4RF

Aprisa SR+

User Manual

September 2015

Version 1.5.2a

Copyright

Trademarks

Aprisa and the 4RF logo are trademarks of 4RF Limited.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries. Java and all Java-related trademarks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All other marks are the property of their respective owners.

Disclaimer

Although every precaution has been taken preparing this information, 4RF Limited 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 interests of improving the product.

RoHS and WEEE Compliance

The Aprisa SR+ 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).

4RF 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.

4RF 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).

4RF invites questions from customers and partners on its environmental programmes and compliance with the European Commission's Directives (sales@4RF.com).

Compliance General

The Aprisa SR+ radio predominantly operates within frequency bands that require a site license be issued by the radio regulatory authority with jurisdiction over the territory in which the equipment is being operated.

It is the responsibility of the user, before operating the equipment, to ensure that where required the appropriate license has been granted and all conditions attendant to that license 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 4RF are based on the Aprisa SR+ radio equipment being installed at a fixed restricted access location and operated in point-to-multipoint or point-to-point mode within the environmental profile defined by EN 300 019, Class 3.4. Operation outside these criteria may invalidate the authorizations and / or license conditions.

The term 'Radio' with reference to the Aprisa SR+ User Manual, is a generic term for one end station of a point-to-multipoint Aprisa SR+ network and does not confer any rights to connect to any public network or to operate the equipment within any territory.

Compliance European Telecommunications Standards Institute

The Aprisa SR+ radio is designed to comply with the European Telecommunications Standards Institute (ETSI) specifications as follows:

	12.5 kHz and 25 kHz Channel	50 kHz Channel
Radio performance	EN 300 113-2	EN 302 561 (pending)
EMC	EN 301 489 Parts 1 & 5	
Environmental	EN 300 019, Class 3.4 Ingress Protection code IP51	
Safety	EN 60950-1:2006 Class 1 div 2 for hazardous locations	

Frequency band	**Channel size**	**Power input**	**Notified body**
135-175 MHz	12.5 kHz, 25 kHz	12 VDC	
320-400 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	
400-470 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	
450-520 MHz	12.5 kHz, 25 kHz	12 VDC	

Compliance Federal Communications Commission

The Aprisa SR+ radio is designed to comply with the Federal Communications Commission (FCC) specifications as follows:

Radio	47CFR part 24, part 90 and part 101 Private Land Mobile Radio Services
EMC	47CFR part 15 Radio Frequency Devices, EN 301 489 Parts 1 & 4
Environmental	EN 300 019, Class 3.4 Ingress Protection code IP51
Safety	EN 60950-1:2006 Class 1 div 2 for hazardous locations

Frequency Band *	**Channel size**	**Power input**	**Authorization**	**FCC ID**
135-175 MHz	12.5 kHz, 25 kHz	12 VDC	Part 90	Pending
215-240 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	Part 90	UIPSQ215M141
400-470 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	Part 90	UIPSQ400M131
450-520 MHz	12.5 kHz, 25 kHz	12 VDC	Part 90	UIPSQ450M140
896-902 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	Part 24 / Part 90	UIPSQ896M141
928-960 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	Part 24 / Part 90	UIPSQ928M140

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

* The Frequency Band is not an indication of the exact frequencies approved by FCC.

Compliance Industry Canada

The Aprisa SR+ radio is designed to comply with Industry Canada (IC) specifications as follows:

Radio	RSS-119 / RSS-134
EMC	This Class A digital apparatus complies with Canadian standard ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.
Environmental	EN 300 019, Class 3.4 Ingress Protection code IP51
Safety	EN 60950-1:2006 Class 1 div 2 for hazardous locations

Frequency Band *	**Channel size**	**Power input**	**Authorization**	**IC**
135-175 MHz	12.5 kHz, 25 kHz	12 VDC	RSS-119	Pending
215-240 MHz	12.5 kHz	12 VDC	RSS-119	6772A-SQ215M141
400-470 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	RSS-119	6772A-SQ400M131
896-902 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	RSS-119 and RSS-134	6772A-SQ896M141
928-960 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	RSS-119 and RSS-134	6772A-SQ928M140

* The Frequency Band is not an indication of the exact frequencies approved by IC.

Compliance Brazil

Este produto será comercializado no Brasil com as configurações abaixo:

Faixa de frequência: 406,10 a 413,05, 423,05 a 430 MHz, 451,00625 a 452,0065 MHz, 459 a 460 MHz, 461,0025 a 462,00625 MHz e 469 a 470 MHz.

Modulações: QPSK, 16QAM e 64QAM

BW: 12,5 e 25 KHz.

Compliance Hazardous Locations Notice

This product is suitable for use in Class 1, Division 2, Groups A - D hazardous locations or non-hazardous locations.

The following text is printed on the Aprisa SR+ fascia:

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 SR+ 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.

The USB service ports are not to be used unless the area is known to be non-hazardous.

RF Exposure Warning

WARNING:

The installer and / or user of Aprisa SR+ radios shall ensure that a separation distance as given in the following table is maintained between the main axis of the terminal's antenna and the body of the user or nearby persons.

Minimum separation distances given are based on the maximum values of the following methodologies:

1. Maximum Permissible Exposure non-occupational limit (B or general public) of 47 CFR 1.1310 and the methodology of FCC's OST/OET Bulletin number 65.
2. Reference levels as given in Annex III, European Directive on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz) (1999/519/EC). These distances will ensure indirect compliance with the requirements of EN 50385:2002.

Frequency (MHz)	Maximum Power (dBm) Note 1	Maximum Antenna Gain (dBi)	Minimum Separation Distance (m)
135	+ 37	15	3.5
175	+ 37	15	3.5
215	+ 37	15	3.5
240	+ 37	15	3.5
320	+ 37	15	3.5
400	+ 37	15	3.0
450	+ 37	15	3.0
470	+ 37	15	3.0
520	+ 37	15	3.0
896	+ 37	28	10.0
902	+ 37	28	10.0
928	+ 37	28	9.5
960	+ 37	28	9.5

Note 1: The Peak Envelope Power (PEP) at maximum set power level is +41 dBm.

Contents

1. Getting Started

This section is an overview of the steps required to commission an Aprisa SR+ radio network in the field:

Phase 1:	Pre-installation	
1.	Confirm path planning.	Page 50
2.	Ensure that the site preparation is complete: • Power requirements • Tower requirements • Environmental considerations, for example, temperature control • Mounting space	Page 53

Phase 2:	Installing the radios	
1.	Mount the radio.	Page 56
2.	Connect earthing to the radio.	Page 55
3.	Confirm that the: • Antenna is mounted and visually aligned • Feeder cable is connected to the antenna • Feeder connections are tightened to recommended level • Tower earthing is complete	
4.	Install lightning protection.	Page 55
5.	Connect the coaxial jumper cable between the lightning protection and the radio antenna port.	Page 60
6.	Connect the power to the radio.	Page 61

Phase 3:	Establishing the link	
1.	If radio's IP address is not the default IP address (169.254.50.10 with a subnet mask of 255.255.0.0) and you don't know the radio's IP address see 'Command Line Interface' on page 305.	Page 305
2.	Connect the Ethernet cable between the radio's Ethernet port and the PC.	
3.	Confirm that the PC IP settings are correct for the Ethernet connection: • IP address • Subnet mask • Gateway IP address	Page 69
4.	Open a web browser and login to the radio.	Page 73
5.	Set or confirm the RF characteristics: • TX and RX frequencies • TX output power	Page 96
6.	Compare the actual RSSI to the expected RSSI value (from your path planning).	
7.	Align the antennas.	Page 311
8.	Confirm that the radio is operating correctly; the OK, MODE and AUX LEDs are green.	

2. Introduction

About This Manual

What It Covers

This user manual describes how to install and configure an Aprisa SR+ point-to-multipoint digital radio network.

It specifically documents an Aprisa SR+ radio running system software version 1.5.2 .

It is recommended that you read the relevant sections of this manual before installing or operating the radios.

Who Should Read It

This manual has been written for professional field technicians and engineers who have an appropriate level of training and experience.

Contact Us

If you experience any difficulty installing or using Aprisa SR+ after reading this manual, please contact Customer Support or your local 4RF representative.

Our area representative contact details are available from our website:

4RF Limited

26 Glover Street, Ngauranga

PO Box 13-506

Wellington 6032

New Zealand

E-mail	support@4rf.com
Web site	www.4rf.com
Telephone	+64 4 499 6000
Facsimile	+64 4 473 4447
Attention	Customer Services

What's in the Box

Inside the box you will find:

- One Aprisa SR+ radio fitted with a power connector.
- One Aprisa SR+ Accessory kit containing the following:

  Aprisa SR+ CD
  Aprisa SR+ Quick Start Guide
  Management Cable

Aprisa SR+ Accessory Kit

The accessory kit contains the following items:

Aprisa SR+ Quick Start Guide

Aprisa SR+ CD

Management Cable
USB Cable USB A to USB micro B, 1m

Aprisa SR+ CD Contents

The Aprisa SR+ CD contains the following:

Software

- The latest version of the radio software (see 'Software Upgrade' on page 340)
- USB Serial Driver
- Web browsers - Mozilla Firefox and Internet Explorer are included for your convenience
- Adobe™ Acrobat® Reader® which you need to view the PDF files on the Aprisa SR+ CD

Documentation

- User manual - an electronic (PDF) version for you to view online or print
- Product collateral - application overviews, product description, quick start guide, case studies, software release notes and white papers

3. About the Radio

The 4RF Aprisa SR+ Radio

The 4RF Aprisa SR+ is a point-to-multipoint digital radio providing secure narrowband wireless data connectivity for SCADA, infrastructure and telemetry applications.

The radios carry a combination of serial data and Ethernet data between the base station, repeater stations and remote stations.

A single Aprisa SR+ is configurable as a point-to-multipoint base station, a remote station or a repeater station.

Product Overview

Network Coverage and Capacity

The Aprisa SR+ has a typical link range of up to 120 km, however, geographic features, such as hills, mountains, trees and foliage, or other path obstructions, such as buildings, will limit radio coverage. Additionally, geography may reduce network capacity at the edge of the network where errors may occur and require retransmission. However, the Aprisa SR+ uses 10W output power and Forward Error Correction (FEC) which greatly improves the sensitivity and system gain performance of the radio resulting in less retries and minimal reduction in capacity.

Ultimately, the overall performance of any specific network will be defined by a range of factors including the RF output power, the modulation used and its related receiver sensitivity, the geographic location, the number of remote stations in the base station coverage area and the traffic profile across the network. Effective network design will distribute the total number of remote stations across the available base stations to ensure optimal geographic coverage and network capacity.

One base station can register and operate with up to 500 remote / repeater stations.

The practical limit of remote / repeater stations that can operate with one base station is determined by a range of factors including the number of services, the packet sizes, the protocols used, the message types and network timeouts.

Automatic Registration

On start-up, the remote station transmits a registration message to the base stations which responds with a registration response. This allows the base station to record the details of all the remote stations active in the network.

If a remote station cannot register with the base station after multiple attempts within 10 minutes, it will automatically reboot. If remote is not able to register with base station in 5 attempts, then a ‘Network Configuration Warning’ alarm event will be raised indicating that a remote is not registered with the base station.

If a remote station has registered with the base station but then loses communication, it will automatically reboot within 2 minutes.

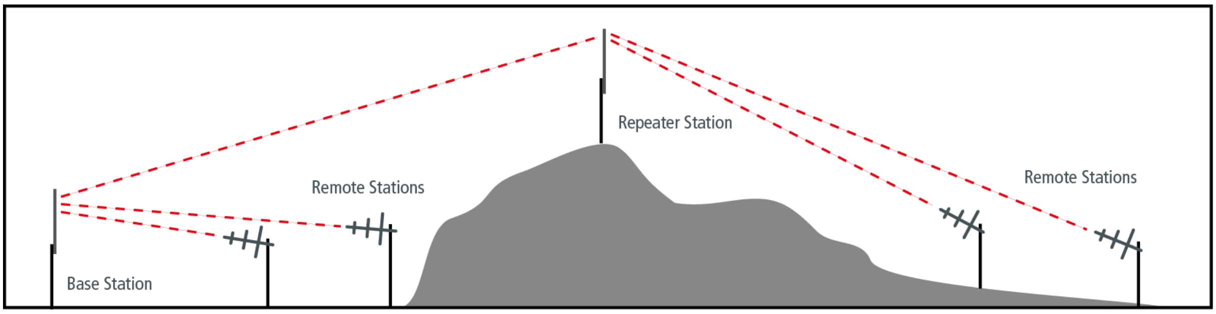
Remote Messaging

There are two message types in the Aprisa SR+ network, broadcast messages and unicast messages. Broadcast messages are transmitted by the base station to the remote stations and unicast messages are transmitted by the remote station to the base station. These messages are commonly referred to as uplink (unicast remote to base) and downlink (broadcast base to remote).

All remotes within the coverage area will receive broadcast messages and pass them on to either the Ethernet or serial interface. The RTU determines if the message is intended for it and will accept it or discard it.

Store and Forward Repeater

The Aprisa SR+ in Repeater mode is used to link remote stations to the base station when direct communication is not possible due to terrain, distance, fade margin or other obstructions in the network. The following example depicts a repeater on the hill top to allow communication between the base station and the remote stations on the other side of hilly terrain.



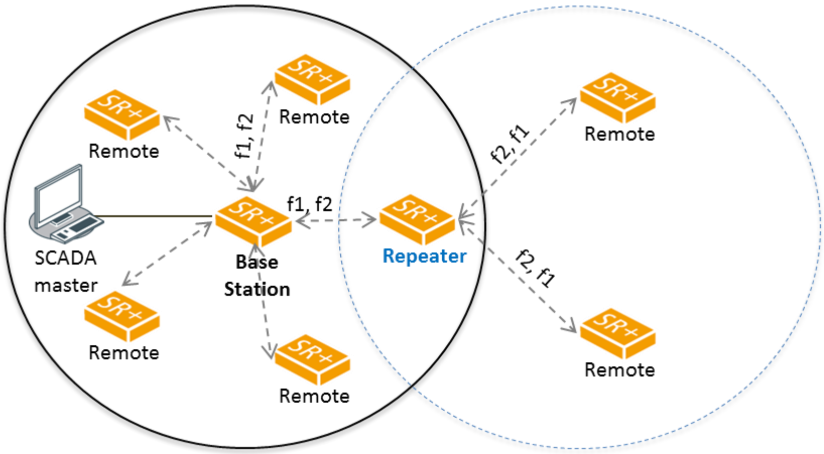
Repeater Packet Forwarding

The Aprisa SR+ works in packet Store and Forward (S&F) for simple and low cost repeater network.

Repeater mode is available in both Access Request (AR) and Listen Before Send (LBS/CSMA) MAC operating modes. It allows a radio in Repeater mode to store a received packet and retransmit it.

Single Repeater Single Hop

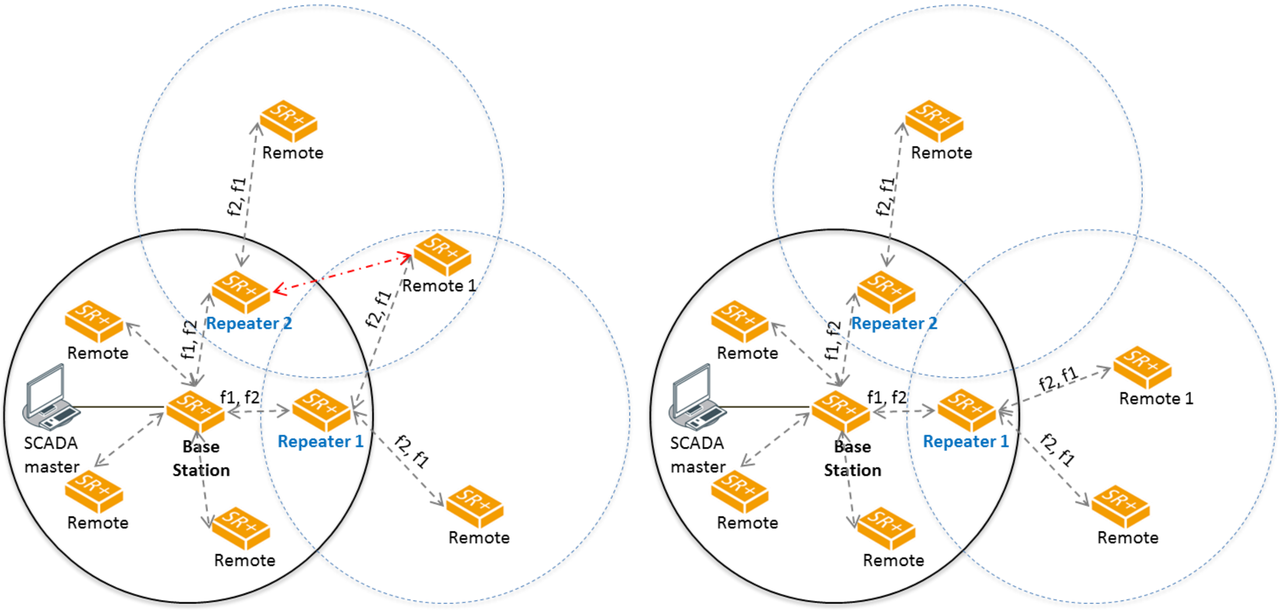
The following example depicts an Aprisa SR+ single repeater single hop Store and Forward network.



Single Hop Store and Forward Repeater

Multiple Repeater Single Hop

The following example depicts an Aprisa SR+ multiple repeater single hop store and forward network supporting both overlapping and non-overlapping coverage repeater networks. An overlapped RF coverage area creates radio interference and might affect network performance and reduce throughput, as show in figure (a), where Remote 1 is in overlapped RF coverage with Repeater 1 and Repeater 2.

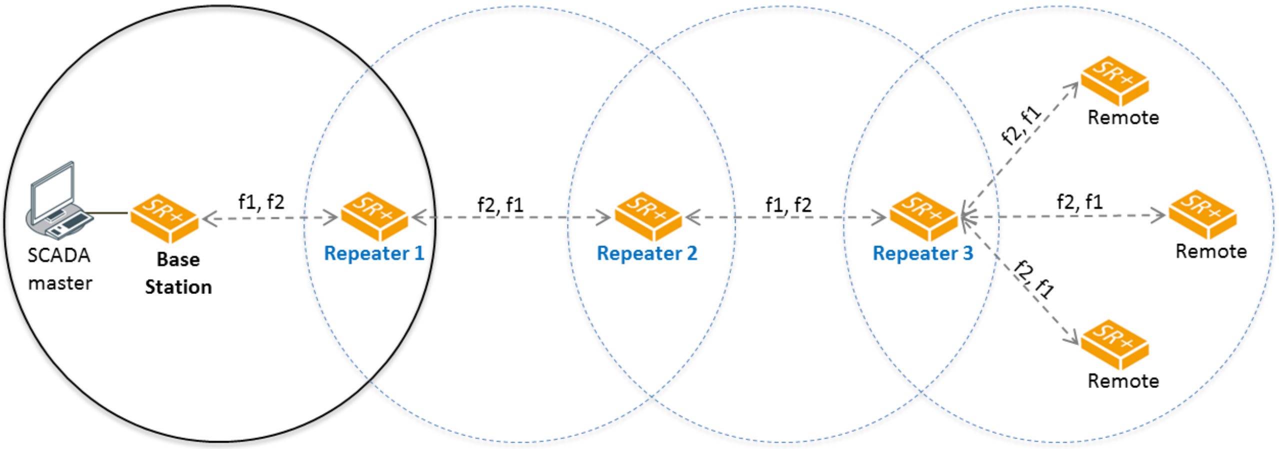


(a) Multiple Repeaters with Overlapping RF Coverage

(b) Multiple Repeaters with Non-Overlapping RF Coverage

Multiple Repeater Multiple Hop

The following example depicts an Aprisa SR+ daisy chain multiple repeater multiple hop store and forward network i.e. multiple hops and multiple repeaters in non-overlapping RF coverage. The Aprisa SR+ daisy chain store and forward repeaters are currently supported in LBS MAC mode only.



Multiple Hop Multiple Store and Forward Repeaters

In any type of store and forward repeater network base, repeater and remote radios must have their Tx/Rx frequencies sets to match to their appropriate linking devices as shown in the figures.

Note: Frequencies shown in the figures relates to the device on the left where {Tx, Rx} = {fx, fy}. In this example, the Base Station, Repeater 2 and remotes are deployed with Tx=f1 and Rx=f2. On the other hand Repeater 1 and Repeater 3 are deployed with Tx=f2 and Rx=f1, creating the required linking for daisy chain operation.

Repeater Messaging

The Aprisa SR+ uses a routed protocol throughout the network whereby messages contain source and destination addresses. The remote and repeater stations will register with a base station. In networks with a repeater, the repeater must register with the base station before the remotes can register with the base station.

Additionally, based on destination address, messages are designated as either a 'broadcast' message, (mostly originating from a base station) or a 'unicast' message (mostly originating from a remote station).

In a network with a repeater, or multiple repeaters, the base station broadcasts a message which contains a source address and a destination address. The repeater receives the message and recognizes it is a broadcast message, from the destination address and re-broadcasts the message across the network. In IP routing mode all remote stations in the coverage area will receive the message but only the radio with the destination address will act upon the message.

Similarly, the remote station will send a unicast message which contains a unicast destination address (the base station). The repeater will receive this message; recognize the destination address and forward it to the appropriate destination address.

In order to prevent repeater-repeater loops, a detection mechanism of 'duplicate message' and use of unicast messaging in remote to base/repeater direction is used.

For example, in the Multiple Repeater Single Hop figure above, the topology is of Base, Repeater 1, Repeater 2 and Remote 1 connected to Repeater 1 in overlapping coverage, where Remote 1 can also hear Repeater 2. When the Base station broadcasts a message, Remote1 will receive this message from both Repeater 1 and Repeater 2 but will drop one of them as 'duplicate message'. It is possible that Repeater 1, for example, can also hear the broadcast sent out by Repeater 2. In this case, Repeater 1 will drop this broadcast as a 'duplicate message'.

These phenomena will not happen in the upstream direction as all messages are sent 'unicast'. Remote 1 will send a packet to Base station, setting the destination address in packet to Base station and 'next hop' address in packet to Repeater 1. Thus, only Repeater 1 will forward the packet to Base station and Repeater 2 will drop the packet as the 'next hop' address is not Repeater 2.

Product Features

Functions

- Point-to-Point (PTP) or Point-to-Multipoint (PMP) operation
- Licensed frequency bands:

VHF 135	135-175 MHz
VHF 220	215-240 MHz
UHF 320	320-400 MHz
UHF 400	400-470 MHz
UHF 450	450-520 MHz
UHF 896	896-902 MHz
UHF 928	928-960 MHz

- Channel sizes – software selectable:
  - 12.5 kHz
  - 25 kHz
  - 50 kHz
- Adaptive Coding Modulation (ACM): QPSK to 64 QAM
- Half duplex or full duplex RF operation
- Ethernet data interface and RS-232 / RS-485 asynchronous multiple port options
- Software selectable dual / single antenna port options (dual antenna port for external duplexers or filters)
- Data encryption and authentication using 128,192 and 256 bit AES and CCM security standards
- Terminal server operation for transporting RS-232 / RS-485 traffic over IP or Ethernet
- Mirrored Bits ® and SLIP support for RS-232
- IEEE 802.1Q VLAN support with single and double VLAN tagged and add/remove VLAN manipulation to adapt to the appropriate RTU / PLCs
- QoS supports using IEEE 802.1p VLAN priority bits to prioritize and handle the VLAN / traffic types
- QoS per port (Ethernet, serial, management)
- L2/3/4 filtering for security and avoiding narrow band radio network overload
- L3 Gateway Router mode with standard static IP route for simple routing network integration
- L3 Router mode with per Ethernet interface IP address and subnet
- L2 Bridge mode with VLAN aware for standard Industrial LAN integration
- Ethernet header and IP/TCP / UDP ROHC header compression to increase the narrow band radio capacity
- Ethernet and serial payload compression to increase the narrow band radio capacity
- Pseudo peer to peer communication between remote stations through base-repeater or repeater stations
- SuperVisor web management support for element and sub-network (base-repeater-remotes) management
- SNMPv1/2/3 & encryption MIB supports for 4RF SNMP manager or third party SNMP agent network management
- SNMP context addressing for compressed SNMP access to remote stations
- SNTP for accurate wide radio network time and date
- RADIUS security for remote user authorization, authentication and accounting
- Build-configuration / flexibility of serial and Ethernet interface ports (3+1, 2+2, 4+0)

- Radio and user interface redundancy (provided with Aprisa SR+ Protected Station)
- Protected Station fully hot swappable and monitored hot standby
- Transparent to all common SCADA protocols; e.g. Modbus, IEC 60870-5-101/104, DNP3 or similar
- Complies with international standards, including ETSI, FCC, IC, ACMA, EMC, safety and environmental standards

Security

The Aprisa SR+ provides security features to implement the key recommendations for industrial control systems. The security provided builds upon the best in class from multiple standards bodies, including:

- IEC/TR 62443 (TC65) 'Industrial Communications Networks – Network and System Security'
- IEC/TS 62351 (TC57) 'Power System Control and Associated Communications – Data and Communication Security'
- FIPS PUB 197, NIST SP 800-38C, IETF RFC3394, RFC3610 and IEEE P1711/P1689/P1685
- FIPS 140-2: Security Requirements for Cryptographic Modules

The security features implemented are:

- Data encryption

  Counter Mode Encryption (CTR) using Advanced Encryption Standard (AES) 128, 192, 256 bit, based on FIPS PUB 197 AES encryption (using Rijndael version 3.0)

- Data authentication

  NIST SP 800-38C Cipher Block Chaining Message Authentication Code (CBC-MAC) based on RFC 3610 using Advanced Encryption Standard (AES)

- Data payload security

  CCM Counter with CBC-MAC integrity (NIST special publication 800-38C)

- Secured management interface protects configuration
- L2 / L3 / L4 Address filtering enables traffic source authorization
- Proprietary physical layer protocol and modified MAC layer protocol based on standardized IEEE 802.15.4
- Licensed radio spectrum provides recourse against interference
- SNMPv3 with Encryption for NMS secure access
- Secure USB software upgrade
- Key Encryption Key (KEK) based on RFC 3394, for secure Over The Air Re-keying (OTAR) of encryption keys
- User privilege allows the accessibility control of the different radio network users and the user permissions

Performance

- Typical deployment of 30 remote stations from one base station with a practical limit of a few hundred remote stations
- Long distance operation
- High transmit power
- Low noise receiver
- Forward Error Correction
- Electronic tuning over the frequency band
- Thermal management for high power over a wide temperature range

Usability

- Configuration / diagnostics via front panel Management Port USB interface, Ethernet interface
- Built-in webserver SuperVisor with full configuration, diagnostics and monitoring functionality, including remote station configuration / diagnostics over the radio link
- LED display for on-site diagnostics
- Dedicated alarm port
- Software upgrade and diagnostic reporting via the host port USB flash drive
- Over-the-air software distribution and upgrades
- Simple installation with integrated mounting holes for wall, DIN rail and rack shelf mounting

System Gain vs FEC Coding

This table shows the relationship between modulation, FEC coding, system gain, capacity and coverage.

- Maximum FEC coding results in the highest system gain, the best coverage but the least capacity
- Minimum FEC coding results in lower system gain, lower coverage but higher capacity
- No FEC coding results in the lowest system gain, the lowest coverage but the highest capacity

This table defines the modulation order based on gross capacity:

Modulation	FEC Coding	Capacity
QPSK (High Gain)	Max Coded FEC	Minimum
QPSK (Low Gain)	Min Coded FEC	
16QAM (High Gain)	Max Coded FEC	
QPSK	No FEC	
16QAM (Low Gain)	Min Coded FEC	
16QAM	No FEC	
64QAM (High Gain)	Max Coded FEC	
64QAM (Low Gain)	Min Coded FEC	Maximum

This table defines the modulation order based on receiver sensitivity:

Modulation	FEC Coding	Coverage
QPSK (High Gain)	Max Coded FEC	Maximum
QPSK (Low Gain)	Min Coded FEC	
16QAM (High Gain)	Max Coded FEC	
QPSK	No FEC	
16QAM (Low Gain)	Min Coded FEC	
64QAM (High Gain)	Max Coded FEC	
16QAM	No FEC	
64QAM (Low Gain)	Min Coded FEC	Minimum

Architecture

The Aprisa SR+ Architecture is based around a layered TCP/IP protocol stack:

- Physical
  Proprietary wireless
  RS-232 and Ethernet interfaces

- Link
  Proprietary wireless (channel access, ARQ, segmentation)
  VLAN aware Ethernet bridge

- Network
  Standard IP
  Proprietary automatic radio routing table population algorithm

- Transport
  TCP, UDP

- Application
  HTTPS web management access through base station with proprietary management application software including management of remote stations over the radio link
  SNMPv1/2/3 for network management application software

Product Operation

There are three components to the wireless interface: the Physical Layer (PHY), the Data Link Layer (DLL) and the Network Layer. These three layers are required to transport data across the wireless channel in the Point-to-Multipoint (PMP) configuration. The Aprisa SR+ DLL is largely based on the 802.15.4 Media Access Control (MAC) layer using a proprietary implementation.

Physical Layer

The Aprisa SR+ PHY uses a one or two frequency half duplex transmission mode which eliminates the need for a duplexer. However, a Dual Antenna port option is available for separate transmit and receive antenna connection to support external duplexers or filters (half duplex operation).

Remote nodes are predominantly in receive mode with only sporadic bursts of transmit data. This reduces power consumption.

The Aprisa SR+ is a packet based radio. Data is sent over the wireless channel in discrete packets / frames, separated in time. The PHY demodulates data within these packets with coherent detection.

The Aprisa SR+ PHY provides carrier, symbol and frame synchronization predominantly through the use of preambles. This preamble prefixes all packets sent over the wireless channel which enables fast Synchronization.

Data Link Layer / MAC layer

The Aprisa SR+ PHY enables multiple users to be able to share a single wireless channel; however a DLL is required to manage data transport. The two key components to the DLL are channel access and hop by hop transmission.

Channel Access

The Aprisa SR+ radio has two modes of channel access, Access Request and Listen Before Send.

Option	Function
Access Request	Channel access scheme where the base stations controls the communication on the channel. Remotes ask for access to the channel, and the base station grants access if the channel is not occupied.
Listen Before Send	Channel access scheme where network elements listen to ensure the channel is clear, before trying to access the channel.

Access Request

This scheme is particularly suited to digital SCADA systems where all data flows through the base station. In this case it is important that the base station has contention-free access as it is involved in every transaction. The channel access scheme assigns the base station as the channel access arbitrator and therefore inherently it has contention-free access to the channel. This means that there is no possibility of contention on data originating from the base station. As all data flows to or from the base station, this significantly improves the robustness of the system.

All data messages are controlled via the AG (access grant) control message and therefore there is no possibility of contention on the actual end user data. If a remote station accesses the channel, the only contention risk is on the AR (access request) control message. These control messages are designed to be as short as possible and therefore the risk of collision of these control messages is significantly reduced. Should collisions occur these are resolved using a random back off and retry mechanism.

As the base station controls all data transactions multiple applications can be effectively handled, including a mixture of polling and report by exception.

Access Request – Full Duplex

This scheme is used in a network with a full duplex base / master station and half duplex repeater / remote stations. Full duplex Access Request utilizes the existing (half duplex) Access Request scheme as described in the section above.

The base / master station can transmit while simultaneously receiving from the remote / repeaters. This increases Access Request efficiency, especially in the report by exception scheme (spontaneous messages).

This feature can be operated on full duplex hardware only (see 'Product Options' section on page 312).

If the Access Scheme is set to full duplex on a repeater, packets start to egress a repeater before the entire packet has been received by the repeater. This scheme reduces latency on long packets through a repeater and improves performance in Overlapping Coverage mode.

To allow this new MAC scheme to operate, two new RF Network Detail parameters have been added; Base Station ID and Repeater Network Segment ID (see 'Base Station ID' on page 86 and 'Repeater Network Segment ID' on page 87).

Listen Before Send

The Listen Before Send channel access scheme is realized using Carrier Sense Multiple Access (CSMA). In this mode, a pending transmission requires the channel to be clear. This is determined by monitoring the channel for other signals for a set time prior to transmission. This results in reduced collisions and improved channel capacity.

There are still possibilities for collisions with this technique e.g. if two radios simultaneously determine the channel is clear and transmit at the same time. In this case an acknowledged transaction may be used. The transmitter requests an ACK to ensure that the transmission has been successful. If the transmitter does not receive an ACK, then random backoffs are used to reschedule the next transmission.

Hop by Hop Transmission

Hop by Hop Transmission is realized in the Aprisa SR+ by adding a MAC address header to the packet. For 802.15.4, there are 2 addresses, the source and destination addresses.

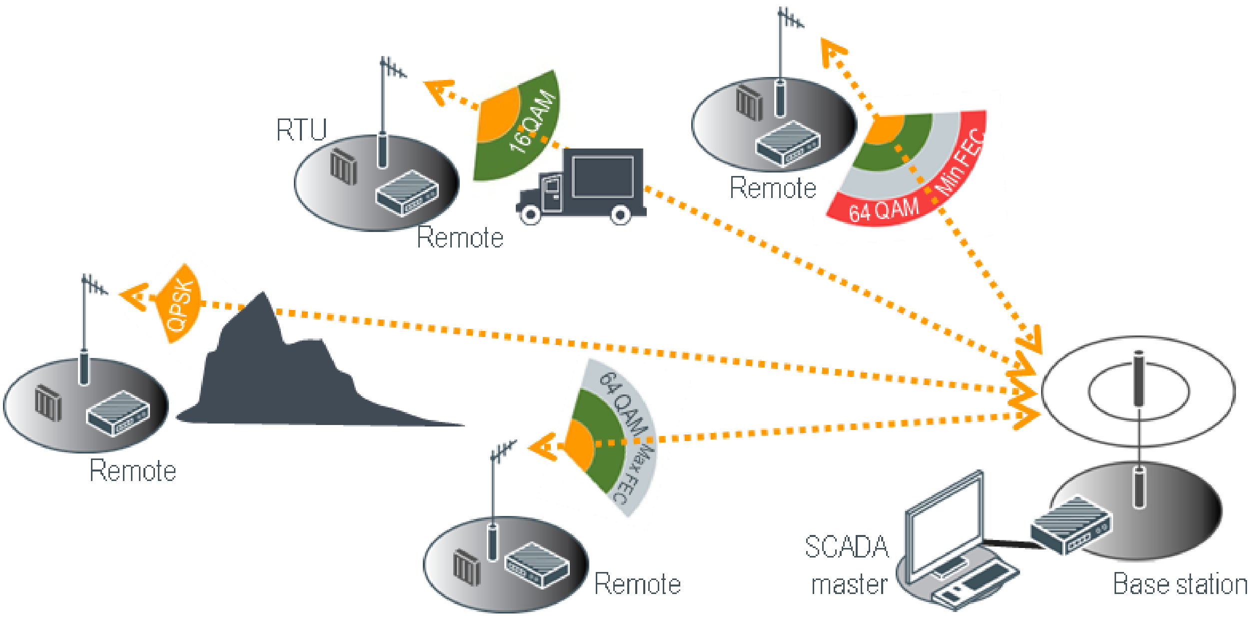
Adaptive Coding Modulation

The Aprisa SR+ provides Adaptive Coding Modulation (ACM) which maximizes the use of the RF path to provide the highest radio capacity available.

ACM automatically adjusts the modulation coding and FEC code rate in the remote to base direction of transmission over the defined modulation range based on the signal quality <u>for each individual remote radio.</u>

When the RF path is healthy (no fading), modulation coding is increased and the FEC code rate is decreased to maximize the data capacity.

If the RF path quality degrades, modulation coding is decreased and the FEC code rate is increased for maximum robustness to maintain path connectivity.



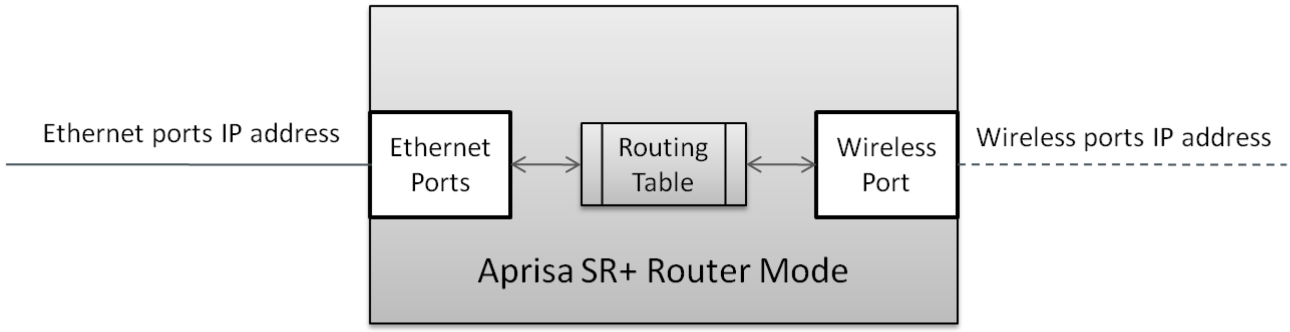
Network Layer

Packet Routing

Aprisa SR+ is a standard static IP router which routes and forwards IP packet based on standard IP address and routing table decisions.

Aprisa SR+ router mode (see figure below), enables the routing of IP packets within the Aprisa SR+ wireless network and in and out to the external router / IP RTUs devices connected to the Aprisa SR+ wired Ethernet ports.

Within the Aprisa SR+ Router mode, each incoming Ethernet packet on the Ethernet port is stripped from its Ethernet header to reveal the IP packet and to route the IP packet based on its routing table. If the destination IP address is one of the RTUs, the packet is then forwarded to the wireless ports and broadcasted as a PMP wireless packet to all the repeater / remotes stations. The appropriate remote then routes the IP packet and forwards it based on its routing table to the appropriate Ethernet port, encapsulating the appropriate next hop MAC header and forwarding it to the RTU. The RTU can then interpret and process the IP data and communication is established between the RTU and the initiating communication device.



Static IP Router

The Aprisa SR+ works in the point-to-multipoint (PMP) network as a standard static IP router with the Ethernet and wireless / radio as interfaces and serial ports using terminal server as a virtual interface.

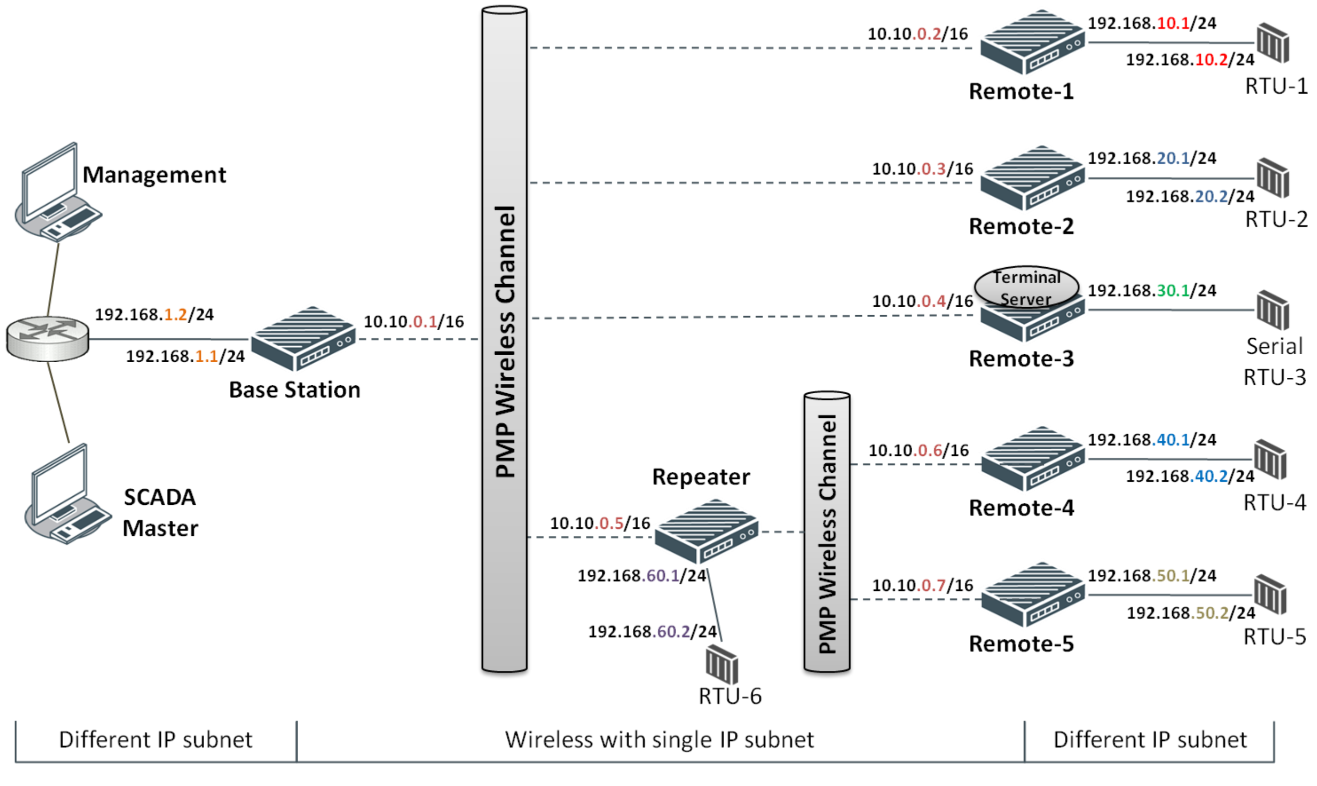
The Aprisa SR+ static router is semi-automated operation, where the routing table is automatically created in the base station and populated with routes to all remotes and repeater stations in the network during the registration process and vice versa, where the routing table is automatically created in remote and repeater stations and populated with routes to base station during the registration process. Updates occur when remote is disconnected from network for any reason, with the routing table updated in a controlled fashion.

Also, in decommission operation, the base station routing tables are completely flushed allowing an automatic rebuild. This avoids the user manually inserting / removing of multiple static routes to build / change the routes in the network which might be tedious and introduce significant human error. The Aprisa SR+ works as a static IP router without using any routing protocol and therefore does not have the overhead of a routing protocol for better utilization of the narrow bandwidth network.

In addition to the semi-automated routes, the user can manually add / remove routes in the routing table for the radio interface, Ethernet Interface and for routers which are connected to the radio network.

The Aprisa SR+ base station is used as a gateway to other networks. Thus, a configurable IP address default gateway can be set using a static route in the routing table with a destination IP address of the destination network address. It is recommended to use a real network IP address (actual device IP) for the gateway and not 0.0.0.0.

The Aprisa SR+ sub-netting rules distinguish between the wireless interface and the remote Ethernet interface where RTUs are connected. The entire wireless network is set on a single IP subnet, while each Aprisa SR+ remote's Ethernet interface is set to a different subnet network. In this way, the user can easily distinguish between the remotes subnet IP addresses.



The Radio Network as a Router

The Aprisa SR+ point-to-multipoint radio network can be considered as a router where the 'network Ethernet interface' on each radio in the network is the 'router port'.

The routing table for all directly attached devices to the Aprisa SR+ network, at the Base or the Remote stations is automatically built and no static routes are required to be entered for those device routes.

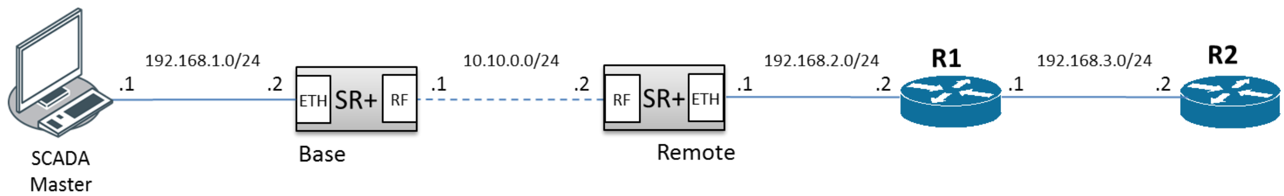
The 'Radio interface IP address' is used internally for the radio network and automatic routes. It is not used when setting static routes or default gateways.

Static route IP addresses or the default gateway should use the 'network Ethernet interface' IP address.

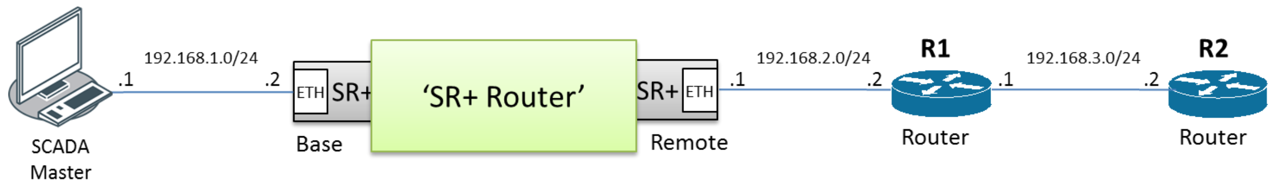
External network routers should be set with a high metric for the SR+ path, to prevent route updates being sent over the radio network.

The Radio Network as a Router – Example

The purpose of this example is to determine the static route setting for router R2 in the base station and remote station in the following network.



Since the Aprisa SR+ network should be considered as a router where the network Ethernet interface is the 'router port', the network configuration for setting the static routes or the default gateway IP addresses is described in the follow figure:



Thus, the static route setting for router R2 at the Aprisa SR+ base station and remote station will be:

Destination Address	Destination Mask	Gateway Address	Static Route Setting at ?
192.168.3.0	255.255.255.0	192.168.2.1	Base station
192.168.3.0	255.255.255.0	192.168.2.2	Remote station

Note: The radio network (base station and remote stations) will automatically build routes to the attached device e.g. SCADA Master station or attached router e.g. router R1 so static routes are not required for these devices.

Static IP Router – Human Error Free

To ensure correct operation, the Aprisa SR+ router base station alerts when one (or more) of the devices is not configured for router mode or a duplicated IP is detected when manually added.

When the user changes the base station IP address / subnet, the base station sends an ARP unsolicited announcement message and the remotes / repeaters auto-update their routing table accordingly. This also allows the router that is connected to the base station to update its next hop IP address and its routing table.

When the user changes the remote / repeater station IP address / subnet, a re-registration process in the base station then auto-updates its routing table accordingly.

Terminal Server - Transition to Converged Ethernet / IP Network

Customers that are transitioning their SCADA network to an Ethernet / IP SCADA network, can simultaneously operate their legacy serial RTUs, not as a separate serial network to the new Ethernet / IP network, but as part of the Ethernet / IP network, by using the terminal server feature.

The Aprisa SR+ terminal server is an application running in the radio that encapsulates serial traffic into Ethernet / IP traffic. For SCADA networks, this enables the use of both serial and Ethernet / IP RTUs within an Ethernet / IP based SCADA network.

Bridge Mode with VLAN Aware

Ethernet VLAN Bridge / Switch Overview

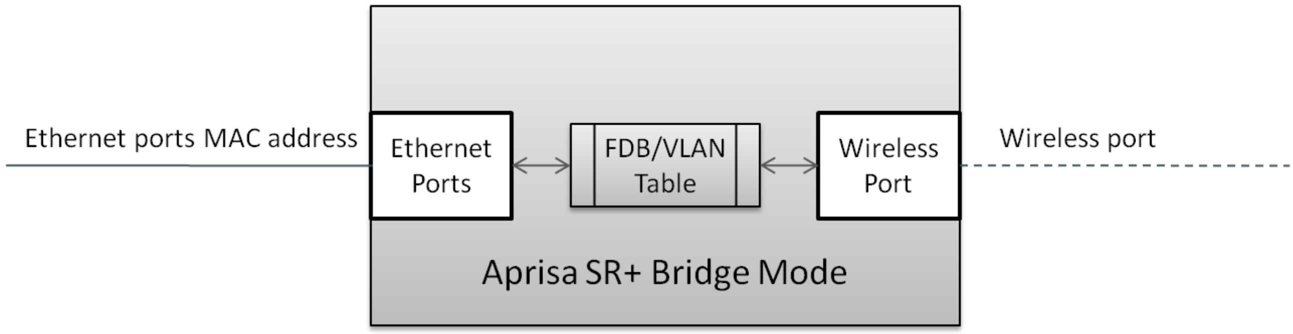
The Aprisa SR+ in Bridge mode of operation is a standard Ethernet Bridge based on IEEE 802.1d or VLAN Bridge based on IEEE 802.1q/p which forward / switch Ethernet packet based on standard MAC addresses and VLANs using FDB (forwarding database) table decisions. VLAN is short for Virtual LAN and is a virtual separate network, within its own broadcast domain, but across the same physical network.

VLANs offer several important benefits such as improved network performance, increased security and simplified network management.

The Aprisa SR+ Bridge mode (see figure below), is the default mode of operation and it enables the switching / bridging of Ethernet VLAN tagged or untagged packets within the Aprisa SR+ wireless network and in and out to the external Industrial LAN network and RTUs devices connected to the Aprisa SR+ wired Ethernet ports or serial ports through the terminal server function.

Within the Aprisa SR+ Bridge mode, each incoming Ethernet packet is inspected for the destination MAC address (and VLAN) and looks up its FDB table for information on where to send the specific Ethernet frame. If the FDB table doesn't contain the specific MAC address, it will flood the Ethernet frame out to all ports in the broadcast domain and when using VLAN, the broadcast domain is narrowed to the specific VLAN used in the packet (i.e. broadcast will be done only to the ports which configured with that specific VLAN).

The FDB table is used to store the MAC addresses that have been learnt and the ports associated with that MAC address. If the destination MAC address is one of the RTUs, the packet is then forwarded to the wireless ports and broadcast as a PMP wireless packet to all the repeater / remote stations. The appropriate remote then switches the Ethernet packet and forwards it based on its FDB table (based on the MAC or VLAN & MAC) to the appropriate Ethernet port to the RTU. The RTU can then interpret and process the Ethernet / IP data and communication is established between the RTU and the initiating communication device.



VLAN Bridge Mode Description

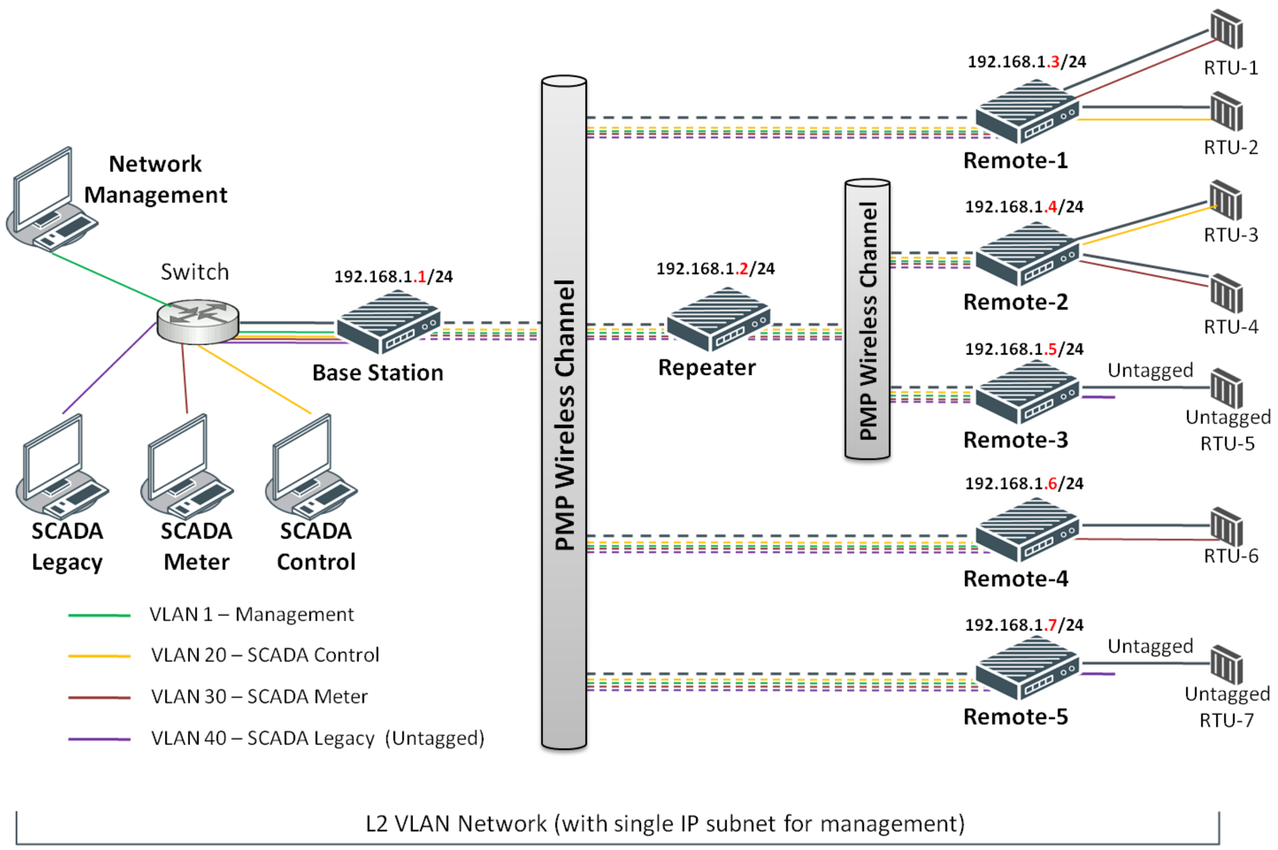
General – Aprisa SR+ VLAN Bridge

The Aprisa SR+ works in a point-to-multipoint (PMP) network as a standard VLAN bridge with the Ethernet and wireless / radio as interfaces and serial ports using terminal server as a virtual interface.

The Aprisa SR+ is a standard IEEE 802.1q VLAN bridge, where the FDB table is created by the bridge learning / aging process. New MACs are learnt and the FDB table updated. Unused MACs are aged out and flushed automatically after aging period.

VLANs are statically configured by the user on the ports where a Virtual LAN is required across the radio network. An example of VLAN isolation of traffic type is shown in the figure below, where RTUs #1, 4 and 6 together with SCADA meter master form a Virtual LAN which is isolated from the other devices, even though they are on the same physical network. VLAN management can be used to manage with external NMS all the Aprisa SR+ devices on the radio network and is automatically created with a VLAN ID = 1 default value. The VLAN ID can be changed by the user later on.

Each device in the Aprisa SR+ bridge is identified by its own IP address, as shown in the figure.



VLANs – Single, Double and Trunk VLAN ports

The Aprisa SR+ supports single VLAN (CVLAN), double VLAN (SVLAN) and trunk VLAN.

A single VLAN can be used to segregate traffic type.

A double VLAN can be used to distinguish between Aprisa SR+ sub-networks (base-repeater-remote), where the outer SVLAN is used to identify the sub-network and the CVLAN is used to identify the traffic type. In this case, a double tagged VLAN will be forwarded across the Industrial LAN network and switched based on the SVLAN to the appropriate Aprisa SR+ sub-network. When packet enters the Aprisa SR+ network, the SVLAN will be stripped off (removed) and the forwarding will be done based on the CVLAN, so only a single VLAN will pass through over the radio network and double VLAN will be valid on the borders of the radio network.

Trunk VLAN is also supported by the Aprisa SR+ where the user can configure multiple VLANs on a specific Ethernet port, creating a trunk VLAN port. For example, in the above figure, a single trunk VLAN port is created between the switch and the Aprisa SR+ base station, carrying VLAN ID #1, 20, 30 and 40.

VLAN Manipulation – Add / Remove VLAN Tags

In order to support double VLAN and different device types connected to the Aprisa SR+ e.g. switches, RTUs, etc, which can be VLAN tagged or untagged / plain Ethernet devices, add / remove VLAN manipulation is required.

In an Aprisa SR+ VLAN tagged network, a remote Aprisa SR+ connected to a plain RTU without VLAN support, will remove (strip-off) the VLAN tag from the packet before sending it to the RTU. On the other direction, when the RTU is sending an untagged packet, the Aprisa SR+ will add (append) an appropriate user pre-configure VLAN tag before sending it over the air to the base station. This is shown in the above figure on untagged RTU #5 and 7.

QoS using VLAN

VLANs carry 3 priority bits (PCP field) in the VLAN tag allowing prioritization of VLAN tagged traffic types with 8 levels of priority (where 7 is the highest priority and 0 is the lowest priority). The Aprisa SR+ supports QoS (Quality of Service) where the priority bits in the VLAN tagged frame are evaluated and mapped to four priority levels and four queues supported by the Aprisa SR+ radio. Packets in the queues are then scheduled out in a strict priority fashion for transmission over-the-air as per the priority level from high to low.

Avoiding Narrow Band Radio Traffic Overloading

The Aprisa SR+ supports mechanisms to prevent narrowband radio network overload:

1. L3/L4 Filtering

The L3 filtering can be used to block undesired traffic from being transferred on the narrow band channel, occupying the channel and risking the SCADA critical traffic. L3/4 filtering has the ability to block a known IP address and applications using TCP/IP or UDP/IP protocols with multiple filtering rules. The L3 (/L4) filter can block/forward (discard/process) a specific IP address and a range of IP addresses. Each IP addressing filtering rule set can also be set to filter a L4 TCP or UDP port/s which in most cases relates to specific applications as per IANA official and unofficial well-known ports. For example, filter and block E-mail SMTP or TFTP protocol as undesired traffic over the SCADA network. The user can block a specific or range of IP port addresses, examples SMTP (Simple Mail Transfer Protocol) TCP port 25 or TFTP (Simple Trivial File Transfer Protocol) UDP port 69.

2. L2 Address Filtering

L2 Filtering (Bridge Mode) provides the ability to filter radio link traffic based on specified Layer 2 MAC addresses. Destination MAC (DA) addresses and a Source MAC (SA) addresses and protocol type (ARP, VLAN, IPv4, IPv6 or Any type) that meet the filtering criteria will be transmitted over the radio link. Traffic that does not meet the filtering criteria will not be transmitted over the radio link.

3. L2 Port VLANs Ingress Filtering and QoS

Double VLAN (Bridge Mode)

Double VLAN is used to distinguish/segregate between different radio sub-networks (Base-repeaters-remotes). Traffic with double VLANs which are not destined to a specific sub-network will be discarded on the ingress of the radio sub-network, avoiding the overload of the radio sub-network.

Single VLAN (Bridge Mode)

Single VLAN is used to distinguish/segregate between different traffic types assigned by the user in its industrial corporate LAN. In order to avoid the overload of the radio network, traffic with single VLANs which are not destined to a specific radio network will be discarded on the Ethernet ingress port of the radio network. All single VLANs which set and are eligible will be transmitted over the radio link.

QoS using 802.1p priority bits (Bridge Mode)

The priority bits can be used in the VLAN tagged frames to prioritized critical mission SCADA traffic and ensure SCADA traffic transmission relative to any other unimportant traffic. In this case, traffic based on VLAN priority (priority 0 to 7) enters one of the four priority queues of the Aprisa SR+ (Very High, High, Medium and Low). Traffic leaves the queues (to the radio network) from highest priority to lowest in a strict priority fashion.

4. Ethernet port QoS

The Aprisa SR+ supports 'Ethernet Per Port Prioritization'. Each Ethernet port can be assigned a priority and traffic shall be prioritized accordingly. This is quite useful in networks where customers do not use VLANs or cannot use 802.1p prioritization.

5. Ethernet Data and Management Priority and Background Bulk Data Transfer Rate

Alternatively to VLAN priority, users can control the Ethernet traffic priority (vs serial), management priority and rate in order to control the traffic load of the radio network, where important and high priority data (SCADA) will pass-through first assuring SCADA network operation. The user can set the use of the Ethernet Data Priority, which controls the priority of the Ethernet customer traffic relative to the serial customer traffic and can be set to one of the four queues. The Ethernet Management Priority controls the priority of the Ethernet management traffic relative to Ethernet customer traffic and can be set to one of the four queues. The Background Bulk Data Transfer Rate sets the data transfer rate (high, medium, low) for large amounts of management data.

6. Ethernet Packet Time to Live

Another aspect of avoiding overload radio network is the Ethernet packet TTL, which is used to prevent old, redundant packets being transmitted through the radio network. This sets the time an Ethernet packet is allowed to live in the system before being dropped if it cannot be transmitted over the air.

7. Robust Header Compression (ROHC) and Payload Compression

Aprisa SR+ supports ROHC (Robust Header Compression RFC3095). ROHC is a standard way to compress IP, UDP and TCP headers and this significantly increases IP traffic throughput especially in narrow band network.

Aprisa SR+ supports payload compression. A Lempel–Ziv (LZ) algorithm is used to efficiently compress up to 50% traffic with high percentage of repetitive strings. Both serial and Ethernet / IP payload traffic are compressed.

Interfaces

Antenna Interface

- 2 x TNC, 50 ohm, female connectors

  Single or dual antenna ports (with or without the use of external duplexer/filter)

Ethernet Interface

- 2, 3 or 4 ports 10/100 base-T Ethernet layer 2 switch using RJ45

  Used for Ethernet user traffic and radio sub-network management.

RS-232 / RS-485 Interface

- 2, 1 or 0 RS-232 asynchronous ports using RJ45 connector
- Optional 1x RS-232 or RS-485 asynchronous port using USB host port with USB to RS-232 or USB to RS-485 converters

USB Interfaces

- 1 x Management port using USB micro type B connector

  Used for product configuration with the Command Line Interface (CLI).

- 1 x Host port using USB standard type A connector

  Used for software upgrade and diagnostic reporting.

Protect Interface

- 1x Protect interface port

  Used for the Protected Station operation.

Alarms Interface

- 1x Alarm port using RJ45 connector

  Used to provide 2 x hardware alarm inputs and 2 x hardware alarm outputs

Front Panel Connections

Example; 2 Ethernet ports and 2 RS-232 serial ports - see 'Data Interface Ports' on page 312 for the other interface port options.

Interface Port Option	**Part Number**
2 Ethernet ports and 2 RS-232 serial ports	APSQ-N400-SSC-HD-22-ENAA

All connections to the radio are made on the front panel. The functions of the connectors are (from left to right):

Designator	Description
10 - 30 VDC; 3A	+10 to +30 VDC (negative ground) DC power input using Molex 2 pin male screw fitting connector. AC/DC and DC/DC power supplies are available as accessories. See 'External Power Supplies' on page 61.
ETHERNET 1 & 2	Integrated 10Base-T/100Base-TX layer-3 Ethernet switch using RJ45 connectors. Used for Ethernet user traffic and product management. See 'Ethernet > Port Setup' on page 127.
SERIAL 1 & 2	Two ports of RS-232 serial using RJ45 connectors. Used for RS-232 asynchronous user traffic. See 'Serial > Port Setup' on page 117.
	Host Port using a USB standard type A connector. Used for software upgrade and diagnostic reporting and optional: 1x RS-232 asynchronous port with USB to RS-232 converter. See 'Software Upgrade' on page 340 and 'Maintenance > General' on page 193.
ALARM	Alarm Port using a RJ45 connector. Used for two alarm inputs and two alarm outputs. See 'Hardware Alarms Interface' on page 372.
MGMT	Management Port using a USB micro type B connector. Used for product configuration with the Command Line Interface. See 'Connecting to the Management Port' on page 305.
PROTECT	Protect port. Used for Protected Station operation.
TX / ANT	TNC, 50 ohm, female connector for connection of antenna feeder cable for half duplex RF operation or the Transmit connection to an external duplexer for full duplex RF operation. See 'Coaxial Feeder Cables' on page 53.
RX	TNC, 50 ohm, female connector for the Receive connection to an external duplexer for full duplex RF operation.

LED Display Panel

The Aprisa SR+ has an LED Display panel which provides on-site alarms / diagnostics without the need for PC.

Normal Operation

In normal radio operation, the LEDs indicate the following conditions:

	OK	MODE	AUX	TX	RX
Flashing Red		*Radio has not registered*			
Solid Red	*Alarm present with severity Critical, Major and Minor*			*TX path fail*	*RX path fail*
Flashing Orange		*Diagnostics Function Active* *OTA software distribution*	*Management traffic on the USB MGMT port*		
Solid Orange	*Alarm present with Warning Severity*		*Device detect on the USB host port (momentary)*		
Flashing Green	*Software Upgrade Successful*	*Stand-by radio in protected station*	*Tx / Rx Data on the USB host port*	*RF path TX is active*	*RF path RX is active*
Solid Green	*Power on and functions OK and no alarms*	*Processor Block is OK* *or active radio in protected station*	*USB interface OK*	*Tx path OK*	*Rx path OK*

LED Colour	**Severity**
Green	No alarm - information only
Orange	Warning alarm
Red	Critical, major or minor alarm

Single Radio Software Upgrade

During a radio software upgrade, the LEDs indicate the following conditions:

- Software upgrade started - the OK LED flashes orange
- Software upgrade progress indicated by running AUX to MODE LEDs
- Software upgrade completed successfully - the OK LED flashes green
- Software upgrade failed - any LED flashing red during the upgrade

Network Software Upgrade

During a network software upgrade, the MODE LED flashes orange on the base station and all remote stations.

Test Mode

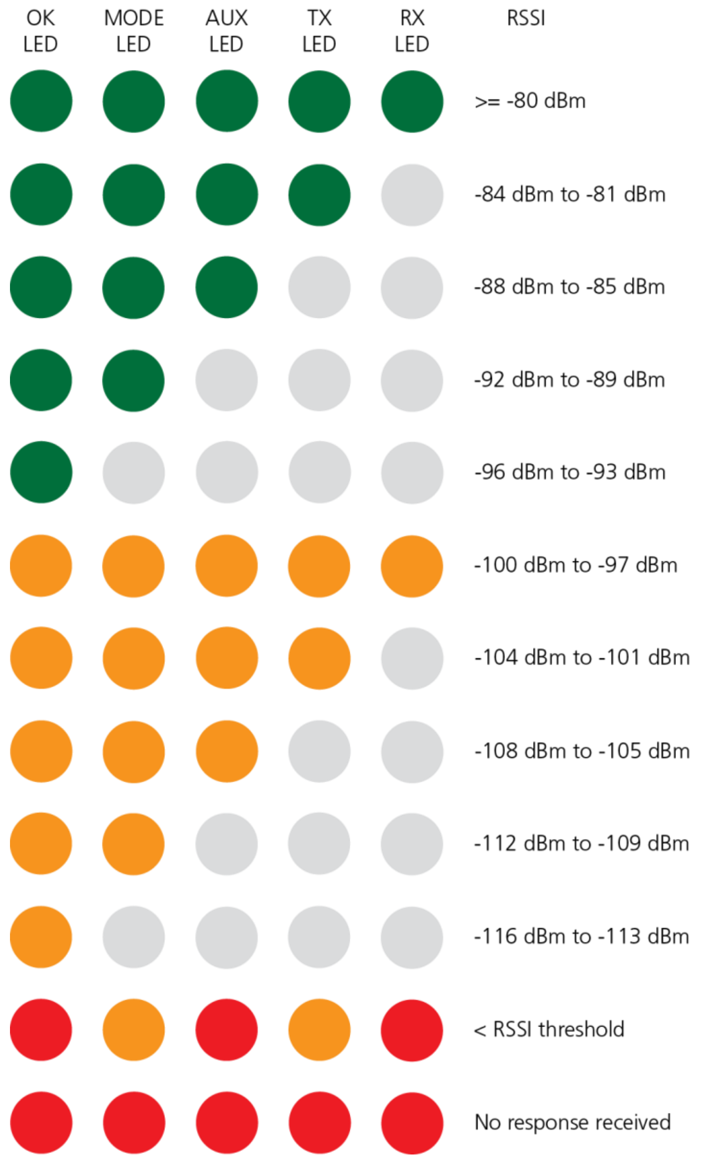
Remote station and repeater station radios have a Test Mode which presents a real time visual display of the RSSI on the LED Display panel. This can be used to adjust the antenna for optimum signal strength (see ‘Maintenance > Test Mode’ on page 195 for Test Mode options).

To enter Test Mode, press and hold the TEST button on the radio LED panel until all the LEDs flash green (about 3 - 5 seconds). The response time is variable and can be up to 5 seconds.

To exit Test Mode, press and hold the TEST button until all the LEDs flash red (about 3 – 5 seconds).

Note: Test Mode traffic has a low priority but could affect customer traffic depending on the relative priorities setup.

The RSSI result is displayed on the LED Display panel as a combination of LED states:



Network Management

The Aprisa SR+ contains an embedded web server application (SuperVisor) to enable element management with any major web browser (such as Mozilla Firefox or Microsoft® Internet Explorer).

SuperVisor enables operators to configure and manage the Aprisa SR+ base station radio and repeater / remote station radios over the radio link.

The key features of SuperVisor are:

- Full element management, configuration and diagnostics
- Manage the entire network from the Base Station (remote management of elements)
- Managed network software distribution and upgrades
- Performance and alarm monitoring of the entire network, including RSSI, alarm states, time-stamped events, etc.
- View and set standard radio configuration parameters including frequencies, transmit power, channel access, serial, Ethernet port settings
- Set and view security parameters
- User management
- Operates over a secure HTTPS session on the access connection to the base station

SuperVisor, when connected to the base station radio allows management of all radios in the network. The Network Table displays a list of all the registered remote stations for the base station and provides management access to each of the remote stations (see ‘Network Status > Network Table’ on page 254).

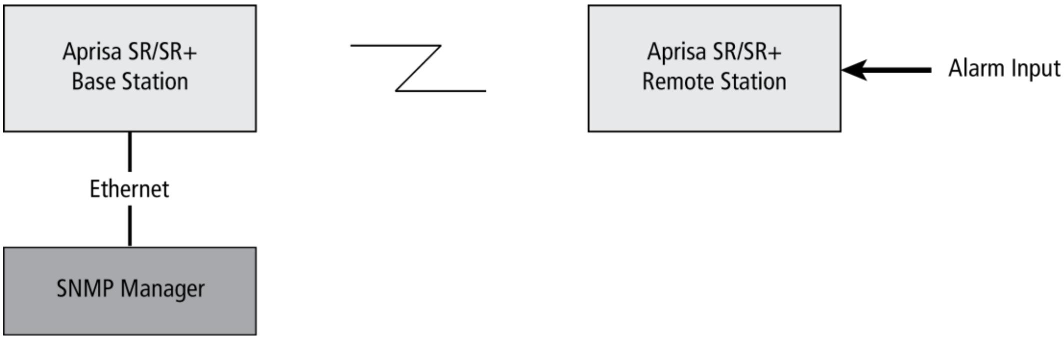
Hardware Alarm Inputs / Outputs

The Aprisa SR+ provides two hardware alarm inputs to generate alarm events in the network and two hardware alarm outputs to receive alarm events from the network.

The hardware alarm inputs and outputs are part of the event system. All alarm events can be viewed in SuperVisor event history log (see 'Events > Event History' on page 207). These include the alarm events generated by the hardware alarm inputs.

Alarm Input to SNMP Trap

An alarm event from an Aprisa SR+ hardware alarm input can be sent over the air to any SNMP Manager using SNMP traps.



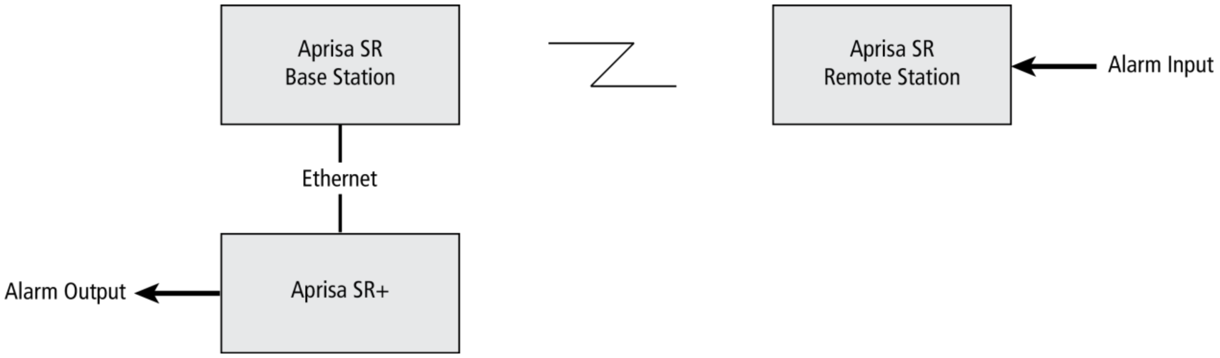
Alarm Input to Alarm Output

An alarm event from an Aprisa SR+ hardware alarm input can be mapped to an hardware alarm output of another SR+ using an event action setup (see 'Events > Event Action Setup' on page 215).

Aprisa SR Alarm Input to Aprisa SR+ Alarm Output

The Aprisa SR+ event action setup feature is compatible with the Aprisa SR.

Since, the Aprisa SR only supports hardware alarm inputs, the Aprisa SR+ can be used as an option to provide a hardware alarm output. As shown in the figure below, an Aprisa SR+ connected on the same IP network of the Aprisa SR, alarm events from the SR hardware alarm input can be mapped to the hardware alarm output of the SR+ using an event action setup.

