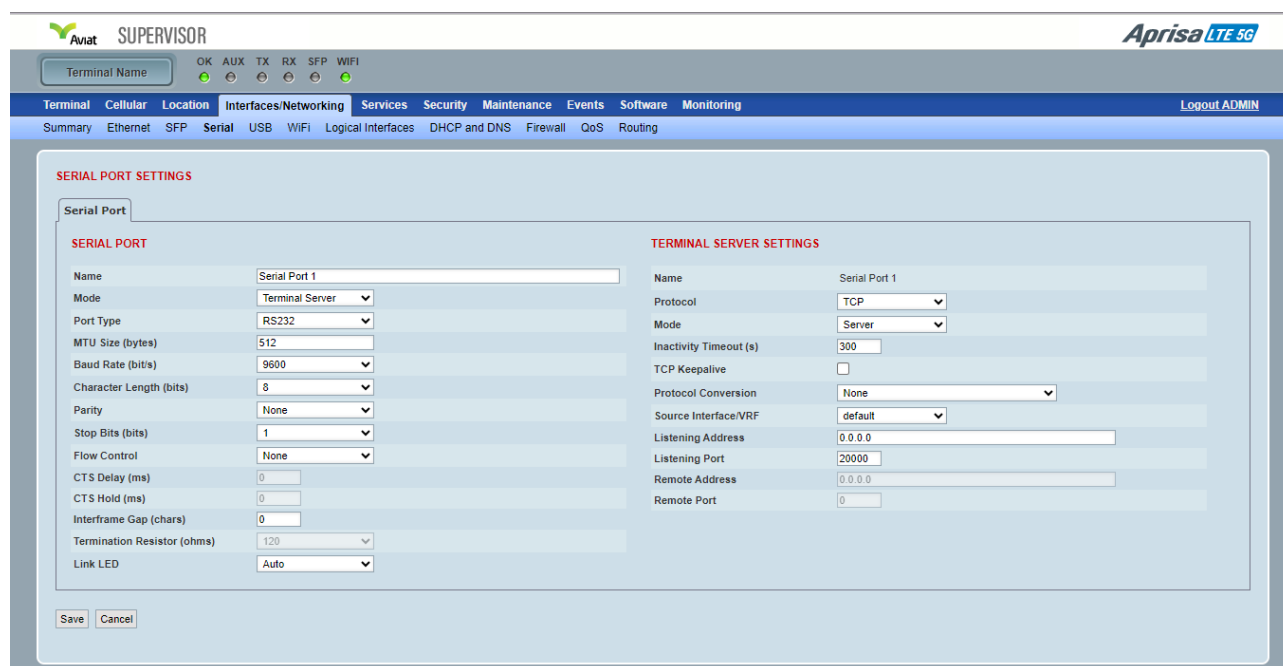
Duplex

This parameter controls the transmission mode of the SFP Ethernet port. The default setting is Auto.

Option	Function
Auto	Provides auto selection of SFP Port duplex setting.

Interfaces/Networking > Serial

This page provides setup of the Serial port parameters.

SERIAL PORTS SETTINGS

Name

This parameter sets the port name which can be up to 32 characters.

Mode

This parameter defines the mode of operation of the serial port. The default setting is Standard.

Option	Function
PPP	Serial traffic is Point-to-Point Protocol.
Disabled	The serial port is not required.
Terminal Server	Serial traffic is encapsulated in IP packets.

Port Type

This parameter defines the mode of operation of the serial port. The default setting is Standard.

Option	Function
RS-232	RS-232 provides asynchronous communication between two devices over unbalanced TX, RX and control lines.
	It defines signals connecting between a DTE such as a computer terminal, and a DCE, such as a modem
RS-422	RS-422 only offers one-way high speed and/or long distance data transmission. A single transmitting (master) device to up to 10 receiving (slave) devices. This is dependent on the wire type, baud rate, distance etc.
	Two-way communication requires two pairs, one for each direction.
RS-485 Half Duplex	RS-485 half duplex provides multi-drop two way communication between a master device and up to 32 slave devices on a 2 wire bus.
	With Half Duplex, data can only pass in one direction at a time to and from the devices. A 120 ohm termination is required at the end of the bus pair.
RS-485 Full Duplex	RS-485 full duplex provides multi-drop two way communication between a master device and up to 32 slave devices on a 4 wire bus.
	With Full Duplex, data can pass simultaneously both to and from the devices. A 120 ohm termination is required at the end of each pair of the bus.

MTU Size (bytes)

This parameter sets the size of the packet in bytes received before it is transmitted if an inter-frame gap is not detected. Setting a smaller Maximum Transmission Unit (MTU) may reduce latency, but this should only be done if the serial protocol is known to allow gaps at the receiver. The default setting is 512 bytes.

Baud Rate (bit/s)

This parameter sets the baud rate to 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 128000 or 230400 bit/s. The default setting is 9600 bit/s.

Character Length (bits)

This parameter sets the character length to 7 or 8 bits. The default setting is 8 bits.

Parity

This parameter sets the parity to Even, Odd or None. The default setting is None.

Stop Bits (bits)

This parameter sets the number of stop bits to 1 or 2 bits. The default setting is 1 bit.

Flow Control

This parameter sets the flow control of the serial port. The default setting is Disabled.

Option	Function
None	The LTE port (DCE) CTS is in a permanent ON (+ve) state.
	If router enters sleep state, then CTE goes OFF.
CTS-RTS	CTS / RTS hardware flow control between the DTE and the Aprisa SR+ router port (DCE) is enabled.
	The CTS state follows the RTS state.
	If the LTE buffer is full or the LTE is in sleep state, the CTS goes OFF.
CTS-Keying	CTS Keying is needed when working with devices that require to be keyed before sending data;
	• Driving legacy modems that use the CTS signal as a key-up signal.
	• Driving external RS-485 converters, where the CTS signal is used as a Tx enable

CTS Delay ms

In CTS-RTS mode, this parameter sets the delay between CTS and RTS. The default setting is 0 ms.

In CTS-Keying mode, this parameter sets the period the between the CTS being set and data being transmitted. The default setting is 0 ms.

CTS Hold ms

In CTS-Keying mode, this parameter sets the period the between the end of the data and CTS being cleared. The default setting is 0 ms.

Inter-Frame Gap (chars)

This parameter defines the gap between successive serial data frames. It is used to delimit the serial data to define the end of a packet.

Smaller values give better serial latency, however if this value is too small then packets may be incorrectly split and serial speed may be much slower. If this value is too large serial packets may be incorrectly joined together.

The Inter-Frame Gap limits are 0 to 9999 chars in steps of 0.1 char. The default setting is 3.6 chars.

An alarm event indicates if the value is set larger than the maximum for the serial mode selected.

Terminating Resistor (ohms)

Used for Port Types of RS-422 and RS-485.

When enabled, the RX port, or the TX/RX port for RS-485 half-duplex port is terminated in 120 ohms. The default setting is disabled.

Link LED

This parameter defines the operation serial port Link LED (left LED on RJ45 connector). The default setting is Auto.

Option	Function
Auto	For RS232 mode only, the link LED is on if either CTS or DSR is asserted by peer device, or if data has been received in last 10 seconds. If using RS422 HD, RS232 FD or RS485 the link LED is always on.
Always On	The link LED is always on regardless of link status.

TERMINAL SERVER SETTINGS

Protocol

This parameter sets the protocol used for terminal server operation. The default setting is TCP.

Option	Function
UDP	Selects UDP/IP protocol.
TCP	Selects TCP/IP protocol.
TCP (Persistent)	Selects TCP/IP protocol.
	This option is only relevant when Mode = 'Client' or Mode = 'Client and Server'. In TCP (Persistent) option, the Client will always establish and keep connection open with the Server (even without serial traffic). If the TCP connection is closed for any reason, the Client will automatically reconnect to the Server.
	When this option is selected, the 'TCP Keep Alive' must be enabled and therefore the checkbox is automatically forced to be enabled (ticked) and grey out.
	If this option is no longer selected and either TCP or UDP is selected, then the 'TCP Keep Alive' checkbox will be returned to the state it was when the TCP (Persistent) was last selected.

Mode

This parameter defines the mode of operation of the terminal server connection. The default setting is Client and Server.

Option	Function
Client	The LTE will attempt to establish a TCP connection with the specified remote address when data is presented on the serial port.
Server	The LTE will listen for a TCP connection on the specified local port.
	Data received from any client shall be forwarded to the associated serial port while data received from that serial port shall be forwarded to every client with an open TCP connection.
	If no existing TCP connections exist, all data received from the associated serial port shall be discarded.
Client and Server	The LTE will listen for a TCP connection on the specified local port and if necessary, establish a TCP connection with the specified remote unit.
	Data received from any client shall be forwarded to the associated serial port while data received from that serial port shall be forwarded to every client with an open TCP connection.

Inactivity Timeout (seconds)

This specifies the duration (in seconds) to automatically terminate the connection with the remote TCP server if no data has been received from either the remote TCP server or its associated serial port for the duration of the configured inactivity time.

TCP Keep Alive

A TCP keep alive is a message sent by one device to another to check that the link between the two is operating, or to prevent the link from being broken.

If the TCP keep alive is enabled, the LTE will be notified if the TCP connection fails.

If the TCP keep alive is disabled, the LTE relies on the Inactivity Timeout to detect a TCP connection failure. The default setting is disabled.

Note: An active TCP keep alive will generate a small amount of extra network traffic.

Protocol Conversion

This parameter sets the protocol conversion of the serial port. The default setting is None.

Option	Function
None	No protocol conversion
Modbus TCP to Modbus RTU	The LTE provides a gateway between Modbus TCP to Modbus RTU
Modbus TCP to Modbus ASCII	The LTE provides a gateway between Modbus TCP to Modbus ASCII

Source Interface / VRF

This parameter sets the source VRF (Virtual Routing and Forwarding) interface of the serial port. This option allows the user to connect the terminal server to any VRF the user created. The default setting is Default.

Option	Function
Default	The default / main VRF is the source interface for the serial port.
Customer defined VRFs (e.g. RED)	The customer defined VRF (e.g. RED) is the source interface for the serial port.

Listening Address

This parameter sets the serial Terminal Server local IP address.

Listening Port

This parameter sets the TCP or UDP port number of the local serial port.

Exclusions can be set by other enabled services – tcp ports 80 (http), 443 (https), and 22 (ssh), udp ports 161 and 162 (snmp). The default setting is 20000.

The user is responsible for ensuring that there is no conflict on the network.

Remote Address
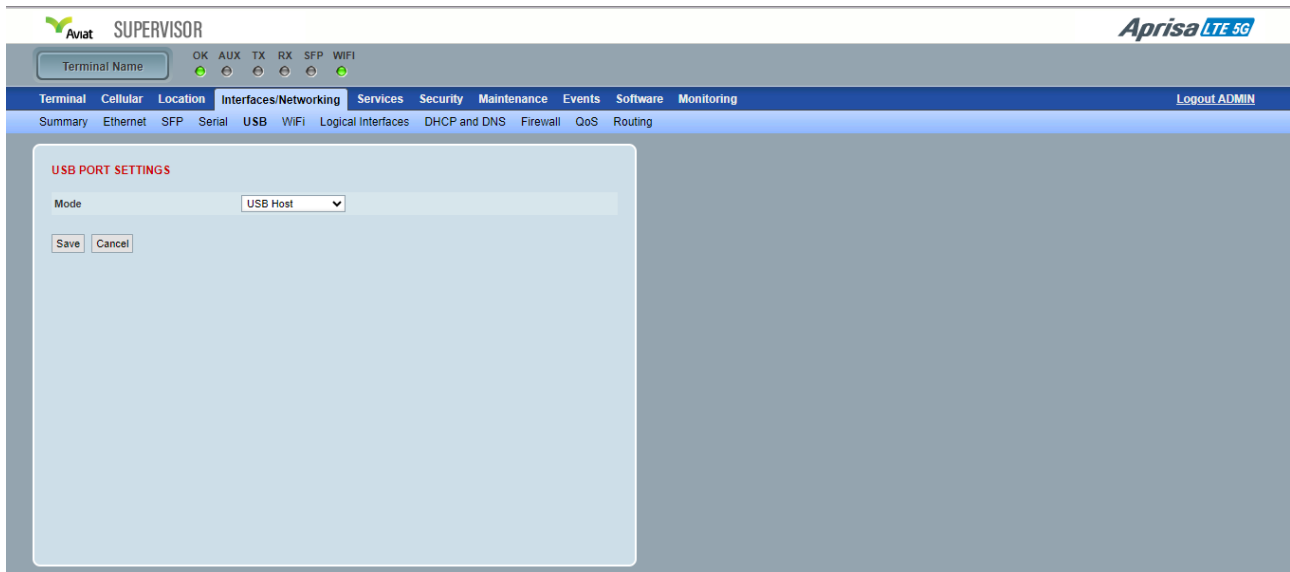
This parameter sets the IP address of the server connected to the LTE Ethernet port. When the remote address / port is configured as 0.0.0.0/0, each outgoing UDP packet will be sent to the source address of the last received UDP packet.

Remote Port

This parameter sets the port number of the server used in TCP client, TCP client server or UDP modes. The default setting is 0.

Interfaces/Networking > USB

This page provides setup of the USB host port parameters.

USB DETAILS
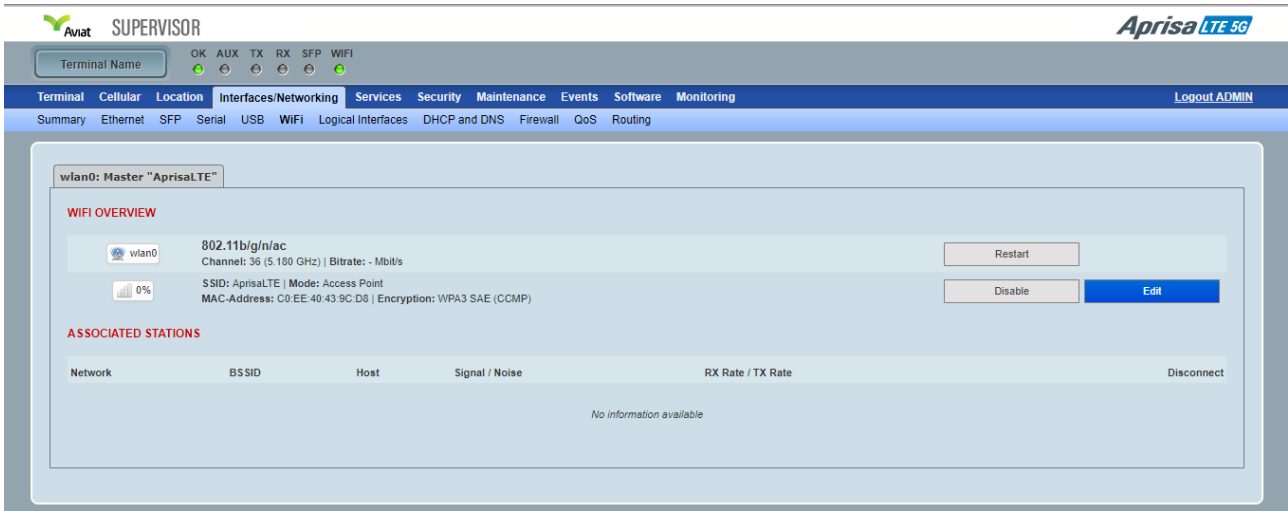
Mode

This parameter defines the mode of operation of the USB port. The default setting is Auto.

Option	Function
Auto	The mode is determined by what is connected at bootup. If nothing is connected, then CLI Management is assumed.
Disabled	The USB port is not required.
USB Host	The USB port is active for QR code scanning, software upgrades etc.
CLI Management	The USB port is active for local CLI Management access.

Interfaces/Networking > WiFi

This section provides setup of the WiFi port parameters.

Scan Button

The Scan Button scans for Wi-Fi networks.

Edit Button

The Edit Button edits the Wi-Fi device configuration.

DEVICE CONFIGURATION

This page provides setup of the WiFi Device General Setup.
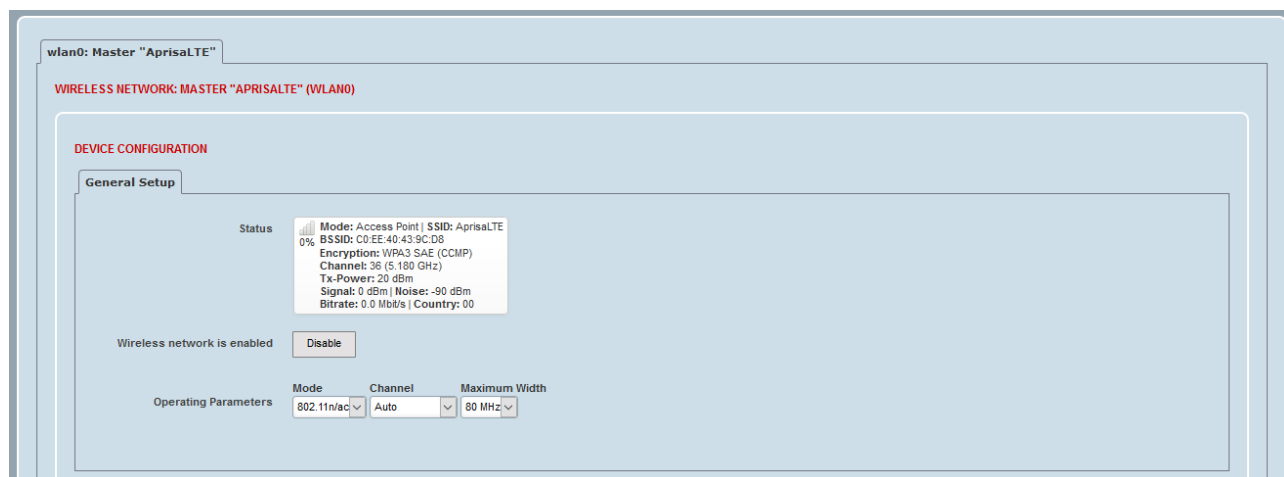
SSID

The Service Set ID (SSID) is the unique name of WLAN (wireless WiFi LAN) network. Since multiple WLANs can coexist in one airspace, each WLAN needs a unique name which is the SSID of the network. A WiFi client device can see the SSIDs for all available networks.

BSSID

The Basic Service Set Identifier (BSSID) is by convention, an Access Point's MAC address. The SSID keeps the packets from client device within the correct WLAN, even when overlapping WLANs are present. However, there are usually multiple APs and their associated clients within each WLAN and BSSID is the AP identifier which makes the bound between AP and its clients and included in all wireless packets. User (client device) are aware to the network SSID but usually unaware to which BSSID they are currently connected.
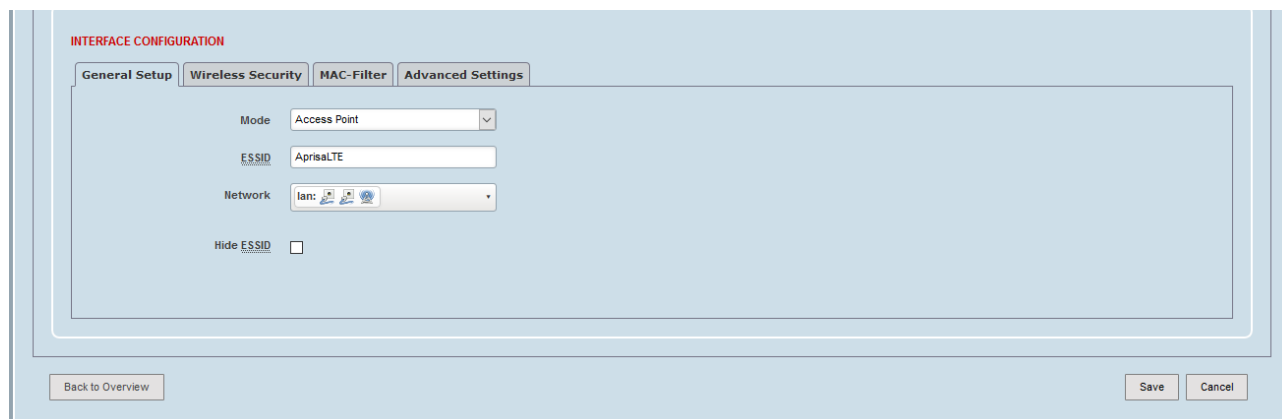
ESSID

The Extended Service Set Identifier (ESSID) consists of all the BSSIDs in the network. For practical purposes, the ESSID identifies the same network as the SSID.

INTERFACE CONFIGURATION

WiFi Interface Configuration > General Setup

This page provides setup of the WiFi Interface General Setup.

Mode

This parameter sets the WiFi mode. The default setting is Access Point.

Option	Function
Access Point	In Access Point (AP) mode, the LTE provides connectivity to other Wi-Fi clients, and can share its network connections with them.
Client	In Client mode, the wireless client is assigned an IP from the associated AP, and is able to access to wired network through associated AP.

ESSID
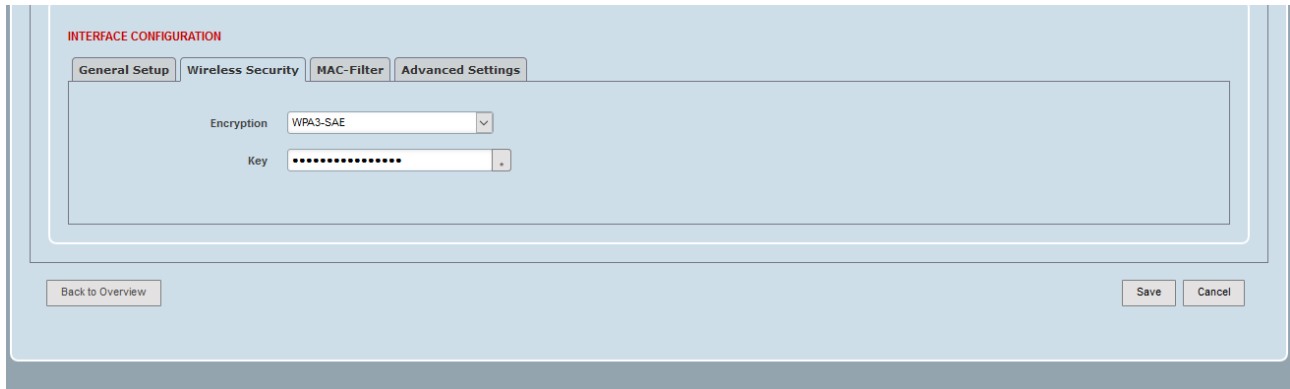
This parameter sets the WiFi ESSID. The Extended Service Set Identifier (ESSID) consists of all the BSSIDs in the network. For practical purposes, the ESSID identifies the same network as the SSID. The default setting is AprisaLTE.

Network

This parameter sets the logical network to associate the Wi-Fi network with. Select a network from the presented list, or you may choose to create a new network.

WiFi Interface Configuration > Wireless Security

This page provides setup of the WiFi Wireless Security.
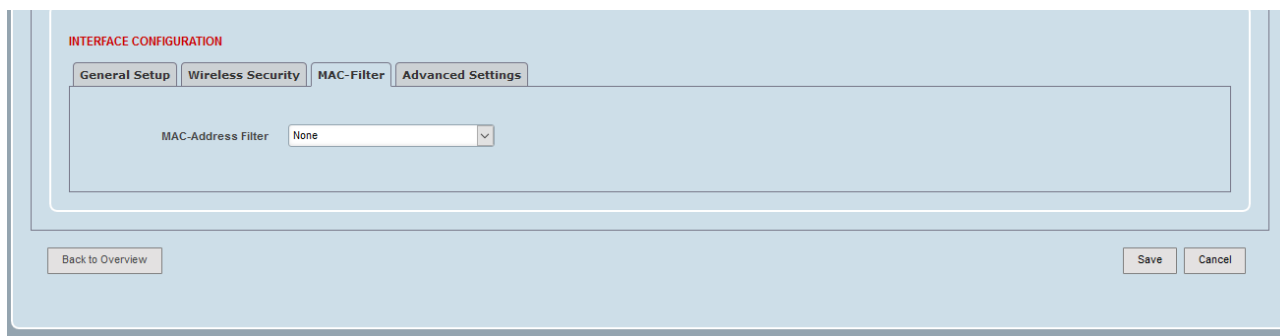
Encryption

This parameter sets the WiFi encryption. The default setting is No Encryption.

Option	Function
No Encryption	No Wi-Fi encryption
WEP Open System	Wired Equivalent Privacy (WEP) is an older Wi-Fi security standard. It is not secure and should only be used for compatibility with older equipment.
WEP Shared key	Wired Equivalent Privacy (WEP) is an older Wi-Fi security standard. It is not secure and should only be used for compatibility with older equipment.
WPA-PSK	Wi-Fi Protected Access (WPA) is an older Wi-Fi security standard that is still in common use.
WPA2-PSK	WPA2 is an enhanced version of WPA which provides improved security. WPA2-PSK (Pre Shared Key) is commonly used in home and small office scenarios.
WPA-EAP	WPA with Extensible Authentication Protocol (EAP). Often called WPA-Enterprise, it is based on the 802.1X standard.
WPA2-EAP	WPA2 with Extensible Authentication Protocol (EAP). Often called WPA-Enterprise, it is based on the 802.1X standard.
WPA3-SAE	WPA3 with Simultaneous Authentication of Equals (SAE). Often called WPA3-Personal.
WPA3-EAP	WPA3 with Extensible Authentication Protocol (EAP). Often called WPA-Enterprise, it is based on the 802.1X standard.
WPA3-EAP / WPA2-EAP	Combination of WPA3-EAP and WPA2-EAP.

WiFi Interface Configuration > MAC Address Filter

This page provides setup of the WiFi MAC Address Filter.
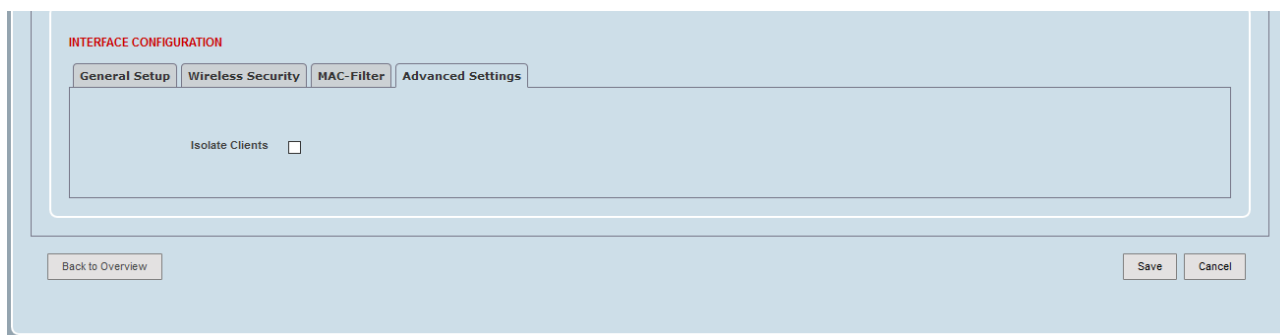
MAC Address Filter

This parameter sets the WiFi MAC address filter. The default setting is None.

Option	Function
None	No Wi-Fi MAC address filter
Allow Listed MACs	Allow access to all MAC addresses in the Wi-Fi MAC access control list (ACL).
Allow all Except Listed MACs	Allow access to all MAC addresses except those in the Wi-Fi MAC access control list (ACL).

WiFi Interface Configuration MAC > Advanced Settings

This page provides setup of the WiFi Advanced Settings.
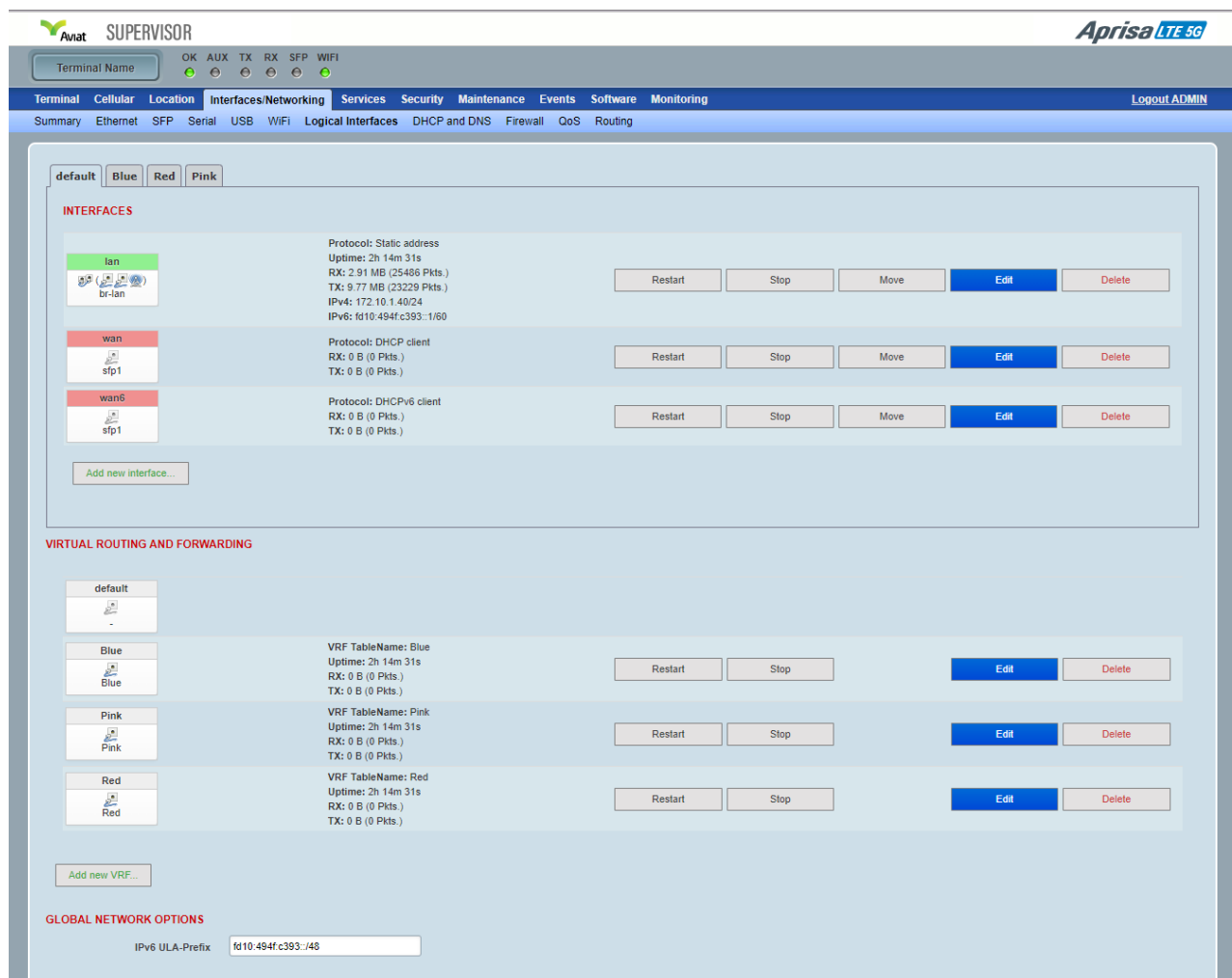
Isolate Clients

This parameter confines and restricts clients connected to the Wi-Fi network. When enabled, clients cannot communicate with each other or with wired network when the WiFi interface is bridged with other interfaces. They can only access routed networks (such as the Internet) through the Aprisa LTE 5G. The default setting is Inactive.

Interfaces/Networking > Logical Interfaces

This section configures the logical interfaces. Logical interfaces can be added or deleted.

IPv6 ULA-Prefix

This parameter sets the IPv6 ULA (Unique Local Address) prefix in use in this network. A ULA prefix is analogous to the IPv4 private address spaces (192.168/16, 172.16/12 and 10/8). This is normally a /48 prefix within the fd00::/8 range defined in RFC4192.

The default value is randomly generated and different on each Aprisa LTE 5G. If your organization uses ULA addressing, this should be modified to the appropriate prefix.

Controls

Restart

This restarts the interface which causes the interface to be disabled (with link status down), then restarted. This will clear address tables learnt on that interface and break any ongoing connections using that interface.

Stop

This disables the interface.

Edit

This button opens the selected interface configuration page.

Delete

This deletes the interface.

Add New Interface

Interface Name

This parameter sets the name of the interface up to 15 chars.

Protocol

This parameter sets the protocol used on the interface. The default setting is Static Address.

Option	Function
Static Address	Allows assignment of one or more IPv4 and/or IPv6 static addresses, along with manual configuration of default gateway.
DHCP Client	Allows automatic configuration of IPv4 address, netmask, gateway and DNS servers through the DHCP protocol.
DHCPv6 Client	Allows automatic configuration of IPv6 from any combination of stateless DHCPv6, stateful DHCPv6, DHCPv6-PD and SLAAC.
PPP	Sets the protocol to PPP (Point-to-Point Protocol).

Create Loopback

This creates a loopback interface. A loopback interface is a virtual network interface (i.e. a software-based interface) that is not associated with a physical interface. In general, this interface is always in the UP state.

Create a bridge over multiple interfaces

If this parameter is selected, a bridge (virtual switch), can be created by selecting multiple physical interfaces.

Cover the following interface

This option selects the physical interface to assign to the logical interface being created. If 'Create a bridge over multiple interfaces' is selected, you can select multiple options.

Option	Function
Ethernet Adapter 'erspan0'	Currently not available in this software.
Ethernet Adapter 'eth1'	This selects the ETH1 port.
Ethernet Adapter 'eth2'	This selects the ETH2 port.
Bridge	This selects the virtual bridge/switch. Multiple virtual switch instance (VSI) can be created/used.
Ethernet Adapter 'loop0-7'	This selects a loopback adaptor. This is a virtual adaptor allowing assignment of IP addresses that will always be active. This type of adaptor cannot be used as part of a bridge.
Ethernet Adapter 'sfp1'	This selects the SFP port.
Ethernet Adapter 'teq10'	Currently not available in this software.
Ethernet Adapter 'wlan0'	This selects the Wi-Fi modem.
Ethernet Adapter 'wwan0'	This selects the cellular modem. This type of adaptor cannot be used as part of a bridge.
Custom	Allows creation of custom VLAN tag interfaces. See below for details.

Custom: VLAN interface

This allows creation of virtual 802.1q VLAN tag interfaces. For example, entering 'eth1.100' creates an interface that uses 802.1q packets with VLAN id 100 on ETH1.

Custom: VLAN bridge

To pass for example VLAN id 100 between ETH1 and ETH2, enter 'eth1.100' and 'eth2.100'.

To create a VLAN bridge with ETH1 having id 100, ETH2 having id 200, and SFP being a trunk port:

First create a new logical interface, select 'Create a bridge over multiple interfaces', and then select 'eth1.100' and 'sfp1.100'.

Next create a second logical interface, select 'Create a bridge over multiple interfaces', and then select 'eth2.200' and 'sfp1.200'.

Note: It is not necessary to assign an IP address to every bridge interface. If the Aprisa LTE 5G only needs to do L2 switching on a given VLAN, and not participate in any conversations, then it is normal to use Static protocol, and leave the Address, Netmask etc blank/unassigned.

Custom: Stacked VLAN

It is possible to stack multiple 802.1q VLAN tags. For example, to have an inner tag of 100, and outer tag of 200:

First the outer VLAN create a new logical interface, then enter custom interface of 'eth1.200'. Select Static protocol, and leave address, netmask etc blank/unassigned.

Next create a second logical interface, then enter custom interface of 'eth1.200.100'.

Add New VRF

VRF Device Name
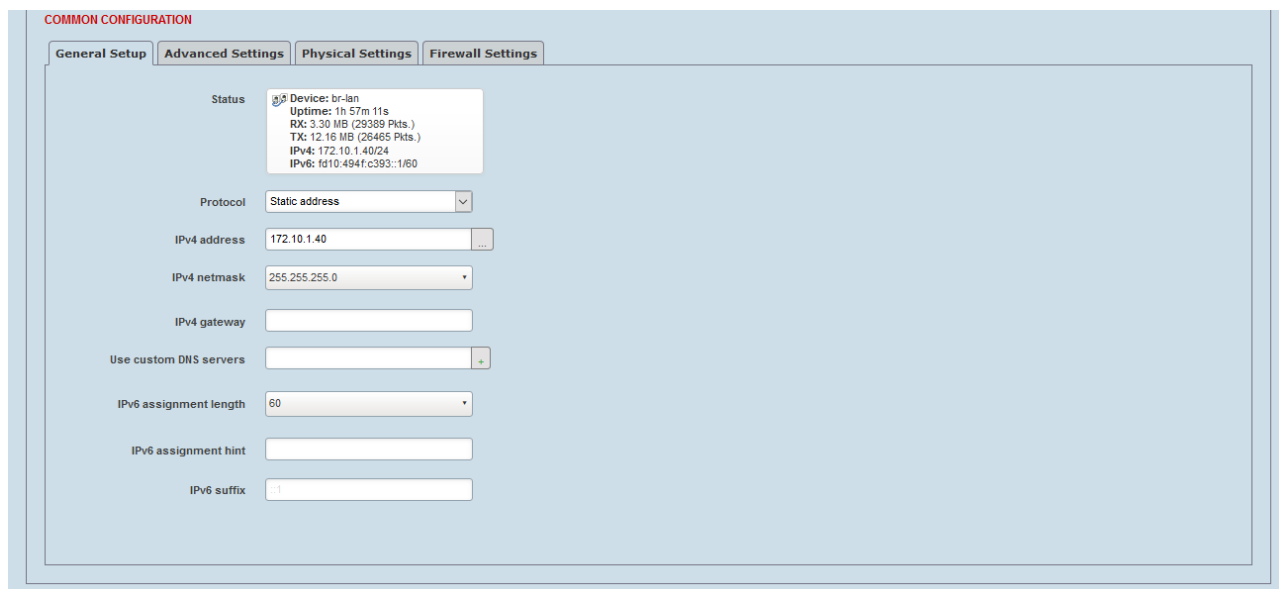
This parameter sets the name of the VRF up to 15 chars. The name must be unique among all VRFs and must not be empty.

VRF is a virtual routing instance that allows group and/or service segregation and isolation each with its own routing table (L3) on the same Aprisa LTE 5G platform to increases security. This allows any interface, virtual interface, and/or some protocol functions in Aprisa LTE 5G to be associated (enslaved) with a specific VRF that the user can create.

For more information see 'VRF (Virtual Routing and Forwarding) and VSI (Virtual Switch Instance)' on page 46.

Static Address > General Setup

This page configures the setup of a static address interface.

Protocol

This parameter allows changing the Protocol for this logical interface. If you want to switch protocols, select the desired one from the drop down list, then click the 'Switch protocol' button when prompted with 'Really switch protocol?'. The default setting is Static Address.

Option	Function
Static Address	Allows assignment of one or more IPv4 and/or IPv6 static addresses, along with manual configuration of default gateway.
DHCP Client	Allows automatic configuration of IPv4 address, netmask, gateway and DNS servers through the DHCP protocol.
DHCPv6 Client	Allows automatic configuration of IPv6 from any combination of stateless DHCPv6, stateful DHCPv6, DHCPv6-PD and SLAAC.

IPv4 Address

When the Protocol is set to 'Static Address' this sets the static IP Address of the Aprisa LTE 5G (Management and Ethernet ports) assigned by your site network administrator using the standard format xxx.xxx.xxx.xxx. This IP address is used both in Bridge mode and in Router mode. The default IP address is 192.168.4.1.

IPv4 netmask

Set the Subnet Mask of the Aprisa LTE 5G (Management and Ethernet ports) using the standard format xxx.xxx.xxx.xxx. The default subnet mask is 255.255.255.0.

IPv4 gateway

Set the Gateway address of the Aprisa LTE 5G, if required, using the standard format xxx.xxx.xxx.

A default gateway is the node on the network that traffic is directed to when an IP address does not match any other routes in the routing table. It can be the IP address of the router or PC connected to the Aprisa LTE 5G. The default Gateway is 0.0.0.0.

Use customer DNS servers

This parameter is only present for a 'static' interface configuration and specifies any DNS servers available on this interface. This is the same as the settings in windows networking.

IPv6 assignment length

This parameter is only present for a 'static' interface configuration. Specifies the delegated prefix length for this interface.

IPv6 assignment hint
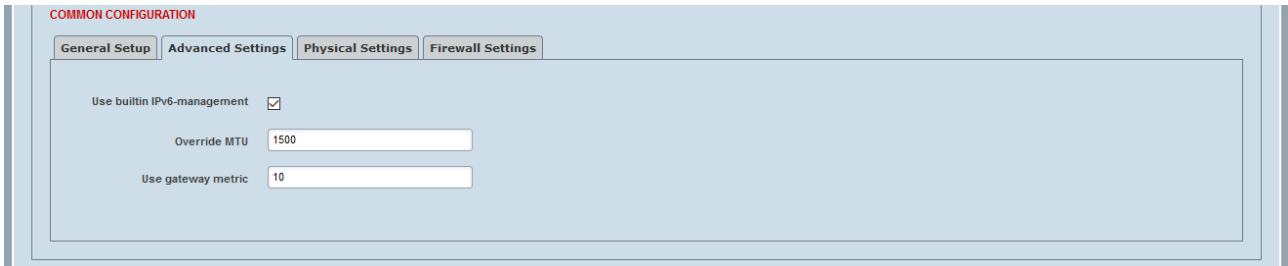
This parameter is only present for a 'static' interface configuration. Specifies a sub-prefix to use e.g. if assignment length is 64, and hint is 1234, will assign downstream prefixes of form xxx:1234::/6.

IPv6 assignment suffix

This parameter is what is applied to the delegated upstream prefix to form the local IP address i.e. for delegated prefix xx:yy::, and suffix of ::1234, you would end up with IP address of xx:yy::1234.

Static Address > Advanced Settings

This page configures the advanced settings of a static address interface.

Use builtin IPv6-management

This parameter sets if IPv6 address ranges allocated to this interface will be delegated to other downstream facing interfaces. Usually relevant to ports using DHCPv6 protocol, although can sometimes apply in other unusual topologies.

Override MTU
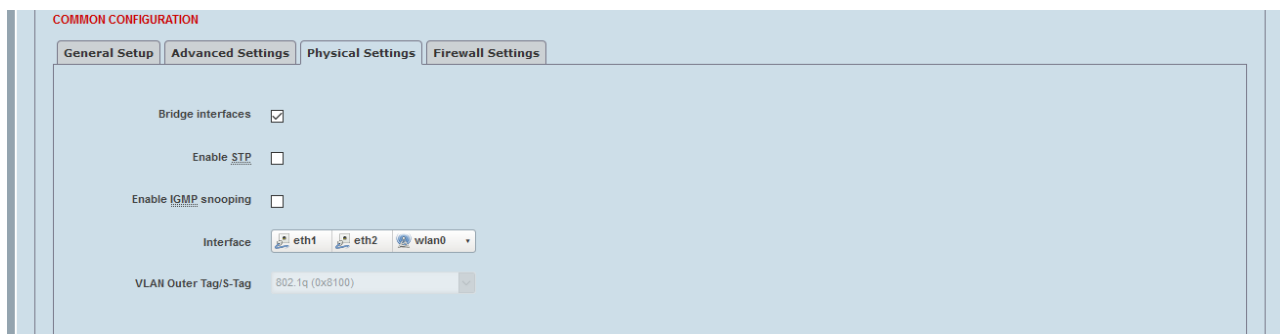
This parameter sets the MTU (Maximum Transmission Unit) largest possible size of a data packet between 0 and 1500. The default setting is 1500.

Use gateway metric

Any gateways on this interface, either statically assigned or automatically discovered (e.g. through DHCP) will be assigned this metric when added to the routing table. The default setting is 10.

Static Address > Physical Settings

This page configures the physical settings of a static address interface.

VLAN outer Tag/S-Tag

This parameter allows setting the use of a single VLAN (C-VLAN) or double VLAN (S-VLAN) for this interface.

Option	Function
802.1q (0x8100)	Allows setting of single VLAN (C-VLAN) on this interface. This C-VLAN is set with EtherType of 0x8100 according to IEEE 802.1Q standard.
802.1ad (0x8100)	Allows setting of double VLANs with outer VLAN as S-VLAN (where inner VLAN is C-VLAN) on this interface. This S-VLAN is set with EtherType of 0x88A8 according to IEEE 802.1ad which part of 802.1Q-2018 standard.

Bridge interfaces

When disabled, the logical interface covers only a single physical interface. When enabled, the user may choose to bridge two or more interfaces together. A bridge switches packets between the ports in the bridge based on L2 (ethernet) addresses, ignoring the L3 (IP) addresses. The IP addresses are used for routing only for packets between logical interfaces.

By default, the LAN is a bridge of ETH1 and ETH2 ports.

If the user wishes to include the SFP1 port (default as WAN interface) in the LAN bridge, the WAN interface must be deleted first, and then add the SFP1 port to the LAN bridge.

If the user wishes to change the ETH1 and ETH2 default LAN bridge interface to Router port (each with its own IP/subnet), the LAN is changed to not bridged first (selecting only ETH1), and then create another logical interface and attach ETH2, where now each port is mapped to its own logical interface.

Enable STP

Only for bridged interfaces using Spanning Tree Protocol. This is designed to prevent loops in L2 networks. Enable this protocol if there is any chance of a loop. If connecting to narrow band links (such as Aprisa SR+) it is often advisable to disable the STP protocol.

Enable IGMP snooping
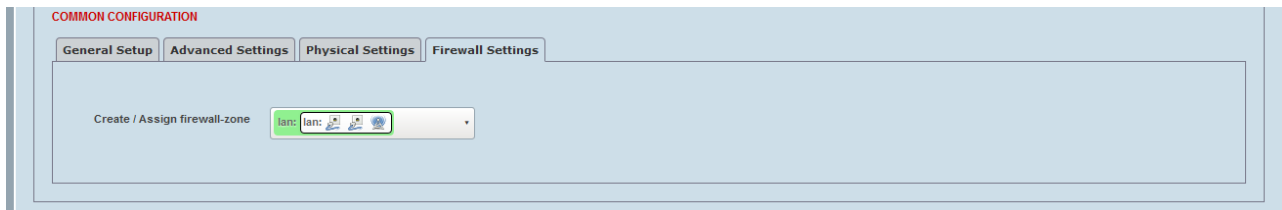
Only for bridged interfaces. When enabled, the bridge can determine what ports to deliver multicast packets to by listening to the IGMP (Internet Group Management Protocol) packets. When disabled, multicast packets are sent to all ports in the same way as broadcast packets. This helps to reduce traffic going to links not involved in the multicast conversation.

Interface

Select the physical interface (e.g. ETH1, ETH2 or SFP) that this logical interface covers. If 'Bridge interfaces' is selected, then you may select multiple.

Static Address > Firewall Settings

This page configures the firewall settings of a static address interface.

Create / Assign firewall zone

Choose the firewall zone you want to assign to the interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

Static Address DHCP Server > General Setup

This page configures the DHCP general setup.

DHCP SERVER

| General Setup | IPv4 Settings | IPv6 Settings |

Lease time   12h

Back to Overview   Save   Cancel
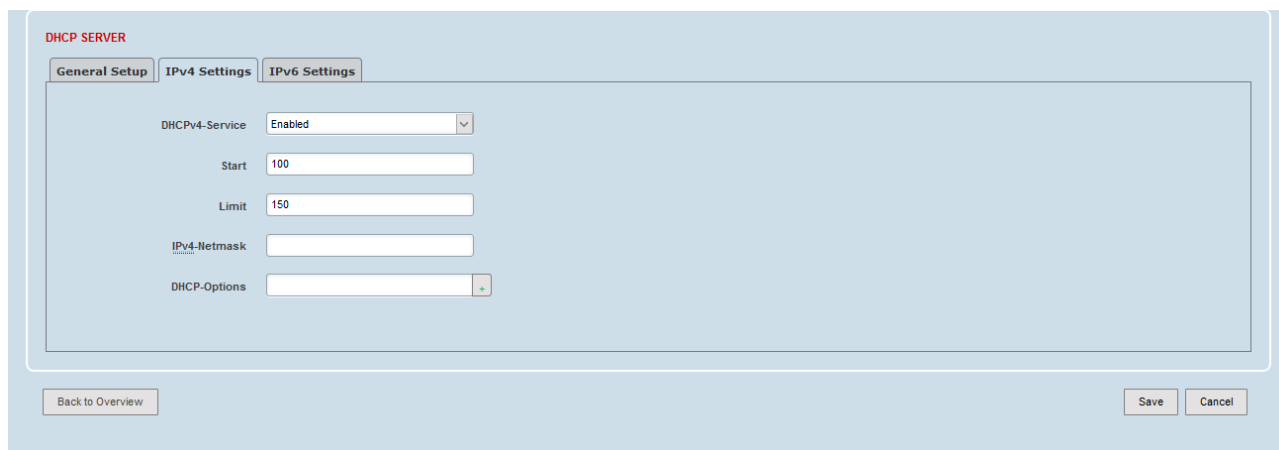
Lease time

This parameter sets duration of an IP lease. Leased out addresses will expire after the amount of time specified in this field and the device that was using the lease will have to request a new DHCP lease.

The lease time can be set in hours (h) or minutes (m). The minimal amount of time that can be specified is 2 minutes. The default value is 12h.

Static Address DHCP Server > IPv4 Settings

This page configures the DHCP Server IPv4 settings.

IPv4-Service

This parameter sets enables or disables DHCP Server on this interface.

Start

This parameter sets the last digit of the starting IP address values to assign. If the Start value is set to 100, and assuming default IP address of 192.168.4.1, then the DHCP server will only lease out addresses starting from 192.168.4.100. The default value is 100.

Limit

This parameter sets the number of addresses the DHCP server can lease out. Continuing from the above example: if the start address is 192.168.4.100 and the server can lease out 150 (default limit value), available addresses will be from 192.168.4.100 to 192.168.4.249. The default value is 150.

IPv4-Netmask
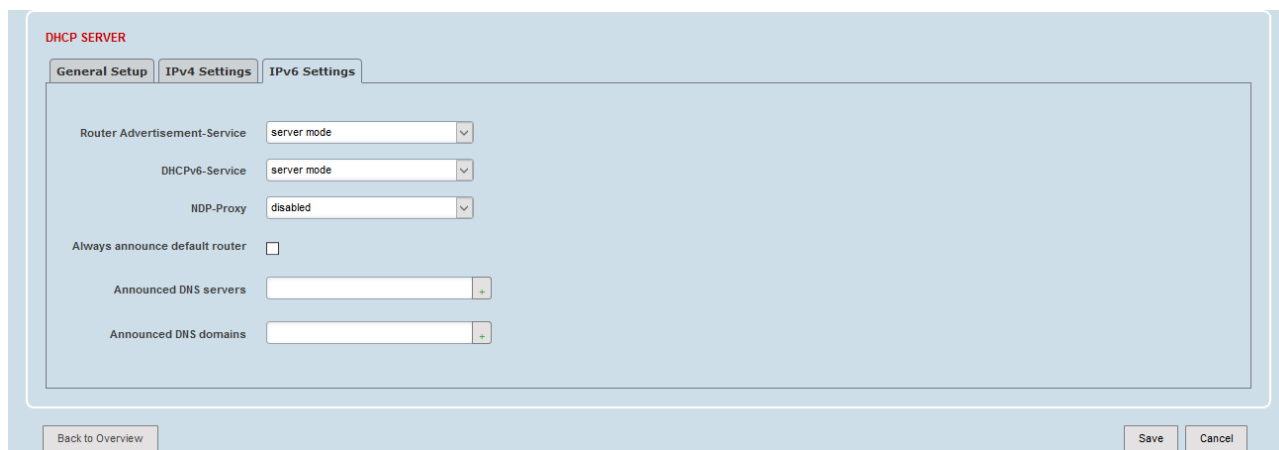
This parameter overrides the LAN netmask sent to DHCP clients. The default value is 255.255.255.0.

DHCP-Options

This parameter allows additional options to be sent by the DHCP server to clients. For example, with '26,1470' or 'option:mtu, 1470' you can inform clients of the specified MTU value.

Static Address DHCP Server > IPv6 Settings

This page configures the DHCP Server IPv6 settings.

Router Advertisement-Service

This parameter specifies how IPv6 router advertisement (RA) packets should be generated on this interface.

Action	Function
Disabled	No Router Advertisement packets
Server	Router Advertisement packets are generated
Relay	Router Advertisement packets are relayed from upstream interface
Hybrid	Server/relay mode chosen automatically

DHCPv6 Service

This parameter choses if how DHCPv6 operates on this interface. Options are same as for Router Advertisement packets.

NDP Proxy

This parameter when in relay mode, acts as a proxy for Neighbour Discovery (ND) packets. This is generally required when DHCPv6 or Router Advertisement acting as a relay. When in hybrid mode, chooses when to proxy automatically.

Always announce default router

This parameter selects this device is advertised as a default route through Router Advertisement packets, even if this device does not have its own default route.

Announced DNS servers
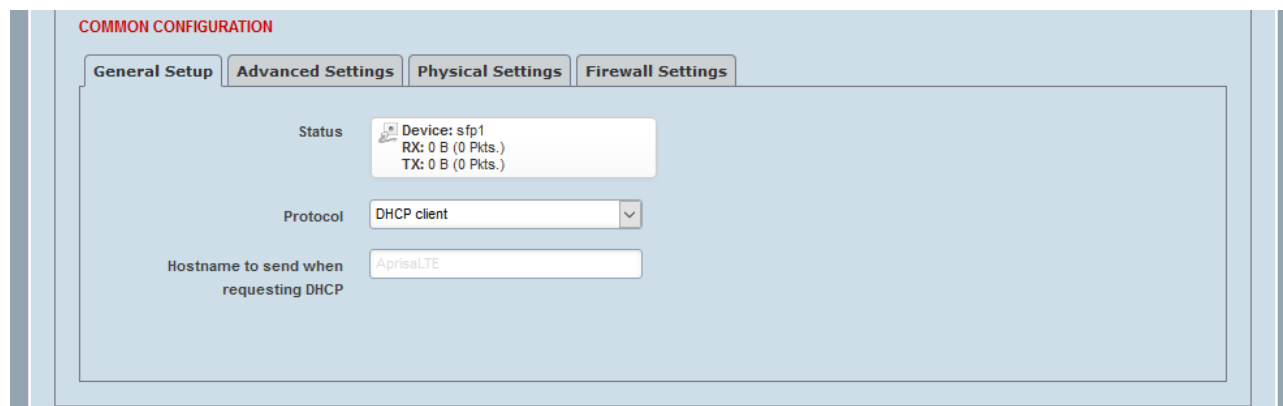
This parameter indicates the DNS server addresses that are sent in Router Advertisement and DHCPv6 messages

Announced DNS domains

This parameter indicates the DNS domains to announce in Router Advertisement and DHCPv6 messages. Can be appended by clients to a bare domain name to form a FQDN (fully qualified domain name).

DHCP Client > General Setup

This page configures the setup of a DHCP Client interface.

Protocol

This parameter allows changing the Protocol for this logical interface. If you want to switch protocols, select the desired one from the drop-down list, then click the 'Switch protocol' button when prompted with 'Really switch protocol?'. The default setting is DHCP Client.
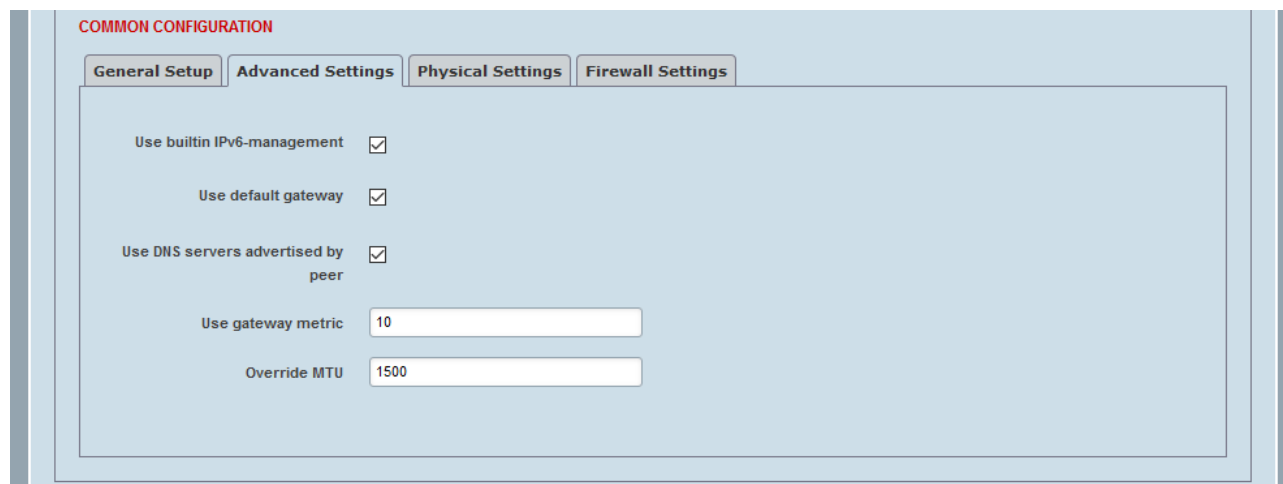
Option	Function
Static Address	Allows assignment of one or more IPv4 and/or IPv6 static addresses, along with manual configuration of default gateway.
DHCP Client	Allows automatic configuration of IPv4 address, netmask, gateway and DNS servers through the DHCP protocol.
DHCPv6 Client	Allows automatic configuration of IPv6 from any combination of stateless DHCPv6, stateful DHCPv6, DHCPv6-PD and SLAAC.

Hostname to send when requesting DHCP

If it is blank (default) then the hostname set in Terminal > Device > Hostname will be used.

DHCP Client > Advanced Settings

This page configures the advanced settings of a DHCP Client interface.

Use builtin IPv6-management

This parameter sets if IPv6 address ranges allocated to this interface will be delegated to other downstream facing interfaces. Usually relevant to ports using DHCPv6 protocol, although can sometimes apply in other unusual topologies.

Use default gateway

When selected, the default route provided by the DHCP server will be added to the routing table.

Use DNS servers advertised by peer

If this parameter is selected, the DNS server advertised by the DHCP server is used.

Use gateway metric
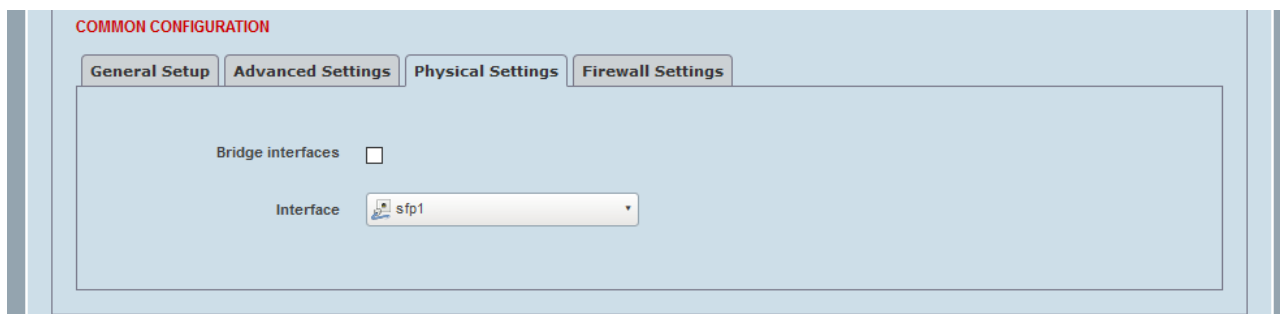
Any gateways on this interface, either statically assigned or automatically discovered (e.g. through DHCP) will be assigned this metric when added to the routing table. The default setting is 10.

Override MTU

This parameter sets the MTU (Maximum Transmission Unit) largest possible size of a data packet between 0 and 1500. The default setting is 1500.

DHCP Client > Physical Settings

This page configures the physical settings of a DHCP Client interface.

Bridge interfaces

When disabled, the logical interface covers only a single physical interface. When enabled, the user may choose to bridge two or more interfaces together. A bridge switches packets between the ports in the bridge based on L2 (ethernet) addresses, ignoring the L3 (IP) addresses. The IP addresses are used for routing only for packets between logical interfaces.

Interface

Select the physical interface (e.g. ETH1, ETH2 or SFP) that this logical interface covers. If 'Bridge interfaces' is selected, then you may select multiple.

Enable STP

Only for bridged interfaces using Spanning Tree Protocol. This is designed to prevent loops in L2 networks. Enable this protocol if there is any chance of a loop. If connecting to narrow band links (such as Aprisa SR+) it is often advisable to disable the STP protocol.

Enable IGMP snooping

Only for bridged interfaces. When enabled, the bridge can determine what ports to deliver multicast packets to by listening to the IGMP (Internet Group Management Protocol) packets. When disabled, multicast packets are sent to all ports in the same way as broadcast packets. This helps to reduce traffic going to links not involved in the multicast conversation.

DHCP Client > Firewall Settings

This page configures the firewall settings of a DHCP Client interface.
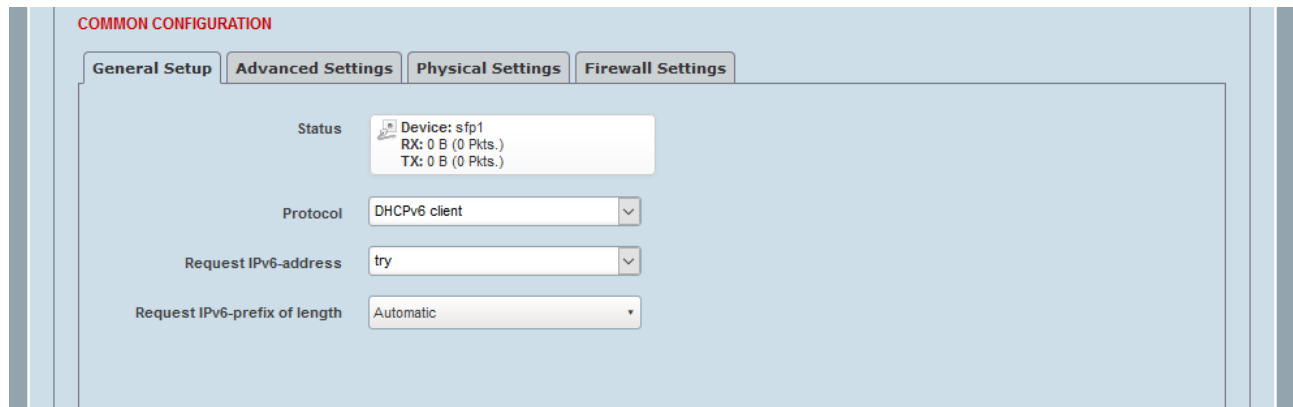
Create / Assign firewall zone

Choose the firewall zone you want to assign to the interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

DHCPv6 Client > General Setup

This page configures the setup of a DHCPv6 Client interface.

Protocol

This parameter allows changing the Protocol for this logical interface. If you want to switch protocols, select the desired one from the drop-down list, then click the 'Switch protocol' button when prompted with 'Really switch protocol?'. The default setting is DHCPv6 Client.

Option	Function
Static Address	Allows assignment of one or more IPv4 and/or IPv6 static addresses, along with manual configuration of default gateway.
DHCP Client	Allows automatic configuration of IPv4 address, netmask, gateway and DNS servers through the DHCP protocol.
DHCPv6 Client	Allows automatic configuration of IPv6 from any combination of stateless DHCPv6, stateful DHCPv6, DHCPv6-PD and SLAAC.

Request IPv6 Address

This parameter specifies how prefix allocation is requested.

Option	Function
Try	Ask server for prefix, but accept whatever is given
Force	Keep requesting if server gives smaller prefix
Disabled	Don't specify prefix length in request
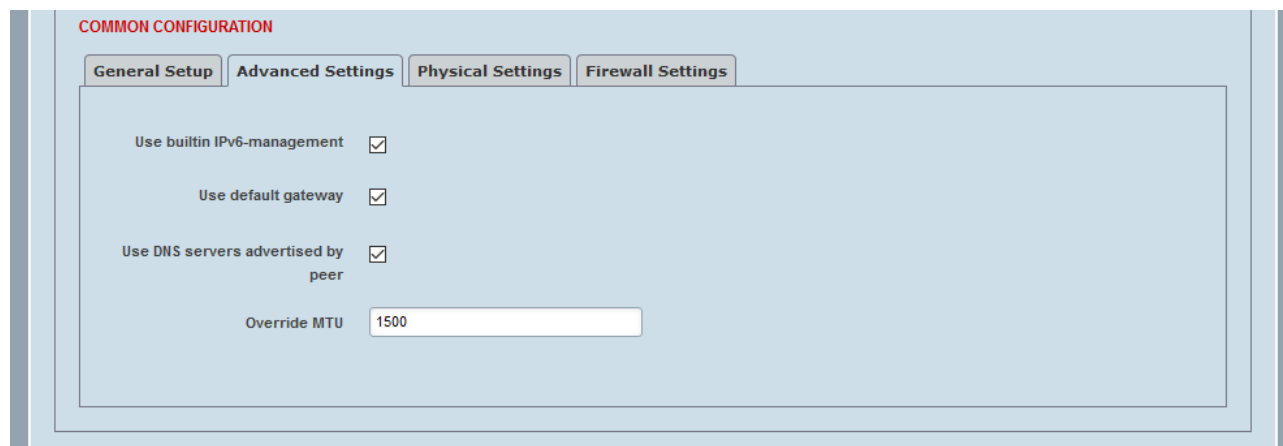
Request IPv6 prefix of length

This parameter Specifies the prefix length to request. Integer between 1 and 128.

Action	Function
Integer between 1 and 128	Request the specified prefix length. Typical values are 56, 60 or 64.
Automatic	The Aprisa LTE 5G will determine an appropriate prefix to request.
Disabled	No prefix will be requested, and only a single IPv6 will be allocated to this device (meaning no delegation can occur for IPv6 routing from other interfaces).

DHCPv6 Client > Advanced Settings

This page configures the advanced settings of a DHCPv6 Client interface.

Use builtin IPv6-management

This parameter sets if IPv6 address ranges allocated to this interface will be delegated to other downstream facing interfaces. Usually relevant to ports using DHCPv6 protocol, although can sometimes apply in other unusual topologies.

Use default gateway

If this parameter is active, a default gateway discovered with RA protocol will be added to the routing table.

Use DNS servers advertised by peer
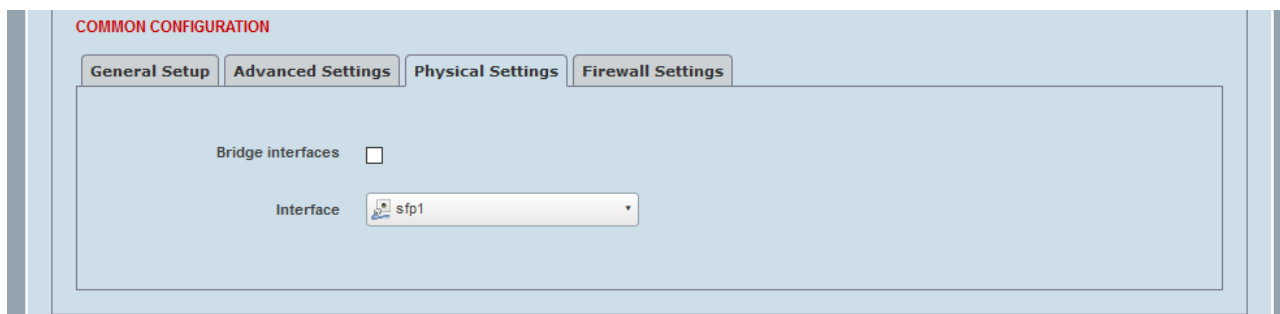
If this parameter is active, the DNS server advertised by the DHCPv6 server is used.

Override MTU

This parameter sets the MTU (Maximum Transmission Unit) largest possible size of a data packet between 0 and 1500. The default setting is 1500.

DHCPv6 Client > Physical Settings

This page configures the physical settings of a DHCPv6 Client interface.

Bridge interfaces

When disabled, the logical interface covers only a single physical interface. When enabled, the user may choose to bridge two or more interfaces together. A bridge switches packets between the ports in the bridge based on L2 (ethernet) addresses, ignoring the L3 (IP) addresses. The IP addresses are used for routing only for packets between logical interfaces.

Interface

Select the physical interface (e.g. ETH1, ETH2 or SFP) that this logical interface covers. If 'Bridge interfaces' is selected, then you may select multiple.

Enable STP

Only for bridged interfaces using Spanning Tree Protocol. This is designed to prevent loops in L2 networks. Enable this protocol if there is any chance of a loop. If connecting to narrow band links (such as Aprisa SR+) it is often advisable to disable the STP protocol.

Enable IGMP snooping

Only for bridged interfaces. When enabled, the bridge can determine what ports to deliver multicast packets to by listening to the IGMP (Internet Group Management Protocol) packets. When disabled, multicast packets are sent to all ports in the same way as broadcast packets. This helps to reduce traffic going to links not involved in the multicast conversation.

DHCPv6 Client > Firewall Settings

This page configures the firewall settings of a DHCPv6 Client interface.

Create / Assign firewall zone

Choose the firewall zone you want to assign to the interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

PPP > General Setup

This page configures the setup of a PPP interface.

Protocol

This parameter allows changing the Protocol for this logical interface. If you want to switch protocols, select the desired one from the drop down list, then click the 'Switch protocol' button when prompted with 'Really switch protocol?'. The default setting is PPP.

Option	Function
Static Address	Allows assignment of one or more IPv4 and/or IPv6 static addresses, along with manual configuration of default gateway.
DHCP Client	Allows automatic configuration of IPv4 address, netmask, gateway and DNS servers through the DHCP protocol.
DHCPv6 Client	Allows automatic configuration of IPv6 from any combination of stateless DHCPv6, stateful DHCPv6, DHCPv6-PD and SLAAC.
PPP	Sets the protocol to PPP (Point-to-Point Protocol).

IPv4 Address

Set the IPv4 address for the local-end of the PPP tunnel.

Remote IP Address

Set the IPv4 address for the far-end of the PPP tunnel.

Inbound Auth Enable

If ticked, authentication of remote user is required. When enabled, the username and password provided by the remote system must match one of the ppp secrets. The default is disabled.

User

Sets the username when requesting authentication with the remote system. If not specified, this defaults to the global hostname setting.

Host Name

Sets the hostname to use when performing authentication with the remote system. If not specified, this defaults to the global hostname setting.

Inbound Auth Required Protocol

When an option is specified, the remote system will be forced to provide authentication using the specified protocol.

Option	Function
chap	Force CHAP (Challenge Handshake Authentication Protocol).
mschap	Force MS-CHAP (Microsoft Challenge Handshake Authentication Protocol).
mschapv2	Force MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol, Version 2).
eap	Force EAP protocol (Extensible Authentication Protocol).
pap	Force PAP (Password Authentication Protocol).

Note that this only affects the auth protocol used for receiving credentials FROM the remote system. The protocol used for sending credentials TO the remote system may still be a different protocol than specified.

Outbound Auth Refused Protocol

When an option is specified, this host will refuse to authenticate using the specified protocol.

Option	Function
chap	Refuse CHAP (Challenge Handshake Authentication Protocol).
mschap	Refuse MS-CHAP (Microsoft Challenge Handshake Authentication Protocol).
mschapv2	Refuse MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol, Version 2).
eap	Refuse EAP protocol (Extensible Authentication Protocol).
pap	Refuse PAP (Password Authentication Protocol).

Note that this only affects the auth protocol used for sending credentials TO the remote to the local system. The protocol used for receiving credentials FROM the remote system may still be the protocol specified here. By default, all authentication protocols are accepted except for pap.

User Peer DNS

If ticked, DNS servers will be requested from the peer.

Provide DNS

If ticked, the DNS server is advertised to the peer.

Default Gateway

Sets if a default route is automatically installed via the peer-ip address on the PPP interface when it is active.

IPv6 Enable

If ticked, IPv6 LL address negotiation through PPP is enabled.

MPPE Enable

If ticked, the MPPE (Microsoft Point to Point Encryption) negotiation is enabled. The default is disabled.

MPPE Require

If ticked, MPPE encryption is forced.

MPPE Stateless

If ticked, the MPPE stateless mode is enabled. The default is disabled.

MPPE Disable Keysize

Sets the length of MPPE keys to refuse 40 bits, 56 bits, 128 bits.

Connection Script

Sets the method used to negotiate the use of PPP on this link.

Option	Function
None	
WindowsNT Client	This sends the 'client' string, and then waits for 'clientserver' before starting the PPP protocol
WindowsNT Server	This waits for the 'client' string, and then sends 'clientserver' in response before starting the PPP protocol
Custom Script	Specify a custom dialing script. The script uses the syntax of the linux chat tool.

Compression Types Allowed

Sets the type of compression.

Option	Function
BSD	Berkeley Software Distribution compression
CCP	CCP allows the devices decide how they will compress data
Deflate	Deflate is a lossless data compression file format that uses a combination of LZ77 and Huffman coding
Van Jacobsen	Reduces the normal 40 byte TCP/IP packet headers down to 3–4 bytes for the average case

Note that all protocols are enabled by default. The actual compression (if any) that is used depends on the results of negotiations with the peer using the IPCP and CCP (if enabled) protocols.

Keepalive Fail Count

Sets the LCP failcount. If failcount echos do not get a response, then the PPP session is closed.

Keepalive Interval
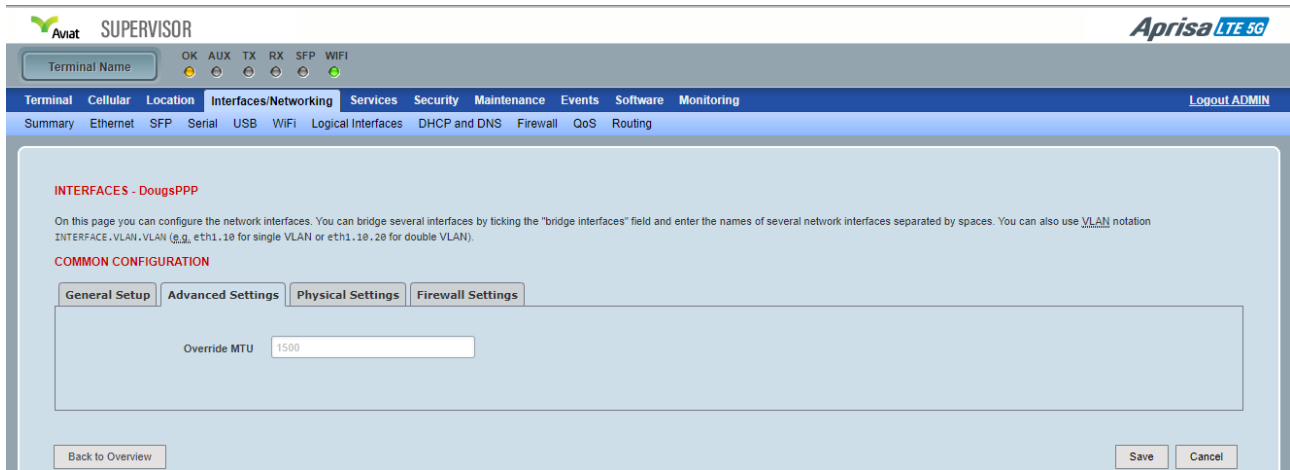
Sets the LCP echo interval in seconds. The PPP connection is checked using LCP echos.

Keepalive Adaptive Mode

If ticked, echoes will only be sent when there is no other traffic flowing.

PPP > Advanced Settings

This page configures the advanced settings of a PPP interface.

Override MTU

This parameter sets the MTU (Maximum Transmission Unit) largest possible size of a data packet between 0 and 1500. The default setting is 1500.

PPP > Physical Settings

This page configures the physical settings of a PPP interface.

Interface

This parameter sets the serial port to use. Select the physical interface (e.g. line1) that this logical interface covers. For PPP interfaces this must be an asynchronous serial port.

PPP > Firewall Settings

This page configures the firewall settings of a PPP interface.

Create / Assign Firewall Zone

Choose the firewall zone you want to assign to the interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

Interfaces/Networking > DHCP and DNS

DHCP and DNS > General Settings

This page provides setup of the DHCP and DNS servers.

Authoritative

When enabled, this parameter relaxes strict RFC behaviour to speed up clients obtaining leases but should only be enabled if there is no other DHCP server.

Local domain

This parameter gets appended to partial domain names when attempting to resolve FQDN. Defaults to lan. With default hostname of aprisalte, this means device can be resolved through either 'aprisalte' or 'aprisalte.lan'.

DNS forwardings

This is a list of DNS servers to forward requests to, optionally specifying the domains that are forwarded. '4.4.4.4' would forward all requests to 4.4.4.4, but '/aviatnetworks.com/4.4.4.4' would forward only requests for aviatnetworks.com to the 4.4.4.4 server. Note that any DNS servers obtained through DHCP, DHCPv6 and IPv6-RA will automatically be used.

Max DHCP leases

Specifies the number of leases the DHCP server will allocate to clients simultaneously. The default value is unlimited.

Static leases

Hostname: sets the hostname to give to the static entry.

MAC address

This parameter specifies the MAC address of the device to statically allocate an IP address. A list of detected MAC addresses is provided for convenience, but any valid 48-bit MAC address can be specified.

IPv4 address

This parameter is the address to allocate to the MAC address.

Lease time

This parameter is the lease time that is given in the DHCP response to this client

DUID

This parameter is the IPv6 DUID of this host

IPv6 suffix
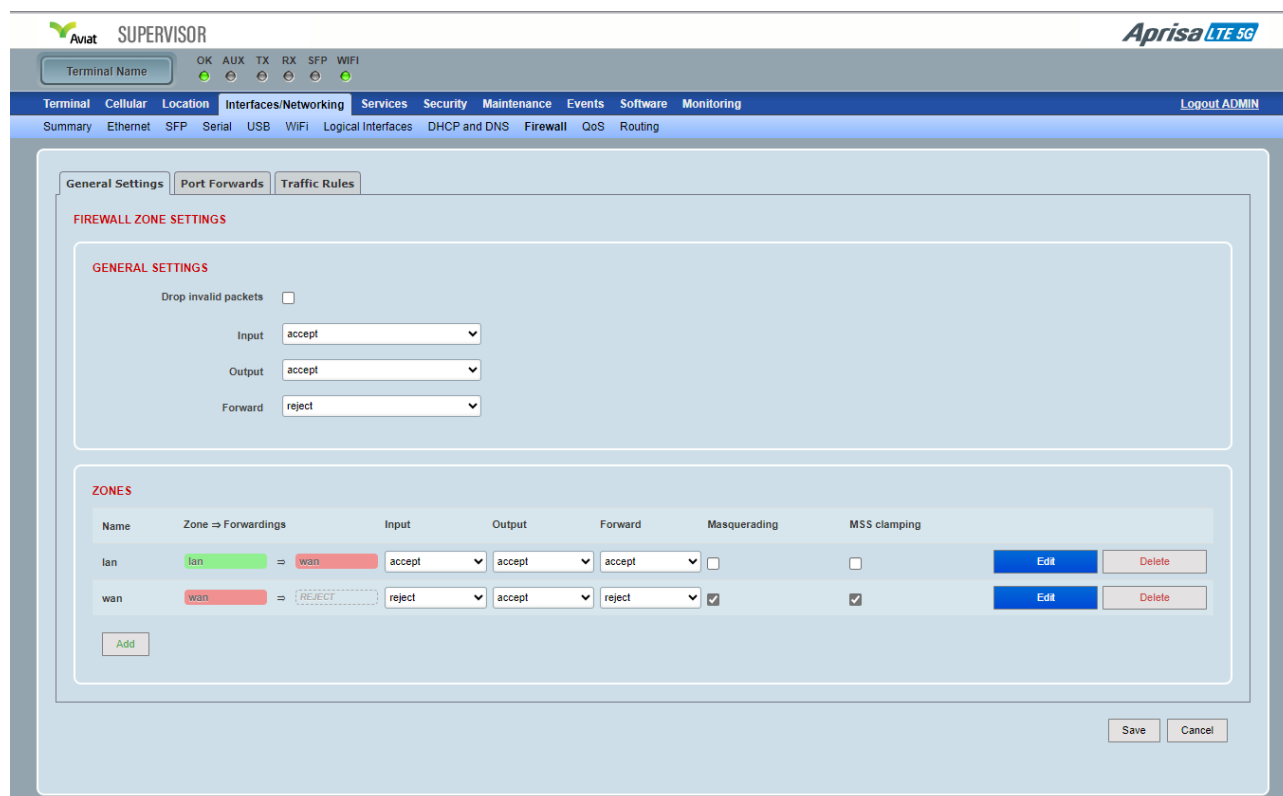
This parameter is the IPv6 suffix to append to the IPv6 prefixes when allocating IPv6 addresses

Interfaces/Networking > Firewall

This page provides setup of the firewall. A firewall is a network security feature that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewall > General Settings

This page provides setup of the firewall main policies and zones policies over your network interfaces to control network traffic flow.

This section defines the main policies of the firewall function. It matches packet against all defined firewall chain rules. If no rule matches, an Action [Accept, Drop, and Reject] is performed.

Drop invalid packets

If enabled, packets that are determined to be invalid will be dropped.

Input, Output, Forward

These parameters define the firewall chain and their associated action options.
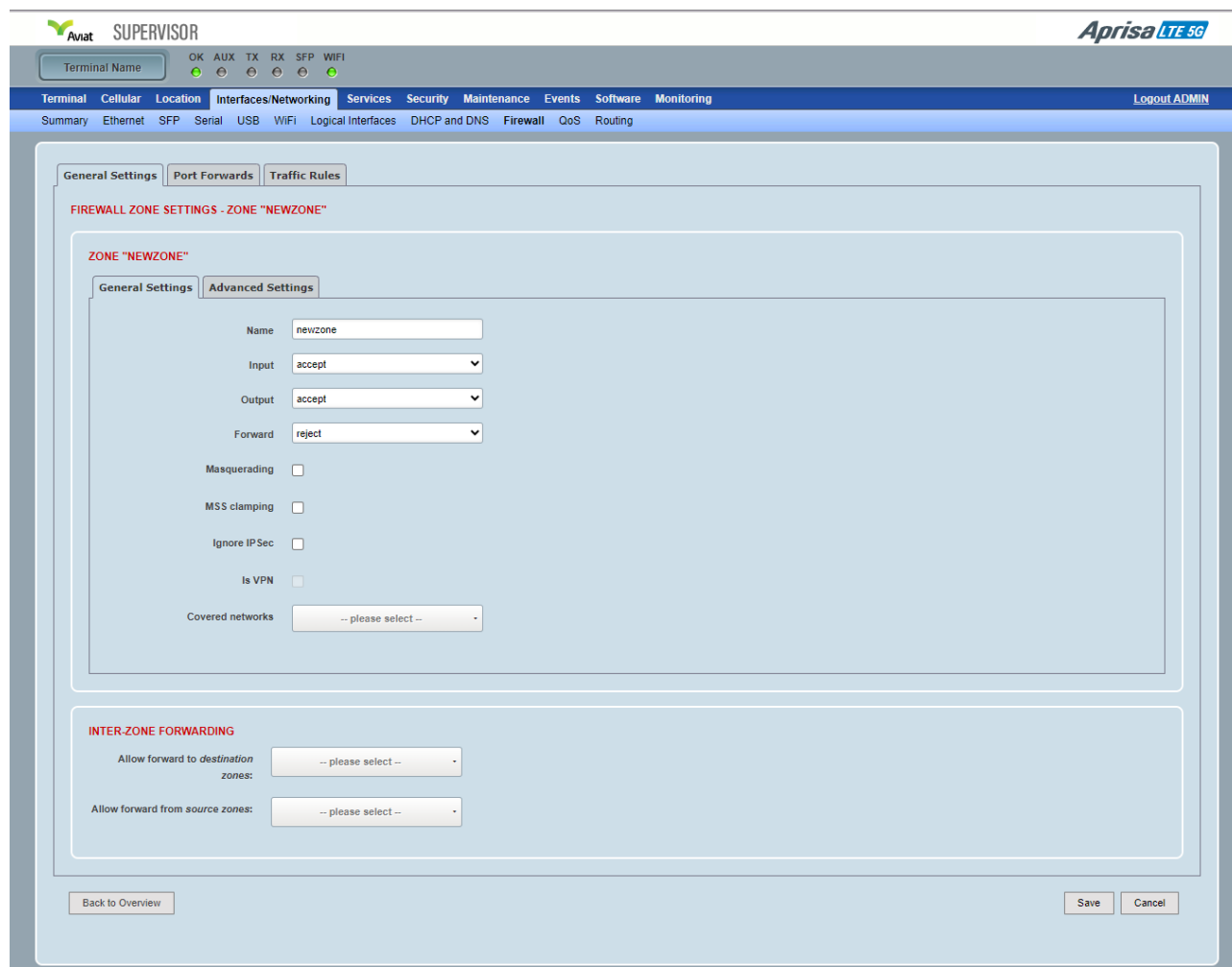
Firewall chain	Default Action	Function
Input	Accept	Perform "Action" (see below) on packets pass input firewall chain
Output	Accept	Perform "Action" on packets pass output firewall chain
Forward	Reject	Perform "Action" on packets pass forwarding firewall chain

The Action parameters define the operation related to the firewall chain.

Action	Function
Accept	The packet gets to continue to the next firewall chain.
Drop	The packet is dropped.
Reject	The packet is dropped and an ICMP packet containing a message of rejection is sent to the source of the dropped packet.

Firewall > General Settings > Add

This page provides setup of the firewall zones.

This section defines network/port zones and their exposer to other zones. Network/port zones entities are defined in 'Interfaces/Networking > Logical Interfaces' per port, network, or group of ports.

Zone ⇒ Forwarding (Inter-Zone Forwarding)

Control the forwarding policies between the specified source and destination zones. The forwarding rule is unidirectional.

Input, Output, Forward

Input / output define the traffic policies in the zone and forward defines the traffic policy between different networks within the zone

Tunnel

When you create a VPN tunnel, a corresponding firewall zone is automatically created. This field shows the tunnel assigned to the firewall zone. This field is only present in the VPN_FW_XXX zones which are automatically created when you add an IPsec tunnel.

Masquerading

If enabled, NAT function is applied

MSS clamping

Reduce the maximum segment size (MSS), that a device can receive in a single TCP segment/MTU (not including TCP/IP header)

Ignore IPsec

When set, packets that are part of a VPN zone are ignored for this zone. Rules for the VPN zone itself will instead apply to the received packet.

Is VPN

Indicates that the firewall zone is to apply to inner traffic going through an IPsec tunnel as opposed to the traffic directly on and interface. When set, the covered networks option is replaced with a covered subnets option.

Covered Networks
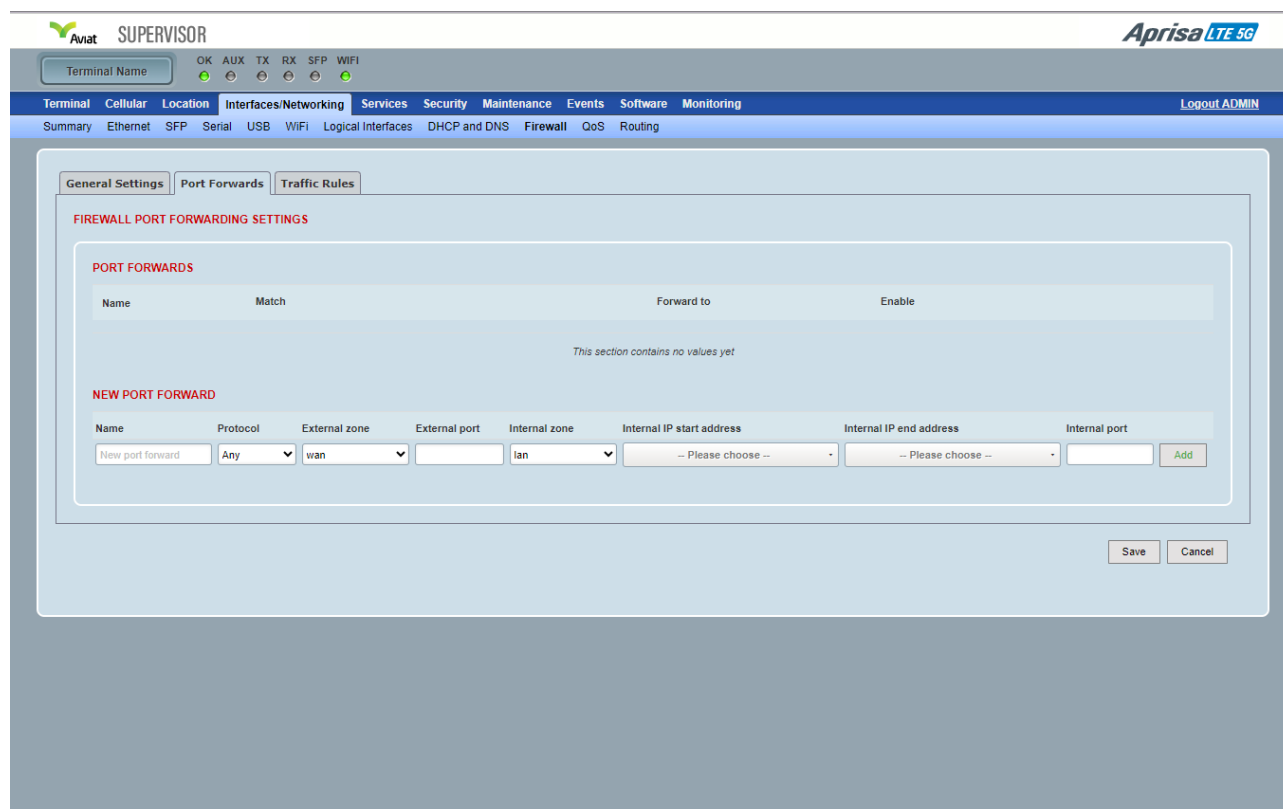
This allows selections of which interfaces this firewall zones rules are applied to. This is not used for VPN tunnels.

Covered Subnets

This allows selection of which subnets, specified in CIDR notation (e.g. a.b.c.d/mask) are covered by this firewall zone. This is only used for zones which are applied to VPN tunnels.

Firewall > Port Forwards

This page provides setup of the port forwarding rules which allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Rule is Enabled

Toggles the rule ON or OFF. If unchecked, the rule will not be deleted, but it also will not be loaded into the firewall.

Name

Name of the rule, used purely for easier management purposes.

Protocol

Specifies to which protocols the rule should apply. The default value is TCP+UDP.

Source zone

The source zone from which data packets will redirected from. The default value is wan.

Source MAC address

Matches incoming traffic from these MACs only.

Source IP address

Matches incoming traffic from this IP or range of IPs only.

Source port

Matches incoming traffic originating from the given source port or port range on the client host only. May be specified as a start-end range.

External IP address

Matches incoming traffic directed at the given IP address only.

External port

Matches incoming traffic directed at the given port only. May be specified as a start-end range (e.g. 10000-10010).

Internal zone

Specifies the internal zone where the incoming connection will be redirected to.

Internal IP address

Specifies the internal IP address to which the incoming connection will be redirected to.