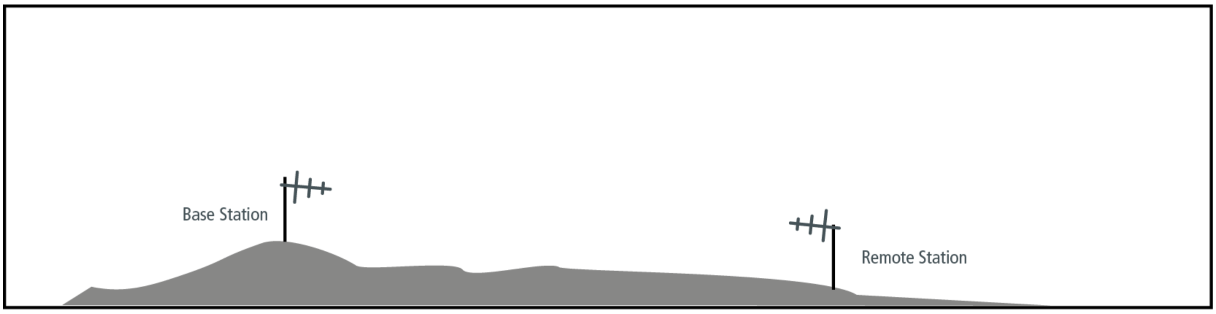


4. Implementing the Network

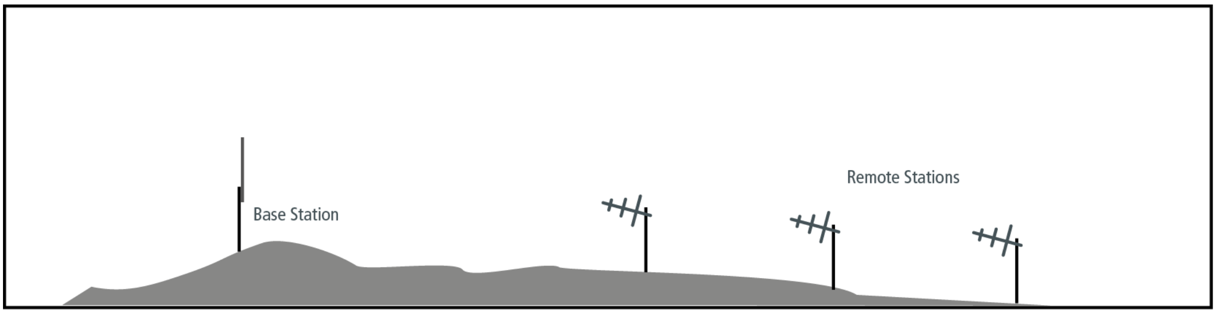
Network Topologies

The following are examples of typical network topologies:

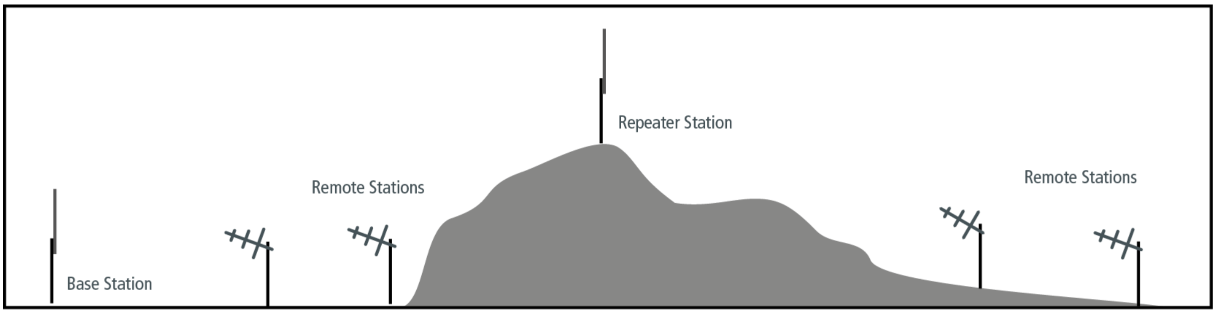
Point-To-Point Network



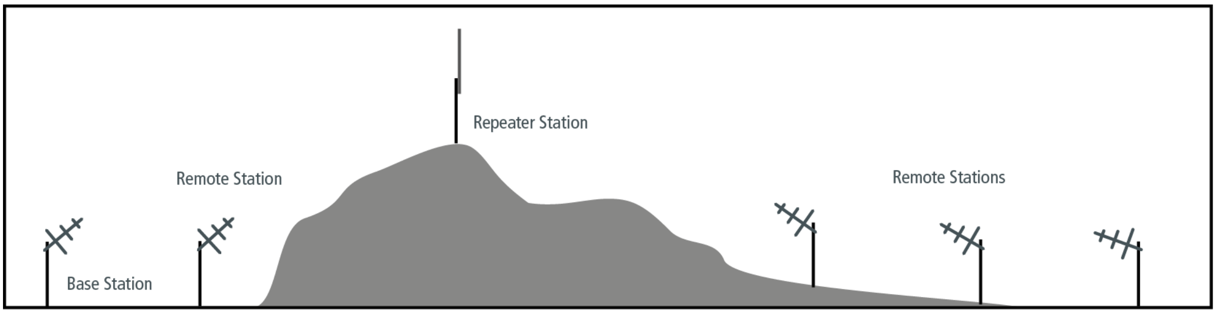
Point-to-Multipoint Network



Point-to-Multipoint with Repeater 1



Point-to-Multipoint with Repeater 2



Initial Network Deployment

Install the Base Station

To install the base station in your network:

1. Install the base station radio (see 'Installing the Radio' on page 56).
2. Set the radio Network ID to a unique ID in your entire network (see 'Terminal > Device' on page 85).
3. Set the radio operating mode to 'base station' (see 'Terminal > Operating Mode' on page 91).
4. Set the radio IP address (see '

.

5. Set the radio frequencies to the frequencies you wish to operate from (see 'Radio > Radio Setup' on page 96).
6. Set the radio security settings (see 'Security > Setup' on page 168).

Installing the Remote Stations

To install the remote stations in your network:

1. Install the remote station radio (see 'Installing the Radio' on page 56).
2. Set the radio Network ID to the same ID as the other stations in the network (see 'Terminal > Device' on page 85).
3. If repeater used in radius 1, set the network radius=2 on all network stations (see 'Terminal > Device' on page 85).
4. Set the radio operating mode to 'remote station' (see 'Terminal > Operating Mode' on page 91).
5. Set the radio IP address (see 'IP > IP Setup > Bridge / Gateway Router Modes' on page 138).
6. Set the radio frequencies to the base station / repeater station frequencies you wish to operate from (see 'Radio > Radio Setup' on page 96).
7. Set the radio security settings to the same as the base station (see 'Security > Setup' on page 168).

The base station will automatically allocate a node address to the new remote station.

Install a Repeater Station

To install a repeater station in your network:

1. Install the repeater station radio (see 'Installing the Radio' on page 56).
2. Set the radio Network ID to the same ID as the other stations in the network (see 'Terminal > Device' on page 85).
3. Increase the radio network radius by one on all stations in the network (see 'Terminal > Device' on page 85).
4. Set the radio operating mode to 'repeater station' (see 'Terminal > Operating Mode' on page 91).
5. Set the radio IP address (see 'IP > IP Setup > Bridge / Gateway Router Modes' on page 138).
6. Set the radio frequencies to base station frequencies you wish to operate from (see 'Radio > Radio Setup' on page 96).
7. Set the radio security settings to the same as the base station (see 'Security > Setup' on page 168).

The base station will automatically allocate a node address to the new repeater station.

Network Changes

Adding a Repeater Station

To add a repeater station to your network:

1. Install the repeater station radio (see 'Installing the Radio' on page 56).
2. Set the radio Network ID to the same ID as the other stations in the network (see 'Terminal > Device' on page 85).
3. Set the radio IP address (see 'IP > IP Setup > Bridge / Gateway Router Modes' on page 138).
4. Set the radio frequencies to the base station frequencies you wish to operate from (see 'Radio > Radio Setup' on page 96).
5. Set the radio operating mode to 'repeater station' (see 'Terminal > Operating Mode' on page 91).
6. Increase the radio network radius by one on all stations in the network (see 'Terminal > Device' on page 85).

The base station will automatically allocate a node address to the new repeater station.

To remove a repeater station from your network:

1. Turn the power off on the remote station radios operating from the repeater station radio you wish to remove.
2. Turn the power off on the repeater station radio you wish to remove.
3. Decrease the network radius by one on all stations in the network (see 'Terminal > Device' on page 85).

Adding a Remote Station

To add a remote station to your network:

1. Install the remote station radio (see 'Installing the Radio' on page 56).
2. Set the radio Network ID to the same ID as the other stations in the network (see 'Terminal > Device' on page 85).
3. If repeater used in radius 1, set the network radius=2 on all network stations (see 'Terminal > Device' on page 85).
4. Set the radio IP address (see 'IP > IP Setup > Bridge / Gateway Router Modes' on page 138).
5. Set the radio frequencies to the base station / repeater station frequencies you wish to operate from (see 'Radio > Radio Setup' on page 96).
6. Set the radio operating mode to 'remote station' (see 'Terminal > Operating Mode' on page 91).

The base station will automatically allocate a node address to the new remote station.

To remove a remote station from your network:

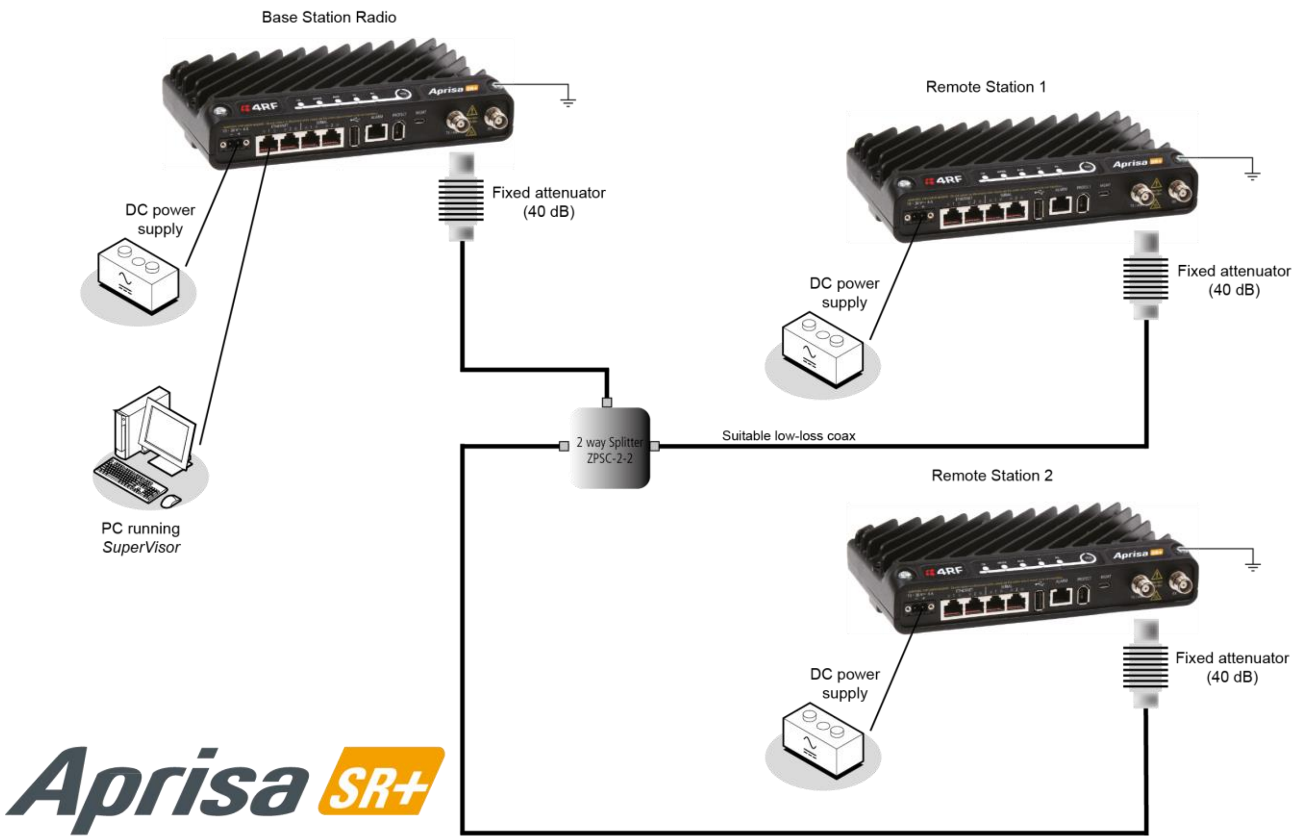
1. Turn the power off on the remote station radio you wish to remove. This is the only action that is required.

Note: The remote station will continue to show in the Network Table list.

5. Preparation

Bench Setup

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



When setting up the equipment for bench testing, note the following:

Earthing

Each radio should be earthed at all times. The radio earth point should be connected to a protection earth.

Attenuators

In a bench setup, there should be 60 - 80 dB at up to 1 GHz of 50 ohm coaxial attenuation, capable of handling the transmit power of +37 dBm (5 W) between the radios' antenna connectors.

Splitter

If more than two radios are required in your bench setup, a multi-way splitter is required. The diagram shows a two way splitter. This splitter should be 50 ohm coaxial up to 1 GHz and capable of handling the transmit power of +37 dBm (5 W).

Cables

Use double-screened coaxial cable that is suitable for use up to 1 GHz at ≈ 1 metre.

CAUTION: Do not apply signals greater than +10 dBm to the antenna connection as they can damage the receiver.

Path Planning

The following factors should be considered to achieve optimum path planning:

- Antenna Selection and Siting
- Coaxial Cable Selection
- Linking System Plan

Antenna Selection and Siting

Selecting and siting antennas are important considerations in your system design. The antenna choice for the site is determined primarily by the frequency of operation and the gain required to establish reliable links.

Base or Repeater Station

The predominant antenna for a base station or a repeater station is an omni-directional collinear gain antenna.

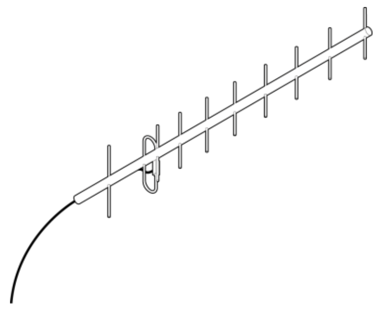
Omni Directional Collinear Antennas

Factor	Explanation
Frequency	Often used in 380-530 MHz bands
Gain	Varies with size (5 dBi to 8 dBi typical)
Wind loading	Minimal
Tower aperture required	Minimal
Size	Range from 2 m to 3 m length
Polarization	Vertical

Remote station

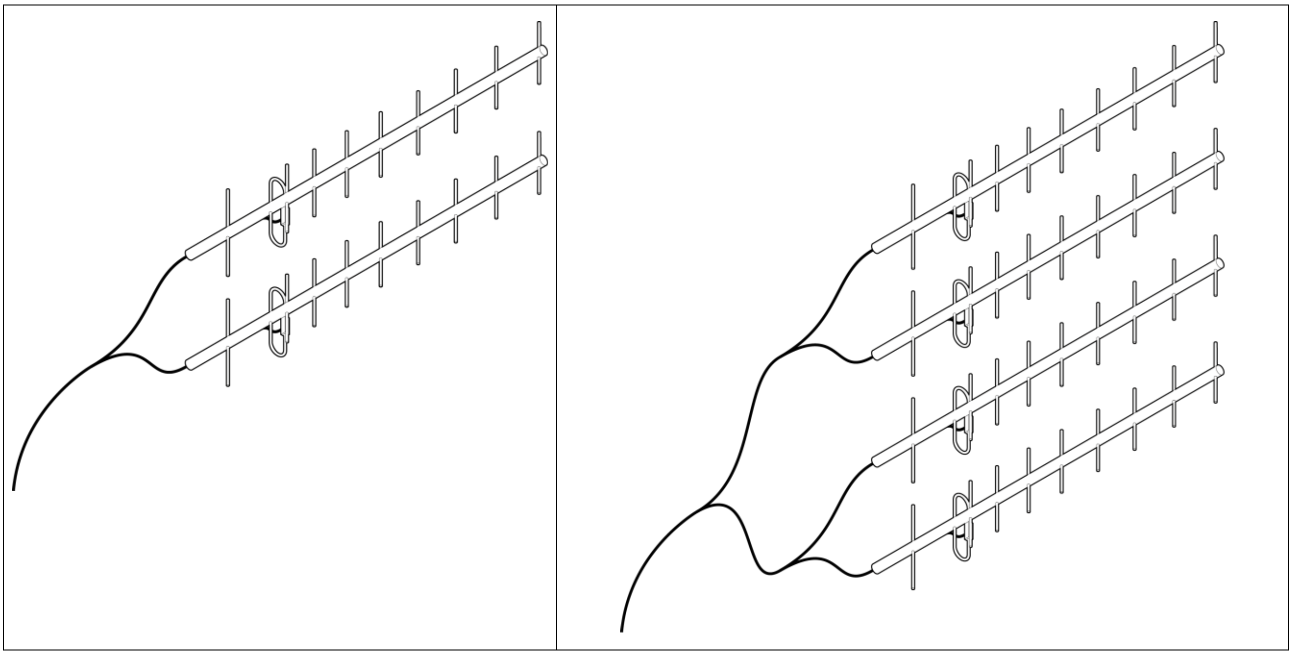
There are two main types of directional antenna that are commonly used for remote stations, Yagi and corner reflector antennas.

Yagi Antennas



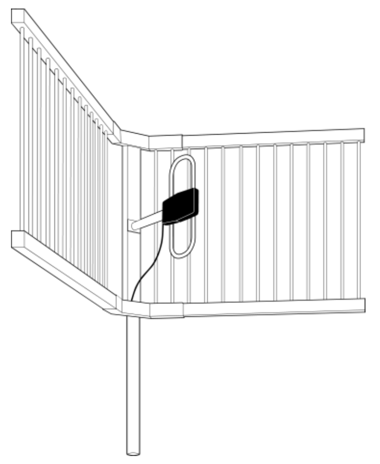
Factor	Explanation
Frequency	Often used in 350-600 MHz bands
Gain	Varies with size (typically 11 dBi to 16 dBi)
Stackable gain increase	2 Yagi antennas (+ 2.8 dB) 4 Yagi antennas (+ 5.6 dB)
Size	Range from 0.6 m to 3 m in length
Front to back ratio	Low (typically 18 to 20 dB)

It is possible to increase the gain of a Yagi antenna installation by placing two or more of them in a stack. The relative position of the antennas is critical.



Example of stacked antennas

Corner Reflector Antennas

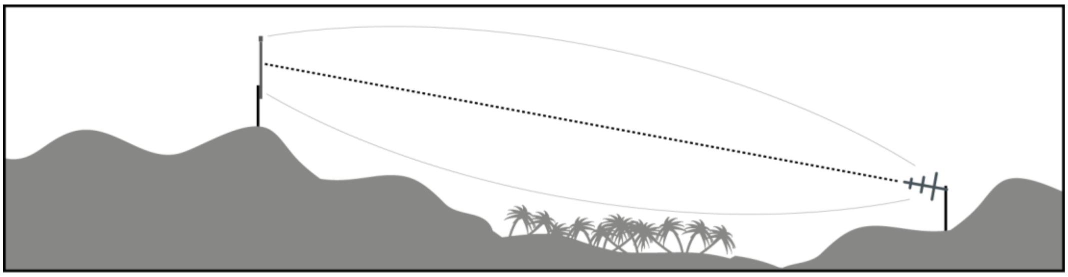


Factor	Explanation
Frequency	Often used in 330-960 MHz bands
Gain	Typically 12 dBi
Size	Range from 0.36 m to 0.75 m in length
Front to back ratio	High (typically 30 dB)
Beamwidth	Broad (up to 60°)

Antenna Siting

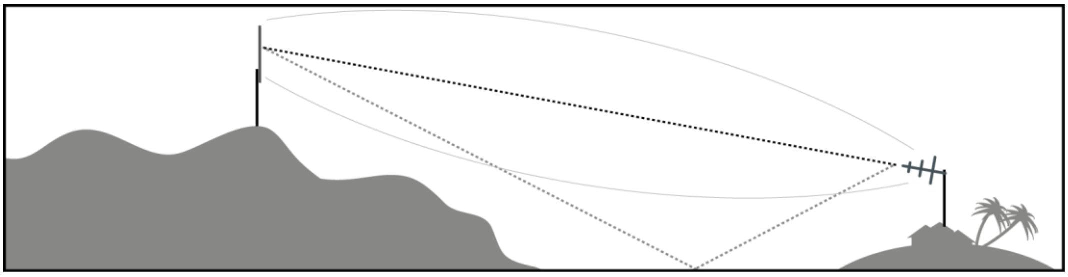
When siting antennas, consider the following points:

A site with a clear line of sight to the remote radio is recommended. Pay particular attention to trees, buildings, and other obstructions close to the antenna site.



Example of a clear line-of-sight path

Any large flat areas that reflect RF energy along the link path, for instance, water, could cause multipath fading. If the link path crosses a feature that is likely to cause RF reflections, shield the antenna from the reflected signals by positioning it on the far side of the roof of the equipment shelter or other structure.



Example of a mid-path reflection path

The antenna site should be as far as possible from other potential sources of RF interference such as electrical equipment, power lines and roads. The antenna site should be as close as possible to the equipment shelter.

Wide angle and zoom photographs taken at the proposed antenna location (looking down the proposed path), can be useful when considering the best mounting positions.

Coaxial Feeder Cables

To ensure maximum performance, it is recommended that you use good quality low-loss coaxial cable for all feeder runs. When selecting a coaxial cable consider the following:

Factor	Effect
Attenuation	Short cables and larger diameter cables have less attenuation
Cost	Smaller diameter cables are cheaper
Ease of installation	Easier with smaller diameter cables or short cables

For installations requiring long feeder cable runs, use the RFI AVA5 50, RFI LDF4 50A or RFI CNT-400 feeder cable or equivalent:

Part Number	Part Description	Specification
RFI AVA5 50	Feeder Cable, 7/8", HELIAX, Low loss	7/8" foam dielectric. Standard Jacket Outer conductor corrugated copper, inner conductor copper-clad aluminum Bending radius of 250 mm min Attenuation of 2.65 dB / 100m @ 520 MHz
RFI LDF4 50A	Feeder cable, 1/2", HELIAX, Loss Loss	1/2" foam dielectric. Standard Jacket Outer conductor corrugated copper, inner conductor copper-clad aluminum Bending radius of 125 mm min Attenuation of 5.1 dB / 100m @ 520 MHz
RFI CNT 400	Feeder, CNT-400, 10.8mm, Double Shielded Solid Polyethylene	Low loss 0.4’ (10.8 mm) feeder cable UV protected black Polyethylene, bonded AL tape outer conductor Bending radius of 30 mm min Attenuation of 8.8 dB / 100m @ 450 MHz

For installations requiring short feeder cable runs, use the RFI 8223 feeder cable or equivalent:

Part Number	Part Description	Specification
RFI 8223	Feeder, RG 223 5.4mm d, Double Shielded Solid Polyethylene	Bending radius of 20 mm min Attenuation of 30.5 dB / 100m @ 450 MHz

When running cables:

Run coaxial feeder cable from the installation to the antenna, ensuring you leave enough extra cable at each end to allow drip loops to be formed.

Terminate and ground the feeder cables in accordance with the manufacturers’ instructions. Bond the outer conductor of the coaxial feeder cables to the base of the tower mast.

Linking System Plan

All of the above factors combine in any proposed installation to create a Linking System Plan. The Linking System Plan predicts how well the radios will perform after it is installed.

Use the outputs of the Linking System Plan during commissioning to confirm the radios have been installed correctly and that it will provide reliable service.

Site Requirements

Power Supply

Ensure a suitable power supply is available for powering the radio.

The nominal input voltage for a radio is +13.8 VDC (negative earth) with an input voltage range of +10 to +30 VDC. The maximum power input is 35 W.

WARNING:

Before connecting power to the radio, ensure that the radio is grounded via the negative terminal of the DC power connection.

Equipment Cooling

If the Aprisa SR+ is operated in an environment where the ambient temperature exceeds 50°C, the Aprisa SR+ convection air flow over the heat sinks must be considered.

The environmental operating conditions are as follows:

Operating temperature	-40 to +70° C
Storage temperature	-40 to +80° C
Humidity	Maximum 95% non-condensing

WARNING:

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

WARNING:

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

Earthing and Lightning Protection

WARNING:

Lightning can easily damage electronic equipment.

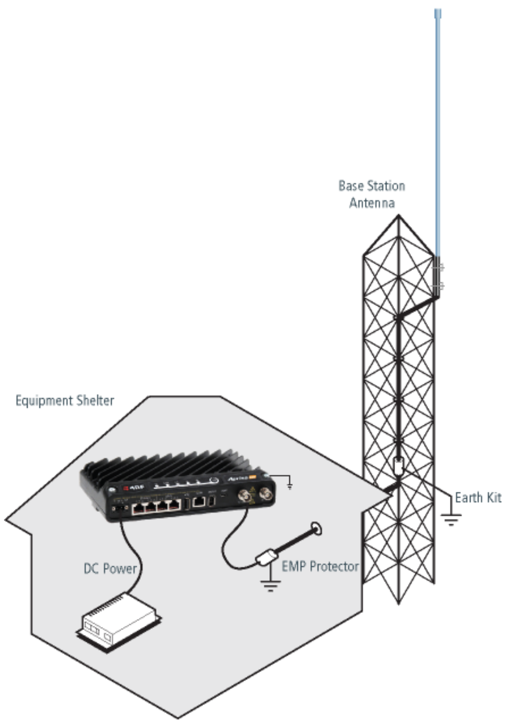
To avoid this risk, install primary lightning protection devices on any interfaces that are reticulated in the local cable network.

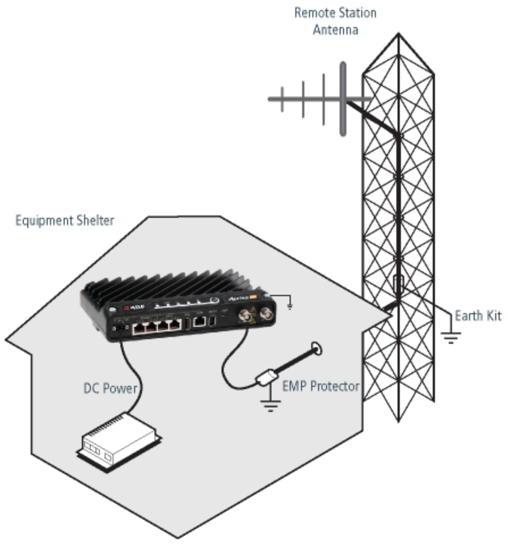
You should also install a coaxial surge suppressor on the radio antenna port.

Feeder Earthing

Earth the antenna tower, feeders and lightning protection devices in accordance with the appropriate local and national standards. The diagram below shows the minimum requirements.

Use grounding kits as specified or supplied by the coaxial cable manufacturer to properly ground or bond the cable outer.





Radio Earthing

The Aprisa SR+ has an earth connection point on the top left and the top right of the enclosure. M4 8mm pan pozi machine screws and M4 lock washers are supplied fitted to the radio. These screws can be used to earth the enclosure to a protection earth.

6. Installing the Radio

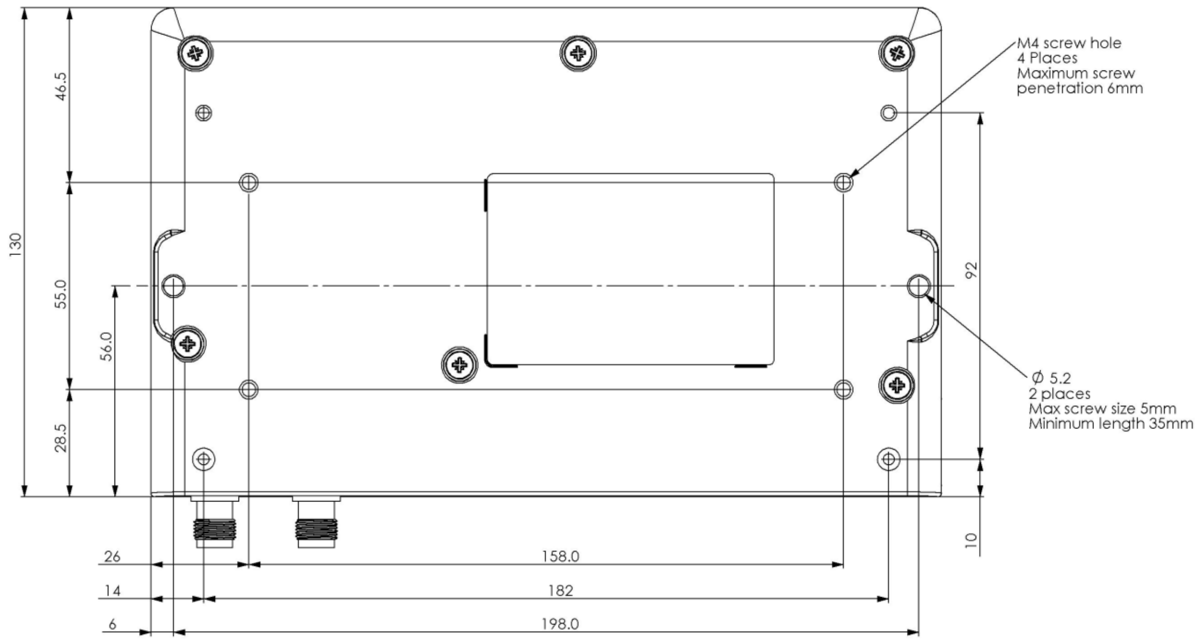
CAUTION:

You must comply with the safety precautions in this manual or on the product itself.

4RF does not assume any liability for failure to comply with these precautions.

Mounting

The Aprisa SR+ 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 Aprisa SR+ DIN Rail Mounting Bracket
- Rack shelf mounting
- Wall mounting
- Outdoor enclosure mounting

WARNING:

If the Aprisa SR+ is operated in an environment where the ambient temperature exceeds 50°C, the Aprisa SR+ must be installed within a restricted access location to prevent human contact with the enclosure heatsink.

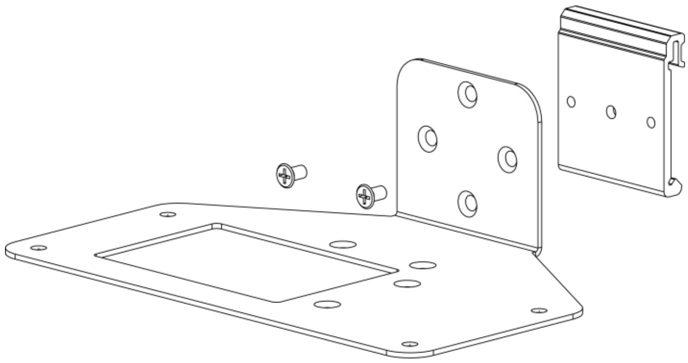
Required Tools

No special tools are needed to install the radio.

DIN Rail Mounting

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

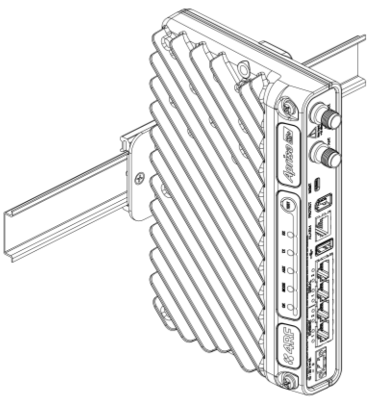
Part Number	Part Description
APSB-MBRK-DIN	4RF SR+ Acc, Mounting, Bracket, DIN Rail



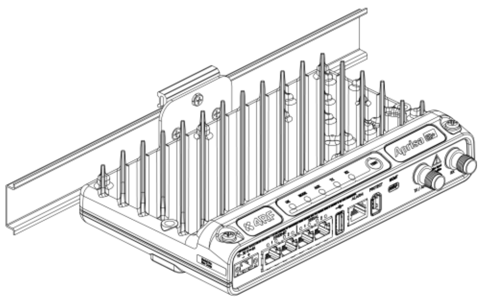
The Aprisa SR+ is mounted into the DIN rail mounting bracket using the four M4 threaded holes in the Aprisa SR+ enclosure base. Four 8 mm M4 pan pozi machine screws are supplied with the bracket.

The Aprisa SR+ DIN rail mounting bracket can be mounted in four positions on a horizontal DIN rail:

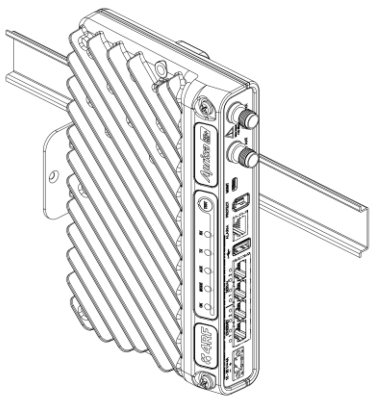
- Vertical Mount (vertical enclosure perpendicular to the mount)
- Horizontal Mount (horizontal enclosure perpendicular to the mount)
- Flat Vertical Mount (vertical enclosure parallel to the mount)
- Flat Horizontal Mount (horizontal enclosure parallel to the mount)



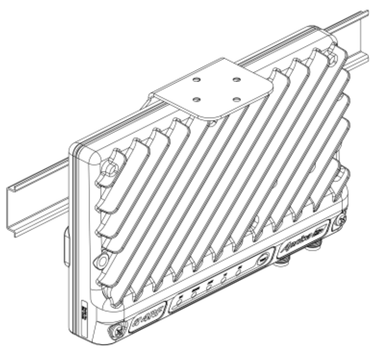
Vertical Mount



Horizontal Mount



Flat Vertical Mount

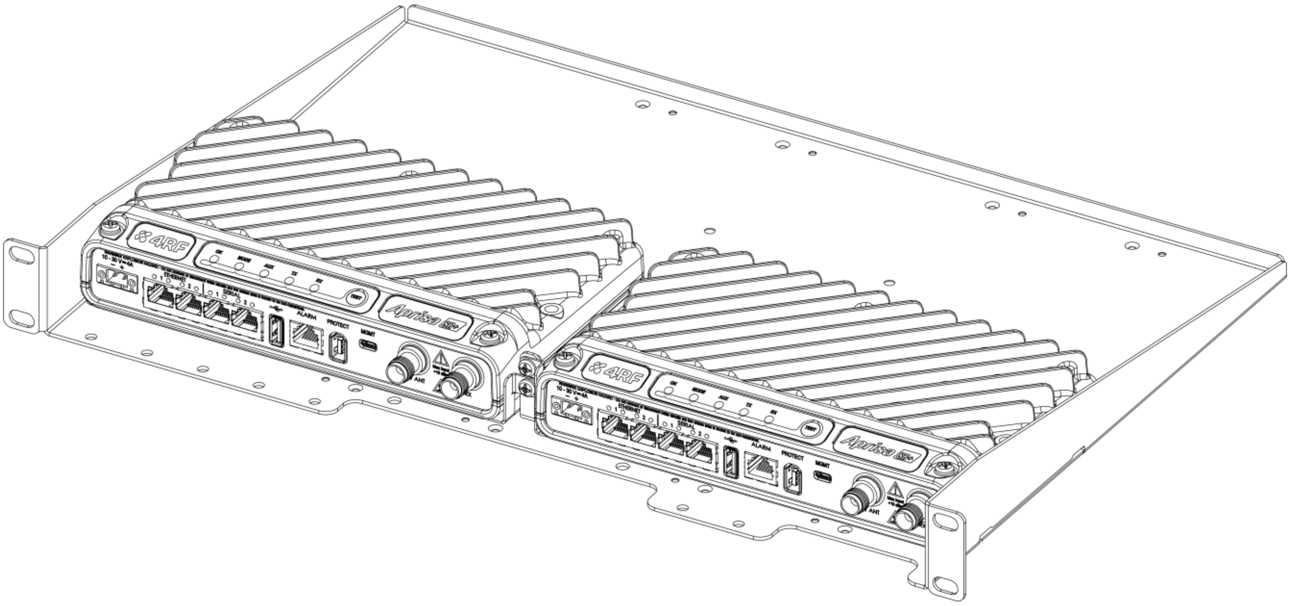


Flat Horizontal Mount

Rack Shelf Mounting

The Aprisa SR+ can be mounted on a rack mount shelf using the four M4 threaded holes in the Aprisa SR+ enclosure base. The following picture shows Aprisa SR+ mounted on a 1 RU rack mounted shelf.

Part Number	Part Description
APSB-MR19-X1U	4RF SR+ Acc, Mounting, 19" Rack Mount Shelf, 1U

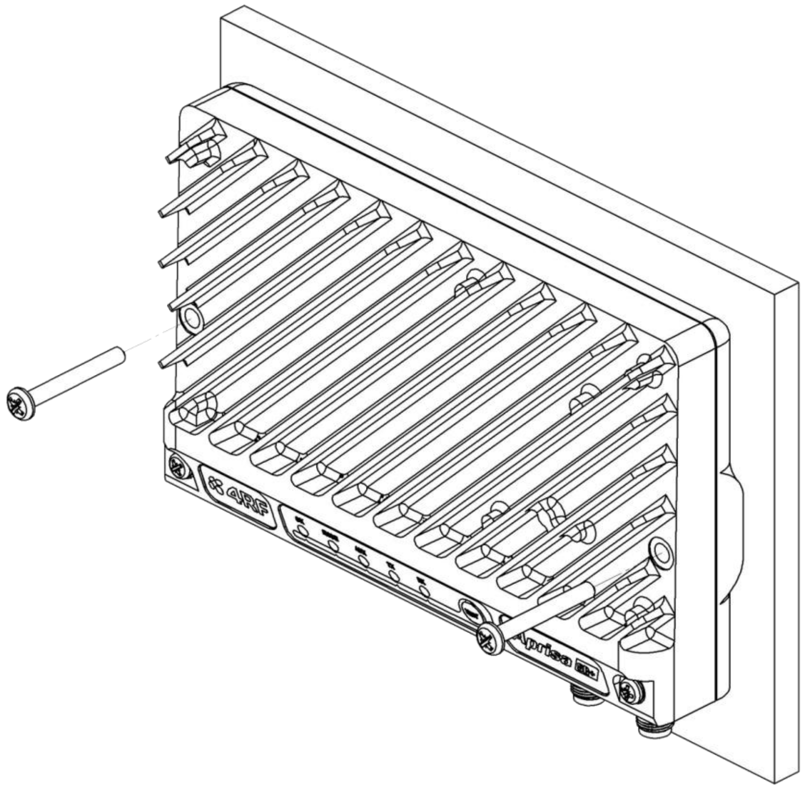


WARNING:

If the Aprisa SR+ is operated in an environment where the ambient temperature exceeds 50°C, the Aprisa SR+ convection air flow over the heat sinks must be considered.

Wall Mounting

The Aprisa SR+ 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.



Installing the Antenna and Feeder Cable

Carefully mount the antenna following the antenna manufacturers' instructions. Run feeder cable from the antenna to the radio location.

Lightning protection must be incorporated into the antenna system (see 'Earthing and Lightning Protection' on page 55).

WARNING:

When the link is operating, there is RF energy radiated from the antenna.
Do not stand in front of the antenna while the radio is operating (see the 'RF Exposure Warning' on page 3).

Fit the appropriate male or female connector (usually N-type) to the antenna feeder at the antenna end. Carefully follow the connector manufacturers' instructions.

Securely attach the feeder cable to the mast and cable trays using cable ties or cable hangers. Follow the cable manufacturer's recommendations about the use of feeder clips, and their recommended spacing.

Connect the antenna and feeder cable. Weatherproof the connection with a boot, tape or other approved method.

The Aprisa SR+ antenna connection is a TNC female connector so the feeder / jumper must be fitted with a TNC male connector.

If a jumper is used between the feeder and the radio, connect a coaxial surge suppressor or similar lightning protector between the feeder and jumper cables (or at the point where the cable enters the equipment shelter). Connect the feeder cable to the antenna port on the radio.

Earth the case of the lightning protector to the site Lightning Protection Earth.

The Aprisa SR+ has an earth connection point on the top left and the top right of the enclosure. M4 8mm pan pozi machine screws and M4 lock washers are supplied fitted to the radio. These screws can be used to earth the enclosure to a protection earth.

Connecting the Power Supply

The nominal input voltage for a radio is +13.8 VDC (negative earth) with an input voltage range of +10 to +30 VDC. The maximum power input is 35 W.

The power connector required is a Molex 2 pin female screw fitting part. This connector is supplied fitted to the radio.

The negative supply of the Aprisa SR+ power connection is internally connected to the Aprisa SR+ enclosure. Power must be supplied from a Negative Earthed power supply.

Wire your power source to power connector and plug the connector into the radio. The connector screws can be fastened to secure the connector.

Spare Molex 2 pin female power connectors can be ordered from 4RF:

Part Number	Part Description
APST-CML2-FEM-01	4RF SR+ Spare, Connector, Molex 2 pin, Female, 1 item

Turn your power source on:

- All the radio LEDs will flash orange for one second and then the OK, MODE and AUX LEDs will light green, the TX and RX LEDs will flash red.
- The Aprisa SR+ radio is ready to operate
- The TX and RX LEDs will be green (steady or flashing) when the radio is registered with the network.

If the LEDs fail to light, carefully check the supply polarity. If the power supply connections have been accidentally reversed, internal fuses will have blown to protect the unit.

Spare fuses are contained within the radio, see ‘Spare Fuses’ on page 62 for instructions on how to locate and replace the fuses.

External Power Supplies

The following external power supplies are available from 4RF as accessories:

Part Number	Part Description
APSB-P230-030-24-TS	4RF SR+ Acc, PSU, 230 VAC, 30W, 24 VDC, -10 to +60C
APSB-P230-048-24-TE	4RF SR+ Acc, PSU, 230 VAC, 48W, 24 VDC, -20 to +75C
APSB-P230-060-24-TS	4RF SR+ Acc, PSU, 230 VAC, 60W, 24 VDC, -10 to +60C
APSB-P48D-050-24-TA	4RF SR+ Acc, PSU, 48 VDC, 50W, 24 VDC, 0 to +50C

Spare Fuses

The Aprisa SR+ 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 Littelfuse 0454007 with a rating of 7 A, 125 V, very fast acting.

To replace the fuses:

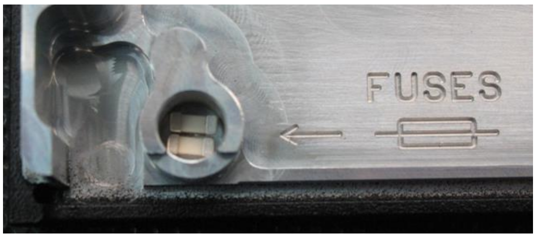
1. Remove the input power and antenna cable.
2. Unscrew the enclosure securing screws (posi 2).

2. Separate the enclosure halves.

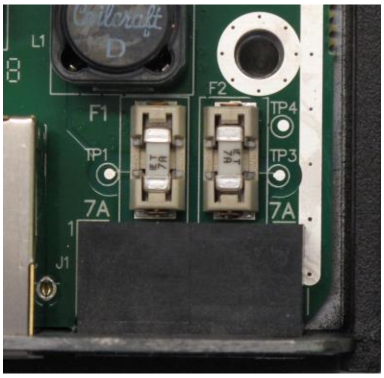
CAUTION: Antistatic precautions must be taken as the internal components are static sensitive.

---

3. Access the enclosure spare fuses under the plastic cap.



4. Replace the two fuses.



5. Close the enclosure and tighten the screws.

Note: Is it critical that the screws are re-tightened to 1.2 Nm. The transmitter adjacent channel performance can be degraded if the screws are not tightened correctly.

Additional Spare Fuses

Additional spare fuses can be ordered from 4RF:

Part Number	Part Description
APST-FNAN-454-07-02	4RF SR+ Spare, Fuse, Nano SMF, 454 Series, 7A, 2 items

7. Managing the Radio

SuperVisor

The Aprisa SR+ contains an embedded web server application (SuperVisor) to enable element management with any major web browser (such as Mozilla Firefox or Microsoft® Internet Explorer).

SuperVisor enables operators to configure and manage the Aprisa SR+ base station radio and repeater / remote station radios over the radio link.

The key features of SuperVisor are:

- Full element management, configuration and diagnostics
- Manage the entire network from the Base Station (remote management of elements)
- Managed network software distribution and upgrades
- Performance and alarm monitoring of the entire network, including RSSI, alarm states, time-stamped events, etc.
- View and set standard radio configuration parameters including frequencies, transmit power, channel access, serial, Ethernet port settings
- Set and view security parameters
- User management
- Operates over a secure HTTPS session on the access connection to the base station

PC Requirements for SuperVisor

SuperVisor requires the following minimum PC requirements:

Browser	Operating System	Processor	RAM
Internet Explorer 7 (oldest browser supported) IE7 can operate with less but will be very slow.	MS-Windows XP Service Pack 2	1 GHz processor	1 GB Ram
Internet Explorer 9 Does not support config file upload from PC	MS-Windows Vista Service Pack 2	1 GHz processor	2 GB Ram
Internet Explorer 10 (recommended minimum browser)	MS-Windows 7 Service Pack 1	1 GHz processor	2 GB Ram
Internet Explorer 11	MS-Windows 8.1	1 GHz processor	2 GB Ram
Mozilla Firefox (MS-Windows)	MS-Windows XP Service Pack 2	1 GHz processor, Pentium 4 and above	1 GB Ram
Mozilla Firefox (Linux)	Gnome desktop 2.18 and above	1 GHz processor, Pentium 4 and above	1 GB Ram
Mozilla Firefox (Apple Mac) (4RF does not support retina displays)	Mac OS X 10.6	1 GHz processor, Pentium 4 and above	1 GB Ram

Note: 4RF does not support Google Chrome, Opera browser or Apple Safari but when they have been used they have worked correctly.

Connecting to SuperVisor

The predominant management connection to the Aprisa SR+ radio is with an Ethernet interface using standard IP networking. There should be only one Ethernet connection from the base station to the management network.

The Aprisa SR+ has a factory default IP address of 169.254.50.10 with a subnet mask of 255.255.0.0. This is an IPv4 Link Local (RFC3927) address which simplifies the connection to a PC.

Each radio in the network must be set up with a unique IP address on the same subnet.

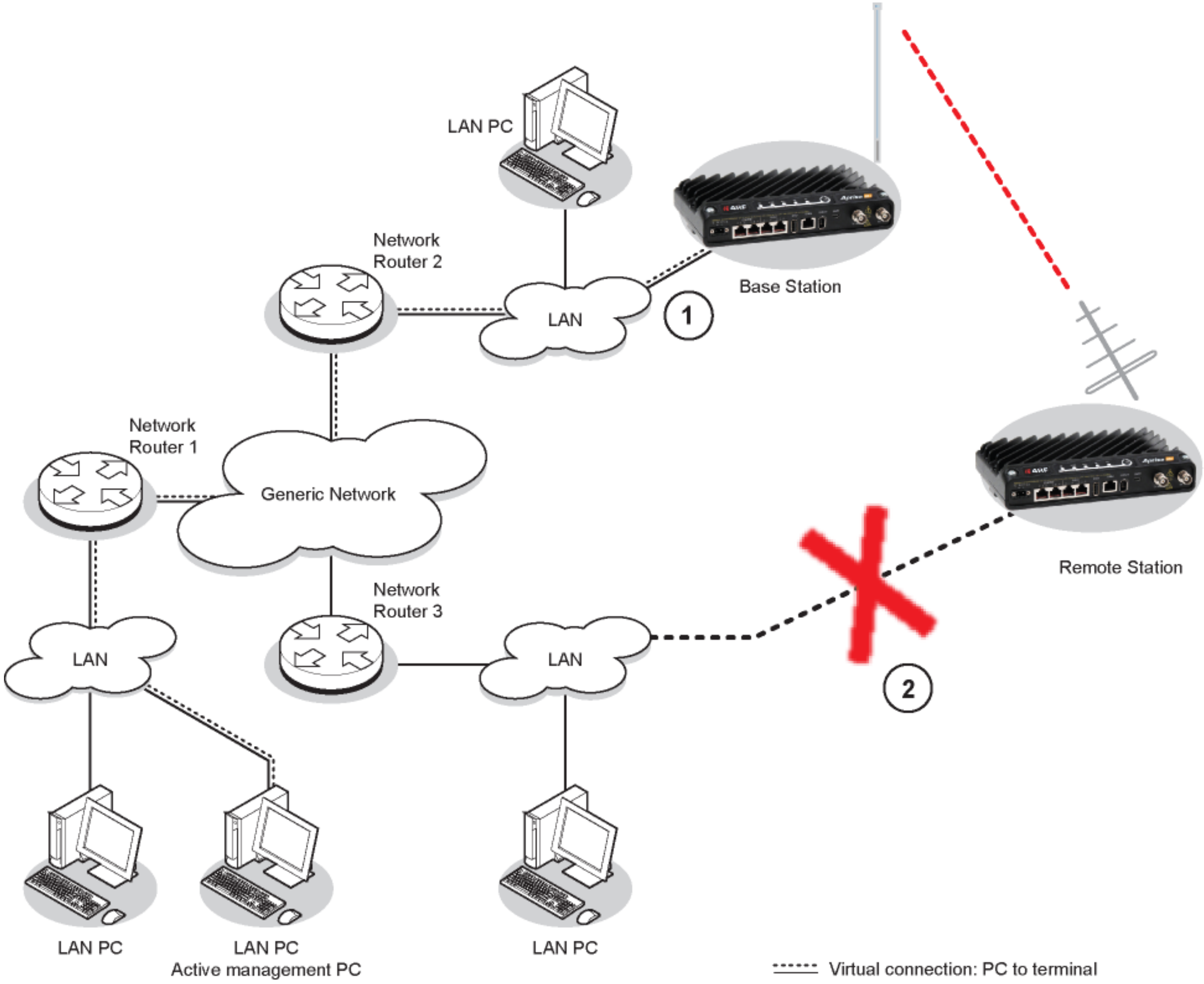
The Aprisa SR+ Protected Station radio A (left radio) has a factory default IP address of 169.254.50.10 and radio B (right radio) has a factory default IP address of 169.254.50.20, both with a subnet mask of 255.255.0.0.

To change the Aprisa SR+ IP address:

1. Set up your PC for a compatible IP address e.g. 169.254.50.1 with a subnet mask of 255.255.0.0.
2. Connect your PC network port to one of the Aprisa SR+ Ethernet ports.
3. Open a browser and enter https://169.254.50.10.
4. Login to the radio with the default Username ‘admin’ and Password ‘admin’.
5. Change the IP address to conform to the network plan in use.

Management PC Connection

The active management PC must only have one connection to the network as shown by path ①. There should not be any alternate path that the active management PC can use via an alternate router or alternate LAN that would allow the management traffic to be looped as shown by path ②.



When logging into a network, it is important to understand the relationship between the Local Radio and the Remote Radios.

The Local Radio is the radio that your IP network is physically connected to.

If the Local Radio is a base station, SuperVisor manages the base station and all the repeater stations and remote stations in the network.

If the Local Radio is a remote station or repeater station, SuperVisor only manages the remote / repeater station radio logged into.

If the user is at the remote station and connects SuperVisor directly to the remote radio via their computer, all relevant features are still available. This includes the ability to monitor the 'Last received packet RSSI. If ICMP is enabled on the base station, the user will also be able to ping the base station to confirm the connectivity.

PC Settings for SuperVisor

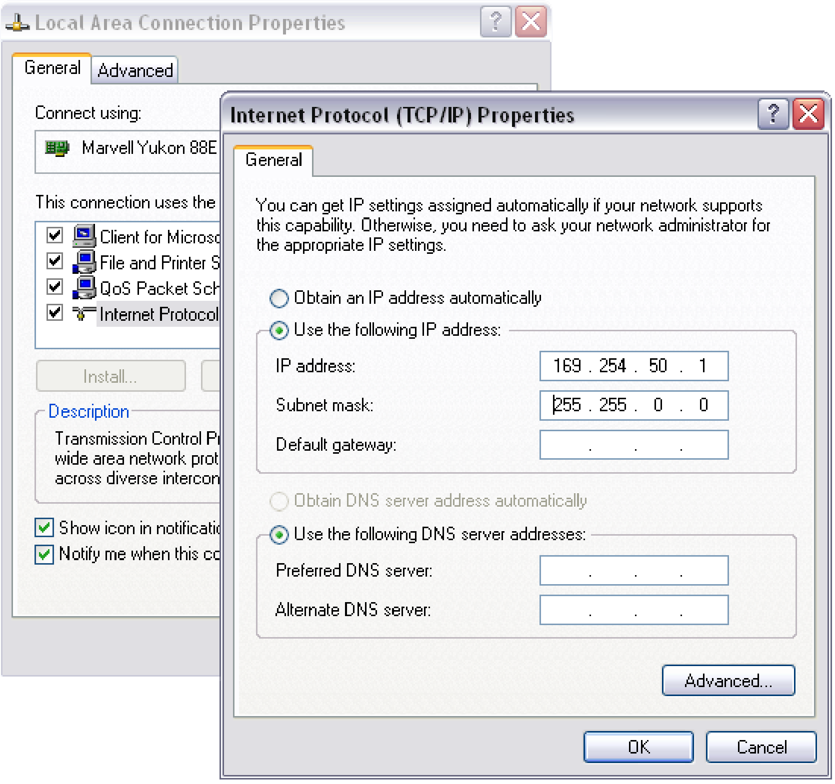
To change the PC IP address:

If your PC has previously been used for other applications, you may need to change the IP address and the subnet mask settings. You will require Administrator rights on your PC to change these.

Windows XP example:

1. Open the ‘Control Panel’.
2. Open ‘Network Connections’ and right click on the ‘Local Area Connection’ and select ‘Properties’.
3. Click on the ‘General’ tab.
4. Click on ‘Internet Protocol (TCP/IP)’ and click on properties.
5. Enter the IP address and the subnet mask (example as shown).
6. Click ‘OK’ then close the Control Panel.

If the radio is on a different subnet from the network the PC is on, set the PC default gateway address to the network gateway address which is the address of the router used to connect the subnets (for details, consult your network administrator).

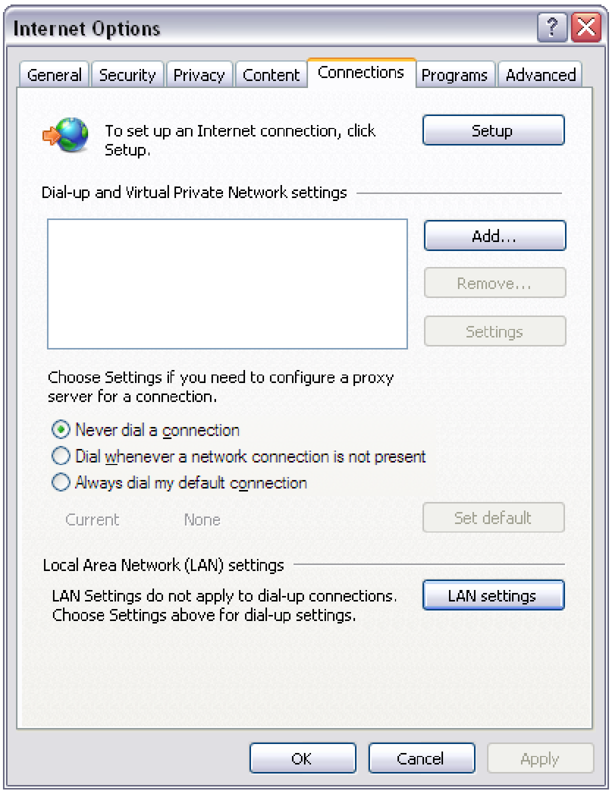


To change the PC connection type:

If your PC has previously been used with Dial-up connections, you may need to change your PC Internet Connection setting to 'Never dial a connection'.

Windows Internet Explorer 8 example:

1. Open Internet Explorer.
2. Open the menu item Tools > Internet Options and click on the 'Connections' tab.
3. Click the 'Never dial a connection' option.

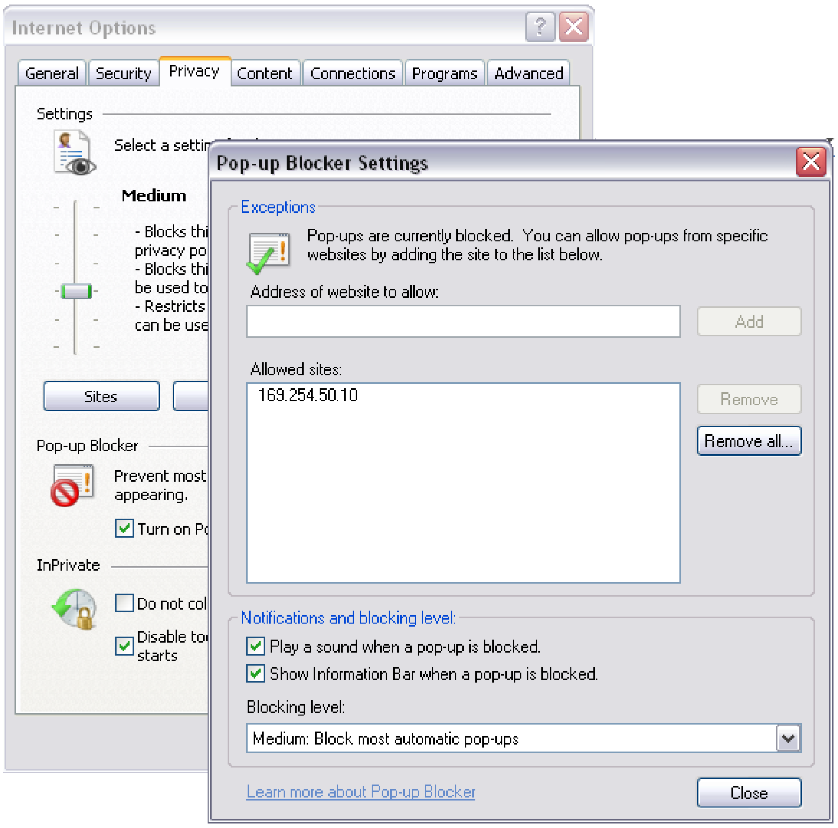


To change the PC pop-up status:

Some functions within SuperVisor require Pop-ups enabled e.g. saving a MIB

Windows Internet Explorer 8 example:

1. Open Internet Explorer.
2. Open the menu item Tools > Internet Options and click on the ‘Privacy’ tab.
3. Click on ‘Pop-up Blocker Settings’.
4. Set the ‘Address of Web site to allow’ to the radio address or set the ‘Blocking Level’ to ‘Low: Allow Pop-ups from secure sites’ and close the window.

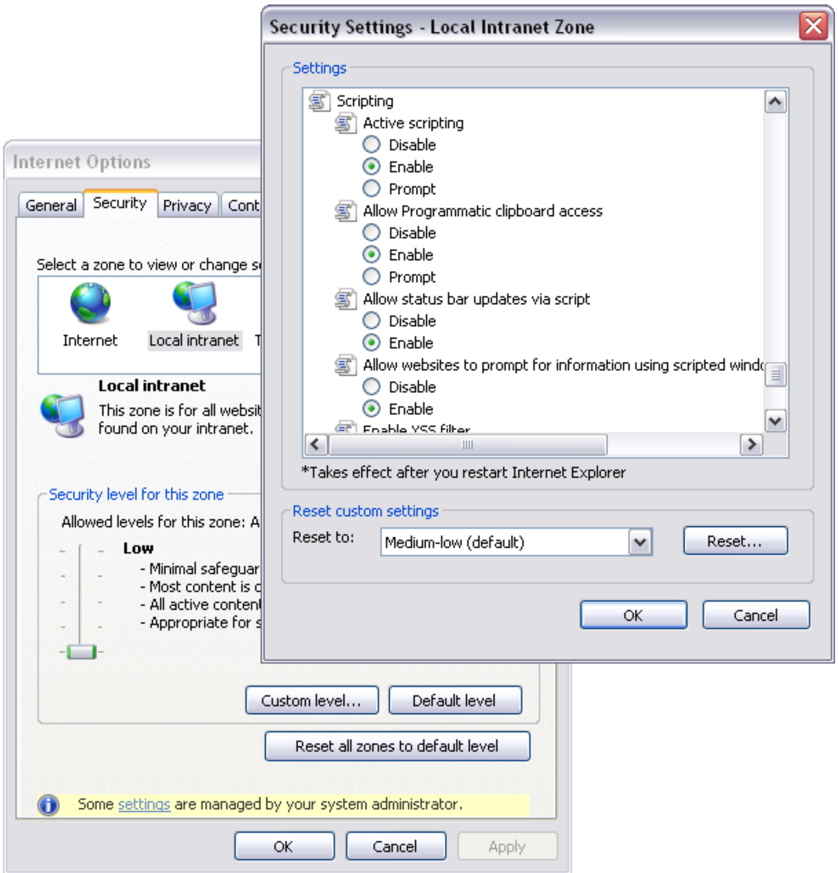


To enable JavaScript in the web browser:

Some functions within SuperVisor require JavaScript in the web browser to be enabled.

Windows Internet Explorer 8 example:

1. Open Internet Explorer.
2. Open the menu item Tools > Internet Options and click on the 'Security' tab.
3. Click on 'Local Intranet'.
4. Click on 'Custom Level'.
5. Scroll down until you see section labeled 'Scripting'.
6. Under 'Active Scripting', select 'Enable'.



Login to SuperVisor

The maximum number of concurrent users that can be logged into a radio is 6.

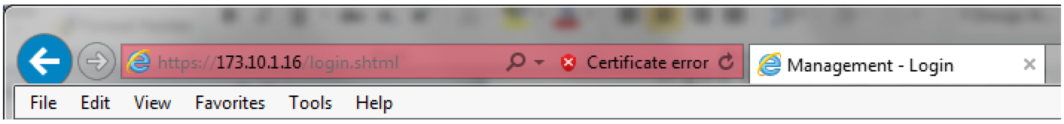
If SuperVisor is inactive for a period defined by the Inactivity Timeout option (see 'Maintenance > General' on page 193), the radio will automatically logout the user.

To login to SuperVisor:

1. Open your web browser and enter the IP address of the radio.

If you haven't assigned an IP address to the radio, use the factory default IP address of 169.254.50.10 with a subnet mask of 255.255.0.0.

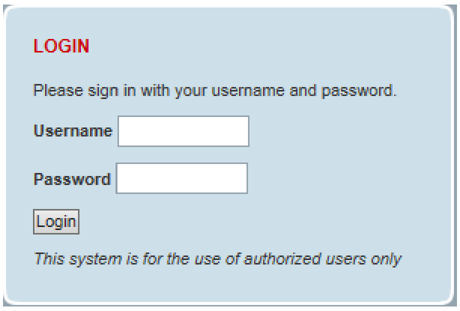
If you don't know the IP address of the radio, you can determine it using the Command Line Interface (see 'Command Line Interface' on page 305).



Note: The Aprisa SR+ has a randomly generated unique self-signed ECC256 security certificate which may cause the browser to prompt a certificate warning. It is safe to ignore the warning and continue. The valid certificate is 'Issued By: 4RF-APRISA' which can be viewed in the browser.

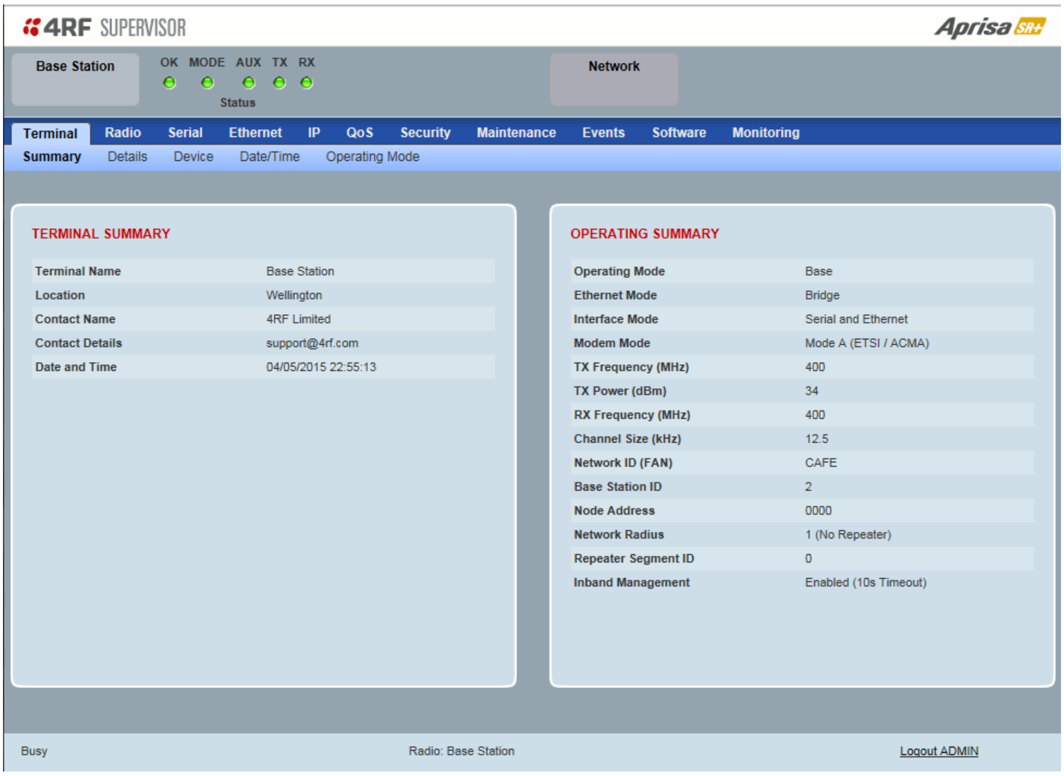
2. Login with the Username and Password assigned to you.

If unique usernames and passwords have not yet been configured, use the default username 'admin' and password 'admin'.

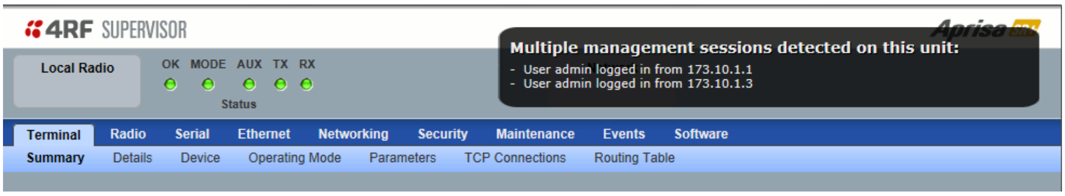


Important: After you login for the very first time, it is recommended that you change the default admin password for security reasons (see 'Changing Passwords' on page 177).

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



If there is more than one user logged into the same radio, the Multiple Management Sessions popup will show the usernames and IP addresses of the users. This popup message will display until 5 seconds after the cursor is moved. The event log will also record the users logged into the radio or logged out the radio.



Logout of SuperVisor

As the maximum number of concurrent users that can be logged into a radio is 6, not logging out correctly can restrict access to the radio until after the timeout period (30 minutes).

Logging out from a radio will logout all users logged in with the same username.

If the SuperVisor window is closed without logging out, the radio will automatically log the user out after a timeout period of 3 minutes.

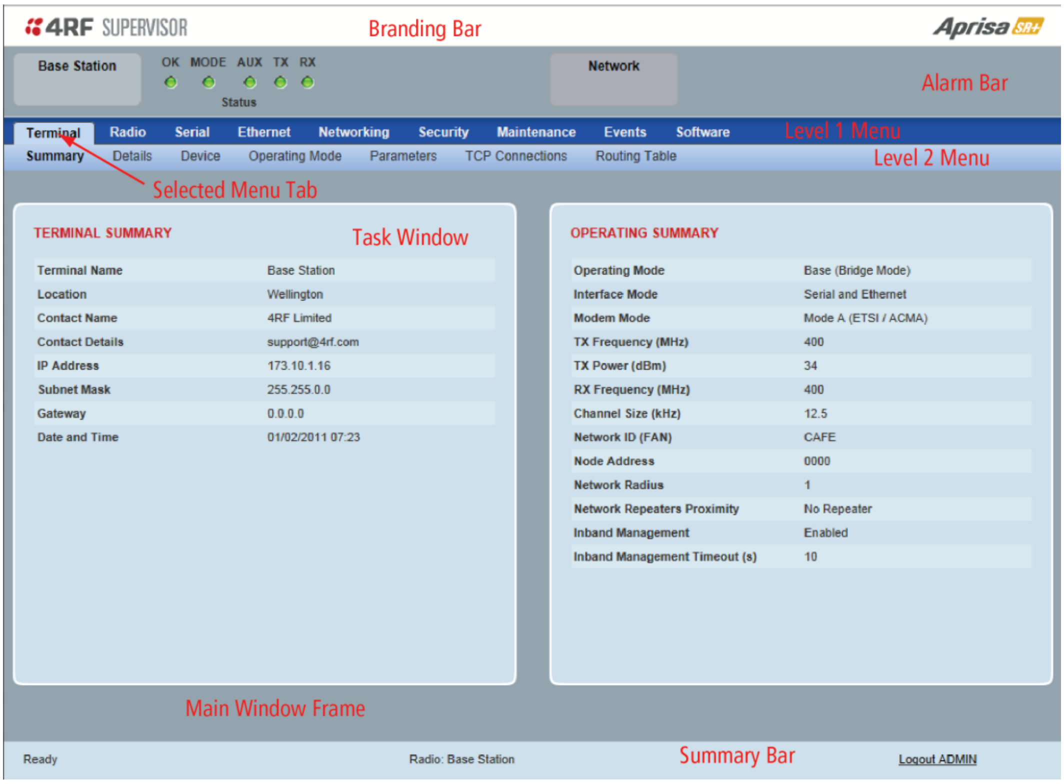
To logout of SuperVisor:

Click on the ‘Logout’ button on the Summary Bar.

SuperVisor Page Layout

Standard Radio

The following shows the components of the SuperVisor page layout for a standard radio:



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 radio terminal that SuperVisor is logged into (the local radio) on the left.

If the local radio is a base station, the page shows the name of the current remote / repeater station (the remote radio) on the right. SuperVisor will manage all the repeater stations and remote stations in the network.

If the local radio is a remote station or repeater station, the page shows the name of the remote / repeater station on the left. The right side of the Alarm Bar will be blank. SuperVisor manages only the remote / repeater station logged into.

The LED alarm indicators reflect the status of the front panel LEDs on the radio.

SuperVisor Summary Bar

The summary bar at the bottom of the page shows:

Position	Function
Left	Busy - SuperVisor is busy retrieving data from the radio that SuperVisor is logged into. Ready - SuperVisor is ready to manage the radio.
Middle	Displays the name of the radio terminal that SuperVisor is currently managing.
Right	The access level logged into SuperVisor. This label also doubles as the SuperVisor logout button.

SuperVisor Menu

The following is a list of SuperVisor top level menu items:

Local Terminal	**Network**
	Network Table
Terminal	Summary
Radio	Exceptions
Serial	View
Ethernet	
IP	
QoS	
Security	
Maintenance	
Events	
Software	
Monitoring	

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.