Internal port
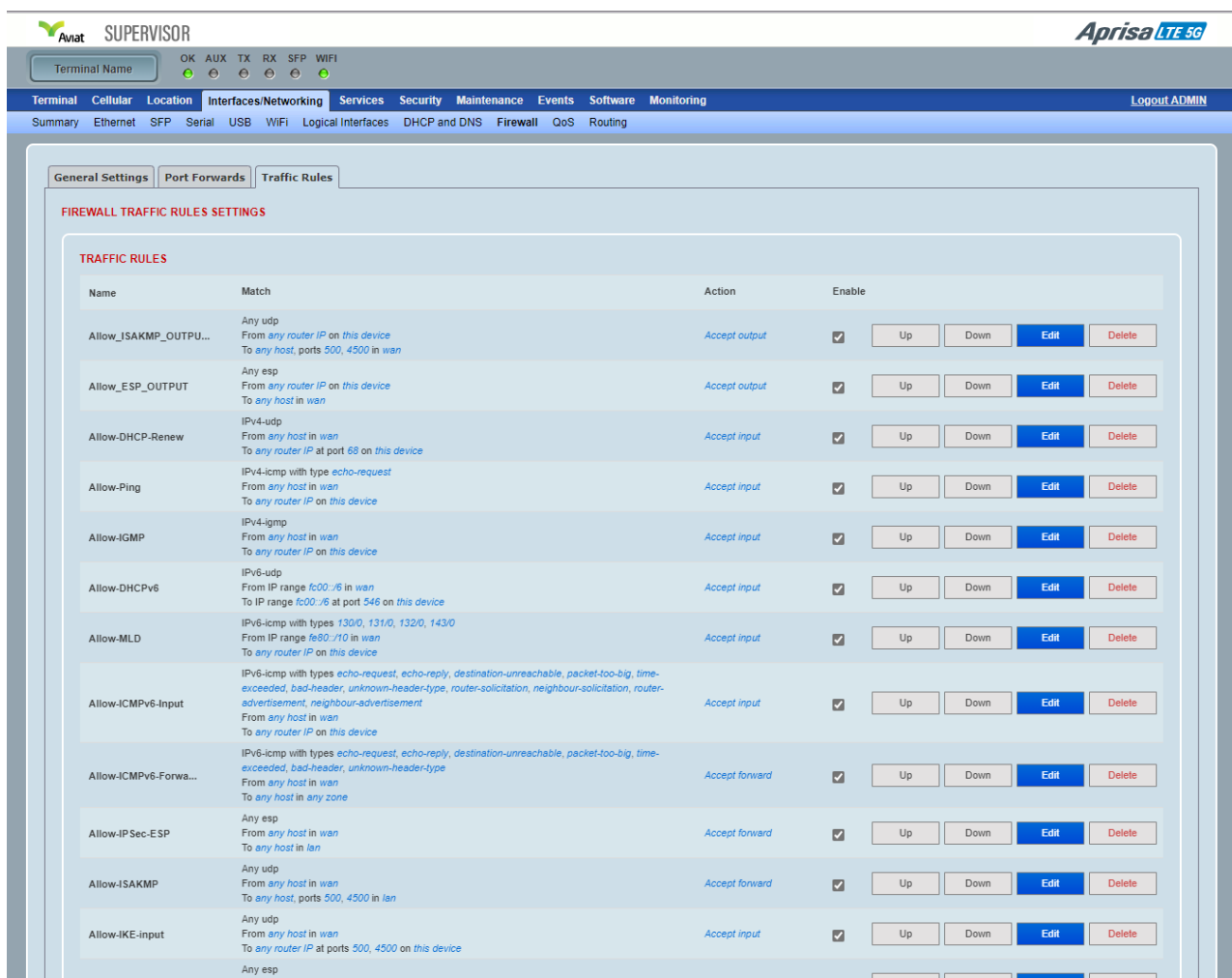
Specifies the internal port to which the incoming connection will be redirected to. May be specified as a range.

Enable NAT loopback

NAT loopback enables connections from your local network on the internal zone to the specified external IP/port to be forwarded to the destination IP/port. When disabled, only connections from the external zone/ip range will be forwarded. The default is no.

Firewall > Traffic Rules

This page provides setup of traffic rules which define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Rule is Enabled

Toggles the rule ON or OFF. If unchecked, the rule will not be deleted, but it also will not be loaded into the firewall.

Name

Name of the rule, used purely for easier management purposes.

Protocol

Type of protocol of incoming packet

Source zone

Packets arriving from the specified source zone will match this rule. The special 'device' zone matches packets that originate from the Aprisa LTE 5G. Any Zone may also be specified. The default value is wan.

Source Address

The source zone from which data packets will redirected from.

Destination Address / Port

Redirect matched traffic to the given IP address and destination port.

Action
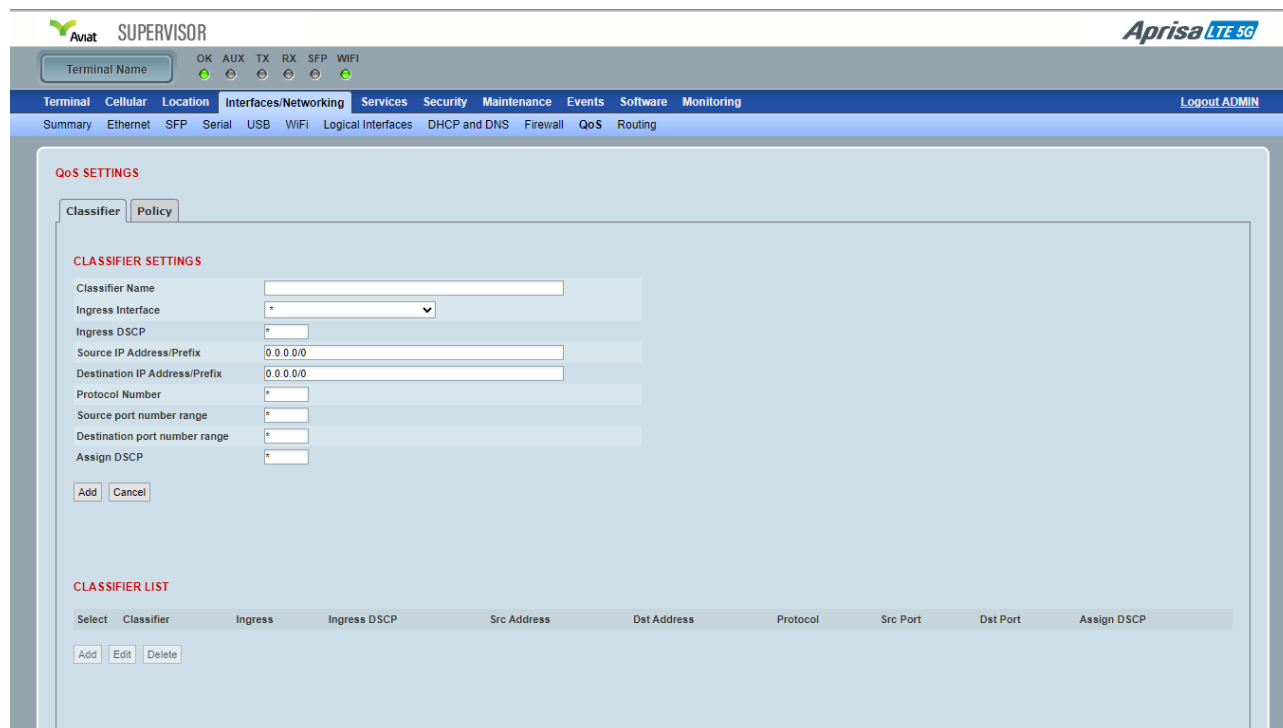
Action to be performed with the packet if it matches the rule.

Interfaces/Networking > QoS

This page provides setup of the Quality of service (QoS). QoS is a feature that lets you give priority to critical traffic, prevent bandwidth hogging, and manage network bottlenecks to prevent packet drops.

QoS > Classifier

This page adds packet classifiers which select packets for QoS management.

Classifier Name

The name of this classifier profile.

Ingress Interface

This parameter sets any interface using * or interface or group of interfaces configured at 'Interfaces/Networking > Logical Interfaces' on page 143 in the selected profile classification rules. For example, LAN, WAN and WAN6 interfaces.

Ingress DSCP

This parameter sets the Differentiated Services (Diffserv) Code Point (DSCP) in the selected profile classification rules. It is a QoS priority value which resides within the IP header (in TOS byte) and can be used to set an IP packet with Diffserv priority. Valid DSCP values are 0 – 63.

Example of commonly used DSCP values:

DSCP (decimal) Value	Meaning	Drop Precedence
46	EF (Expedited Forwarding) (High Priority)	
0	Best Effort	
10	AF11 (Assured Forwarding)	Low
12	AF12	Medium
14	AF13	High
18	AF21	Low
20	AF22	Medium
22	AF23	High
26	AF31	Low
28	AF32	Medium
30	AF33	High
34	AF41	Low
36	AF42	Medium
38	AF43	High
8	CS1 (Class Selector)	
16	CS2	
24	CS3	
32	CS4	
40	CS5	
48	CS6	
56	CS7	

Source and Destination IP Address and prefix

This parameter is only valid when TCP or UDP protocol is matched. It sets the Layer 4 TCP / UDP packet header Source / Destination Port number range field in the selected profile classification rules. Valid range is 1-65535, and setting * define the whole range, i.e. traffic from any source/destination port will meet the criteria.

Following combinations can be used:

- Single port: e.g., 22

- Multiple ports: e.g., 22, 80, 443

- Ranges: e.g., 1000-2000, 3000-4000

- Negations (means not matching this port/ports/port range/combination): e.g., !22

- Combinations: e.g., 80,443,1000-2000

- Negative Combinations (means port must not match any of these) e.g., !80,443,1000-2000

Examples of TCP / UDP Port numbers:

Protocol	TCP / UDP Port # (decimal)
Modbus	502
IEC 60870-5-104	2,404
DNP 3	20,000
SNMP	161
SNMP TRAP	162

Protocol Number

This parameter is IPv4/IPv6 packet header 'Protocol'/'Next Header' field, respectively in the selected profile classification rule. Use value (-1) to ignore this field, or the IP protocol/next header number to match with the following common values able to be set by name. TCP, UDP, ICMP, IGMP, GRE, ESP, AH, EIGRP, OSPF, VRRP, ISIS.

Examples of Protocol/Next header numbers:

IPv4 Protocol / IPv6 Next Header	Protocol value (decimal)
ICMP	1
TCP	6
UDP	17
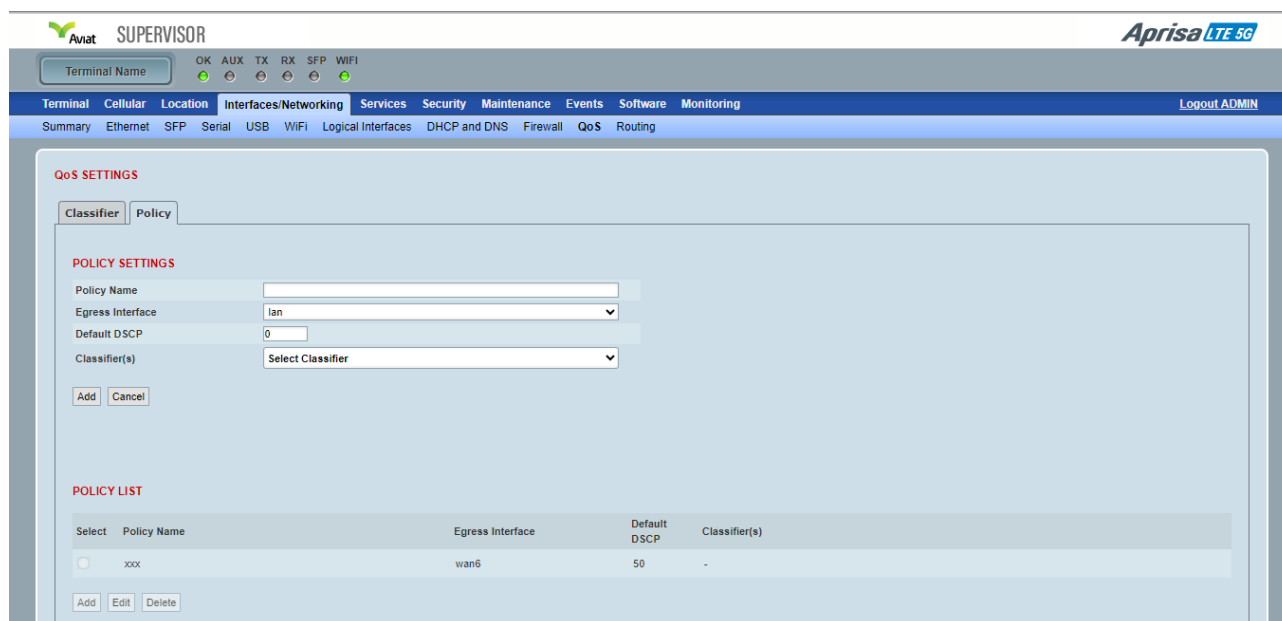
Assigned DSCP

This parameter sets the Differentiated Services (Diffserv) Code Point (DSCP) in the outgoing packet when this profile classification rules match. It is a QoS priority value reside within the IP header (in TOS byte) and can be used to set an IP packet with DIffserv priority.

The default DSCP can be set to -1 for no change or any valid DSCP value 0 – 63. See commonly used DSCP table on the 'ingress DSCP' description.

QoS > Policy

This page provides setup of QoS policies which determine the rules that the policy engine follows per egress interface, deciding which traffic is given priority to the selected egress port.

Policy Name

The defined name of the QoS policy.

Egress Interface

This parameter sets the interface or group of interfaces configured at 'Interfaces/Networking > Logical Interfaces' in the selected profile policy rules. For example, LAN, WAN and WAN6 interfaces. Multiple policy rule can be created, but only a single policy rule can be created per egress interface. Single or multiple classifiers can be assigned to a policy rule which is related to an egress port.

Default DSCP

This parameter assigns the default DSCP to a packet on an egress port when packet does not match any of the classifier/s rules associated with selected profile policy rules. i.e. when a packet matches a classifier rule it will assign to a packet the 'assigned DSCP' value (define in the classifier tab) and in the policy profile the default DSCP will be assigned to a packet if the packet doesn't match to any of the classifier rules associated with the selected profile policy rules.
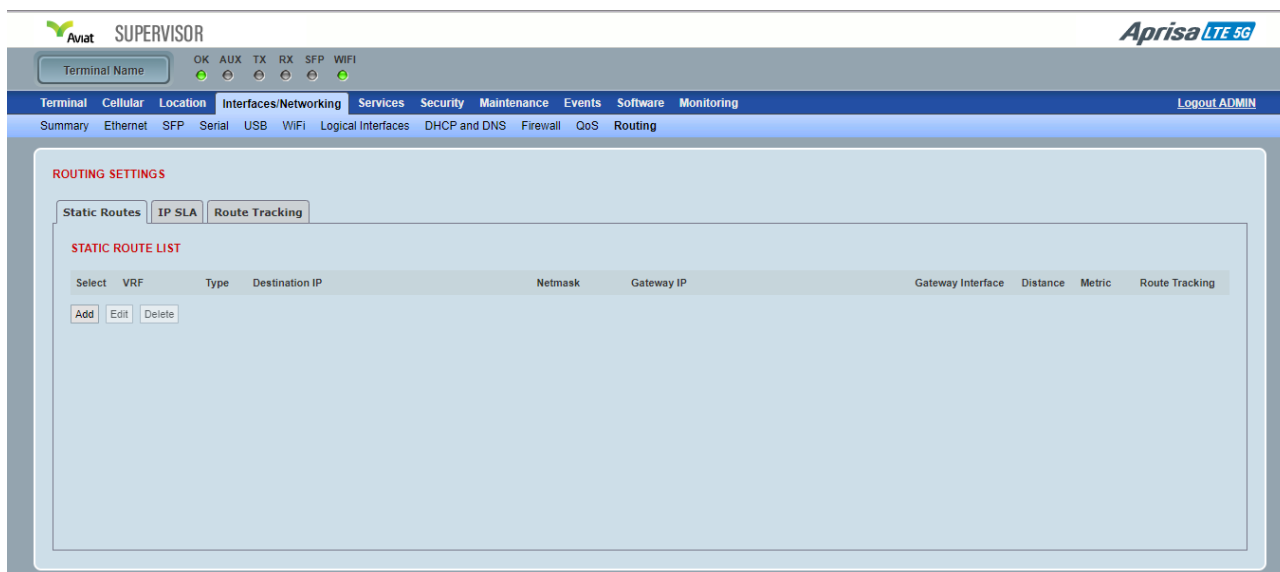
Set * for no change or any valid DSCP value of 0 – 63. See commonly used DSCP table on the 'ingress DSCP description.

Classifier(s)

This parameter sets the classifier/s rule/s with the selected profile policy rules. Single or multiple classifiers can be assigned to a policy rule.

Interfaces/Networking > Routing

This page provides setup of Static Routing.

Controls

The Add button adds a new static route.

The Edit button edits the selected static route.

The Delete button deletes the selected static route.

Routing > Static Routes

This page provides setup of the Static Routes. Routes specify over which interface and gateway a certain host or network can be reached.

ADD STATIC ROUTE

Type

This parameter sets the static route IP protocol type IPv4 or IPv6.

Destination IP

This parameter specifies the destination network IP address.

Destination IP when IPv4

This can be a single IP (such as 192.168.100.100 with netmask of 255.255.255.255), or a network address (such as 192.168.100.0 with netmask of 255.255.255.0) that this route can reach.

Destination IP when IPv6

If the destination IP is a single address, specify it directly (e.g 2402:2380:305:3100::834)

If it is a network address, specify in CIDR notation (e.g. 2402:2380:305:3100::/64).

Netmask (IPv4 only)

A netmask is used to divide an IP address into sub-networks (subnets). Combined, the 'Destination IP' and 'Netmask' values define the exact destination network or IP address to which this route applies. For example, a destination IP/netmask of 192.168.100.0/255.255.255.0 maybe written in CIDR notation as 192.168.100.0/24.

Gateway IP

This parameter specifies the next hop IP address where packets will be forwarded to a router with this IP address when no other route specification in routing table matches the destination IP address of a packet.

Gateway Interface

This parameter sets the default Interface where the specified destination host or network can be accessed, or packets will be forwarded to this interface when no other route specification in the routing table matches the destination IP address of a packet.

Note: Either 'Gateway IP' or 'Gateway Interface' or both can be specified.

Distance

Together with Metric, this parameter represents the priority of the route. Allowed values between 0 and 255.

The routing table will forward the packet based on the following match priority order:

1. Longest prefix match (i.e. if packet destination address is 10.10.10.10 and routing table includes two routes with target IP (a) 10.10.0.0/16 and (b) 10.10.10.0/24 then route (b) with the longest prefix match will be chosen to forward this packet).

2. Administrative distance (AD) or Distance in short – AD/Distance defines the reliability of a dynamic routing protocol, static and directly connected routes. These routes are prioritized in order of most to least reliable with the help of an AD value, where the lowest AD has the highest priority route. AD value range is 0 to 255, where 0 is connected interface, 20 = eBGP, 110 = OSPF, 120 = RIP, and 255 is unreachable route.

    Example: if packet destination address is 10.10.10.10 and routing table includes two routes with {target IP, AD} = {(a) 10.10.10.0/24, 254 and (b) 10.10.10.0/24, 250} then route (b) with the same prefix match, but with the lowest AD will be selected as the best path/route to forward this packet.

3. Metric - router metrics is another value that help the router choose the best route among multiple feasible routes to a destination. The metric value based on information such as path length, bandwidth, load, hop count, path cost, delay that may be used by the different routing protocols. The lowest Metric value has the highest priority route. Metric value range is 0 to 16,777,215.

    Example: if packet destination address is 10.10.10.10 and routing table includes two routes with {target IP, AD, Metric} = {(a) 10.10.10.0/24, 250, 16,000 and (b) 10.10.10.0/24, 250, 1000} then route (b) with the same prefix match, same AD, but with the lowest metric will be selected as the best path/route to forward this packet.

Metric
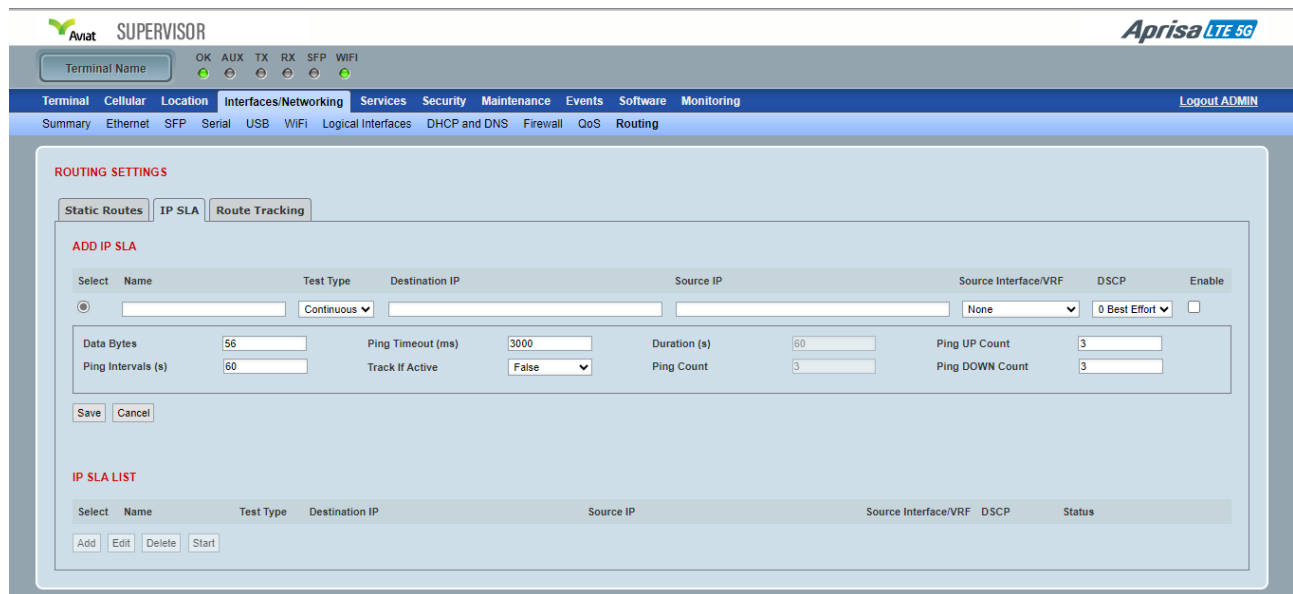
Together with Distance, this parameter represents the priority of the route. Distance is checked first, and if two routes have the same Distance, then the route with the lowest metric will have the highest priority.

Route Tracking

This parameter specifies the user defined name of a tracking object. Tracking objects are a set of alarms that user can select to attach to an IP SLA monitoring profile of the static route, which determine if the static route is healthy or failed. If route tracking fails, the static route will failover to the alternate route.

Routing > IP SLA

This page provides setup of the IP Service Level Agreement.

ADD IP SLA

Name

User defined arbitrary text name for the IP SLA profile. I may contain upper/lower case letters, numbers, and '_' character.

Test Type

This parameter sets the IP SLA profile test type.

Option	Function
Continuous	Runs continuous pings
Timed	Runs pings for a predetermined time
Count	Runs a number of pings

Destination IP

This parameter specifies the IPv4 or IPv6 address where ping packets will be sent to.

Source IP

This parameter specifies the source IPv4 or IPv6 address used in the ping packets. This must be an IP address that is allocated to one of the Aprisa LTE 5G interfaces. Blank, 0.0.0.0 or ::0 all mean that this parameter is ignored.

Source Interface

This parameter sets the Source Interface None, LAN, WAN, WAN6, WWAN interfaces or any newly created virtual interface (e.g. GRE tunnel interface).

DSCP

This parameter sets the Differentiated Services (Diffserv) Code Point (DSCP) for ping packets. It is a QoS priority value which resides within the IP header (in TOS byte) and can be used to set an IP packet with Diffserv priority. Valid DSCP values are:

DSCP (decimal) Value	Meaning
0	Best Effort
10	AF11 (Assured Forwarding)
12	AF12
14	AF13
18	AF21
20	AF22
22	AF23
26	AF31
28	AF32
30	AF33
34	AF41
36	AF42
38	AF43
8	CS1 (Class Selector)
16	CS2
24	CS3
32	CS4
40	CS5
48	CS6
46	EF (Expedited Forwarding)

Data Bytes

This parameter specifies the number of ICMP ping data payload bytes appended to the ICMP header (8 bytes) after the IPv4 header (20 bytes) or IPv6 header (40 bytes), thus a IPv4 ping packet length will be (28 bytes + data bytes) and a IPv6 ping packet length will be (48 bytes + data bytes).

Range 1- 9000.

Ping Timeout (ms)

This parameter sets the time to wait for a ping response in milliseconds. Range 1 – 120,000ms (2 minutes).

Duration – enabled for a Test Type of Timed

This parameter specifies how long the IP SLA profile should be active for. Can be positive integers up to 604800 (7 days).

Ping UP Count

This parameter sets the number of consecutive ping success required to transition the route from DOWN to UP state. Range 1 – 60.

Ping Intervals (s)

This parameter sets the interval between pings in seconds. Range 1 - 86400.

Track If Active

If active, then pings are only sent when that route is the current preferred route to the ping destination. When not active, the state is set to DOWN and 'Failure Reason' will be set to 'Linked Route Not Active'.

Ping Count – enabled for a Test Type of Count
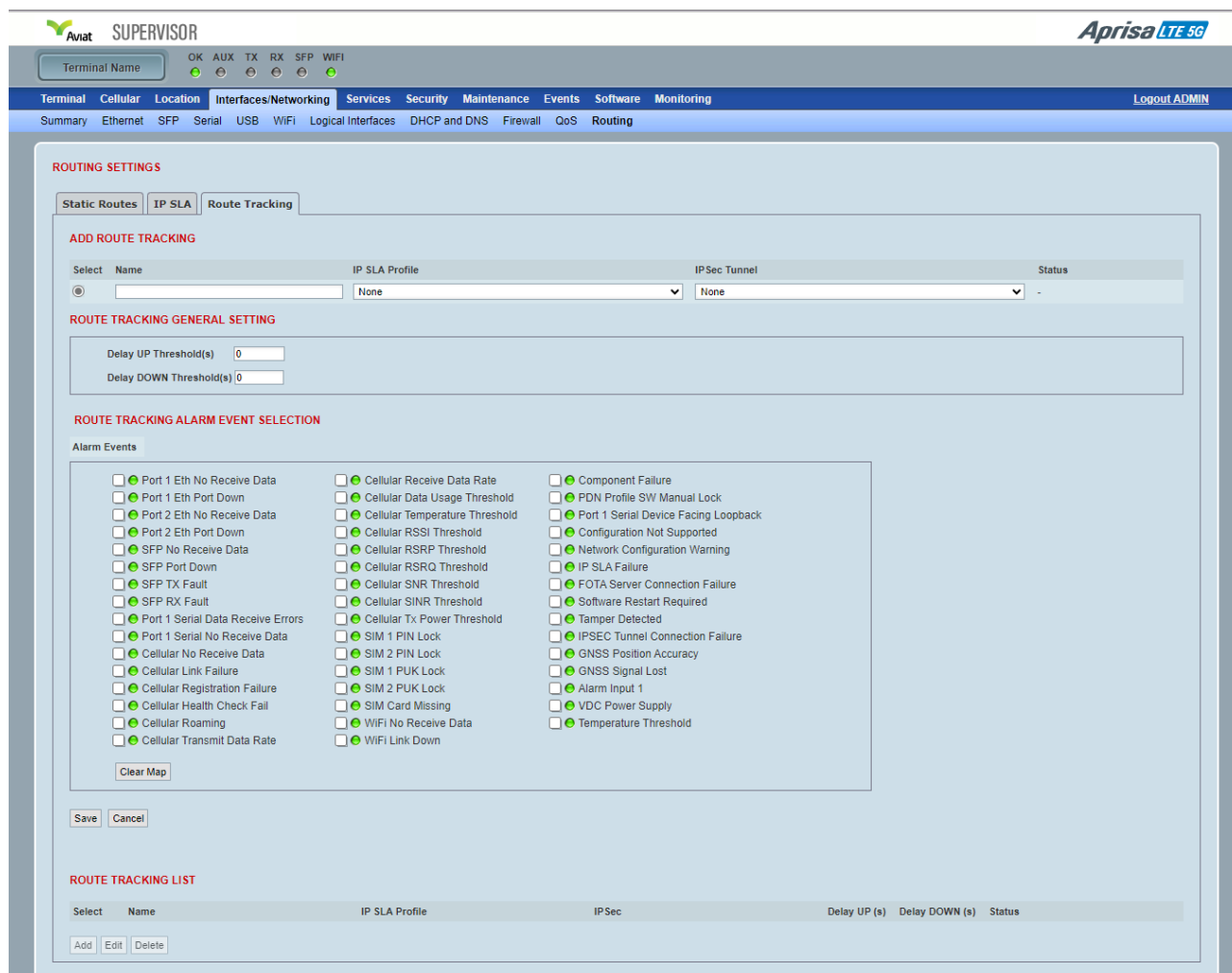
This parameter specifies the number of pings to send for this IP SLA profile.

Ping DOWN Count

This parameter sets the number of consecutive ping failures required to transition the route from UP to DOWN state. Range 1 – 60.

Routing > Route Tracking

This page provides setup of the Route Tracking objects profile to monitor and/or attach to 3 types of services (IPsec Tunnel, IP SLA and Alarm events). These services can be monitored individually and in combination by adding them to the Route Tracking in the static route configuration tab.

ADD ROUTE TRACKING

Name

User defined arbitrary text name for the route tracking objects profile. May contain upper/lower case letters, numbers, and '_' character.

IP SLA Profile

This parameter sets the name of the IP-SLA profile to track / attached to. Can be left unset.

IPsec Tunnel

This parameter sets the name of an IPsec profile to monitor / attached to. Can be left unset.

ROUTE TRACKING GENERAL SETTINGS

Delay UP Threshold (s)

This parameter sets the delay in seconds after all conditions satisfied before changing the route / IPsec tunnel state to UP.

Delay DOWN Threshold (s)

This parameter sets the delay in seconds after any condition failed before changing the route / IPsec tunnel state to DOWN.

ROUTE TRACKING ALARM EVENT SELECTION

Alarm Events

These are the list of alarms that one or more can be associated to the route / IPsec Tunnel tracking objects profile.

Services

Services > Summary

Services > SuperVisor

This page provides setup of SuperVisor.

GENERAL

SuperVisor Polling Period (s)
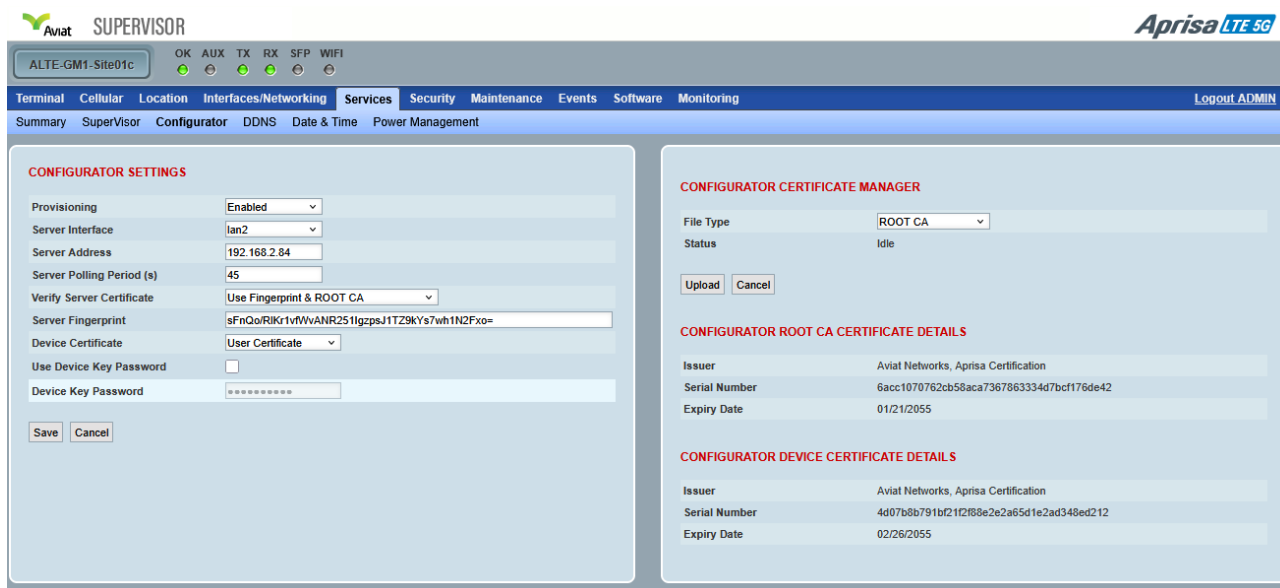
This parameter sets the rate at which SuperVisor refreshes page information and LED states.

SuperVisor Inactivity Timeout (min)

This parameter sets the period of user inactivity before SuperVisor automatically logs out of the LTE.

Services > Configurator

This page provides setup of Aprisa Configurator.

CONFIGURATOR SETTINGS

Provisioning

This parameter sets the Aprisa LTE 5G to connect to the configurator provisioning server.

Server Interface

This parameter sets the network interface that Aprisa LTE 5G uses to connect to the configurator provisioning server.

Server Address

This parameter sets the address of the configurator provisioning server.

Server Polling Period (s)

This parameter sets the polling period of the server.

Verify Server Certificate

This parameter sets how the authenticity of the Configurator server is checked.

Option	Function
Disabled	No validation of the remote server is performed.
Use Fingerprint	The fingerprint of the Configurator server certificate is checked against the provided value.
Use ROOT CA	Use the uploaded CA certificate to verify the Configurator server certificate.
Use Fingerprint & ROOT CA	Use both the provided fingerprint and uploaded CA certificate to verify the Configurator server certificate.

Server Fingerprint

This parameter specifies the fingerprint used for validating the authenticity of the Configurator server. This must be specified as a base64 encoded value.

Root CA Certificate

This parameter sets the polling period of the server.

Device Certificate

This parameter sets the certificate used to identify this Aprisa LTE 5G to the provisioning server.

Option	Function
Default Certificate	Use the factory loaded device certificate and key.
User Certificate	Use the certificate and key uploaded in the Configurator Certificate Manager. This option is only visible if a certificate has been uploaded.

User Device Key Password

This parameter sets if the User Device Key uses a password.

Device Key Password

This parameter sets the Device Key Password.

CONFIGURATOR CERTIFICATE MANAGER

File Type

This parameter sets the File Type to upload. The default setting is ROOT CA.

Option	Function
ROOT CA	Upload a custom Root CA which can be used for server validation.
Device Certificate	Upload a certificate which can be used for identifying this device to the remote Configurator Server. The Device Private Key must match this certificate.
Device Private Key	Upload a private key which can be used for identifying this device to the remote Configurator Server.

Status

This parameter shows the status of the Certificate Manager.

Upload Button

Upload the selected certificate file type.

CONFIGURATOR ROOT CA CERTIFICATE DETAILS

Issuer

This displays the Issuer field of the Root CA certificate.

Serial Number

This displays the Serial Number field of the Root CA certificate.

Expiry Date
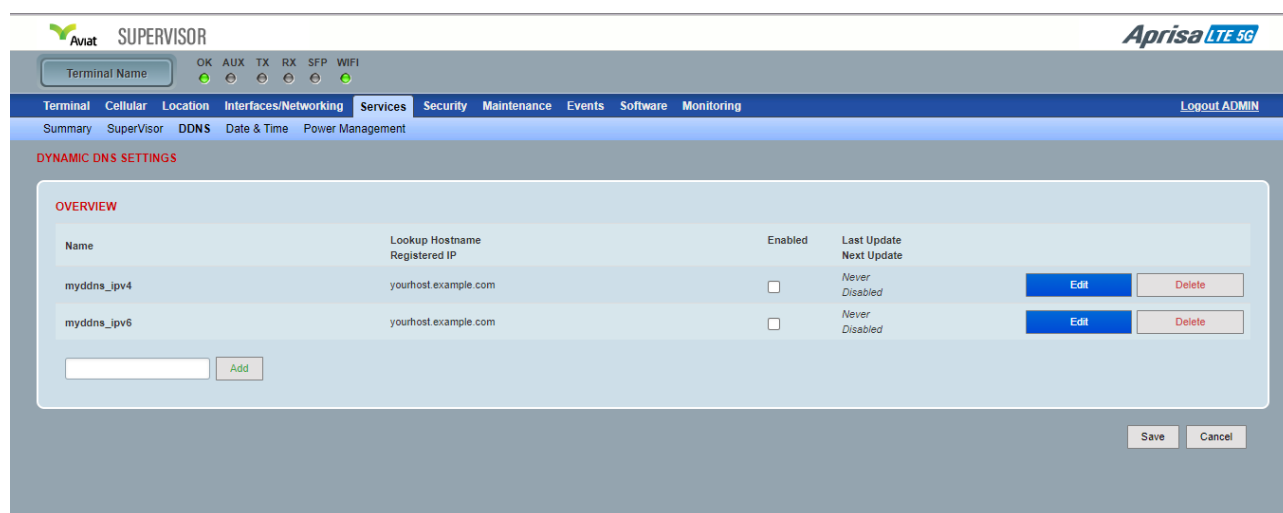
This displays the Expiry Date of the Root CA certificate.

Services > DDNS

This page provides setup of DDNS.

Dynamic DNS (DDNS) is a method of automatically updating a name server in the Domain Name System (DNS). This is most often utilized when the end user has a dynamic IP address and wants to bind it to a static hostname.

The router is compatible with many different third party DNS services that provide the possibility to create a custom hostname and bind it to an IP address. The DDNS service periodically updates the IP address information of the hostname, making sure that the device remains reachable via the same hostname even in cases when its IP address has changed.
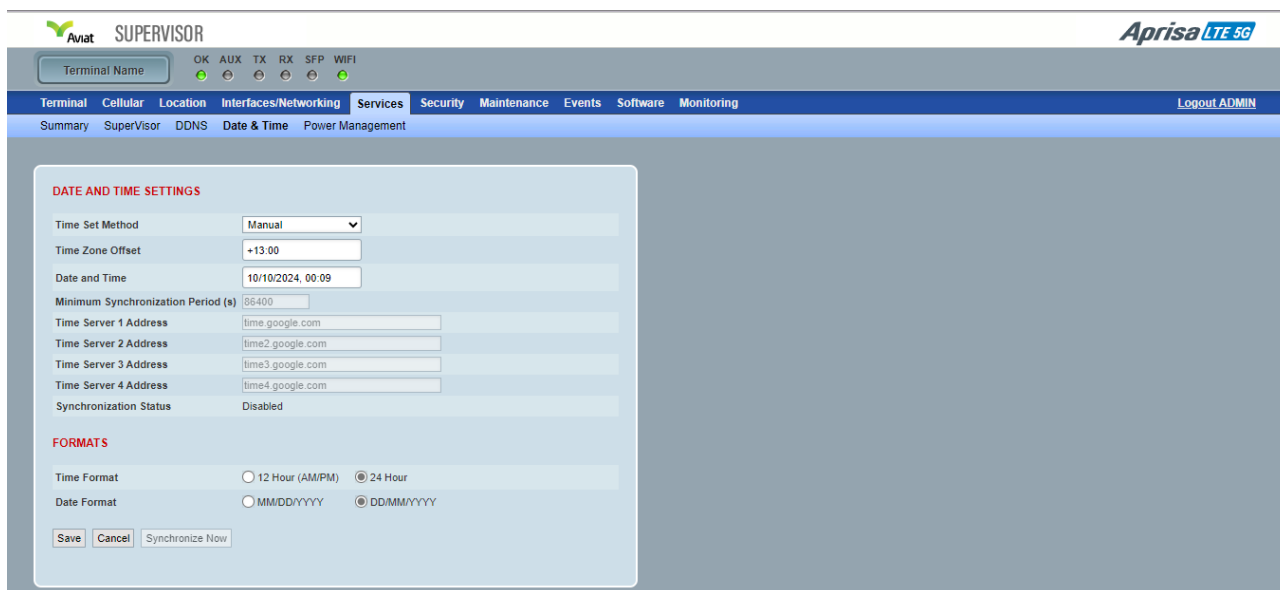
Services > Date & Time

This page sets the device Date and Time.

DATE AND TIME

Sets the device Date and Time. This information is controlled from a software clock.

Time Set Method

This parameter sets the method for setting the Date and Time. The default setting is Manual.

Option	Function
Manual	Time is manually configured through supervisor
NTP	Time is configured using remote NTP server
Cellular	Time is configured using the cellular network
NTP and Cellular	Time is configured using the cellular network and a remote NTP server

Time Zone Offset
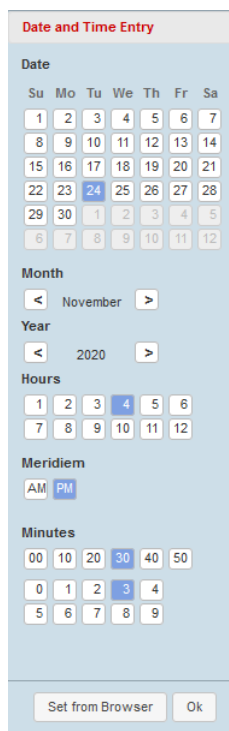
The Time Zone Offset is the number of hours / minutes offset from UTC time. The default setting is enabled but set to 0 hours. Clicking the Time Zone Offset field brings up a pop-up to enter the offset.

Option	Function
Manual	Manual entry of Date and Time
East (+)	Sets 0 to 23 Hours and 00 to 59 Minutes offset from NTP
West (-)	Sets 0 to 23 Hours and 00 to 59 Minutes offset from NTP

After selecting the offset, review the current date and time before saving the changes.

Date and Time

Sets the Date and Time manually by clicking in the Date and Time field.

Minimum Synchronization Period (s)

This parameter sets the minimum number of seconds between the end of the last NTP server synchronization and the next NTP server synchronization attempt. The minimum period is 60 seconds. A period of 0 seconds will disable NTP server synchronization attempts.

Time Server 1 to 4 Address

This parameter sets the address of the four possible NTP servers. Address may be specified as DNS name, IPv4 or IPv6 address.

Synchronization is attempted from all configured servers, and the NTP service intelligently uses offsets from all of them to accurately set the time.

Synchronization Status

This field shows the status of the current synchronization or the result of the last synchronization.

Time Format

This parameter sets the time format for all time based results.

The default setting is 24 Hours.

Date Format

This parameter sets the date format for date based results.

The default setting is DD/MM/YYYY.
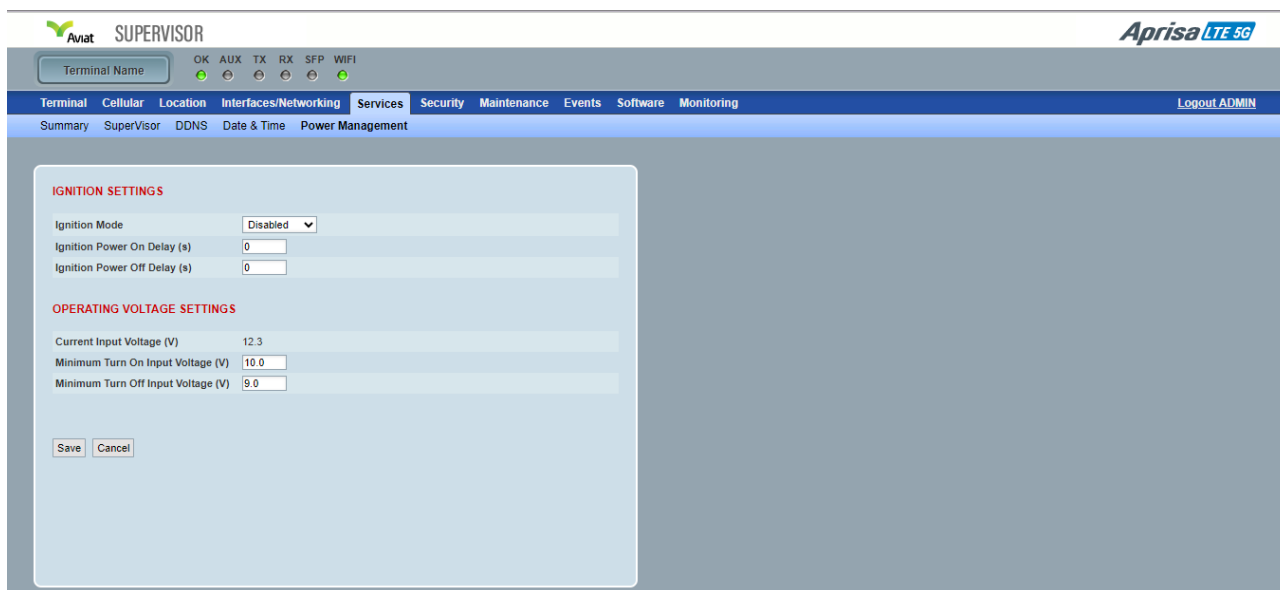
Controls

Synchronize Now

This Synchronize Now button provides manual Synchronization.

Services > Power Management

This page sets power management options for the Aprisa LTE 5G.

IGNITION SETTINGS

Ignition Mode

Sets the method used to turn on and off the Aprisa LTE 5G.

Option	Function
Disabled	As soon as power is applied on pin 1 and 2 of power connector (see 'Power Supply' on page 60), the Aprisa LTE 5G will turn on and stay on. This setting ignores the ignition sense pin behavior (i.e. power supply pin 3 is not controlling the power on/off of the Aprisa LTE 5G. In this setting this pin 3 is acting as GPIO input for any other purpose not related to power on/off.
Enabled	The Aprisa LTE 5G will turn on after the configured 'Minimum Turn On Input Voltage' time only when Ignition sense/GPIO input pin (see 'GPIO' on page 91) is active and turn off after the configured 'Minimum Turn Off Input Voltage' time only when ignition sense/GPIO input pin is inactive. The active state of the GPIO input pin is configured on the 'Events > Alarm I/O Setup' on page 260, and defaults to active high.

Ignition Power On Delay (s)

Sets the time between the alarm input going active and the LTE turning on.

Ignition Power Off Delay (s)

Sets the time between the alarm input going inactive and the LTE turning off.

OPERATING VOLTAGE SETTINGS

Power supply input voltage thresholds are used to trigger LTE sleep mode to reduce power consumption.

The difference between the two thresholds Turn On and Turn Off defines the detection hysteresis.

In sleep mode, the main CPU, Ethernet, SFP, WiFi, Cellular, and serial ports are all shut down.

Minimum Turn On Input Voltage:

The LTE will not turn on when input supply voltage remains lower than this threshold. While voltage is lower than this threshold, but higher than minimum operating voltage of the LTE, the OK led will flash once every 5 seconds. The valid values are from 10.0 V and 27.0 V but the value must always be higher than Minimum Turn Off Input Voltage.

The default value is 10 V.

Minimum Turn Off Input Voltage:

The LTE will turn off when the input supply voltage is lower than this threshold. The valid values are from 9.5 V to 26.5 V but the value must always be lower than Minimum Turn On Input Voltage.
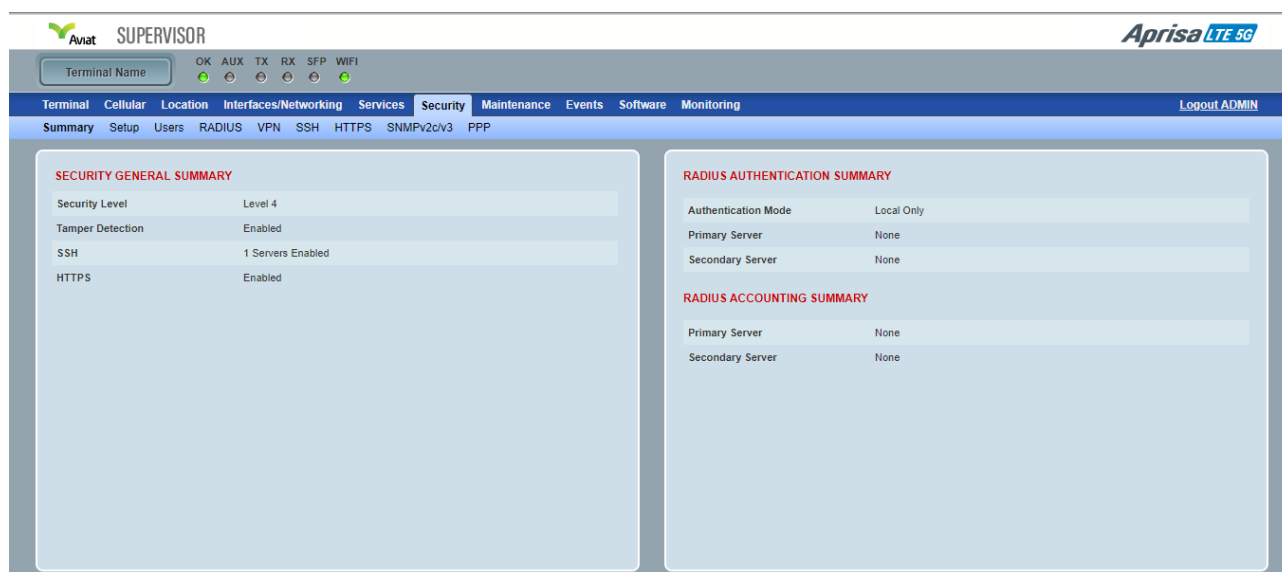
The default value is 9.5 V.

Note: There must also be a 0.3 V difference between the 'Minimum Turn On Input Voltage' and the 'Minimum Turn Off Input Voltage'.

Security

Security > Summary

This page displays the current security settings.

Security > Setup

This page sets the security settings.

SECURITY LEVEL SETTINGS

Security Level

If the Aprisa LTE 5G was purchased from Aviat Networks with Enhanced Security Features, the Security Level will be set to Level 4 and cannot be reduced.

If the Security Level is set to Level 4 and a range of enhanced security restrictions will be enforced. These enforced restrictions include;

- the security level cannot be reduced lower than Level 4
- mandatory brute force login protection
- mandatory password change notification
- only secure protocols for File Transfers, WiFi, WEB and SNMP
  Configuration files that contain a security level lower than Level 4 cannot be loaded into the LTE.
- the software cannot be downgraded to a less secure version and future upgrades and downgrades will only be possible if the version contains 'Enhanced Security Features'

If the Security Level was set to less than Level 4, changing the Security Level to Level 4 will popup;

WARNING

Device configuration of the below services will be updated to comply to Security Level 4.

1. Inactivity Timeout
2. Supervisor webserver
3. WiFi connectivity
4. User password restrictions.

Press OK to continue or Cancel.

[Ok]   [Cancel]
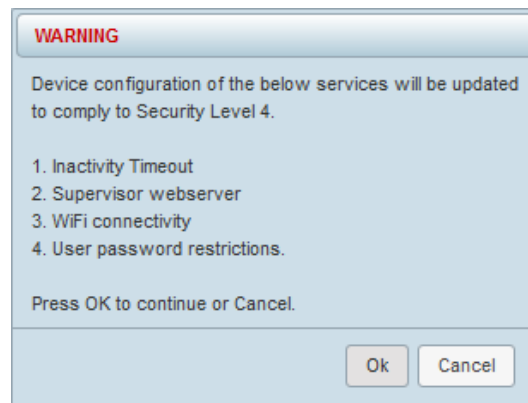
Security Level vs Security Features

	Feature	Security Level 1	Security Level 3	Security Level 4
1	Brute Force Login Protection	Optional	Optional	Mandatory
2	Two Factor Authentication	Optional	Optional	Optional
3	Password Change Notification	Optional	Optional	Mandatory
4	Stricter Password Requirements	Optional	Optional	Mandatory
5	Secure WEB Interface Protocol (HTTPS)	Optional	Optional	Mandatory
6	Secure SNMP Interface Protocol (SNMPv3)	Optional	Optional	Mandatory
7	Secure Wi-Fi Interface Protocol	Optional	Optional	Mandatory
8	Secure File Transfer Protocol	Optional	Optional	Mandatory
9	Reduced Inactivity Session Timer	Optional	Optional	Mandatory
10	Encrypted File Export	Not Encrypted	Encrypted	Encrypted
11	SSH Key-based Authentication	Optional	Optional	Optional
12	Secure Boot	Mandatory	Mandatory	Mandatory

SECURITY MODULE SETTINGS

Tamper Detection

This parameter sets if tamper detection is enabled.

Option	Function
Disabled	Tamper Detection is disabled.
Enabled	Tamper Detection is enabled. When this setting changes, the LTE needs to be rebooted which will reset all other settings to defaults. The tamper function detects when the case is opened and will securely delete settings and restart the LTE.

ENCRYPTION KEY SETTINGS

Encryption Key
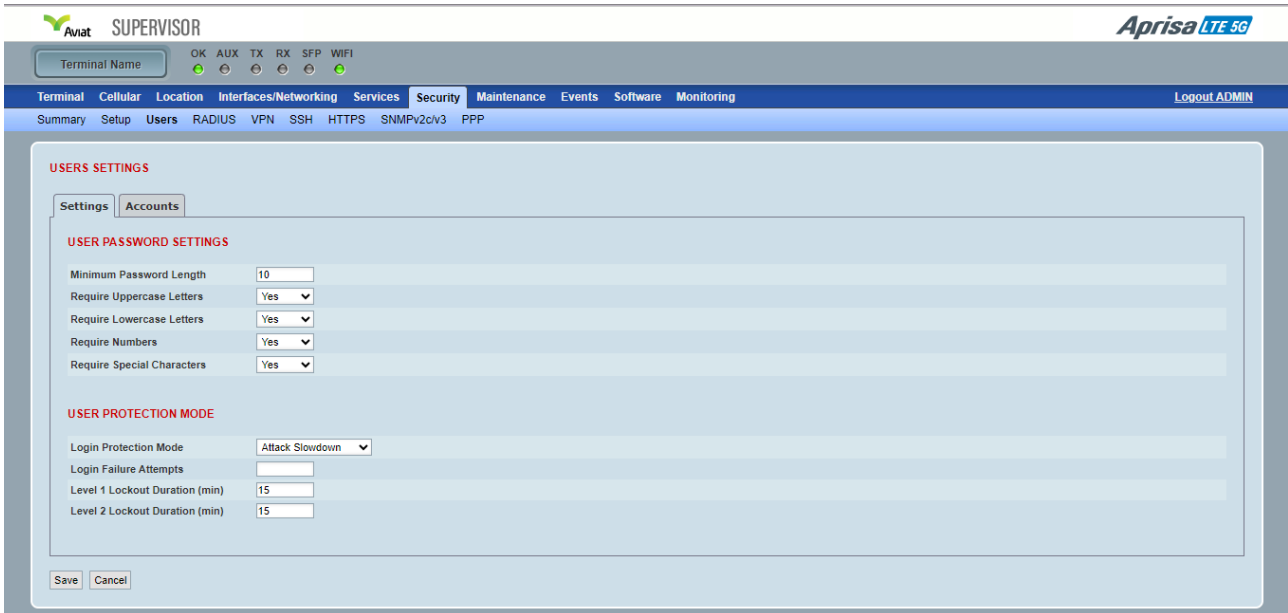
This parameter sets the password for 'Severity Level = Level 3' or higher level. It uses AES-256-CBC encryption. The password is converted to AES key using the PBKDF2 (Password-Based Key Derivation Function 2) key derivation algorithm. This key is also used to encrypt the configuration file of the Aprisa LTE 5G router.

Allow Insecure Secure SNMPv3 Protocols

This option supports customers using Security Level 4 but with an NMS that only supports SNMPv3 SHA-1. This selection is only displayed when the Security Level is set to 4.

Security > Users

Security > Users > Settings

USER PASSWORD SETTINGS

Good password policy:

- contains at least one upper case letter, and
- contains at least one lower case letter, and
- contains at least one digit, and
- is not a term in a familiar language or jargon, and
- is not identical to or derived from the accompanying account name, from personal characteristics or from information from one's family/social circle, and
- is easy to remember, for instance by means of a key sentence

USER PROTECTION MODE

Login Protection Mode

This parameter sets the Login Protection Mode. They provide user account lockout mechanisms to mitigate brute force password guessing attacks.

Option	Function
Disabled	Disables login protection
Attack Slowdown	In this mode, the user account will be locked out for the duration specified in Level 1 Lockout Duration and Level 2 Lockout Duration, cycling between the two. This mode slows down attacks.
Attack Lockout	In this mode, the user account will be permanently locked out if the protection mechanism has reached Locked Level 1 and Locked Level 2 and the next login attempt fails. The user account must then be manually unlocked by an 'Admin' user account either from SuperVisor or via SNMP. This mode blocks persistent attacks.

Attack Slowdown

The Attack Slowdown login protection lockout mechanism will be processed as follows:

- When the number of login failure attempts is less than the setting of the 'Login Failure Attempts' field, the login attempt is processed.

- When the number of login failure attempts is greater than the setting of the 'Login Failure Attempts' field, the user account will be:

  o temporarily disabled at level 1 for the 'Level 1 Lockout Duration' period if the user account was not previously already released from locked level 2.

  o temporarily disabled at level 2 for the 'Level 2 Lockout Duration' period if the user account was previously already released from locked level 1.

This lockout mode will cycle the lockout of the accounts between locked level 1 and locked level 2.

Attack Lockout

The Attack Lockout login protection lockout mechanism will be processed as follows:

- When the number of login failure attempts is less than the setting of the 'Login Failure Attempts' field, the login attempt is processed.

- When the number of login failure attempts is greater than the setting of the 'Login Failure Attempts' field, the user account will be:

  o temporarily disabled at level 1 for the 'Level 1 Lockout Duration' period if the user account was not previously already released from locked level 1.

  o temporarily disabled at level 2 for the 'Level 2 Lockout Duration' period if the user account was previously already released from locked level 1.

  o permanently disabled if the user account was previously already released from locked level 2. The user account must then be manually unlocked by an 'Admin' user account either from SuperVisor or via SNMP.
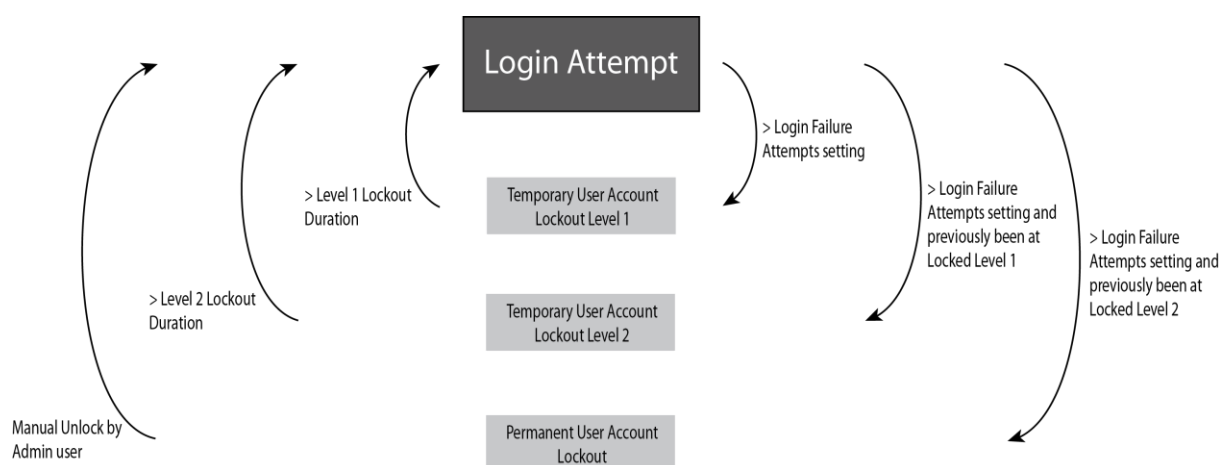
Login Failure Attempts

When Login Protection Mode is active, this parameter sets the maximum number of consecutive failed login attempts before the relevant user account lockout process is initiated. This field can be set from 3 to 10 times and the default value is 5.

Level 1 Lockout Duration (min)

When Login Protection Mode is active and the user account is in the state of 'locked level 1', the user account will be locked out for the duration specified. This field can be set from 1 to 15 minutes and the default value is 1 minute.
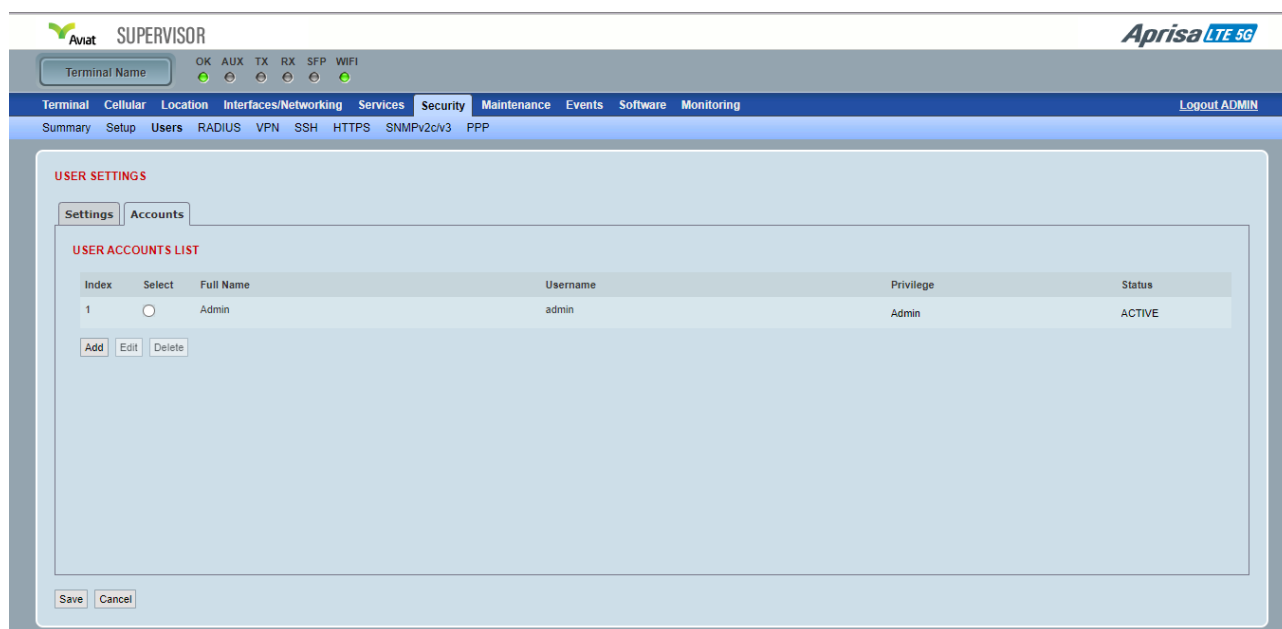
A user account in the state of 'locked level 1' shall be unlocked and put in the released from level 1 lockout state after this level 1 lockout duration has expired.

Level 2 Lockout Duration (min)

When Login Protection Mode is active and the user account is in the state of 'locked level 2', the user account will be locked out for the duration specified. This field can be set from 5 to 30 minutes and the default value is 5 minutes.

A user account in the state of 'locked level 2' shall be unlocked and put in the released from level 2 lockout state after this level 2 lockout duration has expired.

Security > Users > Accounts

Note: You must login with 'admin' privileges to add, disable, delete a user or change a password.

Shows a list of the current user accounts setup in the LTE.

If the currently viewed page is full (displaying 8 user accounts), SuperVisor shall automatically display the last user account page when a new user is added. However, if there are unsaved changes on the current page, the user shall be prompted to save the changes first before adding a new user.

Status

The Status indicates whether a user account is active or locked out.
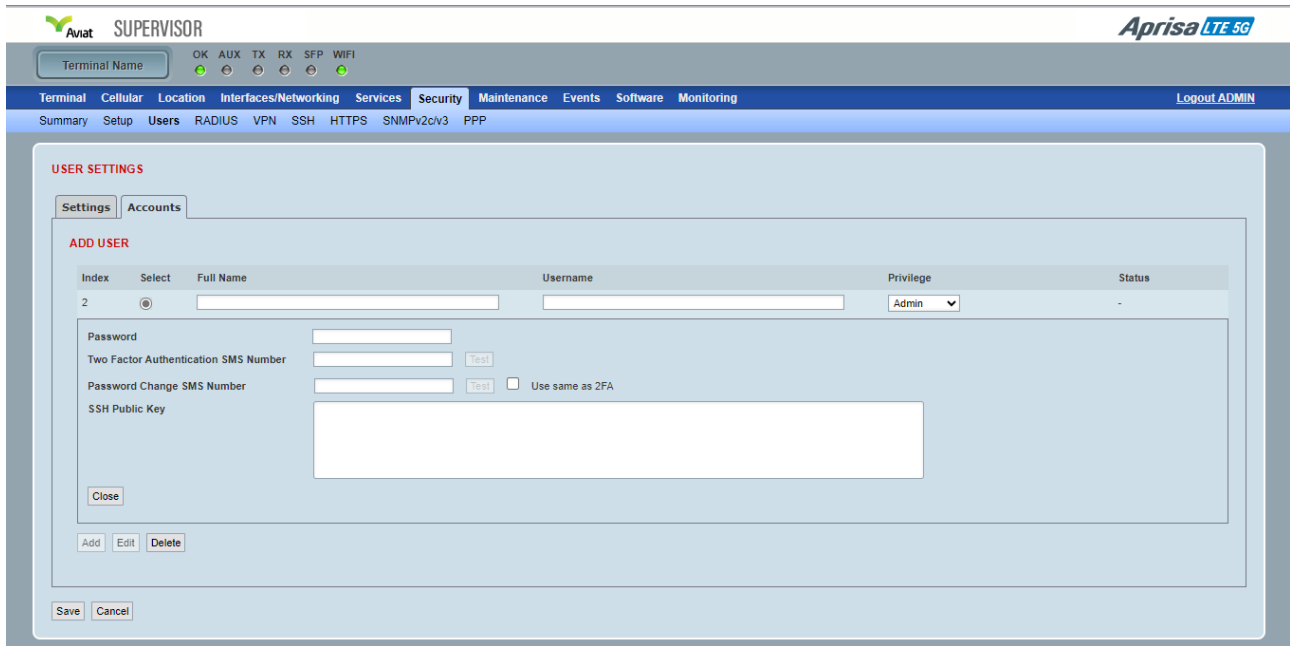
Option	Function
ACTIVE	The user account is currently active.
PENDING	The user account has been entered but not saved.
LOCKED (Level 1)	Login Protection Mode is active, and the user account has been locked out due to repeated unsuccessful login attempts. The account will remain locked out for a period defined in 'Level 1 Lockout Duration' at the 'Security > Users > Settings' on page 209.
LOCKED (Level 2)	Login Protection Mode is active, and the user account has been locked out due to repeated unsuccessful login attempts. The account will remain locked out for a period defined in 'Level 2 Lockout Duration' at the 'Security > Users > Settings' on page 209.
LOCKED	Login Protection Mode is active, and the user account has been locked out due to repeated unsuccessful login attempts. The user account is permanently locked out.

This tab shall also provide the interface for the ADMIN user to unlock any locked user accounts.

The 'Unlock' button shall be disabled unless a locked account is selected, in which case, clicking the button will unlock the selected account.

To add a new user:

1. Click Add.

2. Enter the Full Name.

A full name can be 32 characters but cannot contain tabs.

3. Enter the Username.

A username can be up to 32 characters but cannot contain tabs. Usernames are case sensitive.

4. Select the User Privileges

There are four pre-defined User Privilege settings to allocate access rights to users. These user privileges have associated default usernames and passwords of the same name.

The default login is 'admin'.

This login has full access to all LTE parameters including the ability to add and change users. There can only be a maximum of two usernames with admin privileges and the last username with admin privileges cannot be deleted.
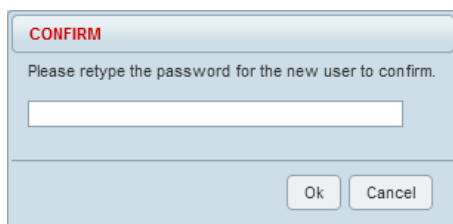
User Privilege	Default Username	Default Password	User Privileges
Admin	admin	admin	Users in this group can view and edit all parameters.
Engineer			Users in this group can view and edit parameters except Security > Users.
Technician			Users in this group can view and edit parameters except Security > Users and Security > Setup.
View Only			Users in this group can only view the summary pages.

See 'SuperVisor Menu Access' on page 100 for the list of SuperVisor menu items versus user privileges.

5. Enter the Password.

The password must meet the password rules defined in 'Security > Users > Settings' on page 209.

When the password is changed, you will be prompted for confirmation of the password to avoid mistypes.

The Status will show PENDING until the entry is saved.

6. Enter the Two Factor Authentication SMS Number (optional).

When a Two Factor Authentication SMS Number has been entered, then the user cannot login without entering the correct verification code.

The Two Factor Authentication SMS Number entry can be entered as '+972525811125' or '00622972525811'. Any spaces entered will be stripped out before processing.

7. Enter the Password Change SMS Number.

When a user's password is changed, an SMS notification will be sent to that configured number to inform of the password change.

If you want the same number for the Password Change SMS Number as the Two Factor Authentication SMS Number, tick the 'Use same as 2FA' or untick the 'Use same as 2FA' and enter the Password Change SMS Number you want.

When SMS numbers are not compulsory, and a number has not been entered in the Password Change SMS Number textbox, then an SMS message is not sent when the password is changed.

If a Password Change SMS Number has been entered, then an SMS message will be sent to the Password Change SMS Number if the password is changed.
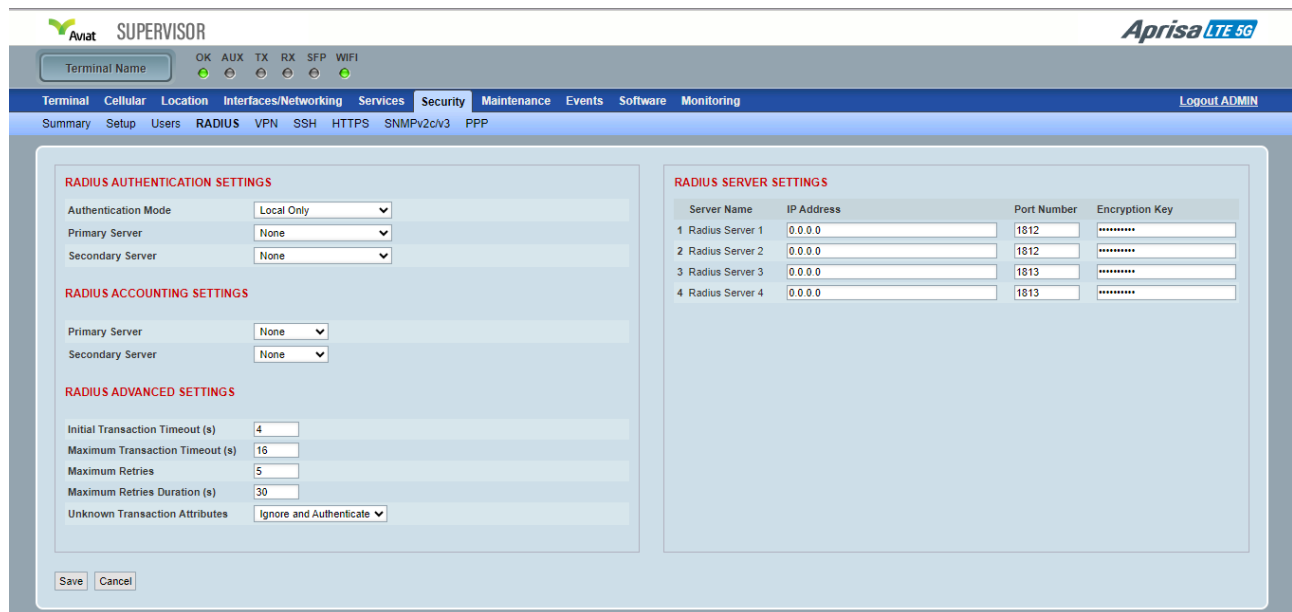
8. Enter SSH Public key

Public key authentication is an alternative means of identifying user to a SSH server, instead of password-based authentication. Public key authentication is more secure as it provides cryptographic strength that even strong and long password cannot provide.

9. Click Save.

Security > RADIUS

This page enables setup of the LTE RADIUS server.

RADIUS - Remote Authentication Dial In User Service

RADIUS is a client / server system that secures the LTE against unauthorized access. It is based on open standard RFCs: RFC 2865/6, 5607, 5080 and 2869. It is used for remote user Authorization, Authentication and Accounting.

When a user logs into an LTE with RADIUS enabled, the user's credentials are sent to the RADIUS server for authentication of the user.

Transactions between the RADIUS client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network.

A RADIUS server responding to an LTE must be configured to provide the access level of the user. This may be via the Management-Privilege-level attributes:

> Admin Level = 4
>
> Engineer Level = 3
>
> Technician Level = 2
>
> Viewer Level = 1

Alternatively, a RADIUS server may provide the access level by setting Service-Type (6) = Administrative (6) which will grant the user Admin Level access to the LTE, or Service-Type (6) = NAS Prompt (7) which will grant the user Viewer Level access to the LTE.

A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

RADIUS AUTHENTICATION SETTINGS

Authentication Mode

This parameter sets the Authentication Mode.

Option	Function
Local Only	No radius Authentication – allows any local user privilege
Radius Only	Only radius Authentication – no local user privilege
Radius and Local admin	Uses radius Authentication if it is available. If radius Authentication is not available, uses local Admin login
Radius Then Local	If the user is not authenticated in the radius server, it allows any local user privilege.
Local Then Radius	If the user is not allowed in the local user privilege, radius authentication is used.

Primary Server

This parameter sets which radius server is used as the primary server for authentication. Select one of the possible authentication servers setup in Radius Server Settings.

Secondary Server

This parameter sets which radius server is used as the secondary server for authentication. Select one of the possible authentication servers setup in Radius Server Settings.

RADIUS ACCOUNTING SETTINGS

Primary Server

This parameter sets which radius server is used as the primary server for accounting (log of user activity). Select one of the possible accounting servers setup in Radius Server Settings.

Secondary Server

This parameter sets which radius server is used as the secondary server for accounting. Select one of the possible accounting servers setup in Radius Server Settings.

RADIUS ADVANCED SETTINGS

Initial Transaction Timeouts (IRT) (seconds)

This parameter sets the initial time to wait before the retry mechanism starts when the server is not responding.

Default Transaction Timeouts (MRT) (seconds)

This parameter sets the maximum time between retries.

Maximum Retries

This parameter sets the maximum number of retry attempts when the server is not responding.

Maximum Retries Duration (s)

This parameter sets the maximum duration it will attempt retries when the server is not responding.

Unknown Transaction Attributes

This parameter sets the LTE's response to unknown attributes received from the radius server.

Option	Function
Ignore and Authenticate	Ignore the unknown attributes and accept the authentication received from the radius server
Reject and Deny	Reject the authentication received from the radius server

RADIUS SERVER SETTINGS

Server Name

You can enter up to four radius servers 1-4.

IP Address

The IP address of the Radius server.

Port Number

The Port Number of the Radius server. RADIUS uses UDP as the transport protocol.
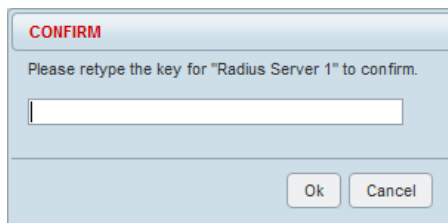
- UDP port 1812 is used for authentication / authorization
- UDP port 1813 is used for accounting.

Old RADIUS servers may use unofficial UDP ports 1645 and 1646.

Encryption Key

The password of the Radius server.

When the password is changed, you will be prompted for confirmation of the password to avoid mistypes.

Security > VPN

Secure VPN to data center and multipoint (peer to peer) VPNs

Setting up a secure connection to the customer data center or to other multiple Aprisa LTE 5G (peer to peer) requires setting up a VPN connection to the required end point/s. The Aprisa LTE 5G allows a few VPN connection options, non-secure and secure PTP VPNs and Multi-Point (MP) VPNs, which are listed list below:

1. Setup unsecure GRE PTP VPN connections.
2. Setup secure GRE-over-IPsec connections.
3. Setup secure Multipoint (peer to peer) GRE-over-IPsec VPN connections.
4. Checking and monitoring the VPN connections.

The VPN menu allows configuration of the above list of VPN options while monitoring the VPNs is under the Maintenance menu.

Setup unsecure GRE PTP VPN connections

The user can use a regular unsecure IPv4/v6 connection or unsecure GRE VPN tunnel. The Aprisa LTE 5G can act as a GRE tunnel endpoint. The benefit of GRE tunnel is that it provides a tunnelling connection to multiple protocols between two endpoints (or two private networks) over another network like they were locally connected. It allows the user to reconfigure its local device IP addressing without worrying about connectivity. It allows transport of L2/L3/L4 unicast and multicast protocols between two endpoints.

Figure 19 describes the unsecure GRE VPN tunnel connection to the corporate data center.
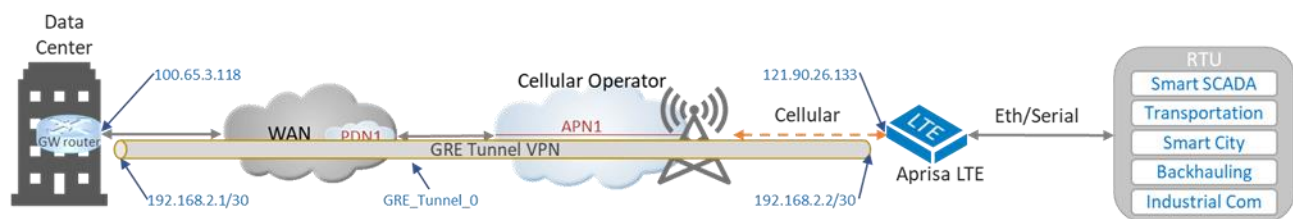
Figure 19 Setup unsecure GRE PTP VPN connections

To setup the GRE tunnel VPN connection per the above figure, perform the following steps on Aprisa LTE 5G:

1. Navigate to SuperVisor 'Security > VPN' and on the GRE tab click the Add button.
2. Set 'Mode = IP over GRE' (or 'IP over GREv6' in case of IPv6 GRE tunnel).
3. Set 'Tunnel Name = GRE_Tunnel_0'. This sets the tunnel ID. This ID is recommended to be used on both ends of the tunnel configuration.
4. Set 'Tunnel IPv4 address/Netmask = 192.168.2.2 / 255.255.255.252 (/30)' (or Tunnel IPv6 Address/Prefix in case of IPv6). This is the IP address of the virtual tunnel interface. This is the GRE tunnel "glue" IP address to the transport IP address (or per standard notation the delivery IP). Note: those IP addresses must be unique and without subnet overlapping at both ends of the GRE tunnel.
5. Set 'Tunnel Key = 42'. This is the GRE tunnel key number and is required in DMVPN setup.
6. Set 'Source Public Address (SPA) = 121.90.26.133'. This is the source transport IP address (or the outer IP source address of the GRE tunnel across the cellular and wan networks) which is "glue" to the virtual tunnel IP address. On the data center endpoint set 'Source Public Address = 100.65.3.118'. The SPA can be public port or local port, and in this example, it is a public port. Alternatively, the SPA can be set to 0.0.0.0 if the source interface is selected. In this example it can be wwan.
7. Set 'Destination Public Address = 100.65.3.118'. This is the destination transport IP address (or the outer IP destination address of the GRE tunnel across the cellular and wan networks) which is "glue" to the virtual tunnel IP address. On the data center endpoint set 'Destination Public Address =

121.90.26.133'. Alternatively, the SPA can be set to 0.0.0.0 if the source interface is selected. In this example it can be wwan.

8. Set 'TTL = 255' for max hop count and MTU to any max MTU required size (recommended 1500 byte). Note that the MTU must be lower than the operator 'Cellular MTU' shown in Cellular > Summary page.

9. Set 'Source Interface' = wwan. If all traffic is directed via this interface and public IP address might change, it is recommended to set the source interface only and leave the source/destination public address with default value 0.0.0.0 to eliminate the tunnel disconnection on public IP change.

Setup secure GRE-over-IPsec connections (GRE tunnel inside IPsec VPN)

If the user requires a secure VPN, the IPsec VPN can be used without using inside a GRE tunnel, but IPsec alone does not support multicast only GRE can provide that. Thus, it is more common to use GRE tunnel inside an IPsec for a secure VPN that can carry any protocol. The Aprisa LTE 5G can act as a GRE-over-IPsec VPN endpoint.

Figure 20 describes the secure GRE-over-IPsec VPN connection to the corporate data center.
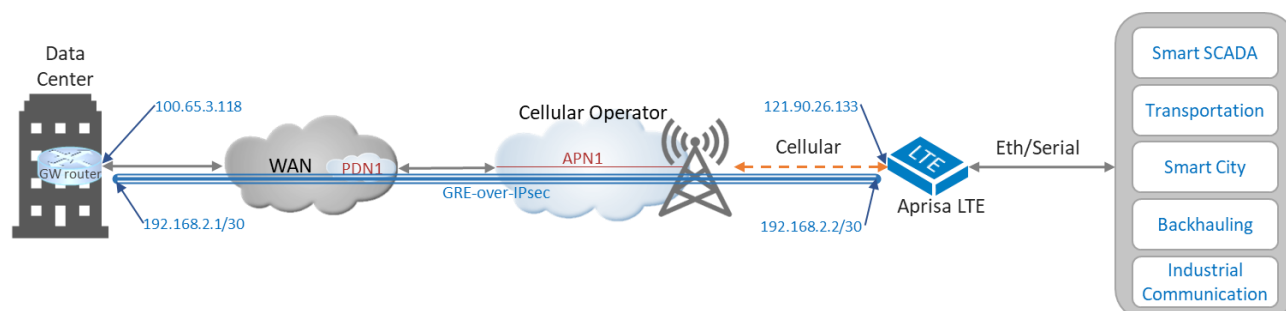
Figure 20 Setup secure GRE-over-IPsec connections

To setup the GRE-over-IPsec VPN connection per the above figure, perform the following steps:

1. Create a GRE tunnel. Navigate to SuperVisor 'Security > VPN' and on the GRE tab, click the Add button. Set the GRE tunnel as described in the section above 'Setup unsecure GRE PTP VPN connections'.

2. Create the IPsec Tunnel VPN. Navigate to the 'IPsec Tunnel' tab and click the Add button.
   a. Set 'Tunnel Name = IPsec_Tunnel_0'. This sets the IPsec tunnel ID. This ID is recommended to be used on both end of the tunnel configuration.
   b. Set 'Mode' as required, either 'Tunnel' or 'Transport'. See description under 'Security > VPN > IPsec Tunnel'. In this example Mode = Transport.
   c. Set 'Local Subnet = 121.90.26.133' when Mode = Tunnel. This is the source transport IP address and subnet, i.e. the local endpoint interface of the IPsec tunnel. This is the same IP address of 'Source Public Address' in GRE tunnel settings. This field is greyed out when Mode = Transport.
   d. Set 'Remote Subnet = 100.65.3.118' when Mode = Tunnel. This is the destination transport IP address and subnet, i.e. the remote endpoint interface of the IPsec tunnel. This is the same IP address of 'Destination Public Address' in GRE tunnel settings. This field is greyed out when Mode = Transport.
   e. Set the 'Local subnet' and 'Remote subnet' at the data center, respectively (IP address are swapped at the data center for appropriate local/remote IP address interfacing).
   f. Set the appropriate encryption, Authentication and DHGroup as required. Make sure this settings match with the peer IPsec connection.

3. Create the IPsec VPN connection. Navigate to the 'IPsec Connection' tab and click the Add button.
   a. Set 'IKE Connection Name = IKE_Tunnel_0'. This sets the security association of Internet Key Exchange protocol ID used by IPsec security suite. This ID is recommended to be used on both ends of the IKE IPsec configuration.
   b. Set 'Remote Gateway = 100.65.3.118'. This is the destination transport IP address, i.e. the remote endpoint interface of the IPsec tunnel. This is the same IP address of 'Destination Public Address' in GRE tunnel settings and 'Remote Subnet' in IPsec tunnel settings Note that in DMVPN the remote gateway shall set to 0.0.0.0, since DMVPN automatically determine the address.
   c. Set the 'Authentication Method' and the associated pre-shared key or certification.
   d. Set the appropriate encryption, Authentication and DHGroup as required. Make sure this settings match with the peer IPsec connection.
   e. Set the 'Associated Transport List' by select the IPsec Tunnel name 'IPsec_Tunnel_0' from the list.

Note: after GRE-over-IPsec VPN setup, the Aprisa LTE 5G is connected directly to the data center and in terms of routing, the hop count is considered as a single hop count event though there are multiple routers across the path.
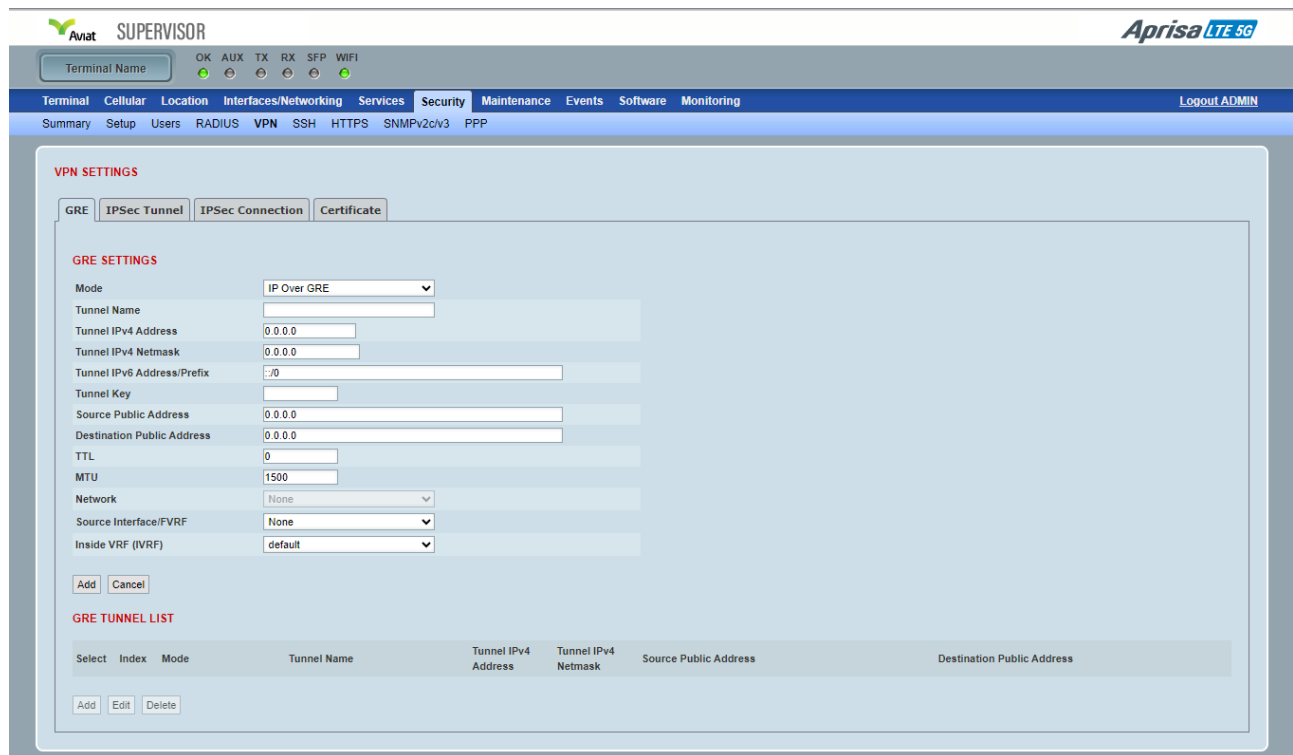
VPN > GRE

This page provides VPN Generic Routing Encapsulation (GRE) configuration.

GRE encapsulates data inside IP packets and routes it over an IP network through virtual point to point links.

It is a simple encapsulation protocol allowing both L2 and L3 networks to be joined through a tunnel. A virtual interface is created, and route table entries are used to send traffic into the tunnel interface (for L3 tunnels), or the interface is joined to a bridge (for L2 tunnels).

Data in a GRE tunnel is NOT encrypted. IPsec can be used to encrypt GRE tunnels.

Mode

Option	Function
IP over GRE	IP over GRE is a L3 tunnel for IP packets (both IPv4 and IPv6) over IPv4 networks
IP over GREv6	IP over GREv6 is a L3 tunnel for IP packets (both IPv4 and IPv6) over IPv6 networks
Ethernet over GRE	Ethernet over GRE transports L2 packets of any type over IPv4 networks
Ethernet over GREv6	Ethernet over GREv6 transports L2 packets of any type over IPv6 networks

Tunnel Name

The name of the tunnel

Tunnel IPv4 address/netmask

This defines the IPv4 address and netmask of the virtual interface used for routing. Not valid for Ethernet over GRE/GREv6.

Tunnel IPv6 address/prefix

This defines the IPv6 address and prefix of the virtual interface used for routing. Not valid for Ethernet over GRE/GREv6.

Tunnel Key

An optional setting, to enables an ID key for a GRE tunnel interface. The tunnel key specifies a number from 0 to 4,294,967,295 that identifies the tunnel key. Note: The tunnel key must be set to the same value on all hubs and spokes that are in the same DMVPN network.

Source Public Address

This configures the external IP address that is used for GRE packets. If left blank, the source address is automatically determined based on best route to destination public address. For IP/Ethernet over GRE this should be an IPv4 address, and for IP/Ethernet over GREv6 this should be an IPv6 address.

Destination public address

The address of the remote device that will terminate the tunnel.

TTL

The TTL to set on outgoing GRE packets. The default is 0, which means the TTL of encapsulated packets is inherited.

MTU

The MTU to set on the virtual interface. When GRE is setup over the cellular interface, this MTU value shall be equal or lower than the operator 'Cellular MTU' shown in Cellular > Summary. This rule is true for any other interface.

Network

When Ethernet over GRE/GREv6 is used, this bridge interface that the tunnel will be joined to.

Source Interface/FVRF

Optional; The source interface or FVRF where the GRE tunnel encapsulated packets go through, this includes a FVRF interface.

Inside VRF (IVRF)
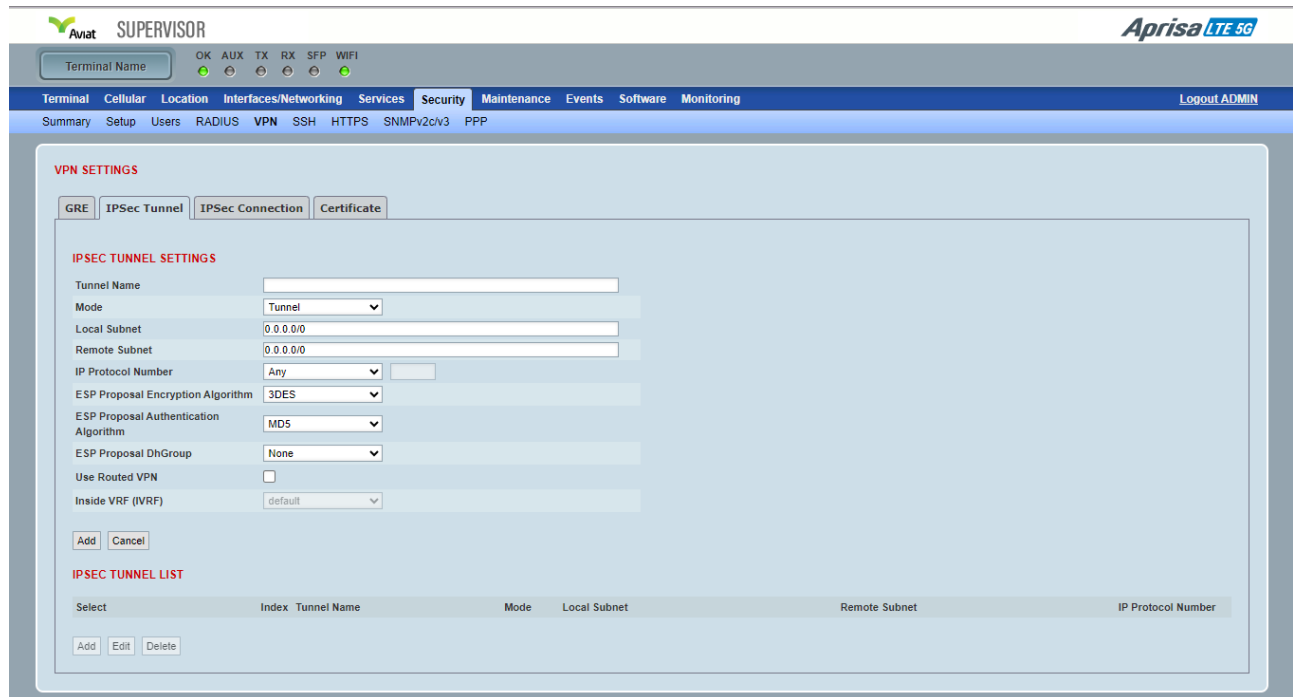
An Inside VRF (IVRF) specifies the VRF that this GRE tunnel sends / receives decapsulated packets to / from.

Aprisa LTE 5G Multi-VRF supports Front Door VRF (FVRF) and Inside VRF (IVRF). IVRF/FVRF allows to build multiple isolated services or groups and isolate between inside IVRF to outside FVRF. A GRE tunnel can be associated with two VRF domains, the FVRF and IVRF where the outer encapsulated packet or local endpoint of the GRE tunnel belongs to the FVRF domain, while the inner, protected IP packet or the source and destination addresses of the inside packet belongs to the IVRF. For more information see 'VRF (Virtual Routing and Forwarding) and VSI (Virtual Switch Instance)' on page 46.