SuperVisor Menu Access

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

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

Terminal Settings Menu Items

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
Terminal > Date / Time	Read-Only	Read-Only	Read-Only	Read-Only
Terminal > Operating Mode	No Access	Read-Write	Read-Write	Read-Write
Radio > Radio Summary	Read-Only	Read-Only	Read-Only	Read-Only
Radio > Channel Summary	Read-Only	Read-Only	Read-Only	Read-Only
Radio > Radio Setup	No Access	Read-Write	Read-Write	Read-Write
Radio > Channel Setup	No Access	Read-Write	Read-Write	Read-Write
Radio > Advanced Setup	No Access	Read-Write	Read-Write	Read-Write
Serial > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Serial > Port Setup	No Access	Read-Write	Read-Write	Read-Write
Ethernet > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Ethernet > Port Setup	No Access	Read-Write	Read-Write	Read-Write
Ethernet > L2 Filtering	No Access	No Access	Read-Write	Read-Write
Ethernet > VLAN	No Access	No Access	Read-Write	Read-Write
IP > IP Summary	Read-Only	Read-Only	Read-Only	Read-Only
IP > IP Setup	No Access	Read-Write	Read-Write	Read-Write
IP > L3 Filtering	No Access	No Access	Read-Write	Read-Write
IP > IP Routes	No Access	No Access	Read-Write	Read-Write
QoS > Summary	Read-Only	Read-Only	Read-Only	Read-Only
QoS > Traffic Priority	No Access	No Access	Read-Write	Read-Write
QoS > Traffic Classification	No Access	No Access	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 > SNMP	No Access	No Access	No Access	Read-Write
Security > Manager	No Access	No Access	Read-Write	Read-Write
Security > Distribution	No Access	No Access	Read-Write	Read-Write
Maintenance > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Maintenance > General	No Access	Read-Write	Read-Write	Read-Write
Maintenance > Test Mode	No Access	Read-Write	Read-Write	Read-Write
Maintenance > Defaults	No Access	No Access	No Access	Read-Write
Maintenance > Protection	No Access	Read-Write	Read-Write	Read-Write
Maintenance > Licence	No Access	No Access	Read-Write	Read-Write

Menu Item	View	Technician	Engineer	Admin
Maintenance > Advanced	No Access	No Access	Read-Write	Read-Write
Events > Alarm Summary	Read-Only	Read-Only	Read-Only	Read-Only
Events > Event History	Read-Only	Read-Only	Read-Only	Read-Only
Events > Event Primary History	Read-Only	Read-Only	Read-Only	Read-Only
Events > Event Secondary History	Read-Only	Read-Only	Read-Only	Read-Only
Events > Events Setup	No Access	No Access	Read-Write	Read-Write
Events > Traps Setup	No Access	No Access	Read-Write	Read-Write
Events > Alarm I/O Setup	Read-Only	Read-Only	Read-Write	Read-Write
Events > Event Action Setup	No Access	No Access	Read-Write	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	No Access	Read-Write	Read-Write
Software > File Transfer	No Access	No Access	Read-Write	Read-Write
Software > File Primary Transfer	No Access	No Access	Read-Write	Read-Write
Software > File Secondary Transfer	No Access	No Access	Read-Write	Read-Write
Software > Manager	No Access	No Access	Read-Write	Read-Write
Software > Remote Distribution	No Access	No Access	Read-Write	Read-Write
Software > Remote Activation	No Access	No Access	Read-Write	Read-Write
Monitoring > Terminal	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Serial	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Ethernet	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Radio	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > User Selected	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > TCP Connections	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Routing Table	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Address Tables	Read-Only	Read-Only	Read-Only	Read-Only

Network Settings Menu Items

Menu Item	View	Technician	Engineer	Admin
Network Table	Read-Only	Read-Only	Read-Only	Read-Only
Summary	Read-Only	Read-Only	Read-Only	Read-Only
Exceptions	Read-Only	Read-Only	Read-Only	Read-Only
View	Read-Only	Read-Only	Read-Only	Read-Only

SuperVisor Menu Items

As SuperVisor screens are dependent on the Aprisa SR+ configuration deployed, the following section is split into two sections:

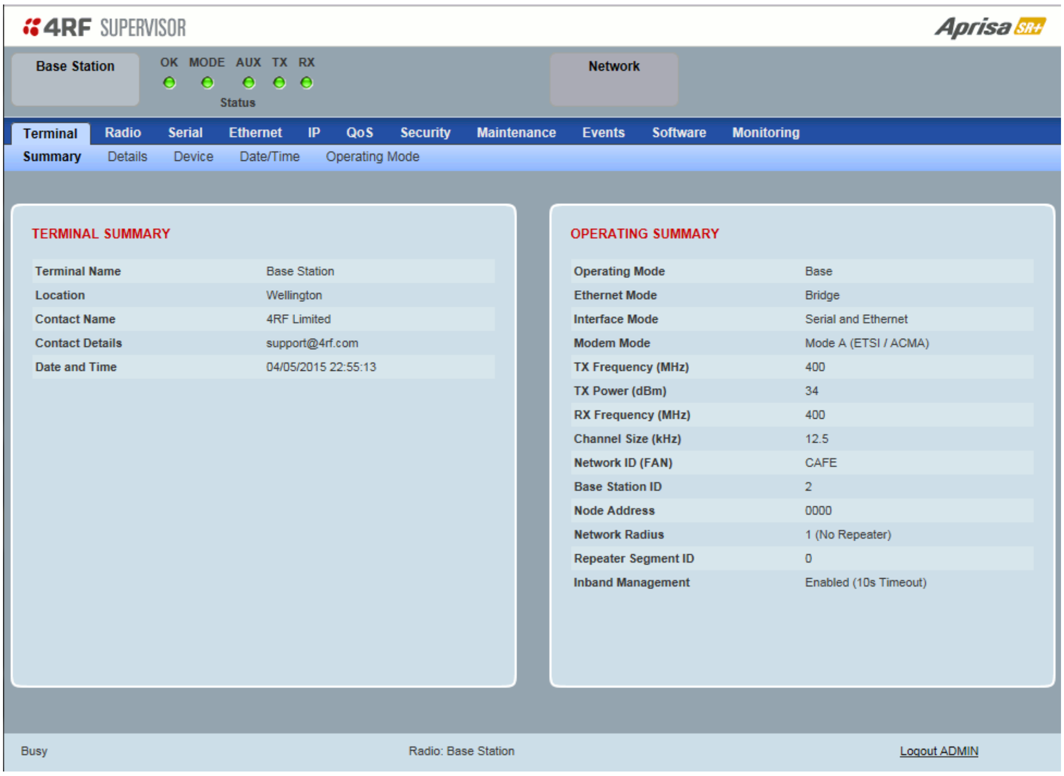
- Standard Radio
- Protected Station

All SuperVisor menu item descriptions assume full access 'Admin' user privileges:

Standard Radio

Terminal

Terminal > Summary



TERMINAL SUMMARY

This page displays the current settings for the Terminal parameters. See 'Terminal > Details' on page 83, 'Terminal > Device' on page 85 and 'Terminal > Operating Mode' on page 91 for setting details.

OPERATING SUMMARY

Operating Mode

This parameter displays the current Operating Mode i.e. if the radio is operating as a base station, repeater station or remote station and the network operating mode of Bridge Mode or Router Mode.

Interface Mode

This parameter displays the Interfaces available for traffic on the radio such as Ethernet and Serial. For Ethernet availability on the radio see 'Maintenance > Licence' on page 201.

Modem Mode

This parameter displays the modem mode selected e.g. ETSI / FCC etc.

TX Frequency (MHz)

This parameter displays the current Transmit Frequency in MHz.

TX Power (dBm)

This parameter displays the current Transmit Power in dBm.

RX Frequency (MHz)

This parameter displays the current Receive Frequency in MHz.

Channel Size (kHz)

This parameter displays the current Channel Size in kHz.

Network ID

This parameter is the network ID of this base station node and its remote / repeater stations in the network. The entry is four hex chars (not case sensitive).

Base Station ID

This parameter identifies the base station. All radios operating to the base station in the same network must use the same Base Station ID setting.

It is especially important to set different values for each network when two or more networks using the same frequencies are operating with some overlapping coverage. The entry is an integer from 1 to 8.

Node Address

The Node Address of the base station is 0000.

If the Node Address shown is FFFE, this radio is a remote station or repeater station but has not been registered with the base station.

The base station will automatically allocate a Node Address to all its registered repeater station and remote station radios. This address can be between 000B to 01FE.

Network Radius

This parameter displays the maximum number of hops in this network.

Network Repeaters Proximity

This parameter displays the proximity of repeaters in the network.

Repeater Network Segment ID

This parameter identifies a repeater network segment and its associated remotes.

In an overlapping coverage network where remote radios can 'see' multiple repeaters, it's especially important to set different values for each repeater network segment and its associated remotes, so the associated remotes will communicate only with the appropriate repeater.

The same setting applies in remote overlapping coverage between a base and a repeater. Different values per base and repeater are required if the requirements are that the remote will be communicating via the repeater and not directly with the base station (or vice-versa), i.e. the repeater and remotes will have the same value but different from the base station value. In this case, if the repeater fails, the remote will re-register to the base station even though they are on different values until the repeater recovers.

The entry is an integer from 0 and 31, where 0 is reserved for broadcast i.e. all radios will 'see' this radio traffic even if they are set to different values.

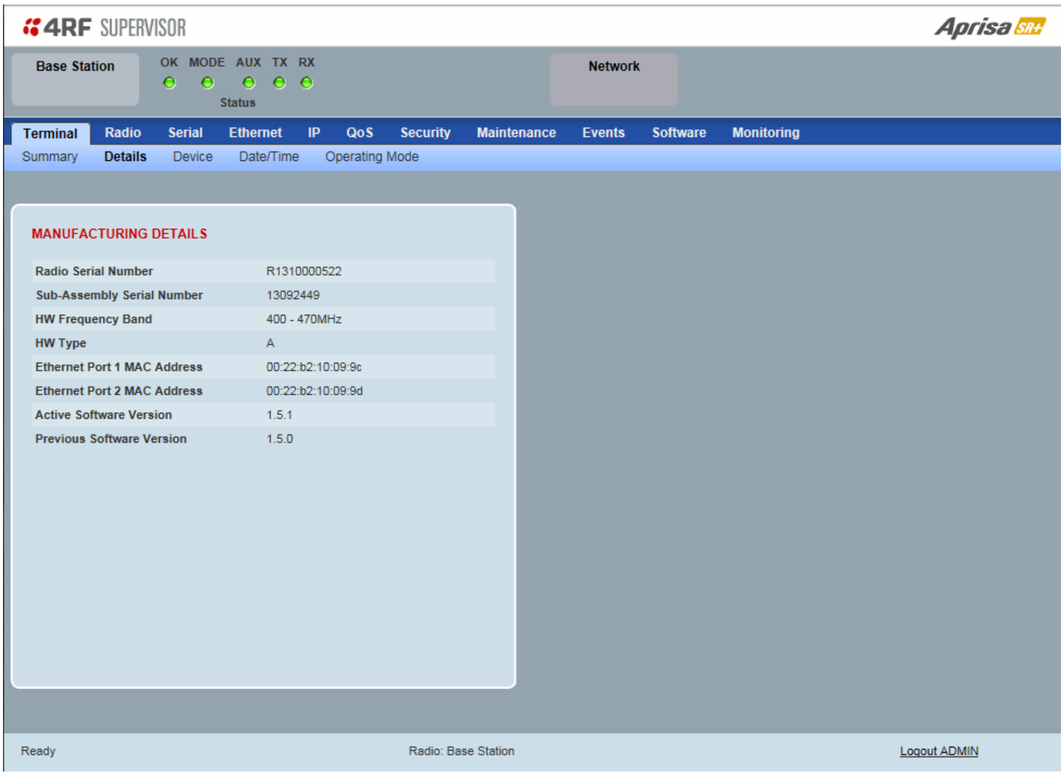
Inband Management

This parameter displays the status of the Inband Management option.

Inband Management Timeout (sec)

This parameter displays the number of seconds that the base station waits for a response from a Remote or repeater station before aborting the Inband Management request.

Terminal > Details



MANUFACTURING DETAILS

Radio Serial Number

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

Sub-Assembly Serial Number

This parameter displays the Serial Number of the printed circuit board assembly (shown on the PCB label).

HW Frequency Band

This parameter displays the hardware radio frequency operating range.

HW Type

This parameter displays the hardware board assembly type.

Radio MAC Address

This parameter displays the MAC address of the radio (the management Ethernet MAC address).

Active Software Version

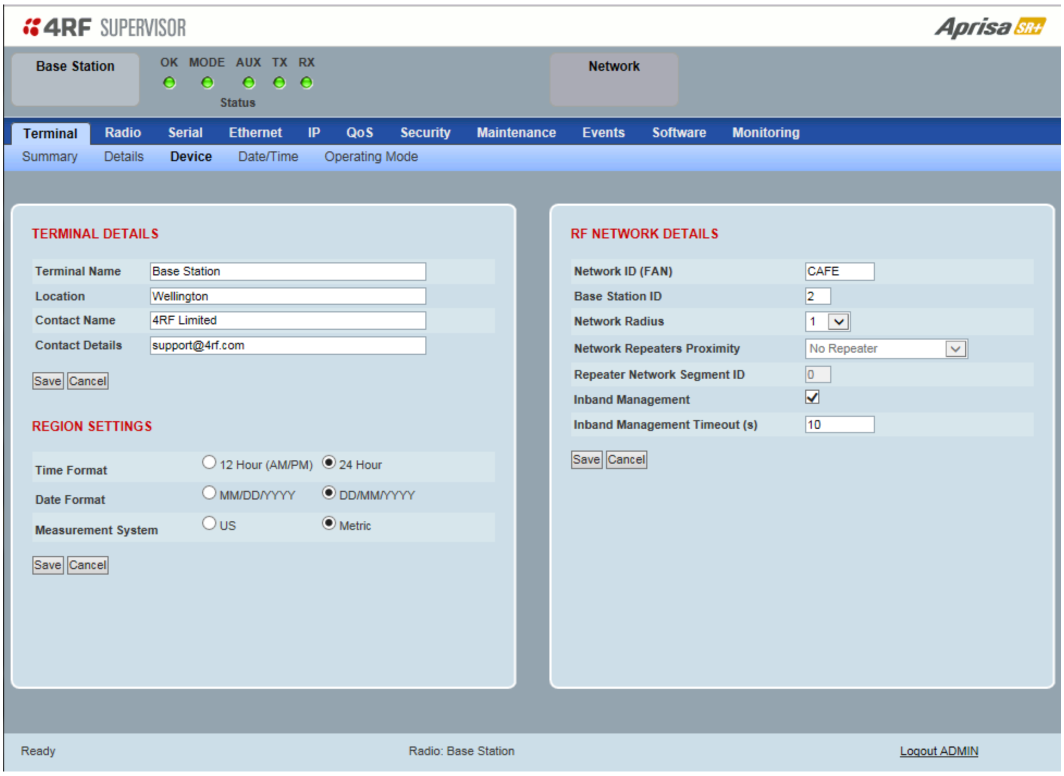
This parameter displays the version of the software currently operating the radio.

Previous Software Version

This parameter displays the software version that was running on the radio prior to the current software being activated.

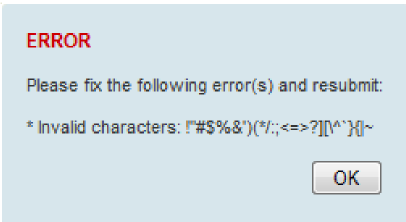
A new radio from the factory will display 'None' for the Previous SW Version.

Terminal > Device



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 Terminal Name.
2. Enter the Location of the radio.
3. Enter a Contact Name. The default value is ‘4RF Limited’.
4. Enter the Contact Details. The default value is ‘support@4RF.com’.

RF NETWORK DETAILS

Network ID

This parameter sets the network ID of this base station node and its remote / repeater stations in the network. The entry is four hexadecimal chars (not case sensitive).

The default setting is CAFE.

Base Station ID

This parameter identifies the base station. All radios operating to the base station in the same network must use the same Base Station ID setting.

It is especially important to set different values for each network when two or more networks using the same frequencies are operating with some overlapping coverage. The entry is an integer from 1 to 8.

Network Radius

This parameter sets the maximum number of hops in this network e.g. in a network with base station, repeater and remotes communicating via the repeater, the Network Radius should be set to 2. If the Network Radius is set to 2, a message from that node will only pass 2 hops before it is blocked.

The default setting is 1.

When base station is configured as a ‘Base-Repeater’ (used for remote peer to peer operation via the base station), the use of Network Radius does not change and works the same as if it were a Base Station i.e. the Network Radius is always the number of hops from the base station to the most distant remote in the network.

All stations in the network should be set to the same value.

Network Repeaters Proximity

This parameter is set in base stations, remote stations and repeater stations to indicate the proximity of repeaters in the network when the Network Radius is set to greater than 1.

Option	**Function**
Single Repeater Only	Use when there is only one repeater in the network.
Overlapping Coverage	Use for multiple one hop repeaters where the remote station can see more than one repeater or repeaters can see each other. The communication protocol is slower because each repeater is addressed individually and in-turn.
Separated Coverage	Use for multiple one hop repeaters where the remote station can only see one repeater and the repeaters can’t see each other. This option provides better network downlink performance than the Overlapping Coverage option. However, if the repeaters can see each other, the resultant collisions will cause corruptions and dramatically reduce network downlink performance.

This parameter is set in remote stations to indicate the proximity of repeaters in the network when the Network Radius is set to 1.

Option	Function
No Repeater	Use when there are no repeaters in the network.
Base Repeater	Use when there is a base-repeater in the network.

The Network Repeaters Proximity options are dependent on the Terminal Operating Mode and the Terminal Network Radius settings:

Operating Mode	Network Radius	Network Repeaters Proximity Options	Default
Base	1	No Repeater	No Repeater
Base	2	Single Repeater Only, Overlapping Coverage, Separated Coverage	Single Repeater Only
Remote	1	No Repeater, Base Repeater	No Repeater
Remote	2	Single Repeater Only, Overlapping Coverage, Separated Coverage	Single Repeater Only
Repeater	1	No Repeater, Base Repeater	No Repeater
Repeater	2	Single Repeater Only, Overlapping Coverage, Separated Coverage	Single Repeater Only
Base Repeater	1	Base Repeater	Base Repeater
Base Repeater	2	Single Repeater Only, Overlapping Coverage, Separated Coverage	Single Repeater Only

Repeater Network Segment ID

This parameter identifies a repeater network segment and its associated remotes.

In an overlapping coverage network where remote radios can 'see' multiple repeaters, it's especially important to set different values for each repeater network segment and its associated remotes, so the associated remotes will communicate only with the appropriate repeater.

The same setting applies in remote overlapping coverage between a base and a repeater. Different values per base and repeater are required if the requirements are that the remote will be communicating via the repeater and not directly with the base station (or vice-versa), i.e. the repeater and remotes will have the same value but different from the base station value. In this case, if the repeater fails, the remote will re-register to the base station even though they are on different values until the repeater recovers.

The entry is an integer from 0 and 31, where 0 is reserved for broadcast i.e. all radios will 'see' this radio traffic even if they are set to different values.

Inband Management

This parameter sets the Inband Management option.

If the Inband Management option is enabled, SuperVisor operating on a base station can also manage all the remote / repeater stations in the network.

Inband Management Timeout (sec)

This parameter sets the Inband Management timeout period. This determines the time the base station waits for a response from a remote or repeater station before aborting the Inband Management request. The default setting is 10 seconds.

REGION SETTINGS

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.

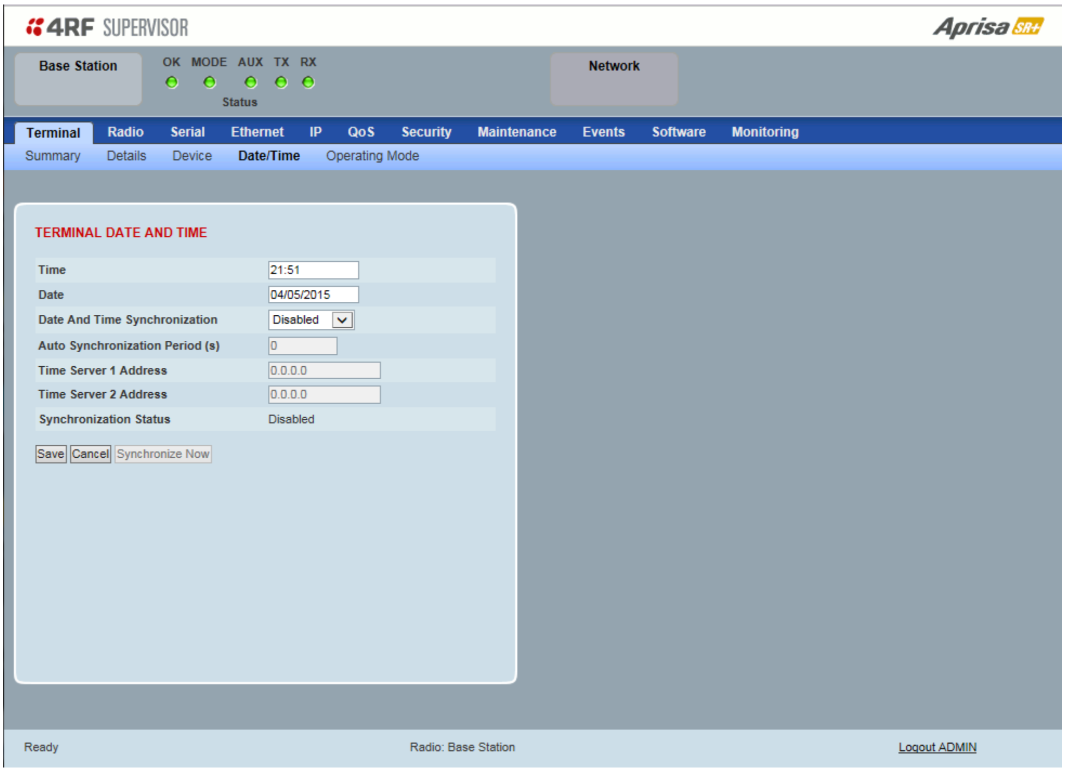
The default setting is DD/MM/YYYY.

Measurement System

This parameter sets the unit type for parameters like temperature readings.

The default setting is Metric.

Terminal > Date / Time



TERMINAL DATE AND TIME

Sets the Time and Date. This information is controlled from a software clock.

Date and Time Synchronization

This Date and Time Synchronization feature allows a radio to synchronize its date and time from an SNTP server. It would predominantly be used on the base station but could be used on a remote station.

Using the SNTP feature will ensure that all radios in the network has the same date and time required for accurate network diagnostics.

For high availability time/date synchronization, SNTP can be synchronized from two SNTP servers for server backup.

The default setting is Disabled.

Option	Function
Disabled	No SNTP Date and Time Synchronization
SNTP	Date and Time will be synchronized to a SNTP server

The base station periodically sends a broadcast message to the remote stations to synchronize the radio date and time.

Auto Synchronization Period (s)

This parameter sets the number of seconds between the end of the last synchronization and the next synchronization attempt. The minimum period is 60 seconds. A period of 0 seconds will disable synchronization attempts.

Time Server 1 Address

This parameter sets the IP address of the first priority SNTP server. If the synchronization is successful to this server, Time Server 2 Address will not be used.

Time Server 2 Address

This parameter sets the IP address of the second priority SNTP server. If the synchronization fails using the SNTP server on Time Server 1 Address, synchronization will be attempted to the SNTP server on this address.

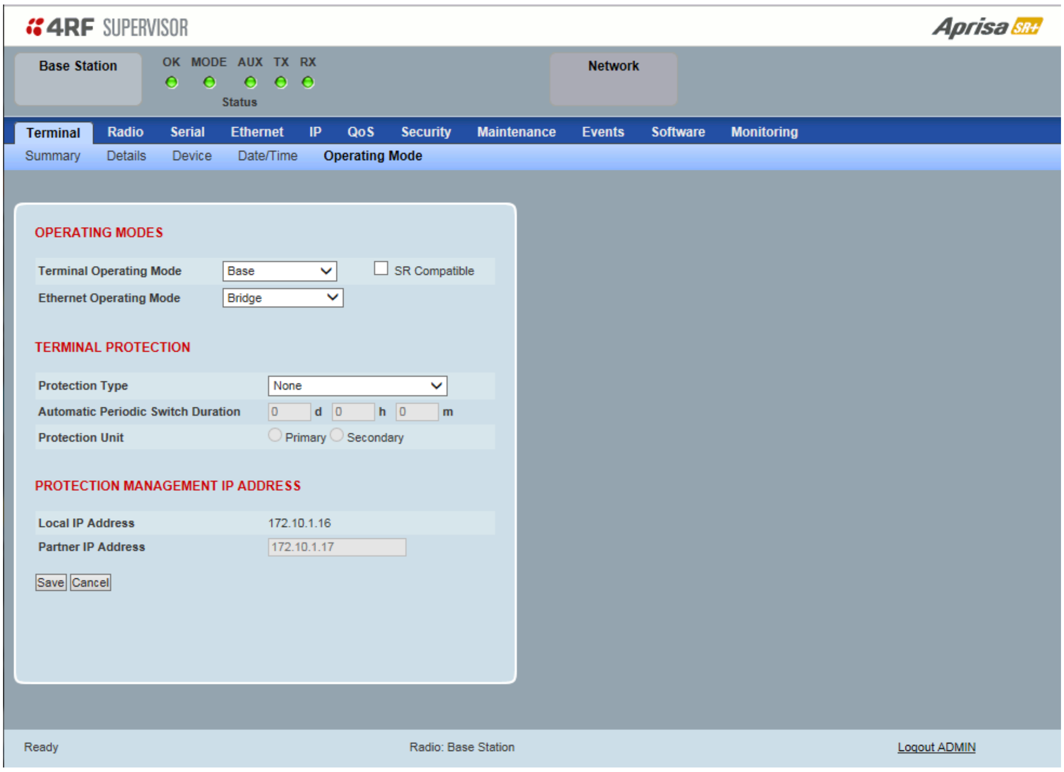
Synchronization Status

This field shows the status of the current synchronization or the result of the last synchronization.

Synchronize Now

This Synchronize Now button provides manual Synchronization.

Terminal > Operating Mode



OPERATING MODES

Terminal Operating Mode

The Terminal Operating Mode can be set to Base, Base Repeater, Repeater or Remote station. The default setting is Remote.

Option	Function
Base	The base station manages all traffic activity between itself, repeaters and remotes. It is the center-point of network where in most cases will be connected to a SCADA master.
Base Repeater	The base-repeater has the same function as the base station (and repeater station), but used when peer to peer connections between remotes is required via the base station.
Repeater	The repeater forwards packets coming from base station and other repeaters e.g. in daisy chain LBS mode and /or remote stations.
Remote	The remote in most cases is used as the end-point of the SCADA network connected to an RTU or PLC device for SCADA network control and monitoring.

SR Compatible

The SR Compatible option enables over-the-air point-to-multipoint interoperation between an Aprisa SR+ network and New Aprisa SR radios. The default setting is unticked.

When the Aprisa SR+ 'SR Compatible' option is activated, the Aprisa SR+ locks its modulation to QPSK (as per the New Aprisa SR modulation) and disables functionality which is not available in New Aprisa SR for full compatibility / interoperability operation.

This compatibility option allows the user a smooth migration to Aprisa SR+ when higher speeds of 120, 60 kbit/s (at 25, 12.5 kHz channel sizes), Adaptive Coding Modulation, full duplex and more features are required.

Note: Any mix between the New Aprisa SR and Aprisa SR+ in the network will force the whole network to work in SR Compatible mode.

Ethernet Operating Mode

The Ethernet Operating Mode defines how Ethernet / IP traffic is processed in the radio. The default setting is Bridge.

Option	Function
Bridge	Bridge mode inspects each incoming Ethernet frame source and destination MAC addresses to determine if the frame is forwarded over the radio link or discarded.
Gateway Router	Gateway Router mode inspects each incoming IP source and destination IP addresses to determine if the packet is forwarded over the radio link or discarded. In this mode, all Ethernet interfaces have the same IP address and subnet.
Router	Router mode inspects each incoming IP source and destination IP addresses to determine if the packet is forwarded over the radio link or discarded. In this mode, each Ethernet interface has a different IP address and subnet.

TERMINAL PROTECTION

Protection Type

The Protection Type defines if a radio is a stand-alone radio or part of an Aprisa SR+ Protected Station. The default setting is None.

Option	Function
None	The SR+ radio is stand-alone radio (not part of an Aprisa SR+ Protected Station).
Redundant (Protected Station)	Set to make this SR+ radio part of an Aprisa SR+ Protected Station. The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio
Monitored Hot Standby (Protected Station)	Set to make this SR+ radio part of an Aprisa SR+ Protected Station. The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio. The standby radio is monitored to ensure its correct operation should a switch-over be required. See 'Monitored Alarms' on page 316 for the list of monitored alarms.
Serial Data Driven Switching	Set to make this SR+ radio part of an Aprisa SR+ Data Driven Protected Station.

Protection Unit

The Protection Unit defines if this radio is the primary radio or secondary radio in a Protected Station.

One radio in the Protected Station is set to Primary and the other radio to Secondary.

It is recommended that radio A (the left radio) be configured as the Primary and that radio B (the right radio) be configured as the Secondary. The default setting is Primary.

This menu item is only applicable if this radio is to become part of an Aprisa SR+ Protected Station.

PROTECTION MANAGEMENT IP ADDRESS

Local IP Address

The Local IP Address shows the IP address of this radio.

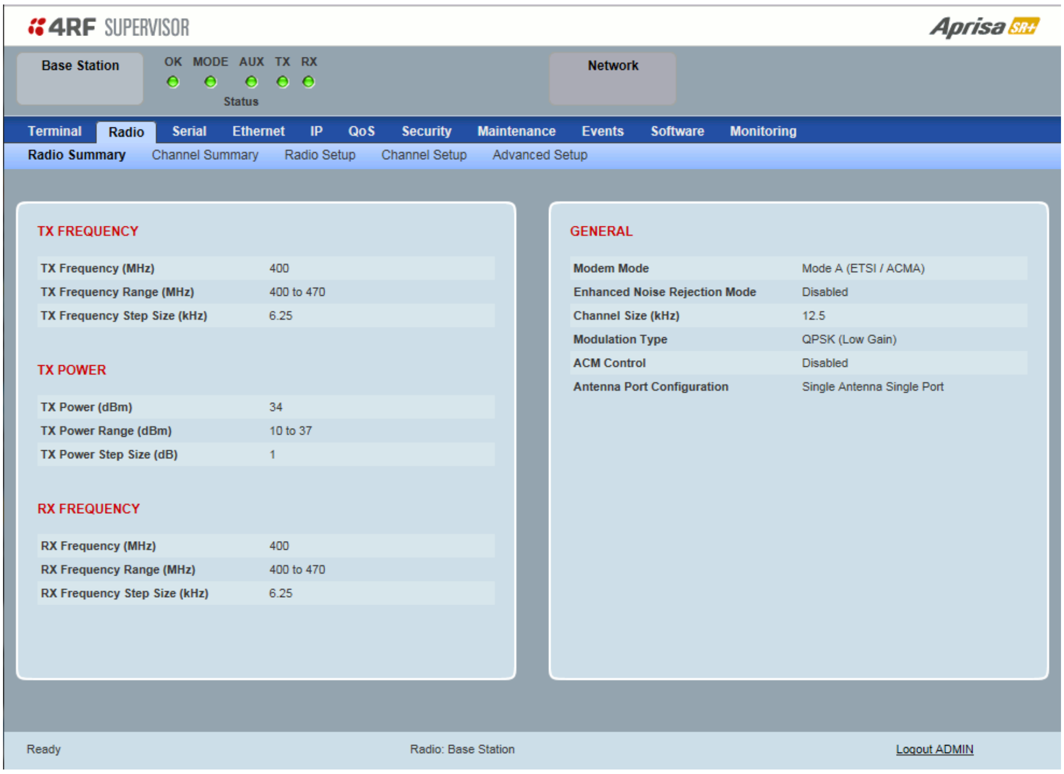
Partner IP Address

The Partner IP Address parameter is used to set the partner IP address if this radio is to become part of a Protected Station.

Radio

Radio > Radio Summary

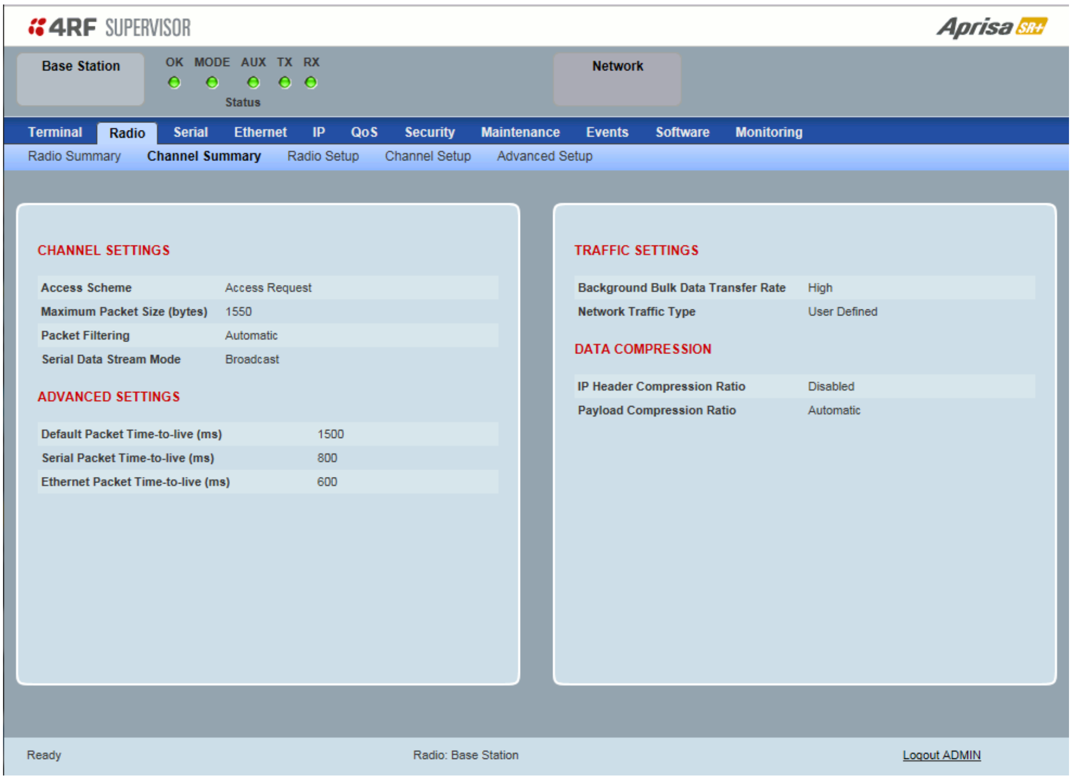
This page displays the current settings for the Radio parameters.



See ‘Radio > Radio Setup’ and ‘Radio > Channel Setup’ for setting details.

Radio > Channel Summary

This page displays the current settings for the Channel parameters.



See 'Radio > Channel Setup' for setting details.

DATA COMPRESSION

IP Header Compression Ratio

See 'IP Header Compression Ratio' on page 112.

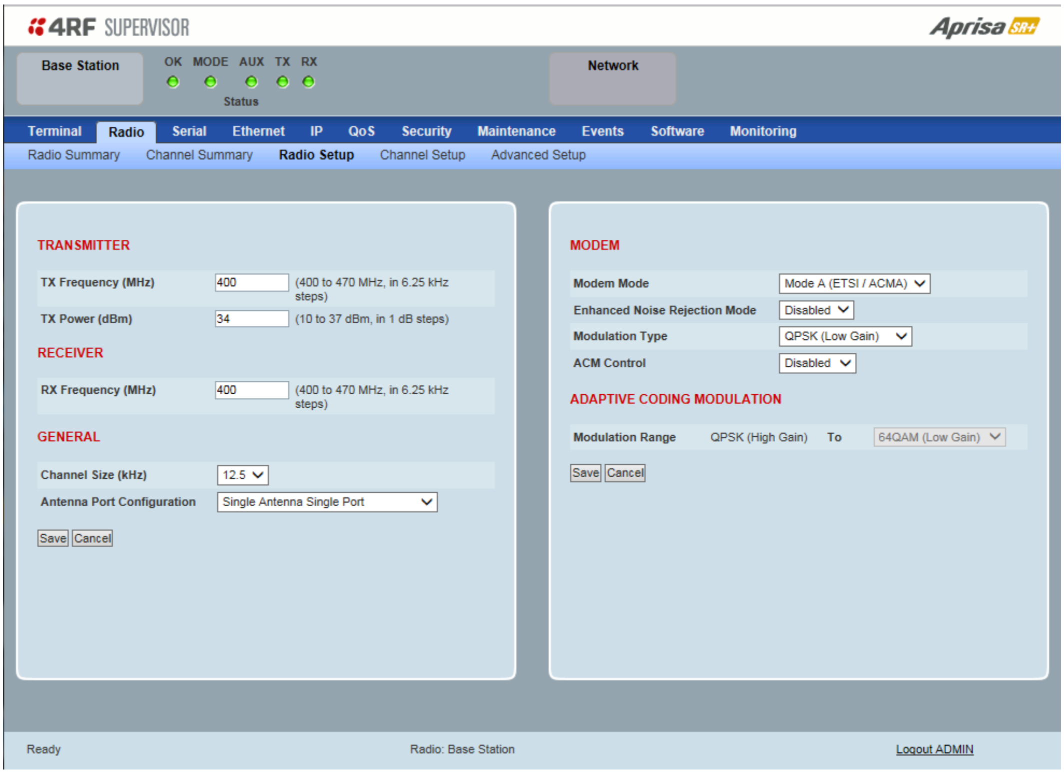
Payload Compression Ratio

The payload is compressed using level 3 QuickLZ data compression. Payload Compression is automatic and cannot be turned off by SuperVisor.

Compression is not attempted on data that is already compressed e.g. jpg files.

Radio > Radio Setup

Transmit frequency, transmit power and channel size would normally be defined by a local regulatory body and licensed to a particular user. Refer to your site license details when setting these fields.



TRANSMITTER / RECEIVER

Important:

1. Changing the remote / repeater station frequencies will disable all management communication to the remote / repeater stations but then by changing the base station to match the remote / repeater stations, the radio links will be restored as will the management communication.

2. Enter the TX frequency and the RX frequency and then click 'Save'. This is to prevent remote management communication from being lost before both frequencies have been changed in the remote stations.

TX and RX Frequencies.

The TX and RX frequencies entered must be within the frequency tuning range of the product frequency band (see 'Frequency Bands' on page 357).

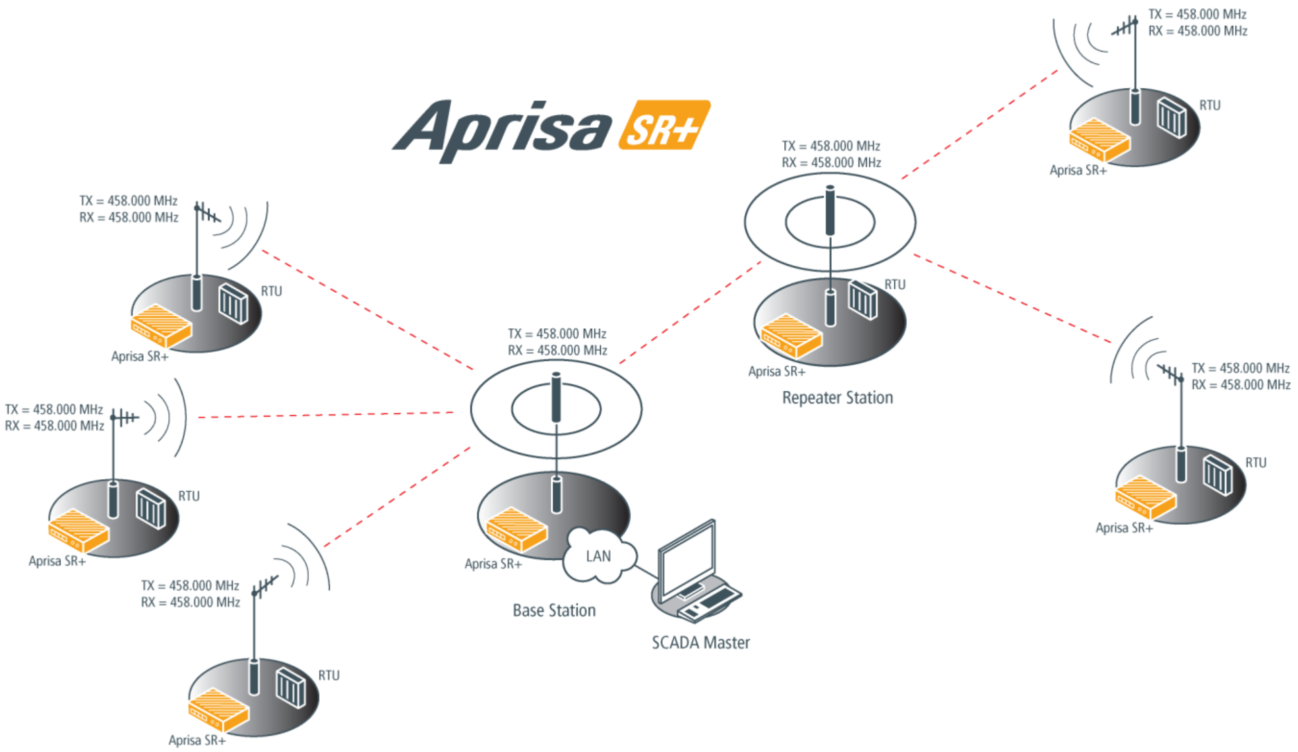
If the frequency entered is not resolvable to the synthesizer step size for the frequency band it is rejected. For example; a 400 MHz radio has a synthesizer step size of 6.250 kHz.

The TX and RX frequencies can be single frequency half duplex or dual frequency half duplex. Dual frequency half duplex is often used for reasons of:

- Channel Planning
- Network Efficiencies
- Regulatory rules

Single Frequency Operation

The TX and RX frequencies of the base station, repeater station and all the remote stations are on the same frequency.



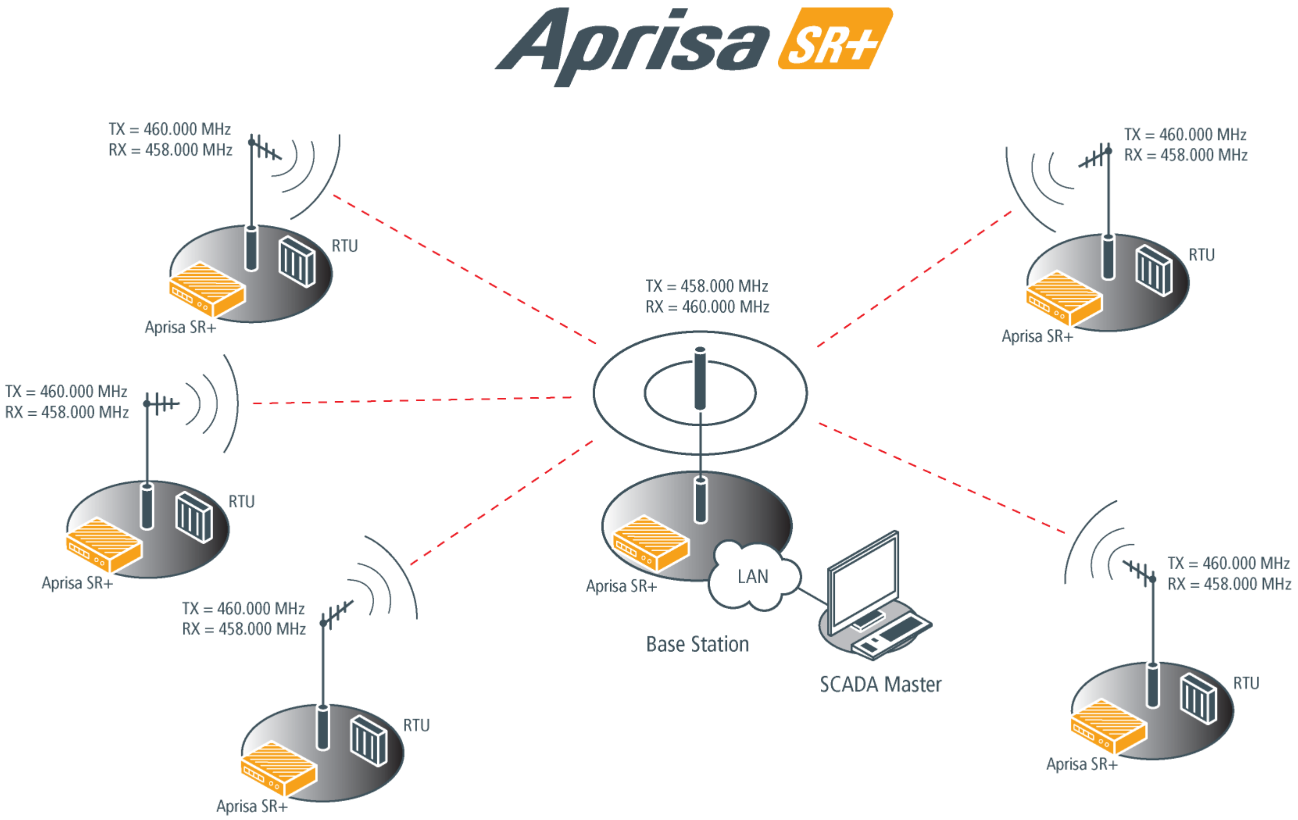
To change the TX and RX frequencies:

1. Change the TX and RX frequencies of the remote stations operating from the repeater station to the new frequency. The radio links to these remote stations will fail.
2. Change the TX and RX frequencies of the repeater station operating from the base station to the new frequency. The radio links to the repeater station and its remote stations will fail.
3. Change the TX and RX frequencies of the remote stations operating from the base station to the new frequency. The radio links to these remote stations will fail.
4. Change the TX and RX frequencies of the base station to the new frequency. The radio links to all stations will restore.

Dual Frequency No Repeater

The TX frequency of all the remote stations matches the RX frequency of the base station.

The RX frequency of all the remote stations matches the TX frequency of the base station.



To change the TX and RX frequencies:

1. For all the remote stations, change the RX frequency to frequency A and the TX frequency to frequency B. The radio links to the remote stations will fail.
2. For the base station, change the TX frequency to frequency A and the RX frequency to frequency B. The radio links to the remote stations will restore.

Dual Frequency with Repeater

The TX frequency of the remote stations associated with the base station matches the RX frequency of the base station.

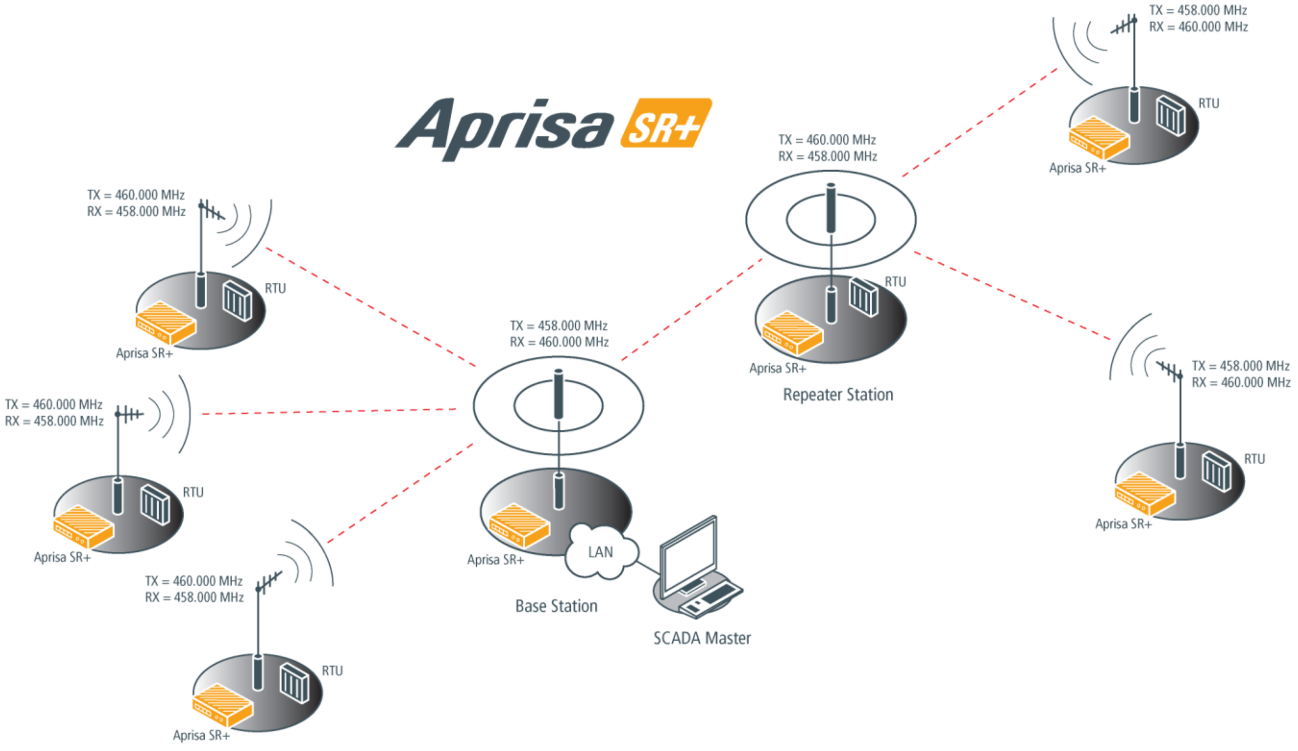
The TX frequency of the repeater station associated with the base station matches the RX frequency of the base station.

The TX frequency of the remote stations associated with the repeater station matches the RX frequency of the repeater station.

The RX frequency of the remote stations associated with the base station matches the TX frequency of the base station.

The RX frequency of the repeater station associated with the base station matches the TX frequency of the base station.

The RX frequency of the remote stations associated with the repeater station matches the TX frequency of the repeater station.



To change the TX and RX frequencies:

1. For all the remote stations operating from the repeater station, change the RX frequency to frequency A and the TX frequency to frequency B. The radio links to these remote stations will fail.
2. For the repeater station, change the TX frequency to frequency A and the RX frequency to frequency B. The remote stations operating from the repeater station, will now establish a connection to the repeater.
3. For all the remote stations operating from the base station, change the TX frequency to frequency A and the RX frequency to frequency B. The radio links to these remote stations will fail.
4. For the base station, change the RX frequency to frequency A and the TX frequency to frequency B. The radio links to the remote stations operating from the repeater station or the base station will restore.

TX Power

The transmitter power is the power measured at the antenna output port when transmitting. The transmitter power has a direct impact on the radio power consumption.

The default setting is +37 dBm.

If TX Power setting is higher than the high limit or lower than the low limit for the current modulation, an Informational Event (55 Terminal Unit Information) will be raised to notify the user that transmit power has been changed. This only applies to fixed modulation (not ACM).

Note: The Aprisa SR+ transmitter contains power amplifier protection which allows the antenna to be disconnected from the antenna port without product damage.

GENERAL

Channel Size (kHz)

This parameter sets the Channel Size for the radio (see ‘Channel Sizes’ on page 358 for Radio Capacities). The default setting is 12.5 kHz.

Antenna Port Configuration

This parameter sets the Antenna Port Configuration for the radio.

Option	Function
Single Antenna Single Port	Select Single Antenna Single Port if using one or two frequency half duplex transmission. The antenna is connected to the ANT port.
Single Antenna Dual Port (duplexer)	Select Single Antenna Dual Port if using: (1) One or two frequency in half duplex transmission with an external duplexer (for filtering) connected to the ANT/TX and RX antenna ports and single antenna connected to the duplexer. (2) Two frequency in full duplex transmission with an external duplexer (for full duplex operation) connected to the ANT/TX and RX antenna ports and single antenna connected to the duplexer. (3) Single frequency in half duplex transmission with external dual antennas, connected to the ANT/TX and RX antenna ports. (4) Two frequency in half or full duplex transmission with external dual antennas, connected to the ANT/TX and RX antenna ports.

The default setting is Single Antenna Single Port.

MODEM

The Radio > Radio Setup screen Modem section is different for a base / repeater / base-repeater station and a remote station.

Modem Mode

This parameter sets the Modem Mode in the radio. The Modem Mode option list is dependent on the radio Hardware Variant.

HW Variant	Option	Channel Sizes
136 MHz	Mode A (FCC / IC)	15 and 30 kHz
	Mode B (ETSI)	12.5 and 25 kHz
220 MHz	Mode A (FCC / IC)	12.5, 15, 25 and 50 kHz
320 MHz	Mode A (ETSI / ACMA)	12.5, 20, 25 and 50 kHz
400 MHz	Mode A (ETSI / ACMA)	12.5, 20 and 25 kHz
	Mode B (FCC / IC)	12.5 and 25 kHz
450 MHz	Mode A (ETSI / ACMA)	12.5 and 25 kHz
	Mode B (FCC)	12.5 and 25 kHz
896 MHz	Mode A (FCC / IC)	12.5, 25 and 50 kHz
	Mode B (FCC Part 24)	12.5, 25 and 50 kHz
	Mode C (IC RSS-134)	12.5, 25 and 50 kHz
928 MHz	Mode A (FCC)	12.5, 25 and 50 kHz
	Mode B (IC)	12.5, 25 and 50 kHz
	Mode C (FCC Part 24)	12.5, 25 and 50 kHz
	Mode D (IC RSS-134)	12.5, 25 and 50 kHz

Enhanced Noise Rejection Mode

This parameter enables / disables the Enhanced Noise Rejection Mode in the radio. This feature improves co-channel interference performance at strong receiver signal levels. All radios in an Aprisa SR+ network must use the same setting i.e. enabled or disabled.

The default setting is Disabled.

MODEM - Base / Repeater/ Base-Repeater Station

Modulation Type

The base to remote / repeater or repeater to remote / base direction of transmission is always fixed i.e. not adaptive.

This parameter sets the fixed TX Modulation Type for the base / base-repeater / repeater radio.

Option	Function
QPSK (High Gain)	Sets the modulation to QPSK with Max Coded FEC.
QPSK (Low Gain)	Sets the modulation to QPSK with Min Coded FEC.
QPSK	Sets the modulation to QPSK with no FEC.
16QAM (High Gain)	Sets the modulation to 16 QAM with Max Coded FEC.
16QAM (Low Gain)	Sets the modulation to 16 QAM with Min Coded FEC.
16QAM	Sets the modulation to 16 QAM with no FEC.
64QAM (High Gain)	Sets the modulation to 64 QAM with Max Coded FEC.
64QAM (Low Gain)	Sets the modulation to 64 QAM with Min Coded FEC.

The default setting is QPSK (Low Gain).

The base / base-repeater radio TX modulation will be set based on the worse case (RSSI) path profile scenario of all the radios (remotes and repeaters) in one hop distance from the base / base-repeater radio.

The repeater radio TX modulation will be set based on the worse case (RSSI) path profile scenario of all the radios (remotes and base) in one hop distance from the repeater radio.

ACM Control

This parameter enables / disables Adaptive Code Modulation for the remote to base direction of transmission (upstream).

When ACM is enabled (ACM Control set to Standard or Fast), the base station sends a modulation type recommendation to each remote radio based on the signal quality for each individual remote radio.

Option	Function
Disabled	Disables Adaptive Code Modulation for the upstream. The base station does not send a modulation type recommendation to any remote radio.
Fast	Enables Adaptive Code Modulation for the upstream. The ACM will switch down one ACM level if an errored packet is received. The ACM will switch up when the link quality exceeds the performance threshold. This option maintains the highest network speeds for as long as possible.
Standard	Enables Adaptive Code Modulation for the upstream. The ACM will switch down one ACM level if the link quality degrades in advance of the level where errored packets would be expected and will switch to the lowest ACM level if an errored packet is received. The ACM will switch up when the link quality exceeds the performance threshold. This option preserves packet integrity but reduces network speeds.

The default setting is Fast.

ADAPTIVE CODING MODULATION

These settings are only used if the ACM Control is set to Enabled and only apply to the base to remote direction of transmission (downstream).

Modulation Range

This parameter sets the upper limit of the range that the base station will recommend to the remote radios.

The lower limit is fixed to QPSK (High Gain).

<u>MODEM - Remote Station</u>

Modulation Type

The remote to base / base-repeater / repeater direction of transmission can be adaptive modulation or fixed modulation.

This parameter sets the TX Modulation Type for the remote station radio.

Option	Function
Adaptive	Sets the modulation type to Adaptive Code Modulation. The remote radio receives the modulation type recommendation from the base / base-repeater / repeater station and adjusts the modulation and FEC code rate in the remote to base / base-repeater / repeater direction of transmission (upstream) if the modulation type recommendation is within the defined Modulation Range (see Modulation Range setting below). If the recommendation is outside the defined Modulation Range, the upper limit is used for the remote radio.
QPSK (High Gain)	Sets the modulation to QPSK with Max Coded FEC.
QPSK (Low Gain)	Sets the modulation to QPSK with Min Coded FEC.
QPSK	Sets the modulation to QPSK with no FEC.
16QAM (High Gain)	Sets the modulation to 16 QAM with Max Coded FEC.
16QAM (Low Gain)	Sets the modulation to 16 QAM with Min Coded FEC.
16QAM	Sets the modulation to 16 QAM with no FEC.
64QAM (High Gain)	Sets the modulation to 64 QAM with Max Coded FEC.
64QAM (Low Gain)	Sets the modulation to 64 QAM with Min Coded FEC.

ADAPTIVE CODING MODULATION

These settings are only used if the Modulation Type is set to Adaptive and only apply to the remote to base / base-repeater / repeater direction of transmission (upstream).

Default Modulation

This parameter sets the default modulation and FEC code rate for the remote to base / base-repeater / repeater direction of transmission when the ACM mechanism fails for whatever reason. It is also used when the radio starts up, and subsequently, if there are no recommendations received from the base / base-repeater / repeater station, it will remain at that setting.

Upstream recommendations are always expected to be received from the base / base-repeater / repeater station. For example, when the base / base-repeater / repeater station 'ACM control' is set to 'disabled' and the 'modulation type' at the remote is set to 'adaptive', the default modulation will be used. In this case, the base / base-repeater / repeater station will not recommend any changes to the remote radios and so the remote radio will remain on the configured ‘Default Modulation’.

This parameter sets the TX Modulation Type for the remote station radio.

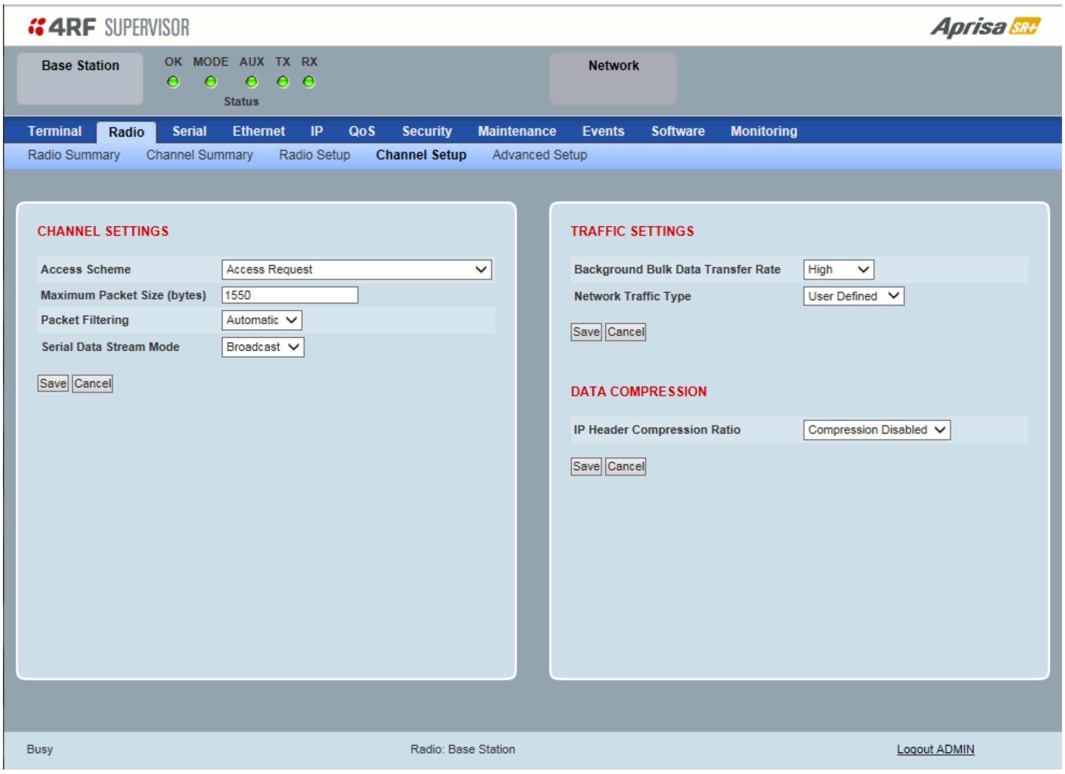
Option	Function
QPSK (High Gain)	Sets the modulation to QPSK with Max Coded FEC.
QPSK (Low Gain)	Sets the modulation to QPSK with Min Coded FEC.
QPSK	Sets the modulation to QPSK with no FEC.
16QAM (High Gain)	Sets the modulation to 16 QAM with Max Coded FEC.
16QAM (Low Gain)	Sets the modulation to 16 QAM with Min Coded FEC.
16QAM	Sets the modulation to 16 QAM with no FEC.
64QAM (High Gain)	Sets the modulation to 64 QAM with Max Coded FEC.
64QAM (Low Gain)	Sets the modulation to 64 QAM with Min Coded FEC.

Modulation Range

This parameter sets the upper limit that the Adaptive Code Modulation can automatically adjust up to.

The lower limit is fixed to QPSK (High Gain).

Radio > Channel Setup



CHANNEL SETTINGS

Access Scheme

This parameter sets the Media Access Control (MAC) used by the radio for over the air communication.

Option	Function
Access Request	Channel access scheme where the base station controls the communication on the channel. Remotes ask for access to the channel, and the base station grants access if the channel is not occupied. This mode is a general purpose access method for high and low load networks.
Access Request (full duplex)	Used on a network with full duplex base station hardware and half duplex repeaters / remotes. A full duplex version of Access Request channel access scheme where the base station controls the communication on the channel. Remotes ask for access to the channel, and the base station grants access if the channel is not occupied. The base station can send traffic during remote transmit, exploiting the base station full duplex capabilities.
Listen Before Send without Acknowledgement	Channel access scheme where network elements listen to ensure the channel is clear, before trying to access the channel. This mode is optimised for low load networks and repeated networks. Acknowledgements are disabled.

Listen Before Send with Acknowledgement	Channel access scheme where network elements listen to ensure the channel is clear, before trying to access the channel. This mode is optimised for low load networks and repeated networks. With Acknowledgement, unicast requests from the remote station are acknowledged by the base station to ensure that the transmission has been successful. If the remote station does not receive an acknowledgement, then random back-offs are used to reschedule the next transmission. Enabling acknowledgments increases reliability of transport but reduces available channel capacity so if application has the capability to handle lost or duplicate messages, the Access Scheme should be set to Listen Before Send without Acknowledgement.
Point To Point (Half Duplex)	Channel access scheme used for Mirrored Bits ®.

The default setting is Access Request.

Repeater

This parameter sets the Media Access Control (MAC) used by the radio for over the air communication.

Maximum Packet Size (Bytes)

This parameter sets the maximum over-the-air packet size in bytes. A smaller maximum Packet Size is beneficial when many remote stations or repeater stations are trying to access the channel. The default setting is 1550 bytes.

As radios dispatched from the factory have a Packet Size set to the maximum value of 1550 bytes, if a new radio is installed in an existing network, the Packet Size must be changed to ensure it is the same value for all radios in the network. The new radio will not register an existing network if the Packet Size is not the same as the other radios in the network.

This packet size includes the wireless protocol header and security payload (0 to 16 bytes). The length of the security header depends on the level of security selected.

When the security setting is 0, the maximum user data transfer over-the-air is 1516 bytes.

When encryption is enabled, the entire packet of user data (payload) is encrypted. If authentication is being used, the security frame will be added (up to 16 bytes). The wireless protocol header is then added which is proprietary to the Aprisa SR+. This is not encrypted.

Packet Filtering

Each Aprisa SR+ radio can filter packets not destined for itself. The Packet Filtering parameter controls this functionality.

In an Aprisa SR+ network, all communication from remote stations is destined for the base station in the Aprisa SR+ network communication protocol. In a repeater or base-repeater network, a remote station will send a message to the base station. The repeater station will receive this and then repeat the message. The repeated message will then be received by the base station. Other remote stations connected to the repeater station will receive this message and depending on the Packet Filtering parameter, either forward this packet or discard it.

This filtering capability can provide the ability for remote stations to communicate with each other (peer to peer communication) when connected to a repeater station or to a base-repeater station, particularly useful in the event of losing communication with a SCADA Master, assuming the Aprisa SR+ network is still operational. For example, to create peer to peer communication between two remotes in a network with a base-repeater, the base-repeater packet filtering setting is set to 'Automatic' and the two remotes packet filtering setting is set to 'Disabled'.

Note: IP Header Compression must be disabled for this feature to operate correctly (see 'IP Header Compression Ratio' on page 112).

Option	Function
Disabled	Every packet received by the radio will be forwarded to the relevant interface.
Automatic	The radio will filter (discard) packets not destined for itself according to the Aprisa SR+ traffic protocols

The default setting is Automatic.

Note: The Aprisa SR+ network is transparent to the protocol being transmitted; therefore the Packet Filtering parameter is based on the Aprisa SR+ addressing and network protocols, not the user (SCADA, etc.) traffic protocols.

Serial Data Stream Mode

This parameter controls the traffic flow in the radio serial ports.

Option	Function
Broadcast	Serial port traffic from the network is broadcast on all serial ports on this radio. This will include the RS-232 port derived from the USB port.
Segregate	Serial port traffic from the network from a specific port number is directed to the respective serial port only (see Segregated Port Directions).

The default setting is Broadcast.

Segregated Port Directions

If the base station and the remote radios were deployed with the same Data Port product option e.g. all radios were purchased as 2E2S (two Ethernet ports and two Serial ports), serial port traffic from the network from a specific port number is directed to the respective serial port on all radios.

2E2S **Port Number**	**2E2S** **Port Number**
1	1
2	2
USB	USB

But if the base station and the remote radios were deployed with different Data Port product options, the following table shows how serial port traffic is directed:

2E2S **Port Number**	**3E1S** **Port Number**
1	1
2	NA
USB	USB

TRAFFIC SETTINGS

Background Bulk Data Transfer Rate

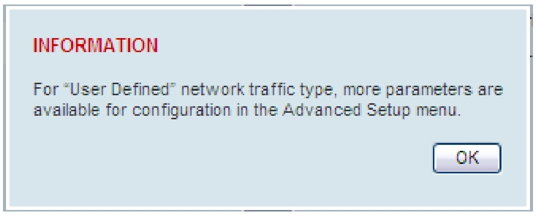
This parameter sets the data transfer rate for large amounts of management data.

Option	Function
High	Utilizes more of the available capacity for large amounts of management data. Highest impact on user traffic.
Medium	Utilizes a moderate of the available capacity for large amounts of management data. Medium impact on user traffic.
Low	Utilizes a minimal of the available capacity for large amounts of management data. Lowest impact on user traffic.

The default setting is high.

Network Traffic Type

This parameter optimizes the channel settings for the predominant traffic type.

Option	Function
User Defined	Allows the user to define the channel settings (see 'Radio > Advanced Setup' on page 113). 
Serial Only	Optimizes the channel settings for the predominantly serial traffic.
Ethernet Only	Optimizes the channel settings for the predominantly Ethernet traffic.
Mixed	Optimizes the channel settings for a mix of Ethernet and serial traffic.

The default setting is Mixed.

DATA COMPRESSION

IP Header Compression Ratio

The IP Header Compression implements TCP/IP ROHC v2 (Robust Header Compression v2. RFC4995, RFC5225, RFC4996) to compress the IP header. IP header compression allows for faster point-to-point transactions, but only in a star network.

IP Header Compression module comprises of two main components, compressor and decompressor. Both these components maintain some state information for an IP flow to achieve header compression. However, for reasons like packet drops or station reboots this state information can go out of sync between the compressor and decompressor resulting in compression and/or decompression failure resulting in loss of packets.

The compression ratio controls the rate at which compressor and decompressor synchronize state information with each other. Frequent synchronization results in reduced ratio.

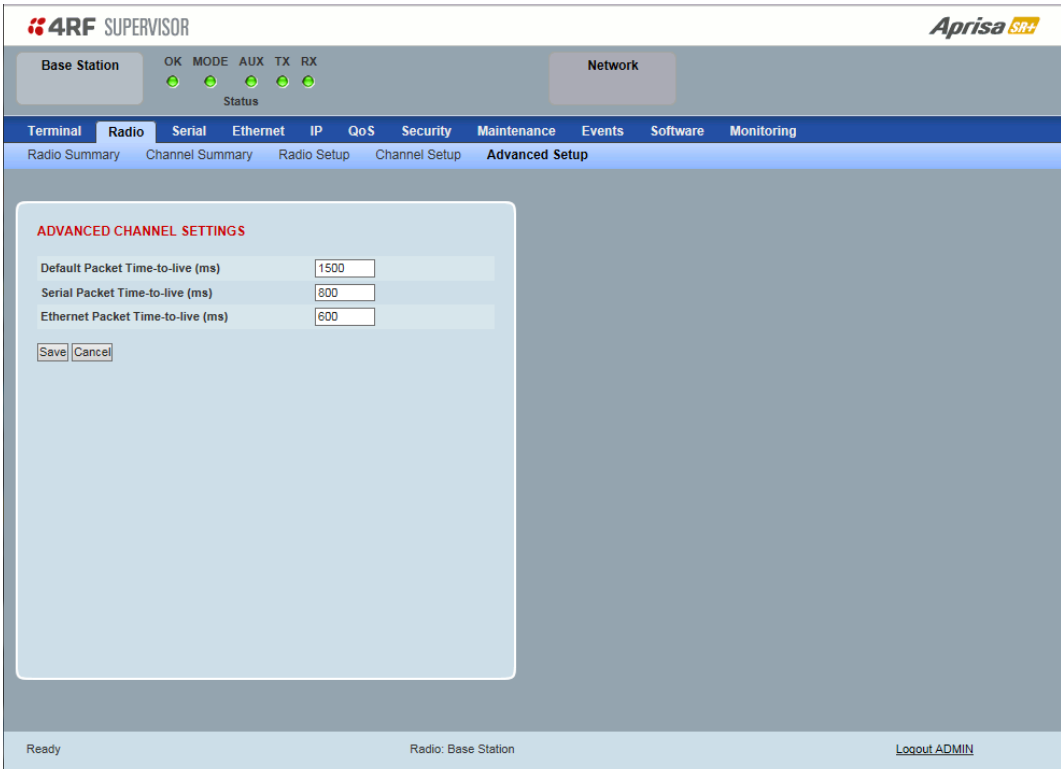
Option	Function
Compression Disabled	Disables IP header compression.
High	State information is synchronized less frequently thus achieving the best compression ratio.
Medium	State information is synchronization less frequently than 'High' setting but more frequently than 'Low' setting.
Low	State information is synchronized frequently thus reducing the compression ratio.

The default setting is High.

When IP Header Compression is enabled, it is important that the Network Radius is set correctly. If it was incorrectly set to 1, header compression could not be interpreted by radius 2 radios.

Radio > Advanced Setup

This page is only visible when the Channel Setup > Network Traffic Type is set to User Defined.



ADVANCED CHANNEL SETTINGS

Default Packet Time to Live (ms)

This parameter sets the default time a packet is allowed to live in the system before being dropped if it cannot be transmitted over the air. It is used to prevent old, redundant packets being transmitted through the Aprisa SR+ network. The default setting is 1500 ms.

In the case of serial poll SCADA networks such as MODBUS and IEC 60870.50.101, it is important to ensure the replies from the RTU are in the correct sequence and are not timed out replies from Master requests. If the TTL value is too long, the SCADA master will detect sequence errors.

It is recommended to use a TTL which is half the serial SCADA timeout. This is commonly called the ‘scan timeout’ or ‘link layer time out’ or ‘retry timeout’.

When using TCP protocols, a TTL of 1500 ms is recommended because a TCP re-transmission usually occurs after approximately 3 second.

In SCADA networks which use both serial and Ethernet, it is recommended that the TTL is set to half the serial SCADA timeout for serial remotes, and 1500 ms for Ethernet (TCP) remotes. For example, if the serial SCADA timeout is 1000 ms, a remote radio which is connected to the serial RTU should be set to 500 ms, a remote radio which is connected to an Ethernet (TCP) RTU should have a 1500 ms timeout.

In this case, the base station TTL should be set to 1500 ms as well; or whichever is the longer TTL of serial or Ethernet.

Serial Packet Time to Live (ms)

This parameter sets the time a serial packet is allowed to live in the system before being dropped if it cannot be transmitted over the air. The default setting is 800 ms.

Ethernet Packet Time to Live (ms)

This parameter sets the time an Ethernet packet is allowed to live in the system before being dropped if it cannot be transmitted over the air. The default setting is 600 ms.

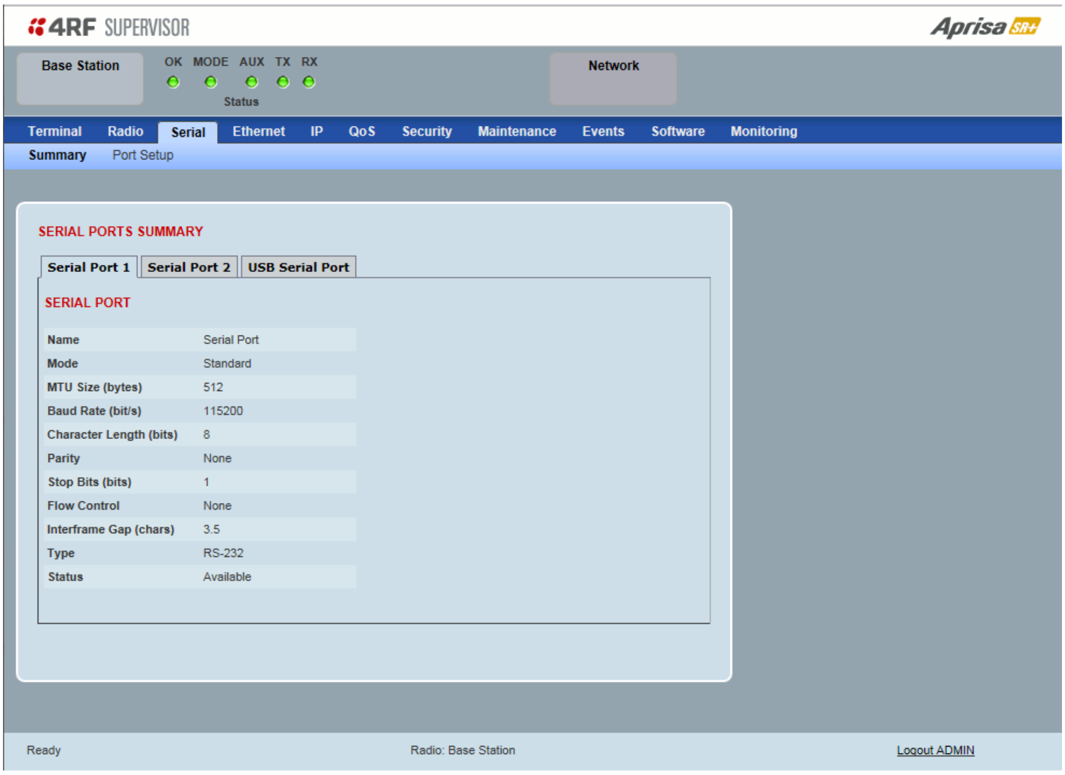
Serial

Serial > Summary

RS-232 Hardware Ports

This page displays the current settings for the serial port parameters.