VPN > IPsec Tunnel

This page provides VPN IPsec Tunnel configuration.

IPsec tunnels define what networks are connected at each end of the link. The actual connection to the remote end-point used for a given tunnel is configured separately in the IPsec connection tab (this is because multiple tunnels may use the same connection).

Tunnel Name

Name of this tunnel

Mode

Option	Function
Tunnel	This encapsulates the IP header and the payload and introduces a new outer header. Can be used to create site-site VPNs
Transport	This encapsulates only the IP payload, and not the header. It provides a secure connection between two endpoints. Often combined with other tunneling protocol (e.g. GRE) to create site-site VPNs

Local Subnet

An IPv4 or IPv6 address/prefix. Packets with source address matching this will be sent on the tunnel

Remote Subnet

An IPv4 or IPv6 address/prefix. Packets with destination address matching this will be sent on the tunnel

IP Protocol Number

The type of protocol to tunnel. Drop down menu includes GRE, TCP, UDP, ICMP and specific protocol (number) or any protocol to allow all protocols to be tunneled. DMVPN typically uses GRE for IPsec+GRE tunneling (so other traffic like pings are unencrypted).

ESP Proposal Encryption Algorithm

Encryption algorithm for IKE SA exchange for this tunnel.

ESP Proposal Authentication Algorithm

Authentication algorithm for IKE SA exchange for this tunnel/transport. Only applicable for CBC and CTR based encryption algorithms.

ESP Proposal DhGroup

Diffie-Hellman algorithm for IKE SA exchange for this tunnel, or none if not required.

In addition, this field enables the PFS (perfect forward secrecy) on the IKE Phase 2 negotiation.

Use Routed VPN

When enabled (checked), a tunnel interface is created (with name based on tunnel name parameter), and all traffic to be encrypted must be routed via that interface. Defaults to unchecked.

Note: When there is no user defined VRF, then this field is not displayed.
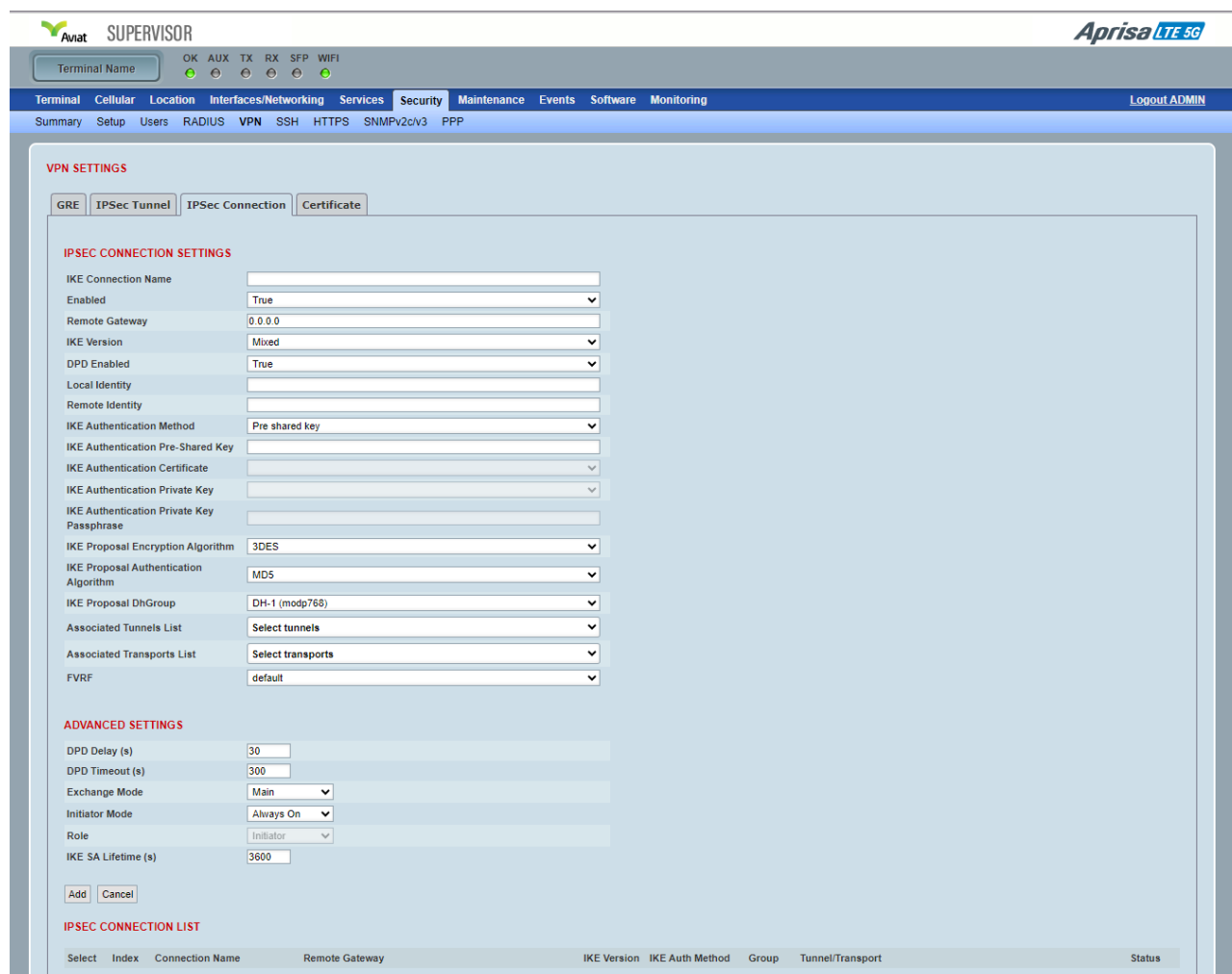
Inside VRF (IVRF)

This field is enabled when 'Use Routed VPN' is enabled. It specifies the VRF where packets inside the tunnel interface are routed to / from (the IVRF). If left blank, it uses the default VRF.

Note: The encapsulated packet VRF is controlled by the Source Interface parameter of 'IPsec Connection' page. In addition, when there is no user defined VRF, then this field is not displayed.

VPN > IPsec Connection

This page provides VPN IPsec connection configuration of the remote gateway address, and the algorithms used for authentication between gateways.

IPSEC CONNECTION SETTINGS

IKE Connection Name

Name of the IKE connection

Remote Gateway

The public IP address or FQDN of the gateway to establish a connection with. Use 0.0.0.0 if the remote end will initiate the connection, and any remote address may connect.

IKE Version

The protocol version to allow. IKEv1, IKEv2 or mixed, where IKEv2 is initiated, but can respond on either. The default value is mixed.

DPD Enabled

When enabled, messages are periodically sent to check that the remote gateway is still active. The default value is true.

Local/Remote Identity

How this IPsec gateway should be identified for authentication.

- If left blank it defaults to local/remote IP address used for IKE negotiation.
- If 'IKE Authentication Method' is configured as 'Pre Shared Key', the identity can be specified in format such as IP address (1.2.3.4), user FQDN (user@domain.com) or FQDN (domain.com) or any text value.
- If 'IKE Authentication Method' is configured as 'Certificate', the identity has to be confirmed by the certificate, such that it has to match the full subject DN or one of the subjectAltName extensions contained in the certificate.

Make sure the 'Local Identity' specified on this IPsec gateway is configured as 'Remote Identify' on remote IPsec gateway.

IKE Authentication Method

How the two gateways should authenticate each other. Either Pre-Shared Key (PSK) or Certificate. If certificate is chosen, ensure that a ROOT_CA certificate is uploaded that will verify the remote gateway. If more than one ROOT_CA certificate is uploaded, then only one of them need match to allow remote authentication.

IKE Authentication Pre-Shared Key

Shared secret if authentication method is "pre-shared-key". The shared secret should be same on both the IPsec gateways.

IKE Authentication Certificate

If authentication method is 'Certificate', select a Device Certificate previously uploaded on the Certificate page. This is used to identify this gateway to remote device.

IKE Authentication Private Key

The private key file that matches the certificate specified in 'IKE Authentication Certificate'.

IKE Authentication Private Key Passphrase

The passphrase to decrypt the private key file (if required).

IKE Proposal Authentication Algorithm

Authentication algorithm to be used during negotiation.

IKE Proposal Encryption Algorithm

Encryption algorithms to be used during negotiation.

IKE Proposal DhGroup

Diffie-Hellman group to be used during negotiation.

In addition, this field enables the PFS (perfect forward secrecy) on the IKE Phase 1 negotiation.

Associated Tunnels List / Associated Transport List

Select one or more tunnels configured in the Tunnel tab. Only tunnel mode, or only transport mode tunnels can be selected, not both types for the same connection.

ADVANCED SETTINGS

DPD Delay

Defines the interval between checking remote gateway. The default value is 30 seconds

DPD Timeout

Defines the timeout after which all connections to a peer are deleted. Applies only to IKEv1. Must be greater than DPD Delay. The default value is 300 seconds

Exchange mode

Main or Aggressive. Aggressive is faster (as less messages to establish connection) but is not recommended due to known security flaws. Only valid for IKEv1 or mixed connections.

Initiator mode

Always on: Immediately start key exchange when created, or at router startup. On Demand: Start key exchange when matching tunnel traffic detected. The default value is Always On

Role

Responder waits for connection from peer. Initiator initiates the connection.

IKE SA Lifetime

Specifies the number of seconds an IKE SA (security association) will live before expiring.

FVRF

The ISAKMP and ESP traffic that goes through any interface in this VRF (FVRF). The default setting is 'default VRF'.

VPN > Certificate

This page provides IPsec Certificate configuration provides the method to upload certificates for IPsec. These are then selected in the IPsec tunnel/connection pages when configuring.
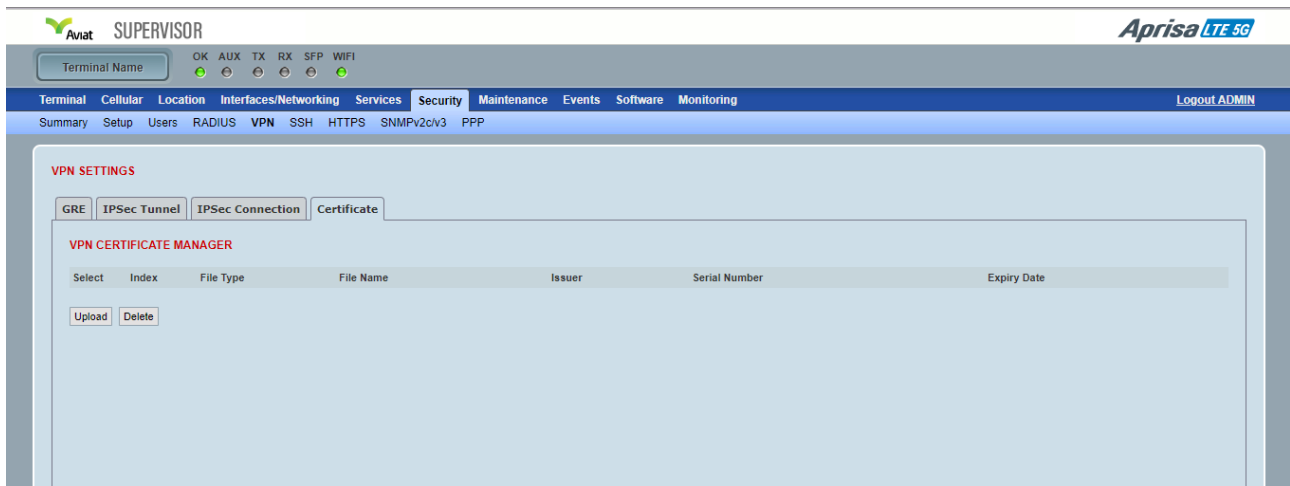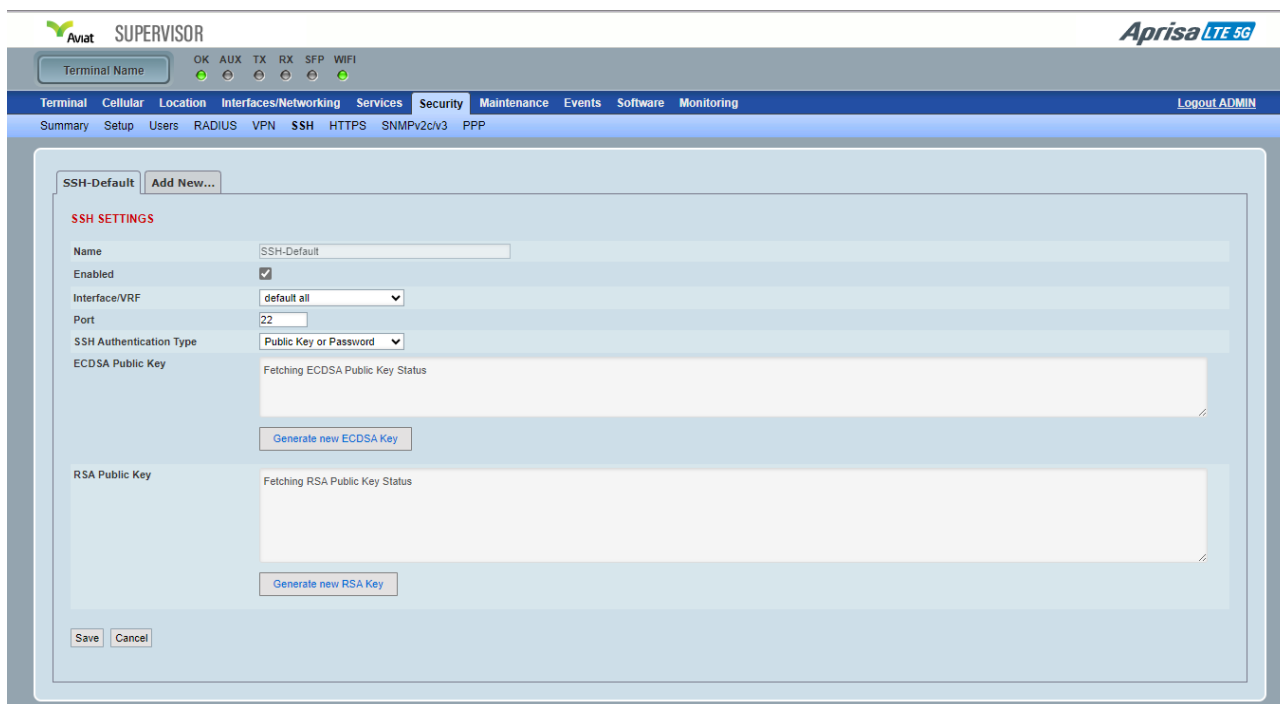
File Type

Option	Function
ROOT CA	This is a public key that identifies a root certificate authority and is used to verify the identity of a remote device.
Device Certificate	This is a public certificate that can be used as the identity of this device when communicating with a remote device. Requires a matching private key.
Device Private Key	This is a private key used for proving that this device identity matches the device certificate.

Security > SSH

This page provides configuration of the SSH settings.

Enabled

Sets if this SSH interface is enabled.

Interface/VRF

Listen only on the given interface or if unspecified on all interfaces.

Port

Specifies the listening port of the SSH interface.

SSH Authentication Type

This parameter sets the type of SSH Authentication. The default value is Public Key or Password

Option	Function
Public Key or Password	Allows a Public Key or Password for SSH Authentication.
Public Key	Allows only a Public Key for SSH Authentication.
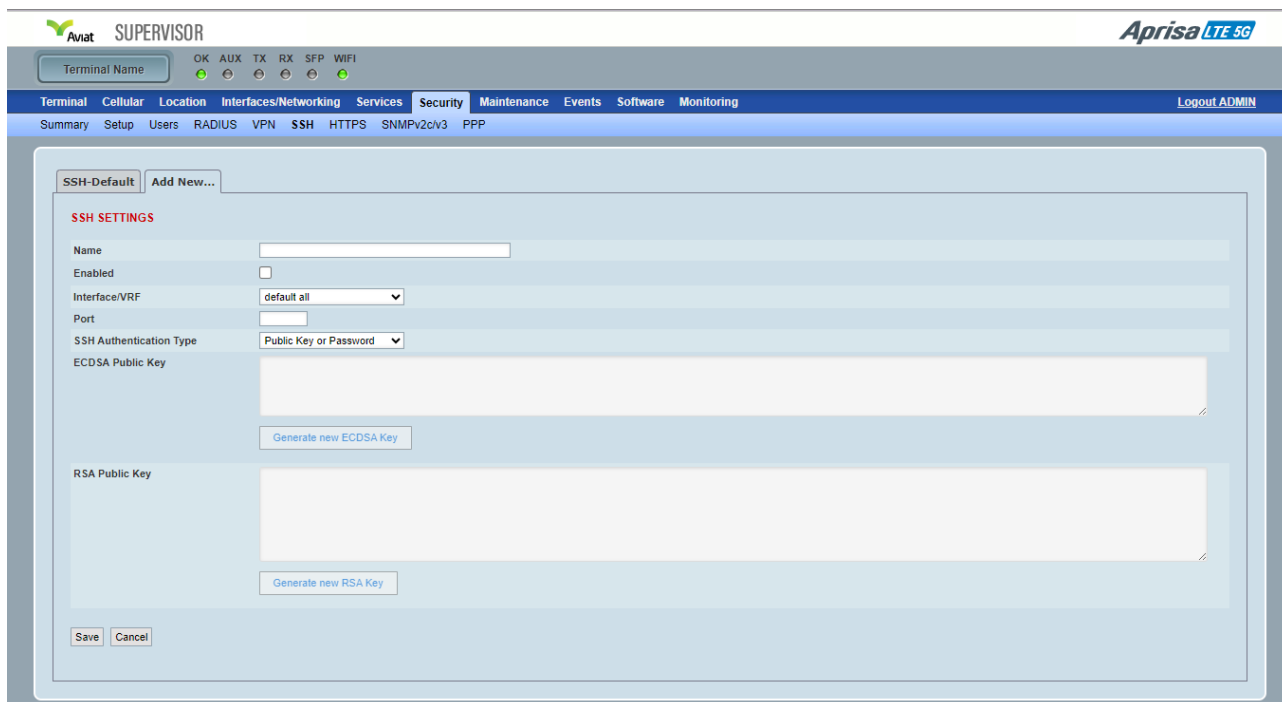
Generate ECDSA/RSA Key

Generates a new random private key for SSH server identity.

ECDSA/RSA Public key

This is the server identity. For extra security, users may configure their SSH client to only connect to servers with this identity.

Add a new SSH interface

As above

Security > HTTPS

This page provides HTTPS configuration.

HTTPS SETTINGS

HTTPS

Enables HTTPS operation.

HTTP Port Number

This parameter sets the HTTP Port Number. The default value is 80

HTTPS Port Number

This parameter sets the HTTPS Port Number. The default value is 443.

HTTPS CERTIFICATE MANAGER

Status

This shows the status of the HTTP Certificate e.g. 'Idle (Last Updated: 20/03/2020, 12:06:47, +13:00)'.
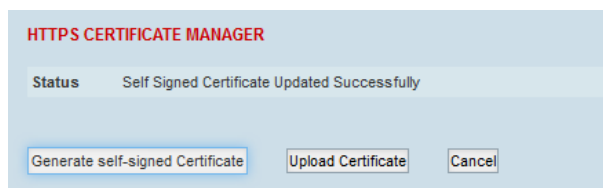
HTTPS CERTIFICATE DETAILS

Controls

Generate self-signed Certificate > Creates a self-signed certificate

Uploads a ZIP file containing a certificate and private key for use by the HTTP web server. The zip file must contain two files:

1.	certificate_name.crt	This must be a PEM format certificate
2.	certificate_name.key	A private key that was used to sign the .crt file

Any file name may be used – only the extension (.crt and .key) of the two files is important.

Allowed certificate algorithms are RSA (1024, 2048 or 4096 bit) or ECDSA (256 bit), with hashes of SHA-1, SHA-256, SHA-384 or SHA-512.
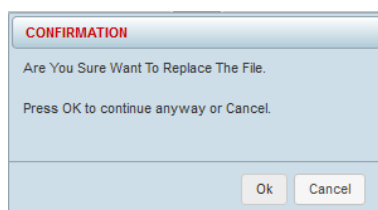
HTTPS CERTIFICATE DETAILS

Issuer

Shows the Issuer of the certificate e.g.Aviat Networks Ltd, Radio WEB Server

Serial Number

Shows the Serial Number of the certificate e.g. 3c4eecb046719ececdcba5c53f0f2faf86cf4e20
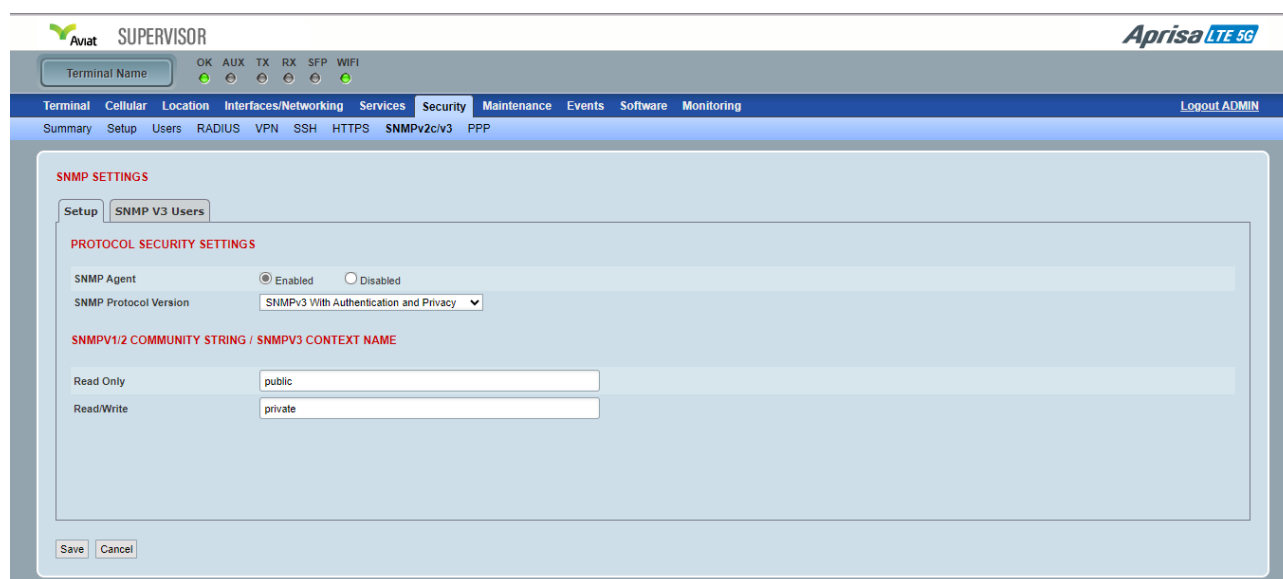
Expiry Date

Shows the Expiry Date of the certificate e.g. 13/03/2050

Security > SNMPv2/v3

This page provides SNMPv2/v3 configuration.

SNMPv2/v3 > Setup

PROTOCOL SECURITY SETTINGS

SNMP Agent

Enables SNMP agent.

SNMP Protocol Version

This parameter sets the SNMP Protocol Version. The default value is All Versions

Option	Function
All Version	Allows all SNMP protocol versions.
SNMPv3 Only	Only SNMPv3 transactions will be accepted.
SNMPv3 With Authentication Only	Only SNMPv3 transactions using authentication protocol (define in SNMPv3 users TAB) will be accepted.
SNMPv3 With Authentication and Privacy	Only SNMPv3 transactions using authentication and encryption protocol (define in SNMPv3 users TAB) will be accepted.
All Version	Allows all SNMP protocol versions.

ACCESS CONTROL SETUP

This section describes the SNMPv1/v2c Community String or the SNMPv3 Context Name as per the SNMP protocol version selected.
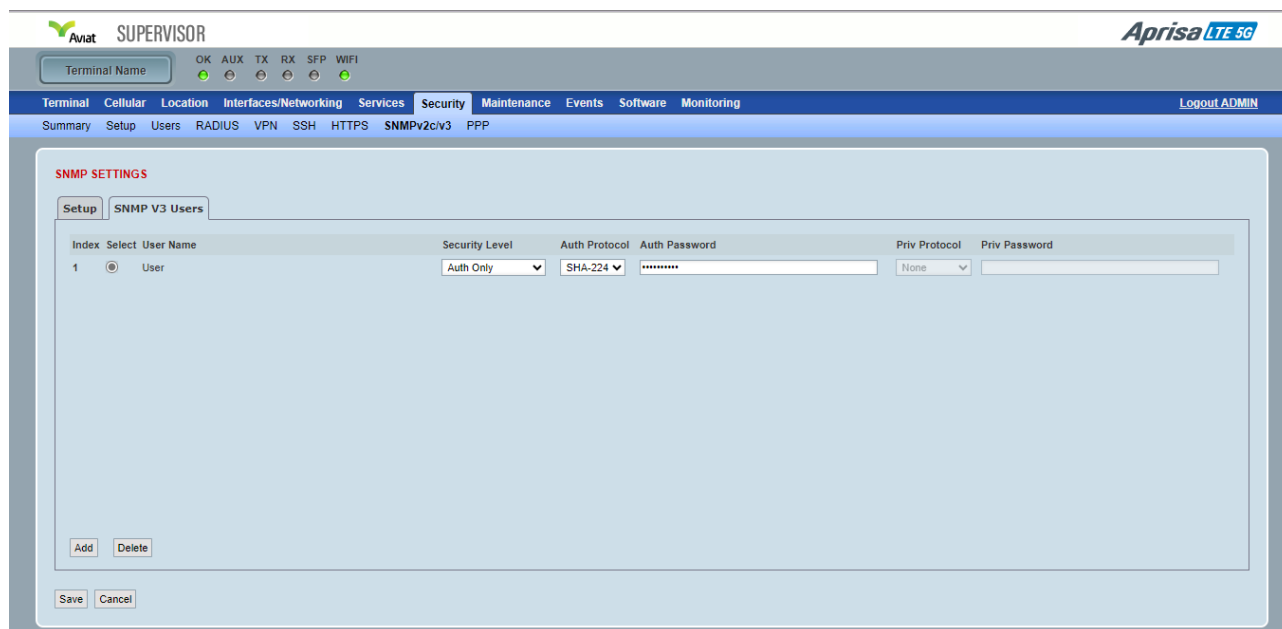
Read Only

This parameter sets the Community String when SNMPv1/v2c is used and Context Name when SNMPv3 is used for read only objects. The default value is public.

Read/Write

This parameter sets the Community String when SNMPv1/v2c is used and Context Name when SNMPv3 is used for read/write objects. The default value is private.

SNMPv2/v3 > SNMP V3 Users

User Name

This parameter sets the User Name which can be between 8 and 64 characters.

Security Level

Option	Function
None	No Security
Auth Only	Use secure SNMPv3 authentication protocol only
Auth And Priv	Use secure SNMPv3 authentication and privacy (encryption) protocols

Auth Protocol

Option	Function
None	No SNMPv3 authentication protocol selected to be used
MD5	MD5 authentication protocol is used with SNMPv3 transaction
SHA	SHA authentication protocol is used with SNMPv3 transaction
SHA-224	SHA-224 authentication protocol is used with SNMPv3 transaction
SHA-256	SHA-256 authentication protocol is used with SNMPv3 transaction
SHA-384	SHA-384 authentication protocol is used with SNMPv3 transaction
SHA-512	SHA-512 authentication protocol is used with SNMPv3 transaction

Auth Password

This parameter sets the Authentication protocol password which can be between 8 and 64 characters.

Priv Protocol
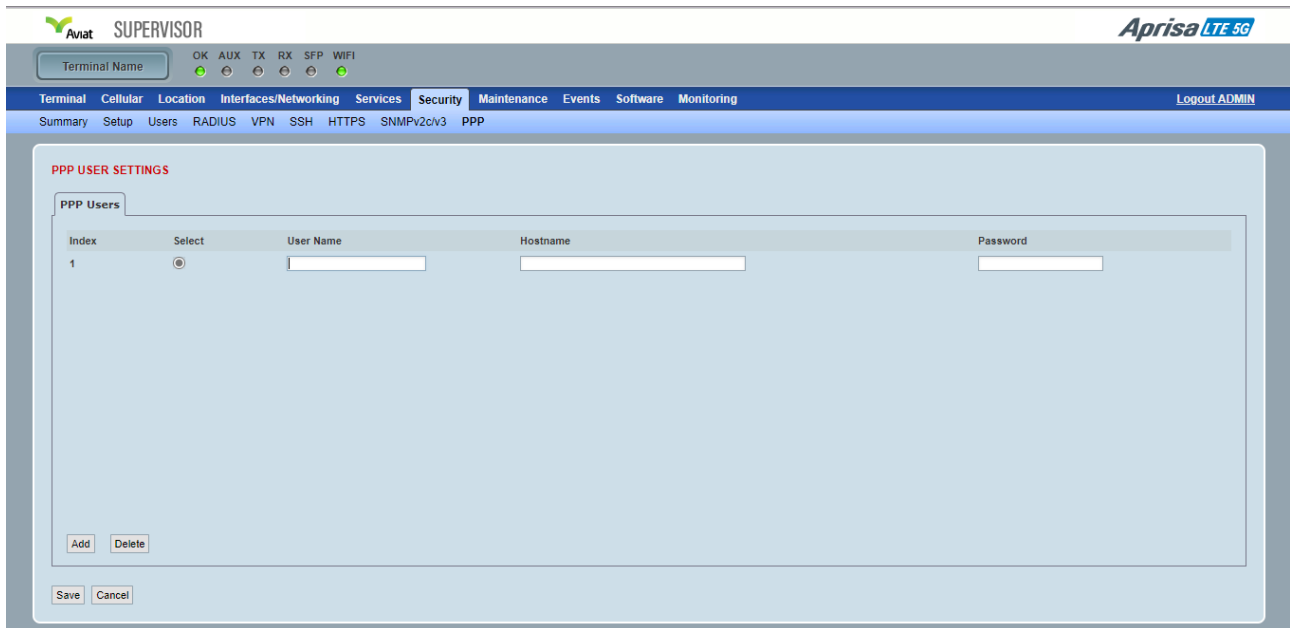
Option	Function
None	No SNMPv3 privacy (encryption) protocol selected to be used
DES	DES privacy (encryption) protocol is used with SNMPv3 transaction
AES-128	AES-128 privacy (encryption) protocol is used with SNMPv3 transaction
AES-192	AES-192 privacy (encryption) protocol is used with SNMPv3 transaction
AES-256	AES-256 privacy (encryption) protocol is used with SNMPv3 transaction

Priv Password

This parameter sets the Privacy (encryption) protocol password which can be between 8 and 64 characters.

Security > PPP

This page provides entry for PPP (Point-to-Point Protocol) users.

User Name

This parameter sets the PPP User Name.

The PPP User Name can be up to 32 characters but cannot contain special escape characters like back slash, forward slash, single quote, double quote, and space.

Host Name

This parameter sets the PPP Host Name.

The PPP Host Name can be up to 64 characters but cannot contain special escape characters like back slash, forward slash, single quote, double quote, and space.

Password

This parameter sets the PPP password.

The PPP password can be between 1 and 64 characters with no special characters' restriction.

Maintenance

Maintenance > General

This page controls the Aprisa LTE 5G reboot and reset to defaults.
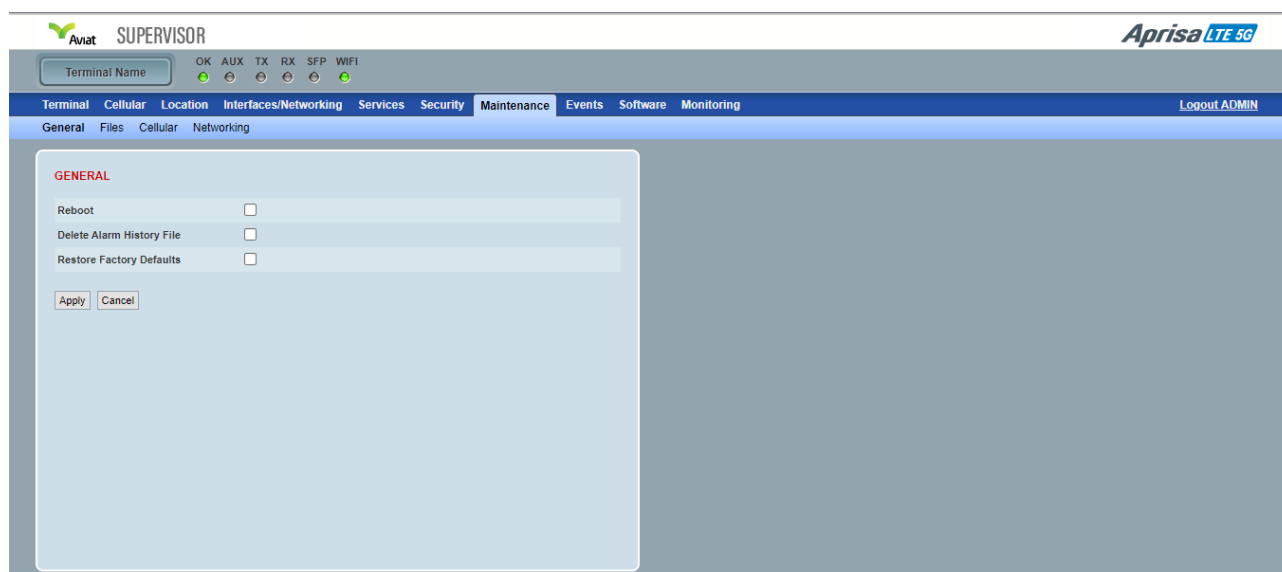
Reboot

Reboots the Aprisa LTE 5G software. Note this reboot is traffic affecting.

To reboot the Aprisa LTE 5G:

1. Tick the 'Reboot' checkbox.

2. Click 'Apply' to continue or 'Cancel' to abort.
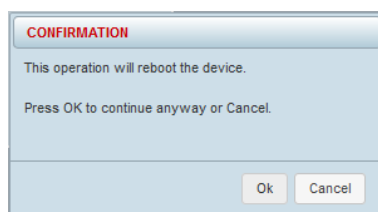
3. Click 'OK' to reboot the router or 'Cancel' to abort.

All the Aprisa LTE 5G LEDs will turn off except the OK LED.

The Aprisa LTE 5G will be operational again in about 10 seconds.

The Aprisa LTE 5G LEDs will light appropriately when the router is ready to operate.

4. Login to SuperVisor.

Delete Alarm History File

When activated, the alarm history will be deleted.

Restore Factory Defaults

When activated, all router parameters will be set to the factory default values. This includes resetting the router LAN IP address to the default of 192.168.4.1.

CONFIRMATION

Configuration will be restored to factory defaults.
This operation will reboot the device.

Press OK to continue anyway or Cancel.

Ok   Cancel
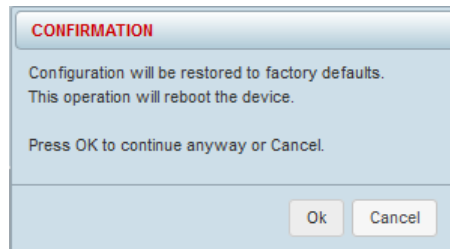
Note: Take care using this command.

Maintenance > Files

This page enables Aprisa LTE 5G configuration / log files to be saved to a PC.

MAINTENANCE FILES

There are four maintenance file types which can saved to your PC. The Configuration Settings can be restored from a previously saved config file:

Option	Function
Configuration Settings	Saved to and restored from PC Note: If the security level is set to Level 3 in 'Security > Setup' the config file will be encrypted and cannot be opened with regular compression applications.
Event Log History	Saved to a PC
GNSS Log	Saved to a PC
Support Information	Saved to a PC Note: If the security level is set to Level 3 in 'Security > Setup' the support file will be encrypted and cannot be opened with regular compression applications.

Include Keys and Passwords

When activated, encryption keys and passwords are included in the saved files.

File - Configuration Settings

This feature enables the configuration of a Aprisa LTE 5G to be saved to a file for configuration backup or for copying to another Aprisa LTE 5G, however the target Aprisa LTE 5G being restored must be operating on the same software version as the source Aprisa LTE 5G the configuration file was saved from e.g. if the configuration file was saved from a Aprisa LTE 5G operating on software version 1.0.0, it can only be restored to a Aprisa LTE 5G operating on software version 1.0.0.

Action
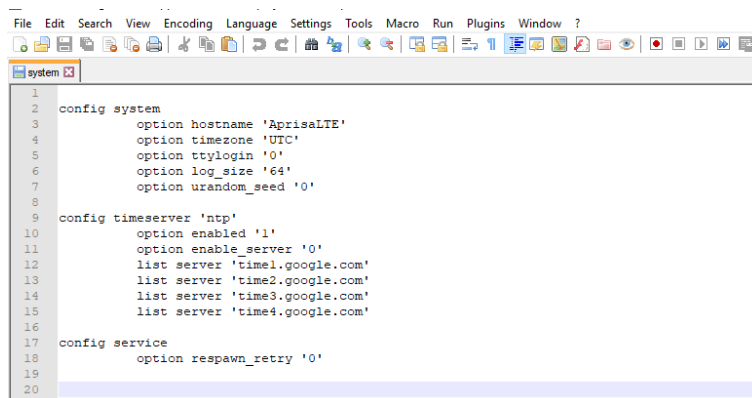
Action	Option
Save to PC	This saves the Configuration Settings with a filename of 'AprisaLTE-<serialnumber>-config.tar.gz' (for standard security) or 'AprisaLTE-<serialnumber>-config.tar.gz.enc' (for strong security) to your PC 'downloads' directory. If you wish to open the config file, check the security level is set to 'Level 1' in 'Security > Setup' on page 206.

To open the configuration file, perform the following steps:

1. Unzip the 'AprisaLTE-<serialnumber>-config.tar.gz' file with compression applications like WinZip or 7-ZIP to a new directory. It includes multiple configuration files for each configuration section of the LTE.
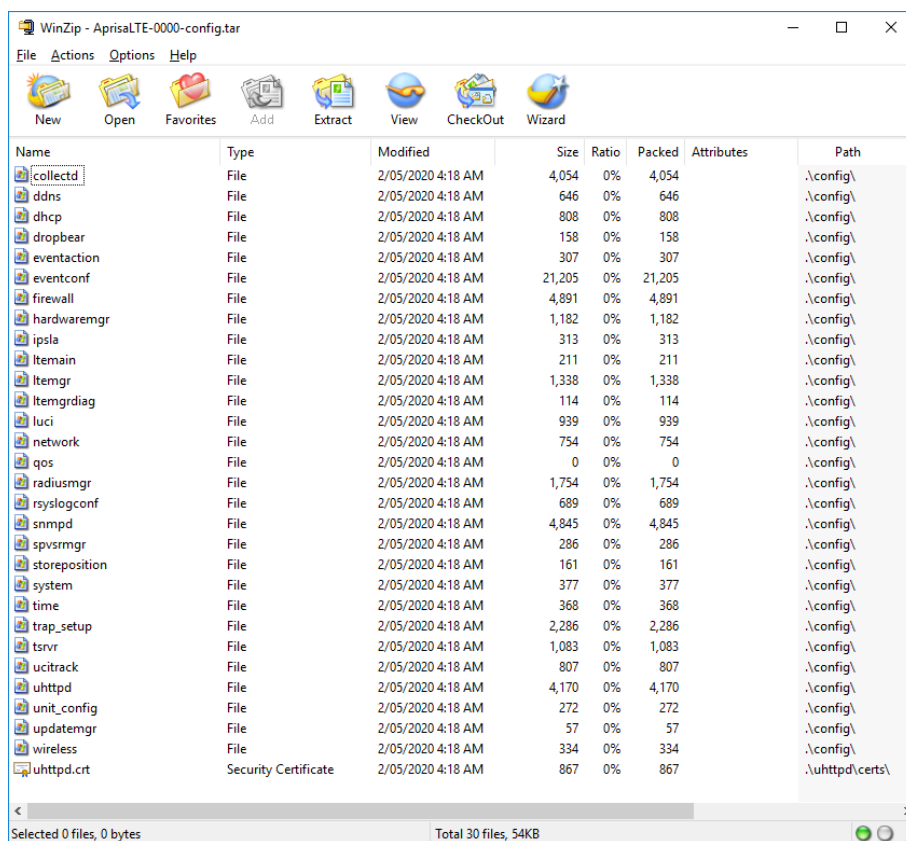
2. The files in the config path are all text files that can be viewed if required by right clicking on the file and using 'Open With' your text file editor. This is the 'System' file opened with Notepad ++.

```
File  Edit  Search  View  Encoding  Language  Settings  Tools  Macro  Run  Plugins  Window  ?

system

  1
  2   config system
  3           option hostname 'AprisaLTE'
  4           option timezone 'UTC'
  5           option ttylogin '0'
  6           option log_size '64'
  7           option urandom_seed '0'
  8
  9   config timeserver 'ntp'
 10           option enabled '1'
 11           option enable_server '0'
 12           list server 'time1.google.com'
 13           list server 'time2.google.com'
 14           list server 'time3.google.com'
 15           list server 'time4.google.com'
 16
 17   config service
 18           option respawn_retry '0'
 19
 20
```

Restore from PC	This restores all user configuration settings from a previously saved Aprisa LTE 5G Configuration Settings file.
	A reboot warning message will warn of a pending reboot after the PC file is selected. Clicking OK will open a browser file selection window to select the file.
	Note: If you are using Explorer, it must be IE10 or above for this feature to work correctly.

File - Event Log History

Action

Action	Option
Save to PC	This saves the Event Log History with a filename of 'AprisaLTE-<serialnumber>-logs.tar.gz' to your PC 'downloads' directory.

File - GNSS Log

Action

Action	Option
Save to PC	This saves the GNSS Log with a filename of 'AprisaLTE-<serialnumber>-gnsslogs.tar.gz' to your PC 'downloads' directory.
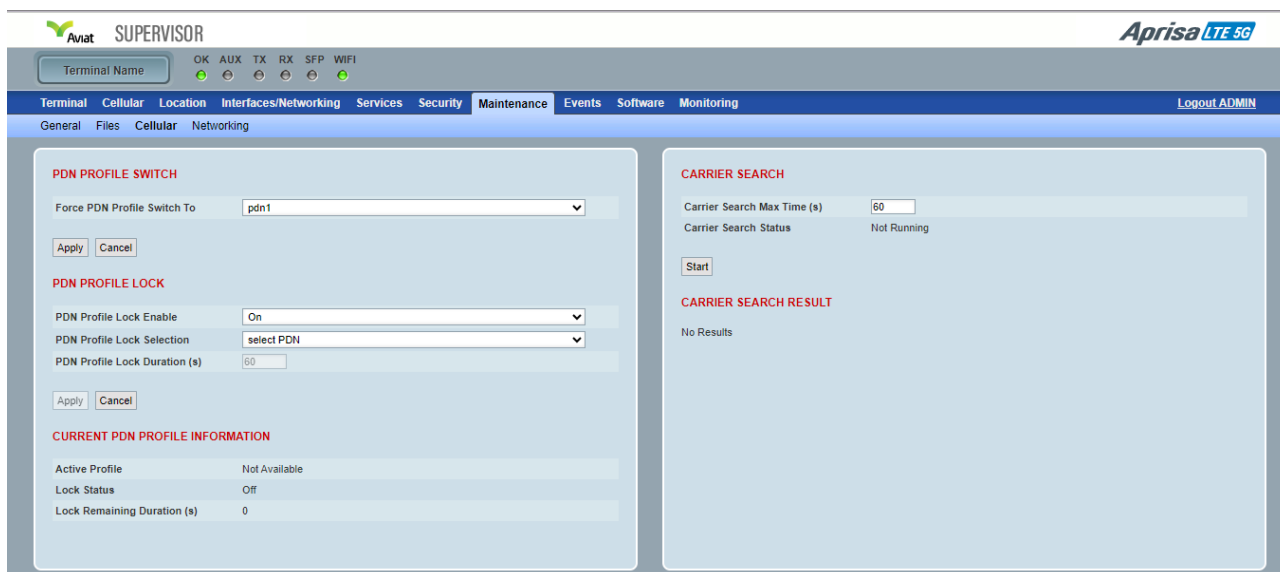
File - Support Information

Action

Action	Option
Save to PC	This saves the Support Information with a filename of 'AprisaLTE-<serialnumber>-support' (for Standard security) or 'AprisaLTE-<serialnumber>-support.enc' (for Strong security) to your PC 'downloads' directory. If you wish to open the support file, check the security level is set to 'Standard' in 'Security > Setup'.

Maintenance > Cellular

This page enables Cellular profile setup.

Force PDN Profile Switch To

Forces switch to the selected PDN. The PDN must be enabled in Cellular->General

PDN Profile Lock Enable

Setting	Function
On	Enables the PDN Profile Lock
Off	Disables the PDN Profile Lock
Timer	Enables the PDN profile lock for a specified duration

PDN Profile Lock Selection

Selects which PDN profile to lock.

PDN Profile Lock Duration

Locks the PDN for a specified duration if 'PDN Profile Lock Enable' is set to Timer.

Active Profile

Shows which PDN profile is currently active.

Lock Status

Shows if lock is enabled on current active PDN profile.

Lock Remaining Duration

How much time is left for active PDN to go back to unlock state.

Carrier Search Max Time (s)
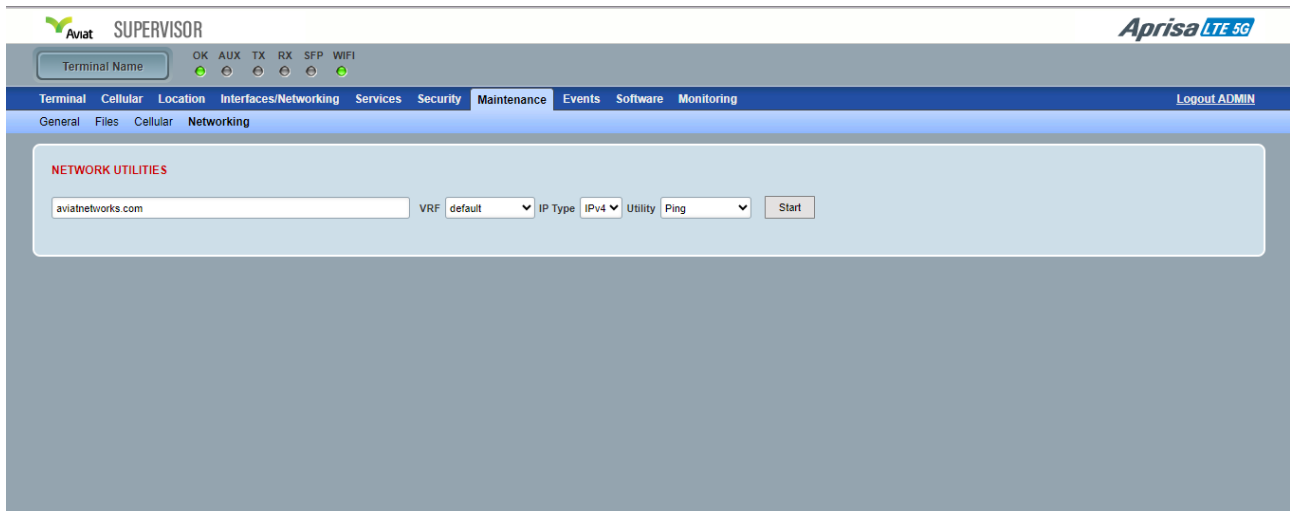
When Carrier search is started using the 'start' button then this time specifies the maximum time to scan for networks.

Carrier Search Status

Displays the status of the Carrier search.

Maintenance > Networking

This page contains networking utilities.

Address

Sends an ICMP or ICMPv6 echo request to the specified address.

VRF

Selects the VRF.

IP Type

Selects the IP Type; IPv4 or IPv6.

Utility

Setting	Function
Traceroute	Sends packets with gradually increasing TTL values, to discover the route that a packet takes to reach a destination. Note that many routers disable ICMP time exceeded messages, so not all intermediary hops will be discovered
Nslookup	Attempts to resolve the given domain name to an IP address using the configured and/or discovered DNS servers
Ping	Sends an ICMP or ICMPv6 echo request to the specified address
Advanced Ping	Sends an ICMP or ICMPv6 echo request to the specified address with the same IP SLA options. See more information on 'Routing > IP SLA' on page 189.

Events

The Events menu contains the setup and management of the alarms, alarm events and traps.

Events > Alarm Summary

There are two types of events that can be generated on the Aprisa LTE 5G. These are:

1. Alarm Events
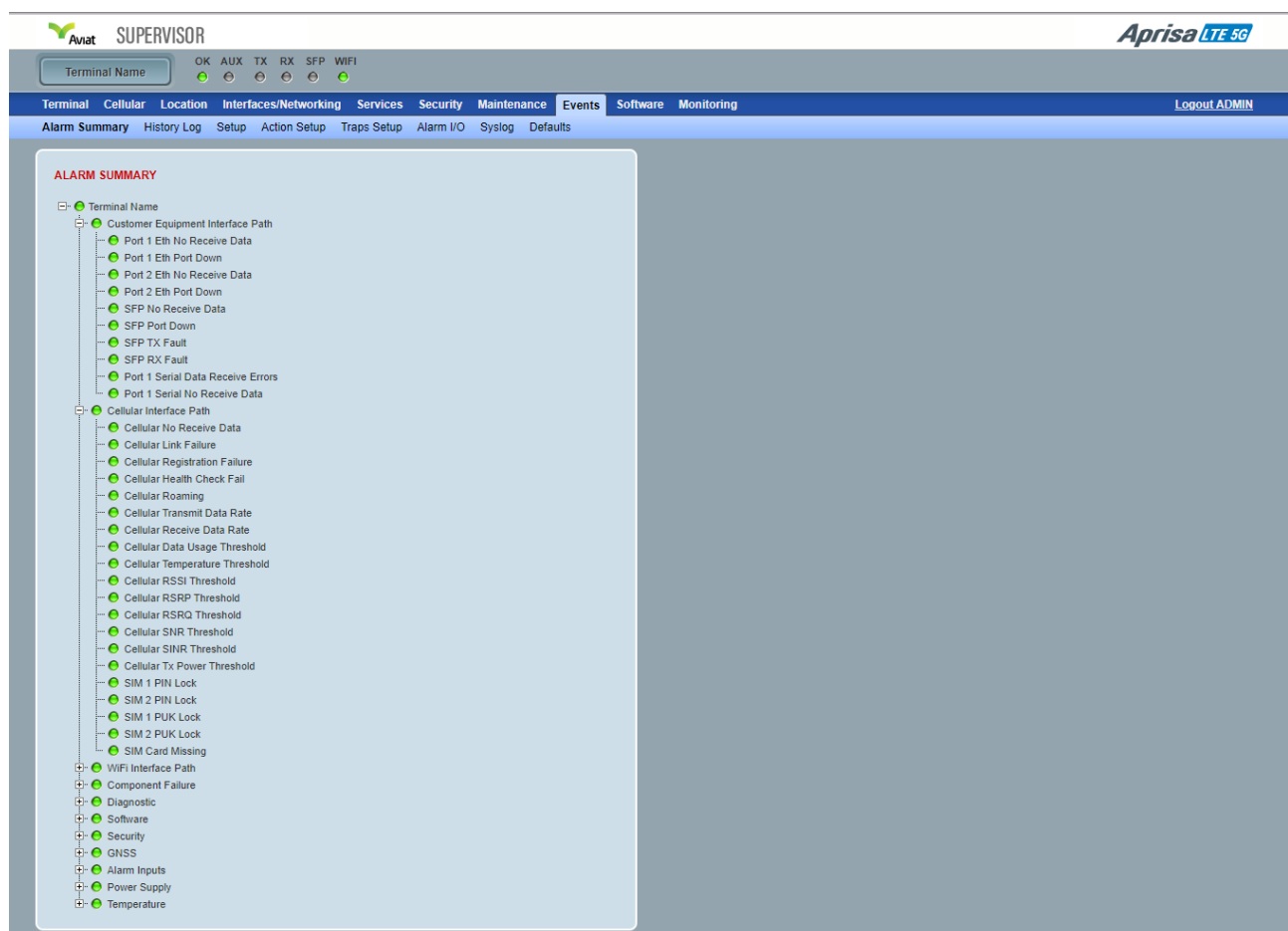
Alarm Events are generated to indicate a problem on the Aprisa LTE 5G.

2. Informational Events

Informational Events are generated to provide information on key activities that are occurring on the Aprisa LTE 5G. These events do not indicate an alarm on the Aprisa LTE 5G and are used to provide information only.

See 'Alarm Events' on page 311 for a complete list of events.

4G / 5G Modules

ALARM SUMMARY

The Alarm Summary is a display tree that displays the current states of all Aprisa LTE 5G alarms. The alarm states refresh automatically every 12 seconds.

LED Colour	Severity
Green	No alarm
Orange	Warning alarm
Red	Critical, major or minor alarm

Events > History Log

This page displays the log of all Alarm events.

EVENT HISTORY

The last 1500 events are stored in the Aprisa LTE 5G. The complete event history list can be downloaded to your PC (see 'File - Event Log History' on page 246).

The Event History can display the last 50 events stored in the Aprisa LTE 5G in blocks of 8 events.
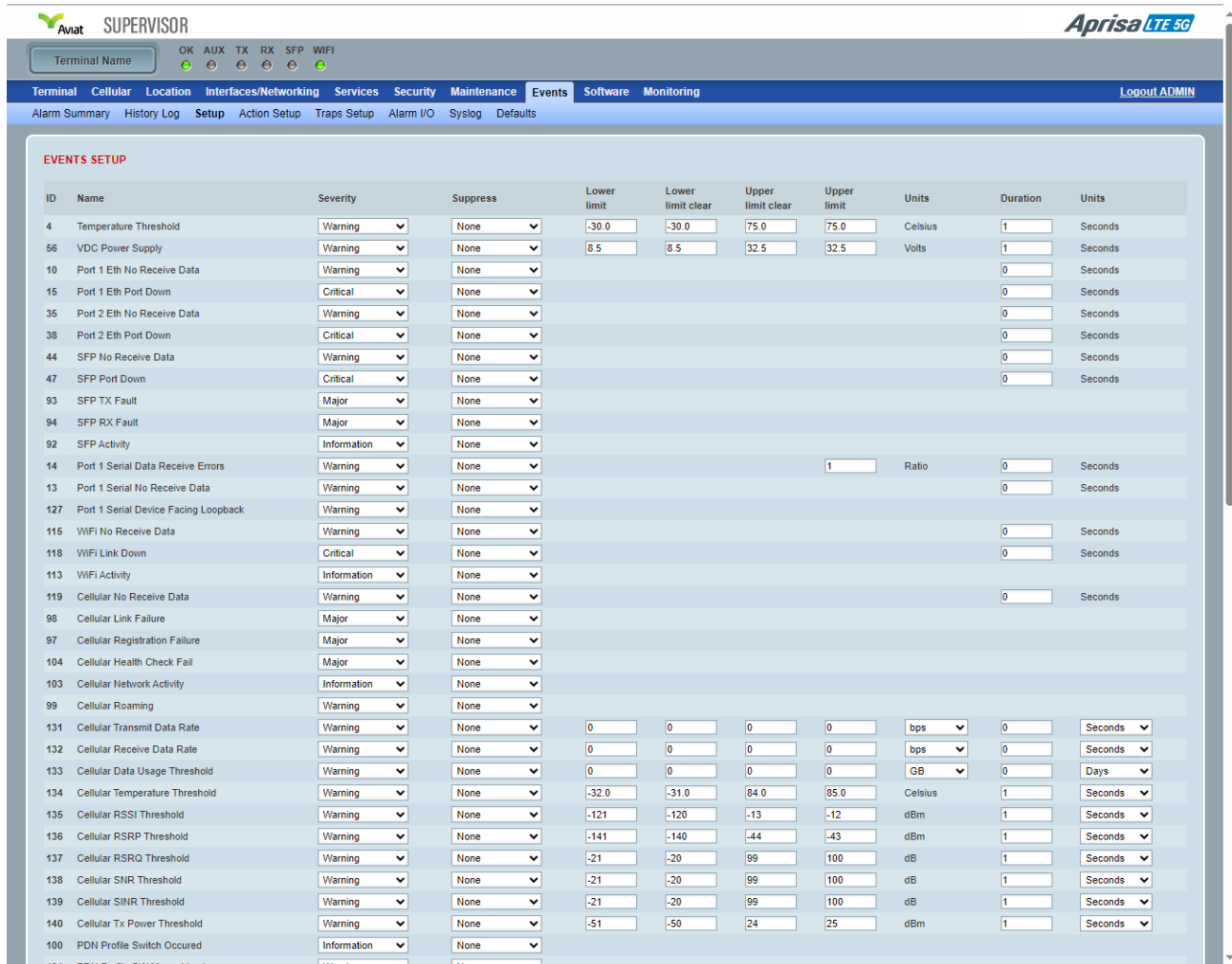
Auto Refresh

The Event History page selected will refresh automatically every 12 seconds if the Auto Refresh is ticked.

Events > Setup

This page allows alarm event parameters to be configured for all alarm events (see 'Alarm Events' on page 311).

4G / 5G Modules

EVENTS SETUP

All active alarms for configured alarm events will be displayed on the Monitoring pages (see 'Monitoring' on page 272).

Severity

The Severity parameter sets the alarm severity.

Severity	Function
Critical	The Critical severity level indicates that a service affecting condition has occurred and an immediate corrective action is required. Such a severity can be reported, for example, when a managed object becomes totally out of service and its capability must be restored.
Major	The Major severity level indicates that a service affecting condition has developed and an urgent corrective action is required. Such a severity can be reported, for example, when there is a severe degradation in the capability of the managed object and its full capability must be restored.

Severity	Function
Minor	The Minor severity level indicates the existence of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious (for example, service affecting) fault. Such a severity can be reported, for example, when the detected alarm condition is not currently degrading the capacity of the managed object.
Warning	The Warning severity level indicates the detection of a potential or impending service affecting fault, before any significant effects have been felt. Action should be taken to further diagnose (if necessary) and correct the problem in order to prevent it from becoming a more serious service affecting fault.
Information	No problem indicated – purely information

Suppress

This parameter determines if the action taken by an alarm.

Option	Function
None	Alarm triggers an event trap and is logged in the Aprisa LTE 5G
Traps	Alarm is logged in the Aprisa LTE 5G but does not trigger an event trap
Traps and Log	Alarm neither triggers an event trap nor is logged in the Aprisa LTE 5G

Lower Limit / Upper Limit

Threshold alarm events have lower and upper limit settings. The alarm is activated if the current reading is outside the limits.

Example: 4 Temperature Threshold

The Lower Limit is -30 C and the Upper Limit is 75 C. If the temperature exceeds 75 C, the alarm will activate.

Units (1)

The Units parameter shows the unit for the Lower Limit and Upper Limit parameters.

Duration

This parameter determines the period to wait before an alarm is raised if no data is received.
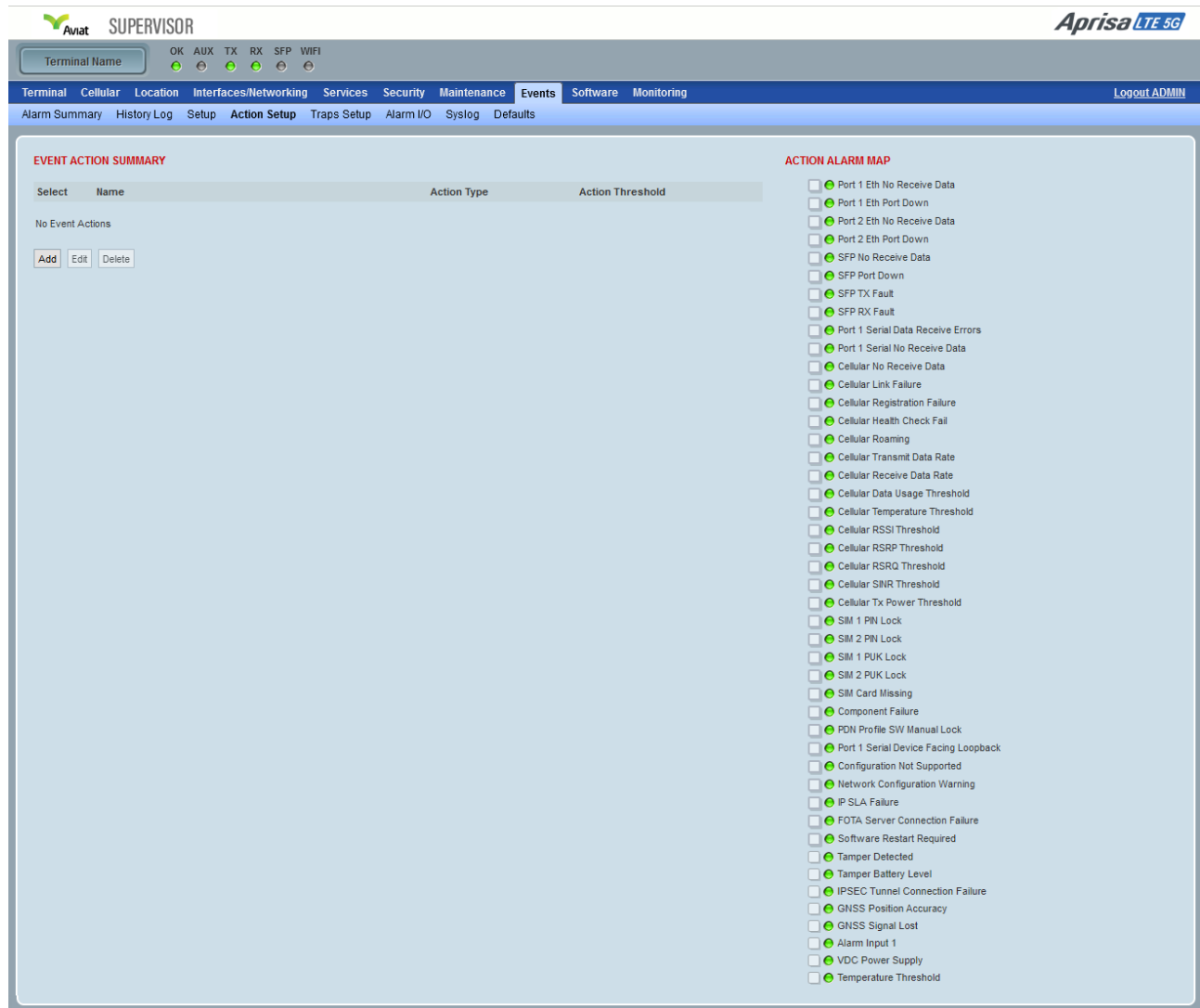
Units (2)

This parameter shows the unit for the Duration parameters.

Events > Action Setup

This page provides control of the mapping of events to specific actions. Specific alarm events can setup to trigger outputs.

4G / 5G Modules

EVENT ACTION SETUP

Action Type

This parameter sets the action type that will be activated on the Aprisa LTE 5G for the condition defined in Action Threshold Criteria.

Option	Function
None	This action setup does not activate any alarm output
Activate Alarm Output 1	This action setup activates alarm output 1
Hardware Reset	This action resets the Aprisa LTE 5G hardware

Action Threshold Criteria

This parameter sets the Aprisa LTE 5G event that will trigger the action output.

Option	Function
None	No action output.
Equal Critical	Activates the action output when an Aprisa LTE 5G alarm is critical alarm
Equal Major	Activates the action output when an Aprisa LTE 5G alarm is a major alarm
Equal Minor	Activates the action output when an Aprisa LTE 5G alarm is minor alarm
Equal Warning	Activates the action output when an Aprisa LTE 5G alarm is a warning alarm
Equal Cleared	Activates the action output when an Aprisa LTE 5G alarm is cleared
Equal or Worse than Major	Activates the action output when an Aprisa LTE 5G alarm is a major alarm or a critical alarm
Equal or Worse than Minor	Activates the action output when an Aprisa LTE 5G alarm is a minor alarm, a major alarm or a critical alarm
Equal or Worse than Warning	Activates the action output when an Aprisa LTE 5G alarm is a warning, a major alarm, a minor alarm or a critical alarm

Controls

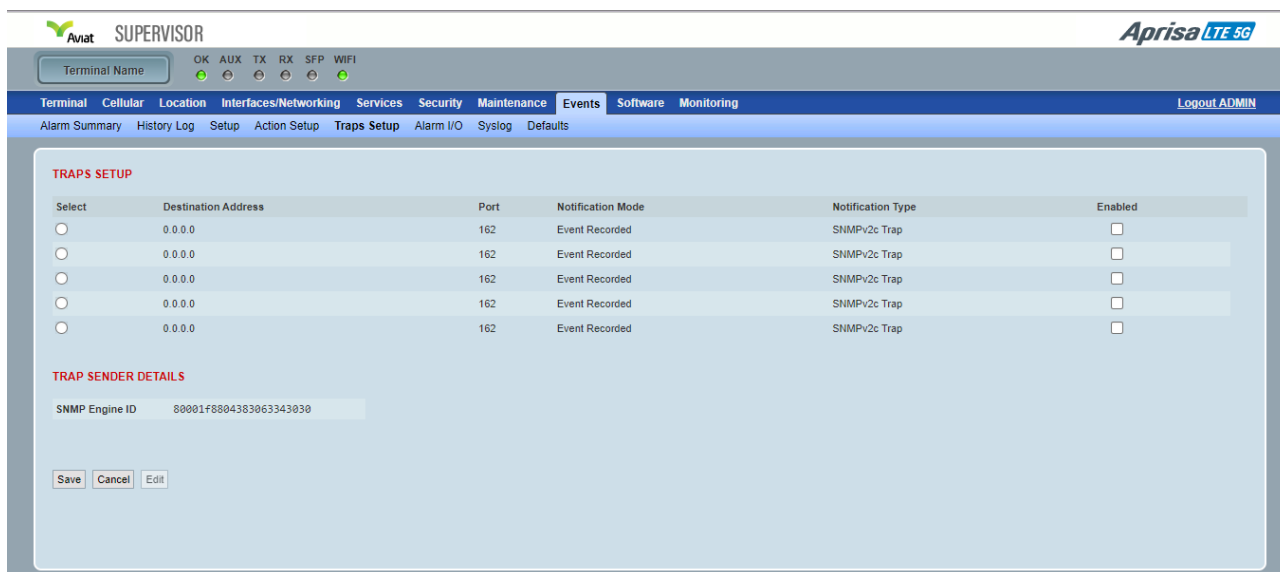The Save button saves the current event action setup.

The Cancel button cancels the new event action setup.

The Clear Map button clears all alarm selections on the current setup.

Events > Trap Setup

This page enables the setup of SNMP traps to capture Aprisa LTE 5G alarm events.
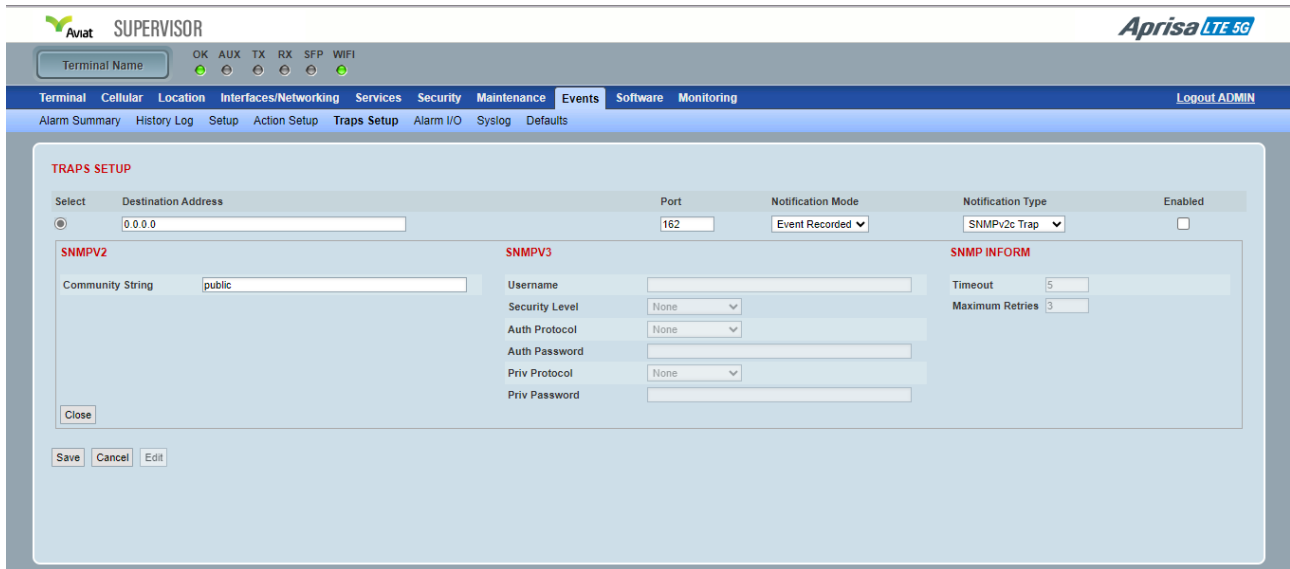
TRAPS SETUP

All events can generate SNMP traps. The types of traps that are supported are defined in the 'Notification Mode'.

Destination Address

This parameter sets the IP address of the server running the SNMP manager.

Port

This parameter sets the port number the server running the SNMP manager.

Community String

This parameter sets the community string which is sent with the IP address for security. The default community string is 'public'.

Notification Mode

This parameter sets when an event related trap is sent:

Option	Function
Event Recorded	When an event is recorded in the event history log, a trap is sent.
Event Updated	When an event is updated in the event history log, a trap is sent.
All Events	When an event is recorded or updated in the event history log, a trap is sent.

Notification Type

This parameter sets the type of event notification:

Option	Function
Standard Trap	Provides a standard SNMP trap event
Inform Request	Provides a SNMP v2 Inform Request trap event including trap retry and acknowledgement

Timeout (second)

This parameter sets the time interval to wait for an acknowledgement before sending another retry.

Maximum Retries

This parameter sets the maximum number of retries to send the event without acknowledgement before it gives up.

Enabled

This parameter determines if the entry is used.
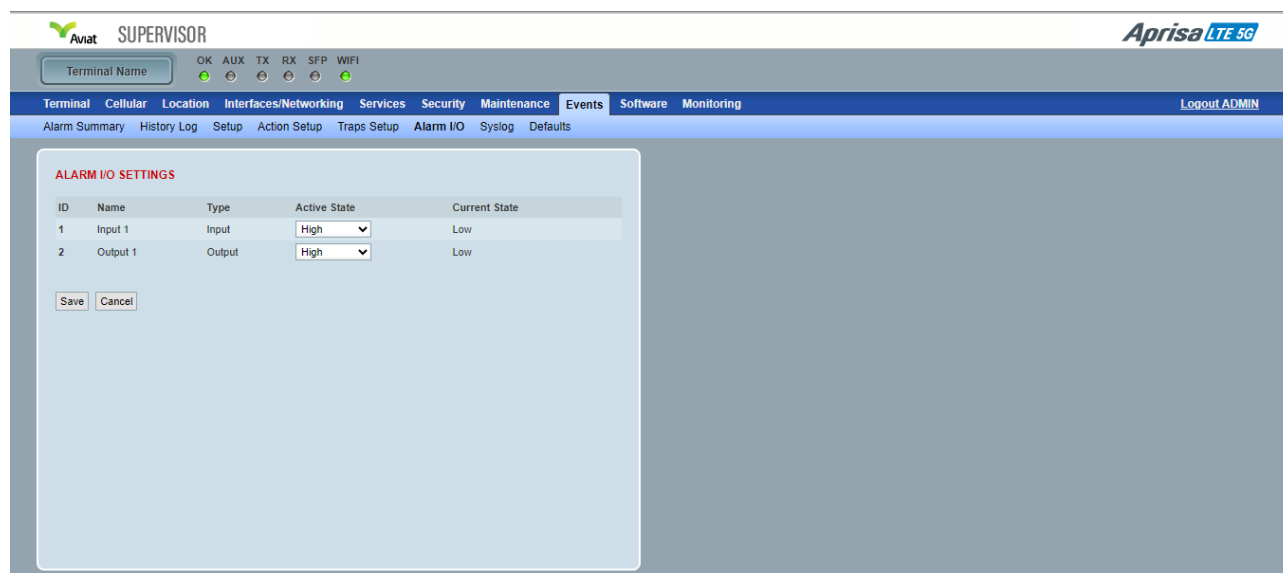
Events > Alarm I/O Setup

This page provides control of the hardware alarm input and hardware alarm output provided on the power connector.

The alarm inputs can be used for the following functions:

- Programmable ignition turn on and turn off
- Input sensing for externally triggered alarms

The alarm outputs can be used to interconnect to Aprisa SR and SR+ radio alarm inputs.

ALARM PORTS

Name

The alarm IO number.

Type

The Type shows if the alarm is an input or output.

Active State

The Active State parameter sets the alarm state when the alarm (or ignition input if that is enabled) is active.

Alarm Input

Option	Function
Low	The alarm is active low i.e. voltage less than 7 VDC, a grounded or open contact on the port will cause an active alarm state
High	The alarm is active high i.e. voltage higher than 10 VDC on the port will cause an active alarm state

Alarm Output

Option	Function
Low	The alarm is active low i.e. the active alarm state will generate a ground contact output
High	The alarm is active high i.e. the active alarm state will drive the output with the same voltage as the Aprisa LTE 5G supply input.

Current State

The Current State shows the current state of the alarm.

Events > Syslog

This menu allows configuring events that are recorded in the History Log, to also be sent to remote servers using the syslog protocol (compliant with RFC 5424). Messages from the Aprisa LTE 5G contain a MSG field with. Example message:

<13>1 2020-04-09T01:08:45+00:00 AprisaLTE - 14 5000 - {"logId":"449","timestamp":"2020-04-09T01:08:45+00:00","eventId":"24","auth":"0","eventName":"AlarmInput1","alarmStatus":"active","severity":"Warning","message":"Input 1 is Active"}

The MSG field contains json formatted fields that match the fields seen in the Events->History Log screen:

logId: Integer identifier

timestamp: The time the event occurred, in RFC3339 format

eventid: Integer identifier of the type of event. Identifiers are defined in the 4RF-EVENT MIB
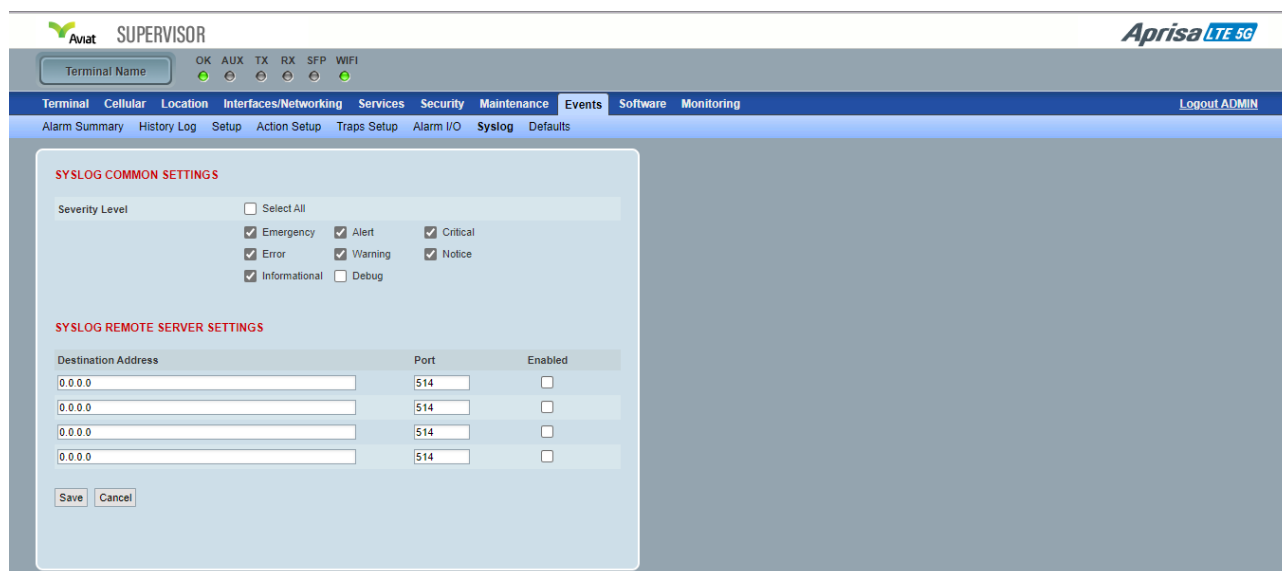
auth: 1 for authorization (login/logout) messages, 0 otherwise

eventName: String name of the event (maps to the eventid)

alarmStatus: State of the alarm (active or inactive)

severity: Can be Information, Warning, Minor, Major, or Cleared

message: Detailed description of the event and what caused it to occur

SYSLOG COMMON SETTINGS

Severity Level

The Severity Level selection options provide filtering of Syslog messages.

SYSLOG REMOTE SERVER SETTINGS

Destination Address

The IP address of the remote syslog server. May be IPv4 or IPv6 address.

Destination Port

The TCP/UDP port of the remote syslog server. Defaults to 514.

Enabled

Syslog messages are only sent to enabled servers.

Events > Defaults

This page enables the restoring of setup events back to factory defaults.
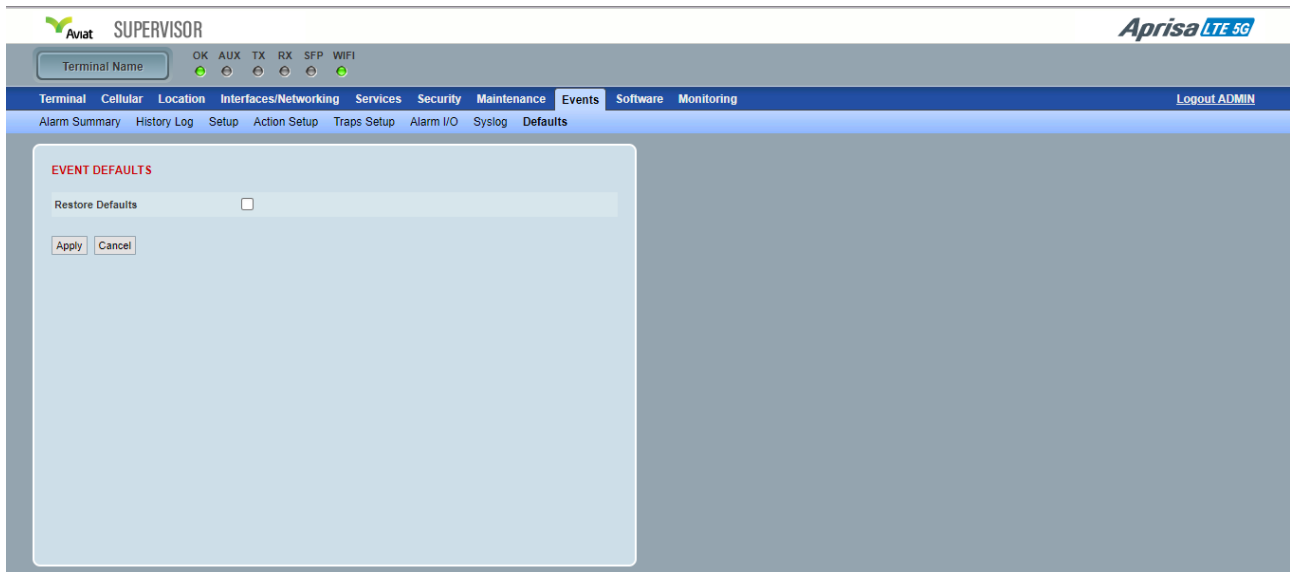
EVENT DEFAULTS
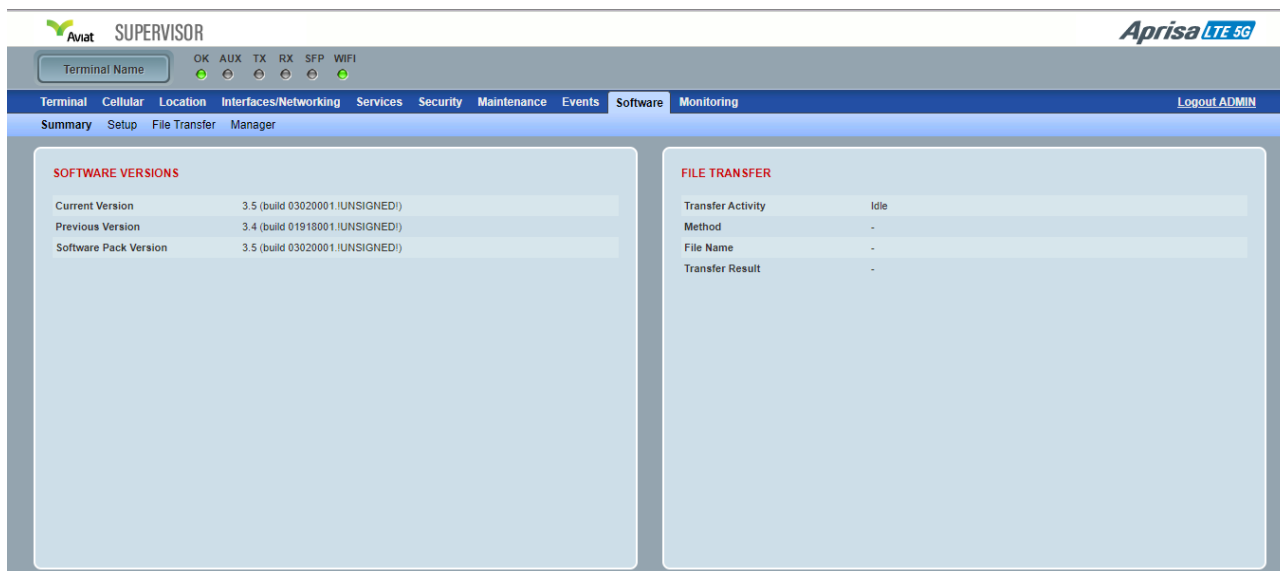
Restore Defaults

This parameter when activated restores all previously configured event parameters using 'Events > Setup' on page 253' to the factory default settings.

Software

Software > Summary

This page provides a summary of the software versions installed on the router, the setup options and the status of the File Transfer

SOFTWARE VERSIONS

Current Version

This parameter displays the software version running on the router.

Previous Version

This parameter displays the software version that was running on the router prior to the current software being activated.

Software Pack Version

This parameter displays the software that has been uploaded to the router and is ready for activation.

FILE TRANSFER

Transfer Activity

This parameter shows the status of the transfer, 'Idle', 'In Progress' or 'Completed'.

Method

This parameter shows the file transfer method e.g. HTTPS

File
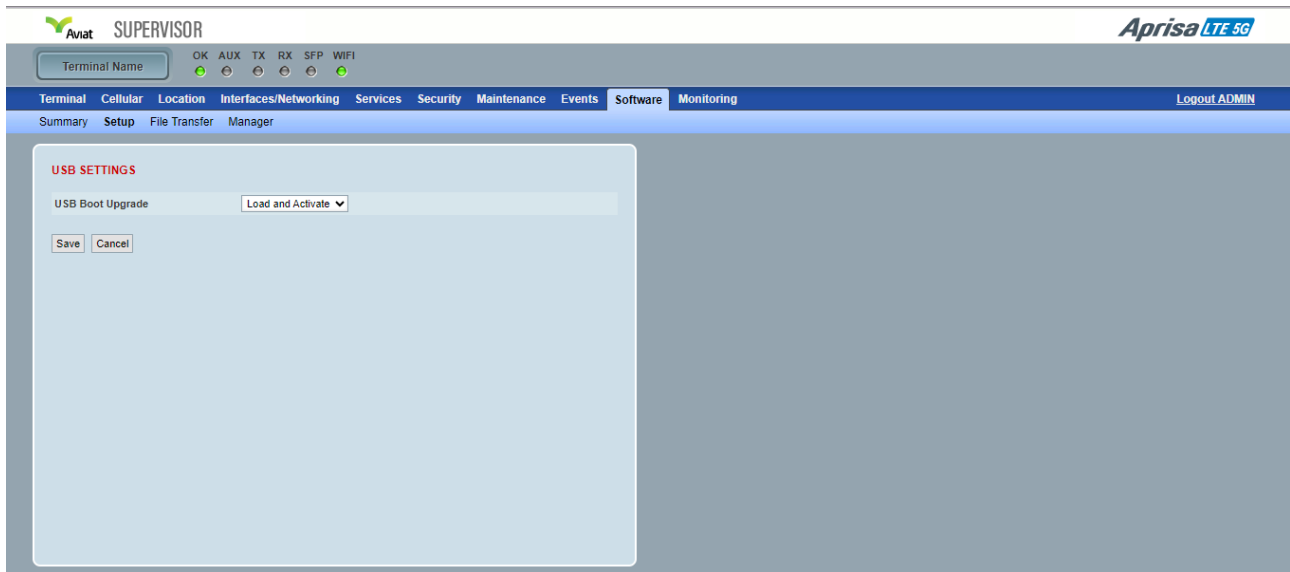
This parameter shows the software file source.

Transfer Result

This parameter shows the progress of the transfer.

Software > Setup

This page provides the setup of the USB flash drive containing a Software Pack.

USB SETUP
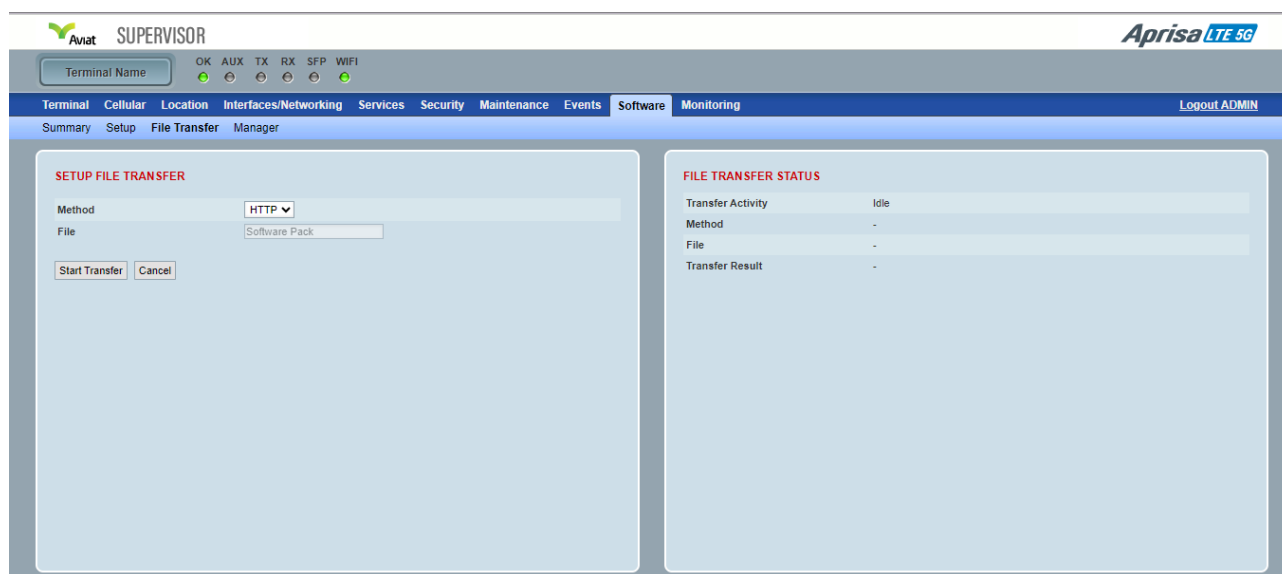
USB Boot Upgrade

This parameter determines the action taken when the router detects a USB flash drive in the Host port, either at power on, or when inserted at any time. The default setting is 'Load Only'.

Option	Function
Load and Activate	New software will be loaded from a USB flash drive in to the Aprisa LTE 5G and activated automatically.
Load Only	New software will be loaded from a USB flash drive in to the Aprisa LTE 5G. The software will need to be manually activated (see 'Software > Manager' on page 270).
None	Software will not be loaded from a USB flash drive into the Aprisa LTE 5G.

Software > File Transfer

This page provides the mechanism to transfer new software from a file source into the router.

SETUP FILE TRANSFER

Method

This parameter sets the method of file transfer.

Option	Function
HTTP / HTTPS	Transfers the software pack file (4nu) from a PC to the LTE.

File

This parameter shows the software file source.

FILE TRANSFER STATUS

Transfer Activity

This parameter shows the status of the transfer, 'Idle', 'In Progress' or 'Completed'.

Method

This parameter shows the file transfer method.

File

This parameter shows the software file source.

Transfer Result

This parameter shows the progress of the transfer:

Transfer Result	Function
Starting Transfer	The transfer has started but no data has transferred.
In Progress (x %)	The transfer has started and has transferred x % of the data.
Successful	The transfer has finished successfully.
File Error	The transfer has failed.
Verification Failed	The transfer was completed, but the file was not valid. Check that the file uploaded was an Aprisa LTE 5G software upgrade file.

Note: To check that the Aprisa LTE 5G software upgrade file (4nu) is valid, obtain the checksum (sha1) file for that software release contained in the Software Release zip file on the Aviat Networks website https://www.Aviat Networks.com.

On windows open a command prompt and type 'certutil -hashfile <updatefile>.4nu SHA1'. Next open the sha1 file in a text editor such as notepad and confirm the hashes match.
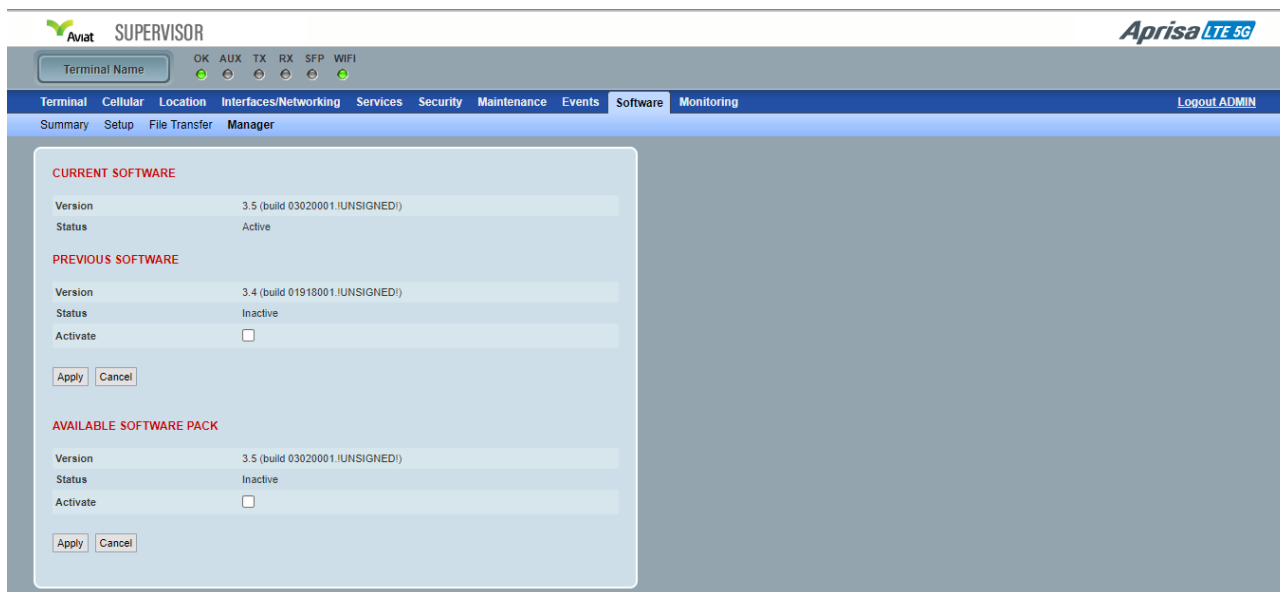
On linux type 'sha1sum -c <updatefile>.sha1' and check that the output contains 'OK'.

Software > Manager

This page summarizes and manages the software versions available in the router.

The manager is predominantly used to activate new software on the Aprisa LTE 5G.

Both the previous software (if available) and Software Pack versions can be activated on the device from this page.

CURRENT SOFTWARE

Version

This parameter displays the software version running on the device.

Status

This parameter displays the status of the software version running on the device (always active).

PREVIOUS SOFTWARE

Version

This parameter displays the software version that was running on the device prior to the current software being activated.

Status

This parameter displays the status of the software version that was running on the device prior to the current software being activated (always inactive).

Activate

This parameter activates the previous software version (restores to previous version).

The device will automatically reboot after activation.

AVAILABLE SOFTWARE PACK

Version

This parameter displays the software pack version available.

Status

This parameter displays the status of the software pack version.