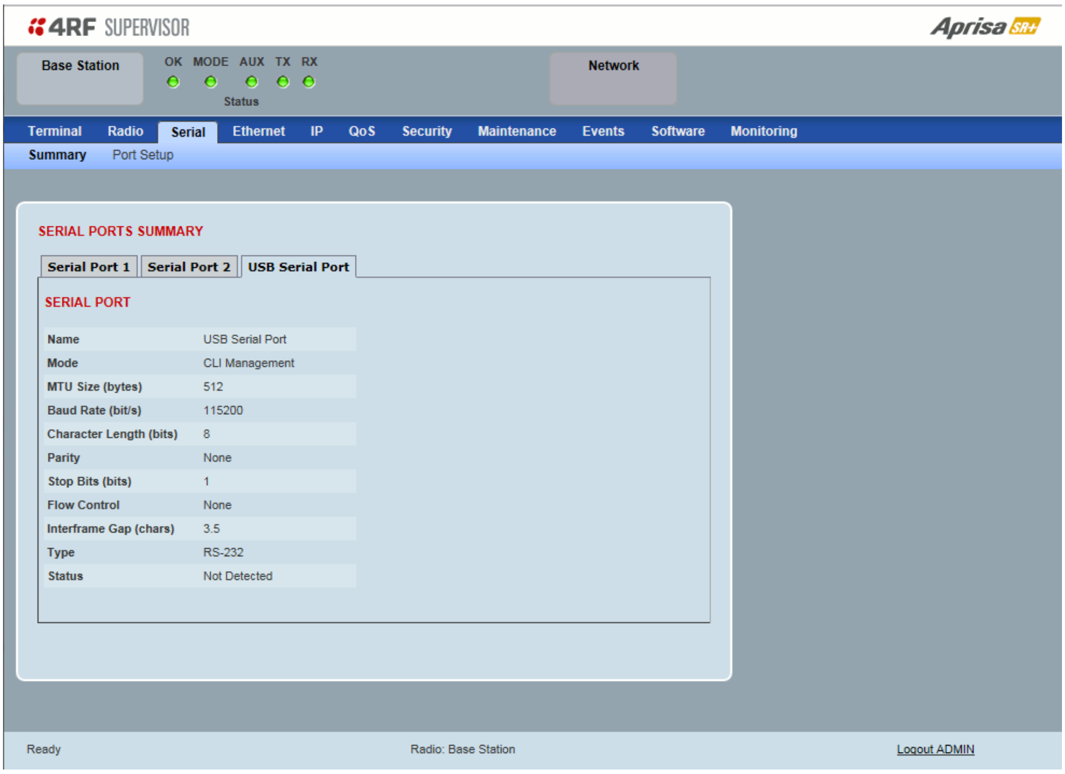
Note: This screen is dependent on the Data Port product option purchased (see 'Data Interface Ports' on page 312). The Data Port product option shown is a 2E2S – two Ethernet ports and two Serial ports



See 'Serial > Port Setup' on page 117 for configuration options.

USB Serial Ports

This page displays the current settings for the USB serial port parameters.



Type

This parameter displays the Serial Port interface type.

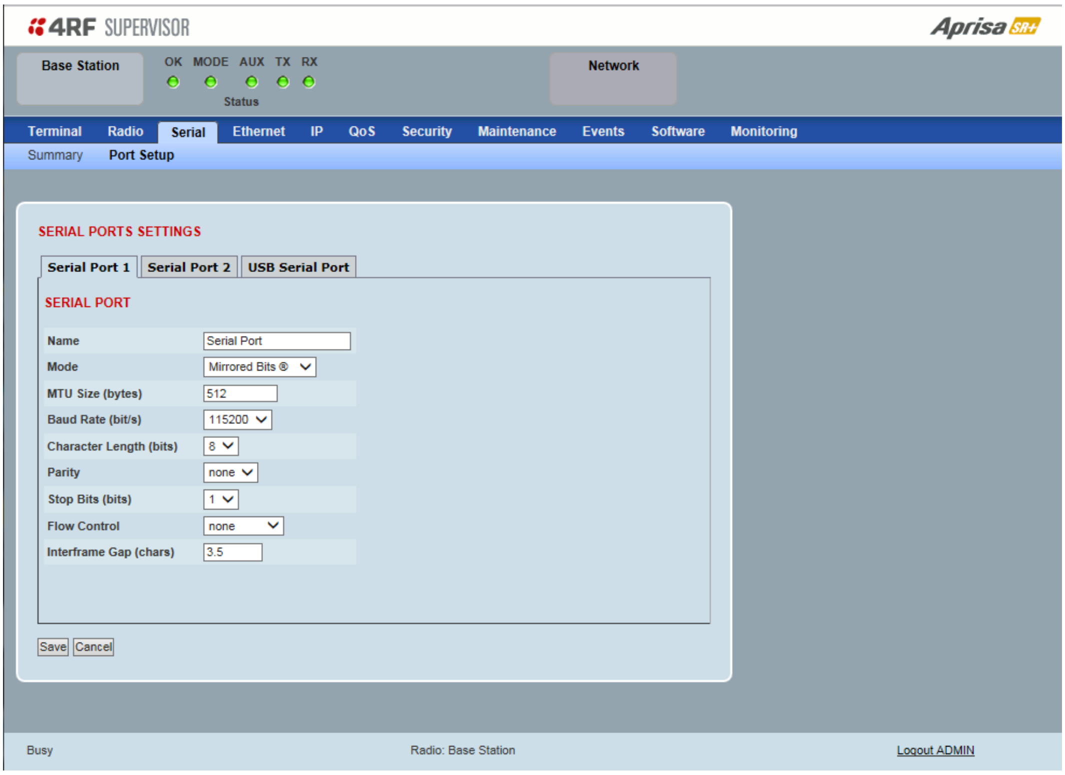
If the Name is USB Serial Port:

Option	Function
RS-232	Indicates that a USB to RS-232 serial converter is plugged into the radio.
RS-485	Indicates that a USB to RS-485 serial converter is plugged into the radio.

Serial > Port Setup

RS-232 Hardware Ports

This page provides the setup for the serial port settings.



SERIAL PORTS SETTINGS

Note: This screen is dependent on the Data Port product option purchased (see 'Data Interface Ports' on page 312). The Data Port product option shown is a 2E2S – two Ethernet ports and two Serial ports

Name

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

Option	Function
Serial Port	This is the normal RS-232 serial ports provided with the RJ45 connector.
USB Serial Port	This is the optional RS-232 / RS-485 serial port provided with the USB host port connector with a USB to RS-232 / RS-485 RJ45 converter cable (see 'USB RS-232 / RS-485 Serial Port' on page 336).

Mode

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

Option	Function
Disabled	The serial port is not required.
Standard	The serial port is communicating with serial ports on other stations.
Mirrored Bits ®	Mirrored Bits® is a serial communications protocol used to exchange internal logic status messages directly between relays and devices used in line protection, remote control and monitoring, relay remote tripping, sectionalizing and other such applications. The protocol is often described as a relay-to-relay communications technology.
Terminal Server	A base station Ethernet port can communicate with both Ethernet ports and serial ports on remote stations. RS-232 traffic is encapsulated in IP packets (see 'Serial > Port Setup' Terminal Server on page 121).
SLIP	IP packets are encapsulated over RS-232 interface port (see 'Serial > Port Setup' Serial Line Interface Protocol (SLIP)' on page 123).

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. 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 or 115200 bit/s. The default setting is 115200 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 Aprisa SR+ radio port (DCE) CTS is in a permanent ON (+ve) state. This does not go to OFF if the radio link fails.
CTS-RTS	CTS / RTS hardware flow control between the DTE and the Aprisa SR+ radio port (DCE) is enabled. If the Aprisa SR+ buffer is full, the CTS goes OFF. In the case of radio link failure the signal goes to OFF (-ve) state.

In terminal server mode, the serial packet is no different from an Ethernet packet and travels through various packet queues before being transmitted over the air. Thus, the serial flow control has no affect in terminal server mode.

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. The Inter-Frame Gap limits are 0 to 20 chars in steps of 0.1 char. The default setting is 3.5 chars.

Mirrored Bits®

4RF has introduced a channel access scheme optimized for Mirrored Bits® support between two devices. Error free transport of the protocol can be achieved through specific serial traffic configuration settings, which are dependent on the radio RF configuration, Mirrored Bits® devices and network characteristics.

The following are the recommended RF configurations and serial data configuration settings and to optimize the performance over Aprisa SR+ radios.

Recommended RF configurations are:

- Radio->Channel Setup->Serial Data Stream Mode to 'Segregate'
- Radio->Channel Setup->Access Scheme to Point To Point (Half Duplex)
- Radio->Channel Setup->Network Traffic Type to 'Serial Only'
- Radio > Radio Setup > Channel size – set to meet license requirements (the wider the better for performance)
- Radio > Radio Setup > Modulation – 64 QAM low

The IFG and the MTU are adjusted to optimize performance for different RF configurations, connected devices and traffic configurations. The following is an example of a 9600 baud, 64 QAM modulation and 12.5 kHz channel size connecting a SEL 2505 device:

Recommended serial data configurations are:

- Inter Frame Gap (IFG) set to 0.2

  The IFG is dependent on serial line bit rate only. The Mirrored Bits® protocol is essentially timed to a base clock, the slower the bit rate the longer the period to transmit a packet resulting in less time between packets.

  A low bit rate is ideal as it increase the time period before a ROK error will occur as this is dependent on serial packet transmission time

  The minimum bit rate currently proven to provide reliable communications is 9600 bit, with this rate an IFG of 0.2 is required to be used.

- Maximum Transmission Unit (MTU) set to 32 bytes

  Increasing the MTU allows some 'space in each packet for additional data from the second serial port or the Ethernet ports but it will impact latency for each packet. A point may be reached where the gaps between individual packets are too high and the Mirrored Bits® ROK or other alarms will assert.

  The MTU can be adjusted up or down in steps of 8 bytes. The target is to find the smallest MTU for reliable transport (running without alarms or ROK assertions).

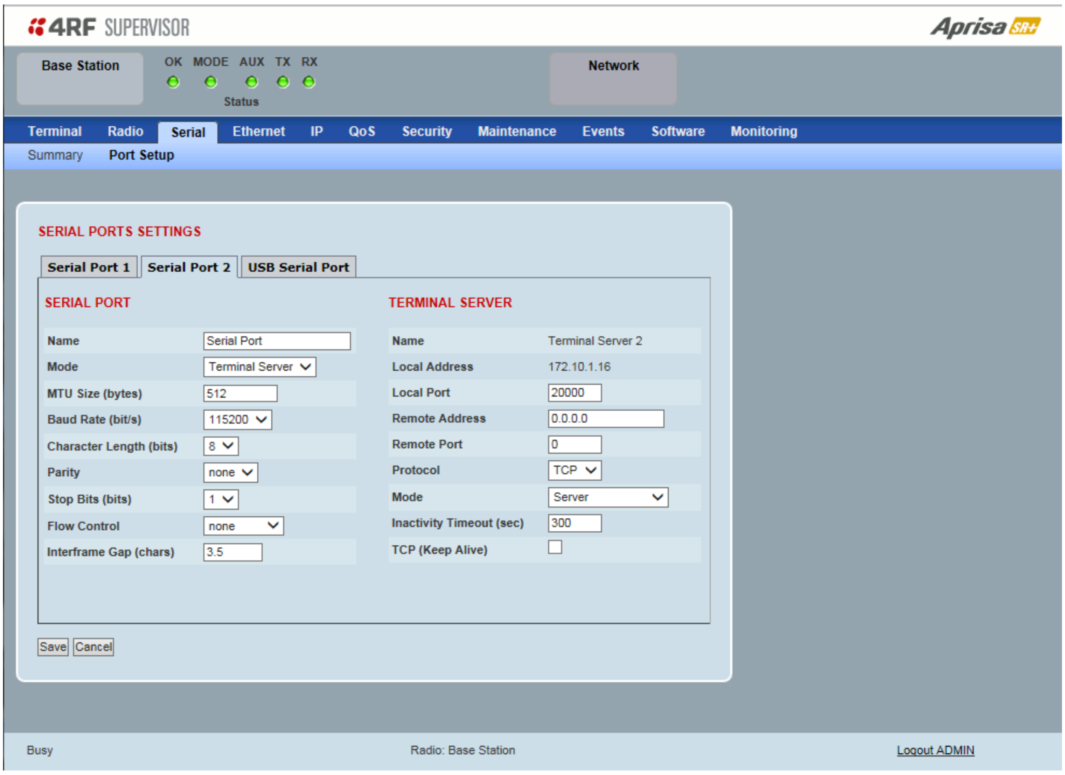
Refer to the application note 'AN 15-1 Optimization for MB communications.docx' for further setup configurations.

Terminal Server

This menu item is only applicable if the serial port has an operating mode of Terminal Server.

The Terminal Server operating mode provides encapsulation of serial data into an IP packet (over TCP or UDP).

A server connected to a base station Ethernet port can communicate with all remote station Ethernet ports and serial ports.



Local Address

This parameter displays the IP address of this radio.

Local Port

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

The valid port number range is greater than or equal to 1024 and less than or equal to 49151 but with exclusions of 0, 5445, 6445, 9930 or 9931. The default setting is 20000.

Remote Address

This parameter sets the IP address of the server connected to the base station Ethernet port.

Remote Port

This parameter sets the TCP or UDP port number of the server connected to the base station Ethernet port. The default setting is 0.

Protocol

This parameter sets the L4 TCP/IP or UDP/IP protocol used for terminal server operation. The default setting is TCP.

Mode

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

Option	Function
Client	The radio will attempt to establish a TCP connection with the specified remote unit. Generally, this setting is for the base station with an Ethernet connection to the SCADA master.
Server	The radio will listen for a TCP connection on the specified local port. Generally, this setting is for the remote station with a serial connection to the RTU. 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 radio will listen for a TCP connection on the specified local port and if necessary, establish a TCP connection with the specified remote unit. Generally, this setting is used for the remote station but it should be used carefully as two connections might be established with the base station. 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 radio will be notified if the TCP connection fails.

If the TCP keep alive is disabled, the radio 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.

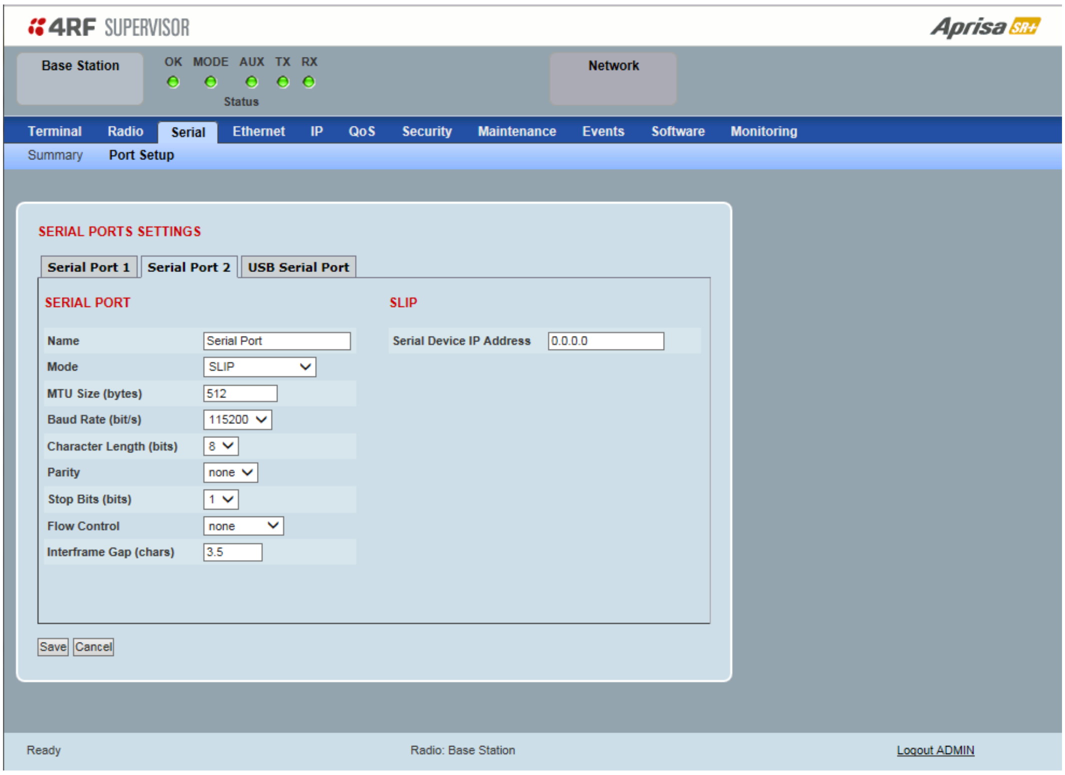
Serial Line Interface Protocol (SLIP)

This menu item is only applicable if the serial port has an operating mode of SLIP.

The SLIP operating mode provides IP packet encapsulation over RS-232 serial interface as per the SLIP protocol RFC 1055.

A SLIP serial interface contains the IP address of the serially connected RTU as per the RTU/PLC SLIP protocol. The SLIP interfaces on the remote radios can be part of the bridge network and can coexist and operate with a mix of Ethernet interfaces, serial SLIP and terminal server interfaces.

As the RTU/PLC serial SLIP interface doesn't supports MAC address, a remote or repeater radio SLIP interface uses a proxy ARP function that returns its own MAC address for ARP requests based on the IP address of the RTU/PLC SLIP interface.



Serial Device IP Address

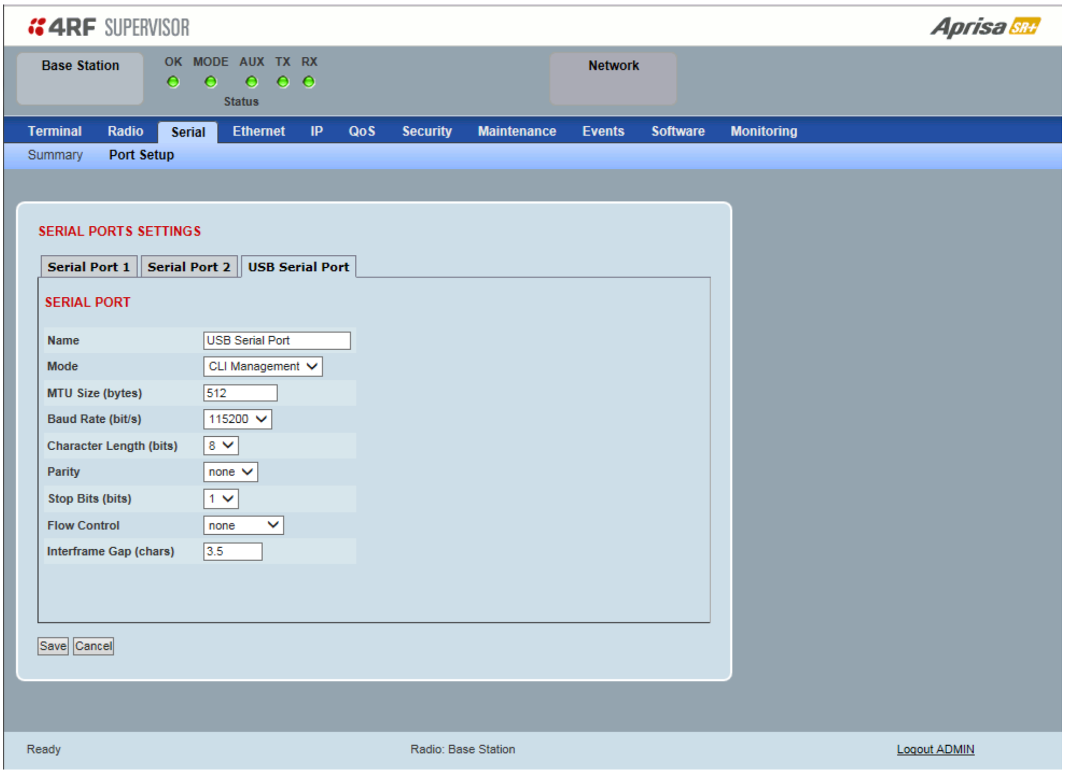
This parameter sets the IP address of the RTU connected on the configured serial port.

Baud Rate (bit/s)

This parameter sets the baud rate to 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200 bit/s. The default setting is 115200 bit/s. The minimum supported baud rate is 1200 bit/s as SLIP will not work on baud rates below 1200.

USB Serial Ports

This page provides the setup for the USB serial port settings.



SERIAL PORTS SETTINGS

Mode

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

Option	Function
Disabled	The serial port is not required.
Standard	The serial port is communicating with serial ports on other stations.
Terminal Server	A base station Ethernet port can communicate with both Ethernet ports and serial ports on remote stations. RS-232 traffic is encapsulated in IP packets (see 'Serial > Port Setup' Terminal Server on page 121).
CLI Management	The USB host port is used to access the radio Command Line Interface (CLI). A USB converter to RS-232 convertor will be required to connect to a PC.

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. 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 or 115200 bit/s. The default setting is 115200 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 Aprisa SR+ radio port (DCE) CTS is in a permanent ON (+ve) state. This does not go to OFF if the radio link fails.
CTS-RTS	CTS / RTS hardware flow control between the DTE and the Aprisa SR+ radio port (DCE) is enabled. If the Aprisa SR+ buffer is full, the CTS goes OFF. In the case of radio link failure the signal goes to OFF (-ve) state.

In terminal server mode, the serial packet is no different from an Ethernet packet and travels through various packet queues before being transmitted over the air. Thus, the serial flow control has no affect in terminal server mode.

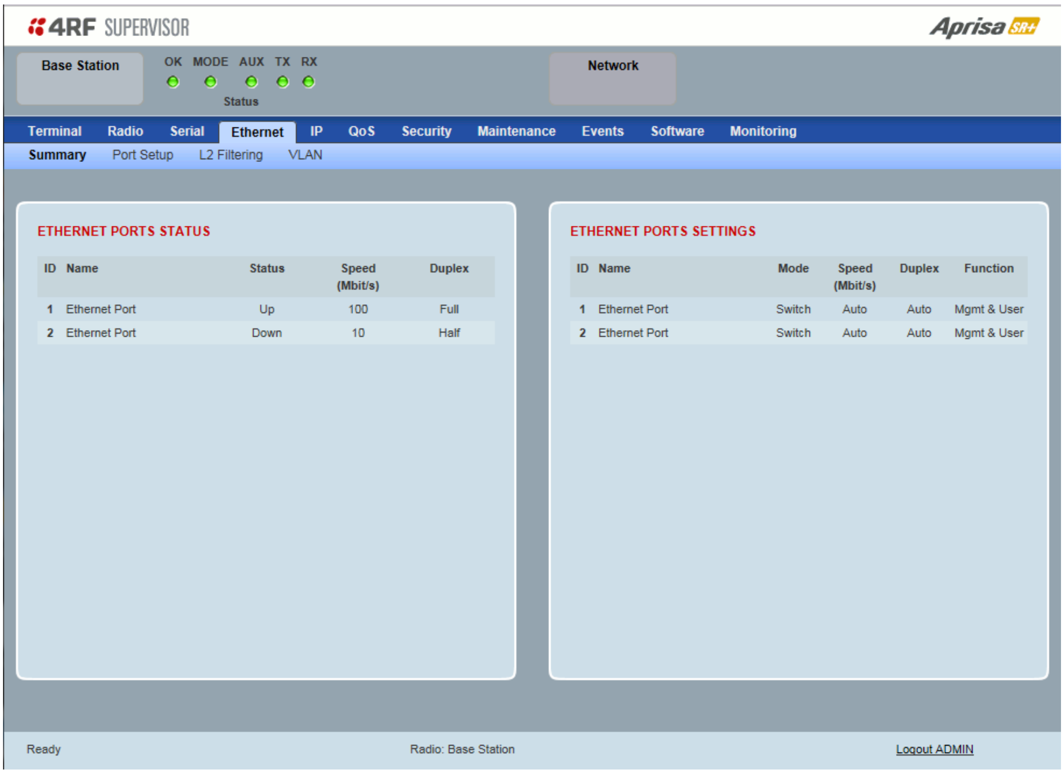
Inter-Frame Gap (chars)

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. The Inter-Frame Gap limits are 0 to 20 chars in steps of 0.1 char. The default setting is 3.5 chars.

Ethernet

Ethernet > Summary

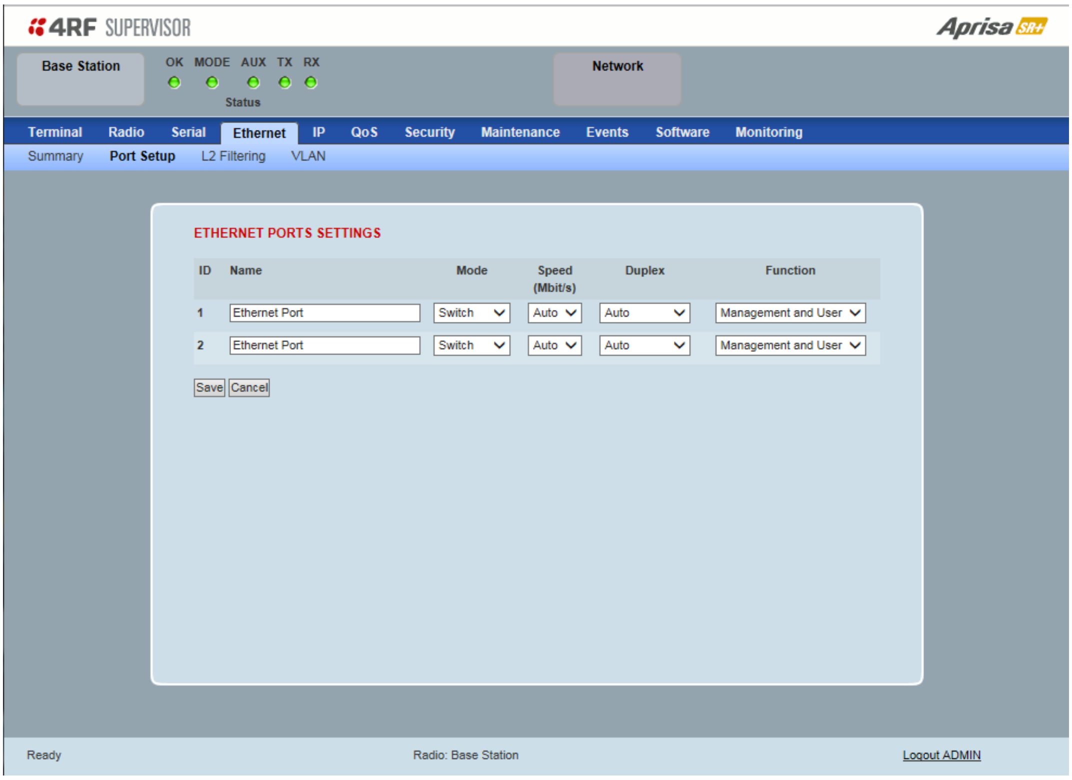
This page displays the current settings for the Ethernet port parameters and the status of the ports.



See ‘Ethernet > Port Setup’ for configuration options.

Ethernet > Port Setup

This page provides the setup for the Ethernet ports settings.



ETHERNET PORT SETTINGS

Note: This screen is dependent on the Data Port product option purchased (see 'Data Interface Ports' on page 312). The Data Port product option shown is a 2E2S – two Ethernet ports and two Serial ports

Mode

This parameter controls the Ethernet traffic flow. The default setting is Standard.

Option	Function
Standard	Enables Ethernet data communication over the radio link but Ethernet traffic is not switched locally between the two Ethernet ports.
Switch	Ethernet traffic is switched locally between the two Ethernet ports and communicated over the radio link
Disabled	Disables all Ethernet data communications.

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 Mbit/s
10	The Ethernet Port Speed is manually set to 10 Mbit/s
100	The Ethernet Port Speed is manually set to 100 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.
Half Duplex	The Ethernet Port is manually set to Half Duplex.
Full Duplex	The Ethernet Port is manually set to Full Duplex.

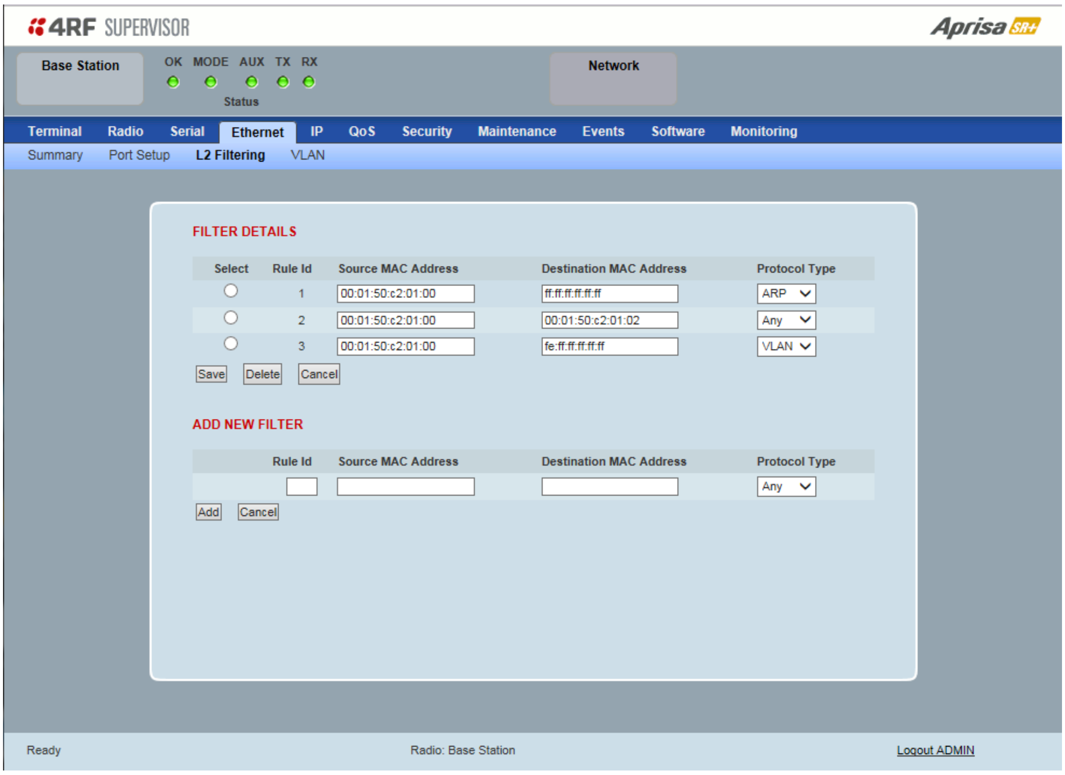
Function

This parameter controls the use for the Ethernet port. The default setting is Management and User.

Option	Function
Management Only	The Ethernet port is only used for management of the network.
Management and User	The Ethernet port is used for management of the network and User traffic over the radio link.
User Only	The Ethernet port is only used for User traffic over the radio link.

Ethernet > L2 Filtering

This page is only available if the Ethernet traffic option has been licensed (see ‘Maintenance > Licence’ on page 201).



FILTER DETAILS

L2 Filtering provides the ability to filter (white list) radio link user traffic based on specified Layer 2 MAC addresses.

User traffic originating from specified Source MAC Addresses destined for specified Destination MAC Addresses that meets the protocol type criteria will be transmitted over the radio link.

User traffic that does not meet the filtering criteria will not be transmitted over the radio link.

Management traffic to the radio will never be blocked.

Source MAC Address

This parameter sets the filter to the Source MAC address of the packet in the format ‘hh:hh:hh:hh:hh:hh’.

If the Source MAC Address is set to ‘FF:FF:FF:FF:FF:FF’, traffic will be accepted from any source MAC address.

Destination MAC Address

This parameter sets the filter to the Destination MAC address of the packet in the format ‘hh:hh:hh:hh:hh:hh’.

If the Destination MAC Address is set to ‘FF:FF:FF:FF:FF:FF’, traffic will be delivered to any destination MAC address.

Protocol Type

This parameter sets the EtherType accepted ARP, VLAN, IPv4, IPv6 or Any type.

Example:

In the screen shot, the rules are configured in the base station which controls the Ethernet traffic to the radio link.

Traffic from an external device with the Source MAC address 00:01:50:c2:01:00 is forwarded over the radio link if it meets the criteria. All other traffic will be blocked.

- Rule 1 If the Protocol Type is ARP going to any destination MAC address or
- Rule 2 If the Protocol Type is Any and the destination MAC address is 01:00:50:c2:01:02 or
- Rule 3 If the Protocol Type is VLAN tagged packets going to any unicast destination MAC address.

Special L2 Filtering Rules:

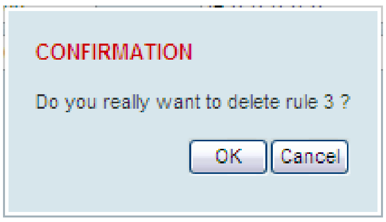
Unicast Only Traffic

This L2 filtering allows for Unicast only traffic and drop broadcast and multicast traffic. This filtering is achieved by adding the two rules:

Rule	Source MAC Address	Destination MAC Address	Protocol Type
Allow ARPS	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	ARP
Allow Unicasts from Any source	FF:FF:FF:FF:FF:FF	**FE**:FF:FF:FF:FF:FF	Any

To delete a L2 Filter:

1. Click on an existing rule 'Select'.
2. Click on Delete.



3. Click on OK.

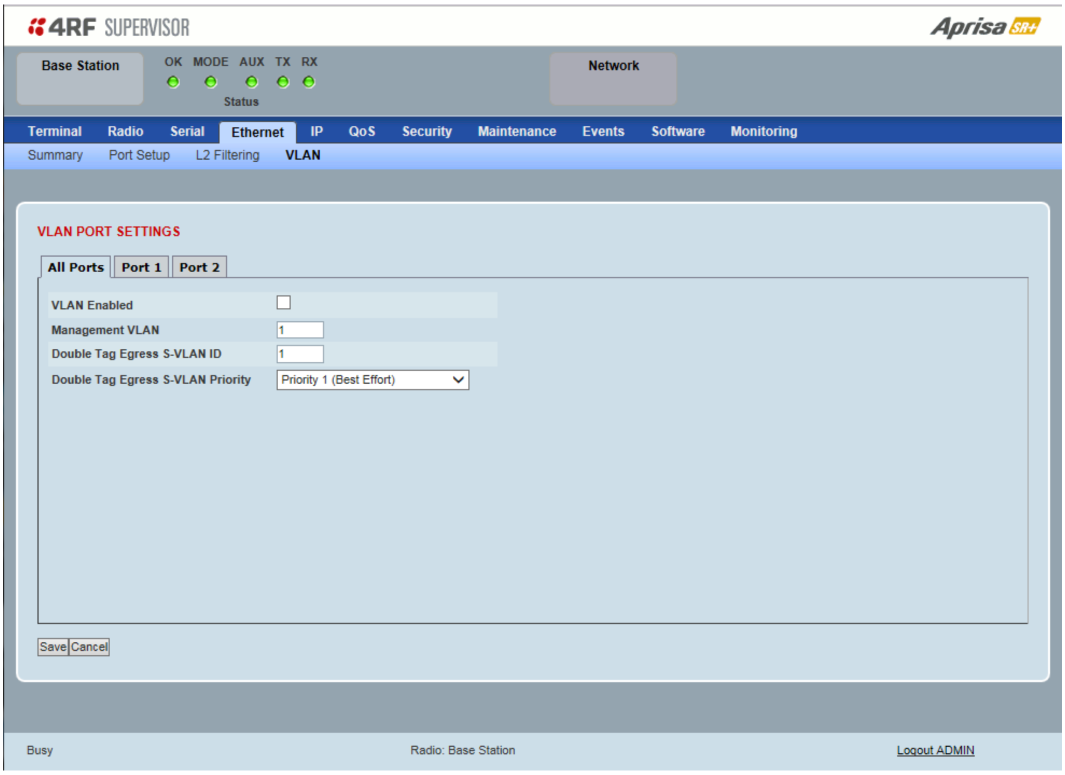
ADD NEW FILTER

To add a L2 Filter:

1. Enter the Rule ID number. This is a unique rule number between 1 and 25.
2. Enter the Source MAC address of the packet or 'FF:FF:FF:FF:FF:FF' to accept traffic from any MAC address.
3. Enter the Destination MAC address of the packet or 'FF:FF:FF:FF:FF:FF' to deliver traffic to any MAC address.
4. Select the Protocol Type to ARP, VLAN, IPv4, IPv6 or Any type.
5. Click on Add.

Ethernet > VLAN

This page is only available if the Ethernet traffic option has been licensed (see ‘Maintenance > Licence’ on page 201).



VLAN PORT SETTINGS – All Ports

This page specifies the parameters that relate to all Ethernet ports when working in Bridge Mode. Three parameters are global parameters for the Ethernet Bridge; enable / disable VLANs, Management VLAN ID and the Double VLAN ID(S-VLAN) and the priority bit. These parameters can't be defined per port and are globally defined for the Ethernet Bridge.

VLAN Enabled

This parameter sets if VLAN operation is required on the network. If it is enabled on the base station, it must also be enabled on the remote / repeater stations. The default is disabled.

Management VLAN

This parameter sets the VLAN ID for management traffic only. The value can be between 1 and 4094. The default is 1.

Double Tag Egress S-VLAN ID

This parameter sets the S-VLAN ID (outer tag) in the egress direction. The value can be between 1 and 4094. The default is 1.

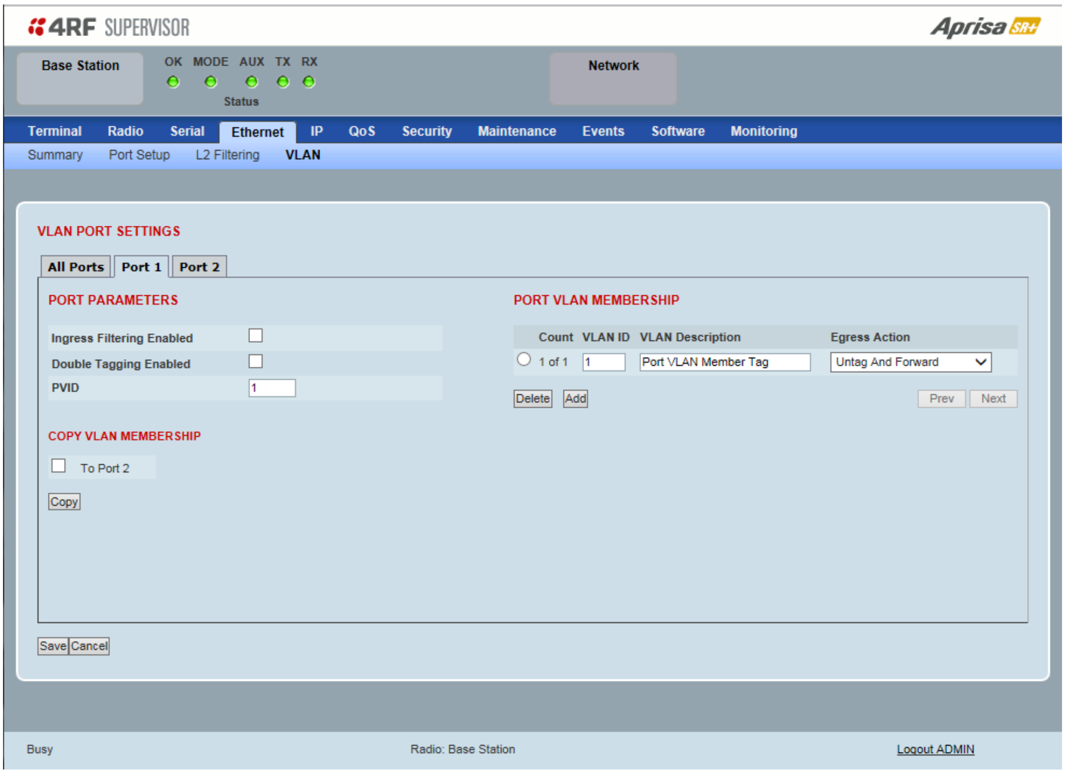
Double Tag Egress S-VLAN Priority

This parameter sets the S-VLAN egress traffic priority. The default is Priority 1 (Best Effort).

Option	Egress Priority Classification	High / Low Priority
Priority 0 Background	0	Lowest Priority
Priority 1 (Best Effort)	1	
Priority 2 (Excellent Effort)	2	
Priority 3 (Critical Applications)	3	
Priority 4 (Video)	4	
Priority 5 (Voice)	5	
Priority 6 (Internetwork Control)	6	
Priority 7 (Network Control)	7	Highest Priority

VLAN PORT SETTINGS – Port 1

This example is shown for the product option of 2E2S i.e. two Ethernet ports.



PORT PARAMETERS

Ingress Filtering Enabled

This parameter enables ingress filtering. When enabled, if ingress VLAN ID is not included in its member set (inner tagged), the frame will be discarded.

If the Ingress Filtering is disabled, the Aprisa SR+ supports ‘Admit All Frames’ so that all frames tagged, untagged and priority-tagged-frames are allowed to pass through the Ethernet ports. The default is disabled.

Double Tagging Enabled

This parameter enables double tagging on this specific port. When enabled, if the ingress traffic is double tagged, the Aprisa SR+ will check and validate that the S-VLAN ID matches the S-VLAN defined in 'Double Tag Egress S-VLAN ID' in the 'all ports' tab. If there is a match, the packet will be forwarded into the Bridge and the S-VLAN outer tag will be removed, thus the radio network will only forward a single VLAN. If there isn’t a matching S-VLAN, the packet will be discarded. On egress, the outer tag (S-VLAN) is appended with the 'Double Tag Egress S-VLAN ID' defined in the 'all ports' tab (see page 131). The default is disabled.

If double tagging is enabled on the port, incoming frames should always be double tagged.

- If the incoming frame is untagged, then the PVID (port VLAN ID) is used and forwarded with the Port Ingress priority provided the PVID is configured in the Port VLAN Membership of any of the Ethernet ports. If not, the frames are dropped.
- If the incoming frame is single tagged, then PVID is used and forwarded with the Port Ingress priority provided the PVID is configured in the Port VLAN Membership of any of the Ethernet ports. If not the frames are dropped.

If double tagging is disabled on the port, incoming frames should always be single tagged, untagged or priority-tagged frames.

Double tagged frames are simply forwarded treating them as if they were single tagged frames. At the egress of the Ethernet port, such frames are forwarded only if the S-VLAN ID of that frame is a member of the Port VLAN Membership.

PVID (Port VLAN ID)

This parameter sets the frame VLAN ID when the ingress frame is untagged (e.g. when in 'port VLAN membership' the 'egress action' is set to 'untagged and forward') or priority-tagged (VLAN=0). The value can be between 1 and 4094. The default is 1.

Note: The Port VLAN Membership must contain the PVID. If the Port VLAN Membership does not contain the PVID, untagged or priority-tagged frames will be discarded.

COPY VLAN MEMBERSHIP

To Port

This parameter when set copies the port VLAN Membership settings to the other ports.

PORT VLAN MEMBERSHIP

VLAN ID

This parameter sets the VLAN ID of the port for a maximum 64 active VLANs. The value can be between 1 and 4094. The default is 1.

VLAN Description

This parameter is a freeform field used to identify the VLAN. It can be up to a maximum of 32 characters.

Egress Action

This parameter sets the action taken on the frame on egress from the Ethernet port. The default is Untag and forward.

Option	Function
Untag and forward	Removes the tagged information and forwards the frame. On Ingress, the VLAN tag will be added to the PVID tag.
Forward	Forwards the tagged frame as it is on egress. On Ingress, traffic is expected to include the VLAN tag with a member VLAN ID, otherwise the packet will be dropped.

Controls

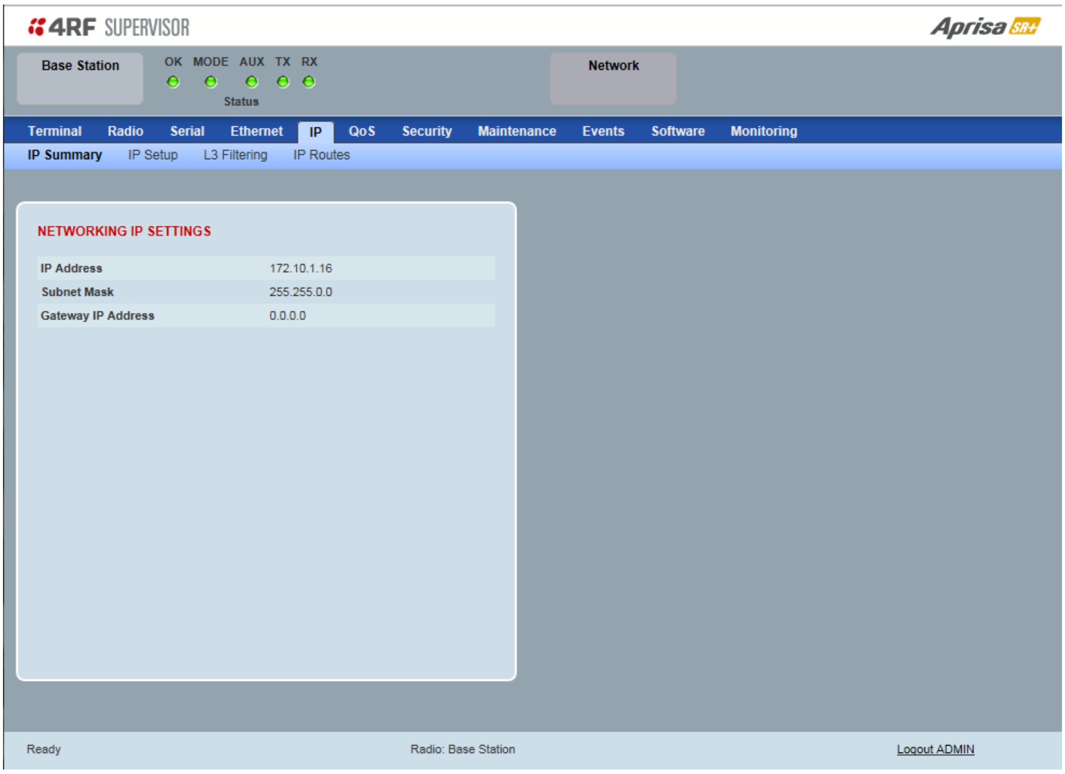
The Add button adds the selected entry.

The Delete button deletes the selected entry.

IP

IP > IP Summary > Bridge / Gateway Router Modes

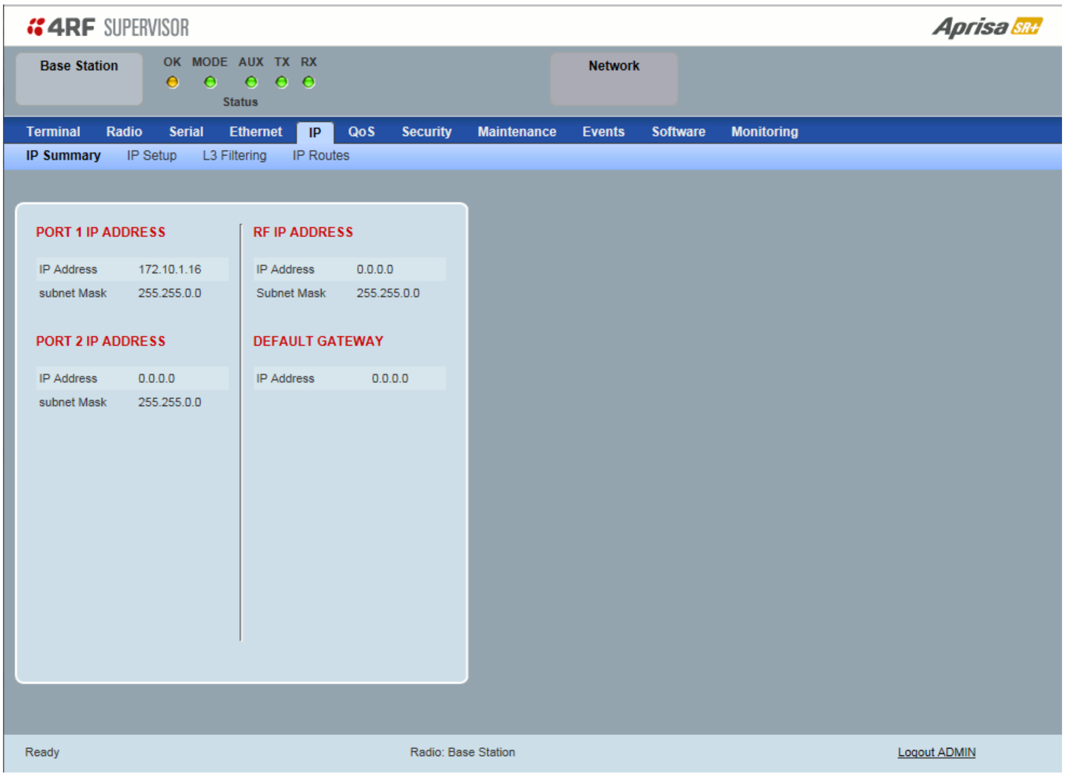
This page displays the current settings for the Networking IP Settings for an Ethernet Operating Mode of ‘Bridge’ or ‘Gateway Router’.



See ‘IP > IP Setup > Bridge / Gateway Router Modes’ on page 138 for configuration options.

IP > IP Summary > Router Mode

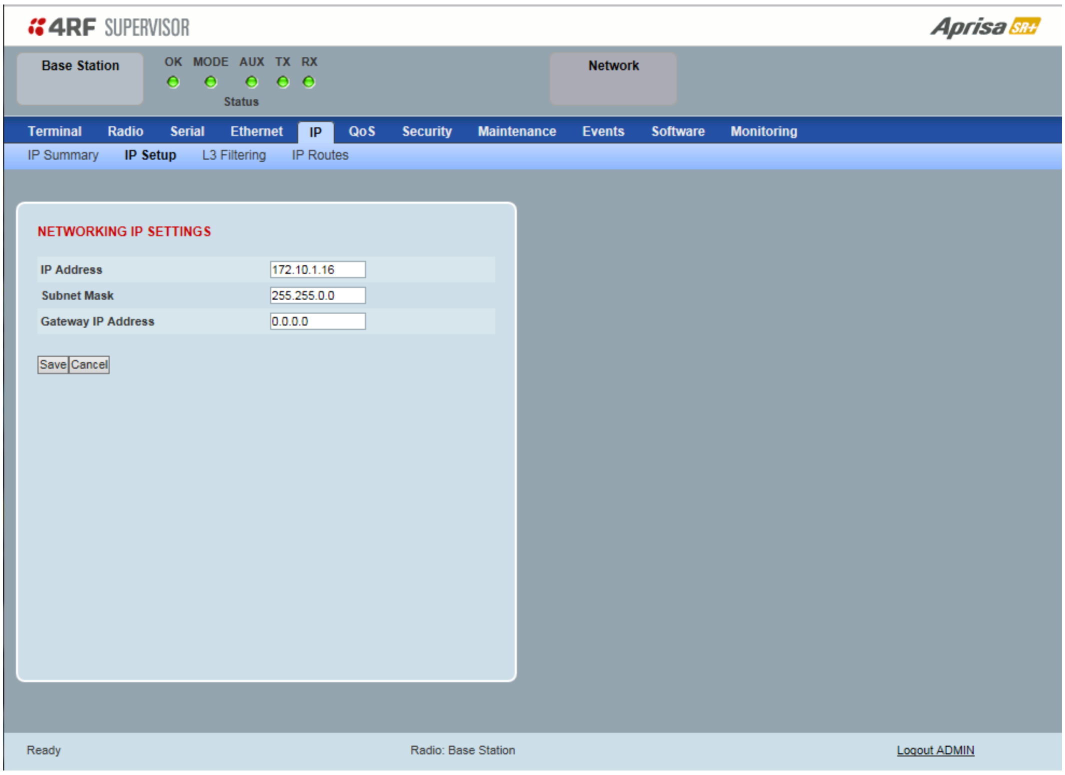
This page displays the current settings for the Networking IP Settings for an Ethernet Operating Mode of ‘Router’.



See ‘IP > IP Setup > Router Mode’ on page 139 for configuration options.

IP > IP Setup > Bridge / Gateway Router Modes

This page provides the setup for the IP Settings for an Ethernet Operating Mode of 'Bridge' or 'Gateway Router'.



NETWORKING IP SETTINGS

IP Address

Set the static IP Address of the radio (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 in the range 169.254.50.10.

Subnet Mask

Set the Subnet Mask of the radio (Management and Ethernet ports) using the standard format xxx.xxx.xxx.xxx. The default subnet mask is 255.255.0.0 (/16).

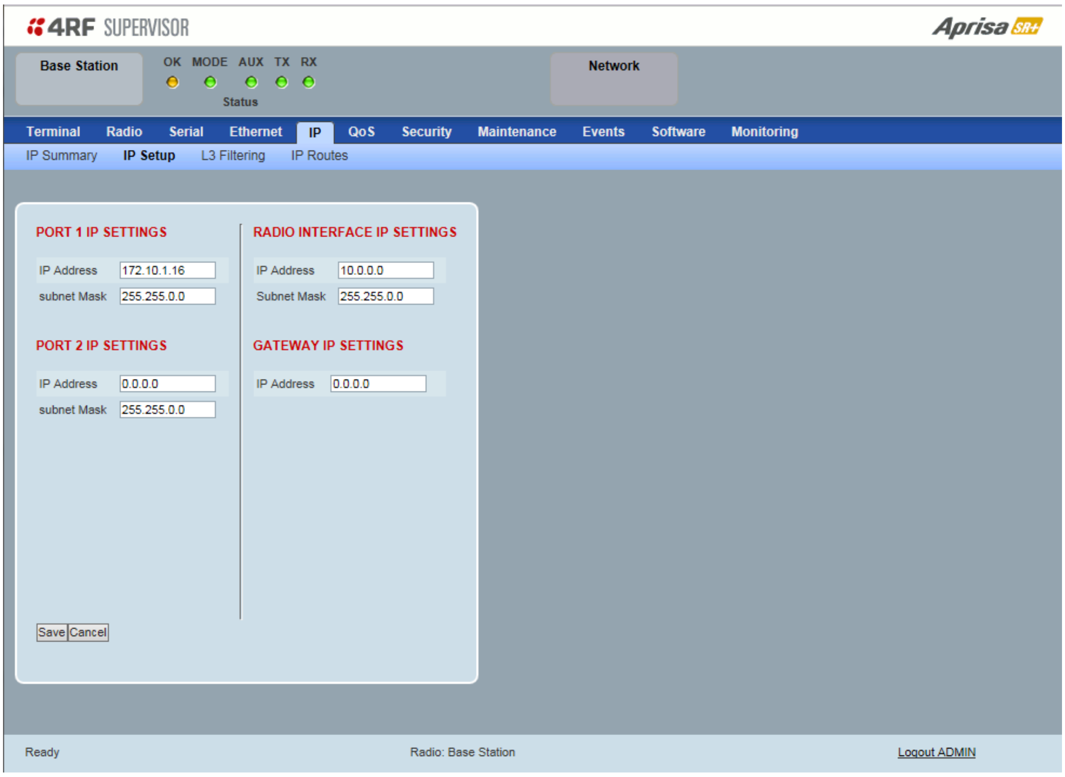
Gateway

Set the Gateway address of the radio, 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 base station. The default gateway commonly connects the internal radio network and the outside network. The default Gateway is 0.0.0.0.

IP > IP Setup > Router Mode

This page provides the setup for the IP Settings for and Ethernet Operating Mode of 'Router'.



PORT SETTINGS – port (n)

Note: This screen is dependent on the Data Port product option purchased (see 'Data Interface Ports' on page 312). The Data Port product option shown is a 2E2S – two Ethernet ports and two Serial ports

IP Address

Set the static IP Address of the radio Ethernet port (n) assigned by your site network administrator using the standard format xxx.xxx.xxx.xxx. This IP address is used for this Ethernet port Router mode.

Subnet Mask

Set the Subnet Mask of the of the radio Ethernet port (n) using the standard format xxx.xxx.xxx.xxx. The default subnet mask is 255.255.0.0 (/16).

Gateway

Set the Gateway address of the radio Ethernet port (n), 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 base station. The default gateway commonly connects the internal radio network and the outside network. The default Gateway is 0.0.0.0.

RADIO INTERFACE IP SETTINGS

The RF interface IP address is the address that traffic is routed to for transport over the radio link. This IP address is only used when Router Mode is selected i.e. not used in Bridge Mode.

Radio Interface IP Address

Set the IP Address of the RF interface using the standard format xxx.xxx.xxx.xxx. The default IP address is in the range 10.0.0.0.

Radio Interface Subnet Mask

Set the Subnet Mask of the RF interface using the standard format xxx.xxx.xxx.xxx. The default subnet mask is 255.255.0.0 (/16).

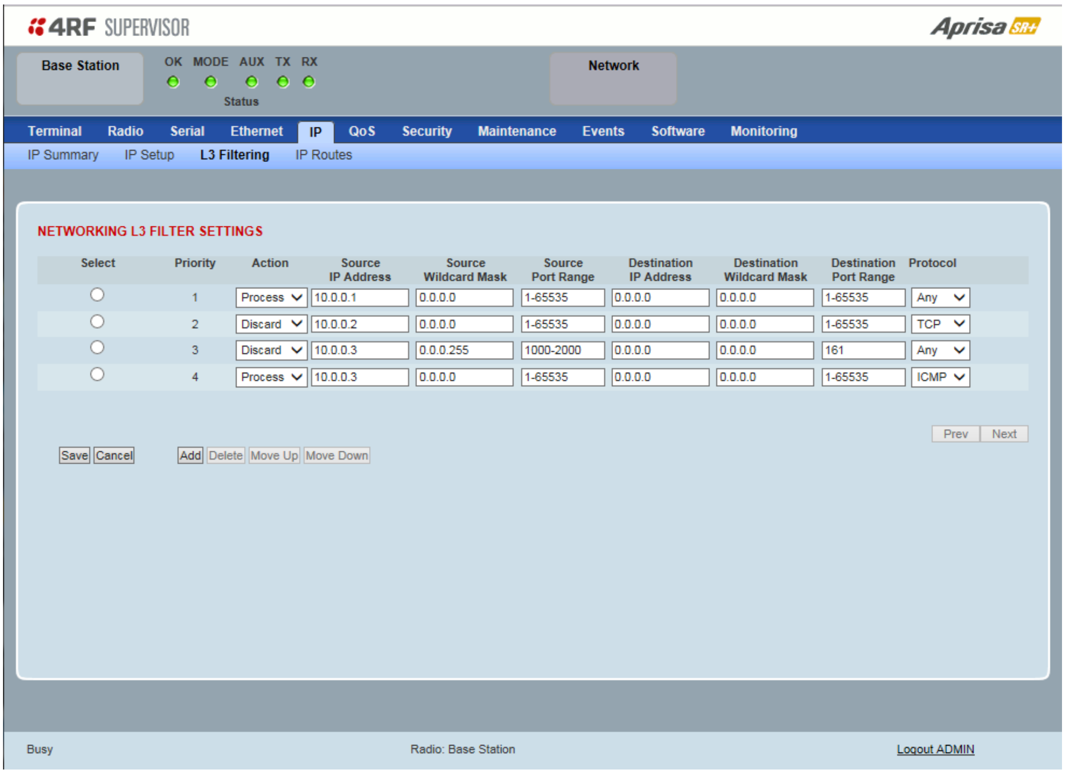
Note 1: If the base station RF interface IP address is a network IP address, and if the remote radio is also using a network IP address within the same subnet or different subnet, then the base radio will assign an automatic RF interface IP address from its own subnet.

When the base radio has a host specific RF interface IP address, then all the remotes must have a host specific RF interface IP address from the same subnet.

Note 2: When a remote radio is configured for Router Mode and the base radio is changed from Bridge Mode to Router Mode and the RF interface IP address is set to AUTO IP configuration (at least the last octet of the RF interface IP address is zero), it is mandatory to configure the network topology by using the 'Decommission Node' and 'Discover Nodes' (see 'Maintenance > Advanced' on page 202).

IP > L3 Filtering

This page is only available if the Ethernet traffic option has been licensed (see 'Maintenance > Licence' on page 201) and Router Mode selected. It is not active in Bridge Mode (see 'Terminal > Operating Mode' on page 91).



NETWORKING L3 FILTER SETTINGS

L3 Filtering provides the ability to evaluate traffic and take specific action based on the filter criteria.

This filtering can also be used for L4 TCP / UDP port filtering which in most cases relates to specific applications as per IANA official and unofficial well-known ports.

Entering a * into any to field will automatically enter the wildcard values when the data is saved.

Priority

This parameter shows the priority order in which the filters are processed.

Action

This parameter defines the action taken on the packet when it meets the filter criteria.

Option	Function
Process	Processes the packet if it meets the filter criteria
Discard	Discards the packet if it meets the filter criteria

Source IP Address

If the source IP address is set to 0.0.0.0, any source IP address will meet the filter criteria.

Source Wildcard Mask

This parameter defines the mask applied to the source IP address. 0 means that it must be a match.

If the source wildcard mask is set to 0.0.0.0, the complete source IP address will be evaluated for the filter criteria.

If the source wildcard mask is set to 0.0.255.255, the first 2 octets of the source IP address will be evaluated for the filter criteria.

If the source wildcard mask is set to 255.255.255.255, none of the source IP address will be evaluated for the filter criteria.

Note: The source wildcard mask operation is the inverse of subnet mask operation

Source Port Range

This parameter defines the port or port range for the source. To specify a range, insert a dash between the ports e.g. 1000-2000. If the source port range is set to 1-65535, traffic from any source port will meet the filter criteria.

Destination IP Address

This parameter defines the destination IP address of the filter. If the destination IP address is set to 0.0.0.0, any destination IP address will meet the filter criteria.

Destination Wildcard Mask

This parameter defines the mask applied to the destination IP address. 0 means that it must be a match.

If the destination wildcard mask is set to 0.0.0.0, the complete destination IP address will be evaluated for the filter criteria.

If the destination wildcard mask is set to 0.0.255.255, the first 2 octets of the destination IP address will be evaluated for the filter criteria.

If the destination wildcard mask is set to 255.255.255.255, none of the destination IP address will be evaluated for the filter criteria.

Note: The destination wildcard mask operation is the inverse of subnet mask operation

Destination Port Range

This parameter defines the port or port range for the destination. To specify a range, insert a dash between the ports e.g. 1000-2000. If the destination port range is set to 1-65535, traffic to any destination port will meet the filter criteria.

Protocol

This parameter defines the Ethernet packet type that will meet the filter criteria.

Controls

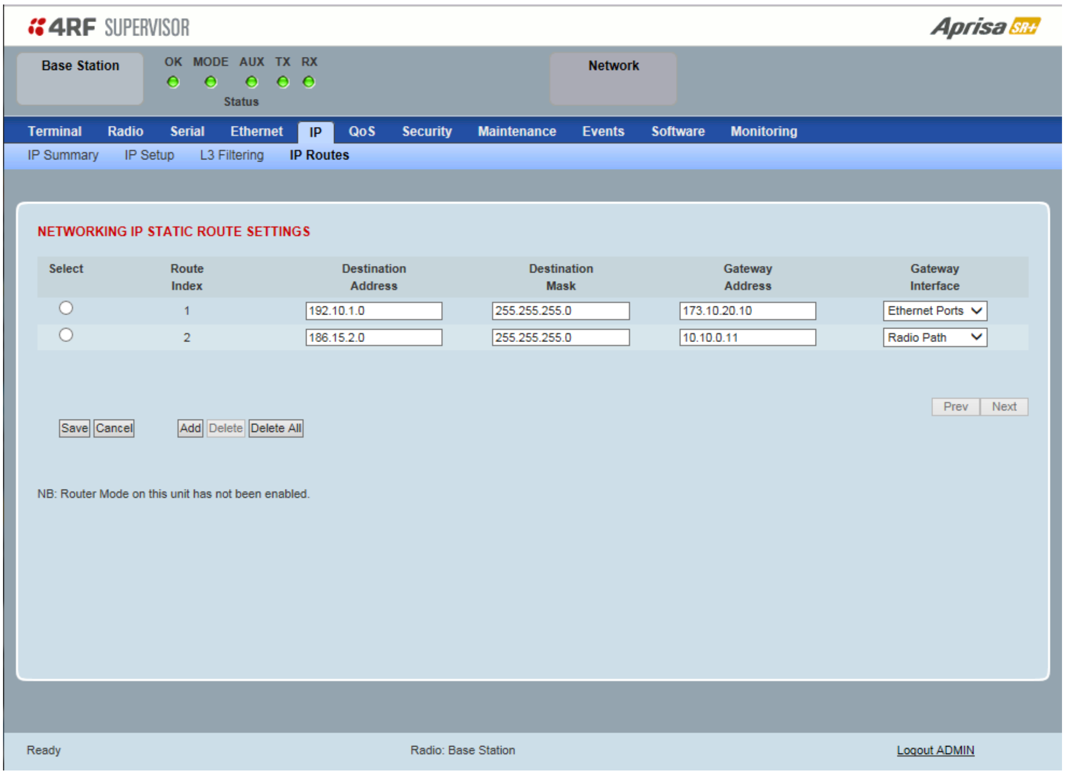
The Delete button deletes the selected entry.

The Move Up button moves the selected entry above the entry above it increasing its process priority.

The Move Down button moves the selected entry below the entry above it reducing its process priority.

IP > IP Routes

This page is only available if the Ethernet traffic option has been licensed (see ‘Maintenance > Licence’ on page 201) and Router Mode selected. It is not valid for Bridge Mode (see 'Terminal > Operating Mode’ on page 91).



NETWORKING IP STATIC ROUTE SETTINGS

Static routing provides the ability to evaluate traffic to determine if packets are forwarded over the radio link or discarded based on the route criteria.

Route Index

This parameter shows the route index.

Destination Address

This parameter defines the destination IP address of the route criteria.

Destination Mask

This parameter defines the subnet mask applied to the Destination IP Address. 255 means that it must be a match.

If the destination subnet mask is set to 255.255.255.255, all octets of the Destination IP Address will be evaluated for the route criteria.

If the destination subnet mask is set to 255.255. 0.0, the first 2 octets of the Destination IP Address will be evaluated for the route criteria.

Gateway Address

This parameter sets the gateway address where packets will be forwarded to.

- If the gateway interface is set to Ethernet Ports, the gateway address is the IP address of the device connected to the Ethernet port.
- If the gateway interface is set to Radio Path, the gateway address is the IP address of the remote radio.

Gateway Interface

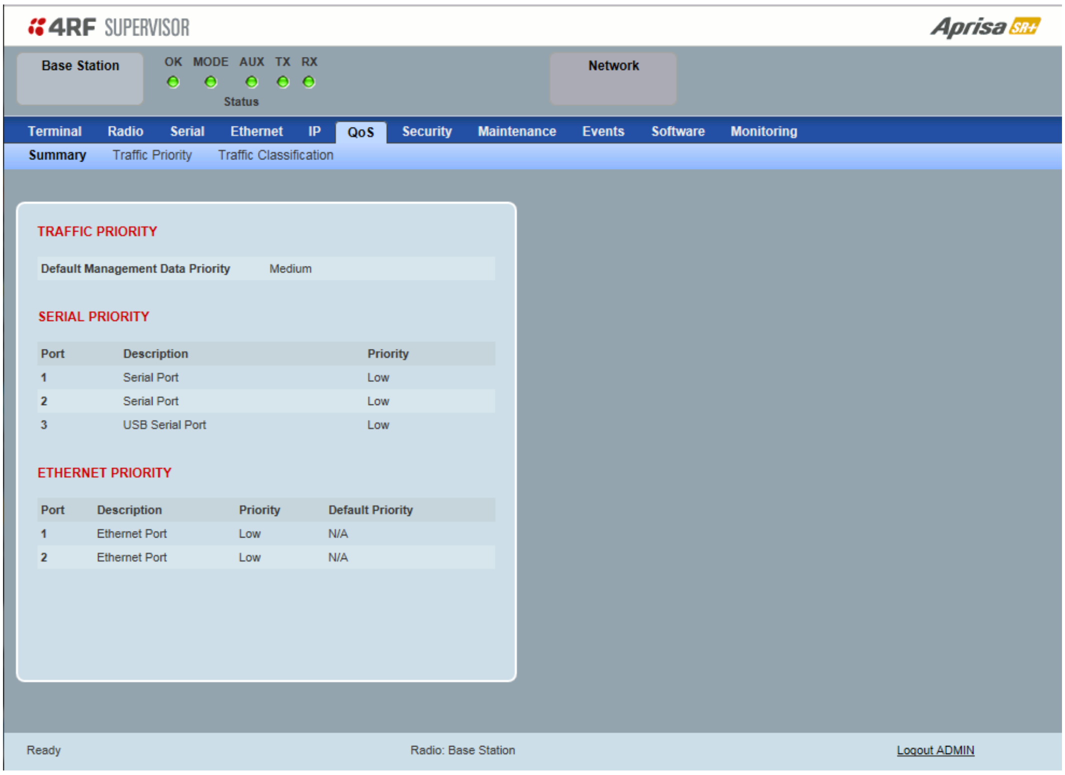
This parameter sets the destination interface.

Option	Function
Ethernet Ports	Packets are forwarded to the Ethernet interface port.
Radio Path	Packets are forwarded to the RF Interface radio path.

QoS

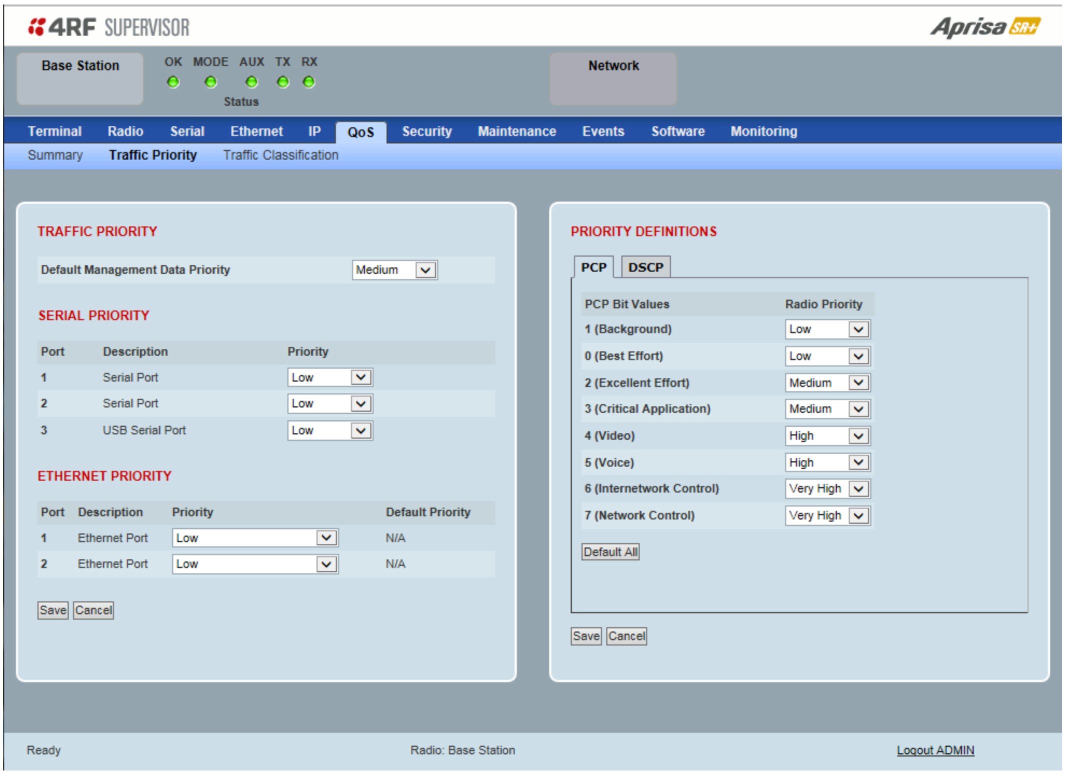
QoS > Summary

This page provides a summary of the QoS Settings.



See ‘QoS > Traffic Priority’ and ‘QoS > Traffic Classification’ for configuration options.

QoS > Traffic Priority



TRAFFIC PRIORITY

Default Management Data Priority

The Default Management Data Priority controls the priority of the Ethernet management traffic relative to Ethernet customer traffic. It can be set to Very High, High, Medium and Low. The default setting is Medium.

SERIAL PRIORITY

This parameter controls the per port priority of the serial customer traffic relative to the Ethernet customer traffic. If equal priority is required to Ethernet traffic, this setting must be the same as the Ethernet Data Priority setting.

The serial data priority can be set to Very High, High, Medium and Low. The default setting is Low.

A queuing system is used to prioritize traffic from the serial and Ethernet interfaces for over the air transmission. A weighting may be given to each data type and this is used to schedule the next transmission over the air e.g. if there are pending data packets in multiple buffers but serial data has a higher weighting it will be transmitted first. The serial buffer is 20 serial packets (1 packet can be up to 512 bytes).

There are four priority queues in the Aprisa SR: Very High, High, Medium and Low. Data is added to one of these queues depending on the priority setting. Data leaves the queues from highest priority to lowest: the Very High queue is emptied first, followed by High then Medium and finally Low.

ETHERNET PRIORITY

This parameter controls the per port priority of the Ethernet customer traffic relative to the serial customer traffic. If equal priority is required to serial traffic, this setting must be the same as the Serial Data Priority setting.

The Ethernet Priority enables users to set the priority of Ethernet port ingress frames. The priority for each port can be:

1. From PCP priority bits (VLAN priority) in VLAN tagged frames or priority tag (VLAN 0) frames
2. From DSCP priority bits in an IP packet (DSCP in IPv4 TOS field)
3. All frames are set to 'very high' priority
4. All frames are set to 'high' priority
5. All frames are set to 'medium' priority
6. All frames are set to 'low' priority

The default setting is Low.

A queuing system is used to prioritize customer traffic from the serial and Ethernet interfaces for over the air transmission. A weighting may be given to each data type and this is used to schedule the next transmission over the air e.g. if there are pending data packets in multiple buffers but serial data has a higher weighting it will be transmitted first. The Ethernet buffer is 10 Ethernet packets (1 packet can be up to Ethernet MTU, 1536 bytes).

There are four priority queues in the Aprisa SR+: Very High, High, Medium and Low. Data is added to one of these queues depending on the priority setting. Data leaves the queues from highest priority to lowest: the Very High queue is emptied first, followed by High then Medium and finally Low.

Default Priority

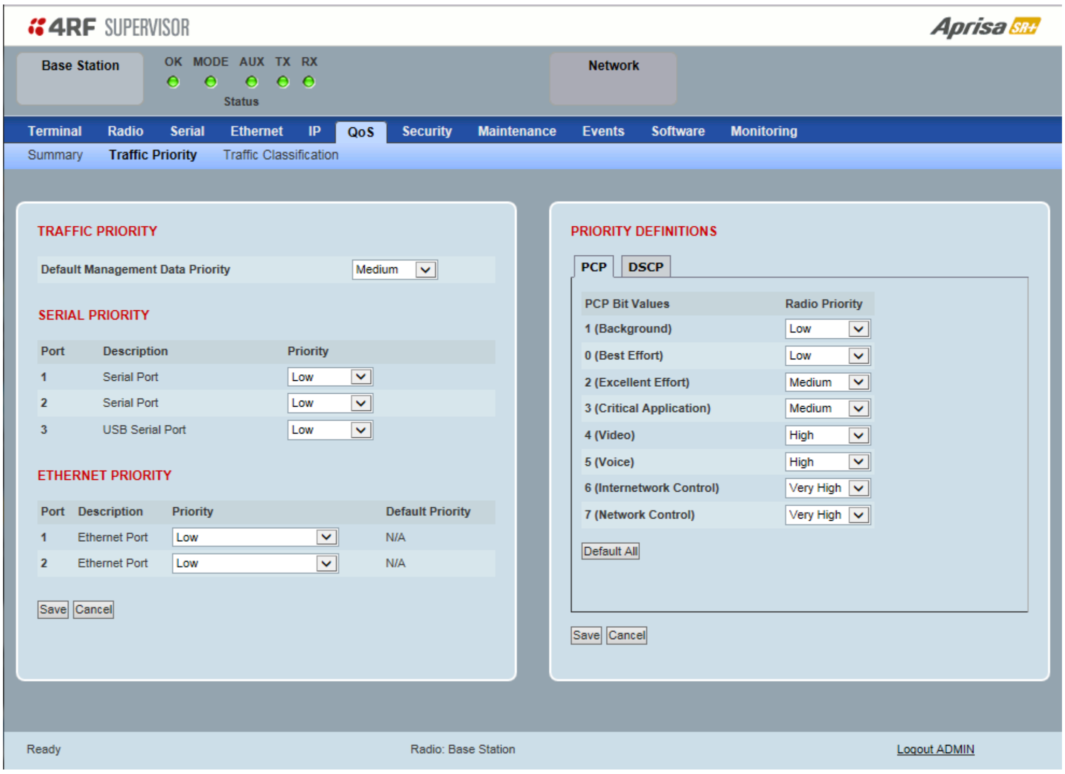
When the priority of an Ethernet port uses the PCP bits (VLAN priority) values the 'Default Priority' option is enabled, allowing the priority of untagged VLAN frames to be set.

When the priority of an Ethernet port uses the DSCP priority (in IPv4 TOS field) values the 'Default Priority' option is enabled, allowing the priority of ARP frames to be set.

PRIORITY DEFINITIONS

PCP (Priority Code Point)

These settings provide priority translation / mapping between the external radio LAN VLAN priority network and the radio internal VLAN priority network, using the VLAN tagged PCP (Priority Code Point) priority field in the Ethernet/VLAN frame.



The IEEE 802.1Q specification defines a standards-based mechanism for providing VLAN tagging and class of service (CoS) across Ethernet networks. This is accomplished through an additional VLAN tag, which carries VLAN tag ID and frame prioritization information (PCP field), inserted within the header of a Layer 2 Ethernet frame.

Priority Code Point (PCP) is a 3-bit field that indicates the frame priority level (or CoS). The operation of the PCP field is defined within the IEEE 802.1p standard, which is an extension of 802.1Q. The standard establishes eight levels of priority, referred to as CoS values, where CoS 7 ('111' in PCP filed) is the highest priority and CoS 0 ('000') is the lowest priority.

The radio in bridge mode used the PCP value in the VLAN tag to prioritize packets and provide the appropriate QoS treatment per traffic type. The radio implements 4 priority queuing techniques that base its QoS on the VLAN priority (PCP). Based on VLAN priority bits, traffic can be put into a particular Class of Service (CoS) queue. Packets with higher CoS will always serve first for OTA transfer and on ingress/egress Ethernet ports.

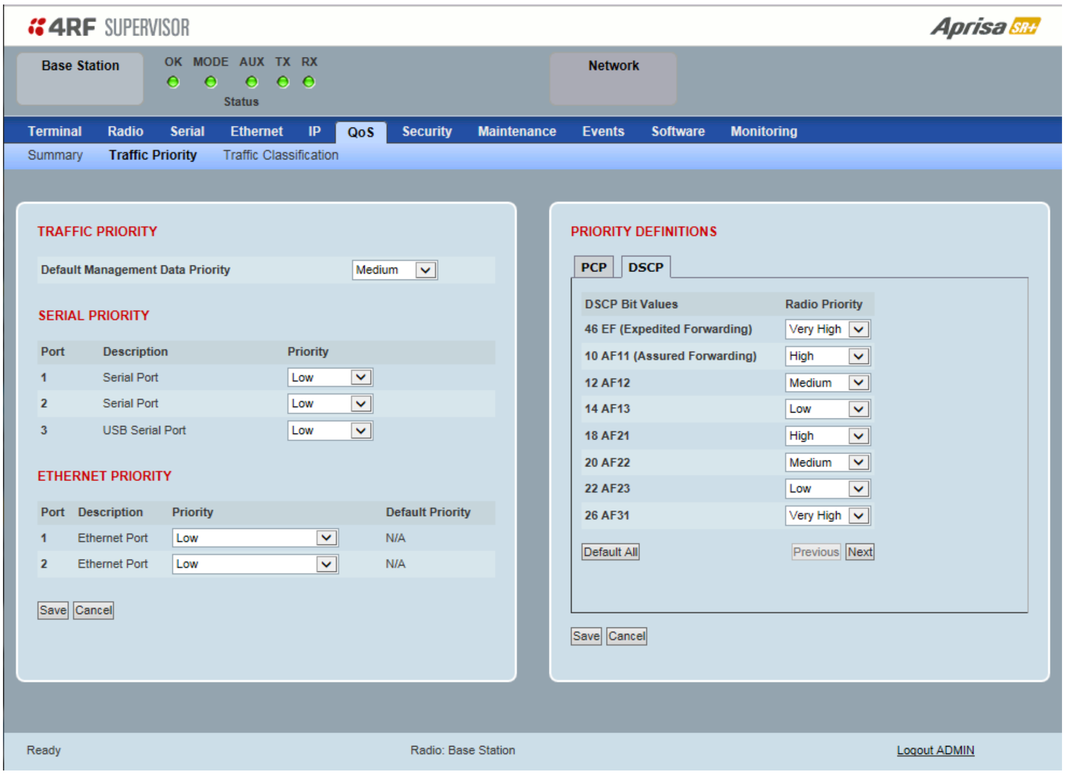
The 'PCP priority definition' tab is used to map ingress VLAN packet with PCP priority to the radio internal CoS (priority). Since, in most of the cases the radio VLAN network is connected to the corporate VLAN networks, the network administrator might like to have a different VLAN priority scheme of the radio network CoS. For example, management traffic in the multi-gigabit corporate VLAN network might be prioritize with priority 7 (highest priority) and SCADA traffic with priority 5, but in the narrow bandwidth radio network, SCADA traffic will be map to radio very high CoS / priority (i.e. set PCP 5 = Very high) and management traffic might will be map to radio medium CoS / priority (i.e. set PCP 7 = medium) in order to serve first the mission-critical SCADA traffic over the radio network.

This is done by mapping the external radio network VLAN priority to the internal radio CoS / priority using the ‘PCP priority definition’ tab. The radio support 4 queues, thus at maximum an 8 -> 4 VLAN priority / CoS mapping is done.

Default mapping of ingress packet VLAN priority to radio CoS / priority shown in the ‘PCP priority definition’ tab.

DSCP (Differentiated Services Code Point)

These settings provide translation / mapping between the external radio IP priority network and the radio internal IP priority network, using the DSCP (DiffServ Code Point) priority field in the IP packet header.



Differentiated Services (DiffServ) is a new model in which traffic is treated by routers with relative priorities based on the IPv4 type of services (ToS) field. DSCP (DiffServ Code Point) standard defined in RFC 2474 and RFC 2475. DiffServ increases the number of definable priority levels by reallocating bits of an IP packet for priority marking.

The DiffServ architecture defines the DiffServ (DS) field, which supersedes the ToS field in IPv4 to make per-hop behaviour (PHB) decisions about packet classification and traffic scheduling functions. The six most significant bits of the DiffServ field (in the IPv4 TOS field) is called as the DSCP. The standardized DiffServ field of the packet is marked with a value so that the packet receives a particular routing/forwarding treatment or PHB, at each router node. Using DSCP packet classification, traffic can be partition into multiple priority levels.

The radio in router mode uses the DSCP value in the IP header to select a PHB behaviour for the packet and provide the appropriate QoS treatment. The radio implements 4 priority queuing techniques that base its PHB on the DSCP in the IP header of a packet. Based on DSCP, traffic can be put into a particular priority / CoS (Class of Service) queue. Packets with higher CoS will always serve first for OTA transfer and on ingress / egress Ethernet ports.

The 'DSCP priority definition' tab is used to map ingress IP packet with DSCP priority to the radio internal priority / CoS. Since, in most of the cases the radio routed network is connected to the corporate routed networks, the network administrator might like to have a different routed network priority scheme of the radio network, for example management traffic in the multi-gigabit corporate routed network might be prioritize with DSCP EF (expedite forwarding) code (DSCP highest priority), and SCADA traffic with DSCP AF11 (assured forwarding) code (high priority), but in the narrow bandwidth radio network, SCADA traffic will be map to radio very high CoS / priority (i.e. set AF11 = Very high) and management traffic might map to radio low CoS / priority (i.e. set EF = Low) in order to serve first the mission-critical SCADA traffic over the radio network.

This is done by mapping the external radio network DSCP priority to the internal radio CoS / priority levels using the ‘DSCP priority definition’ tab. The radio support four queues, thus at maximum a 64 -> 4 CoS / priority mapping is done.

Default mapping of ingress packet DSCP priority to radio CoS shown in the ‘DSCP priority definition’ tab. The radio maps all 64 DSCP values. The user can configure most common used 21 DSCP codes and the rest are mapped by default to low CoS / priority.

QoS > Traffic Classification

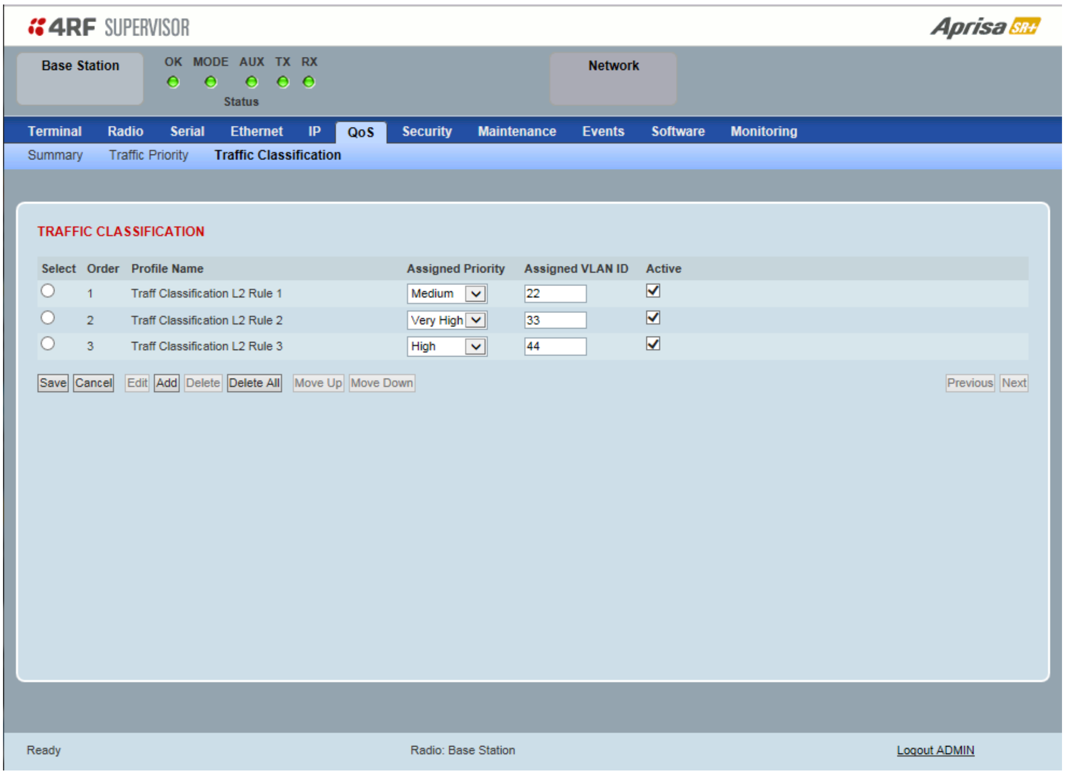
These settings provide multiple traffic classification profiles based on classification rules. Profiles for a specific traffic type, protocol or application can be assigned to a particular VLAN and CoS / priority in bridge mode or to CoS / priority in router mode to provide the appropriate QoS treatment.

For example SCADA traffic, management traffic, FTP traffic, can each have its own profile build with a set of classification rules. A profile can be build using multiple classification rules based on ports, Ethernet, IP, TCP / UDP headers fields (i.e. L1/2/3/4 header fields) such as: Ethernet port #1, VLAN ID, VLAN priority, IP DSCP Priority, MAC/IP address, TCP / UDP port fields to identify and classify the specific traffic type. When an ingress packet matches the profile L2/3/4 header fields settings, the packet is assigned to a particular VLAN and CoS / priority in bridge mode or to CoS / priority in router mode to provide the appropriate QoS treatment.

The radio supports four CoS / priority queues: very high, high, medium and low. These queues are connected to a strict priority scheduler which dispatches packets from the queues out to the egress port by always serving first the ‘very high’ priority queue, whenever there is a packet in this queue. When the highest priority queue empties, the scheduler will serve the next high priority queues and so on. So when SCADA traffic is assigned to a ‘Very high’ priority, it will always served first and send over-the-air (OTA) whenever SCADA traffic enters to the radio, giving it the highest priority over other traffic type.

These settings are different for Bridge Mode and Router Mode.

Bridge Mode Traffic Classification Settings



TRAFFIC CLASSIFICATION

VLAN bridge mode traffic classification settings provide mapping / assigning of profiles (set by rules to match a specific traffic type) to a VLAN ID and VLAN CoS / priority. The profile which is used to match to a specific traffic type will be identified in the radio network by its associated VLAN ID and VLAN CoS / priority to provide the appropriate QoS treatment. CoS / Priority can be set to very high, high, medium, low priority.

Profile name

A free form field to enter the profile name with a maximum of 32 chars.

Assigned Priority

Traffic packets that match the applied profile rules will be assigned to the selected ‘assigned priority’ setting of Very High, High, Medium and Low. This field cannot be set to Don’t Care.

This applies profile rule mapping to the VLAN CoS / Priority with the appropriate internal radio assigned priority setting of Very High, High, Medium and Low.

Assigned VLAN ID

Traffic packets that match the applied profile rules will be assigned to the selected 'assigned VLAN ID' setting of VLAN ID in the range of 0 to 4095.

A VLAN ID of an ingress packet matching the classification rule (see 'VLAN ID' rule in next page) shall be changed to the 'assigned VLAN ID' setting, if below conditions are met:

1. The VLAN ID of Ingress packet is same as PVID of the ingress port.
2. Packet is received untagged at the port

If the VLAN ID of the tagged ingress packet is not the same as the PVID of the ingress port, then it shall not be changed and the 'assigned VLAN ID' setting is ignored i.e. ingress VLANs will pass-through unchanged.

If 'assigned VLAN ID' value is set in the 'port VLAN membership' under Ethernet > VLAN (port x tab), then this VLAN will be available for ingress and egress on the Ethernet and RF ports, otherwise this VLAN will only be available in one direction on the egress RF port.

For example, if the base station Ethernet port 1 'assigned VLAN ID' = 100 (VLAN-100) and it is also defined in the 'port VLAN membership' under Ethernet > VLAN (port 1 tab) and the remote sends a packet to the base with a VLAN of 100, this packet will be egress out to Ethernet port 1 (tagged or untagged based on the 'egress action' definition). If the VLAN-100 wasn't set in the 'port VLAN membership', then the base station will drop a packet from the remote.

This setting parameter can be 'Don't Care' (Assigned VLAN ID = 0) which means that the VLAN ID of ingress frame will never be modified.

Active

Activates or deactivates the profile rule.

Controls

The Save button saves all profiles to the radio.

The Cancel button removes all changes since the last save or first view of the page if there has not been any saves. This button will un-select all the Select radio buttons.

The Edit button will show the next screen for the selected profile where the profile can be configured. This button will be disabled unless a profile is selected.

The Add button adds a new profile,

- If no profile was selected then the new profile is added to the end of the list,
- If a profile is selected the new profile is added after that profile.

The Delete button will delete the selected profile. The button will be disabled unless a profile has been selected.

The Delete All button will delete all the profiles. A pop-up will ask if the action is correct. If the answer is yes, then all profiles are deleted in SuperVisor. The Save button must be pressed to delete all the profiles in the radio.

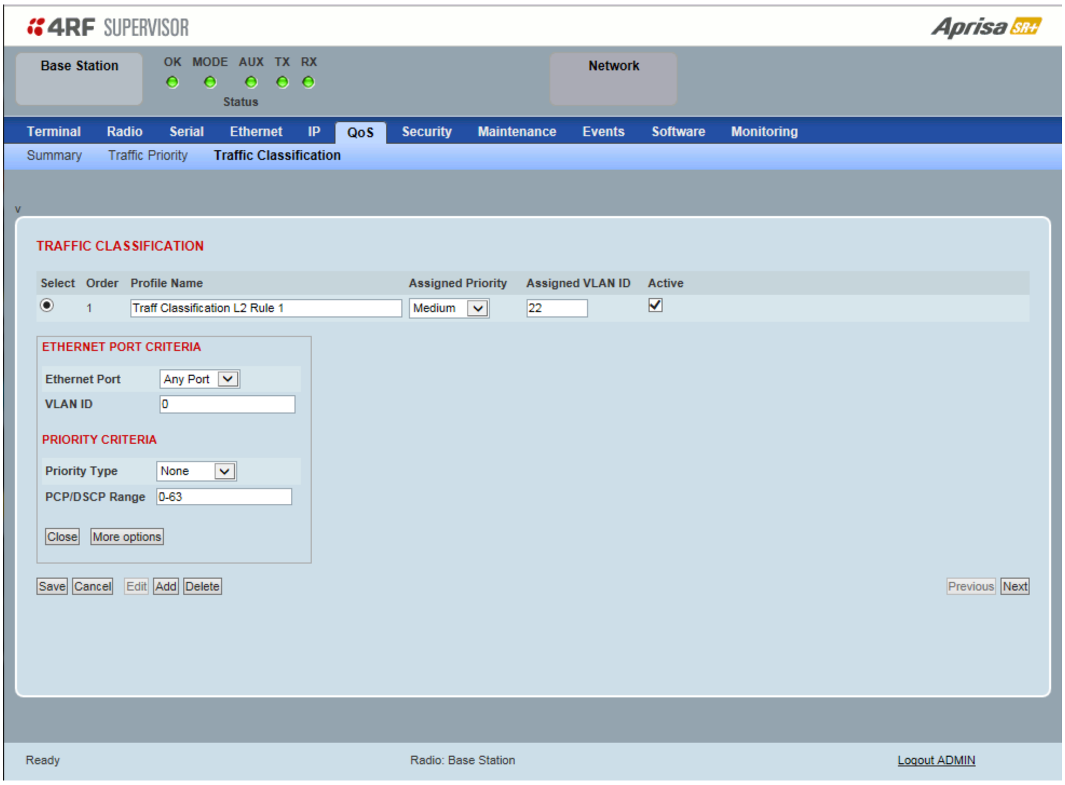
The Move up button will move the selected profile up one in the order of profiles

The Move Down button will move the selected profile down one in the order of profiles

The Previous button displays the previous page in the list of profiles. A pop up will be displayed if any profile has been modified and not saved, preventing the previous page being displayed.

The Next button will display the next page in the list of profiles.

To edit a traffic classification, select the profile and click on the Edit button



ETHERNET PORT CRITERIA

Ethernet Port

Set the layer 1 Ethernet port number or all Ethernet ports in the selected profile classification rule.

VLAN ID

Sets the layer 2 packet Ethernet header VLAD ID field in the selected profile classification rule. Valid values are between 0 and 4095. This VLAN ID should be enabled in the system for using this parameter during classification.

Enable this VLAN in the network by setting the same VLAN ID value in PVID (port VLAN ID) and in the PORT VLAN MEMBERSHIP under 'VLAN PORT SETTINGS – Port 1' on page 133. If the VLAN ID is set to zero, all VLAN IDs will meet the criteria.

PRIORITY CRITERIA

Priority Type

Set the layer 2 Ethernet or layer 3 IP packet header priority type fields in the selected profile classification rules.

Priority Type	Description
None	Do not use any layer 2 / 3 Ethernet or IP header priority fields in the selected profile classification rules.
PCP	Use the layer 2 Ethernet header priority field of PCP (Priority Code Point) VLAN priority bits (per IEEE 802.1p/q) in the selected profile classification rules.
DSCP	Use the layer 3 IP header TOS field used as DSCP (Differentiated Services Code Point per RFC 2474 and RFC 2475) priority bit in the selected profile classification rules.

PCP / DSCP Range

As per the ‘priority type’ selection, this parameter sets the PCP priority value/s or DSCP priority value/s fields in the selected profile classification rule. The value can be set to a single priority or a single range (no multiple ranges are allowed), for example, the PCP selected priority value can be 7 or a range of priority values like 4-7.

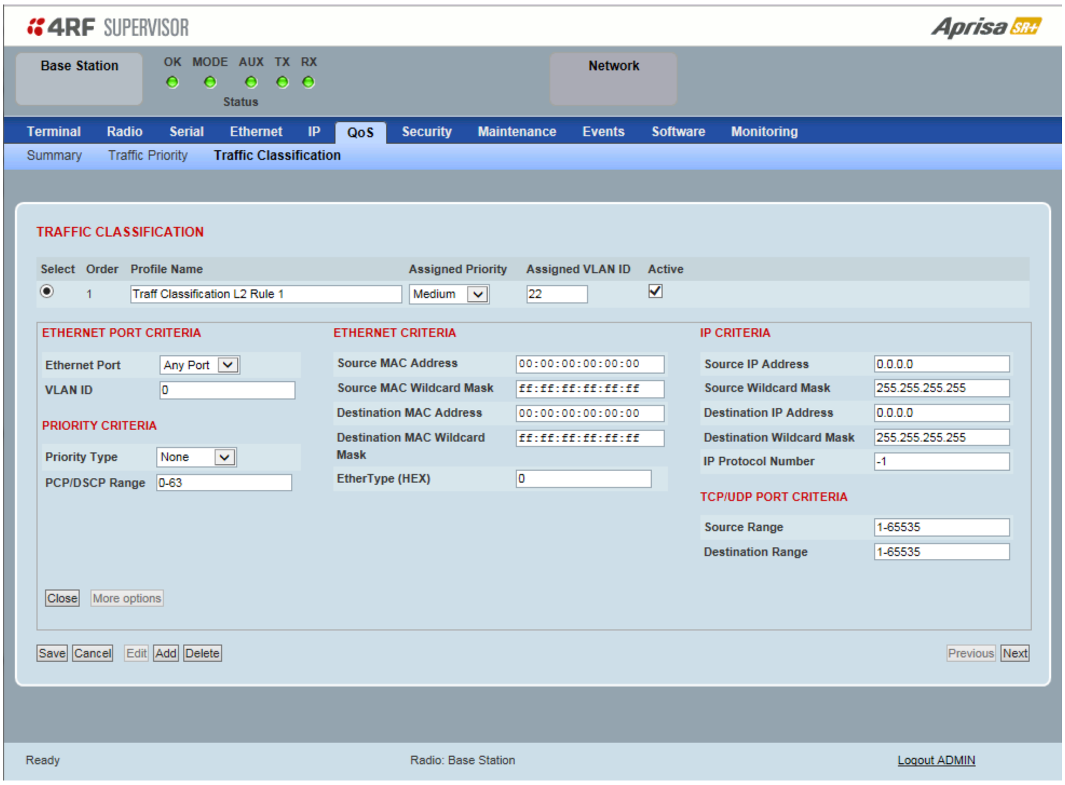
The following table shows the layer 2 packet VLAN tag header PCP priority field values

PCP Value (Decimal)	PCP Priority	Priority Level
7	Priority [7]	Highest
6	Priority [6]	
5	Priority [5]	
4	Priority [4]	
3	Priority [3]	
2	Priority [2]	
1	Priority [1]	
0	Priority [0]	Lowest

The following table shows the layer 3 packet IP header DSCP priority field values

DSCP Value (Decimal)	DSCP Priority
46	EF (Expedited Forwarding)
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
0	CS0/Best Effort (BE)
8	CS1 (Class Selector)
16	CS2
24	CS3
32	CS4
40	CS5
48	CS6
56	CS7

Click on More Options if more Layer 2/3/4 (Ethernet / IP / TCP or UDP) packet header fields are required for the selected profile classification rule. This page describes all the possible fields that can be used for the classification rules in bridge mode.



ETHERNET CRITERIA

Source MAC Address

This parameter sets the Layer 2 Ethernet packet header Source MAC Address field in the selected profile classification rule in the format of 'hh:hh:hh:hh:hh:hh'.

Source MAC Wildcard Mask

This parameter sets the wildcard mask of the 'Source MAC Address'. If the Source MAC Address is set to 'FF:FF:FF:FF:FF:FF', all source MAC addresses will meet the criteria.

Destination MAC Address

This parameter sets the Layer 2 Ethernet packet header Destination MAC Address field in the selected profile classification rule in the format of 'hh:hh:hh:hh:hh:hh'.

Destination MAC Wildcard Mask

This parameter sets the wildcard mask of the 'Destination MAC Address'. If the Destination MAC Address is set to 'FF:FF:FF:FF:FF:FF', all destination MAC addresses will meet the criteria.

EtherType (Hex)

This parameter sets the Layer 2 Ethernet packet header EtherType field in the selected profile classification rule. EtherType is a 16 bit (two octets) field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet Frame.

EtherType Examples:

Protocol	EtherType Value (Hexadecimal)
IPv4	0800
ARP	0806
IPv6	86DD
VLAN	8100

IP CRITERIA

Source IP Address

This parameter sets the Layer 3 IP packet header Source IP Address field in the selected profile classification rule. This parameter is written in the standard IPv4 format of ‘xxx.xxx.xxx.xxx’.

Source IP Wildcard Mask

This parameter sets the wildcard mask applied to the ‘Source IP Address’. This parameter is written in the standard IPv4 format of ‘xxx.xxx.xxx.xxx’.

0 means that it must be a match. If the wildcard mask is set to 0.0.0.0, the complete Source IP Address will be evaluated for the classification rule.

If the wildcard mask is set to 0.0.255.255, the first 2 octets of the Source IP Address will be evaluated for the classification rule.

If the wildcard mask is set to 255.255.255.255, none of the Source IP Address will be evaluated for the classification rule.

Note: The wildcard mask operation is the inverse of subnet mask operation

Destination IP Address

This parameter sets the Layer 3 IP packet header Destination IP Address field in the selected profile classification rule. This parameter is written in the standard IPv4 format of ‘xxx.xxx.xxx.xxx’.

Destination IP Wildcard Mask

This parameter sets the wildcard mask applied to the ‘Destination IP Address’. This parameter is written in the standard IPv4 format of ‘xxx.xxx.xxx.xxx’.

0 means that it must be a match. If the wildcard mask is set to 0.0.0.0, the complete Destination IP Address will be evaluated for the classification rule.

If the wildcard mask is set to 0.0.255.255, the first 2 octets of the Destination IP Address will be evaluated for the classification rule.

If the wildcard mask is set to 255.255.255.255, none of the Destination IP Address will be evaluated for the classification rule.

Note: The wildcard mask operation is the inverse of subnet mask operation

IP Protocol Number

This parameter sets the Layer 3 IP packet header ‘Protocol’ field in the selected profile classification rule. This field defines the protocol used in the data portion of the IP datagram.

Protocol number Examples:

Protocol	Protocol value (decimal)
ICMP	1
TCP	6
UDP	17

TCP / UDP PORT CRITERIA

Source Range

This parameter sets the Layer 4 TCP / UDP packet header Source Port or Source Port range field in the selected profile classification rule. To specify a range, insert a dash between the ports e.g. 1000-2000. If the source port range is set to 1-65535, traffic from any source port will meet the criteria.

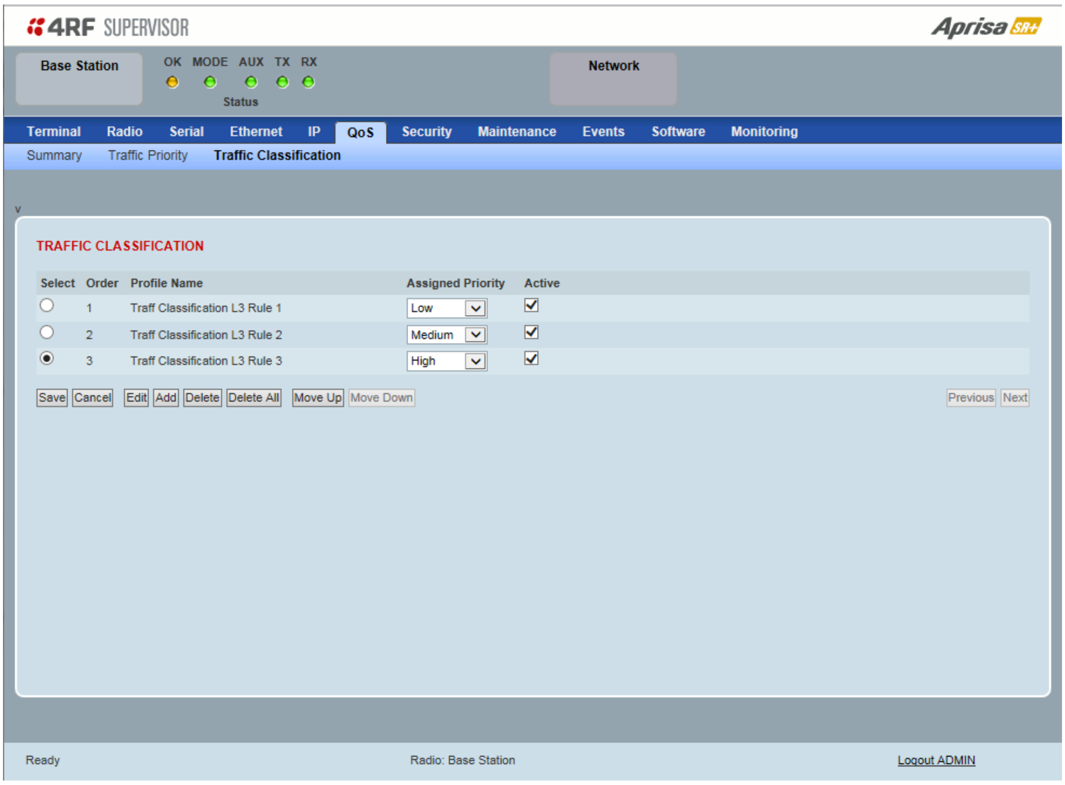
Destination Range

This parameter sets the Layer 4 TCP / UDP packet header Destination Port or Destination Port range field in the selected profile classification rules. To specify a range, insert a dash between the ports e.g. 1000-2000. If the source port range is set to 1-65535, traffic from any source port will meet the criteria.

Examples for 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

Router Mode Traffic Classification Settings



TRAFFIC CLASSIFICATION

Router Mode traffic classification settings provide mapping / assigning of profiles (set by rules to match a specific traffic type) to a CoS / priority. The profile which is used to match to a specific traffic type will be identified in the radio network by its associated CoS / priority to provide the appropriate QoS treatment. CoS / Priority can be set to very high, high, medium, low priority.

Profile name

A free form field to enter the profile name with a maximum of 32 chars.

Assigned Priority

Traffic packets that match the applied profile rules will be assigned to the selected 'assigned priority' setting of Very High, High, Medium and Low. This field cannot be set to Don't Care.

Active

Activated or deactivate the profile rule.

Controls

The Save button saves all profiles to the radio.

The Cancel button removes all changes since the last save or first view of the page if there has not been any saves. This button will un-select all the Select radio buttons.

The Edit button will show the next screen for the selected profile where the profile can be configured. This button will be disabled unless a profile is selected.

The Add button adds a new profile,

- If no profile was selected then the new profile is added to the end of the list,
- If a profile is selected the new profile is added after that profile.

The Delete button will delete the selected profile. The button will be disabled unless a profile has been selected.

The Delete All button will delete all the profiles. A pop-up will ask if the action is correct. If the answer is yes, then all profiles are deleted in SuperVisor. The Save button must be pressed to delete all the profiles in the radio.

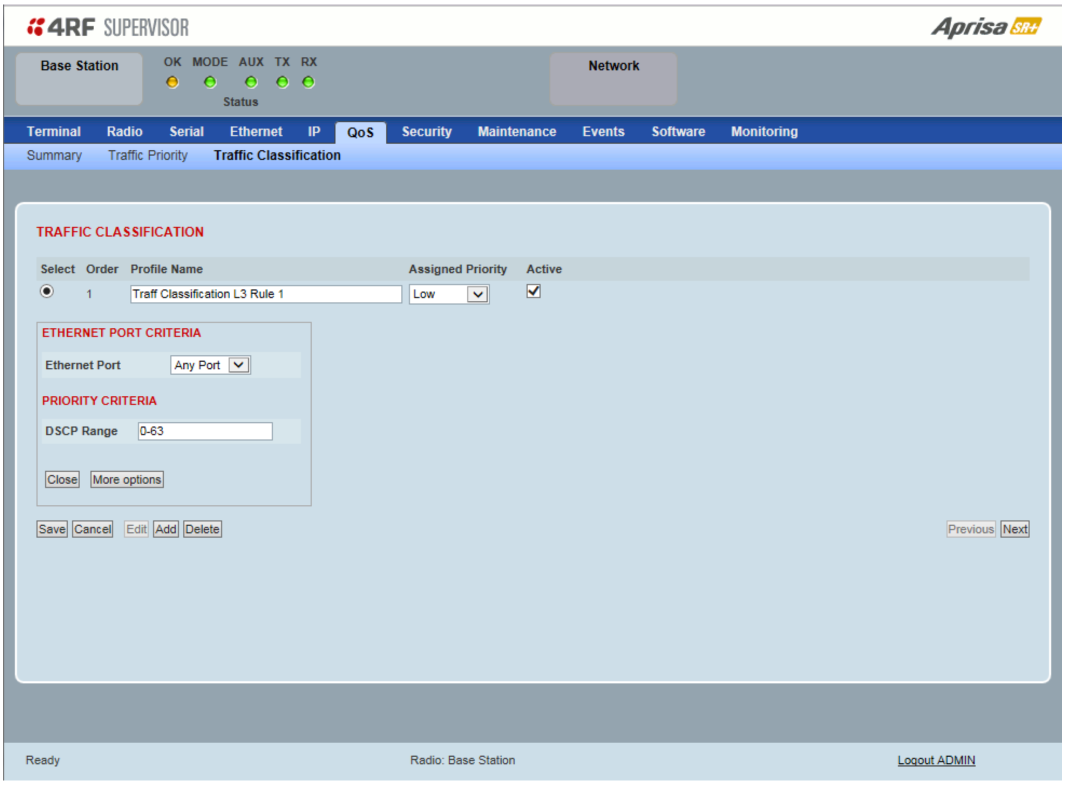
The Move up button will move the selected profile up one in the order of profiles

The Move Down button will move the selected profile down one in the order of profiles

The Previous button displays the previous page in the list of profiles. A pop up will be displayed if any profile has been modified and not saved, preventing the previous page being displayed.

The Next button will display the next page in the list of profiles.

To edit a traffic classification, select the profile and click on the Edit button



ETHERNET PORT CRITERIA

Ethernet Port

Set the layer 1 Ethernet port number or all Ethernet ports in the selected profile classification rules.

PRIORITY CRITERIA

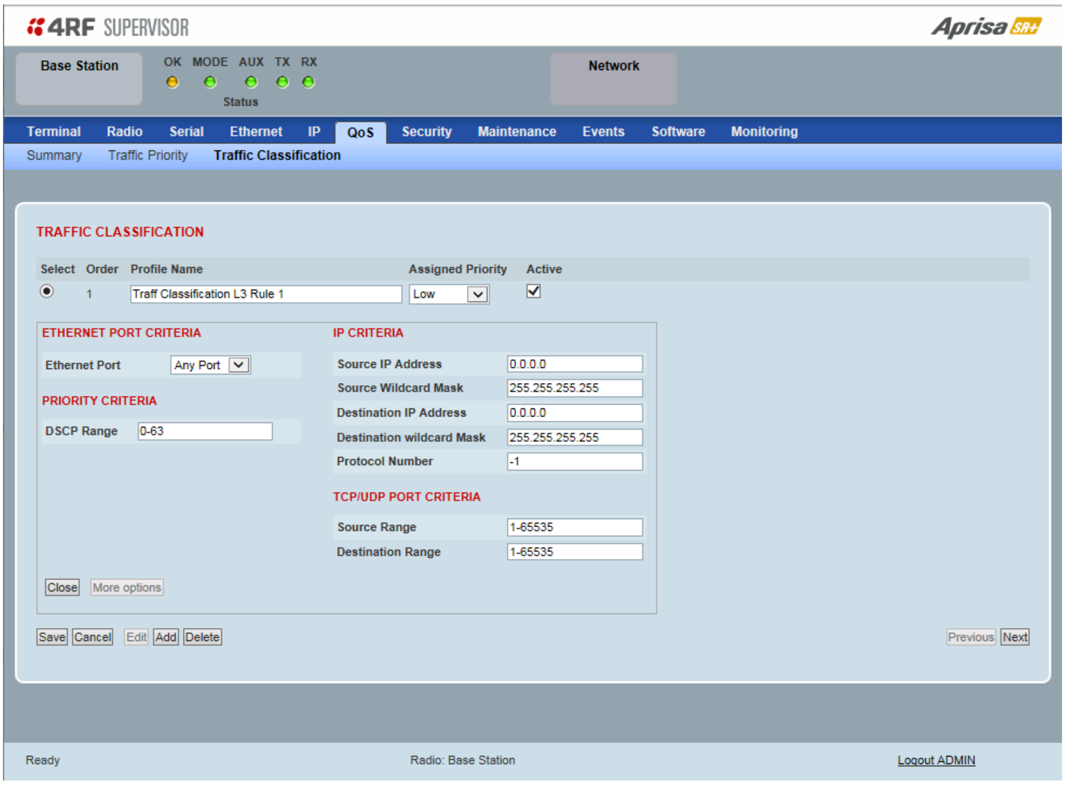
DSCP Range

Sets the DSCP priority value/s field in the selected profile classification rule. The value can be set to a single priority or a single range (no multiple range are allowed), for example, priority value can be 46 (EF) or a range of priority values like 10-14.

The following table shows the layer 3 packet IP header DSCP priority field values

DSCP Value (Decimal)	DSCP Priority
46	EF (Expedited Forwarding)
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
0	CS0/Best Effort (BE)
8	CS1 (Class Selector)
16	CS2
24	CS3
32	CS4
40	CS5
48	CS6
56	CS7

Click on More Options if more Layer 3/4 packet header fields are required for the selected profile classification rule. This page describes all the possible fields that can be used for the classification rules in router mode.



IP CRITERIA

Source IP Address

This parameter sets the Layer 3 packet IP header Source IP Address field in the selected profile classification rules. This parameter is written in the standard IPv4 format of 'xxx.xxx.xxx.xxx'.

Source IP Wildcard Mask

This parameter sets the wildcard mask applied to the 'Source IP Address'. This parameter is written in the standard IPv4 format of 'xxx.xxx.xxx.xxx'.

0 means that it must be a match. If the wildcard mask is set to 0.0.0.0, the complete Source IP Address will be evaluated for the classification rules.

If the wildcard mask is set to 0.0.255.255, the first 2 octets of the Source IP Address will be evaluated for the classification rules.

If the wildcard mask is set to 255.255.255.255, none of the Source IP Address will be evaluated for the classification rules.

Note: The wildcard mask operation is the inverse of subnet mask operation

Destination IP Address

This parameter sets the Layer 3 packet IP header Destination IP Address field in the selected profile classification rules. This parameter is written in the standard IPv4 format of 'xxx.xxx.xxx.xxx'.

Destination IP Wildcard Mask

This parameter sets the wildcard mask applied to the 'Destination IP Address'. This parameter is written in the standard IPv4 format of 'xxx.xxx.xxx.xxx'.

0 means that it must be a match. If the wildcard mask is set to 0.0.0.0, the complete Destination IP Address will be evaluated for the classification rules.

If the wildcard mask is set to 0.0.255.255, the first 2 octets of the Destination IP Address will be evaluated for the classification rules.

If the wildcard mask is set to 255.255.255.255, none of the Destination IP Address will be evaluated for the classification rules.

Note: The wildcard mask operation is the inverse of subnet mask operation

Protocol Number

This parameter sets the Layer 3 IP packet header 'Protocol' field in the selected profile classification rule. This field defines the protocol used in the data portion of the IP datagram.

Protocol number Examples:

Protocol	Protocol value (decimal)
ICMP	1
TCP	6
UDP	17

TCP / UDP Port Criteria

Source Range

This parameter sets the Layer 4 TCP / UDP packet header Source Port or Source Port range field in the selected profile classification rule. To specify a range, insert a dash between the ports e.g. 1000-2000. If the source port range is set to 1-65535, traffic from any source port will meet the criteria.

Destination Range

This parameter sets the Layer 4 TCP / UDP packet header Destination Port or Destination Port range field in the selected profile classification rule. To specify a range, insert a dash between the ports e.g. 1000-2000. If the source port range is set to 1-65535, traffic from any source port will meet the criteria.

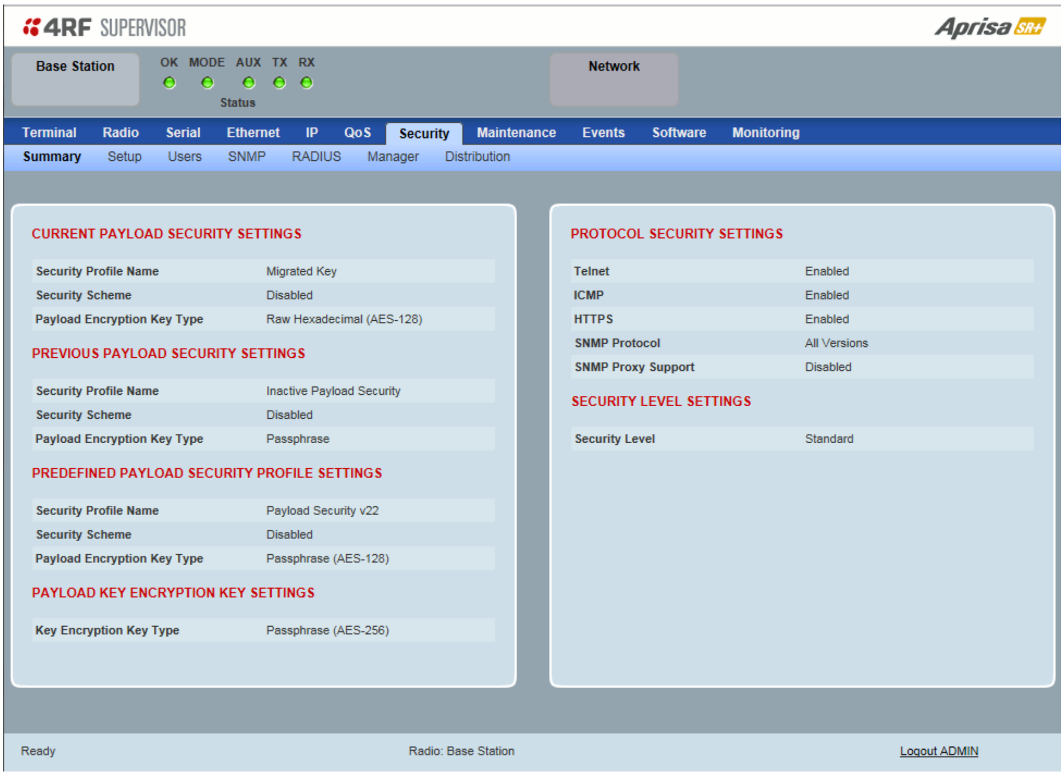
Examples for TCP / UDP Port Numbers:

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

Security

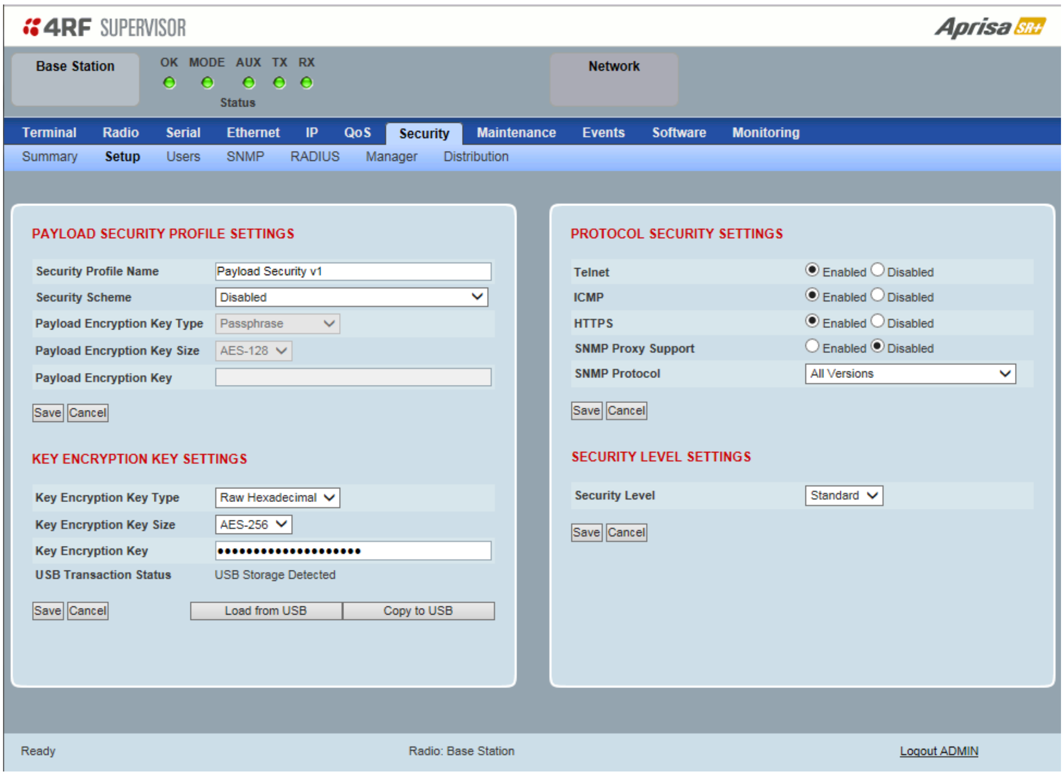
Security > Summary

This page displays the current settings for the Security parameters.



See ‘Security > Setup’ and ‘Security > Manager’ for configuration options.

Security > Setup



PAYLOAD SECURITY PROFILE SETTINGS

Security Profile Name

This parameter enables the user to predefine a security profile with a specified name.

Security Scheme

This parameter sets the security scheme to one of the values in the following table:

Security Scheme
Disabled (No encryption and no Message Authentication Code)
AES Encryption + CCM Authentication 128 bit
AES Encryption + CCM Authentication 64 bit
AES Encryption + CCM Authentication 32 bit
AES Encryption only
CCM Authentication 128 bit
CCM Authentication 64 bit
CCM Authentication 32 bit

The default setting is Disabled.

Payload Encryption Key Type

This parameter sets the Payload Encryption Key Type:

Option	Function
Pass Phrase	Use the Pass Phrase password format for standard security.
Raw Hexadecimal	Use the Raw Hexadecimal key format for better security. It must comply with the specified encryption key size e.g. if Encryption Type to AES128, the encryption key must be 16 bytes (32 chars)

The default setting is Pass Phrase.

Payload Encryption Key Size

This parameter sets the Encryption Type to AES128, AES192 or AES256. The default setting is AES128.

The higher the encryption size the better the security.

Payload Encryption Key

This parameter sets the Payload Encryption password. This key is used to encrypt the payload.

<u>Pass Phrase</u>

Good password policy:

- contains at least eight characters, and
- contains at least one upper case letter, and
- contains at least one lower case letter, and
- contains at least one digit or another character such as @+... , 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

<u>Raw Hexadecimal</u>

The Raw Hexadecimal key must comply with the specified encryption key size e.g. if Encryption Type to AES128, the encryption key must be 16 bytes (32 chars).

KEY ENCRYPTION KEY SETTINGS

The Key Encryption Key provides the ability to encrypt the Payload Encryption Key so it can be safely transmitted over the radio link to remote radios.

The Key Encryption Key Type, Key Encryption Key Size and Key Encryption Key must be the same on all radios in the network.

Key Encryption Key Type

This parameter sets the Payload Encryption Key Type:

Option	Function
Pass Phrase	Use the Pass Phrase password format for standard security.
Raw Hexadecimal	Use the Raw Hexadecimal key format for better security. It must comply with the specified encryption key size e.g. if Encryption Type to AES128, the encryption key must be 16 bytes (32 chars)

The default setting is Pass Phrase.

Key Encryption Key Size

This parameter sets the Encryption Type to AES128, AES192 or AES256. The default setting is AES128.

The higher the encryption type the better the security.

Key Encryption Key

This parameter sets the Key Encryption Key. This is used to encrypt the payload encryption key.

USB Transaction Status

This parameter shows if a USB flash drive is plugged into the radio host port .

Option	Function
USB Storage Not Detected	A USB flash drive is not plugged into the radio host port.
USB Storage Detected	A USB flash drive is plugged into the radio host port.

Controls

The ‘Save’ button saves the Key Encryption Key settings to the radio. If the Security Level is set to Strong (see ‘Security Level’ on page 176), this button will be grayed out.

The ‘Load From USB’ button loads the Key Encryption Key settings from the USB flash drive. If a USB flash drive is not detected, this button will be grayed out

The ‘Copy To USB’ button copies the Key Encryption Key settings to a file called ‘asrkek.txt’ on the USB flash drive. This settings file can be used to load into other radios. If a USB flash drive is not detected or the Security Level is set to Strong (see ‘Security Level’ on page 176), this button will not be shown.

Key Encryption Key Summary

The security of over-the-air-rekeying depends on a truly random Key Encryption Key. This is why the use of a Raw Hexadecimal key is recommended as a plain text phrase based on known spelling and grammar constructs is not very random. The *default* Key Encryption Key is provided only to allow testing of the security mechanism and is not intended for operational use. Using the default Key Encryption Key undermines the security of the AES payload encryption because an attacker using the default Key Encryption Key would immediately recover the AES payload key after the first over-the-air-rekeying event.

When the Security Level is set to Strong, various protections are applied to the Key Encryption Key setting to prevent tampering. In addition, the Key Encryption Key Type, Key Encryption Key Size, and the Key Encryption Key itself are all loaded from a customer prepared USB key. This is a one way operation to prevent key recovery from radios. While the ability to save a Key Encryption Key to USB exists in Standard Security Level, the Strong Security Level Key Encryption Key is not compromised because the Strong Key Encryption Key is not the same as the Standard Security Level Key Encryption Key.

PROTOCOL SECURITY SETTINGS

Telnet option

This parameter option determines if you can manage the radio via a Telnet session. The default setting is disabled.

ICMP option (Internet Control Message Protocol)

This parameter option determines whether the radio will respond to a ping. The default setting is disabled.

HTTPS option

This parameter option determines if you can manage the radio via a HTTPS session (via a Browser). The default setting is enabled.

SNMP Proxy Support

This parameter option enables an SNMP proxy server in the base station. This proxy server reduces the radio link traffic during SNMP communication to remote / repeater stations. This option applies to the base station only. The default setting is disabled.

This option can also be used if the radio has Serial Only interfaces.

SNMP Protocol

This parameter sets the SNMP Protocol:

Option	Function
Disabled	All SNMP functions are disabled.
All Versions	Allows all SNMP protocol versions.
SNMPv3 Only	Only SNMPv3 transactions will be accepted.
SNMPv3 With Authentication Only	Only SNMPv3 transactions authenticated using HMAC-MD5 or HMAC-SHA will be accepted.

The default setting is All Versions.

The default SNMPv3 with Authentication User Details provided are:

User Name	Encryption Type	Authentication Type	Context Name	Authentication Passphrase	Encryption Passphrase
noAuthUser	-	-	noAuth	noAuthUser	noAuthUser
desUserMD5	DES	MD5	priv	desUserMD5	desUserMD5
desUserSHA	DES	SHA	priv	desUserSHA	desUserSHA
authUserMD5	-	MD5	auth	authUserMD5	authUserMD5
authUserSHA	-	SHA	auth	authUserSHA	authUserSHA
privUserMD5	AES	MD5	priv	privUserMD5	privUserMD5
privUserSHA	AES	SHA	priv	privUserSHA	privUserSHA

SNMPv3 Authentication Passphrase

The SNMPv3 Authentication Passphrase can be changed via the SNMPv3 secure management protocol interface (not via SuperVisor).

When viewing / managing the details of the users via SNMPv3, the standard SNMP-USER-BASED-SM-MIB interface is used. This interface can be used to change the SNMPv3 Authentication Passphrase of the users.

The SNMPv3 Authentication Passphrase of a user required to be changed cannot be changed by the same user i.e. a different user must be used for the transactions.

Generate New Keys from SNMPv3 USM User Passphrases

Net-SNMP is a suite of open source software for using and deploying the SNMP protocol. Similar functionality is built into many commercial SNMP managers.

This next step of loading the Aprisa SR+ radios with keys generated from USM user passphrases requires the SNMPv3 USM Management utility provided as part of NET-SNMP.

The utility is called 'snmpusm'. It provides a range of commands including the management of changing passwords for SNMPv3 users. In order to use this utility, the user will need to install NET-SNMP on a Linux (or Windows®) or machine. The examples below are from the Linux environment. This tool automatically obtains the engine ID from the target radio before generating the keys and loading them into the target.

To change a user authentication passphrase:

The following are examples of:

Changing the privUserSHA user encryption key / password from privUserSHA to privUserSHANew:

c:\usr\bin>snmpusm -v 3 -u privUserSHA -n priv -l authPriv -a SHA -A privUserSHA -x AES -X privUserSHA -Cx 172.17.70.17 passwd privUserSHA privUserSHANew

Changing the privUserSHA user authentication key / password from privUserSHA to privUserSHANew:

c:\usr\bin>snmpusm -v 3 -u privUserSHA -n priv -l authPriv -a SHA -A privUserSHA -x AES -X privUserSHANew -Ca 172.17.70.17 passwd privUserSHA privUserSHANew

Changing the desUserSHA user encryption key / password from desUserSHA to desUserSHANew:

c:\usr\bin>snmpusm -v 3 -u desUserSHA -n priv -l authPriv -a SHA -A desUserSHA -x DES -X desUserSHA -Cx 172.17.70.17 passwd desUserSHA desUserSHANew

Changing the desUserSHA user authentication key / password from desUserSHA to desUserSHANew:

c:\usr\bin>snmpusm -v 3 -u desUserSHA -n priv -l authPriv -a SHA -A desUserSHA -x DES -X desUserSHANew -Ca 172.17.70.17 passwd desUserSHA desUserSHANew

Changing the privUserMD5 user encryption key / password from privUserMD5 to privUserMD5New:

c:\usr\bin>snmpusm -v 3 -u privUserMD5 -n priv -l authPriv -a MD5 -A privUserMD5 -x AES -X privUserMD5 -Cx 172.17.70.17 passwd privUserMD5 privUserMD5New

Changing the privUserMD5 user authentication key / password from privUserMD5 to privUserMD5New:

c:\usr\bin>snmpusm -v 3 -u privUserMD5 -n priv -l authPriv -a MD5 -A privUserMD5 -x AES -X privUserMD5New -Ca 172.17.70.17 passwd privUserMD5 privUserMD5New

Changing the desUserMD5 user encryption key / password from desUserMD5 to desUserMD5New:

c:\usr\bin>snmpusm -v 3 -u desUserMD5 -n priv -l authPriv -a MD5 -A desUserMD5 -x DES -X desUserMD5 -Cx 172.17.70.17 passwd desUserMD5 desUserMD5New

Changing the desUserMD5 user authentication key / password from desUserMD5 to desUserMD5New:

c:\usr\bin>snmpusm -v 3 -u desUserMD5 -n priv -l authPriv -a MD5 -A desUserMD5 -x DES -X desUserMD5New -Ca 172.17.70.17 passwd desUserMD5 desUserMD5New

Changing the authUserSHA user authentication key / password from authUserSHA to authUserSHANew:

c:\usr\bin>snmpusm -v 3 -u authUserSHA -n auth -l authNoPriv -a SHA -A authUserSHA -Ca 172.17.70.17 passwd authUserSHA authUserSHANew

Changing the authUserMD5 user authentication key / password from authUserMD5 to authUserMD5New:

c:\usr\bin>snmpusm -v 3 -u authUserMD5 -n auth -l authNoPriv -a MD5 -A authUserMD5 -Ca 172.17.70.17 passwd authUserMD5 authUserMD5New

Notes

-Cx option is to change the Encryption key/password

-Ca option is to change the Authentication key/password

Other information on this utility can be obtained from the utility command help itself or online

Summary

It is necessary to record the new passphrases loaded into the Aprisa SR+ radios and then load the passphrases into the SNMP manager. There is a separate passphrase for the two supported forms of authentication (MD5 and SHA1) only as well as the two forms of authentication used in combination the two forms of encryption (DES and AES). It is vital to change all passphrases even if the depreciated mechanism are not used (MD5 and DES) otherwise an attacker could still use the default passphrases.

Reset Unknown Passphrases with the Command Line Interface

As it is not possible for users to read previously set passphrases, a CLI command is available from Aprisa SR+ software release 1.4.0 to ‘reset’ the SNMPv3 USM users back to defaults.

Note: USM users are not related to CLI and SuperVisor users. This command will only be accessible to the CLI ‘admin’ user logins.

To reset unknown passphrases:

1. Telnet into each radio in the network and via the CLI reset the passphrases
2. Login to the radio with:

   Login: admin

   Password: *********
3. Set all SNMP3 users to default values with the ‘snmpusm reset’ command (see ‘SNMP3 users to default values’ below for the list of default values).
4. Reboot the radio with the ‘reboot’ command.

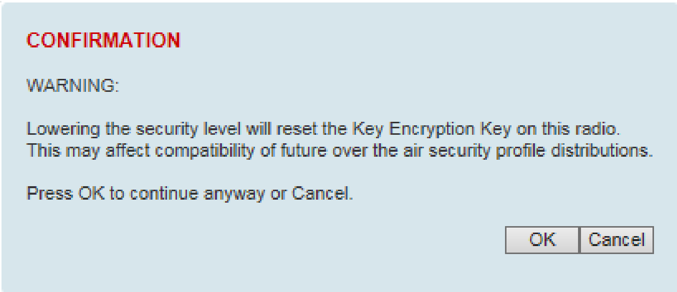
SECURITY LEVEL SETTINGS

Security Level

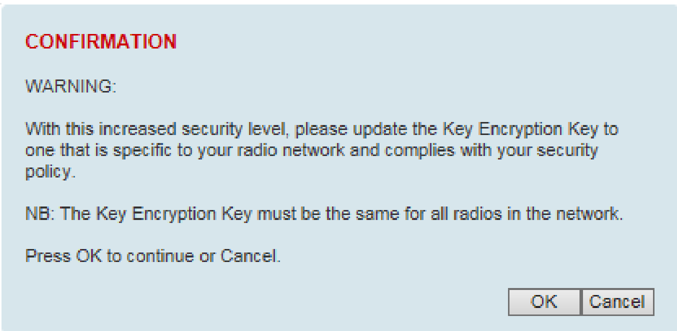
This parameter sets the Security Level active security features. The default setting is Standard.

Option	Payload Encryption	HTTPS	SNMPv3	USB KEK Only
Standard	✓	✓	✓	
Strong	✓	✓	✓	✓

If the Security Level is reduced, there will be a pop up message warning that Key Encryption Key will be reset to the default value.



If the Security Level is increased, there will be a pop up message reminding user to enter a new Key Encryption Key.



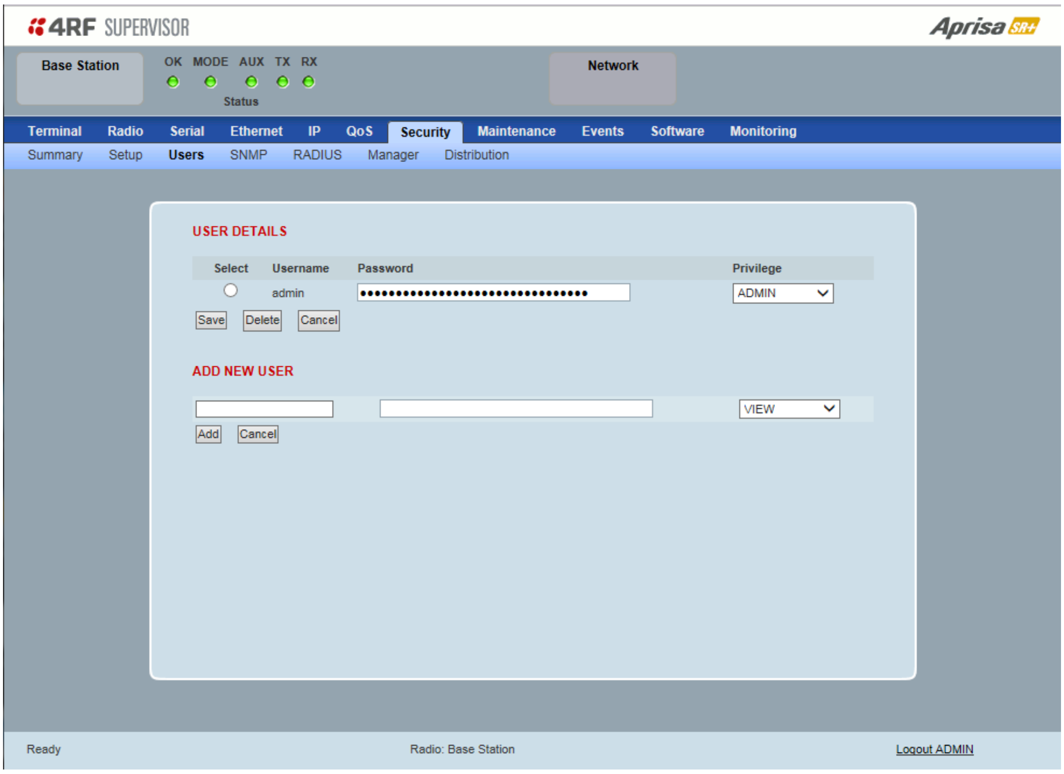
If the Security Level is set to Strong, the 'Save' button will be grayed out and the 'Copy To USB' button will not be shown.

SNMPv3 Context Addressing

SNMPv3 is not user configurable and user can use this option with any NMS. The radio SNMP management interface supports SNMPv3/2 context addressing. The SNMv3 context addressing allows the user to use secure SNMPv3 management while improving NMS performance.

A NMS (Network Management System) can access any remote radio directly by using its IP address or via the base / master station SNMPv3 context addressing. The SNMPv3 context addressing can compress the SNMPv3 management traffic OTA (Over The Air) to the remote station by up to 90% relative to direct OTA SNMPv3 access to remote station, avoiding the radio narrow bandwidth traffic loading.

Security > Users



Note: You must login with ‘admin’ privileges to add, disable, delete a user or change a password.

USER DETAILS

Shows a list of the current users setup in the radio.

ADD NEW USER

To add a new user:

1. Enter the Username.

A username can be up to 32 characters but cannot contain back slashes, forward slashes, spaces, tabs, single or double quotes. Usernames are case sensitive.

2. Enter the Password.

A password can be 8 to 32 printable characters but cannot contain a tab. Passwords are case sensitive.

Good password policy:

- contains at least eight characters, and
- contains at least one upper case letter, and
- contains at least one lower case letter, and
- contains at least one digit or another character such as !@#$%^&(){}[]<>... , 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

3. 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 radio 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
View	view	view	Users in this group can only view the summary pages.
Technician	technician	technician	Users in this group can view and edit parameters except Security > Users, Security > Settings and Advanced settings.
Engineer	engineer	engineer	Users in this group can view and edit parameters except Security > Users.
Admin	admin	admin	Users in this group can view and edit all parameters.

See 'SuperVisor Menu Access' on page 78 for the list of SuperVisor menu items versus user privileges.

4. Click 'Add'

To delete a user:

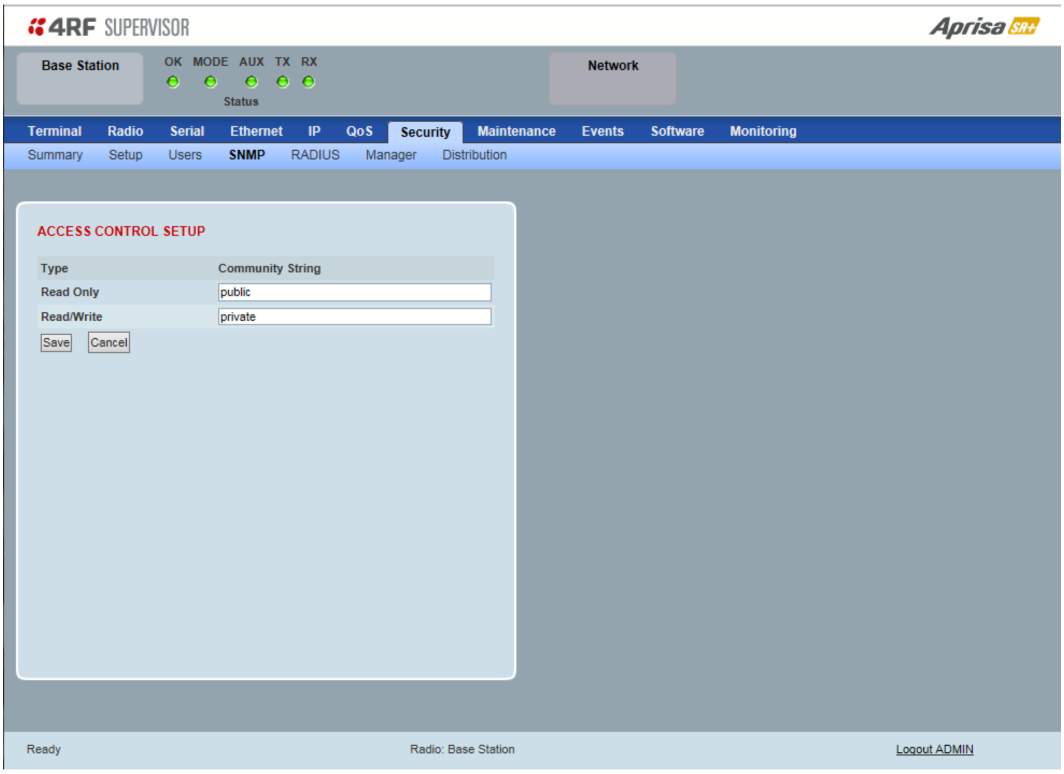
1. Select Terminal Settings > Security > Users
2. Click on the Select button for the user you wish to delete.
3. Click 'Delete

To change a Password:

1. Select Terminal Settings > Security > Users
2. Click on the Select button for the user you wish to change the Password.
3. Enter the Password.

A password can be 8 to 32 characters but cannot contain back slashes, forward slashes, spaces, tabs, single or double quotes.

Security > SNMP



In addition to web-based management (SuperVisor), the network can also be managed using the Simple Network Management Protocol (SNMP) using any version of SNMP v1/2/3. MIB files are supplied, and these can be used by a dedicated SNMP Manager, such as Castle Rock's SNMPc, to access most of the radio's configurable parameters.

For communication between the SNMP manager and the radio, Access Controls and Community strings must be set up as described in the following sections.

A SNMP **Community String** is used to protect against unauthorized access (similar to a password). The SNMP agent (radio or SNMP manager) will check the community string before performing the task requested in the SNMP message.

ACCESS CONTROL SETUP

A SNMP **Access Control** is the IP address of the radio used by an SNMP manager or any other SNMP device to access the radio. The Aprisa SR+ allows access to the radio from any IP address.

Read Only

The default Read Only community string is public.

Read Write

The default ReadWrite community string is private.

SNMP Manager Setup

The SNMP manager community strings must be setup to access the base station and remote / repeater stations.

To access the base station, a community string must be setup on the SNMP manager the same as the community string setup on the radio (see 'Security > SNMP' on page 179).

SNMP access to remote / repeater stations can be achieved by using the radio's IP address and the normal community string or by proxy in the base station.

SNMP Access via Base Station Proxy

To access the remote / repeater stations via the base station proxy, the community strings must be setup on the SNMP manager in the format:

cccccccc:bbbbbb

Where:

cccccccc is the community string of the base station

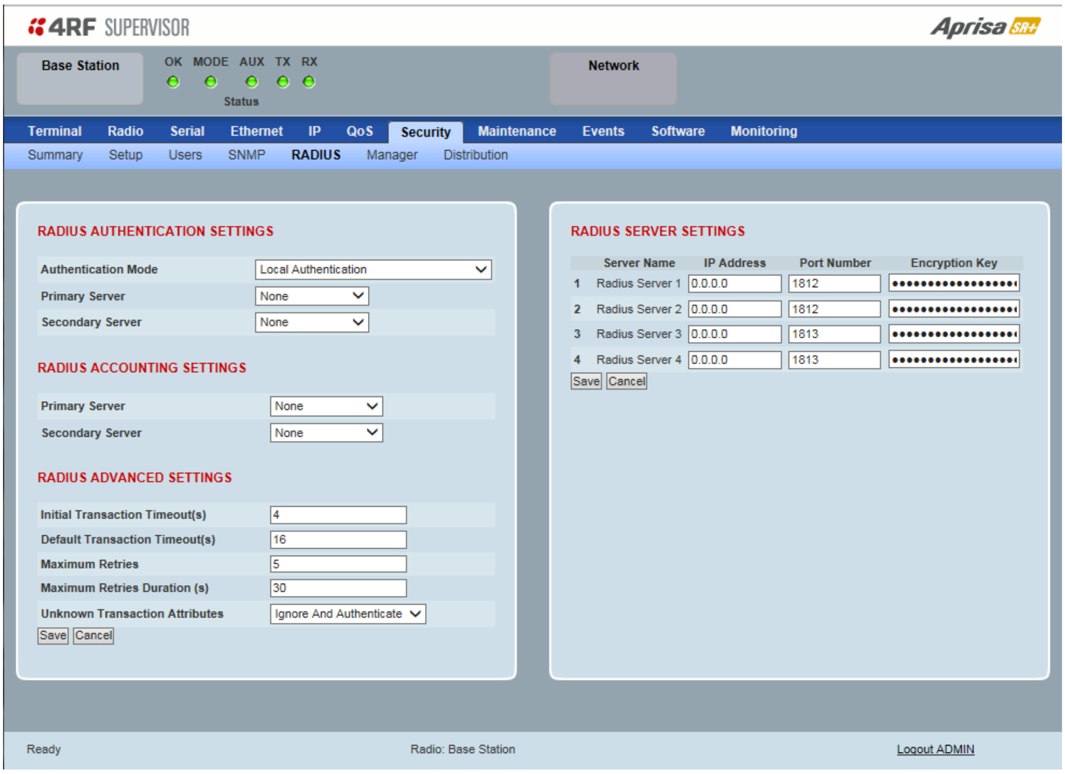
and

bbbbbb is the last 3 bytes of the remote station MAC address (see 'Network Status > Network Table' on page 254).

The SNMP Proxy Support must be enabled for this method of SNMP access to operate (see 'SNMP Proxy Support' on page 172).