Option	Function
Available	The software pack is available for use.
Activating	The software pack is activating in the device.
Unavailable	There is no software pack loaded into the device.

Activate

This parameter activates the software pack.

The device will automatically reboot after activation.

To activate a software version:

1. Tick the software version required to be activated (previous software or software pack).

2. Click 'Apply'.

The page will display a Status of 'Activating'.

Once started, activation cannot be cancelled.
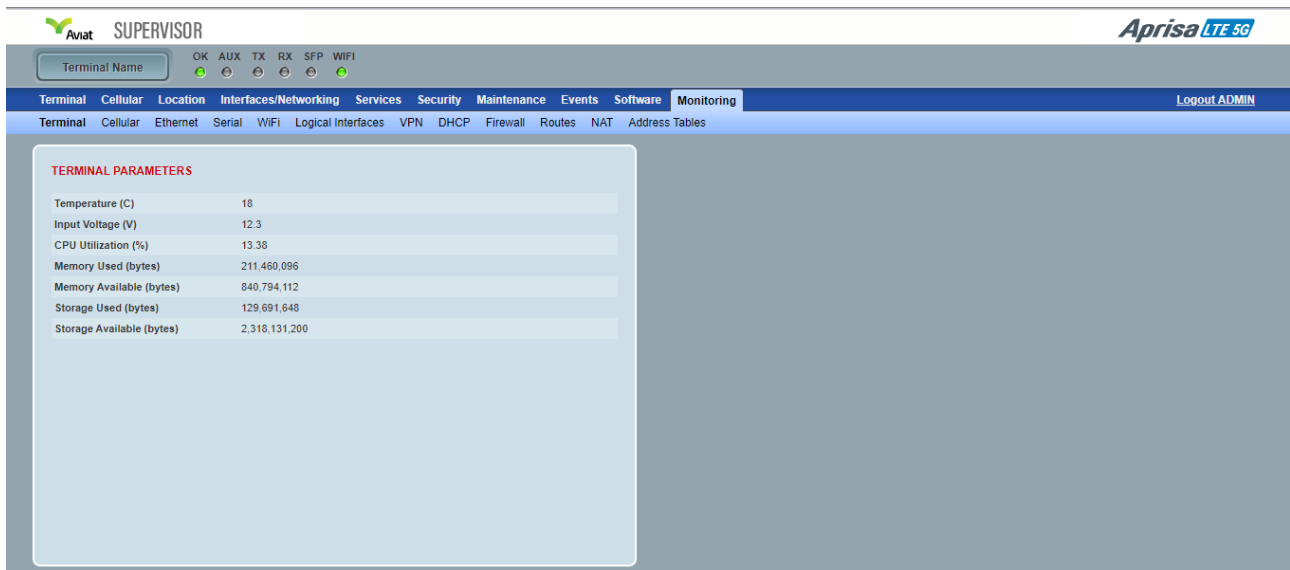
When the activation is completed, the device will reboot. This will cause the current SuperVisor session to expire.

3. Login to SuperVisor to check the result.

Monitoring

Monitoring > Terminal

This page displays the device diagnostic parameters.

Monitored Parameter	Function	Normal Operating Limits
Temperature (Celsius)	Parameter to show the device internal temperature	–30 to +70 ˚C (–30 to +158 ˚F)
Input Voltage (V)	Parameter to show the current power supply input voltage	10 to 30 VDC
CPU Utilization (%)	Parameter to show the current CPU utilization	0 to 100 %
Memory Used (bytes)	Parameter to show the current system memory used	
Memory Available (bytes)	Parameter to show the current system memory available	
Storage Used (bytes)	Parameter to show the current storage memory that has been used	
Storage Available (bytes)	Parameter to show the current storage memory that is available	

Monitoring > Cellular

This page displays the device Aprisa LTE 5G parameters

4G Modules

Monitored Parameter	Function	Normal Operating Lower Limit	Normal Operating Upper Limit
Modem Temperature (Celsius)	Parameter to show the modem internal temperature	–30˚C (–30˚F)	70 ˚C (+158 ˚F)
Current RSSI (dBm)	Parameter to show the current Received Signal Strength Indicator (RSSI) of the MAIN input	-121 dBm	-12 dBm
Current RSRP (dBm)	Parameter to show the current Reference Signal Received Power (RSRP) of the MAIN input	-156 dBm	-31 dBm
Current RSRQ (dB)	Parameter to show the current Reference Signal Received Quality (RSRQ) of the MAIN input	-20 dB	-3 dB
Current SNR (dB)	Parameter to show the current Signal to Noise Ratio (SNR) of the MAIN input		
Current SINR (dB)	Parameter to show the current Signal to Interference & Noise Ratio (SINR) of the MAIN input	-21 dB	50 dB
Last TX Power (dBm)	Parameter to show the actual transmitter power in dBm. The value is stored from the last time the transmitter was active and transmitted a packet	-51 dBm	28 dBm
TX Data Rate	Parameter to show the TX data rate in kbps		
TX Packets	Parameter to show the total number of packets transmitted by modem (includes multicast/broadcast packets)		
TX Bytes	Parameter to show the total number of bytes transmitted by modem		
TX Dropped Packets	Parameter to show the total number of transmit packets dropped by modem (includes multicast/broadcast packets)		

Monitored Parameter	Function	Normal Operating Lower Limit	Normal Operating Upper Limit
RX Data Rate	Parameter to show the RX data rate in kbps		
RX Packets	Parameter to show the total number of packets received by modem (includes multicast/broadcast packets)		
RX Bytes	Parameter to show the total number of bytes received by modem		
RX Multicast Packets	Parameter to show the number of received packets that are multicast		
RX Dropped Packets	Parameter to show the total number of receive packets dropped by modem (includes multicast/broadcast packets)		

4G / 5G Modules

Monitored Parameter	Function	Normal Operating Lower Limit	Normal Operating Upper Limit
Modem Temperature (Celsius)	Parameter to show the modem internal temperature	–30˚C (–30˚F)	70 ˚C (+158 ˚F)
Current 4G RSSI (dBm)	Parameter to show the current Received Signal Strength Indicator (RSSI) of the 4G Main input	-121 dBm	-12 dBm
Current 4G RSRP Main (dBm)	Parameter to show the current Reference Signal Received Power (RSRP) of the 4G Main input	-156 dBm	-31 dBm
Current 4G RSRQ Main (dB)	Parameter to show the current Reference Signal Received Quality (RSRQ) of the 4G Main input	-20 dB	-3 dB
Current 4G SINR Main (dB)	Parameter to show the current Signal to Interference & Noise Ratio (SINR) of the 4G Main input	-21 dB	50 dB
Current 4G RSRP Diversity (dBm)	Parameter to show the current Reference Signal Received Power (RSRP) of the 4G Diversity input	-156 dBm	-31 dBm
Current 4G RSRQ Diversity (dB)	Parameter to show the current Reference Signal Received Quality (RSRQ) of the 4G Diversity input	-20 dB	-3 dB
Current 4G RSRP MIM01 (dBm)	Parameter to show the current Reference Signal Received Power (RSRP) of the 4G MIM01 input	-156 dBm	-31 dBm
Current 4G RSRQ MIM01 (dB)	Parameter to show the current Reference Signal Received Quality (RSRQ) of the 4G MIM01 input	-20 dB	-3 dB

Monitored Parameter	Function	Normal Operating Lower Limit	Normal Operating Upper Limit
Current 4G RSRP MIM02 (dBm)	Parameter to show the current Reference Signal Received Power (RSRP) of the 4G MIM02 input	-156 dBm	-31 dBm
Current 4G RSRQ MIM02 (dB)	Parameter to show the current Reference Signal Received Quality (RSRQ) of the 4G MIM02 input	-20 dB	-3 dB
Current 5G RSSI (dBm)	Parameter to show the current Received Signal Strength Indicator (RSSI) of the 5G Main input	-121 dBm	-12 dBm
Current 5G RSRP Main (ANT 0) (dBm)	Parameter to show the current Reference Signal Received Power (RSRP) of the 5G Main (ANT 0) input	-156 dBm	-31 dBm
Current 5G RSRQ Main (ANT 0) (dB)	Parameter to show the current Reference Signal Received Quality (RSRQ) of the 5G Main (ANT 0) input	-20 dB	-3 dB
Current 5G SINR Main (ANT 0) (dB)	Parameter to show the current Signal to Interference & Noise Ratio (SINR) of the 5G Main (ANT 0) input	-21 dB	50 dB
Current 5G RSRP Diversity (ANT 2) (dBm)	Parameter to show the current Reference Signal Received Power (RSRP) of the 5G Diversity (ANT 2) input	-156 dBm	-31 dBm
Current 5G RSRQ Diversity (ANT 2) (dB)	Parameter to show the current Reference Signal Received Quality (RSRQ) of the 5G Diversity (ANT 2) input	-20 dB	-3 dB
Current 5G SINR Diversity (ANT 2) (dB)	Parameter to show the current Signal to Interference & Noise Ratio (SINR) of the 5G Diversity (ANT 2) input	-21 dB	50 dB
Current 5G RSRP MIM01 (ANT 1) (dBm)	Parameter to show the current Reference Signal Received Power (RSRP) of the 5G MIM01 (ANT 1) input	-156 dBm	-31 dBm
Current 5G RSRQ MIM01 (ANT 1) (dB)	Parameter to show the current Reference Signal Received Quality (RSRQ) of the 5G MIM01 (ANT 1) input	-20 dB	-3 dB
Current 5G SINR MIM01 (ANT 1) (dB)	Parameter to show the current Signal to Interference & Noise Ratio (SINR) of the 5G MIM01 (ANT 1) input	-21 dB	50 dB
Current 5G RSRP MIM02 (ANT 3) (dBm)	Parameter to show the current Reference Signal Received Power (RSRP) of the 5G MIM02 (ANT 3) input	-156 dBm	-31 dBm
Current 5G RSRQ MIM02 (ANT 3) (dB)	Parameter to show the current Reference Signal Received Quality (RSRQ) of the 5G MIM02 (ANT 3) input	-20 dB	-3 dB
Current 5G SINR MIM02 (ANT 3) (dB)	Parameter to show the current Signal to Interference & Noise Ratio (SINR) of the 5G MIM02 (ANT 3) input	-21 dB	50 dB
Last TX Power (dBm)	Parameter to show the actual transmitter power in dBm. The value is stored from the last time the transmitter was active and transmitted a packet	-51 dBm	28 dBm
TX Data Rate	Parameter to show the TX data rate in kbps		
TX Packets	Parameter to show the total number of packets transmitted by modem (includes multicast/broadcast packets)		
TX Bytes	Parameter to show the total number of bytes transmitted by modem		
TX Dropped Packets	Parameter to show the total number of transmit packets dropped by modem (includes multicast/broadcast packets)		

Monitored Parameter	Function	Normal Operating Lower Limit	Normal Operating Upper Limit
RX Data Rate	Parameter to show the RX data rate in kbps		
RX Packets	Parameter to show the total number of packets received by modem (includes multicast/broadcast packets)		
RX Bytes	Parameter to show the total number of bytes received by modem		
RX Multicast Packets	Parameter to show the number of received packets that are multicast		
RX Dropped Packets	Parameter to show the total number of receive packets dropped by modem (includes multicast/broadcast packets)		

Monitoring > Ethernet

This page displays the device performance monitoring parameters per Ethernet port transmission (TX) out of the device in packet and byte level granularity, for Ethernet port high level statistics and troubleshooting.

The results shown are since the page was opened and are updated automatically every 12 seconds
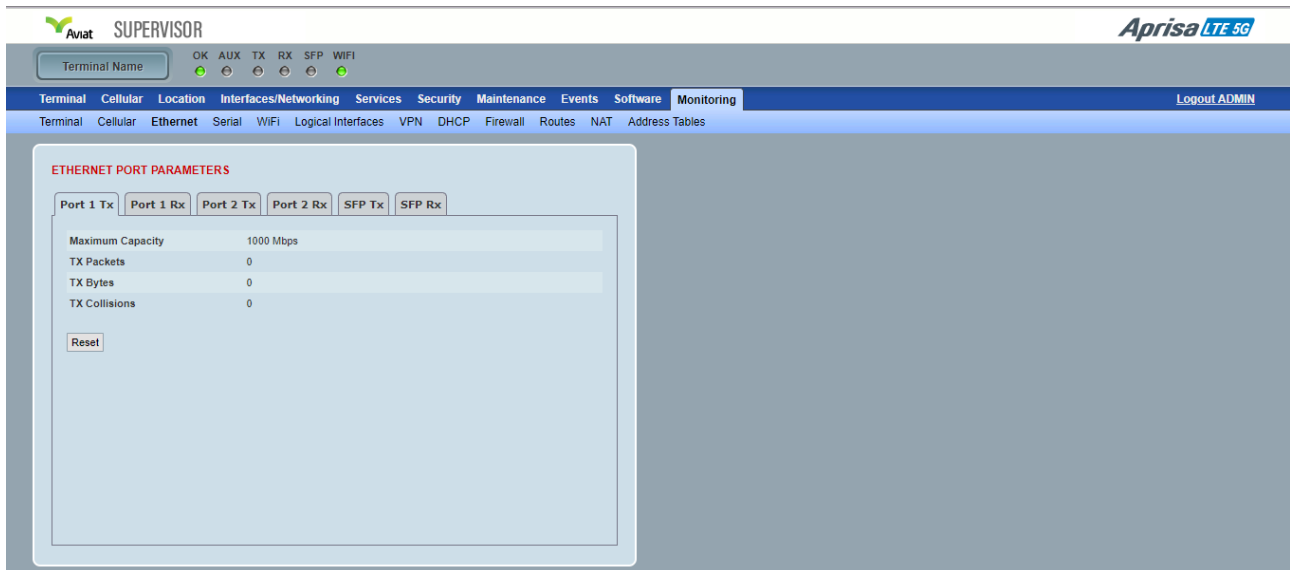
ETHERNET PORT PARAMETERS

All Ethernet Ports TX

Monitored Parameter	Function	Normal Operating Limits
Maximum Capacity	Parameter to show the maximum Ethernet data rate of the Ethernet port	Equal to the Ethernet port speed setting
TX Packets	Parameter to show the number of packets transmitted to the customer from the Ethernet port	
TX Bytes	Parameter to show the number of bytes transmitted to the customer from the Ethernet port	
TX Collisions	Parameter to show the number of packet collisions on the data transmitted to the customer from the Ethernet port on a shared LAN	

Controls

The Reset button clears the current results.

This page displays the device performance monitoring parameters per Ethernet port received (RX) data in packet and byte level granularity, for Ethernet port high level statistics and troubleshooting.

The results shown are since the page was opened and are updated automatically every 12 seconds.
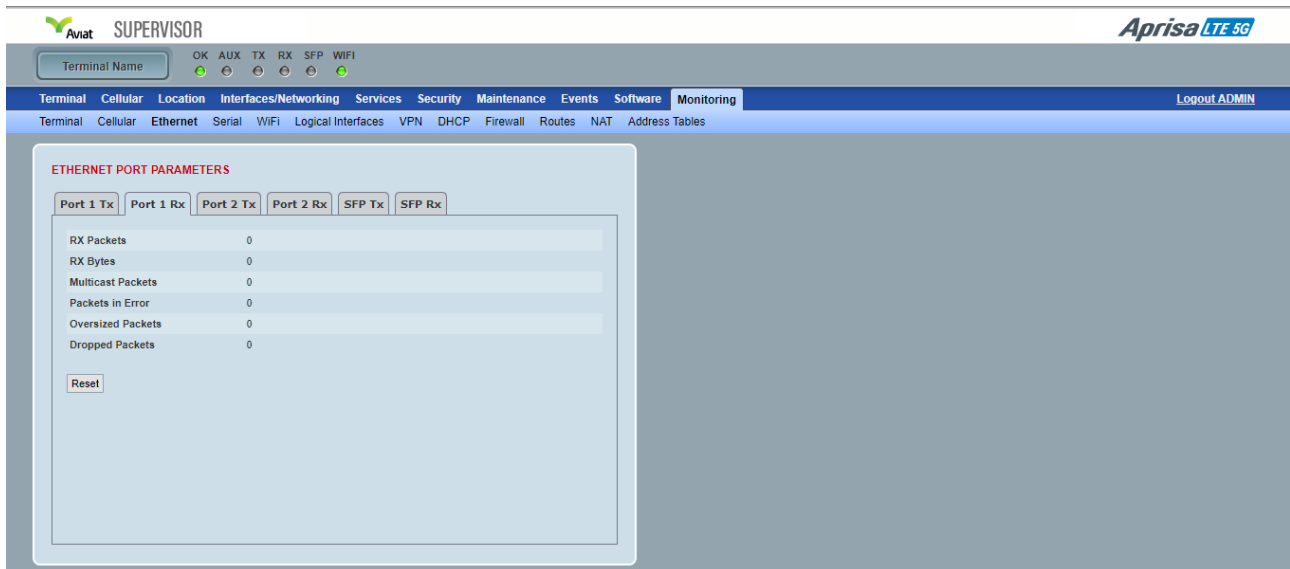
ETHERNET PORT PARAMETERS

All Ethernet Ports RX

Monitored Parameter	Function
RX Packets	Parameter to show the number of packets received by the customer from the Ethernet port (including broadcasts, multicasts, unicasts, FCS/CRC error, alignment error, undersize, jabber, oversize, and fragments)
RX Bytes	Parameter to show the number of bytes received by the customer from the Ethernet port (including broadcasts, multicasts, unicasts, FCS/CRC error, alignment error, undersize, jabber, oversize, and fragments and excluding IFG framing bytes/bits)
Multicast Packets	Parameter to show the number of multicast packets received from the customer into the Ethernet port. Multicast packets are packets that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Packets in Error	Parameter to show the number of errored packets received from the customer into the Ethernet port caused by CRC errors, FCS Errors, alignment errors, oversized packets, undersized packets, fragmented packets and jabber packets
Oversized Packets	Parameter to show the number of oversized packets received from the customer into the Ethernet port. Oversized packets are longer than 1518 octets excluding framing bits, but including FCS octets.
Dropped Packets (congestion)	Parameter to show the number of dropped packets received from the customer into the Ethernet port due to congestion
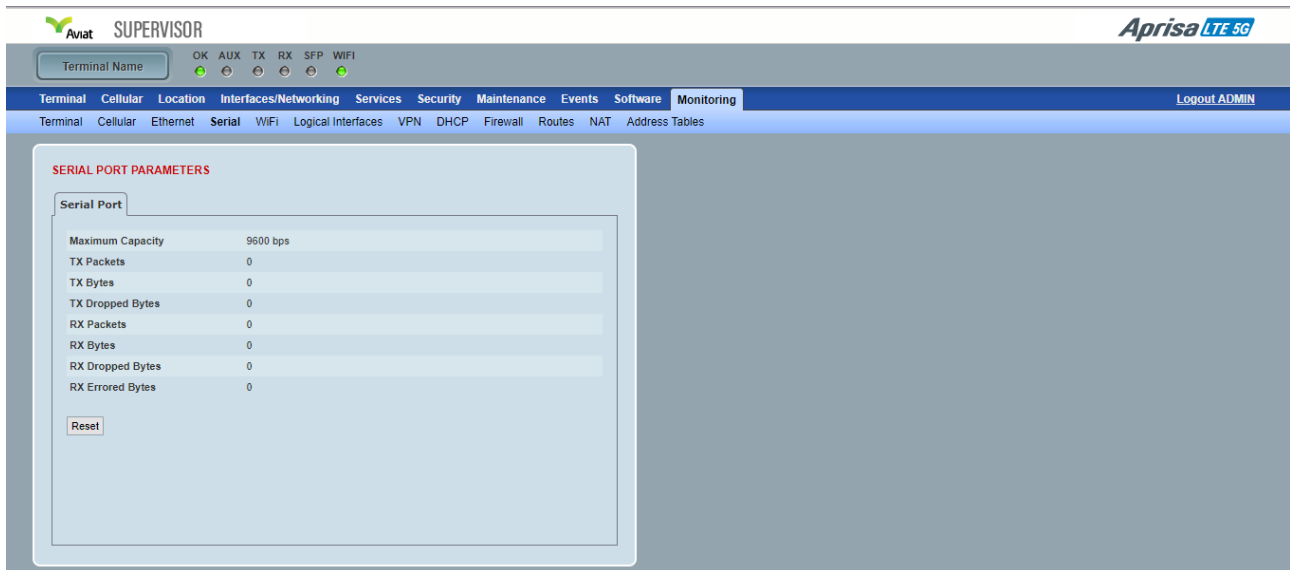
Controls

The Reset button clears the current results.

Monitoring > Serial

This page displays the device performance monitoring parameters per Serial port transmission (TX) out of the device in packet and byte level granularity, for serial port high level statistics and troubleshooting.

The results shown are since the page was opened and are updated automatically every 12 seconds
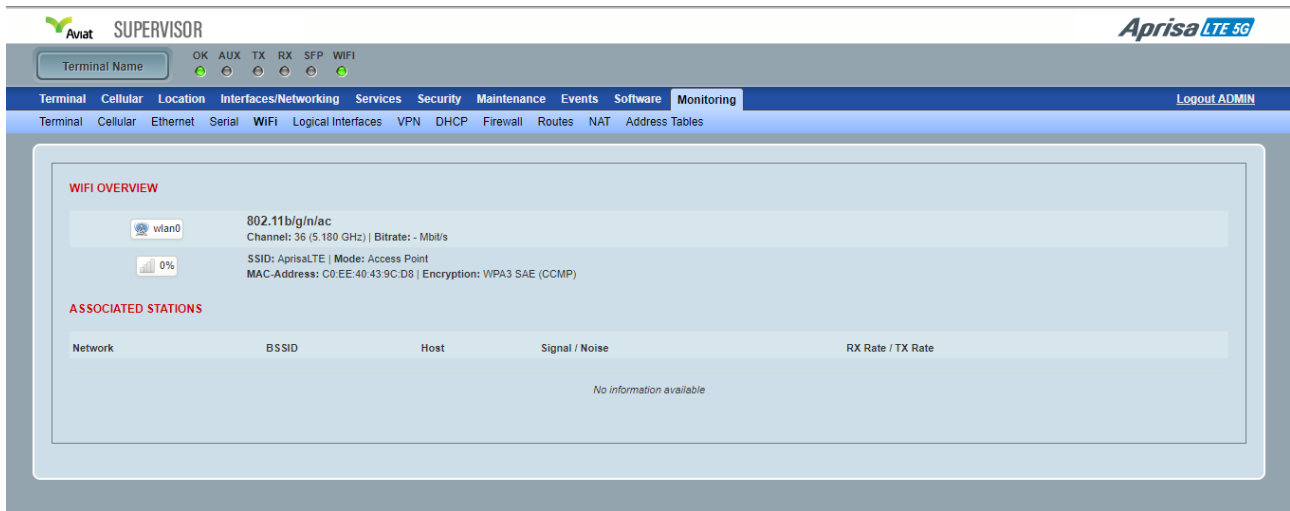
SERIAL PORT PARAMETERS

Monitored Parameter	Function
Maximum Capacity	Parameter to show the maximum serial data rate of the port
TX Packets	Parameter to show the number of packets transmitted on the serial port
TX Bytes	Parameter to show the number of characters transmitted on the serial port
TX Dropped Bytes	Parameter to show the number of bytes that were not transmitted because buffer was full or timed out
RX Packets	Parameter to show the number of packets received on the serial port
RX Bytes	Parameter to show the number of characters received on the serial port
RX Dropped Bytes	Parameter to show the number of bytes that were not received because the buffer was full
RX Errored Bytes	Parameter to show the number of characters received on the serial port in error (for example parity error or framing error)

Monitoring > WiFi

This page displays the device WiFi performance monitoring parameters.

WIFI Overview shows the channel used and current connection speed, along with the encryption mode, and SSID and BSSID of the connection. The bar icon will also vary depending on the signal strength of the connection.

The Associated Stations list shows a list of other WiFi devices in this network. When operating in Client mode, this will only show one entry (the WiFi Access Point). When operating in Access Point mode, this will show a list of all the active clients.

Monitoring > Logical Interfaces

This page displays the device Logical Interfaces performance monitoring parameters.

This shows a list of the logical interfaces.

Monitored Parameter	Function
VRF	The VRF name
Interface	The interface name
TX Packets	Parameter to show the number of packets transmitted on the interface
TX Bytes	Parameter to show the number of characters transmitted on the interface
TX Dropped Packets	Parameter to show the number of packets that were not transmitted because buffer was full
RX Packets	Parameter to show the number of packets received on the interface
RX Bytes	Parameter to show the number of bytes received on the interface
RX Dropped Packets	Parameter to show the number of packets that were not received because the buffer was full
RX Error Packets	Parameter to show the number of packets received on the interface in error (for example parity error or framing error)
RX Multicast Packets	Parameter to show the number of multicast packets received on the interface

Monitoring > VPN

This page displays the router VPN performance monitoring parameters.

This shows a list of active IPsec connections. Each entry in the Connections list corresponds to an IPsec connection configuration entry.
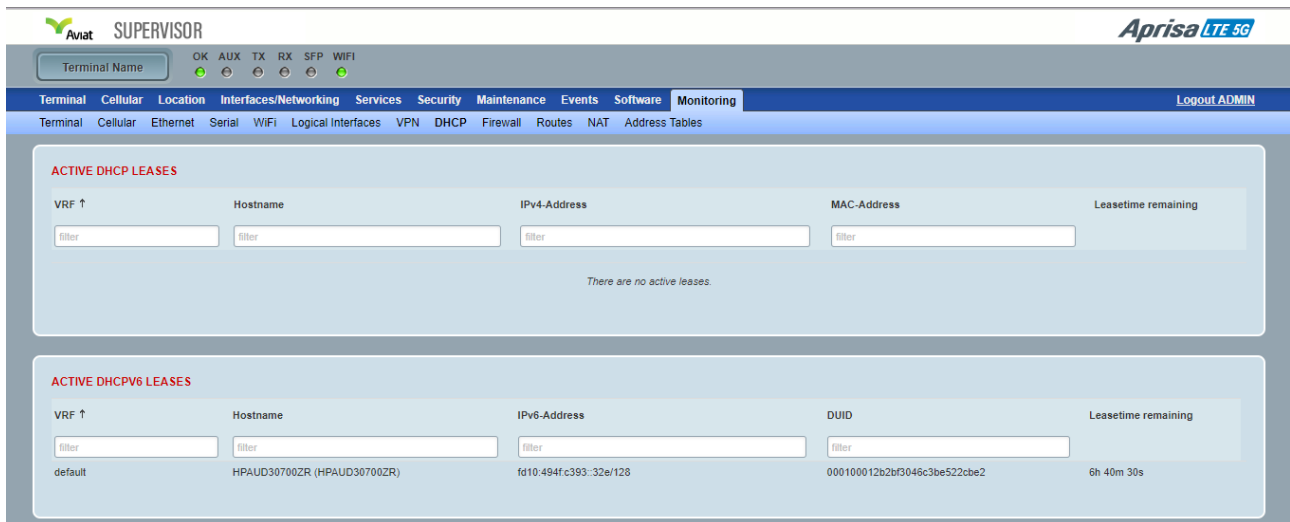
Name	This is the Connection Name configuration for this connection.
Version	The IKE version of the connection (either IKEv1 or IKEv2)
Local	The local address used for the connection
Remote	The remote address used for the connection
Status	The status (CONNECTING or ESTABLISHED)
Reauth In	The remaining time till a re-authentication will be performed
Age	The time since the previous re-authentication

Each entry in the Child Connections list shows an IPsec Tunnel configuration that is active.

ID	ID for this tunnel
Name	The configured Tunnel Name for the IPsec tunnel
Connection	The configured Connection Name for the IPsec connection that this tunnel is using
Local	The local subnet in packets sent over this tunnel
Remote	The remote subnet in packets sent over this tunnel
Status	The status of this tunnel
In/Out Byte	The total number of bytes received/sent on this tunnel
In/Out Pkts	The total number of packets received/sent on this tunnel
Last In/Out	The time since last input/output packet was received/sent
Type	The type of this tunnel. Either Tunnel or Transport

Monitoring > DHCP

This page displays information on the active DHCP server leases that the router has issued to other DHCP clients on the network.

Active DHCP Leases list shows the addresses that the DHCP server in the Aprisa LTE 5G has assigned to other devices.
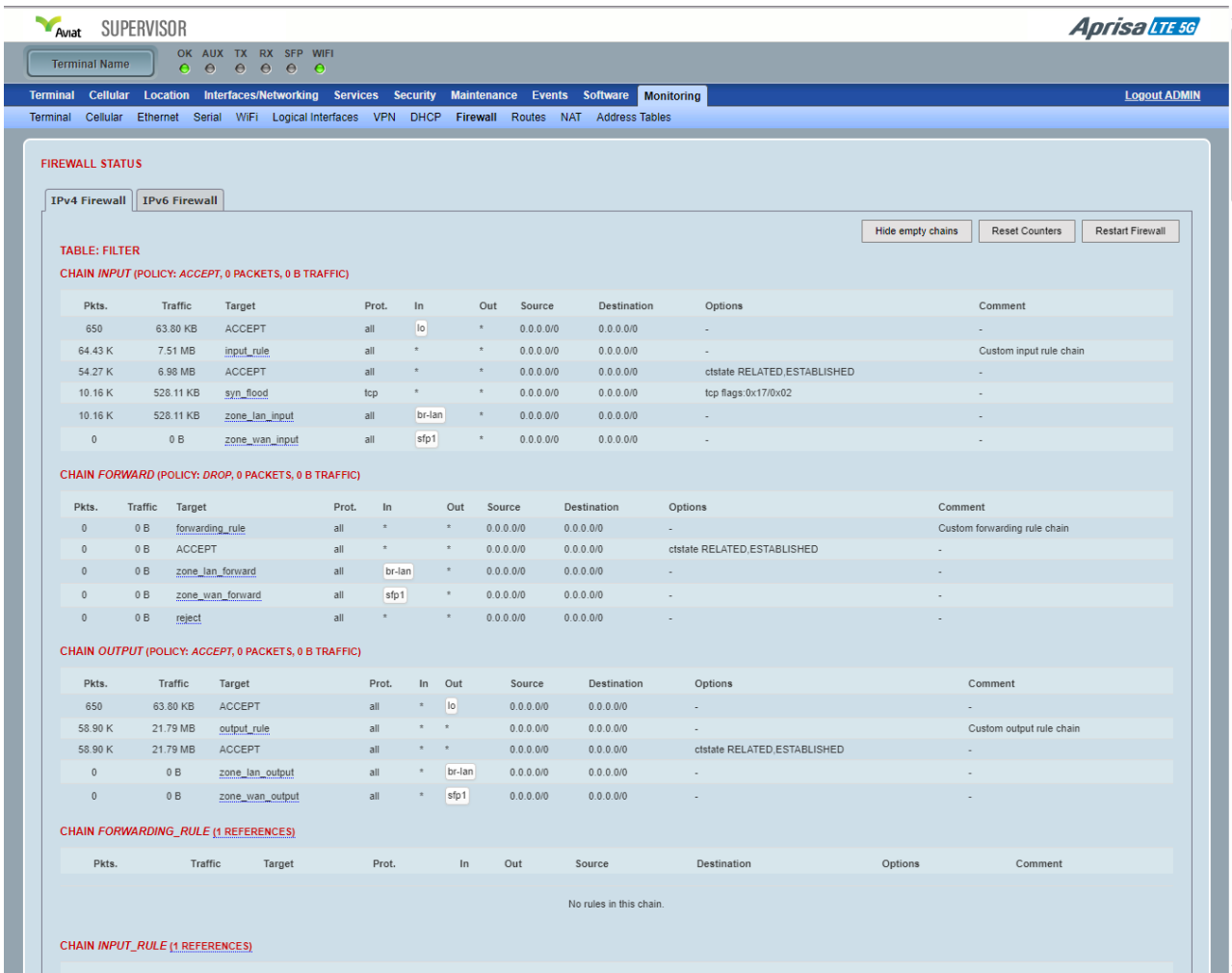
VRF	The VRF name.
Hostname	This is the DNS hostname for the device the lease is assigned to. FQDN (Fully qualified domain name) is in brackets.
IPv4-Address	The address that Aprisa LTE 5G has assigned to this device
MAC-Address	The MAC address for the device
Leasetime remaining	The lease will remain in the table for this amount of time. The device should send another DHCP request before this expires to remain active.

Active DHCPv6 Leases list shows the addresses that the DHCPv6 server in the Aprisa LTE 5G has assigned to other devices.

VRF	The VRF name.
Hostname	This is the DNS hostname for the device the lease is assigned to. FQDN (Fully qualified domain name) is in brackets.
IPv6-Address	The address that Aprisa LTE 5G has assigned to this device
DUID	The DHCP Unique IDentifier for the connected device. This is a unique identifier for the connected device (MAY be related to MAC address as per RFC6939, although this is optional).
Leasetime remaining	The lease will remain in the table for this amount of time. The device should send another DHCP request before this expires to remain active.

Monitoring > Firewall

This page displays the router firewall performance monitoring parameters.

This page shows the status and traffic counters for all firewall rules (including NAT translation).

Monitoring > Routes

Routes > Static Routes

This page displays the router static routes table. The routing table can support more than 100k dynamic and static routes.

The routes displayed here will include configured static routes, routes to directly attached networks, along with routes discovered through discovery protocols (such as DHCP and IPv6 RA).

Routes > IP SLA

This page displays the router IP SLA table.
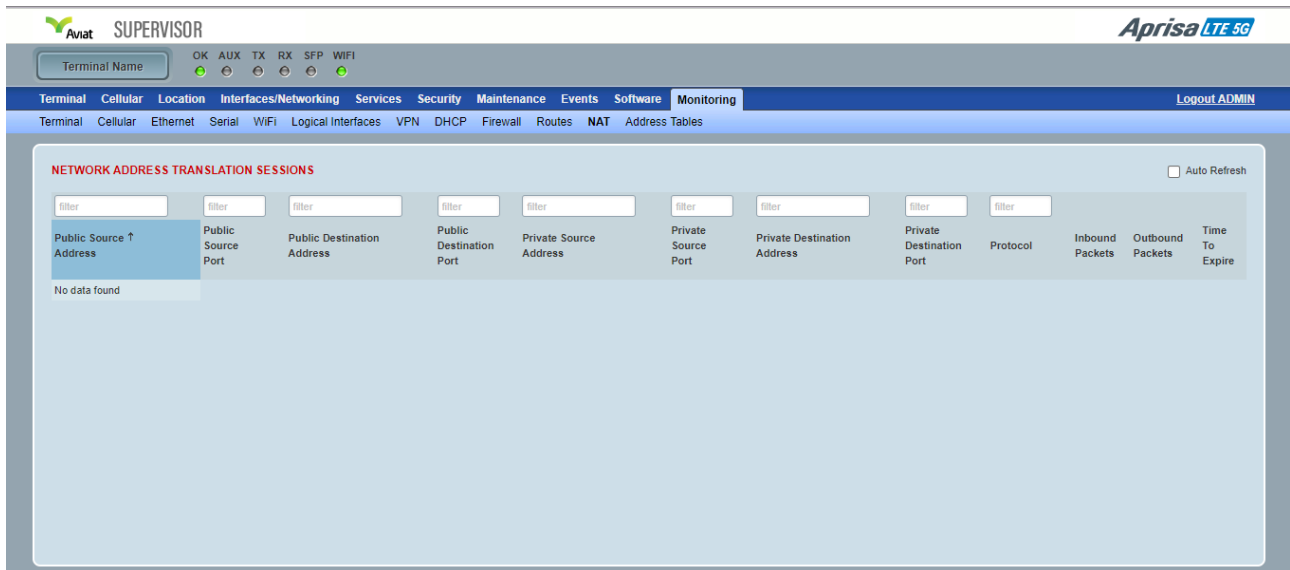
IP SLA LOG

IP SLA Log Column	Function
Run time	The IP SLA profile run time
Name	The IP SLA profile name
RTT minimum	The minimum detected ping RTT in the monitored period
RTT maximum	The maximum detected ping RTT in the monitored period
RTT average	The average detected ping RTT in the monitored period
Request count	The ping request count in the monitored period
Operation	The IP SLA profile operation state: running or stop
Response count	The ping response count in the monitored period
Lost count	The ping response lost count in the monitored period
Lost percent	Ping lost count / (Ping response count + Ping lost count) * 100
Status	The IP SLA profile status: UP, DOWN, UNKOWN with reason in brackets
Last Updated Time Stamp	The last date and time this IP SLA profile has been updated

Monitoring > NAT

This page displays the NAT (Network Address Table) sessions. The maximum number of sessions is 250.

NETWORK ADDRESS TRANSLATION SESSIONS

NAT Session Column	Function
Public Source Address	The source IP address of the session endpoint that lies in the public network.
Public Source Port	When the protocol is TCP or UDP, this represents the source port of the session in public network When the protocol is ICMP (only of query/response type such as ICMP echo), this represents the public network ICMP query identifier (ID) in the ICMP message
Public Destination Address	The destination IP address of the session endpoint that lies in the public network.
Public Destination Port	When the protocol is TCP or UDP, this represents the destination port of the session in public network. When the protocol is ICMP, this field is not relevant.
Private Source Address	The source IP address of the session endpoint that lies in the private network.
Private Source Port	When the protocol is TCP or UDP, this represents the source port of the session in private network. When the protocol is ICMP (only of query/response type such as ICMP echo), this represents the private network ICMP query identifier (ID) in the ICMP message
Private Destination Address	The destination IP address of the session endpoint that lies in the private network.
Private Destination Port	When the protocol is TCP or UDP, this represents the destination port of the session in private network. When the protocol is ICMP, this field is not relevant.
Protocol	Parameter to show the number of characters received on the serial port in error (for example parity error or framing error)
Inbound Packets	The number of inbound packets that were received on the public interface and translated for this session.
Outbound Packets	The number of outbound packets that were transmitted from the public interface and translated for this session.
Time To Expire	The time before the session expires.

Filtering
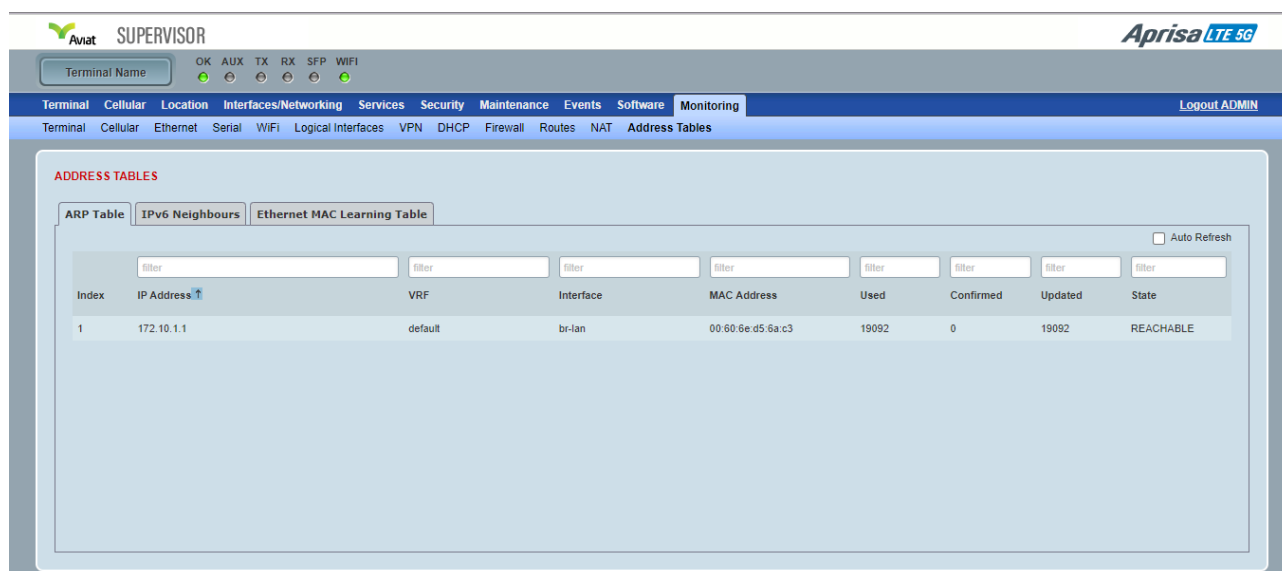
The first row of the table is the search filter. The type of filter is a text entry where any text can be entered. When the filters are applied, the rows in the rest of the table are displayed only if they match all the filters.

Sorting

Clicking on a column header of the table will sort the table by that column.

Monitoring > Address Tables

This page displays the current router ARP and IPv6 neighbour tables.

The ARP table shows mappings between IPv4 address and MAC address, and on which interface that mapping is present. These mappings are discovered using the ARP (Address Resolution Protocol).

The IPv6 Neighbours list shows mappings between IPv6 address and MAC address, and on which interface that mapping is present. These mappings are discovered using the ND (Neighbour Discovery) protocol.

Command Line Interface

The Aprisa LTE 5G router has a Command Line Interface (CLI) which provides basic product setup and configuration. This can be useful if you need to confirm the router's IP address, for example.

You can password-protect the Command Line Interface to prevent unauthorized users from modifying LTE settings.

This interface can be accessed via;

- USB via the USB host port ⬸ (USB type C) (hardware type B or greater devices only) with a USB-C cable.

- Secure Shell (SSH) application via the Ethernet Port (RJ45) using standard TCP/UDP port 22.

Connecting to the CLI via the USB host port

1. Connect the LTE USB host port ⟵⟶ to your PC with a USB cable - USB-C to a USB to suit your PC on the other end.

2. Go to your computer device manager (Windows > Control Panel > Device Manager)

3. Click on 'Ports (COM & LPT)'

4. Make a note of the COM port which has been allocated to the 'Aprisa LTE 5G USB cable' (COM3 in the example below).
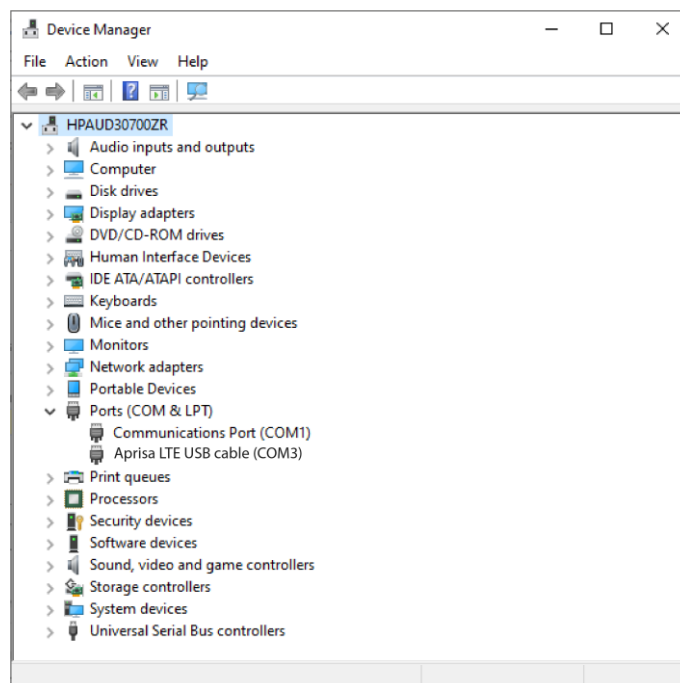
5. Open a terminal emulator program e.g. Putty.

Putty Example

6. Enter a name for the connection e.g. Aprisa LTE 5G CLI and save for future use.
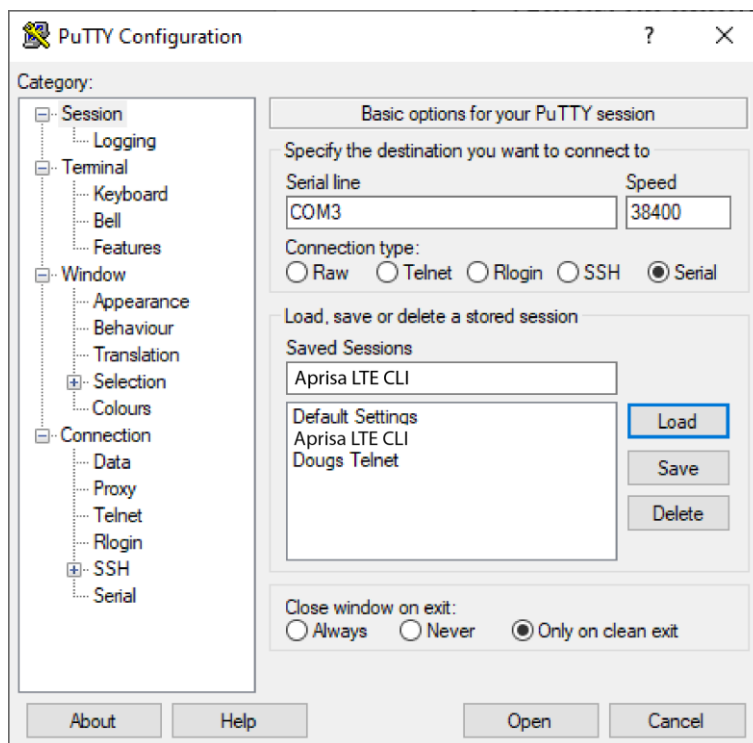
7. Click Open and the terminal window will open.

8. Press the enter key to initiate the session.

9. Login to the CLI with the default username 'admin' and password as shown on the Serial Number label on the left side of the enclosure. If there is no password shown on the Serial Number label, your password will be 'admin'.
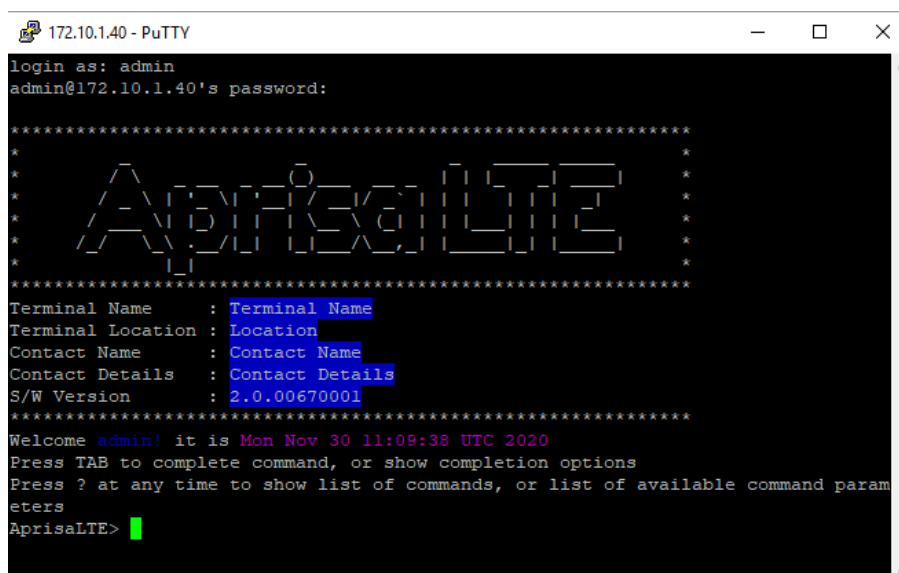
Connecting to the CLI via SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. It is used in the Aprisa LTE 5G to provide a secure CLI remote access connection to the LTE router. SSH is operated in server client mode, where the Aprisa LTE 5G router is acting as the SSH server. The communication between the client and Aprisa LTE 5G router (server) is encrypted in SSHv2 (where SSHv2 vs SSHv1 uses a more enhanced security encryption algorithm).