Security > RADIUS

This page displays the current settings for the Security RADIUS.



RADIUS - Remote Authentication Dial In User Service

RADIUS is a client / server system that secures the Aprisa SR+ radio network against unauthorized access. It is based on open standard RFCs: RFC 2865/6, 5607, 5080 and 2869.

It is a protocol for remote user Authorization, Authentication and Accounting. A standard RADIUS interface is typically used in a pulled model in which the request (authentication query) originates from the radio (RADIUS client or Network Access Server (NAS)) attached to a network and the response is sent from the queried RADIUS servers.

When a radio client is configured to use RADIUS, any user of the radio client presents authentication information to the radio client. This might be with a CLI login prompt or window login (SuperVisor/NMS), where the user is expected to enter their username and password.

RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

User accounting information is delivered from the RADIUS client/NAS to a RADIUS accounting server during RADIUS authentication and authorization operation and transaction.

Transactions between the RADIUS client/NAS and RADIUS AAA server/accounting server are authenticated through the use of a shared secret, which is never sent over the network.

For a RADIUS server to respond to the Aprisa SR+ radio, it must configured with and respond to the following **Management-Privilege-level** attributes:

Admin Level = 4
Engineer Level = 3
Technician Level = 2
Viewer Level = 1

RADIUS AUTHENTICATION SETTINGS

Authentication Mode

This parameter sets the Authentication Mode.

Option	Function
Local Authentication	No radius Authentication – allows any local user privilege
Radius Authentication	Only radius Authentication – no local user privilege
Radius Authentication and Local admin	Uses radius Authentication if it is available. If radius Authentication is not available, uses local Admin login
Radius Then Local Authentication	If the user is not authenticated in the radius server, it allows any local user privilege.
Local Then Radius Authentication	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 (MRC)

This parameter sets the maximum number of retry attempts when the server is not responding.

Maximum Retries Duration (MRD) (seconds)

This parameter sets the maximum duration it will attempt retries when the server is not responding.

Unknown Transaction Attributes

This parameter sets the radio'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.

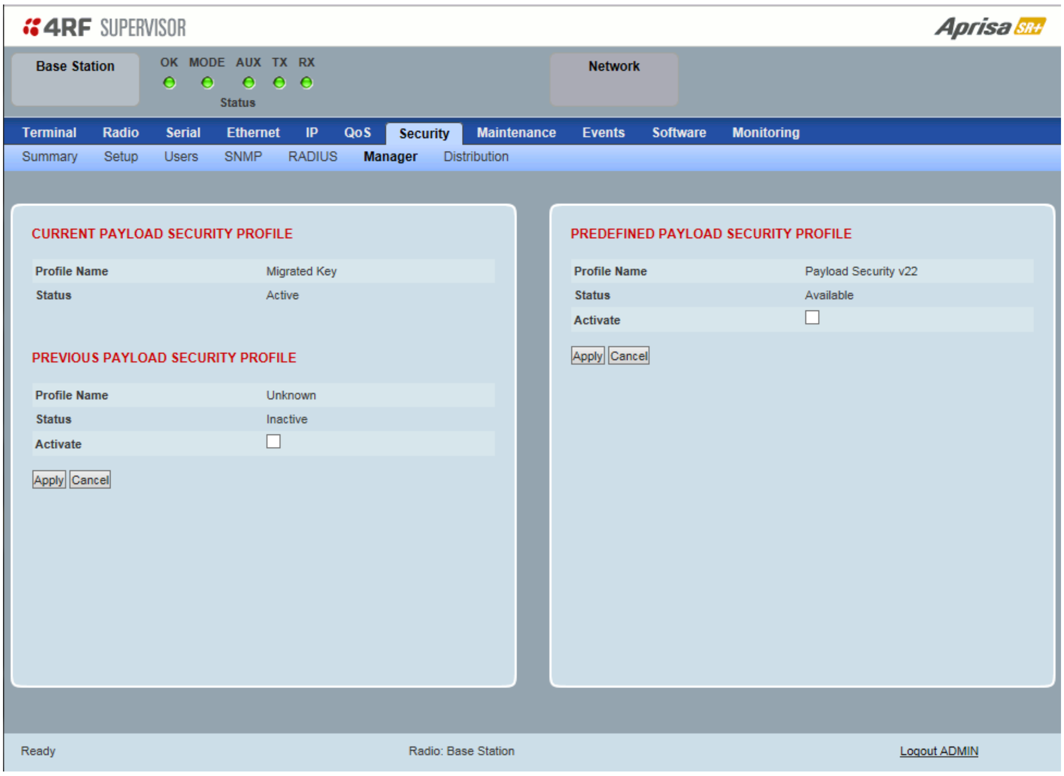
- UDP port 1812 is used for authentication / authorization
- UDP port 1813 is used for accounting.

Old RADIUS servers may use unofficial UDP ports 1645 and 1646.

Encryption Key

The password of the Radius server.

Security > Manager



CURRENT PAYLOAD SECURITY PROFILE

Profile Name

This parameter shows the predefined security profile active on the radio.

Status

This parameter displays the status of the predefined security profile on the radio (always active).

PREVIOUS PAYLOAD SECURITY PROFILE

Profile Name

This parameter displays the security profile that was active on the radio prior to the current profile being activated.

Status

This parameter displays the status of the security profile that was active on the radio prior to the current profile being activated.

Option	Function
Active	The security profile is active on the radio.
Inactive	The security profile is not active on the radio but could be activated if required.

Activate

This parameter activates the previous security profile (restores to previous version).

PREDEFINED PAYLOAD SECURITY PROFILE

Profile Name

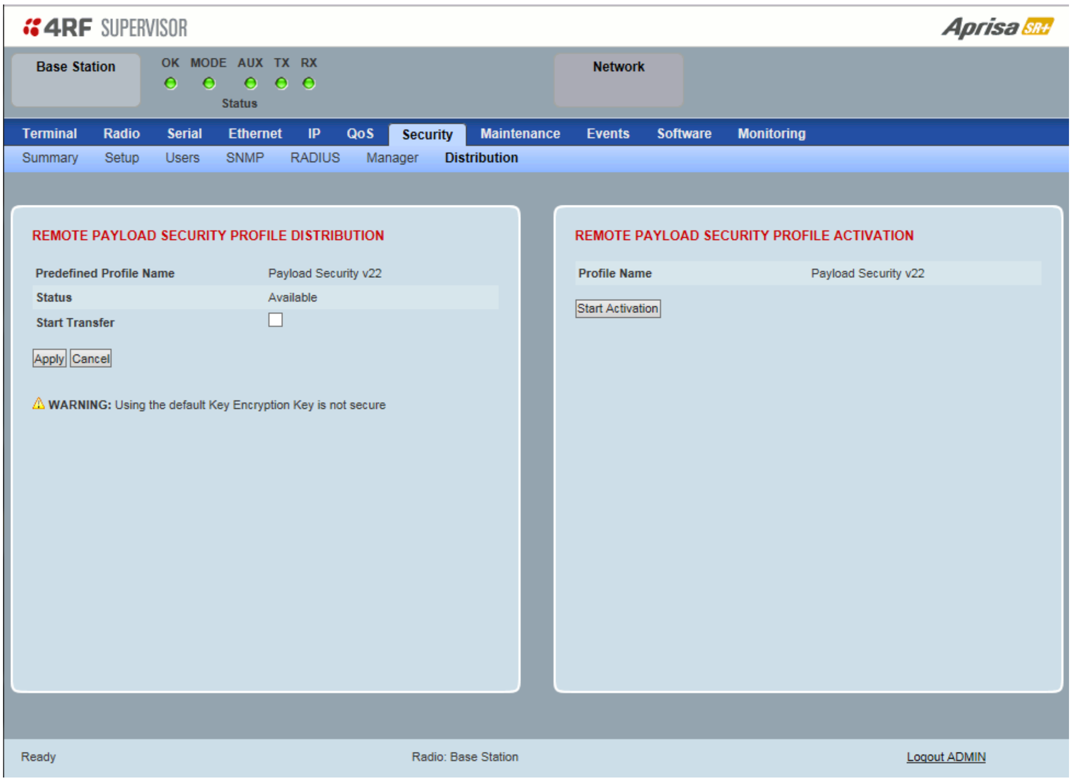
This parameter displays the new security profile that could be activated on the radio or distributed to all remote radios with Security > Distribution.

Status

This parameter displays the status of the new security profile.

Option	Function
Unavailable	A predefined security profile is not available on this radio. To create a predefined security profile, go to 'Security > Setup' on page 168.
Available	A predefined security profile is available on this radio for distribution and activation.

Security > Distribution



REMOTE PAYLOAD SECURITY PROFILE DISTRIBUTION

Predefined Profile Name

This parameter displays the predefined security profile available for distribution to remote stations.

Status

This parameter shows if a predefined security profile is available for distribution to remote stations.

Option	Function
Unavailable	A predefined payload security profile is not available on this radio.
Available	A predefined payload security profile is available on this radio for distribution and activation.

Start Transfer

This parameter when activated distributes (broadcasts) the new payload security profile to all remote stations in the network.

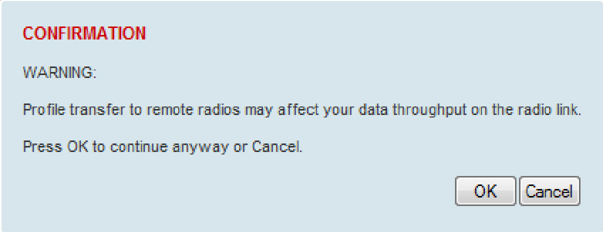
Note: The distribution of the payload security profile to remote stations does not stop customer traffic from being transferred.

Payload security profile distribution traffic is classified as 'management traffic' but does not use the Ethernet management priority setting. Security profile distribution traffic priority has a fixed priority setting of 'very low'.

To distribute the payload security profile to remote stations:

This process assumes that a payload security profile has been setup (see 'Security > Setup' on page 168).

1. Tick Start Transfer and click Apply.



Note: This process could take up to 1 minute per radio depending on channel size, Ethernet Management Priority setting and the amount of customer traffic on the network.

---

2. When the distribution is completed, activate the software with the Remote Payload Security Profile Activation.

REMOTE PAYLOAD SECURITY PROFILE ACTIVATION

When the security profile has been distributed to all the remote stations, the security profile is then activated in all the remote stations with this command.

The base station will always attempt to distribute the profile successfully. This broadcast distribution has its own retry mechanism. The user can find out if all the remote radios have the latest profile when the managed activation process is attempted. A pop up confirmation will be shown by SuperVisor with relevant information and the user can decide to proceed or not. The user can attempt to redistribute again if needed. If the decision is made to continue, on completion of the activation process, communication with the remote radios that did not have the new security profile will be lost.

Predefined Profile Name

This parameter displays the predefined security profile available for activation on all remote stations.

To activate the security profile in remote stations:

This process assumes that a security profile has been setup into the base station (see ‘Security > Setup’ on page 168) and distributed to all remote radios in the network.

Note: Do not navigate SuperVisor away from this page during the activation process (SuperVisor can lose PC focus).

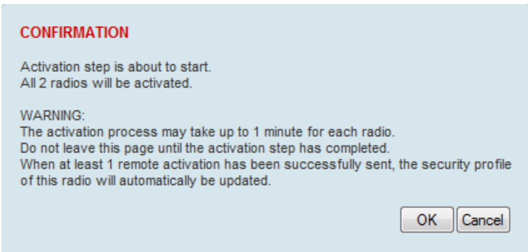
---

1. Click Start Activation

The remote stations will be polled to determine which radios require activation:

Result	Function (X of Y)
Remote Radios Polled for New Profile	X is the number of radios polled to determine if the radio contains the new security profile. Y is the number of remote radios registered with the base station.
Remote Radios Activated	X is the number of radios activated. Y is the number of radios with the new security profile requiring activation.
Remote Radios On New Profile	X is the number of radios activated and on the new security profile. Y is the number of radios with the new security profile that have been activated.

When the activation is ready to start:

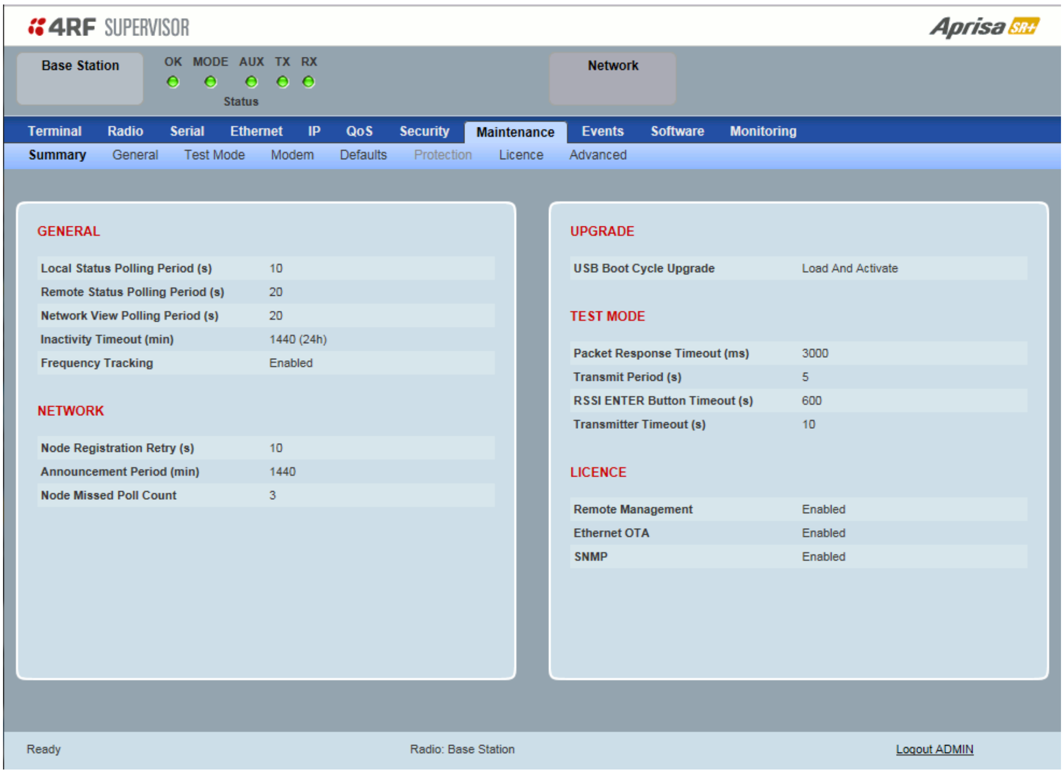


3. Click on ‘OK’ to start the activation process or Cancel to quit.

Maintenance

Maintenance > Summary

This page displays the current settings for the Maintenance parameters.



DIAGNOSTICS

Last RX Packet RSSI (dBm)

This parameter displays the receiver RSSI reading taken from the last data packet received.

GENERAL

Local Status Polling Period (sec)

This parameter displays the rate at which SuperVisor refreshes the Local Radio alarm LED states and RSSI value.

Remote Status Polling Period (sec)

This parameter displays the rate at which SuperVisor refreshes the Remote Radio alarm LED states and RSSI value.

Network View Polling Period (sec)

This parameter displays the rate at which SuperVisor polls all remote radios for status and alarm reporting.

Inactivity Timeout (min)

This parameter displays the period of user inactivity before SuperVisor automatically logs out of the radio.

Frequency Tracking

This parameter displays if Frequency Tracking is enabled or disabled.

NETWORK

Node Registration Retry (sec)

This parameter displays the base station poll time at startup or the remote / repeater station time between retries until registered.

Base Station Announcement Period (min)

This parameter displays the period between base station polls post startup. The default setting is 1440 minutes (24 hours).

Node Missed Poll Count

This parameter displays the number of times the base station attempts to poll the network at startup or if a duplicate IP is detected when a remote / repeater station is replaced.

UPGRADE

USB Boot Cycle Upgrade

This parameter shows the type of USB Boot Cycle upgrade defined in 'Software Setup > USB Boot Upgrade' on page 221.

TEST MODE

Packet Response Timeout (ms)

This parameter displays the time Test Mode waits for a response from the base station before it times out and retries.

Transmit Period (sec)

This parameter displays the time between Test Mode requests to the base station.

Response Timeout (ms)

This parameter sets the time Test Mode waits for a response from the base station before it times out and retries. The default setting is 3000 ms.

RSSI Enter Button Timeout (sec)

This parameter displays the Test Mode timeout period. The radio will automatically exit Test Mode after the Timeout period.

Transmitter Timeout (sec)

This parameter displays the transmitter Test Mode timeout period. The radio will automatically exit the transmitter Test Mode after the Timeout period.

LICENCE

Remote Management

This parameter displays if Remote Management is enabled or disabled. The default setting is enabled.

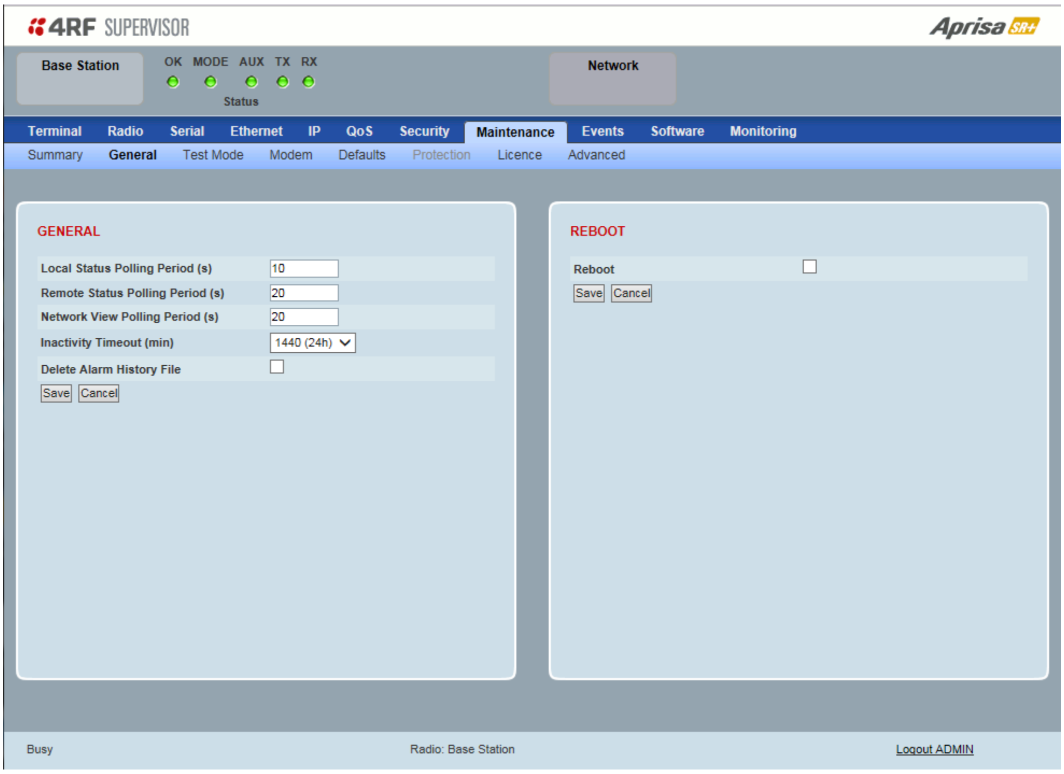
Ethernet OTA (over the air)

This parameter displays if Ethernet traffic is enabled or disabled. The Ethernet OTA will be enabled if the Ethernet feature licence has been purchased (see ‘Maintenance > Licence’ on page 201).

SNMP Management

This parameter displays if SNMP management is enabled or disabled. The default setting is enabled.

Maintenance > General



GENERAL

Local Status Polling Period (sec)

This parameter sets the rate at which SuperVisor refreshes the Local Radio alarm LED states and RSSI value. The default setting is 10 seconds.

Network View Polling Period (sec)

This parameter sets the rate at which SuperVisor polls all remote radios for status and alarm reporting. The default setting is 20 seconds.

Remote Status Polling Period (sec)

This parameter sets the rate at which SuperVisor refreshes the Remote Radio alarm LED states and RSSI value. To avoid problems when managing Aprisa SR+ Networks, ensure that the Remote Polling Period is set to be longer than the Inband Management Timeout (set on page 85). The default setting is 20 seconds.

Inactivity Timeout (min)

This parameter sets the period of user inactivity before SuperVisor automatically logs out of the radio. The default setting is 15 minutes.

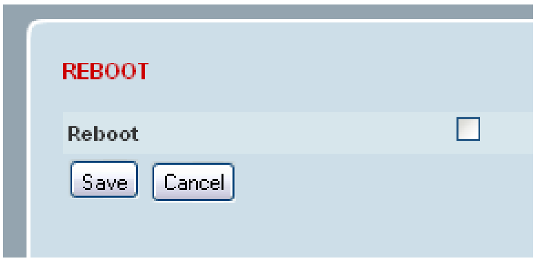
Delete Alarm History file

This parameter when activated deletes the alarm history file stored in the radio.

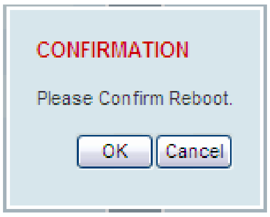
REBOOT

To reboot the radio:

1. Select Maintenance > General.
2. Tick the 'Reboot' checkbox.



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



4. Click 'OK' to reboot the radio or 'Cancel' to abort.

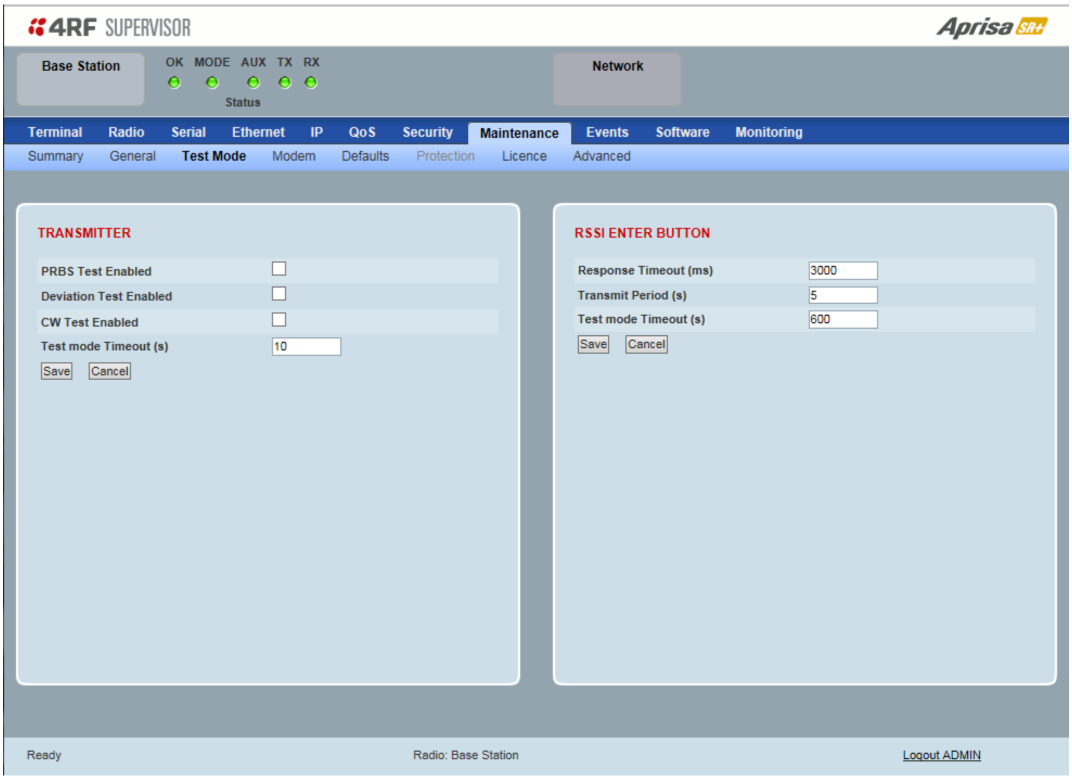
All the radio LEDs will flash repeatedly for 1 second.

The radio will be operational again in about 10 seconds.

The OK, MODE, and AUX LEDs will light green and the TX and RX LEDs will be green (steady or flashing) if the network is operating correctly.

5. Login to SuperVisor.

Maintenance > Test Mode



TRANSMITTER

PRBS Test Enabled

When active, the transmitter outputs a continuous PRBS signal. This can be used for evaluating the output spectrum of the transmitter and verifying adjacent channel power and spurious emission products.

Deviation Test Enabled

When active, the transmitter outputs a sideband tone at the deviation frequency used by the CPFSK modulator. This can be used to evaluate the local oscillator leakage and sideband rejection performance of the transmitter.

CW Test Enabled

When active, the transmitter outputs a continuous wave signal. This can be used to verify the frequency stability of the transmitter.

Test Mode Timeout (s)

This parameter sets the Transmitter Test Mode timeout period. The radio will automatically exit Transmitter Test Mode after the Timeout period. The default setting is 10 seconds.

RSSI TEST BUTTON

Response Timeout (ms)

This parameter sets the time RSSI Test Mode waits for a response from the base station before it times out and retries. The default setting is 3000 ms.

Transmit Period (sec)

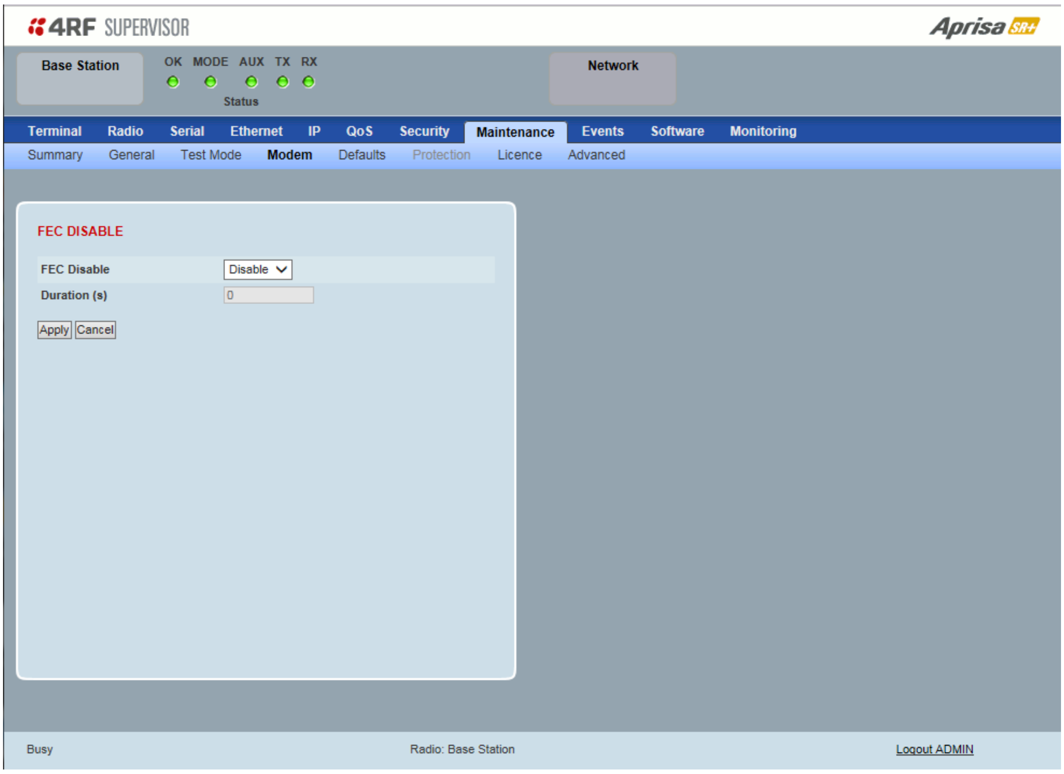
This parameter sets the time between RSSI Test Mode requests to the base station. The default setting is 5 seconds.

Test Mode Timeout (s)

This parameter sets the RSSI Test Mode timeout period. The radio will automatically exit RSSI Test Mode after the Timeout period. The default setting is 600 seconds.

Maintenance > Modem

Base Station



FEC DISABLE

FEC Disable

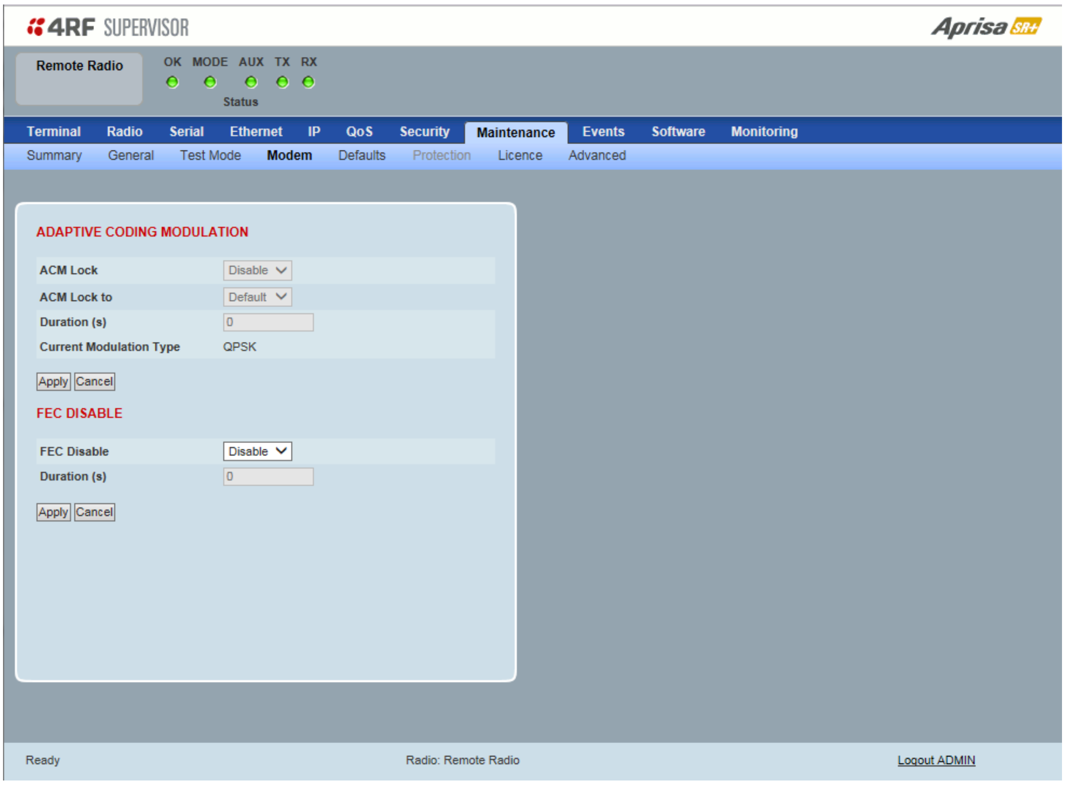
This parameter sets whether the Forward Error Correction can be disabled.

Option	Function
Enable	Enables the FEC Disable diagnostic function
Disable	Disables the FEC Disable diagnostic function
Timer	Allows the FEC to be disabled but only for a predetermined period.

Duration (s)

This parameter defines the period required for disabling of the FEC. When this period elapses, the FEC is enabled.

Remote Station



ADAPTIVE CODING MODULATION

ACM Lock

This parameter sets whether adaptive modulation can be locked or not.

Option	Function
Disable	Disables manual locking of the adaptive modulation i.e. allows for automatic adaptive modulation.
Enable	Allows the adaptive modulation to be manually locked
Timer	Allows the adaptive modulation to be manually locked but only for a predetermined period.

ACM Lock To

This parameter manually locks the adaptive modulation.

Option	Function
Default	Manually locks the adaptive modulation to the default modulation defined in 'Default Modulation' on page 106.
Current	Manually locks the adaptive modulation to the current modulation at that time.

Duration (s)

This parameter defines the period required for manually locking the adaptive modulation. When this period elapses, the adaptive modulation becomes automatic.

FEC DISABLE

FEC Disable

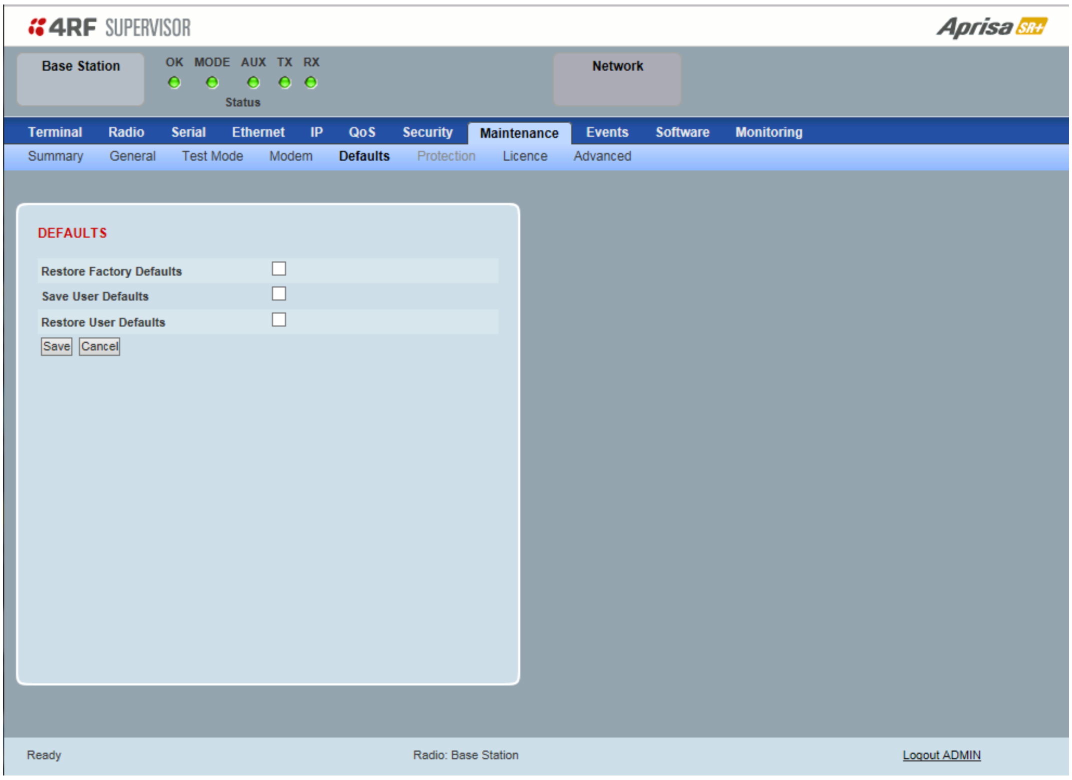
This parameter sets whether the Forward Error Correction can be disabled.

Option	Function
Enable	Enables the FEC Disable diagnostic function
Disable	Disables the FEC Disable diagnostic function
Timer	Allows the FEC to be disabled but only for a predetermined period.

Duration (s)

This parameter defines the period required for disabling of the FEC. When this period elapses, the FEC is enabled.

Maintenance > Defaults

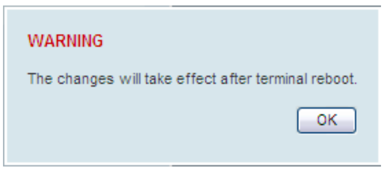


DEFAULTS

The Maintenance Defaults page is only available for the local terminal.

Restore Factory Defaults

When activated, all radio parameters will be set to the factory default values. This includes resetting the radio IP address to the default of 169.254.50.10.



Note: Take care using this command.

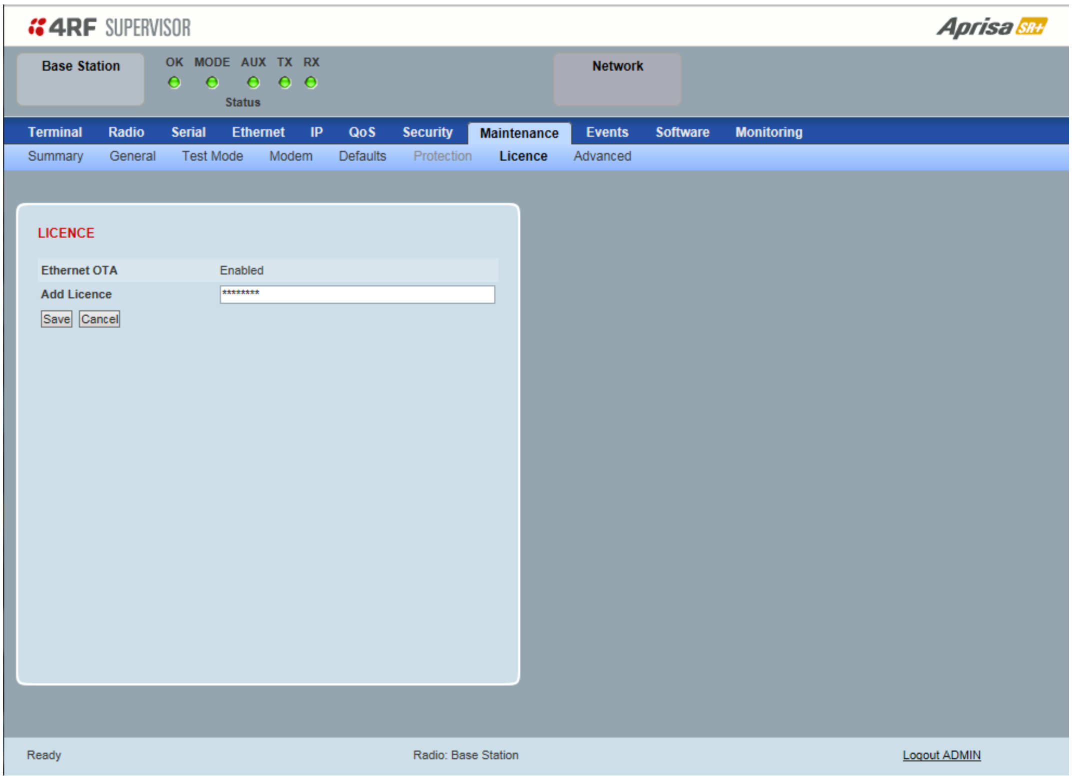
Save User Defaults

When activated, all current radio parameter settings will be saved to non-volatile memory within the radio.

Restore User Defaults

When activated, all radio parameters will be set to the settings previously saved using ‘Save User Defaults’.

Maintenance > Licence



LICENCE

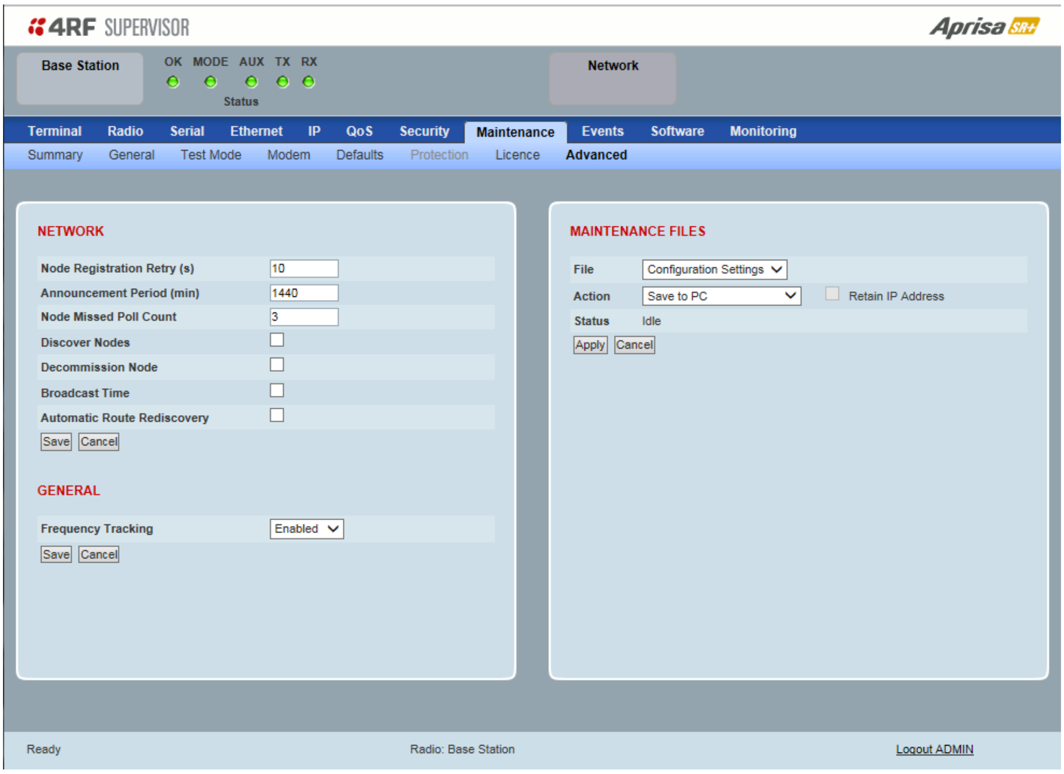
Fully Featured Radio

When a fully featured Aprisa SR+ radio is purchased (indicated by the AA), it contains the licences which activate Remote Management, Ethernet Traffic, and SNMP Management e.g.

Part Number	Part Description
APSQ-N400-SSC-HD-22-ENAA	4RF SR+, BR, 400-470 MHz, SSC, Half Duplex, 2E2S, EN, STD

In this software version, Remote Management, Ethernet Traffic and SNMP management are enabled by default.

Maintenance > Advanced



NETWORK

Node Registration Retry (sec)

This parameter sets the base station poll time at startup or the remote / repeater station time between retries until registered. The default setting is 10 seconds.

Base Station Announcement Period (min)

This parameter sets the period between base station polls post startup. The default setting is 1440 minutes (24 hours).

When a new base station powers on, it announces its presence and each remote that receives the announcement message will be advised that a new base station is present and that they should re-register. This allows the new base station to populate its Network Table, with knowledge of the nodes in the network.

If, during this initial period, there is some temporary path disturbance to one or more remotes, they may miss the initial announcement messages and be left unaware of the base station change. For this reason, the base station must periodically send out announcement messages to pick up any stray nodes and the period of these messages is the base station Announcement Period.

Setting this parameter to 0 will stop periodic announcement messages being transmitted.

If a critical parameter is changed in the base station, such as IP address, then the change is distributed to the network using base station announcement message. Note that in this case, an announcement is sent immediately independent of the Announcement Period setting.

Node Missed Poll Count

This parameter sets the number of times the base station attempts to poll the network at startup or if a duplicate IP is detected when a remote / repeater station is replaced. The default setting is 3.

Discover Nodes

This parameter when activated triggers the base station to poll the network with Node Missed Poll Count and Node Registration Retry values.

Decommission Node(s)

This parameter when activated resets the network registrations to remove the entire network from service.

Note: Take care using this option.

Broadcast Time

This parameter when activated sends the base station Date / Time setting to all the remote and repeater stations in the network and sets their Date / Time. This option applies to the base station only.

Automatic Route Rediscovery

This parameter enables the radio to transmit route discovery messages when packets are unacknowledged.

When enabled, unacknowledged unicast packets are converted into uni-broadcast messages and sent through the network. All nodes see the message and populate their routing tables accordingly.

When the destination node is reached, it sends a route response message via the shortest path. The intermediate nodes see this message and populate their routing tables in the reverse direction, thus re-establishing the route.

The default setting is disabled.

GENERAL

Frequency Tracking

Frequency Tracking enables the receiver to track any frequency drift in the transmitter to maintain optimum SNR and radio link performance over the full temperature range.

When enabled, remote stations adjust their receive frequency to the frequency of the incoming packet rate and the base station notifies remote stations if their transmit frequency requires adjustment.

The default setting is Enabled.

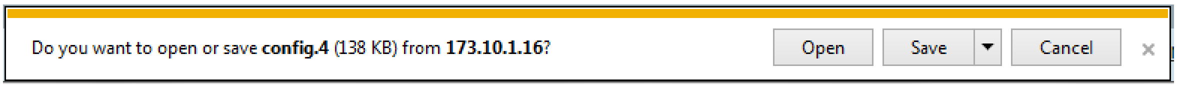
MAINTENANCE FILES

There are three maintenance file types which can saved / restored to / from PC or USB flash drive:

File - Configuration Settings

Action

Action	Option
Save to PC	This saves the file with a filename of 'Config.4' to a binary encrypted file. This can then be saved from the Browser popup (example is Windows Internet Explorer 11). The file should be renamed to be able to identify the radio it was saved from.



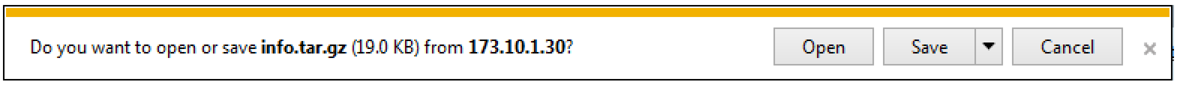
Save to Radio USB	This saves the file with a filename of 'asrcfg_1.5.2' to a binary encrypted file on the radio USB flash drive root directory.
Restore from PC	This restores all user configuration settings from a binary encrypted file on a PC directory to the radio. A reboot warning message will warn 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.
Restore from Radio USB	This restores all user configuration settings from a binary encrypted file on the USB root directory to the radio.

Note: 'Payload Encryption Key' and 'Key Encryption Key' parameters (see 'Security > Setup') are not saved to the configuration file. When a 'Restore from PC' or 'Restore from Radio USB' is used, these parameters will retain their existing values so are not changed by the operation of restoring the configuration file.

File - Event History Log

Action

Action	Option
Save to PC	This saves the file with a filename of 'Info.tar.gz' to a binary encrypted file. This can then be saved from the Browser popup (example is Windows Internet Explorer 11). The file should be renamed to be able to identify the radio it was saved from. The 'gz' file is normally for sending back to 4RF Limited for analysis but can be opened with WinRar.



Save to Radio USB	This saves the file with a filename of e.g. 'alarm_173.10.1.30_2014-11-10,15.54.14.txt' to a text file on the radio USB flash drive root directory.

File - Configuration Script

Action

Action	Option
Load and Execute	This loads and executes configuration script files. There are sample configuration script files on the product CD in a directory called ‘Master Configuration’. The purpose of these files is to use as templates to create your own configuration scripts. Note: Be careful using this feature as incompatible configurations will change the radios settings and break radio connectivity.

Note: Activating this function will over-write all existing configuration settings in the radio (except for the non-saved settings e.g. security passwords, licence keys etc) without any verification of the command setting in the radio. Precautions should be taken to prevent radio outages with incorrect radio configurations. The following process steps are recommended:

a. Save the current radio configuration to a PC or USB before uploading the new configuration script file

b. Upload the new configuration script file to the radio

c. If for some reason the radio doesn’t work as expected, the saved configuration file can be uploaded to the radio (roll back to previous configuration).

Retain IP Address

This parameter when enabled ensures that the radio IP address is not changed when the radio configuration settings are restored from a configuration file with a different IP radio address. It prevents the radio losing connectivity when the configuration settings are restored from a configuration file.

Revert Config if Connection Lost

When the Maintenance Files feature is used on remote radios from the base station, this parameter allows the configurations to be restored to the previous configuration if the connection is lost.

This must be set before executing the Configuration Settings / Configuration Script restore functions.

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 SR+ radio. These are:

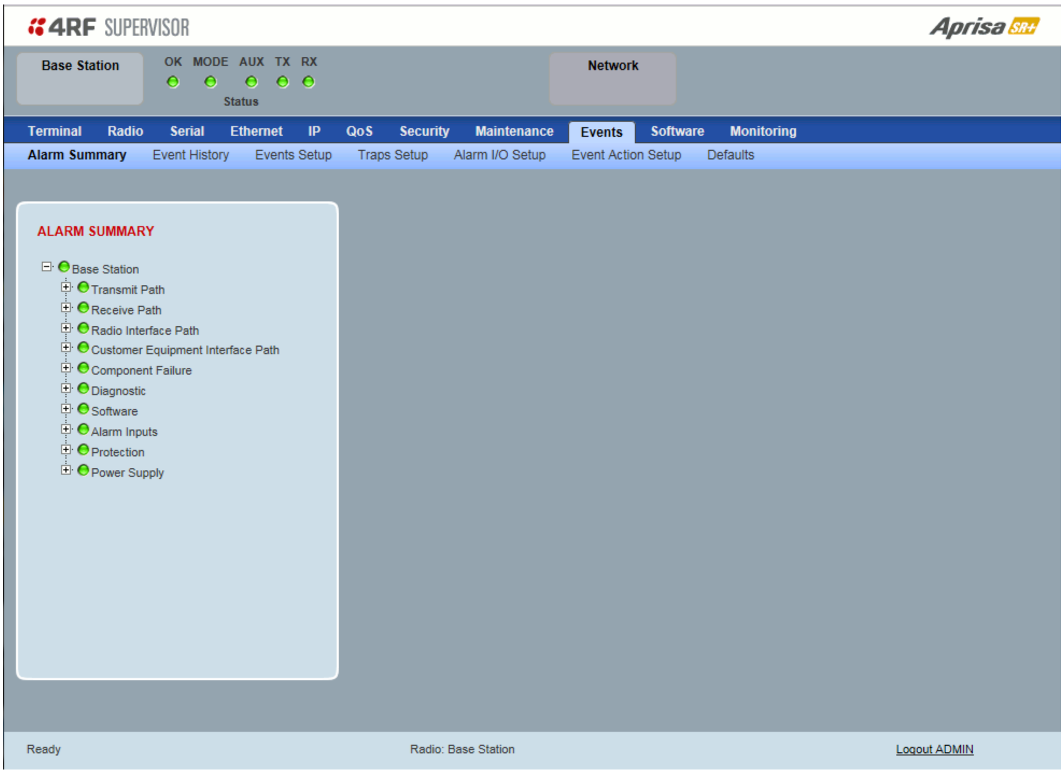
1. Alarm Events

Alarm Events are generated to indicate a problem on the radio.

2. Informational Events

Informational Events are generated to provide information on key activities that are occurring on the radio. These events do not indicate an alarm on the radio and are used to provide information only.

See 'Alarm Types and Sources' on page 350 for a complete list of events.

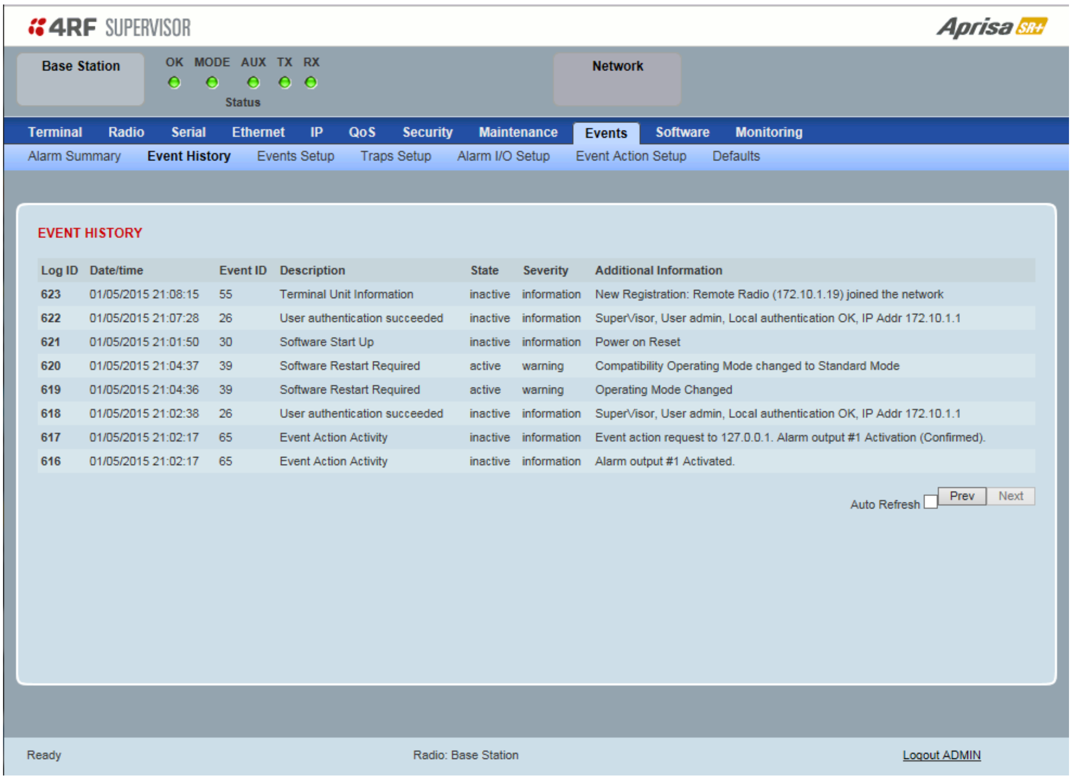


ALARM SUMMARY

The Alarm Summary is a display tree that displays the current states of all radio 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 > Event History



Log ID	Date/time	Event ID	Description	State	Severity	Additional Information
623	01/05/2015 21:08:15	55	Terminal Unit Information	inactive	information	New Registration: Remote Radio (172.10.1.19) joined the network
622	01/05/2015 21:07:28	26	User authentication succeeded	inactive	information	SuperVisor, User admin, Local authentication OK, IP Addr 172.10.1.1
621	01/05/2015 21:01:50	30	Software Start Up	inactive	information	Power on Reset
620	01/05/2015 21:04:37	39	Software Restart Required	active	warning	Compatibility Operating Mode changed to Standard Mode
619	01/05/2015 21:04:36	39	Software Restart Required	active	warning	Operating Mode Changed
618	01/05/2015 21:02:38	26	User authentication succeeded	inactive	information	SuperVisor, User admin, Local authentication OK, IP Addr 172.10.1.1
617	01/05/2015 21:02:17	65	Event Action Activity	inactive	information	Event action request to 127.0.0.1. Alarm output #1 Activation (Confirmed).
616	01/05/2015 21:02:17	65	Event Action Activity	inactive	information	Alarm output #1 Activated.

EVENT HISTORY

The last 1500 events are stored in the radio. The complete event list can be downloaded to a USB flash drive (see 'File - Event History Log' on page 205).

The Event History can display the last 50 events stored in the radio in blocks of 8 events.

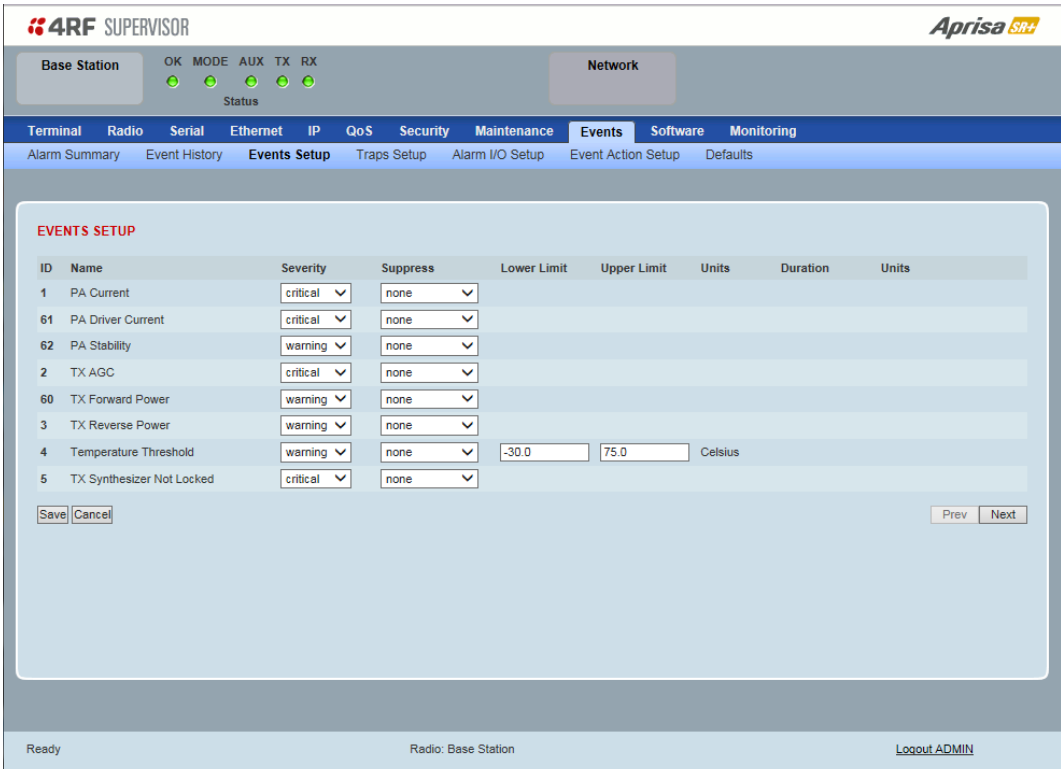
The Next button will display the next page of 8 events and the Prev button will display the previous page of 8 events. Using these buttons will disable Auto Refresh to prevent data refresh and page navigation contention.

The last 50 events stored in the radio are also accessible via an SNMP command.

Auto Refresh

The Event History page selected will refresh automatically every 12 seconds if the Auto Refresh is ticked.

Events > Events Setup



EVENTS SETUP

Alarm event parameters can be configured for all alarm events (see 'Alarm Events' on page 351).

All active alarms for configured alarm events will be displayed on the Monitoring pages (see 'Monitoring' on page 236).

This Switch and Block parameters are only visible / applicable when the radio is part of a Protected Station.

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.
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 radio
Traps	Alarm is logged in the radio but does not trigger an event trap
Traps and Log	Alarm neither triggers an event trap nor is logged in the radio

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: 9 RX CRC Errors

The Upper Limit is set to 0.7 and the Duration is set to 5 seconds.

If in any 5 second period, the total number of errored packets divided by the total number of received packets exceeds 0.7, 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.

Switch

This parameter determines if the alarm when active causes a switch over of the Protection Switch.

This parameter is only applicable when the radio is part of a Protected Station.

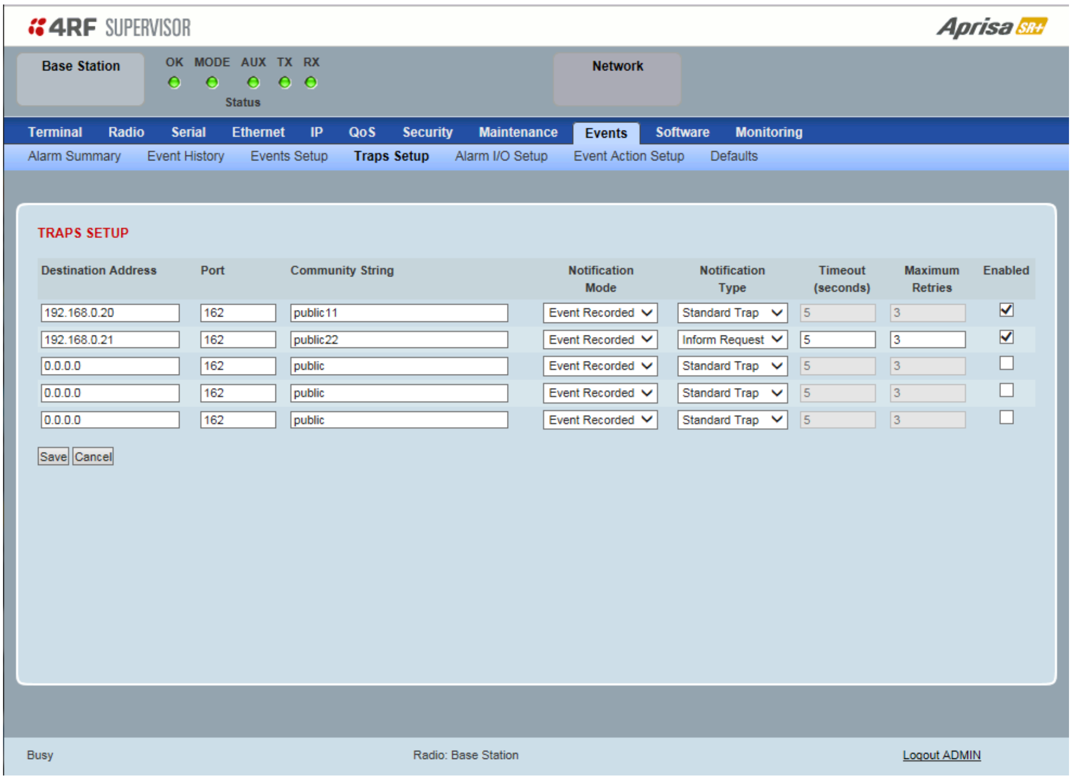
Block

This parameter determines if the alarm is prevented from causing a switch over of the Protection Switch.

This parameter is only applicable when the radio is part of a Protected Station.

The Next button will display the next page of 8 alarm events and the Prev button will display the previous page of 8 alarm events.

Events > Traps Setup



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
None	No event related traps are sent.
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

Notification Type set to Inform Request:

Timeout (second)

This parameter sets the time interval to wait for an acknowledgement before sending another retry.

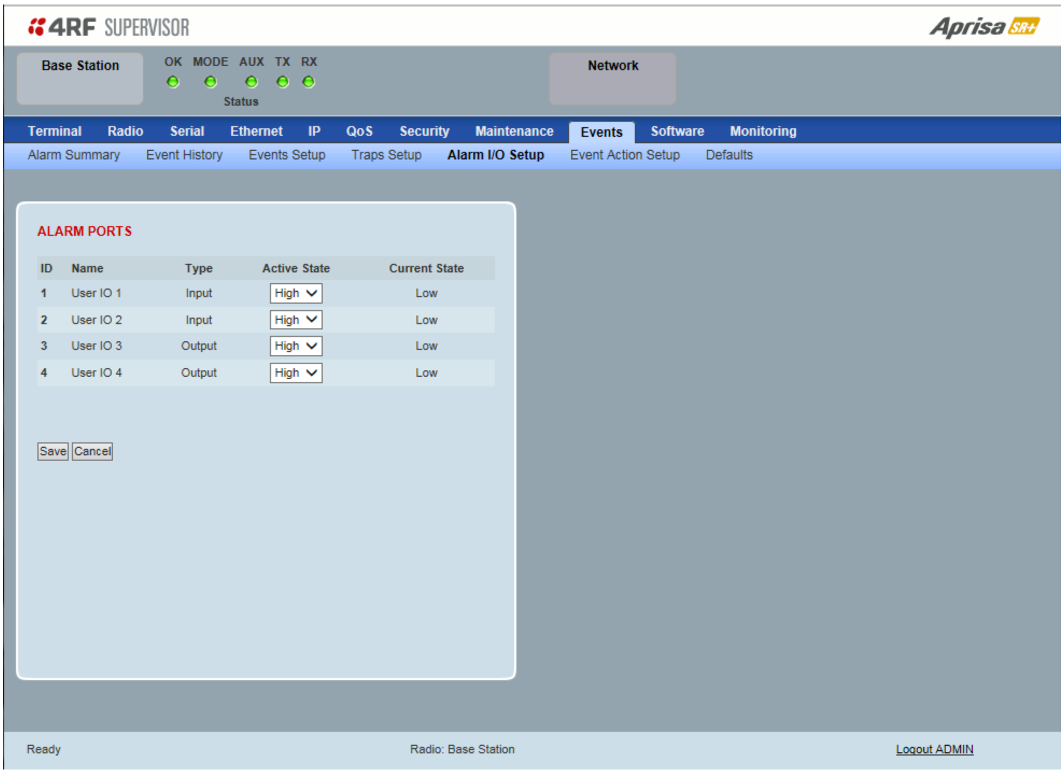
Maximum Retries

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



ALARM PORTS

This page provides control of the two hardware alarm inputs and two hardware alarm outputs provided on the alarm connector.

The alarm inputs are used to transport alarms to the other radios in the network. The alarm outputs are used to receive alarms from other radios in the network.

These alarms are only available when the station is non protected.

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 is active.

Alarm Input

Option	Function
Low	The alarm is active low i.e. a ground contact on the port will cause an active alarm state
High	The alarm is active high i.e. an open contact on the port will cause an active alarm state

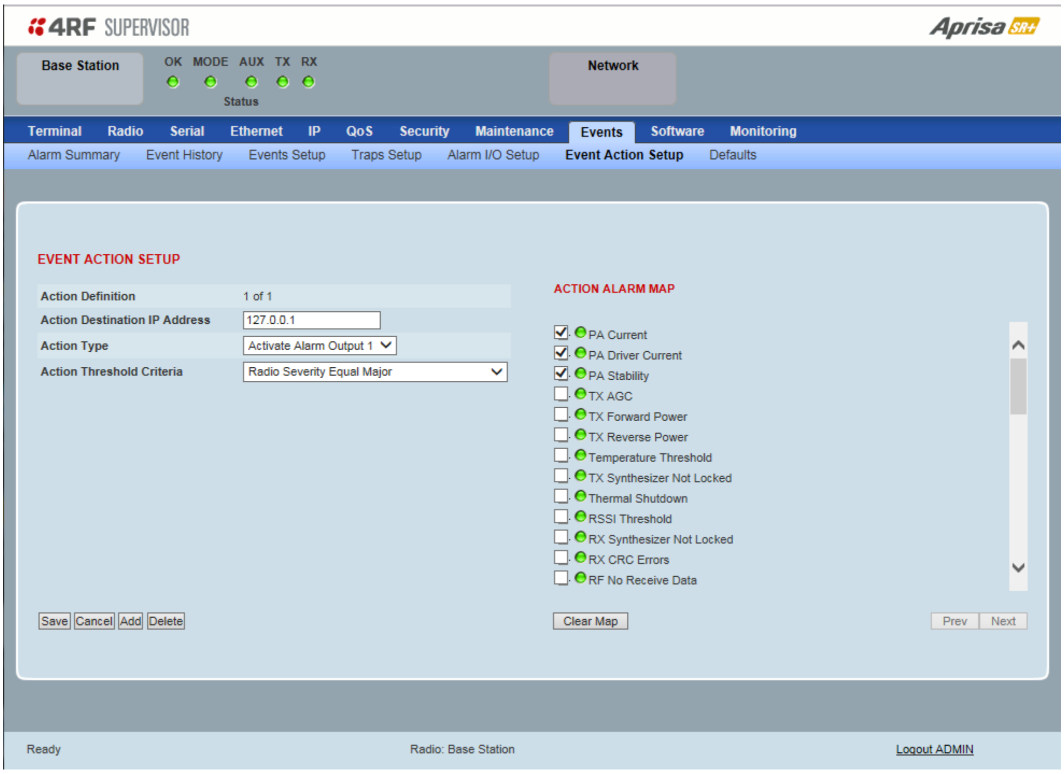
Alarm Output

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 generate a open contact output

Current State

The Current State shows the current state of the alarm.

Events > Event Action Setup



EVENT ACTION SETUP

This page provides control of the mapping of events to specific actions. Specific alarm events can setup to trigger outputs.

Action Definition

This parameter shows the number of the event action setup and the maximum number of setups stored.

Action Destination IP Address

This parameter sets the IP address of the radio that will output the action type.

Action Type

This parameter sets the action type that will be activated on the radio.

Option	Function
None	This action setup does not activate any alarm output
Activate Alarm Output 1	This action setup activates alarm output 1
Activate Alarm Output 2	This action setup activates alarm output 2

Action Threshold Criteria

This parameter sets the radio event that will trigger the action output.

Option	Function
None	No action output.
Radio Severity Equal Critical	Activates the action output when a radio alarm is critical alarm
Radio Severity Equal Major	Activates the action output when a radio alarm is a major alarm
Radio Severity Equal Minor	Activates the action output when a radio alarm is minor alarm
Radio Severity Equal Warning	Activates the action output when a radio alarm is a warning alarm
Radio Severity Equal Cleared	Activates the action output when a radio alarm is cleared
Radio Severity Equal or Worse than Major	Activates the action output when a radio alarm is a major alarm or a critical alarm
Radio Severity Equal or Worse than Minor	Activates the action output when a radio alarm is a minor alarm, a major alarm or a critical alarm
Radio Severity Equal or Worse than Warning	Activates the action output when a radio 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 Add button adds a new event action setup.

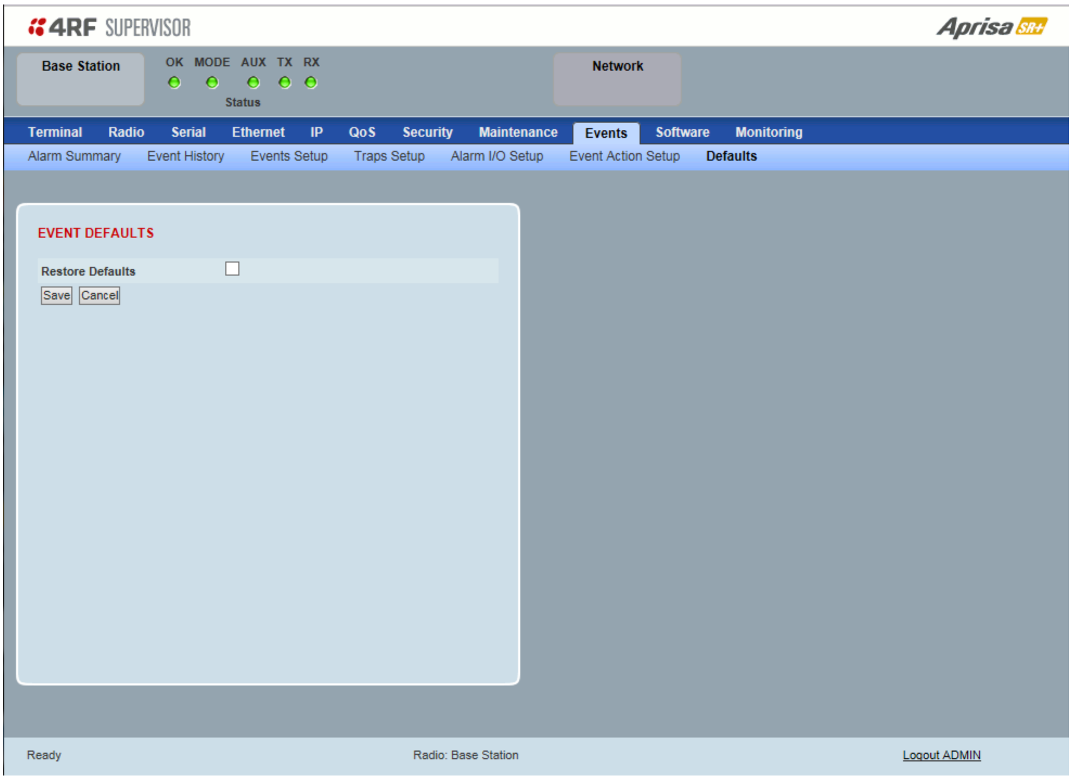
The Delete button deletes the current event action setup.

The Clear Map button clears all alarm selections on the current setup.

To add an event action setup:

1. Click on the Add button.
2. Enter the Action Destination IP Address. This is the IP address of the radio that will output the action type.
3. Select the Action Type from the list.
4. Select the Action Threshold Criteria from the list.
5. Tick the alarms required for the event action setup from the Action Alarm Map. You can clear all alarm selections with the Clear Map button.
6. Click on Save.

Events > Defaults



EVENT DEFAULTS

Restore Defaults

This parameter when activated restores all previously configured event parameters using ‘Events > Events Setup’ to the factory default settings.

Software

The Software menu contains the setup and management of the system software including network software distribution and activation. The distribution of the system software to the remote radios is encrypted by the AES session key over-the-air.

Single Radio Software Upgrade

The radio software can be upgraded on a single Aprisa SR+ radio (see ‘Single Radio Software Upgrade’ on page 344). This process would only be used if the radio was a replacement or a new station in an existing network.

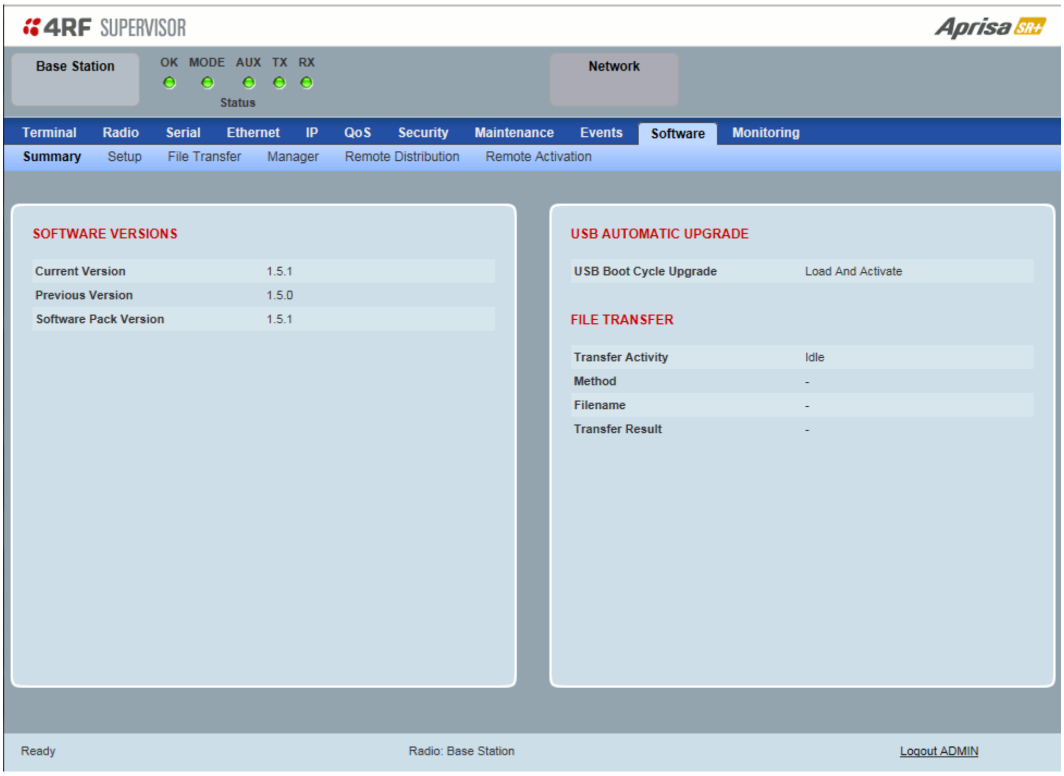
Network Software Upgrade

The radio software can be upgraded on an entire Aprisa SR+ radio network remotely over the radio link (see ‘Network Software Upgrade’ on page 340). This process involves following steps:

1. Transfer the new software to base station with ‘Software > File Transfer’
2. Distribute the new software to all remote stations with ‘Software > Remote Distribution’
3. Activate of the new software on remote stations with ‘Software > Remote Activation’.
4. Finally, activate the new software on the base station radio with ‘Software > Manager’. Note: activating the software will reboot the radio.

Software > Summary

This page provides a summary of the software versions installed on the radio, the setup options and the status of the File Transfer.



SOFTWARE VERSIONS

Current Version

This parameter displays the software version running on the radio.

Previous Version

This parameter displays the software version that was running on the radio prior to the current software being activated.

Software Pack Version

On the base station, this parameter displays the software version available for distribution to all radios in the network.

On the all stations, this parameter displays the software version ready for activation.

USB AUTOMATIC UPGRADE

USB Boot Upgrade

This parameter shows the type of USB Boot upgrade defined in ‘Software Setup > USB Boot Upgrade’ on page 221.

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. When the software distribution is in progress, this parameter will change to 'Over the Air' (from xx.xx.xx.xx) to show that the interface is busy and the transfer is in progress.

File

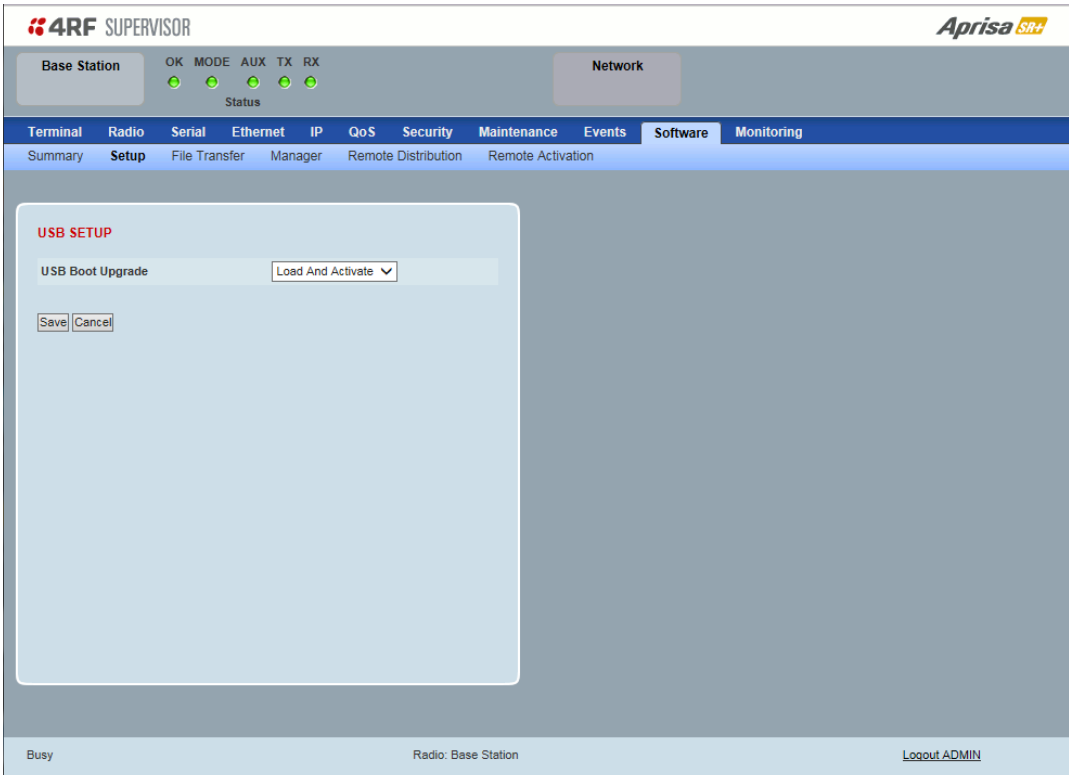
This parameter shows the software file source.

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

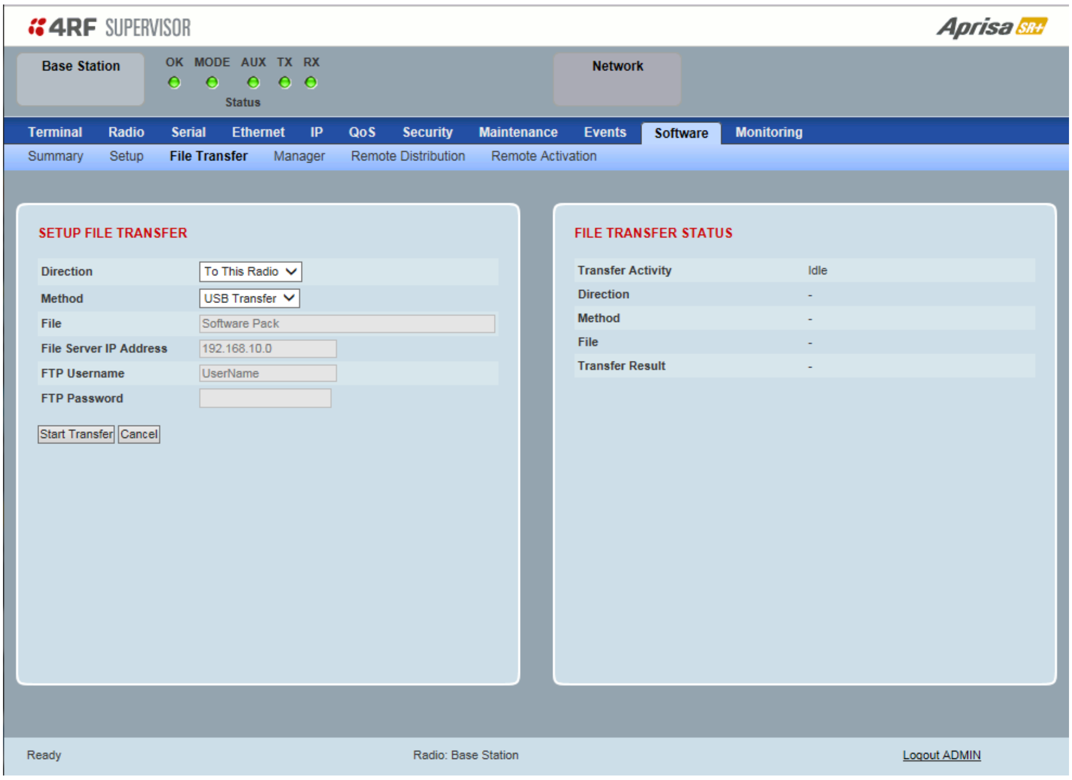
This parameter determines the action taken when the radio power cycles and finds a USB flash drive in the Host port. The default setting is 'Load and Activate'.

Option	Function
Load and Activate	New software will be uploaded from a USB flash drive in to the Aprisa SR+ when the radio is power cycled and activated automatically.
Load Only	New software will be uploaded from a USB flash drive in to the Aprisa SR+ when the radio is power cycled. The software will need to be manually activated (see 'Software > Manager' on page 225).
Disabled	Software will not be uploaded from a USB flash drive into the Aprisa SR+ when the radio is power cycled.

Note: This parameter must be set to 'Disabled' if the 'File Transfer and Activate' method of upgrade is used. This 'Disabled' setting prevents the radio from attempting another software upload when the radio boots (which it does automatically after activation).

Software > File Transfer

This page provides the mechanism to transfer new software from a file source into the radio.



SETUP FILE TRANSFER

Direction

This parameter sets the direction of file transfer. In this software version, the only choice is 'To the Radio'.

Method

This parameter sets the method of file transfer.

Option	Function
USB Transfer	Transfers the software from the USB flash drive to the radio.
FTP	Transfers the software from an FTP server to the radio.

File

This parameter shows the software file source.

FTP Username

This parameter sets the Username to access the FTP server.

FTP Password

This parameter sets the Password to access the FTP server.

FILE TRANSFER STATUS

Transfer Activity

This parameter shows the status of the transfer, ‘Idle’, ‘In Progress’ or ‘Completed’.

Direction

This parameter shows the direction of file transfer. In this software version, the only choice is ‘To The Radio’.

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. Possible causes of failure are: • Is the source file available e.g. USB flash drive plugged in • Does the file source contain the Aprisa SR+ software release files; asrapp 1,332 KB File asrboot 28 KB File asrmain 3,716 KB File asrrootfs 1,944 KB File asrver 8 KB File version.txt 1 KB Text Document

To transfer software into the Aprisa SR+ radio:

USB Transfer Method

1. Unzip the software release files in to the root directory of a USB flash drive.
2. Insert the USB flash drive into the host port .
3. Click on 'Start Transfer'.

FILE TRANSFER STATUS	
Transfer Activity	In Progress
Direction	To This Radio
Method	USB Transfer
File	Software Pack
Transfer Result	In Progress (30%)

4. When the transfer is completed, remove the USB flash drive from the host port. If the SuperVisor 'USB Boot Upgrade' setting is set to 'Disabled' (see 'USB Boot Upgrade' on page 221), the USB flash drive doesn't need to be removed as the radio won't try to load from it.

Go to Supervisor > Software > Manager and activate the Software Pack (see 'Software > Manager' on page 225). The radio will reboot automatically.

If the file transfer fails, check the Event History page (see 'Events > Event History' on page 207) for more details of the transfer.

FTP Method

1. Unzip the software release files in to a temporary directory.
2. Open the FTP server and point it to the temporary directory.
3. Enter the FTP server IP address, Username and password into SuperVisor.
4. Click on 'Start Transfer'.

FILE TRANSFER STATUS	
Transfer Activity	In Progress
Direction	To This Radio
Method	FTP (172.17.10.11)
File	Software Pack
Transfer Result	In Progress (1%)

Go to Supervisor > Software > Manager and activate the Software Pack (see 'Software > Manager' on page 225). The radio will reboot automatically.

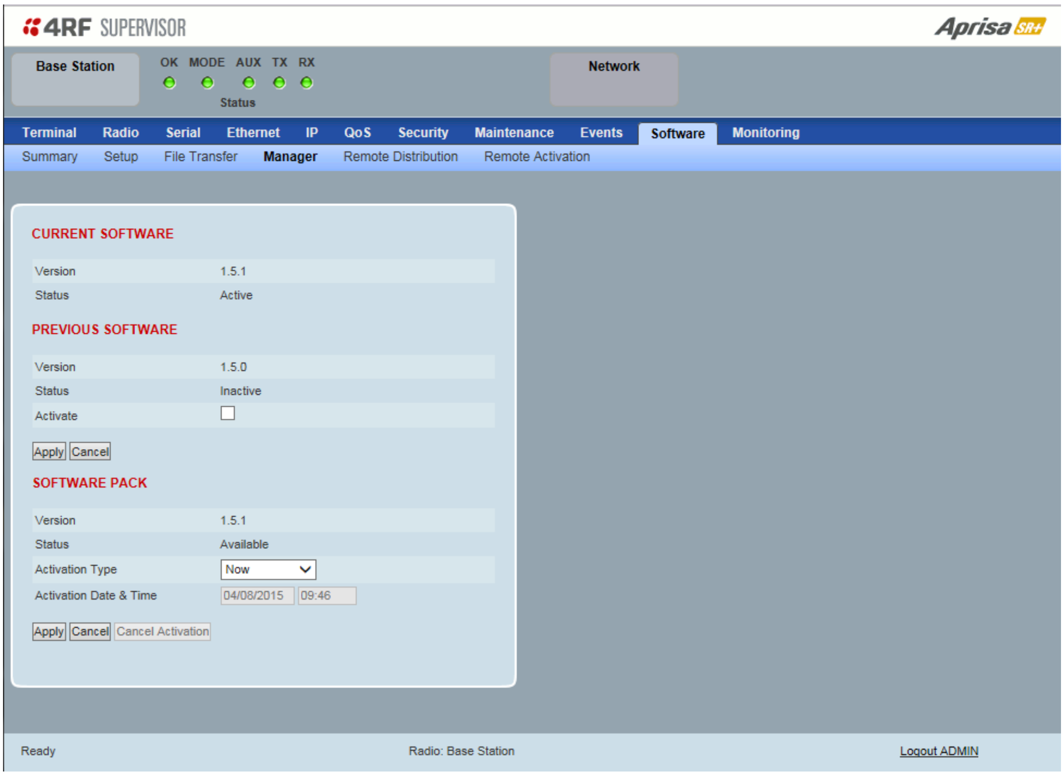
If the file transfer fails, check the Event History page (see 'Events > Event History' on page 207) for more details of the transfer.

Software > Manager

This page summarises and manages the software versions available in the radio.

The manager is predominantly used to activate new software on single radios. Network activation is performed with 'Software > Remote Activation'.

Both the previous software (if available) and Software Pack versions can be activated on the radio from this page.



CURRENT SOFTWARE

Version

This parameter displays the software version running on the radio.

Status

This parameter displays the status of the software version running on the radio (always active).

PREVIOUS SOFTWARE

Version

This parameter displays the software version that was running on the radio prior to the current software being activated.

Status

This parameter displays the status of the software version that was running on the radio prior to the current software being activated.

Option	Function
Active	The software is operating the radio.
Inactive	The software is not operating the radio but could be re-activated if required.

Activate

This parameter activates the previous software version (restores to previous version).

The Aprisa SR+ will automatically reboot after activation.

SOFTWARE PACK

Version

This parameter displays the software pack version available for distribution on base station and activate on all stations.

Status

This parameter displays the status of the software pack version.

Option	Function
Available	On the base station, the software pack is available for distribution. On all stations, the software pack is available for activation.
Activating	The software pack is activating in the radio.
Unavailable	There is no software pack loaded into the radio.

Activate

This parameter activates the software pack.

The Aprisa SR+ will automatically reboot after activation.

Activation Type

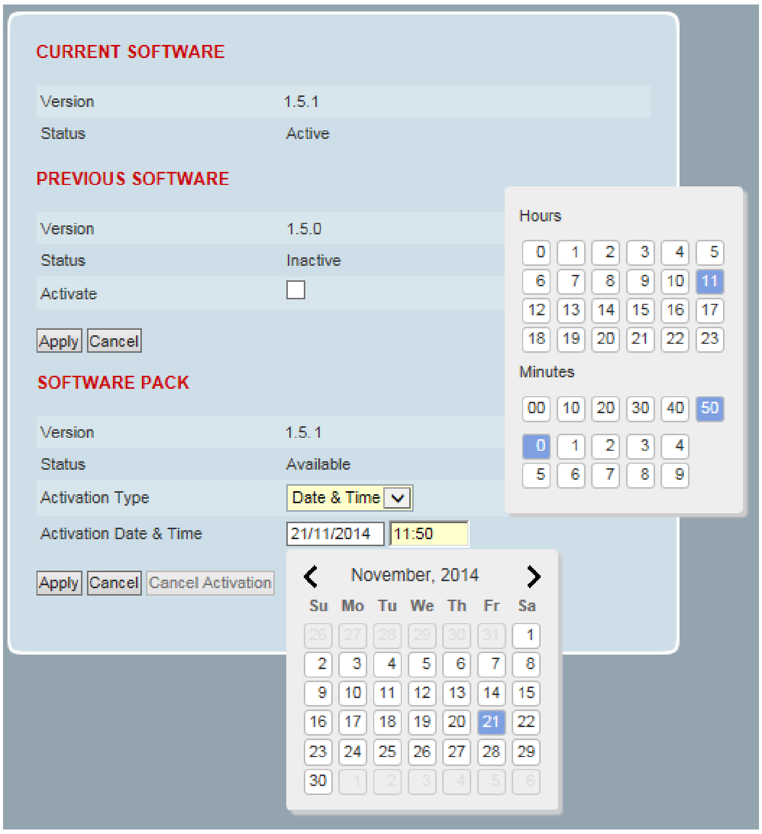
This parameter sets when the software pack activation will occur.

Option	Function
Now	Activates the software pack now.
Date & Time	Activates the software pack at the Date & Time set in the following parameter.

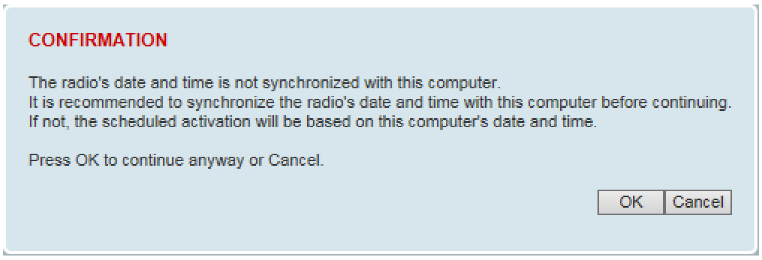
Activation Date & Time

This parameter sets the Date & Time when the software pack activation will occur.

This setting can be any future date and 24 hour time.



If the network base station radio date / time is not synchronized, you will get the following popup:



You can manually enter the base station radio date / time or use the Date And Time Synchronization from a SNTP server feature (see 'Terminal > Date / Time' on page 89).

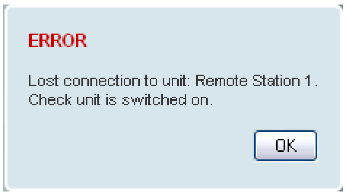
To activate a software version:

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 radio will reboot. This will cause the current SuperVisor session to expire.



3. Login to SuperVisor to check the result.

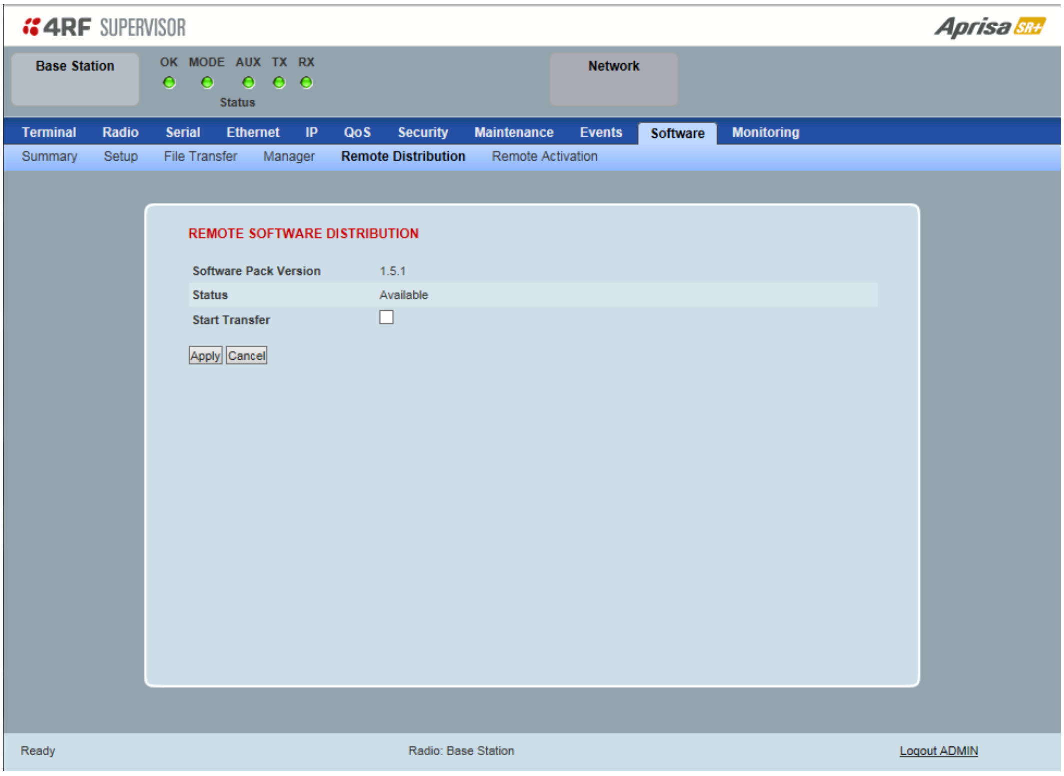
Software > Remote Distribution

This page provides the mechanism to distribute software to all remote stations into the Aprisa SR+ network (network) and then activate it.

The Software Pack that was loaded into the base station with the file transfer process (see 'Software > File Transfer' on page 222) can be distributed via the radio link to all remote stations.

This page is used to manage the distribution of that software pack to all remote radios on the network.

This page is only available when the radio is configured as a Base Station.



REMOTE SOFTWARE DISTRIBUTION

Software Pack Version

This parameter displays the software pack version available for distribution on base station and activate on all stations.

Status

This parameter displays the status of the software pack version.

If a Software Pack is not available, the status will display 'Unavailable' and the software distribution mechanism will not work.

Start Transfer

This parameter when activated distributes (broadcasts) the new Software Pack to all remote stations in the network.

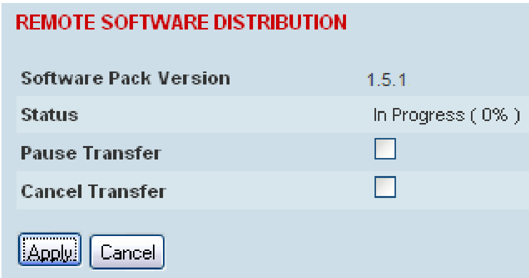
Note: The distribution of software to remote stations does not stop customer traffic from being transferred. However, due to the volume of traffic, the software distribution process may affect customer traffic.

Software distribution traffic is classified as 'management traffic' but does <u>not</u> use the Ethernet management priority setting. Software distribution traffic priority has a fixed priority setting of 'very low'.

To distribute software to remote stations:

This process assumes that a Software Pack has been loaded into the base station with the file transfer process (see 'Software > File Transfer' on page 222).

1. To ensure that the Network Table is up to date, it is recommended running the node discover function (see 'Discover Nodes' on page 203).
2. Click on 'Start Transfer'.



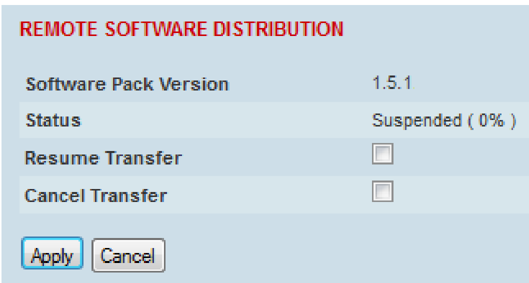
Note: This process could take anywhere between 40 minutes and several hours depending on channel size, Ethernet Management Priority setting and the amount of customer traffic on the network.

---

3. When the distribution is completed, activate the software with the Remote Software Activation.

Pause Transfer

This parameter when activated, pauses the distribution process and shows the distribution status. The distribution process will continue from where it was paused with Resume Transfer.



Cancel Transfer

This parameter when activated, cancels the distribution process immediately.

During the distribution process, it is possible to navigate away from this page and come back to it to check progress. The SuperVisor session will not timeout.

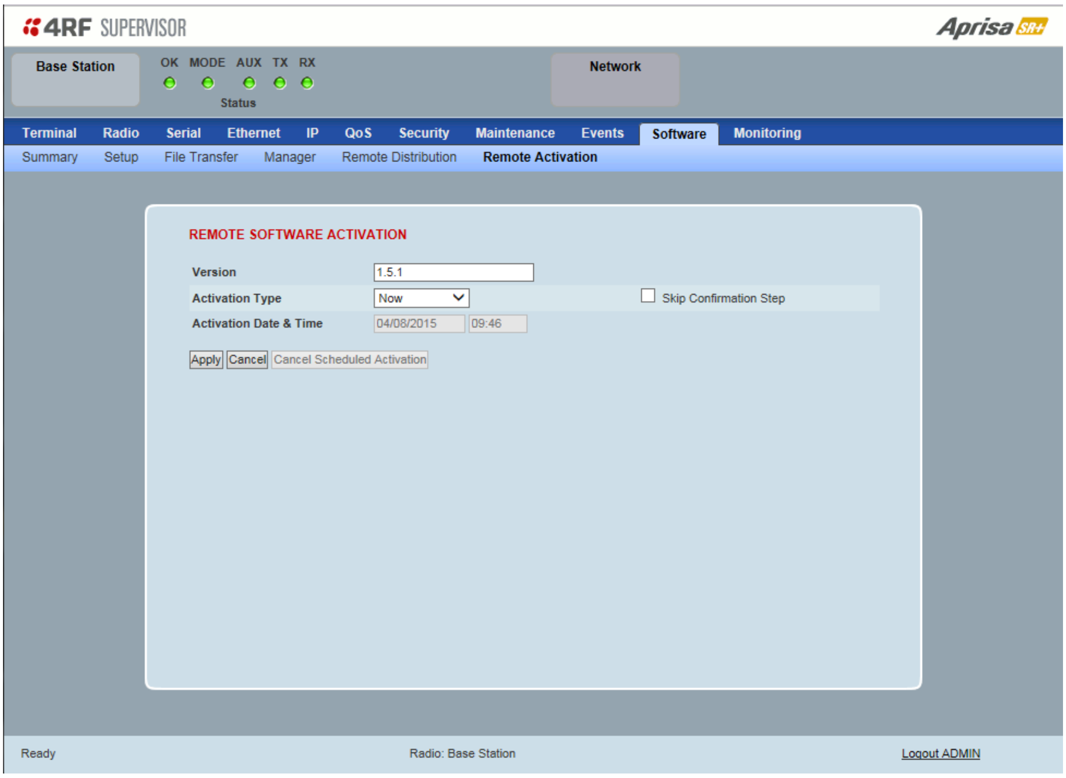
Software > Remote Activation

This page provides the mechanism to activate software on all remote stations.

The Software Pack was loaded into the base station with the file transfer process (see 'Software > File Transfer' on page 222) and was distributed via the radio link to all remote stations.

This page is used to manage the activation of that software pack on all remote radios on the network.

This page is only available when the radio is configured as a Base Station.



REMOTE SOFTWARE ACTIVATION

When the software pack version has been distributed to all the remote stations, the software is then activated in all the remote stations with this command. If successful, then activate the software pack in the base station to complete the network upgrade.

Version

This parameter displays the software version for activation. The default version is the software pack version but any valid software version can be entered in the format 'n.n.n'.

Activation Type

This parameter sets when the software pack activation will occur.

Option	Function
Now	Activates the software pack now.
Date & Time	Activates the software pack at the Date & Time set in the following parameter.

Activation Date & Time

This parameter sets the Date & Time when the software pack activation will occur.

This setting can be any future date and 24 hour time.

Skip Confirmation Step

This parameter when enabled skips the confirmation step during the activation process.

Normally, the confirmation step will require use intervention to accept the confirmation which will halt the activation process. Skipping the confirmation will enable the activation process to continue without use intervention.

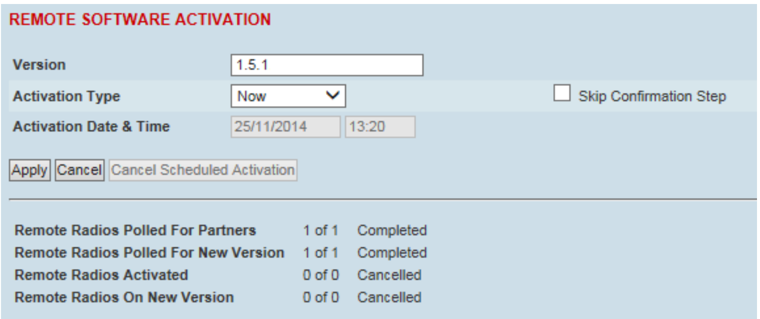
To activate software in remote stations:

This process assumes that a Software Pack has been loaded into the base station with the file transfer process (see 'Software > File Transfer' on page 222) and distributed to all remote radios in the network.

Note: Do not navigate SuperVisor away from this page during the activation process (SuperVisor can lose PC focus).

---

1. Enter the Software Pack version (if different from displayed version).

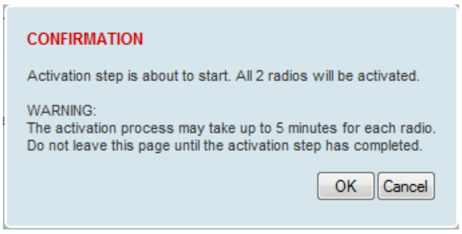


2. Select the Activation type.
3. Click Apply.

The remote stations will be polled to determine which radios require activation:

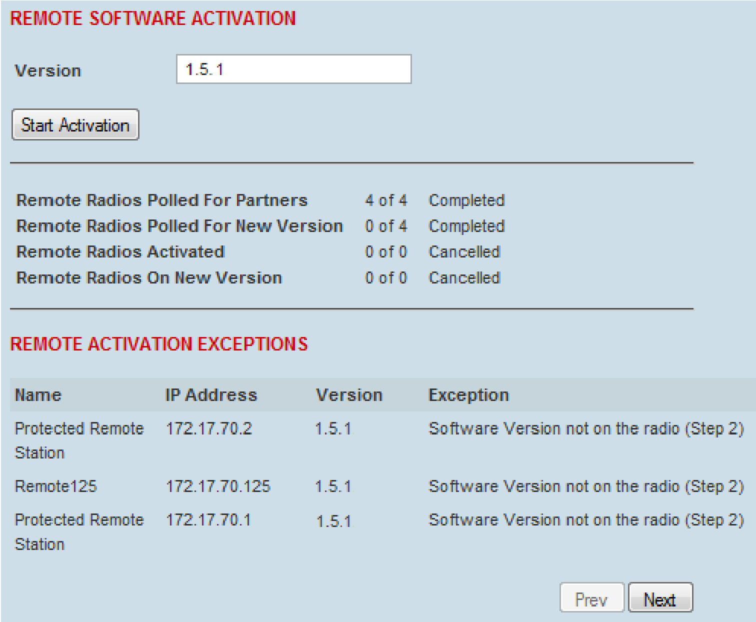
Result	Function (X of Y)
Remote Radios Polled for Partners	X is the number of radios polled to determine the number of protected stations in the network. Y is the number of remote radios registered with the base station.
Remote Radios Polled for New Version	X is the number of radios polled to determine the number of radios that contain the new software version. Y is the number of remote radios registered with the base station.
Remote Radios Activated	X is the number of radios that contain the new software version and have been activated. Y is the number of radios that contain the new software version and can be activated.
Remote Radios On New Version	X is the number of radios that has been successfully activated and now running the new version of software. Y is the number of radios that the activation command was executed on. **Note:** When upgrading from software version 1.2.5 to 1.2.6 or later, communication to all remote radios will be lost due to a MAC protocol change. This will prevent this function from working correctly. In this case, activate the new software on the base station and run the 'Maintenance > Advanced' Discover Nodes function on page 202.

When the activation is ready to start:



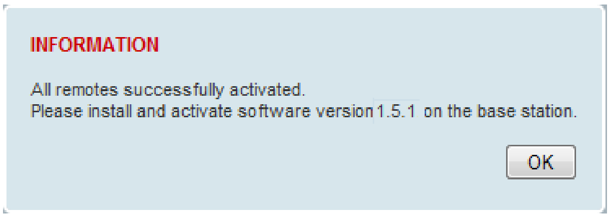
4. Click on 'OK' to start the activation process or Cancel to quit.

The page will display the progress of the activation.



The example shows that during the activation process there were exceptions that may need to be investigated.

When all the remote radios have been activated, the base station radio must now be activated with (see ‘Software > Manager’ on page 225).



4. Click on ‘OK’ to start the activation on the base station.

Activation Type

This parameter sets when the remote software activation will occur.

Option	Function
Now	Activates the remote software now.
Date & Time	Activates the remote software at the Date & Time set in the following parameter.

Skip Confirmation Step

This parameter when enabled skips the confirmation step during the activation process.

Normally, the confirmation step will require use intervention to accept the confirmation which will halt the activation process. Skipping the confirmation will enable the activation process to continue without use intervention.

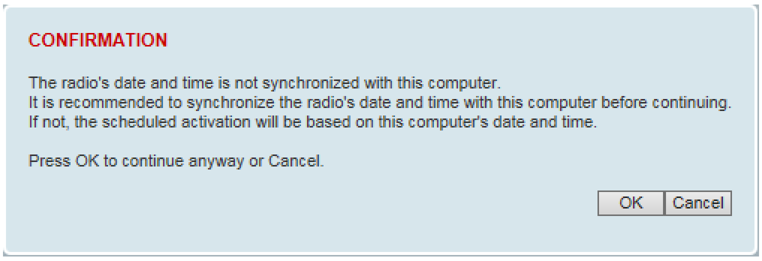
Activation Date & Time

This parameter sets the Date & Time when the remote software activation will occur.

This setting can be any future date and 24 hour time.

When the date and time is set, the remotes will be polled to setup the scheduled activation date and time.

If the network base station radio date / time is not synchronized, you will get the following popup:



You can manually enter the base station radio date / time or use the Date And Time Synchronization from a SNTP server feature (see 'Terminal > Date / Time' on page 89).

Monitoring

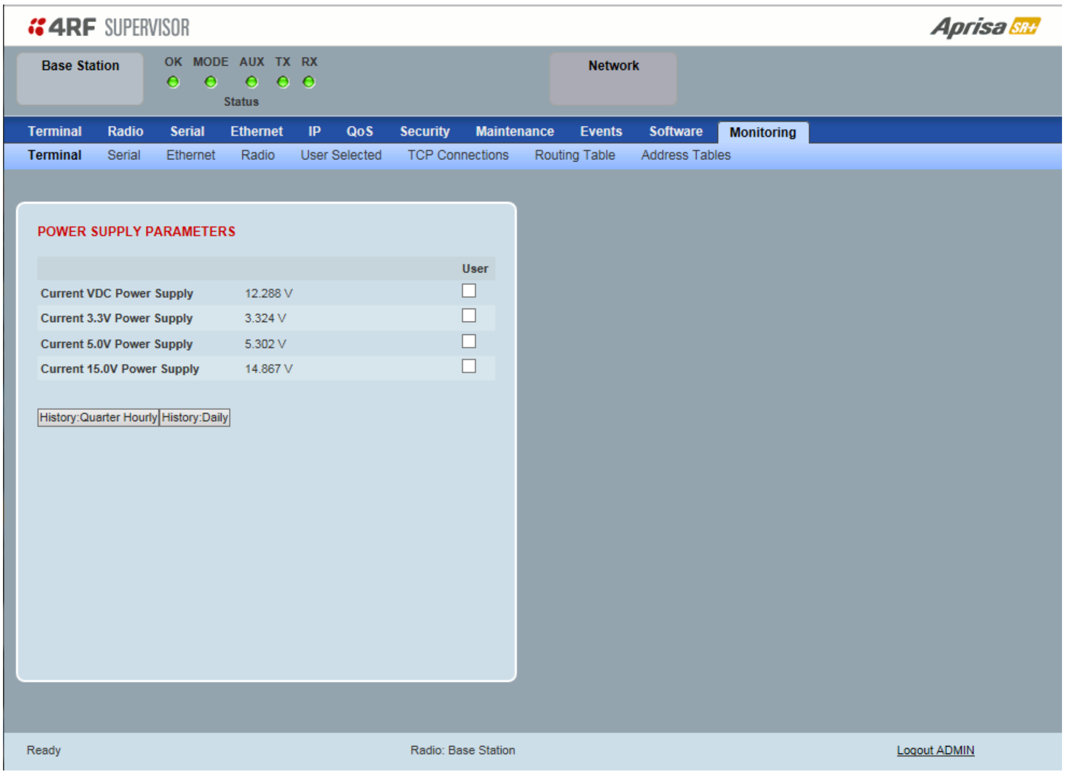
The Terminal, Serial, Ethernet, Radio and User Selected Monitored Parameter results have history log views for both Quarter Hourly and Daily.

Monitored parameter data is accumulated into 2 sets:

- 15 minutes of data, for 96 readings for the last 24 hours
- 24 hours of data, for 31 readings for the last 31 days.

Monitoring > Terminal

This page displays the current radio internal and external input source radio power supply voltage diagnostic parameters.

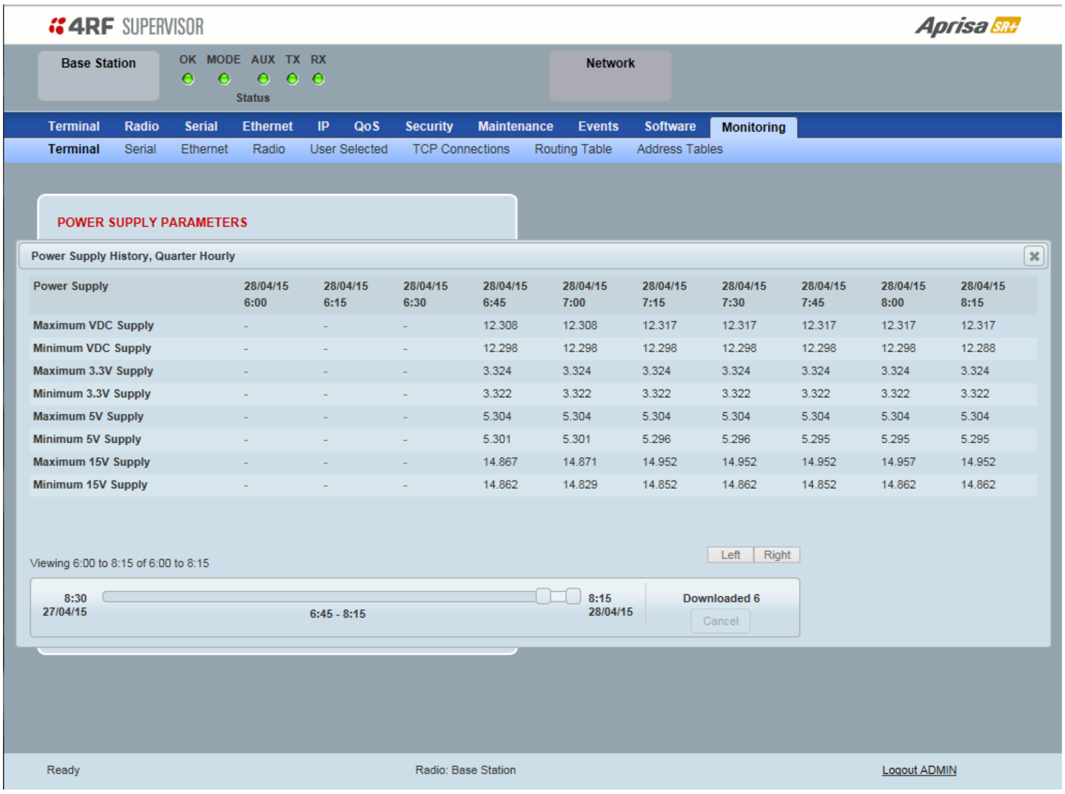


POWER SUPPLY PARAMETERS

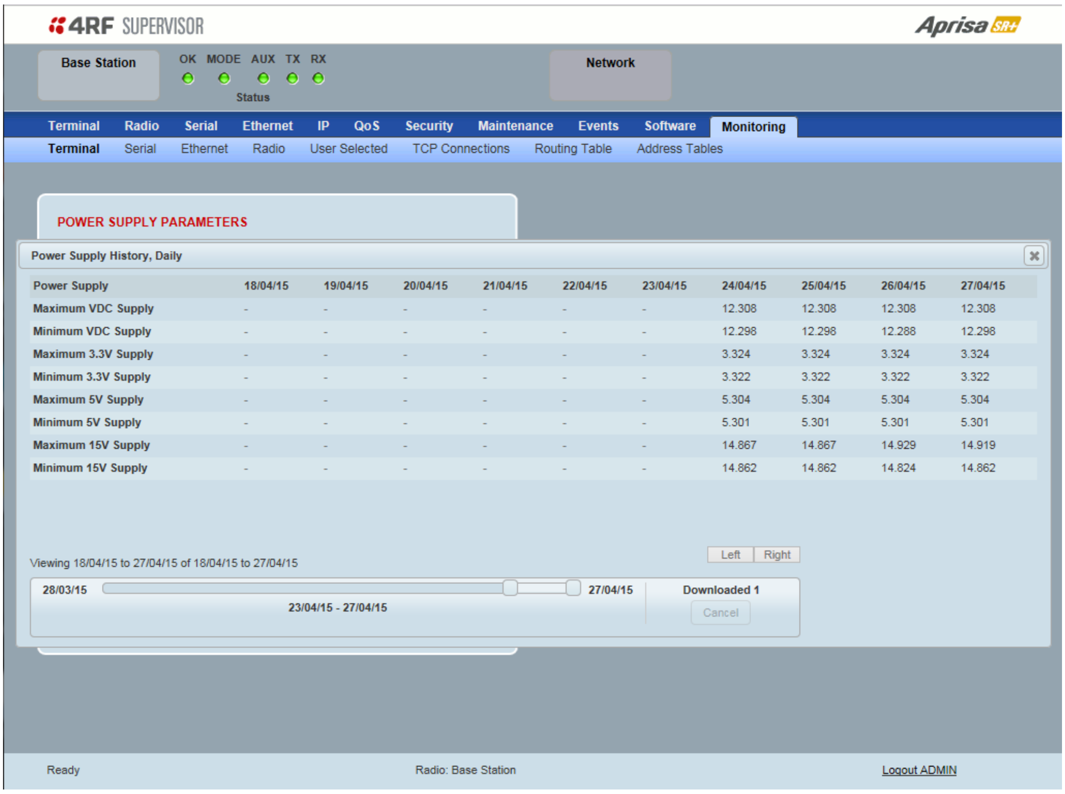
Monitored Parameter	Function	Normal Operating Limits
Current VDC Power Supply	Parameter to show the current power supply input voltage	10 to 30 VDC
Current 3.3 Volts Power Supply	Parameter to show the current 3.3 volt power rail voltage	3.1 to 3.5 VDC
Current 5.0 Volts Power Supply	Parameter to show the current that the current 5.0 volt power rail voltage	4.7 to 5.5 VDC
Current 7.2 Volts Power Supply	Parameter to show the current that the current 7.2 volt power rail voltage	6.9 to 7.5 VDC
Current 15 Volts Power Supply	Parameter to show the current that the current 15 volt power rail voltage. The 15 volt power supply is used to power the transmitter driver and power amplifier.	300,400 and 450 MHz transmitters 14.5 to 15.3 VDC 200 and 900 MHz transmitter 12.7 to 13.5 VDC

Controls

The History Quarter Hourly button presents a log of results every quarter of an hour.



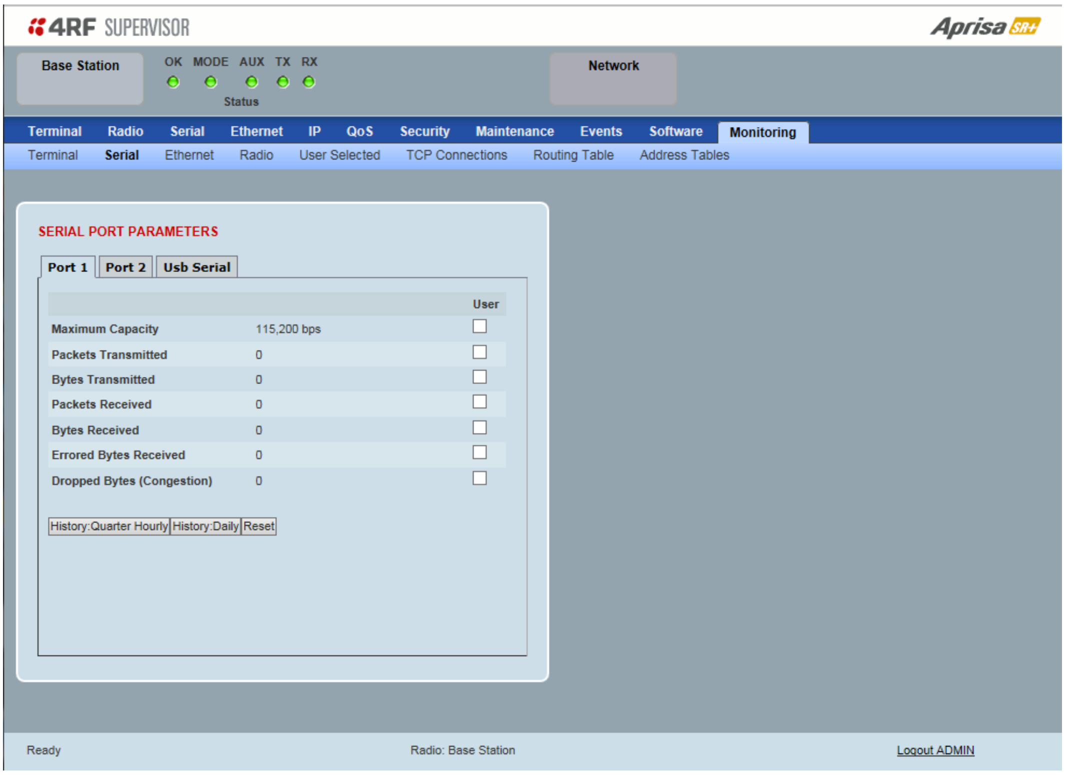
The History Daily button presents a log of results every day.



Monitoring > Serial

This page displays the current radio performance monitoring parameters per serial port 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

All Serial Ports

Monitored Parameter	Function	Normal Operating Limits
Maximum Capacity	Parameter to show the maximum serial data rate of the serial port	Equal to the serial port baud rate setting
Packets Transmitted	Parameter to show the number of packets transmitted to the customer from the serial port	
Packets Received	Parameter to show the number of packets received from the customer into the serial port	
Bytes Received	Parameter to show the number of bytes received from the customer into the serial port	
Errored Bytes Received	Parameter to show the number of bytes received from the customer into the serial port that have errors	
Dropped Bytes (Congestion)	Parameter to show the number of bytes received from the customer into the serial port that are dropped due to over the air congestion	

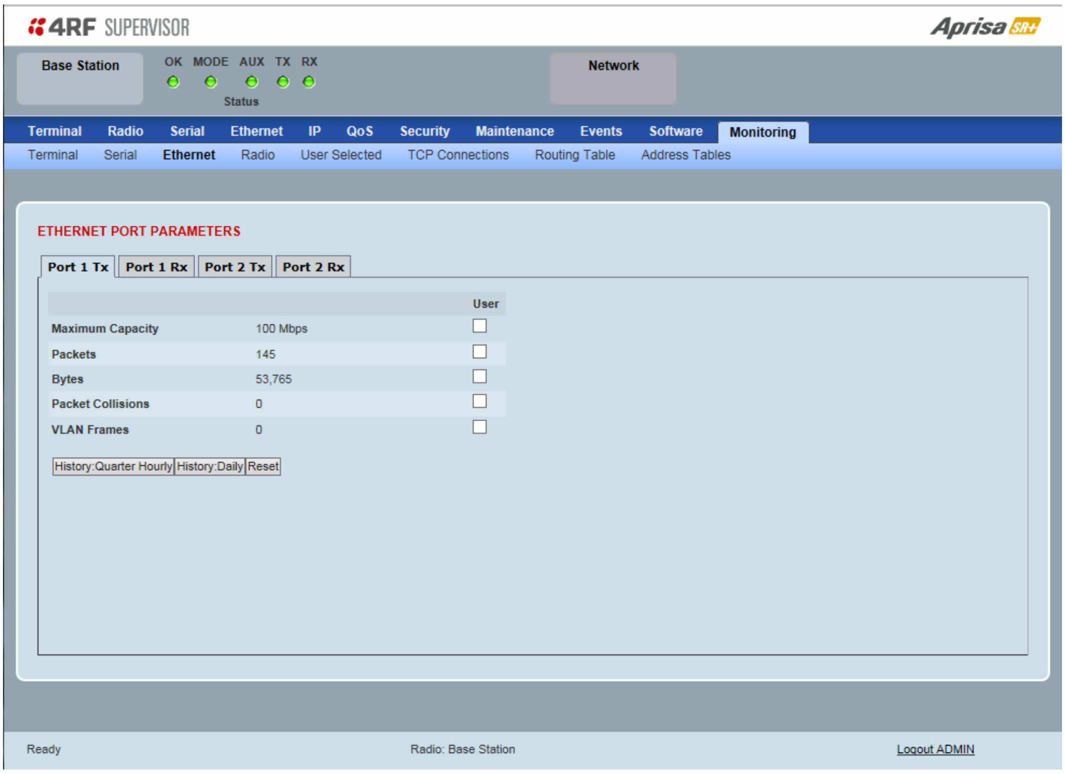
Controls

The Reset button clears the current results.

Monitoring > Ethernet

This page displays the current radio performance monitoring parameters per Ethernet port transmission (TX) out of the radio 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

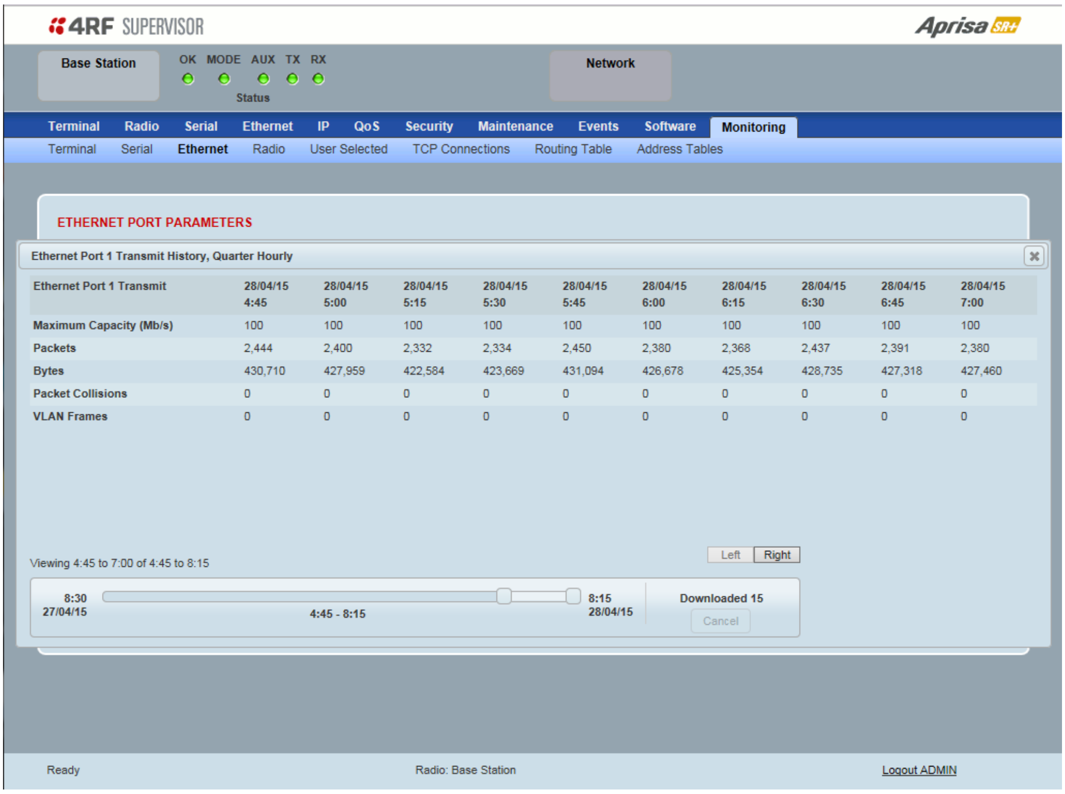
All Ethernet Ports TX

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
Packets	Parameter to show the number of packets transmitted to the customer from the Ethernet port	
Bytes	Parameter to show the number of bytes transmitted to the customer from the Ethernet port	
Packet Collisions	Parameter to show the number of packet collisions on the data transmitted to the customer from the Ethernet port on a shared LAN	
VLAN Frames	Parameter to show the number of VLAN tagged frames transmitted to the customer from the Ethernet port	

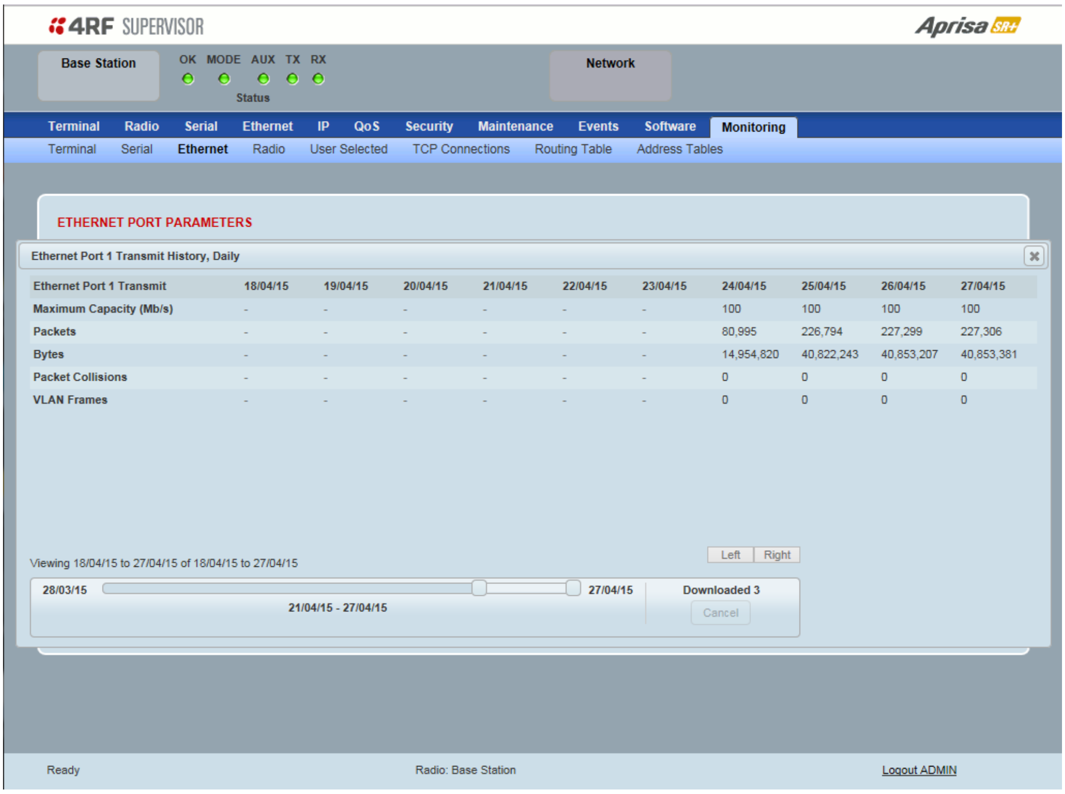
Controls

The Reset button clears the current results.

The History Quarter Hourly button presents a log of results every quarter of an hour.

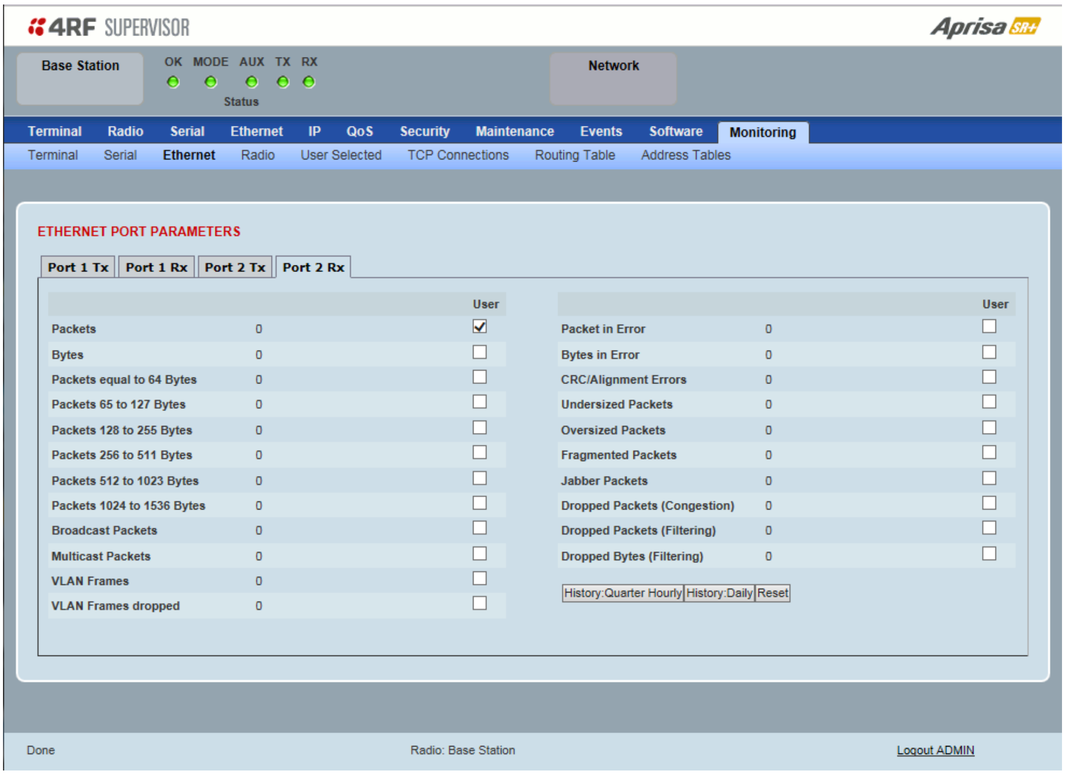


The History Daily button presents a log of results every day.



This page displays the current radio 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

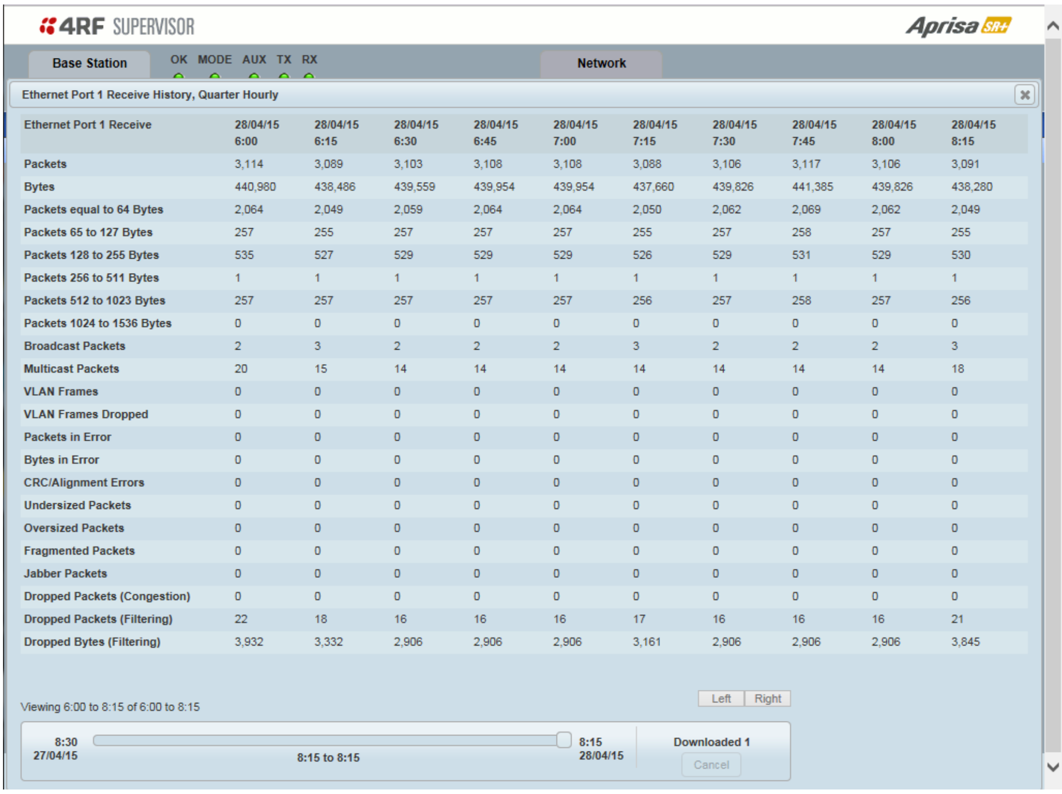
Monitored Parameter	Function
Packets	Parameter to show the number of packets received by the customer from the Ethernet port (including bad packets, broadcast packets, and multicast packets)
Bytes	Parameter to show the number of bytes received (including those in bad packets) by the customer from the Ethernet port (excluding framing bits but including FCS octets)
Packets equal to 64 bytes	Parameter to show the number of packets received (including bad packets) from the customer into the Ethernet port that are equal to 64 bytes (excluding framing bits but including FCS octets)
Packets 65 to 127 bytes	Parameter to show the number of packets received (including bad packets) from the customer into the Ethernet port that are between 65 and 127 bytes (excluding framing bits but including FCS octets)
Packets 128 to 255 bytes	Parameter to show the number of packets received (including bad packets) from the customer into the Ethernet port that are between 128 and 255 bytes (excluding framing bits but including FCS octets)
Packets 256 to 511 bytes	Parameter to show the number of packets received (including bad packets) from the customer into the Ethernet port that are between 256 and 511 bytes(excluding framing bits but including FCS octets)
Packets 512 to 1023 bytes	Parameter to show the number of packets received (including bad packets) from the customer into the Ethernet port that are between 512 and 1023 bytes(excluding framing bits but including FCS octets)
Packets 1024 to 1536 bytes	Parameter to show the number of packets received (including bad packets) from the customer into the Ethernet port that are between 1024 and 1536 bytes(excluding framing bits but including FCS octets)
Broadcast Packets	Parameter to show the number of broadcast packets received from the customer into the Ethernet port. Broadcast packets are good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Monitored Parameter	Function
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.
VLAN Frames	Parameter to show the number of VLAN tagged frames received from the customer into the Ethernet port
VLAN Frames Dropped	Parameter to show the number of VLAN tagged frames received from the customer into the Ethernet port that were dropped due to CRC errored frames, filtered VLAN frames, undersized frames or oversized frames.
Packet 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
Bytes In Error	Parameter to show the number of errored bytes received from the customer into the Ethernet port
CRC / Alignment Error	Parameter to show the number of CRC / alignment errors received from the customer into the Ethernet port. CRC / alignment errors are defined as frames that had a length excluding framing bits, but including FCS octets of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets.
Undersized Packets	Parameter to show the number of undersized packets received from the customer into the Ethernet port. Undersized packets are less than 64 octets long excluding framing bits, but including FCS octets.
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.
Fragmented Packets	Parameter to show the number of fragmented packets received from the customer into the Ethernet port. Fragmented packets have either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS.
Jabber Packets	Parameter to show the number of jabber packets received from the customer into the Ethernet port
Dropped Packets (congestion)	Parameter to show the number of dropped packets received from the customer into the Ethernet port caused by congestion
Dropped Packets (filtering)	Parameter to show the number of dropped packets received from the customer into the Ethernet port caused by packet L2 / L3 filtering
Dropped Bytes (filtering)	Parameter to show the number of dropped bytes received from the customer into the Ethernet port caused by packet L2 / L3 filtering

Controls

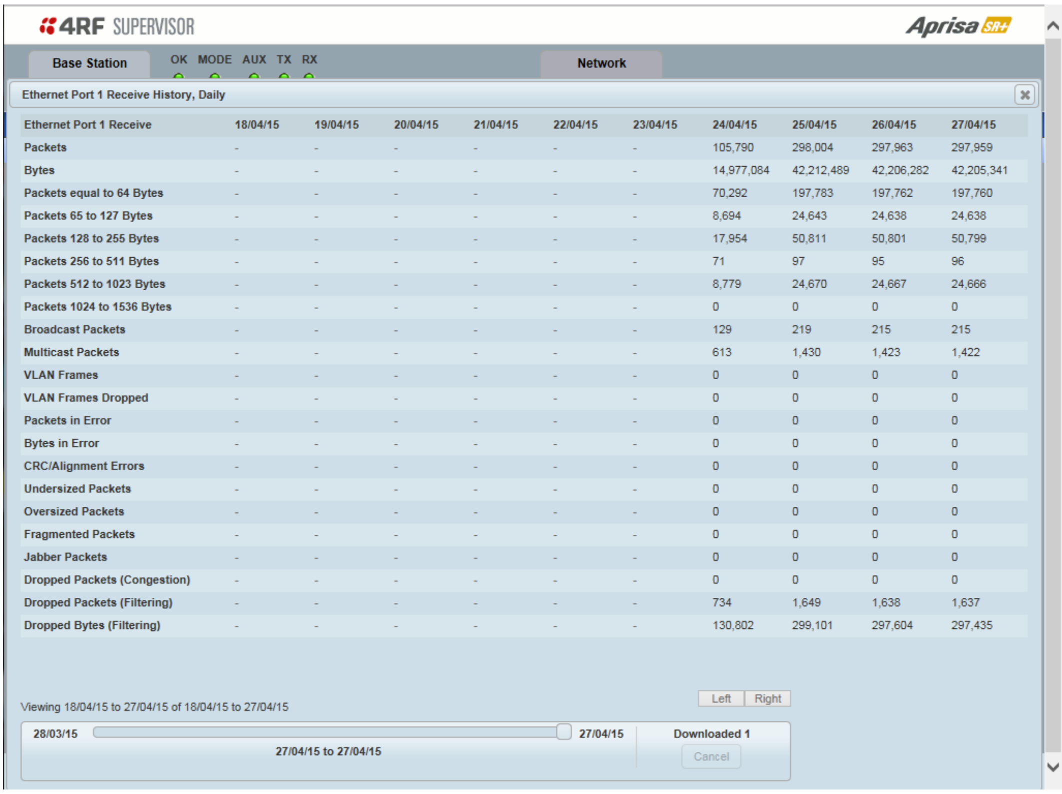
The Reset button clears the current results.

The History Quarter Hourly button presents a log of results every quarter of an hour.



Ethernet Port 1 Receive	28/04/15 6:00	28/04/15 6:15	28/04/15 6:30	28/04/15 6:45	28/04/15 7:00	28/04/15 7:15	28/04/15 7:30	28/04/15 7:45	28/04/15 8:00	28/04/15 8:15
Packets	3,114	3,089	3,103	3,108	3,108	3,088	3,106	3,117	3,106	3,091
Bytes	440,980	438,486	439,559	439,954	439,954	437,660	439,826	441,385	439,826	438,280
Packets equal to 64 Bytes	2,064	2,049	2,059	2,064	2,064	2,050	2,062	2,069	2,062	2,049
Packets 65 to 127 Bytes	257	255	257	257	257	255	257	258	257	255
Packets 128 to 255 Bytes	535	527	529	529	529	526	529	531	529	530
Packets 256 to 511 Bytes	1	1	1	1	1	1	1	1	1	1
Packets 512 to 1023 Bytes	257	257	257	257	257	256	257	258	257	256
Packets 1024 to 1536 Bytes	0	0	0	0	0	0	0	0	0	0
Broadcast Packets	2	3	2	2	2	3	2	2	2	3
Multicast Packets	20	15	14	14	14	14	14	14	14	18
VLAN Frames	0	0	0	0	0	0	0	0	0	0
VLAN Frames Dropped	0	0	0	0	0	0	0	0	0	0
Packets in Error	0	0	0	0	0	0	0	0	0	0
Bytes in Error	0	0	0	0	0	0	0	0	0	0
CRC/Alignment Errors	0	0	0	0	0	0	0	0	0	0
Undersized Packets	0	0	0	0	0	0	0	0	0	0
Oversized Packets	0	0	0	0	0	0	0	0	0	0
Fragmented Packets	0	0	0	0	0	0	0	0	0	0
Jabber Packets	0	0	0	0	0	0	0	0	0	0
Dropped Packets (Congestion)	0	0	0	0	0	0	0	0	0	0
Dropped Packets (Filtering)	22	18	16	16	16	17	16	16	16	21
Dropped Bytes (Filtering)	3,932	3,332	2,906	2,906	2,906	3,161	2,906	2,906	2,906	3,845

The History Daily button presents a log of results every day.

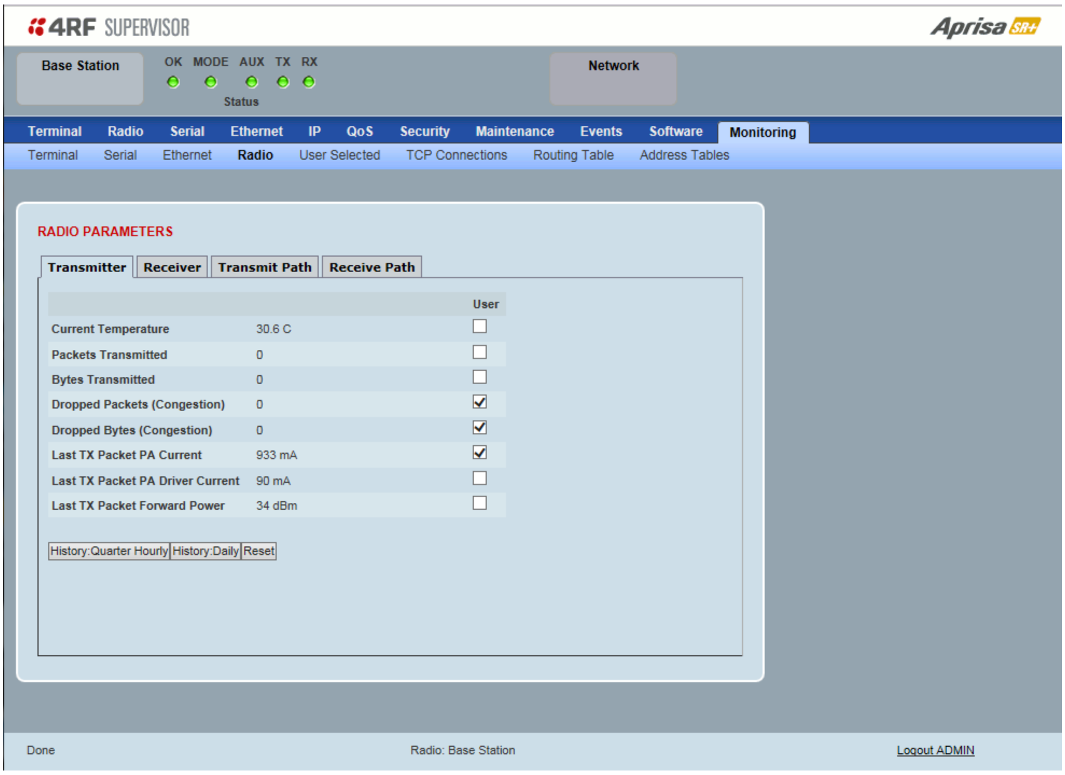


Ethernet Port 1 Receive	18/04/15	19/04/15	20/04/15	21/04/15	22/04/15	23/04/15	24/04/15	25/04/15	26/04/15	27/04/15
Packets	-	-	-	-	-	-	105,790	298,004	297,963	297,959
Bytes	-	-	-	-	-	-	14,977,084	42,212,489	42,206,282	42,205,341
Packets equal to 64 Bytes	-	-	-	-	-	-	70,292	197,783	197,762	197,760
Packets 65 to 127 Bytes	-	-	-	-	-	-	8,694	24,643	24,638	24,638
Packets 128 to 255 Bytes	-	-	-	-	-	-	17,954	50,811	50,801	50,799
Packets 256 to 511 Bytes	-	-	-	-	-	-	71	97	95	96
Packets 512 to 1023 Bytes	-	-	-	-	-	-	8,779	24,670	24,667	24,666
Packets 1024 to 1536 Bytes	-	-	-	-	-	-	0	0	0	0
Broadcast Packets	-	-	-	-	-	-	129	219	215	215
Multicast Packets	-	-	-	-	-	-	613	1,430	1,423	1,422
VLAN Frames	-	-	-	-	-	-	0	0	0	0
VLAN Frames Dropped	-	-	-	-	-	-	0	0	0	0
Packets in Error	-	-	-	-	-	-	0	0	0	0
Bytes in Error	-	-	-	-	-	-	0	0	0	0
CRC/Alignment Errors	-	-	-	-	-	-	0	0	0	0
Undersized Packets	-	-	-	-	-	-	0	0	0	0
Oversized Packets	-	-	-	-	-	-	0	0	0	0
Fragmented Packets	-	-	-	-	-	-	0	0	0	0
Jabber Packets	-	-	-	-	-	-	0	0	0	0
Dropped Packets (Congestion)	-	-	-	-	-	-	0	0	0	0
Dropped Packets (Filtering)	-	-	-	-	-	-	734	1,649	1,638	1,637
Dropped Bytes (Filtering)	-	-	-	-	-	-	130,802	299,101	297,604	297,435

Monitoring > Radio

This page displays the current radio diagnostic and performance monitoring parameters of the radio transmitter.

The results shown are since the page was opened and are updated automatically every 12 seconds.



RADIO PARAMETERS

Transmitter

Monitored Parameter	Function	Normal Operating Limits
Current Temperature	Parameter to show the current temperature of the transmitter	0 to 70 °C
Packets Transmitted	Parameter to show the number of packets transmitted over the air	
Bytes Transmitted	Parameter to show the number of bytes transmitted over the air	
Dropped Packets (congestion)	Parameter to show the number of dropped packets transmitted over the air caused by congestion	
Dropped Bytes (congestion)	Parameter to show the number of dropped bytes transmitted over the air caused by congestion	
Last TX Packet PA Current	Parameter to show the current consumed by the transmitter power amplifier in mA. The value is stored from the last time the transmitter was active and transmitted a packet.	This value will change depending on the transmitter power setting, modulation, temperature and the VSWR of the antenna. The alarm limits for this are 50 mA to 2.5 A
Last TX Packet Driver Current	Parameter to show the current consumed by the transmitter power amplifier driver in mA. The value is stored from the last time the transmitter was active and transmitted a packet.	This value will change depending on the transmitter power setting, modulation and temperature. The alarm limits for the PA Driver Current are 10 mA to 500 mA.