The SSHv2 protocol consists of three major components:

- The Transport Layer Protocol provides server authentication, confidentiality, and integrity with perfect forward secrecy.

- The User Authentication Protocol which authenticates the client to the server.

- The Connection Protocol which multiplexes the encrypted tunnel into several logical channels.

The Aprisa LTE 5G supports the following SSH features.

- Allows secure CLI connection over IPv4 and IPv6 networks.

- The 'SuperVisor Inactivity timeout' in Services > SuperVisor is also used to expire idle SSH sessions.
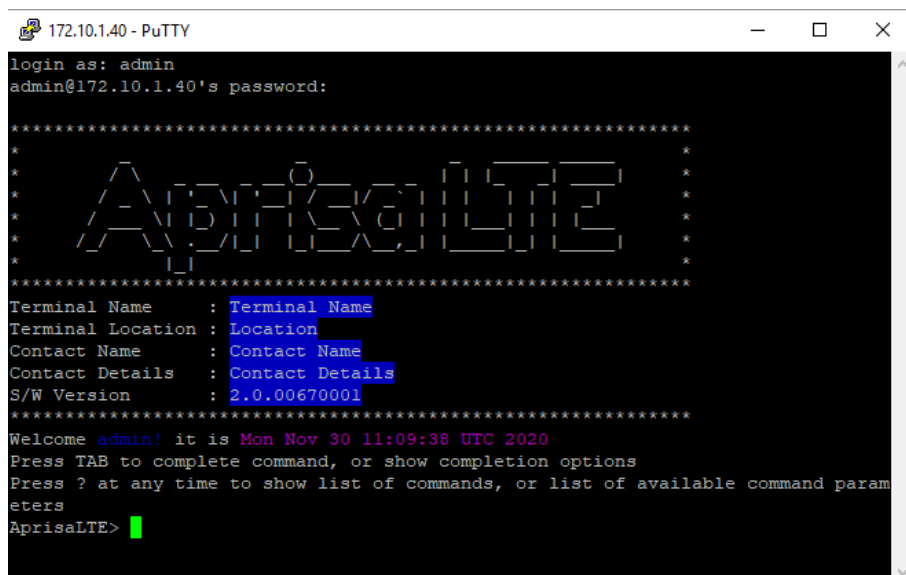
The Aprisa LTE 5G SSH server uses the following algorithms to secure the connection:

- Key exchange: ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256, diffie-hellman-group14-sha256, curve25519-sha256, diffie-hellman-group14-sha1, diffie-hellman-group1-sha256, diffie-hellman-group1-sha1

- Data Integrity: hmac-sha2-256, hmac-sha1

- Encryption: aes128-ctr, aes256-ctr, aes256-cbc

- Host key: ssh-rsa, ecdsa-sha2-nistp256

To connect to the Aprisa LTE 5G router CLI;

1. Connect the PC Ethernet to the Aprisa LTE 5G router Ethernet port (assuming a compatible IP address range).

2. Install one of the following tested SSH clients on your PC.

- PuTTY - Windows / Ubuntu

- TeraTerm

- Secure CRT

- MobaXterm

- OpenSSH

- Linux Terminal (Ubuntu)

- Kitty portal

- DameWare

- smartTTY

- Terminals (https://terminals.codeplex.com/)

- mRemoteng - Multi-Remote Next Generation

2. Open the SSH client.

3. Install the server public key using the method appropriate for your SSH client. This key is available in supervisor on the Security -> SSH page. This step is optional but provides a guarantee that you are correcting directly and there is no man in the middle attack occurring.

4. Login to the CLI with the default username 'admin' and password as shown on the Serial Number label on the left side of the enclosure. If there is no password shown on the Serial Number label, your password will be 'admin'.
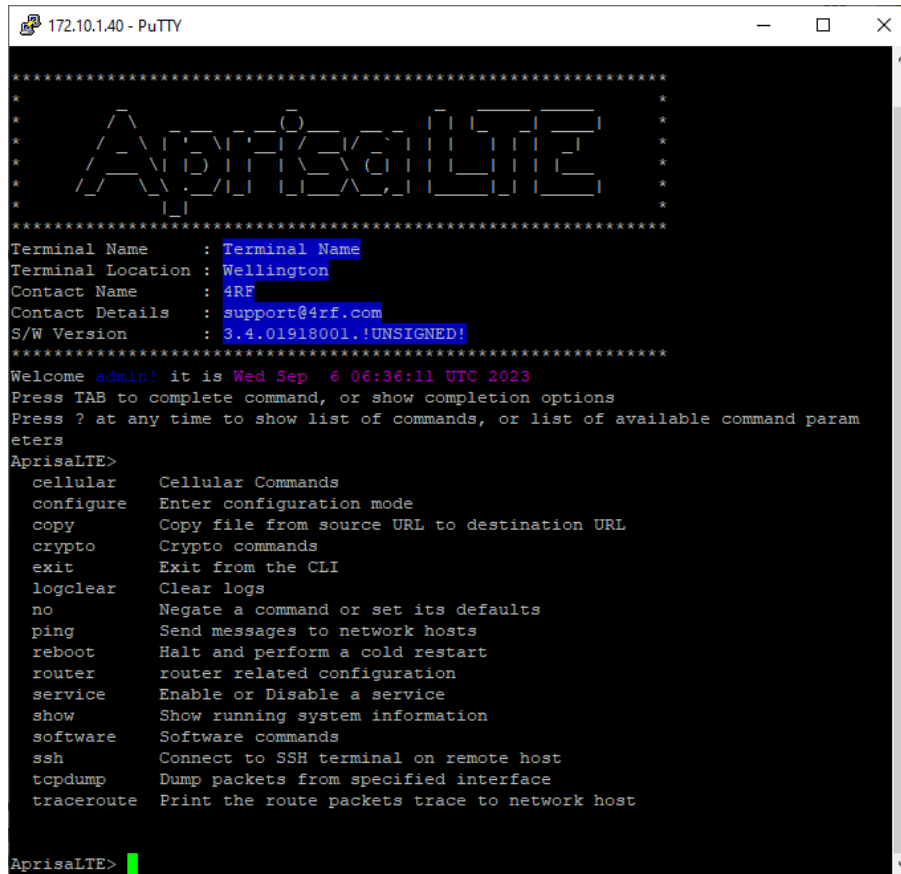
CLI Commands

The top level CLI command list is displayed by typing a ? at the command prompt.

The CLI commands described in this section is a high level view of the commands. For a complete list and descriptions of the CLI commands, please refer to the 'Aprisa LTE User Manual 3.6 Appendix 2 – Command Line Interface Guide' document.

The following is a list of the top level CLI commands and their usage:

CLI Command	Usage
cellular	Configures Cellular parameters. See Cellular CLI Commands below.
configure	Configures key parameters for various network interfaces in the system. See Configure CLI Commands below.
copy	Copies various system parameters. See Copy CLI Commands below.
crypto	See Crypto CLI Commands below.
exit	Exit from the CLI.
logclear	Clears the logs
no	Negates a command

CLI Command	Usage
ping	ping [ip|ipv6|arp] <host> [source <src>] : the network interface to send the packet from [repeat <cnt>] : number of repeats [resolve] : Attempt to resolve host names [broadcast] : Perform broadcast ping [size <bytes>] : Size of ping packet [interval <seconds>] : Interval between pings [flood] : Flood interface with pings [duplicate-detect]
reboot	Reboots the Aprisa LTE 5G
router	see Router CLI Commands below
service	service <name> <action> Performs given action on the given service. 'firewall' service supported with 'start', 'stop' and 'restart' actions supported
show	Shows various Aprisa LTE 5G parameters e.g. 'show ip interface all' to view the interface parameters.
software	See Software Commands below
ssh	See SSH Commands below
tcpdump	Tcpdump Dumps packets from specified interface, ctrl-c stops the capture [verbose] : this shows extra information from the packet header [ethhdr] : this shows information from the ethernet portion of the header. Without this flag, only the IP portion is shown. [iface xxx] : this selects which interface to dump. This could be physical interfaces like eth1, eth2, sfp1, wwan0, wlan0, or can be virtual interfaces like the lan bridge (br-lan) or a gre tunnel. [filter xxx] : allows you to display only packets matching the filter. See here for information on filter syntax: https://www.tcpdump.org/manpages/pcap-filter.7.html Example command to capture icmp packets on eth1: tcpdump iface eth1 filter icmp
traceroute	traceroute ip|ipv6 <hostname>

To see the next level CLI command list, type a ? at the command prompt:

    AprisaLTE> show ?

To go back one level, type Exit at the prompt:

    AprisaLTE(config) > Exit

Cellular CLI Commands

Command Option	Usage	Maximum Access
cellular autoapn clear	clear auto apn for a given IMSI	
cellular autoapn list	list IMSI of SIMs with stored autoapn	
cellular autoapn show	show auto apn for a given IMSI	
cellular debug <off/on>	Disable / enable cellular debug logs in syslog	
cellular modem carrier preferred <xxx>	Set the preferred carrier	Engineer and above
cellular modem reset	Resets the modem	Technician and above
cellular sim enable-lock	Enables the SIM PIN lock function	Engineer and above
cellular sim disable-lock	Disable the SIM PIN lock function	Engineer and above
cellular sim puk-unblock <puk> <newping>	Unblocks a SIM if it is in blocked state.	Engineer and above
cellular sim change-pin <old> <new>	Changes the SIM PN	Engineer and above
cellular pdn <1..4>	Enter to cellular PDN config mode	Engineer and above

Configure CLI Commands

Command Option	Usage	Maximum Access
configure terminal	Enter configuration mode. Example: AprisaLTE> configure terminal AprisaLTE(config)>	
do	Allows execution of any non-configure view command	All
unlock-factory	Unlocks factory mode commands	Admin only
commit	Once all the changes have been made, they can be committed using the 'commit' command. If there is an error during the commit due to missing data, conflicting settings, or other issue, then none of the changes will be committed and the CLI will provide feedback regarding the error. Successful commit saves configuration to configuration database.	Technician and above
discard	Discard uncommitted changes	Technician and above
apply	Applies changed configuration to running system. Does not save changes.	Technician and above
exit	Exit the configuration mode / exit one level of configuration and go to parent configuration level	exit
hostname <name>	Sets network hostname to specified value	hostname <name>
supervisor [httpport xx] [httpsport xx] [redirect on|off]	Configures supervisor listen ports for http, https. Each parameter is optional, and if omitted the value does not change.	
no supervisor httpport no supervisor httpsport	Disables supervisor on http or https	
(config-pdn-x)# auth <pap/chap/pap_chap> <username> <password>	Set cellular PDN <1..4> authentication (either pap or chap or pap_chap (pap and chap) protocol), username and password	Engineer and above
(config-pdn-x)# mtu	Set cellular pdn <1..4> MTU size. Note: If the user configures a PDN MTU greater than the MTU received from the PDN network, then the user setting is ignored (to prevent packet drop) and an alarm is raised. To clear the alarm, the user should set the MTU value equal or lower than the MTU received from the PDN network. An example of the alarm event log message might be like this: 'PDN 1 MTU (1470) larger than carrier requested MTU (1400) and is ignored. Reduce MTU to clear alarm'.no	Engineer and above
(config-pdn-x)# lock timer <delay>	Locks cellular PDN<1..4> for specified <delay> period	Engineer and above
(config-pdn-x)# no auth	Disables cellular PDN<1..4> authentication	Engineer and above
(config-pdn-x)# no lock	Disables cellular PDN<1..4> lock	Engineer and above
(config-pdn-x)# no mtu	Disables cellular PDN<1..4> user MTU setting	Engineer and above
(config-termserver-x)# translate-protocol modbus-tcp modbus-rtu	Enables terminal server Modbus TCP to Modbus RTU protocol conversion	Engineer and above
(config-termserver-x)# no translate-protocol modbus-tcp	Disables terminal server Modbus TCP to Modbus RTU protocol conversion	Engineer and above

Command Option	Usage	Maximum Access
(config-termserver-x)# translate-protocol modbus-tcp modbus-ASCII	Enables terminal server Modbus TCP to Modbus ASCII protocol conversion	Engineer and above
(config-termserver-x)# no translate-protocol modbus-ASCII	Disables terminal server Modbus TCP to Modbus ASCII protocol conversion	Engineer and above
logclear	Clears all entries from the Event History Log	Admin only
loglevel <subsystem> <level>	Sets the subsystem debug level for individual subsystems.	Admin only

Router CLI Commands

Router Command Option	Usage	Maximum Access
router enter	Enters 'Router Configuration and Monitoring Mode'	
add	Add registration	
clear	Reset functions	
configure	Configuration from vty interface	
copy	Copy from one file to another	
debug	Debugging functions	
disable	Turn off privileged mode command	
enable	Turn on privileged mode command	
end	End current mode and change to enable mode	
exit	Exit current mode and down to previous mode	
find	Find CLI command matching a regular expression	
list	Print command list	
mtrace	Multicast trace route to multicast source	
no	Negate a command or set its defaults	
output	Direct vtysh output to file	
ping	Send echo messages	
quit	Exit current mode and down to previous mode	
rpki	Control rpki specific settings	
show	Show running system information	
terminal	Set terminal line parameters	
traceroute	Trace route to destination	

Copy CLI Commands

copy <source> <destination> [include-keys]

Source:Destination	Usage	Maximum Access
vrf	Specify a VRF interface to route through	Any
system:startup-config	Source and destination option. Used to transfer the currently saved config to/from external ftp/s URL. A warning is shown if the security level is high, but the config encryption key is the default or if there is a key mismatch when importing the config Example of export / import of config file: Import: copy ftp://user1:user123@ftp.aviatnetworks.com/config.00 system:startup-config Export: copy system:startup-config ftp://admin:admin@ftp.aviatnetworks.com/config.00	Admin only
system:factory-config	Source only option. Set the device to its factory default configuration. Example: copy system:factory-config system:startup-config	Admin only
system:eventlog	Source only option. Copies the Event History Log to external ftp/s URL. Example: copy system:startup-config ftp://admin:admin@ftp.aviatnetworks.com/eventlog.00	Any (Users below engineer get log without security events)
system:gnsslog	Source only option. Copies the GNSS Log to external ftp/s URL. Example: copy system:startup-config ftp://admin:admin@ftp.aviatnetworks.com/gnsslog.00	Any
system:support	Source only option. Copies the support information file to external ftp/s URL. Example: copy system:support ftp://admin:admin@ftp.aviatnetworks.com/gnsslog.00	Any
ftp:[url]	Source or destination of ftp. Examples: (Anonymous) ftp://1.2.3.4/test/test.cfg (User/Password) ftp://user:pass@1.2.3.4/xyz/test.log	Any
ftps:[url]	Source or destination of ftps. Example: ftps://user:pass@1.2.3.4/xyz/test.log	Any
flash:active-firmware	Destination only. If source is standby firmware, active partition is swapped. If the source is available firmware, then it is first installed to standby before activating. If the source is remote url, it is loaded to available, installed to standby then activated. Example: copy ftp://user1:user123@ftp.aviatnetworks.com/sw.4nu.00 flash:active-firmware	Admin only
flash:standby-firmware	Source only. Activate standby firmware by copying it to active firmware. Example: copy flash:standby-firmware flash:active-firmware	Admin only
flash:available-firmware	Source only option. Activate available firmware by copying it to active firmware. When used as destination, firmware that is not valid will be ignored and an error reported. Example: copy flash:available-firmware flash:active-firmware	Technician and above

Source:Destination	Usage	Maximum Access
ltemodem:available-firmware-1 ltemodem:available-firmware-2	Activate LTE modem available firmware by copying it to LTE modem active firmware . Note: this is the LTE modem module firmware and not the Aprisa LTE 5G router software/firmware. Example: Copy ltemodem:available-firmware-1 ltemodem:active-firmware copy ltemodem:available-firmware-2 ltemodem:active-firmware	Technician and above
ltemodem:active-firmware	Destination only. Used to install Aprisa LTE 5G modem (module) firmware. Note: this is the LTE modem module firmware and not the Aprisa LTE 5G router software/firmware.	Admin only

Show CLI Commands

show <command>[options]

Command Option	Level	Description
show cellular	*modem diagnostics*	Dump of modem diagnostics
	modem firmware	Show information about available and active firmware
	pdn profile	Displays a list of PDN's
	pdn locks	Displays info about any active PDN lock
	sim active info	Displays info about the active SIM
show crypto	*status*	Displays the status of IPsec VPN tunnels
show date		Displays current date/time
show device	*input*	Displays current alarm input status
	output	Display current alarm output status
	netdev [ifacename|all]	Displays detailed port statistics for the specified physical network port
	netdev list	Shows a list of available physical network ports
	sensors all	Shows readings from internal sensors (temperature, voltage and accelerometer)
	sfp	Shows detail diagnostics about the detected SFP devices (manufacture, model, laser signal levels, etc)
	system	Display information about router hardware such as part number, serial number, MAC addresses and what optional devices are present
	usb	Status of USB port, including list of attached devices
show eventlog		Show contents of the event history log
show file	*system*	Shows system files of filesystem / Config / Removable and their Size, Used, Available, and Use% parameters
show ip		Show IP information
	arp	Show ARP v4 / v6 Table Examples: *inet4 show IPv4 ARP table* *inet6 show IPv6 ARP table*
	interface	Show Specific Interface Details Examples: *all Display All Interface Details* *lan Show lan Interface details* *wan Show wan Interface details* *wan6 Show wan6 Interface details* *wwan Show wwan Interface details*
	nat	Show nat session Table. Examples: *show ip nat translations <sort argument>* *<sort argument> used to sort the table based on this argument/s*
	route	Show IPv4 / v6 Route Table Examples: *inet4 show IPv4 routing table* *inet6 show IPv6 routing table*

Command Option	Level	Description
	socket	Show TCP and UDP sockets information Examples: *protocol Select Protocol TCP/UDP* *listen Display listening sockets only* *resolve Resolve Names inet4*
show ipv6 route		Shows the current static ipv6 routes
show loglevel		Show the subsystems syslog severity level (i.e. Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug)
show mac		Show the L2 MAC address table
show memory		Show MemTotal, MemFree, MemAvailable, Buffers, and Cached parameters
show network interfaces		Lists all the network interface names
show processes		Show the running processes and their PID, VSZ, %VSZ, and %CPU parameters
show running-config		Show the running configuration parameters
show software		Show software versions
	active	Show Active software
	all	Show all software versions
	available	Show available software
	running	Show running software
	standby	Show standby software
show startup-config		Show the contents of startup configuration
show syslog		Show syslog output
	ful	Show complete syslog output
	start	Start printing new syslog output on screen. Press CTRL+C to exit
show system		Show system summary
		Show display of all users
show uptime		Show the system uptime since last reboot
show users		Show display of all users
show vrf		List all the VRFs along with their routing table IDs
show wifi		
	interface	Show Wi-Fi interface details
	stations	Show Wi-Fi peer details

Command Option	Level	Description
show termserver		Shows the configuration of the terminal server
		Example:
		show termserver-config
		termserver 0
		tcp timeout inactivity xx
		tcp persist
		tcp keepalive enable
		tcp keepalive interval xx
		tcp keepalive probes xx
		translate-protocol modbus-tcp modbus-rtu
		All options can be preceded by 'no' if disabled (e.g. 'no termserver 0').

SNMP Management

The Aprisa LTE 5G has a built-in SNMP agent to enable NMS (Network Management System) FCAPS (Fault, Configuration, Administration, Provisioning and Security) management model. Any 3rd Party NMS supporting SNMPv1/v2c/v3 can integrate with Aprisa LTE 5G and manage it as part of a network wide management.

SNMPv1/v2c can be used to manage Aprisa LTE 5G in a non-secure management connection.

SNMPv3 is used to manage the Aprisa LTE 5G in a secure management connection. SNMPv3 support standard USM model with the ability to configure user authentication and privacy (encryption) as per the standard and with wider and strong authentication and privacy (encryption) protocols.

To set SNMP management connection, navigate to 'Security > SNMPv2/v3' on page 236.

SNMPv2c and TRAP/Informs

The Aprisa LTE 5G SNMP agent support v1 TRAP, v2c TRAP and inform. It supports configuration of multiple NMS that shall receive TRAP and Inform from the Aprisa LTE 5G when alarms / events are logged.

In general, a standard SNMP TRAP agent supports SNMP engine ID. This is supported by using the standard method of negotiation between the NMS and Aprisa LTE 5G where the Aprisa LTE 5G provides this engine ID to the NMS, thus it is not a configurable parameter in Aprisa LTE 5G. The engine ID must be unique per each device in the network and thus it is composed by a hash function of the Aprisa LTE 5G MAC address.

To set multiple NMSs to receive the SNMP TRAP / Informs from the Aprisa LTE 5G, navigate to 'Events > Trap Setup' on page 257.

SNMP MIB Structure

The Aprisa LTE 5G and in general other Aviat Networks devices provide generic MIB interfaces for its products. This is to help provide a common and easily extendable management interface across the Aviat Networks product range.

To easily find an SNMP object/OID (Object ID) in Aprisa LTE 5G using a MIB browser, navigate to the '.private.enterprises.fourRFRoot.fourRFGeneric' node on the MIB tree structure and walk through the objects within this node.

An example of the Aviat Networks MIB Tree structure is shown as follows:
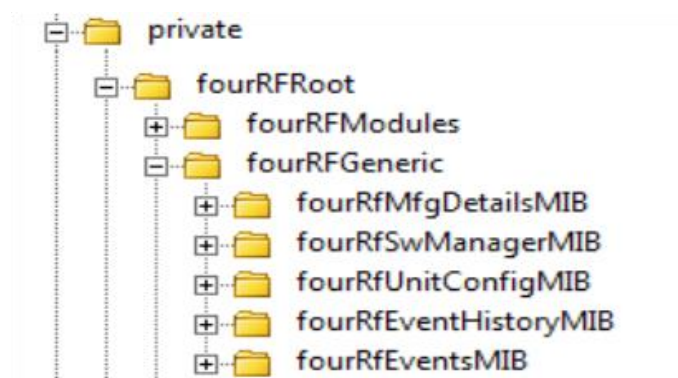
The generic interfaces are common across the family of Aviat Networks products and will enable third party management systems to manage the Aviat Networks products in the same manner and use a common interface.

Standard SNMP MIBs Supported

The Aprisa LTE 5G partially supports the following standard MIBs:

- RFC1213-MIB
- SNMPv2-MIB
- HOST-RESOURCES-MIB
- IF-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-USER-BASED-SM-MIB
- SNMP-VIEW-BASED-ACM-MIB

Aprisa LTE 5G Proprietary MIBs Supported

The Aprisa LTE 5G supports specific SNMP MIBs that are written to support specific objects/OIDs (Object Identifiers) that are only supported in the Aviat Networks Aprisa family of products. The format of the MIB files comply with ITU-T ASN.1 (Abstract Syntax Notation One) standard notation.

The following are the list of the proprietary MIBs supported by Aprisa LTE 5G.

- 4RF-MIB.txt - Top level 4RF products' MIB.
- 4RF-EVENTHISTORY-MIB.txt - 4RF MIB for Aprisa LTE 5G events (history) logging.
- 4RF-EVENTS-MIB.txt – 4RF MIB for Aprisa LTE 5G events/alarms.
- 4RF-MFGDETAILS-MIB.txt - 4RF MIB for Aprisa LTE 5G manufacturing information.
- 4RF-PRODUCTS-MIB.txt - 4RF MIB for product definitions
- 4RF-SWMANAGER-MIB.txt - 4RF MIB for Aprisa LTE 5G software version management.
- 4RF-TEXTCONVENTION-MIB.txt - 4RF MIB Textual Conventions.
- 4RF-UNITCONFIG-MIB.txt - 4RF MIB for basic Aprisa LTE 5G unit configuration.
- 4RF-MONPARAM-MIB.txt - 4RF MIB for Aprisa LTE 5G monitoring (statistics and diagnostic) parameters
- 4RF-CELLULARCONFIG-MIB.txt - 4RF MIB for Aprisa LTE 5G cellular parameters
- 4RF-FILETRANSFER-MIB.txt - 4RF MIB for Aprisa LTE 5G file transfer of firmware, config, evet, GNSS, and support files.

4. Maintenance

Spare Fuses

The Aprisa LTE 5G router PBA contains two fuses in the power input with designators F1 and F2. Both the positive and negative power connections are fused. The fuse type is a Littlefuse 0453005 with a rating of 5 A.

To replace the fuses:

1. Remove the input power and antenna cables.2.   Unscrew the enclosure securing screws (posi 2).

Enclosure Securing Screws
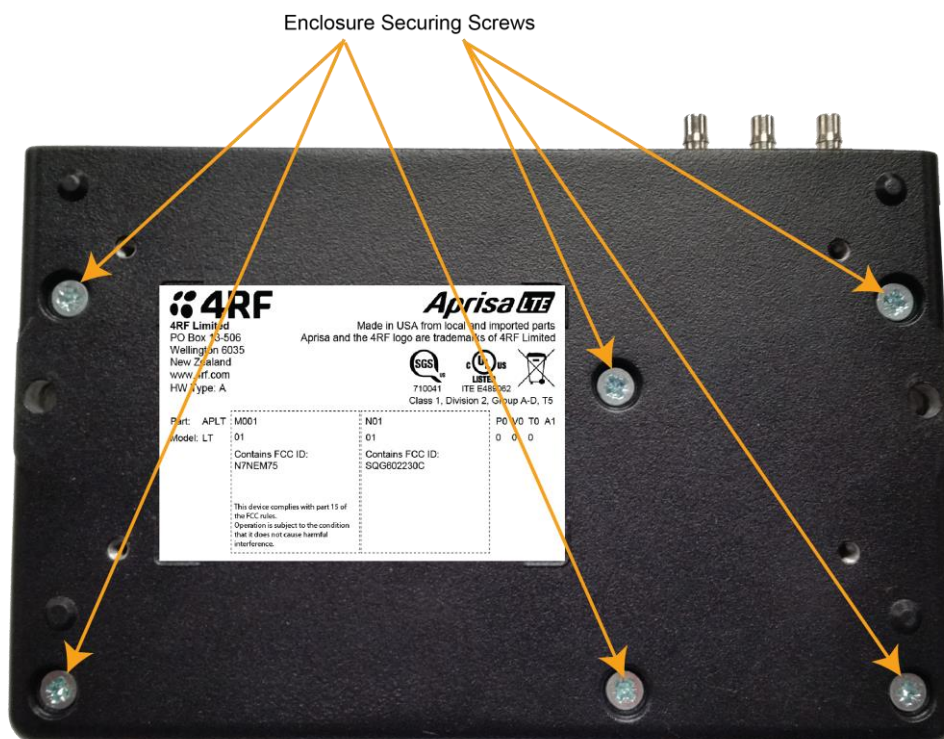
2. Separate the enclosure halves.

CAUTION: Antistatic precautions must be taken as the internal components are static sensitive.

3. Replace the two fuses.

4. Close the enclosure and tighten the screws.

Note: Is it critical that the screws are re-tightened to 0.8 Nm. The regulatory compliance of the Aprisa LTE 5G router may be affected if the screws are not tightened correctly.

Additional spare fuses can be ordered from Aviat Networks see 'Spare Fuses' on page 92.

5.   Alarm Events

Alarm Events

Customer Equipment Interface Path Alarms

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
10	Port 1 Eth No Receive Data	Warning	Alarm to indicate that the Ethernet port 1 has received no data packets in the defined duration period.	Check Ethernet cable and connector. Check IP and VLAN configuration.
15	Port 1 Eth Port Down	Critical	Alarm to indicate that the Ethernet port 1 has no detected connection during the defined duration period.	Check the cable and connector. Check Ethernet Port speed/duplex configuration.
35	Port 2 Eth No Receive Data	Warning	Alarm to indicate that the Ethernet port 2 has received no data packets in the defined duration period.	Check Ethernet cable and connector. Check IP and VLAN configuration.
38	Port 2 Eth Port Down	Critical	Alarm to indicate that the Ethernet port 2 has no detected connection during the defined duration period.	Check the cable and connector. Check Ethernet Port speed/duplex configuration.
44	SFP No Receive Data	Warning	Alarm to indicate that the SFP port has received no data packets in the defined duration period.	Check the SFP is plugged in. Check SFP Port configuration. Check network cabling and connections.
47	SFP Port Down	Critical	Alarm to indicate that the SFP port has no detected connection during the defined duration period.	Check the SFP is plugged in. Check SFP Port configuration. Check network cabling and connections.
93	SFP TX Fault	Major	Alarm to indicate a problem with SFP transmission. This can be cabling / connection issues, or SFP module failure.	Check network cabling and connections. If alarm is still present, replace the SFP module.
94	SFP RX Fault	Major	Alarm to indicate a problem with SFP reception. This can be cabling/connection issues, or SFP module failure.	Check network cabling and connections. If alarm is still present, replace the SFP module.
14	Port 1 Serial Data Receive Errors	Warning	Alarm to indicate that the RS-232 port 1 received input signal contains errors at a higher rate than the defined error rate threshold.	Check serial ports settings, check serial cable and connector.
13	Port 1 Serial No Receive Data	Warning	Alarm to indicate that the RS-232 port 1 has no received input signal in the defined duration period.	Check serial ports settings, check serial cable and connector.

Cellular Interface Path Alarms

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
97	Cellular Registration Failure	Major	Alarm to indicate when cell network registration fails.	Check Cellular configuration and antenna. Check with network operator that the SIM card is enabled on their network.
98	Cellular Link Failure	Major	Alarm to indicate when the cellular link fails.	Check Cellular configuration and antenna.
99	Cellular Roaming	Major	Alarm to indicate when cellular goes on roaming.	Check antenna. Check that signal levels for primary network operator are sufficient for connection.
103	Cellular Network Activity	Information	Alarm to indicate that	
104	Cellular Health Check Fail	Major	Alarm to indicate that the cellular link health check test has detected a connectivity failure.	Check the cellular link health check settings. Check antenna.
119	Cellular No Receive Data	Warning	Alarm to indicate that the cellular connection has received no data packets the defined duration period.	Check Cellular configuration and antenna.
131	Cellular Transmit Data Rate	Warning	Alarm to indicate that the TX data rate is outside the defined thresholds	
132	Cellular Receive Data Rate	Warning	Alarm to indicate that the RX data rate is outside the defined thresholds	
133	Cellular Data Usage Threshold	Warning	Alarm to indicate the cellular data usage is out of limits	
134	Cellular Temperature Threshold	Warning	Alarm to indicate the cellular temperature is out of limits	
135	Cellular RSSI Threshold	Warning	Alarm to indicate the cellular RSSI is out of limits	
136	Cellular RSRP Threshold	Warning	Alarm to indicate the cellular RSRP is out of limits	
137	Cellular RSRQ Threshold	Warning	Alarm to indicate the cellular RSRQ is out of limits	
138	Cellular SNR Threshold	Warning	Alarm to indicate the cellular SNR is out of limits	
139	Cellular SINR Threshold	Warning	Alarm to indicate the cellular SINR is out of limits	
140	Cellular Tx Power Threshold	Warning	Alarm to indicate the cellular Tx Power is out of limits	

SIM Alarms

106	SIM 1 PIN Lock	Major	Alarm to indicate when SIM card 1 has rejected the configured PIN.	Unlock the SIM 1 by entering the correct PIN for SIM 1.
107	SIM 2 PIN Lock	Major	Alarm to indicate when SIM card 1 has rejected the configured PIN.	Unlock the SIM 2 by entering the correct PIN for SIM 2.
108	SIM 1 PUK Lock	Major	Alarm to indicate when SIM card 1 has entered PUK lock state.	Unlock the SIM 1 by entering the PUK key for SIM 1.
109	SIM 2 PUK Lock	Major	Alarm to indicate when SIM card 2 has entered PUK lock state.	Unlock the SIM 2 by entering the PUK key for SIM 2.
96	SIM Card Missing	Critical	Alarm to indicate if a PDN profile is configured for a SIM card that is not present. Alarm shall not be raised for empty slot if it is not configured.	Insert a SIM card.

WiFi Interface Path Alarms

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
115	WiFi No Receive Data	Warning	Alarm to indicate that the Wi-Fi connection has received no data packets the defined duration period.	Check Wi-Fi configuration and antenna.
118	WiFi Link Down	Critical	Alarm to indicate when the Wi-Fi link fails.	Check Wi-Fi configuration and antenna.

Component Failure Alarms

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
16	Component Failure	Major	Alarm to indicate that a hardware component has failed.	Power off and restart the Aprisa LTE 5G. If the fault persists, replace the Aprisa LTE 5G.

Diagnostic Alarms

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
100	PDN Profile Switch Occurred	Information	Alarm to indicate that the PDN Profile switch has occurred.	
101	PDN Profile SW Manual Lock	Warning	Alarm to indicate that the PDN Profile SW Manual Lock has been activated.	Deactivate the function if it is no longer required.
127	Port 1 Serial Device Facing Loopback	Warning	Alarm to indicate that the Port 1 Serial Device Facing Loopback has been activated.	Deactivate the function if it is no longer required.

Software Alarms

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
21	Configuration Not Supported	Warning	Alarm to indicate that a configuration has entered that is invalid.	Restore previous configuration, remove out of range or invalid parameters, updated software.
32	Network Configuration Warning	Warning	Alarm to indicate a network configuration problem.	Check for invalid parameters. Audit network settings.
39	Software Restart Required	Warning	Alarm to indicate that a configuration has changed that requires a software reboot.	Reboot the Aprisa LTE 5G.
130	IP-SLA Failure	Warning	Alarm to indicate that an IP-SLA is in a failed state.	Check the network connectivity for the affected IP SLA.

Security Alarms

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
126	Tamper Detected	Critical	Alarm to indicate that the Tamper detector has been triggered.	Investigate possible security breach. Hardware may no longer be trusted and should be replaced.
1xx	Security Module Battery	Critical	Alarm to indicate that the Security Module battery low battery voltage.	The security module battery should be replaced.
114	IPsec Tunnel Connection Failure	Warning	Alarm to indicate that one or more of the IPsec Tunnel connections have lost connectivity.	Check IPsec configuration. Check network connectivity. Check IP Configuration.

GNSS Alarms

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
125	GNSS Position Accuracy	Warning	Alarm to indicate if GNSS signal HDOP is > 5...	Check GNSS antenna and connection.
124	GNSS Signal Lost	Minor	Alarm to indicate if GNSS signal is lost. Alarm will not show for first 60 seconds after GNSS is enabled. When alarm is cleared, additional info should indicate the newly discovered position.	Check GNSS antenna and connection.

Configurator Alarms

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
143	Config Server Connection Failed	Minor	Alarm to indicate that Aprisa LTE radio is unable to connect or lost connection to Configurator server	Check Configurator settings of Aprisa LTE and ensure all the parameters are set correctly (i.e., Server Address, Certificates, etc. Also verify connectivity by pinging the server.).
144	Config Server Provisioning Not Completed	Warning	Alarm to indicate that configuration is not completed on Aprisa LTE radio by the Configurator server	Check the Configurator server settings and ensure all parameters are set correctly. Also check the server to make sure that the Aprisa LTE has been correctly defined.

Alarm Input Alarms

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
24	Alarm Input 1	Warning	Alarm to indicate that there is an active alarm on hardware alarm input 1.	Action depends on nature of third-party alarm.

Power Supply Alarms

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
56	VDC Power	Warning	Alarm to indicate that the input power source is outside the operating limits of 9 to 32 VDC	Check DC connection to the Aprisa LTE 5G. Replace power supply.

Temperature Alarms

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
4	Temperature Threshold	Warning	Alarm to indicate that the Aprisa LTE 5G is outside the operating limits of -30 to +70˚ C.	Check ambient temperature and for airflow obstructions.

6.   Product Specifications

Aprisa LTE 5G router

Router

Aprisa LTE 5G	Downlink LTE Cat-6 (300 / 50 Mbps) / Cat-12 (600 / 150 Mbps) Uplink LTE Cat-6 / 7 / 12 / 13
USA LTE 4G Band Options	B1, B2, B3, B4, B5, B7, US B8, B9, B12, B13, B14, B17, B18, B19, B20, B21, B25, B26, B28, B29, B30, B32, B34, B38, B39, B40, B41, B42, B43, B46, B48, B66, and B71
Global LTE 4G Band Options	B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B14, B18, B19, B20, B21, B25, B26, B28, B29, B30, B32, B38, B39, B40, B41, B42, B43, B46, B48, and B66
Global LTE 5G Band Options	n1, n2, n3, n5, n7, n8, n12, n13, n14, n18, n20, n25, n28, n30, n38, n40, n41, n48, n66, n71, n75, n77, n78, n79
SIMs	Dual 3FF (micro SIM) cards 15 mm x 12 mm x 0.76 mm
GNSS Positioning and Timing	GPS, GLONASS, Beidou, Galileo, and QZSS (option)

Protocols

Ethernet	IEEE 802.3, 802.1d/q/p Ethernet 10/100/1000BASE-T and 100/1000Base-X
Serial	RS-232 / RS-422 / RS-485
Wi-Fi	IEEE 802.11 b/g/n/ac
VPN	IPsec and GRE
Router	MP-BGP/BGP, EIGRP, OSPF, RIPv2, DMVPN
IP SLA	Supported
QoS	Ingress policing with two rate three colour marking FIFO, fair queue, and prioritised schedulers

Wi-Fi

Frequency Range	2.4 to 2.495 GHz, 5.15 to 5.825 GHz
Performance	802.11ac Wave 2 (2x2) MU-MIMO
Encryption	WPA / WPA2 Personal / Enterprise Mixed with options for TKIP and CCMP ciphers
Modes	Access Point and Client

Security

Symmetric Encryption	3DES AES 128, 192, or 256 CBC/CTR/CCM8-CCM16/GCM8-GCM16
Authentication	MD5/SHA-1/SHA-256/SHA-384/SHA-512
DH Group	DH-1/DH-2/DH-5/DH-14/DH-15/DH-19/DH-20/DH-21
IKE	IKEv1 and IKEv2
Key Wrap	AES Key Wrap Algorithm to RFC 3394
FIPS	FIPS 197 (AES) and FIPS 140-2: Security Requirements
Hardening	NIST SCAP processes monitoring
Tamper	MEMS high-performance 3-axis accelerometer

Interface Specifications

Ethernet Interface

The Aprisa LTE 5G router features two integrated IEEE 802.3 Ethernet 1000Base-TX interfaces.

To simplify network setup, each port supports auto-negotiation and auto-sensing MDI/MDIX. Operators can select from the following preset modes:

- Auto negotiate

The Ethernet ports are IEEE 802.3-compatible. The L2 Bridge (Switch) is IEEE 802.1d/q/p compatible, supporting VLANs and VLAN manipulation of add/remove VLANs.

General	Interface	RJ45 x 2 (Integrated 2-port switch)
	Cabling	CAT-5/5e/6 UTP/STP, supports auto MDIX (Standard Ethernet)
	Maximum line length	100 metres on cat-5 or better
	Bandwidth allocation	The Ethernet capacity maximum is determined by the available Aprisa LTE 5G router link capacity.
	Maximum transmission unit	Option setting up to 9216 bytes (Jumbo packet)
	Address table size	Unlimited
	Ethernet mode	10Base-T, 100Base-TX, 1000Base-TX Full duplex or half duplex (Auto-negotiating and auto-sensing)
Diagnostics	Left Green LED	Off: no Ethernet signal received On: Ethernet signal received
	Right Orange LED	Off: no data present on the interface Flashing: data present on the interface

Note: Do not connect Power over Ethernet (PoE) connections to the Aprisa LTE 5G Ethernet ports as this will damage the port.

Ethernet Interface (with SFP)

The Aprisa LTE 5G router has one SFP Module Socket for fitting of optional SFP modules see 'SFP Modules' on page 64. An Ethernet SFP module can be fitted in this socket.

Operators can select from the following preset modes:

- Auto negotiate

The SFP Ethernet port is IEEE 802.3-compatible. The L2 Bridge (Switch) is IEEE 802.1d/q/p compatible, supporting VLANs and VLAN manipulation of add/remove VLANs.

RS-232 Asynchronous Interface

The Aprisa LTE 5G router's ITU-T V.24 compliant RS-232 interface is configured as a Cisco® pinout DCE. The interface terminates to a DTE using a straight-through cable or to a DCE with a crossover cable (null modem).

The interface uses two handshaking control lines between the DTE and the DCE.

General	Interface	ITU-T V.24 / EIA/TIA RS-232E
	Interface direction	DCE only
	Maximum line length	10 metres (dependent on baud rate)
Async parameters	Standard mode data bits	7 or 8 bits
	Standard mode parity	Configurable for None, Even or Odd
	Standard mode stop bits	1 or 2 bits
	Interface baud rates	300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 and 115200 bit/s
Control signals	DCE to DTE	CTS, RTS, DSR, DTR
Diagnostics	Left Green LED	Off: no RS-232 device connected On: RS-232 device connected
	Right Orange LED	Off: no data present on the interface Flashing: data present on the interface

General Purpose I/O (GPIO) Pin Interface

The GPIO interface supports one input pin and one output pin (on the power connector).

Input

Interface	Pin 3 of Molex Micro-Fit 3.0 Connector
Detector type	Non-isolated ground referenced voltage detector
Detection voltage - on	> +9 VDC
Detection voltage - off	< +4 VDC
Maximum applied input voltage	36 VDC
Maximum input current limit	2.7mA

Output

Interface	Pin 4 of Molex Micro-Fit 3.0 Connector
Output type	Non-isolated ground referenced open collector output
Output voltage	VDC power input voltage
Maximum drive current	200 mA
Overload protection	Internally protected

Power Specifications

Power Supply

Input voltage	+9 to +32 VDC negative earthed
Sleep power	< 40 mW
Idle power	< 3.6 W
Peak power	< 15 W
Connector	Pins 1 & 2 of Molex Micro-Fit 3.0 Male Connector

General Specifications

Environmental

Operating temperature range	-30 to +70˚ C (-22 to +158˚ F)
Storage temperature range	-40 to +85˚ C (-40 to +185˚ F)
Max thermal loading	26.6 BTU/hr
Operating humidity	Maximum 95% non-condensing
Acoustic noise emission	No audible noise emission

Mechanical

Dimensions	Width 177 mm (6.97") Depth 110 mm (4.33") and 136 mm (5.35") with QMA connectors Height 41.5 mm (1.63")
Weight	740 g (1.67 lbs)
Colour	Matt black
Mounting	Wall (2 x M5 screws) Rack shelf (4 x M4 screws) DIN rail bracket

7.   Open Source License Statement

This product contains open source software. Full details and license terms are provided in the separate document *Aprisa LTE 5G Open Source License Statement*. This document is available at www.github.com/4rf/lte.

8.   Trademarks and Service

Trademarks

LTE is a trademark of ETSI, used with permission for Aprisa products containing LTE functionality.

FirstNET and FirstNET Trusted are registered trademarks and service marks of the First Responder Network Authority,

AT&T is a trademark of AT&T Intellectual Property II., L.P., T-Mobile is a trademark of Deutsche Telekom AG, Verizon Wireless is a trademark of Verizon Trademark Services, LLC. UScellular is a trademark of United States Cellular Corporation. Aviat Networks products and services are not affiliated with these companies.

OnGo is a trademark of OnGo Alliance, Aviat Networks is an Advisor Member of the OnGo Alliance.

The use of the trademarks AT&T and Verizon indicates compatibility and does not indicate endorsement.

USB-C is a trademark of the USB Implementers Forum.

Service

All hardware maintenance must be completed by Aviat Networks or an authorized service centre.

Do not attempt to carry out repairs to any boards or parts.

Return faulty Aprisa LTE 5G routers to Aviat Networks or an authorized service centre.

For more information on maintenance and training, please contact Aviat Networks Customer Services at tacsupport@aviatnet.com.

CAUTION: Electro Static Discharge (ESD) can damage or destroy the sensitive electrical components in the Aprisa LTE 5G router.

9. Product End Of Life

End-of-Life Recycling Programme (WEEE)

The WEEE Directive concerns the recovery, reuse, and recycling of electronic and electrical equipment. Under the Directive, used equipment must be marked, collected separately, and disposed of properly.

Aviat Networks has implemented an end-of-life recycling programme to manage the reuse, recycling, and recovery of waste in an environmentally safe manner using processes that comply with the WEEE Directive (EU Waste Electrical and Electronic Equipment 2002/96/EC).

The WEEE Symbol Explained

This symbol appears on Electrical and Electronic Equipment (EEE) as part of the WEEE (Waste EEE) directive. It means that the EEE may contain hazardous substances and must not be thrown away with municipal or other waste.

WEEE Must Be Collected Separately

You must not dispose of electrical and electronic waste with municipal and other waste. You must separate it from other waste and recycling so that it can be easily collected by the proper regional WEEE collection system in your area.

YOUR ROLE in the Recovery of WEEE

By separately collecting and properly disposing of WEEE, you are helping to reduce the amount of WEEE that enters the waste stream.

One of the aims of the WEEE directive is to divert EEE away from landfill and encourage recycling. Recycling EEE means that valuable resources such as metals and other materials (which require energy to source and manufacture) are not wasted. Also, the pollution associated with accessing new materials and manufacturing new products is reduced.

EEE Waste Impacts the Environment and Health

Electrical and electronic equipment (EEE) contains hazardous substances which have potential effects on the environment and human health. If you want environmental information on the Aprisa LTE 5G router, contact us (on page 19).