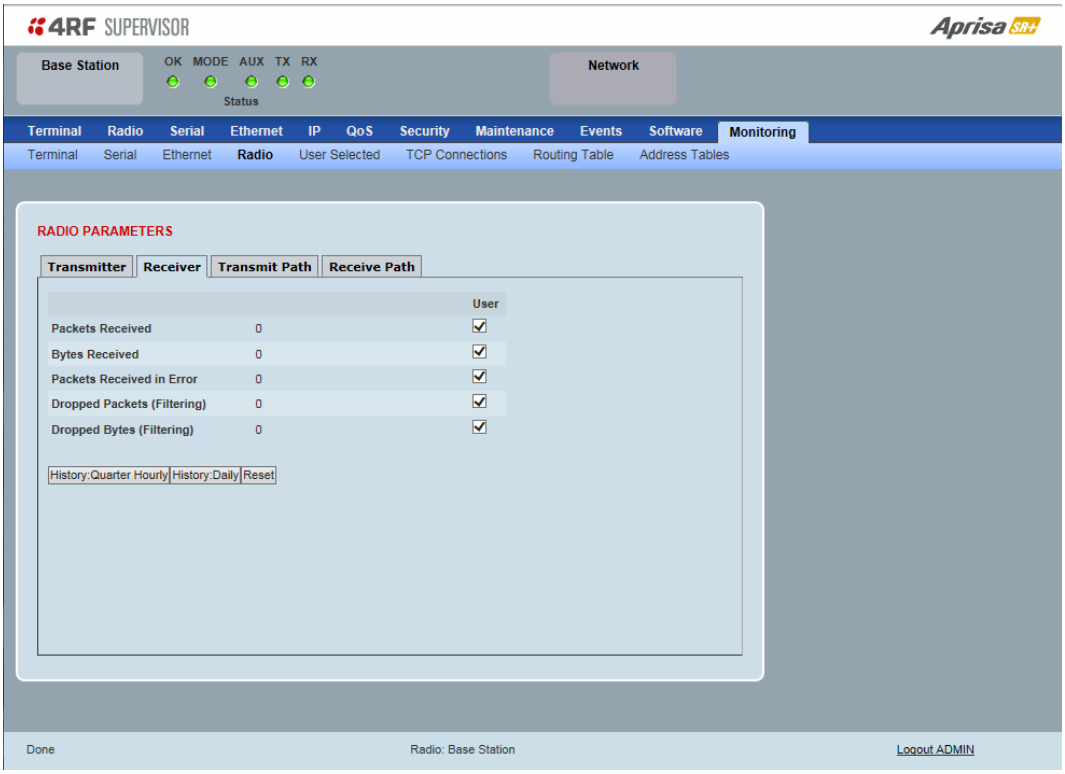
Monitored Parameter	Function	Normal Operating Limits
Last TX Packet Forward Power	Parameter to show the actual transmitter power in dBm. The value is stored from the last time the transmitter was active and transmitted a packet.	This value will be dependent on the output power, the temperature and the VSWR of the antenna. The alarm limits for the Tx forward power are +/-4 dB.

Controls

The Reset button clears the current results.

This page displays the current radio performance monitoring parameters of radio receiver.

The results shown are since the page was opened and are updated automatically every 12 seconds.



RADIO PARAMETERS

Receiver

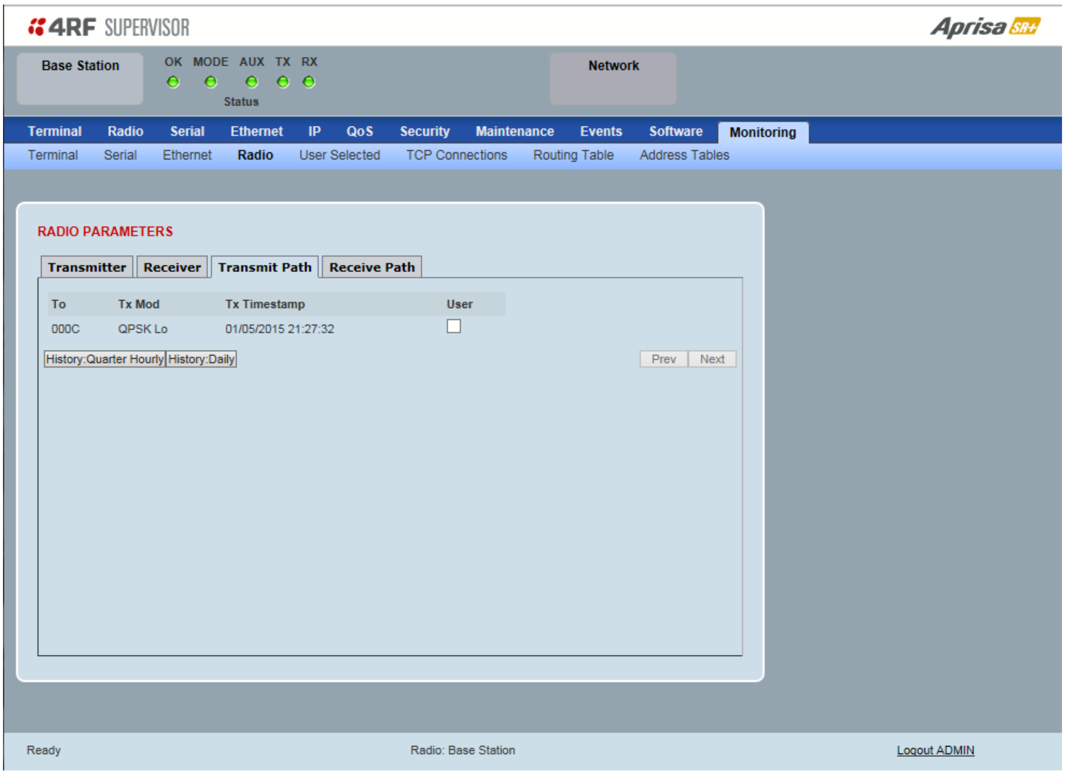
Monitored Parameter	Function
Packets Received	Parameter to show the number of packets received over the air
Bytes Received	Parameter to show the number of bytes received over the air
Packets Received In Error	Parameter to show the number of packets received over the air
Dropped Packets (filtering)	Parameter to show the number of dropped packets received over the air caused by L2 / L3 filtering
Dropped Bytes (filtering)	Parameter to show the number of dropped bytes received over the air caused by L2 / L3 filtering

Controls

The Reset button clears the current results.

This page displays the current radio RF transmit path modulation setting to single or multiple destination radios that the radio is transmitting to.

The results shown are since the page was opened and are updated automatically every 12 seconds.



RADIO PARAMETERS

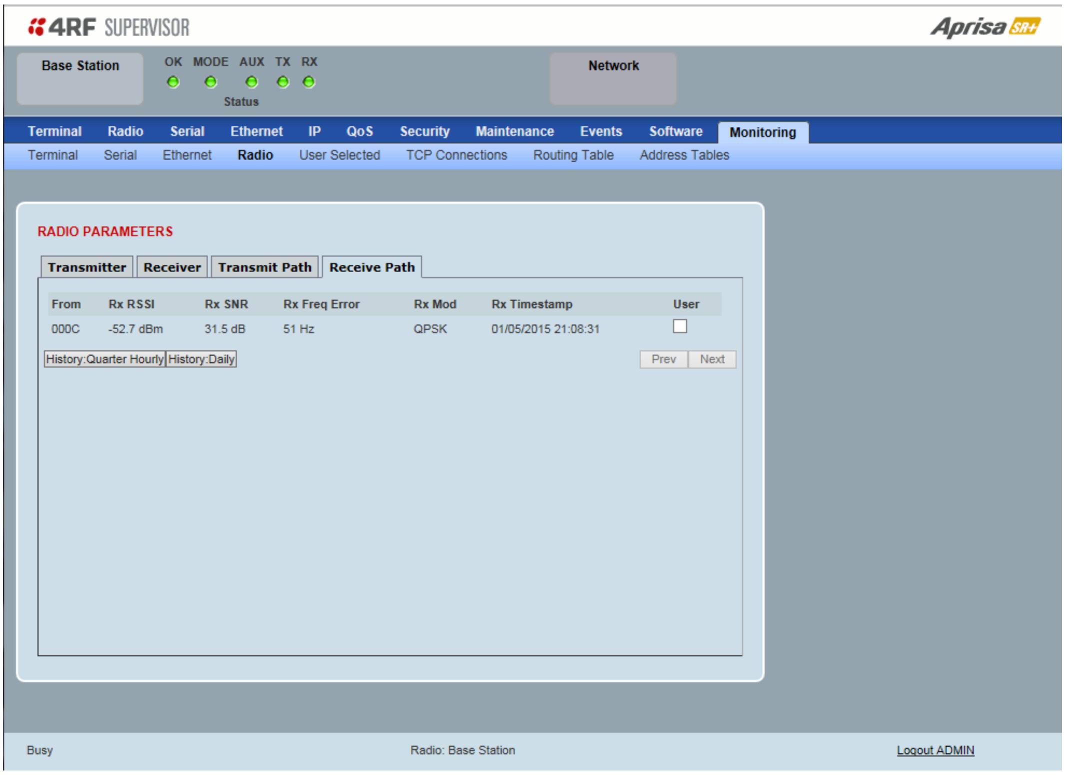
Result	Function
To	The destination Node Address of the radio/s transmitting data to.
Tx Mod	The current radio transmitter modulation being used to communicate with the destination radio/s.
Tx Timestamp	The timestamp of the last transmitted packet to the destination radio/s.

Controls

The Next button will display the next page of 8 radios and the Prev button will display the previous page of 8 radios.

This page displays the current radio RF receive path parameters from single or multiple source radios that the radio is receiving from.

The results shown are since the page was opened and are updated automatically every 12 seconds.



RADIO PARAMETERS

Receive Path

Result	Function
From	The source Node Address of the radio receiving data from.
Rx RSSI	The RSSI of the RF signal received from the source radio/s. This parameter displays the receiver RSSI reading taken from the last data packet received.
Rx SNR	The SNR of the RF signal received from the source radio/s. This parameter displays the receiver SNR reading taken from the last data packet received.
Rx Freq Error	The frequency difference between this radio's receiver and the frequency of the incoming packet rate from the source radio/s.
Rx Mod	The current radio receive modulation being used to communicate with the source radio/s.
Rx Timestamp	The timestamp of the last received packet from the source radio/s.

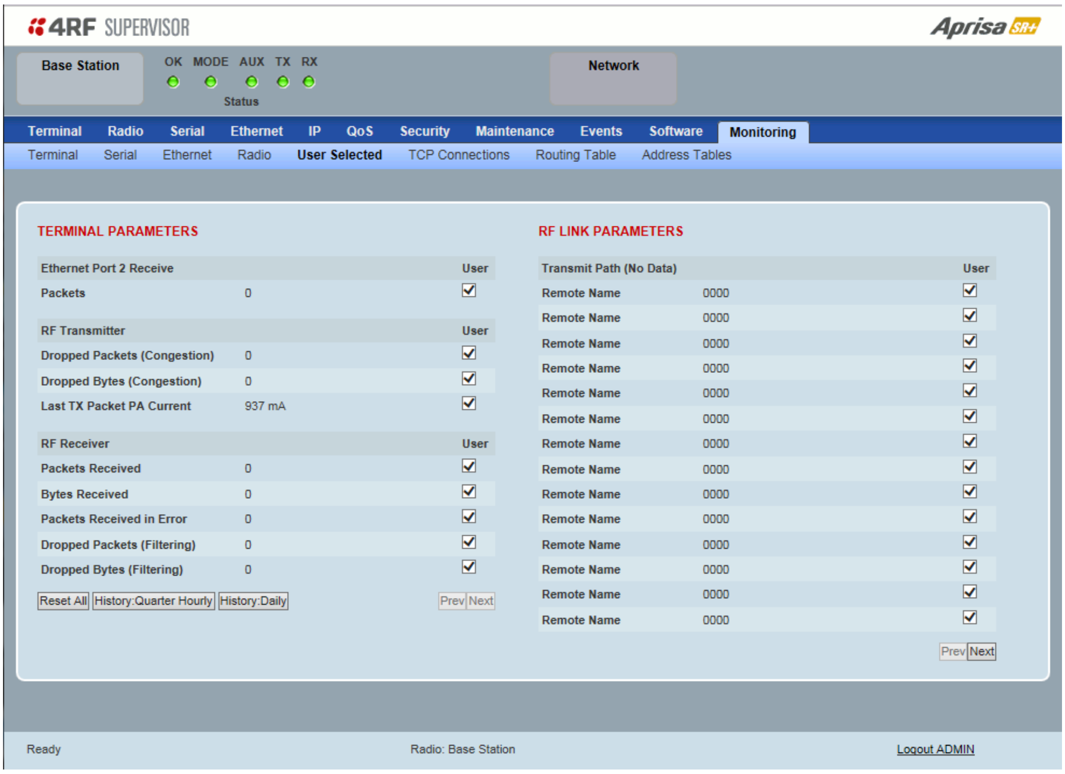
Controls

The Next button will display the next page of 8 radios and the Prev button will display the previous page of 8 radios.

Monitoring > User Selected

This page displays the ‘User’ parameters setup in all the other Monitoring screens e.g. in the Monitoring > Radio > Transmitter, the User checkbox is ticked for the Dropped Packets (Congestion) and Dropped Bytes (Congestion).

The results shown are since the page was opened and are updated automatically every 12 seconds.

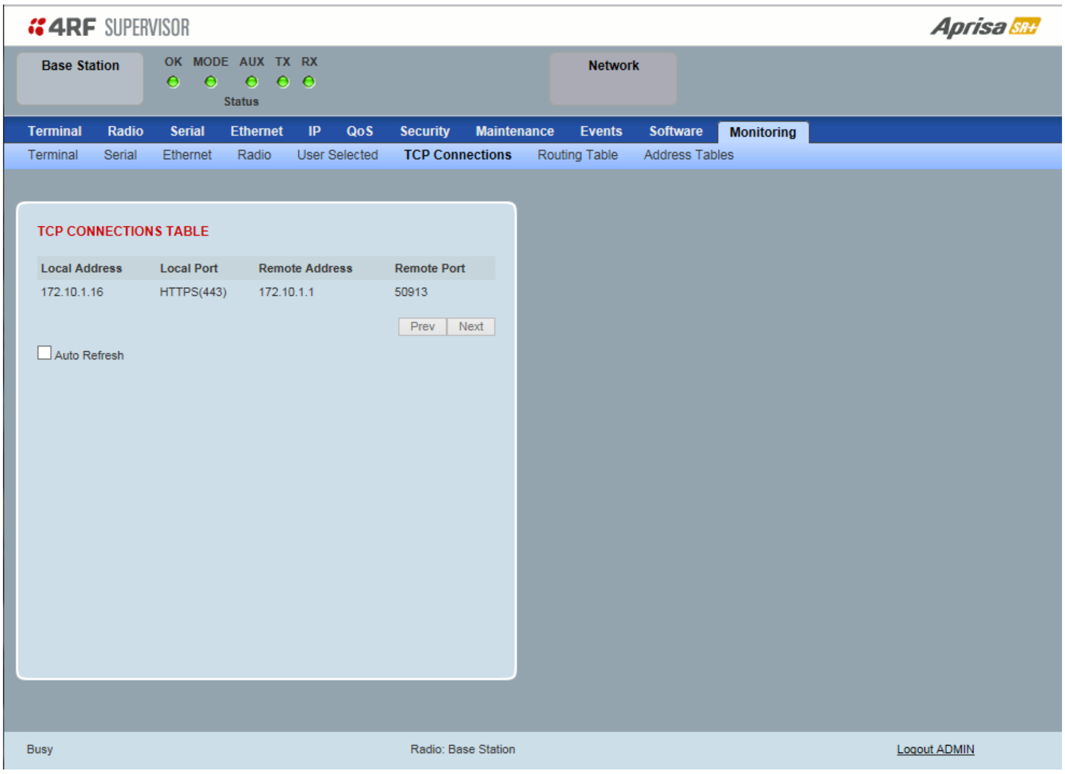


Controls

The Reset button clears the current results.

Monitoring > TCP Connections

This page displays the list of active TCP connections on the radio.



TCP CONNECTIONS TABLE

Result	Function
Local Address	The local radio IP address
Local Port	The local radio TCP port number
Remote Address	The remote host IP address (in most case a host PC connected to radio/network)
Remote Port	The local radio TCP port number (in most case a host PC connected to radio / network)

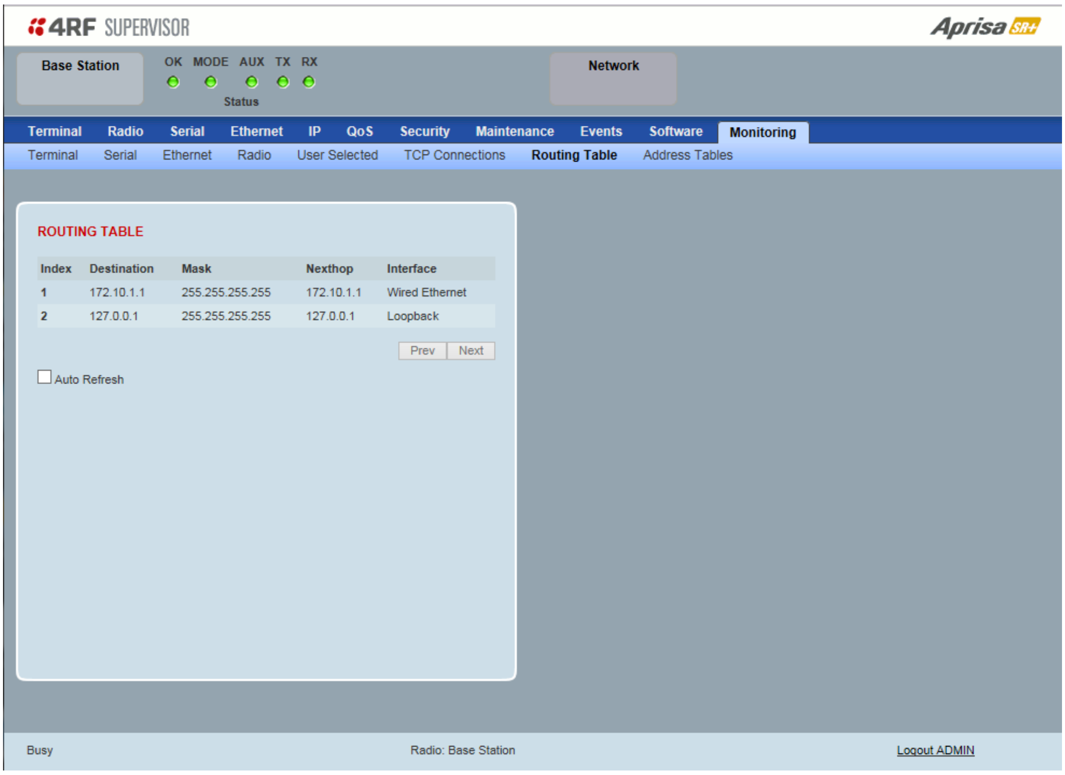
Controls

The Next button will display the next page of 8 connections and the Prev button will display the previous page of 8 connections.

If the Auto Refresh option is ticked, the TCP Connections table will refresh every 12 seconds.

Monitoring > Routing Table

This page displays the list of active routes on the radio.



ROUTING TABLE

Result	Function
Index	The routing table index
Destination	The target destination IP address of the route
Mask	The subnet mask of the destination IP address of the route
Next Hop	The next hop IP address on the path to the destination IP address of the route
Interface	The physical interface output on the path to the destination IP address of the route

Controls

The Next button will display the next page of 8 routes and the Prev button will display the previous page of 8 routes.

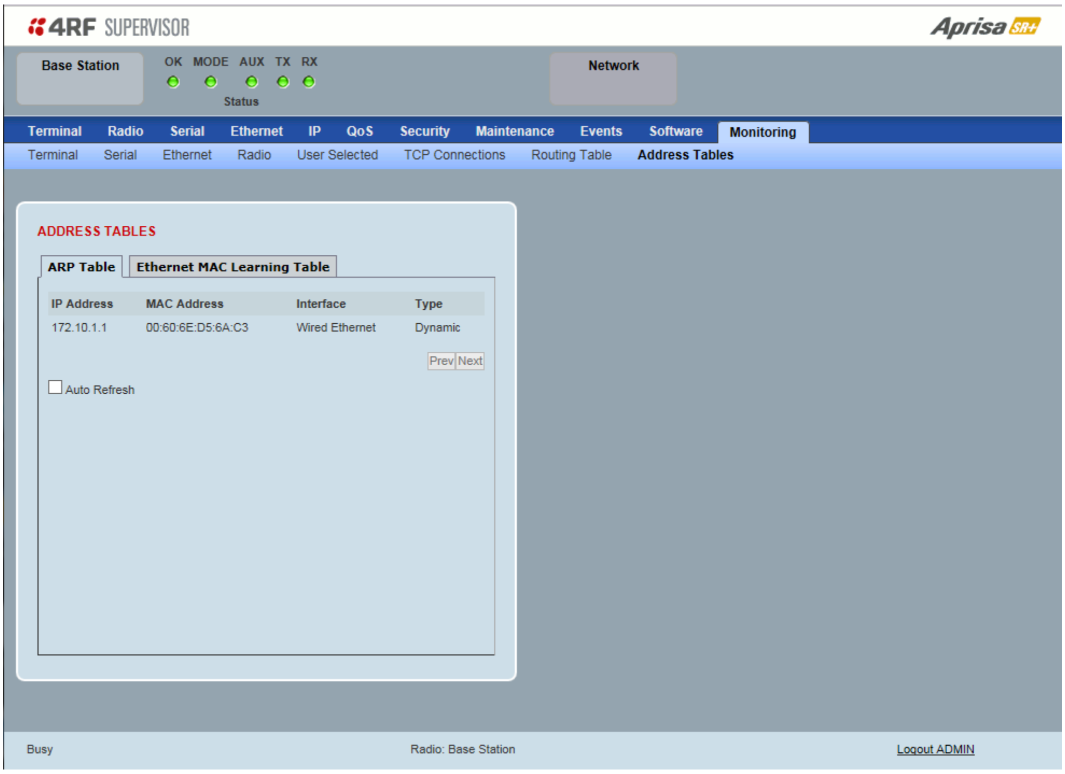
If the Auto Refresh option is ticked, the routing table will refresh every 12 seconds.

Monitoring > Address Tables

ARP Table

This page displays the current Address Resolution Protocols (ARP) on the radio. The radio implemented ARP protocol is used for resolution of network layer addresses into link layer addresses. It is used to map a IPv4 address to an Ethernet MAC address. The ARP table shows the results of the ARP protocol linkage between IPv4 address and Ethernet MAC address of the devices attached to the radio.

In a layer 2 bridge LAN, an upper layer protocol may include the IP address of the destination, but since it is an Ethernet LAN network, it also needs to know the destination MAC address. First, the radio uses a cached ARP table to look up the IPv4 destination address for the matching MAC address records. If the MAC address is found, it sends the IPv4 packet encapsulated in Ethernet frame with the found MAC address. If the ARP cache table did not produce a result for the destination IPv4 address, the radio sends a broadcast ARP message requesting an answer (of MAC address that matches) for IP address. The destination device responds with its MAC address (and IP). The response information is cached in radios' ARP table and the message can now be sent with the appropriate destination MAC address.



ADDRESS TABLES

Title	Function
IP Address	The IPv4 address of a neighboring device in the radio LAN network
MAC Address	The ARP result matching or mapping MAC address from the IPv4 address.
Interface	The Ethernet port interface the ARP results found the matching/mapping
Type	'Dynamic' indicates an ARP result and 'Static' indicates a user static mapping.

Controls

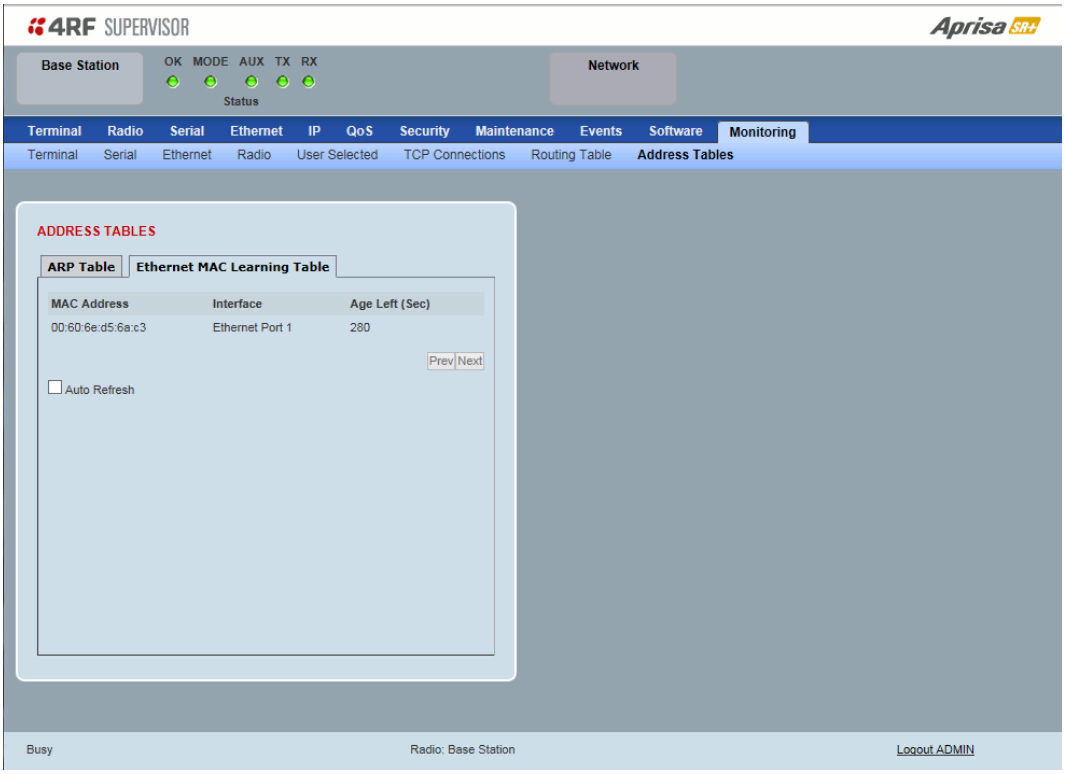
The Next button will display the next page of 8 addresses and the Prev button will display the previous page of 8 addresses.

If the Auto Refresh option is ticked, the ARP table will refresh every 12 seconds.

Ethernet MAC Learning Table

This page displays the current Ethernet Media Access Control (MAC) Address table on the radio LAN network. In order for the radio to switch frames between Ethernet LAN ports efficiently, the radio layer 2 bridge maintains a MAC address table. When the radio bridge receives a frame, it associates the MAC address of the sending network device with the LAN port on which it was received.

The bridge dynamically learns and builds the MAC address table by using the MAC source address of the frames received. When the radio bridge receives a frame for a MAC destination address not listed in its address table, it floods the frame to all LAN ports of the same LAN (or in case of VLAN, to the specific VLAN) except the port that received the frame. When the destination bridge device replies, the radio bridge adds its relevant MAC source address and interface port number to the MAC address table. The switch then forwards subsequent frames to a single LAN port without flooding all LAN ports.



ADDRESS TABLES

Title	Function
MAC Address	The learned MAC address of a neighboring bridge device in the LAN network.
Interface	The Ethernet port interface the MAC address has learned
Age left	The aging time of this MAC entry will stay in the table, even if this MAC address is not used. Every time this MAC address is used, the aging time restarts from its maximum. Default is 300 sec.

Controls

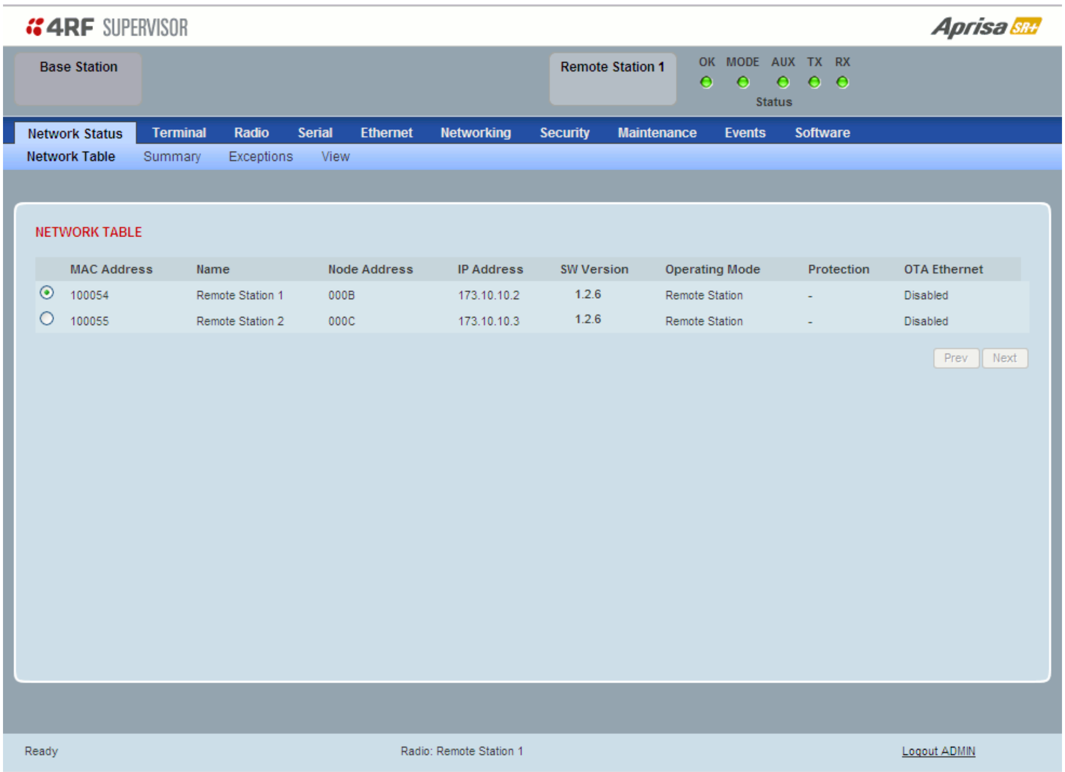
The Next button will display the next page of 8 addresses and the Prev button will display the previous page of 8 addresses.

If the Auto Refresh option is ticked, the routing table will refresh every 12 seconds.

Network Status

Network Status > Network Table

This page displays a list of all the registered remote stations for the base station and provides management access to each of the remote stations.



NETWORK TABLE

This Network Table is only available when the local radio is the base station i.e. SuperVisor is logged into the base station.

To manage a remote / repeater station with SuperVisor:

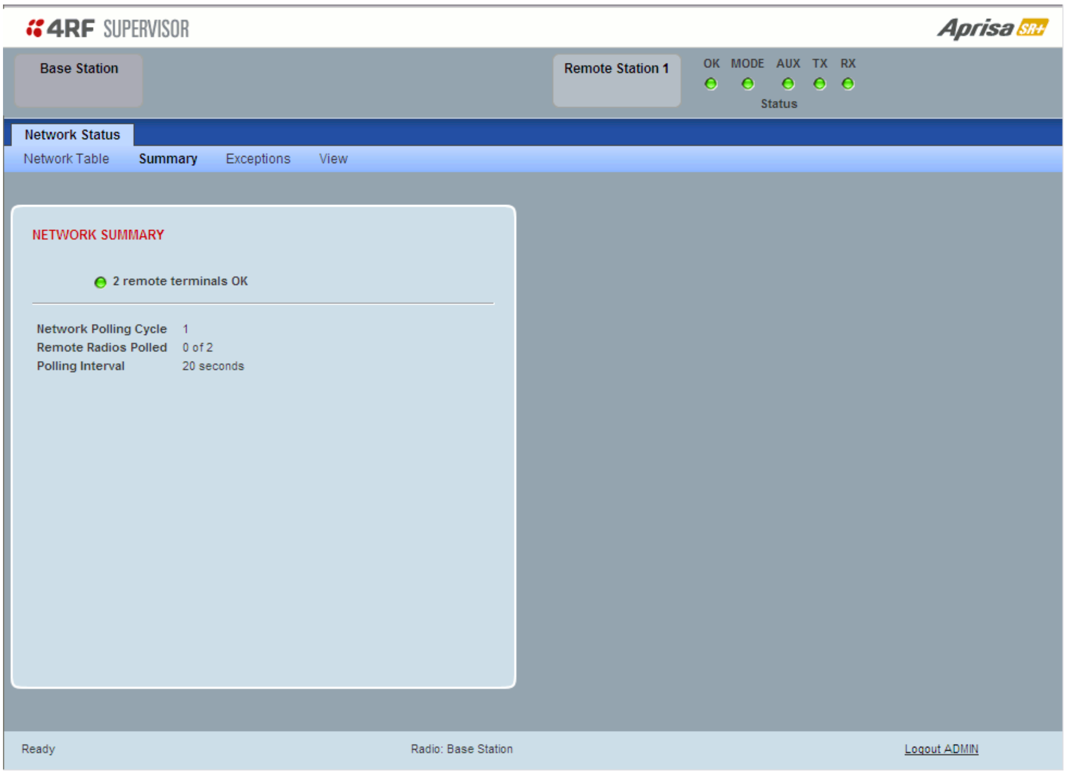
Click on the radio button of the required station. The remaining menu items then apply to the selected remote station.

Network Status > Summary

Network View is an overview of the health of the network providing the ability to investigate issues directly within SuperVisor.

This page provides an overall summary view of the alarm status of all registered remote stations for the base station. When open, it provides a continuous monitor of the network.

Depending on the poll period set (20 seconds minimum) and the number of remotes in the network, it will take at least three poll cycles to indicate a failure in the network. Initial results may indicate 'All ok' until at least three poll cycles completed. This could take Number Of Remotes * Poll Period * 3 seconds to complete.



NETWORK SUMMARY

A network poll will start when any of the Network Status pages are opened (Summary, Exceptions or View). The network poll will only continue to poll the remote stations if one of the Network Status pages is open (SuperVisor can lose PC focus). The network poll continues from where it was stopped last time it was polling.

The initial result assumes that all remote stations are operating correctly.

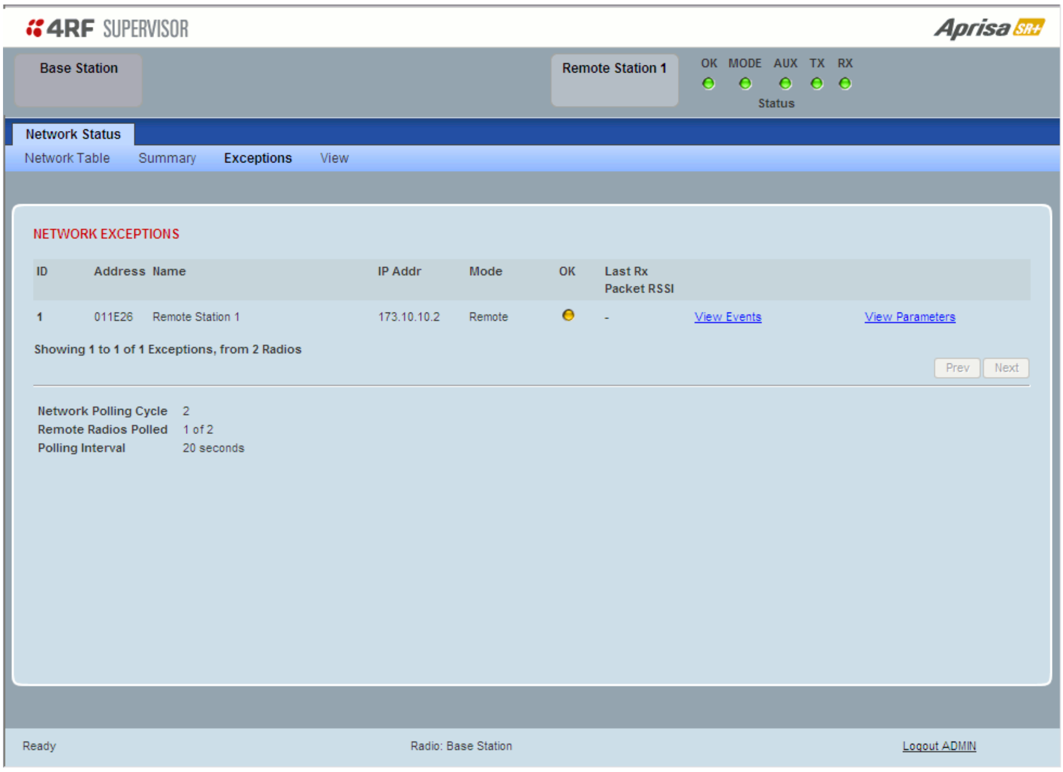
Network Summary Example:

Result	**Function**
Network Polling Cycle	The number of poll cycles since first opening a Network Status > Summary, Exceptions or View page. The page example shows 6 polling cycles.
Remote Radios Polled	This shows the number of radios polled for the current polling cycle out of the number remote radios registered with the base station. The page example shows 1 radio polled for the current polling cycle out of 3 remote radios registered.
Polling Interval	The time interval between the completion of one radio poll and the start of the next radio poll. To set the polling interval, see ‘Maintenance > General’ on page 193.

If a remote radio does not respond to a poll request within 10 seconds, the previous readings from that radio will be presented. Connectivity to a remote radio will be show as ‘lost’ if the remote radio has not responded to 3 consecutive poll requests.

Network Status > Exceptions

This page provides a list of all registered remote radios that are in an alarmed state or have stopped responding to the SuperVisor polling. When open, it provides a continuous monitor of the network.



NETWORK EXCEPTIONS

A network poll will start when any of the Network Status pages are opened (Summary, Exceptions or View). The network poll will only continue to poll the remote stations if one of the Network Status pages is open (SuperVisor can lose PC focus). The network poll continues from where it was stopped last time it was polling.

Network Exceptions Example:

Result	**Function**
Network Polling Cycle	The number of poll cycles since first opening a Network Status > Summary, Exceptions or View page. The page example shows 4 polling cycles.
Remote Radios Polled	This shows the number of radios polled for the current polling cycle out of the number remote radios registered with the base station. The page example shows 3 radios polled for the current polling cycle out of 4 remote radios registered.
Polling Interval	The time interval between the completion of one radio poll and the start of the next radio poll. To set the polling interval, see ‘Maintenance > General’ on page 193.

If a remote radio does not respond to a poll request within 10 seconds, the previous readings from that radio will be presented. Connectivity to a remote radio will be show as 'lost' if the remote radio has not responded to 3 consecutive poll requests.

If a remote radio on the list is detected to be responding to a poll request and no longer be in an alarmed state, the entry for this remote radio will be removed from the list.

View Events

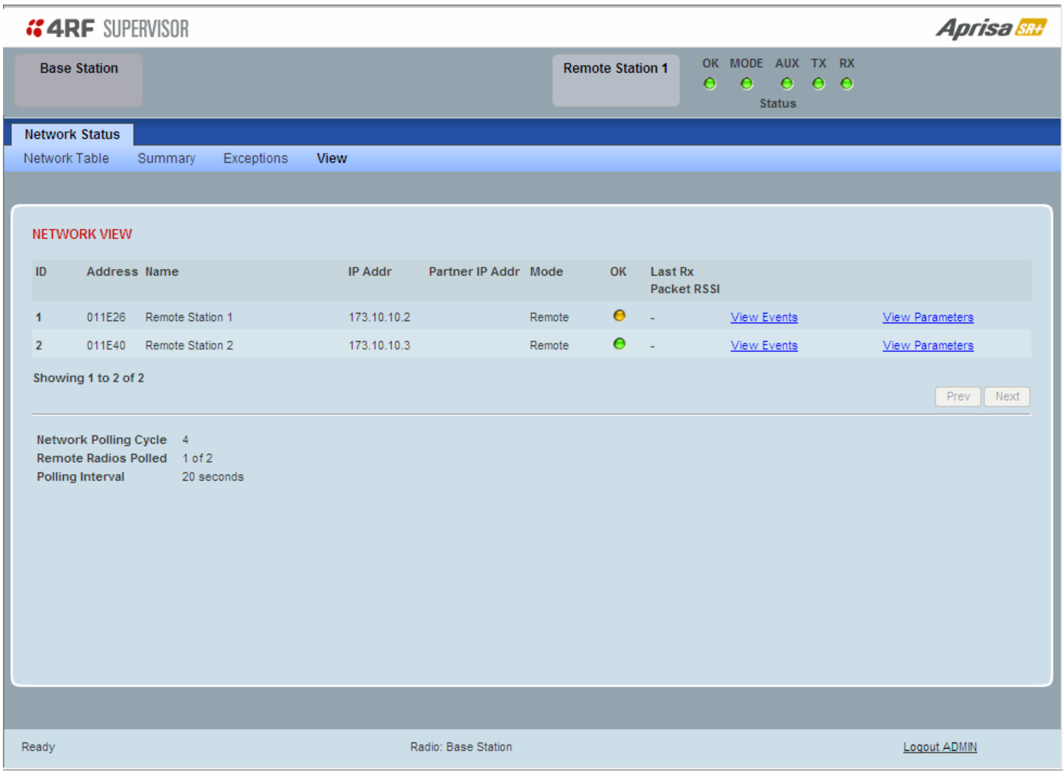
Clicking on View Events navigates to the Events page (see 'Events' on page 206) for the specific remote radio where the radio events will be displayed.

View Parameters

Clicking on View Parameters navigates to the Monitoring page (see 'Monitoring' on page 236) for the specific remote radio where the radio parameters will be displayed.

Network Status > View

This page provides a complete list of all registered remote radios. It is similar to the Exceptions page but it shows all radios, not limited to the radios with alarms. When open, it provides a continuous monitor of the network.



NETWORK VIEW

A network poll will start when any of the Network Status pages are opened (Summary, Exceptions or View). The network poll will only continue to poll the remote stations if one of the Network Status pages is open (SuperVisor can lose PC focus). The network poll continues from where it was stopped last time it was polling.

Network View Example:

Result	Function
Network Polling Cycle	The number of poll cycles since first opening a Network Status > Summary, Exceptions or View page. The page example shows 2 polling cycles.
Remote Radios Polled	This shows the number of radios polled for the current polling cycle out of the number remote radios registered with the base station. The page example shows 1 radio polled for the current polling cycle out of 3 remote radios registered.
Polling Interval	The time interval between the completion of one radio poll and the start of the next radio poll. To set the polling interval, see 'Maintenance > General' on page 193. Note: as this polling feature utilizes air time, the polling interval should be selected to suit the network traffic.

If a remote radio does not respond to a poll request within 10 seconds, the previous readings from that radio will be presented. Connectivity to a remote radio will be show as ‘lost’ if the remote radio has not responded to 3 consecutive poll requests.

View Events

Clicking on View Events navigates to the Events page (see ‘Events’ on page 206) for the specific remote radio where the radio events will be displayed.

View Parameters

Clicking on View Parameters navigates to the Monitoring page (see ‘Monitoring’ on page 236) for the specific remote radio where the radio parameters will be displayed.

Protected Station

The majority of SuperVisor screens are the same for the standard radio and the protected station. The following screens are specific to the protected station.

Logging into a Protected Station

When SuperVisor detects a protected station, it operates in Single Session Management operation mode.

When in Single Session Management mode, SuperVisor will automatically detect the two individual Aprisa SR+ radios configured to pair together for protection, and manage the two units in a single browser session. To the user, it will appear as managing a single unit, but SuperVisor will interact with the two individual units at a lower level.

The user can login with the IP address of either the Primary or Secondary radio to manage the protected station (don't use the PVIP address as it is not a management IP address). SuperVisor will present all information appropriately where 'Common Parameters' will be presented to the user as a single parameter e.g. TX and RX Frequencies and 'Unit Specific Parameters' will be presented to the user as Primary or Secondary parameters e.g. Events and Alarms.

When saving data, SuperVisor will also validate and ensure that the correct settings are written to both units. The SuperVisor Single Session Management ensures that both units of the protected station are always configured correctly to complement each other as protected partners.

The user can still login with two different sessions to the active and standby radios. If the user opens two session management, one session logged into the active radio and a second session logged into the standby radio, the Multiple Management Sessions pop-up message will show the user names and IP addresses of the active and standby radio.

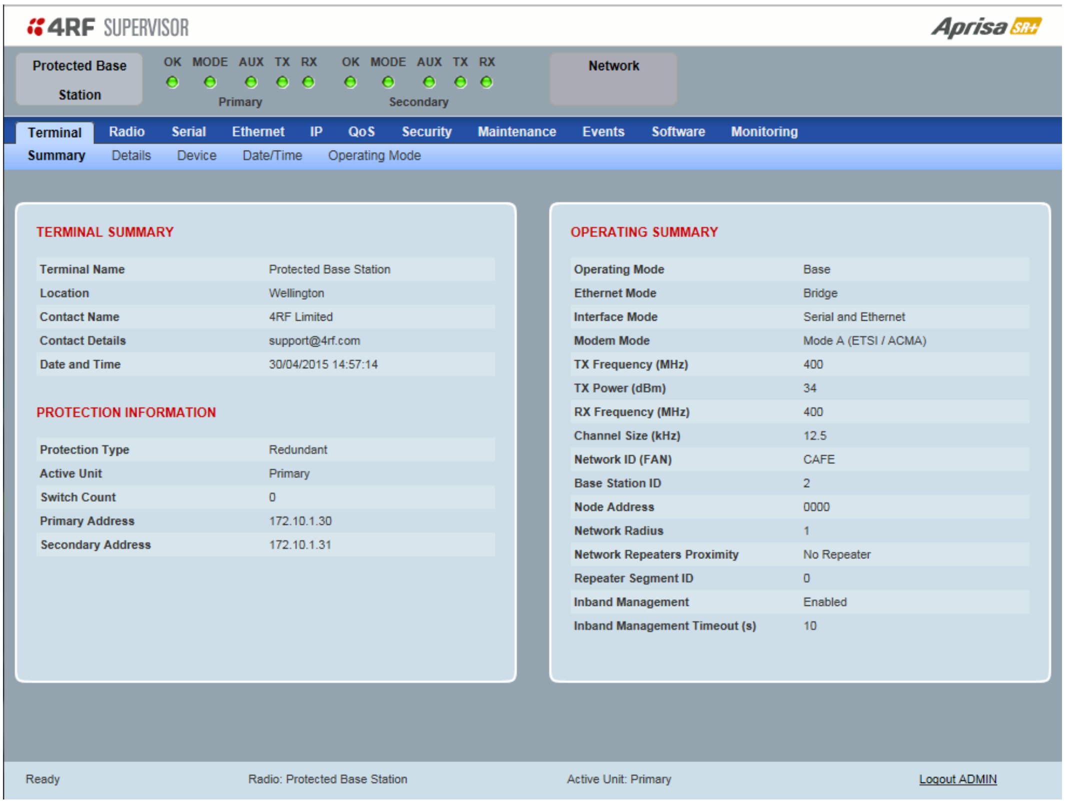
Parameter Errors

On protected station screens, parameter values displayed in red indicate discrepancies in common parameter values between the primary and secondary radios (see 'Protected Station: Terminal > Summary' on page 262 for an example of the red display). The value displayed is from the 'addressed radio'.

These value discrepancies can occur if the two protected station radios have been separately configured. The discrepancies can be corrected by re-entering the values in one of the radios. The value will be copied to the partner radio.

Terminal

Protected Station: Terminal > Summary



TERMINAL SUMMARY

This page displays the current settings for the Terminal parameters.

PROTECTION INFORMATION

Protection Type

This parameter shows the type of protection:

Option	Function
Serial Data Driven Switching	Provides radio and RS-232 serial port user interface protection for Aprisa SR+ radios.
Monitored Hot Standby (Protected Station)	The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio. The standby radio is monitored to ensure its correct operation should a switch-over be required. See 'Monitored Alarms' on page 316 for the list of monitored alarms.
Redundant (Protected Station)	The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio

Active Unit

This parameter shows the radio which is currently active (Primary or Secondary).

Switch Count

This parameter shows the number of protection switch-overs since the last radio reboot (volatile).

Primary Address

This parameter shows the IP address of the primary radio (usually the left side radio A).

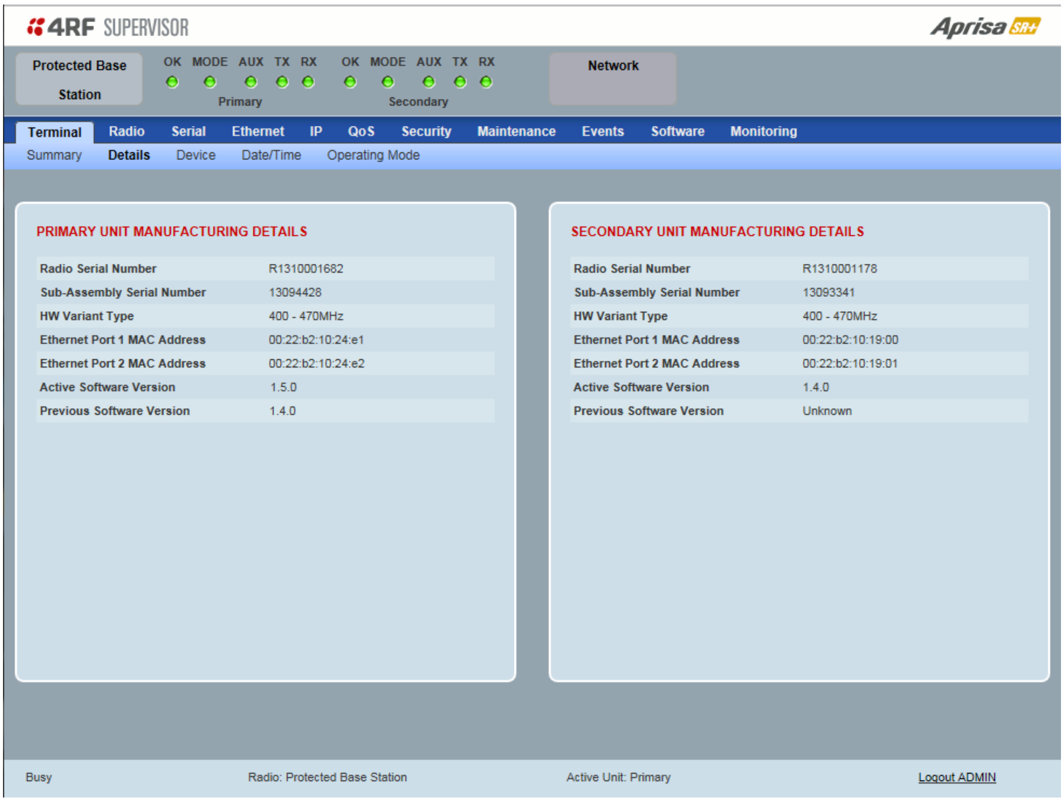
Secondary Address

This parameter shows the IP address of the secondary radio (usually the right side radio B).

OPERATING SUMMARY

See 'Terminal > Summary' on page 80 for parameter details.

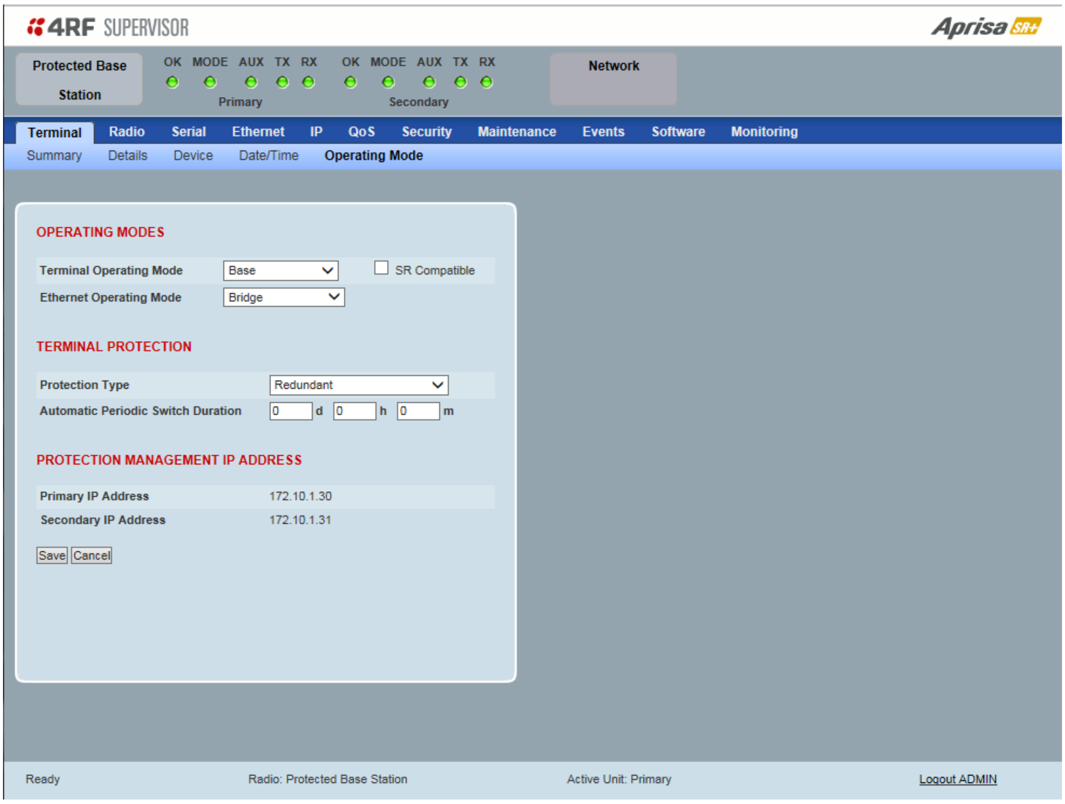
Protected Station: Terminal > Details



PRIMARY UNIT / SECONDARY UNIT MANUFACTURING DETAILS

See 'Terminal > Details' on page 83 for parameter settings.

Protected Station: Terminal > Operating Mode



OPERATING MODES

Terminal Operating Mode

The Terminal Operating Mode can be set to Base, Base Repeater, Repeater or Remote station. The default setting is Remote.

Option	Function
Base	The base station manages all traffic activity between itself, repeaters and remotes. It is the center-point of network where in most cases will be connected to a SCADA master.
Base Repeater	The base-repeater has the same function as the base station (and repeater station), but used when peer to peer connections between remotes is required via the base station.
Repeater	The repeater forwards packets coming from base station and other repeaters e.g. in daisy chain LBS mode and /or remote stations.
Remote	The remote in most cases is used as the end-point of the SCADA network connected to an RTU or PLC device for SCADA network control and monitoring.

Ethernet Operating Mode

The Ethernet Operating Mode defines how Ethernet / IP traffic is processed in the radio. The default setting is Bridge.

Option	Function
Bridge	Bridge mode inspects each incoming Ethernet frame source and destination MAC addresses to determine if the frame is forwarded over the radio link or discarded.
Gateway Router	Gateway Router mode inspects each incoming IP source and destination IP addresses to determine if the packet is forwarded over the radio link or discarded. In this mode, all Ethernet interfaces have the same IP address and subnet.
Router	Router mode inspects each incoming IP source and destination IP addresses to determine if the packet is forwarded over the radio link or discarded. In this mode, each Ethernet interface has a different IP address and subnet.

SR Compatible

The SR Compatible option enables over-the-air point-to-multipoint interoperation between an Aprisa SR+ network and New Aprisa SR radios. The default setting is unticked.

When the Aprisa SR+ ‘SR Compatible’ option is activated, the Aprisa SR+ locks its modulation to QPSK (as per the New Aprisa SR modulation) and disables functionality which is not available in the New Aprisa SR for full compatibility / interoperability operation.

This compatibility option allows the user a smooth migration to Aprisa SR+ when higher speeds of 120, 60 kbit/s (at 25, 12.5 kHz channel sizes), Adaptive Coding Modulation, full duplex and more features are required.

TERMINAL PROTECTION

Protection Type

The Protection Type defines if a radio is a stand-alone radio or part of an Aprisa SR+ Protected Station. The default setting is None.

Option	Function
None	The SR+ radio is a stand-alone radio (not part of an Aprisa SR+ Protected Station).
Redundant (Protected Station)	The SR+ radio is part of an Aprisa SR+ Protected Station. The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio
Monitored Hot Standby (Protected Station)	Set to make this SR+ radio part of an Aprisa SR+ Protected Station. The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio. The standby radio is monitored to ensure its correct operation should a switch-over be required. See 'Monitored Alarms' on page 316 for the list of monitored alarms.
Serial Data Driven Switching	The SR+ radio is part of an Aprisa SR+ Data Driven Protected Station. Provides radio and RS-232 serial port user interface protection for Aprisa SR+ radios.

Automatic Periodic Switch Duration

The Automatic Periodic Switch Duration sets the time interval for automatic switch-over from the active radio to the standby radio.

This feature will automatically switch-over from the active radio to the standby radio if there are no alarms preventing the switch-over to the standby radio. It can be used to provide confidence that the standby radio is still operational maybe after many days of standby operation.

The maximum number of days that can be set is 49 days.

The default setting is 0 which disables the automatic switch-over feature.

PROTECTION MANAGEMENT IP ADDRESS

Primary Address

This parameter shows the IP address of the primary radio (usually the left side radio A).

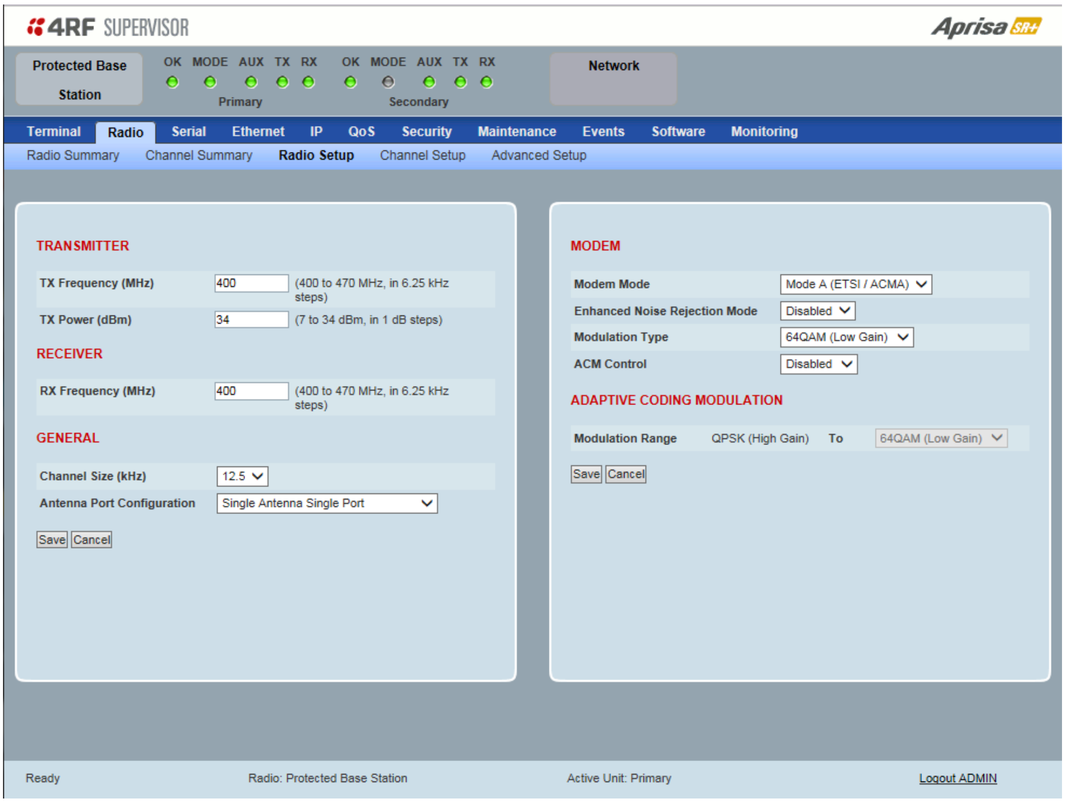
Secondary Address

This parameter shows the IP address of the secondary radio (usually the right side radio B).

Radio

Protected Station: Radio > Radio Setup

Transmit frequency, transmit power and channel size would normally be defined by a local regulatory body and licensed to a particular user. Refer to your site license details when setting these fields.



Antenna Port Configuration

This parameter sets the Antenna Port Configuration for the radio. For more information on single and dual antenna port part numbers and cabling options, see 'Cabling' on page 323.

Option	Function
Single Antenna Single Port	Select Single Antenna Single Port for a single antenna protected station using one or two frequency half duplex transmission. The antenna is connected to the ANT port.
Single Antenna Dual Port (duplexer)	Select Single Antenna Dual Port for a single antenna protected station using: (1) One or two frequency in half duplex transmission with an external duplexer (for filtering) connected to the ANT/TX and RX antenna ports and single antenna connected to the duplexer. (2) Two frequency in full duplex transmission with an external duplexer (for full duplex operation) connected to the ANT/TX and RX antenna ports and single antenna connected to the duplexer. (3) Single frequency in half duplex transmission with external dual antennas, connected to the ANT/TX and RX antenna ports. (4) Two frequency in half or full duplex transmission with external dual antennas, connected to the ANT/TX and RX antenna ports.

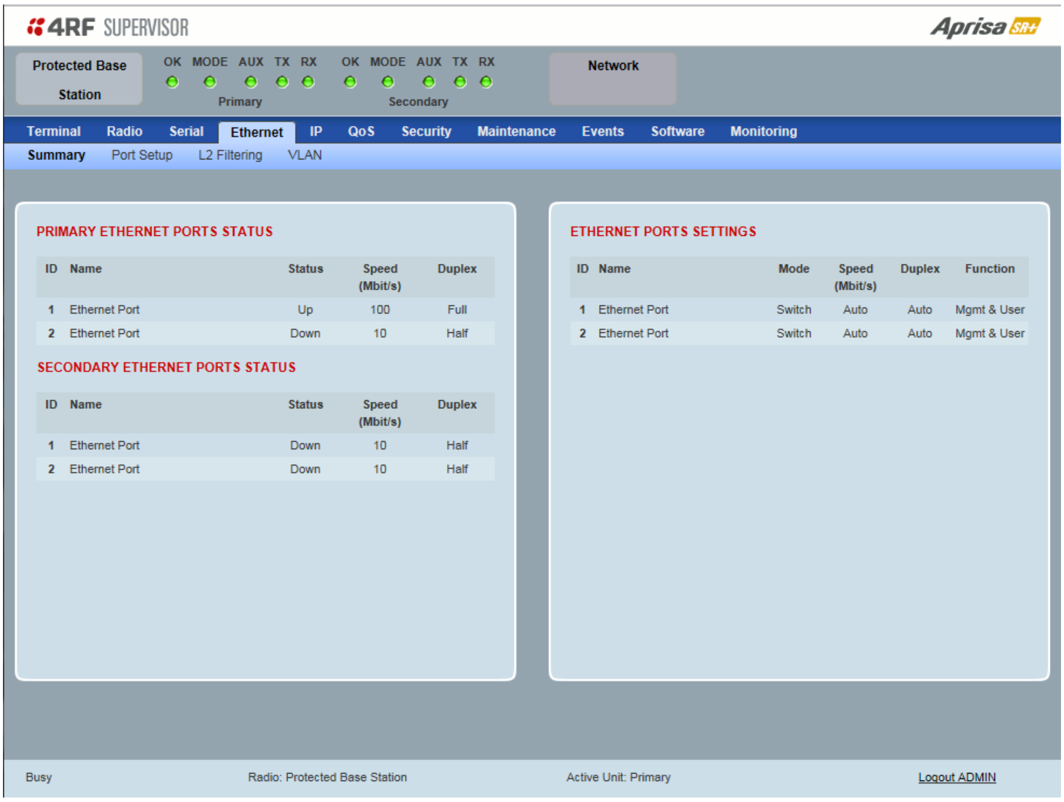
Dual Antenna Single Port	Select Dual Antenna Single Port for a dual antenna protected station using one or two frequency half duplex transmission. The antenna is connected to the A and B TX/ANT ports.
Dual Antenna Dual Port (duplexer)	Select Dual Antenna Dual Port for a dual antenna protected station using: (1) One or two frequency in half duplex transmission with two external duplexer (for filtering) connected to the A and B ANT/TX and RX antenna ports and single antenna connected to the duplexer. (2) Two frequency in full duplex transmission with an external duplexer (for full duplex operation) connected to the A and B ANT/TX and RX antenna ports and single antenna connected to the duplexer. (3) Single frequency in half duplex transmission with an external dual antennas, connected to the A and B ANT/TX and RX antenna ports. (4) Two frequency in half or full duplex transmission with external dual antennas, connected to the A and B ANT/TX and RX antenna ports.

The default setting is Single Antenna Single Port.

Ethernet

Protected Station: Ethernet > Summary

This page displays the current settings for the Protected Station Ethernet port parameters.

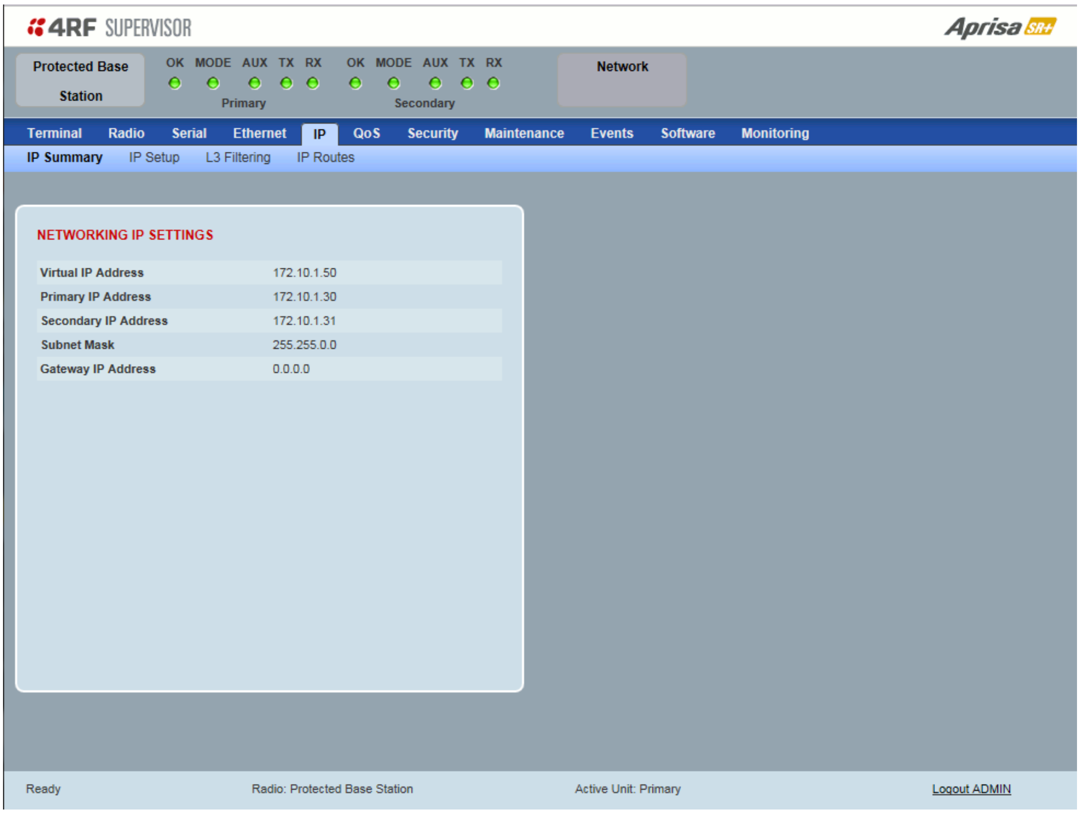


See ‘Ethernet > Port Setup’ for configuration options.

IP

Protected Station: IP > IP Summary

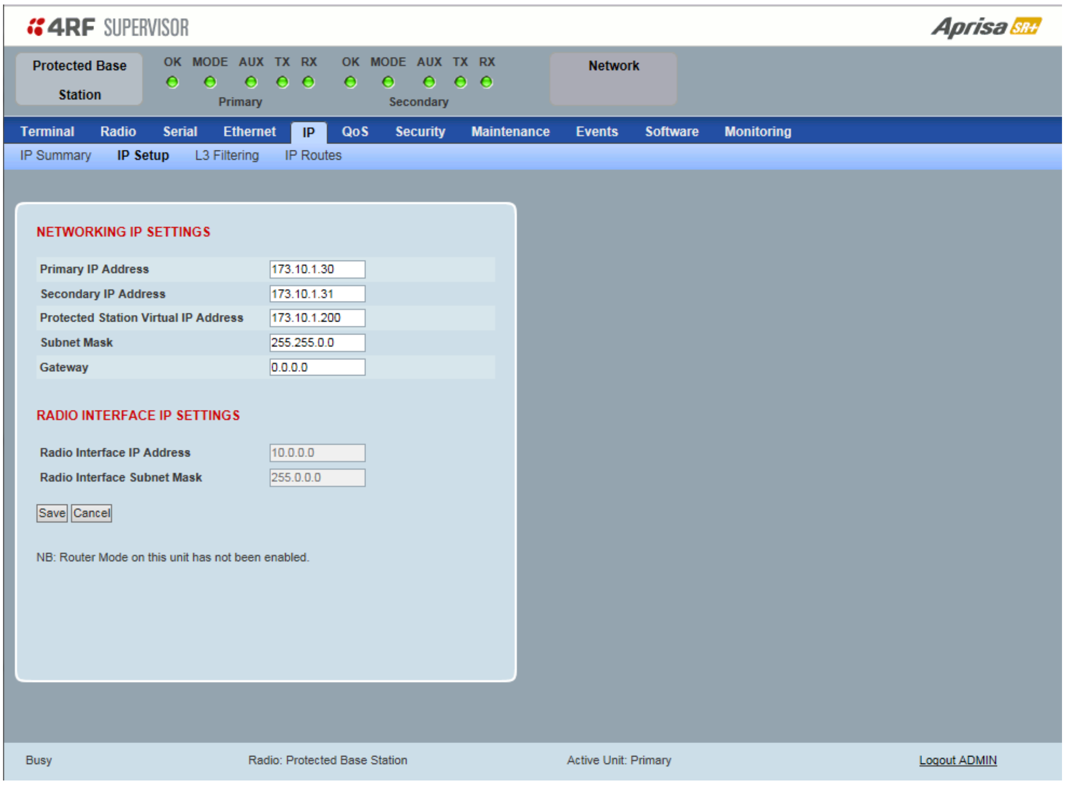
This page displays the current settings for the Protected Station Networking IP settings.



See 'IP > IP Summary > Bridge / Gateway Router Modes' on page 136 for configuration options.

Protected Station: IP > IP Setup

This page provides the setup for the Protected Station Networking IP setup.



NETWORKING IP SETTINGS

Changes in these parameters are automatically changed in the partner radio.

Primary IP Address

Set the static IP Address of the primary radio assigned by your site network administrator using the standard format xxx.xxx.xxx.xxx. The default IP address is in the range 169.254.50.10.

Secondary IP Address

Set the static IP Address of the secondary radio assigned by your site network administrator using the standard format xxx.xxx.xxx.xxx. The default IP address is in the range 169.254.50.10.

Protected Station Virtual IP Address (PVIP)

The Protected Station Virtual IP Address (PVIP) is the IP Address of the active radio whether it is the primary radio or the secondary radio.

The PVIP is available in both bridge and router modes.

In router mode, the PVIP can be used as ‘next hop’ IP address by external routers to reach the protected station so the protection station switch will always be transparent to the external devices and routers.

In both bridge and router modes, the PVIP is used in terminal server mode in remote protected stations. The PVIP is used to reach the protected remote station from the SCADA master connected to base station in terminal server mode.

Note: The radio IP address should be used for SNMP management as using the PVIP for SNMP management will result in undefined behaviour if a switch-over occurs during an SNMP transaction. Thus, using PVIP for SNMP network management is not recommended.

After a switch-over, new active radio owns the PVIP and will send out a gratuitous ARP to clear the MAC learning tables of upstream switches/routers.

Set the static IP Address of the PVIP using the standard format xxx.xxx.xxx.xxx. The default IP address is 0.0.0.0.

Subnet Mask

Set the Subnet Mask of the radio using the standard format xxx.xxx.xxx.xxx. The default subnet mask is 255.255.0.0.

Gateway

Set the Gateway address of the radio, if required, using the standard format xxx.xxx.xxx. The default Gateway is 0.0.0.0.

RADIO INTERFACE IP SETTINGS

The RF interface IP address is the address that traffic is routed to for transport over the radio link. This IP address is only used when Router Mode is selected i.e. not used in Bridge Mode.

Radio Interface IP Address

Set the IP Address of the RF interface using the standard format xxx.xxx.xxx.xxx. The default IP address is in the range 10.0.0.0.

Radio Interface Subnet Mask

Set the Subnet Mask of the RF interface using the standard format xxx.xxx.xxx.xxx. The default subnet mask is 255.255.0.0 (/16).

Note 1: If the base station RF interface IP address is a network IP address, and if the remote radio is also using a network IP address within the same subnet or different subnet, then the base radio will assign an automatic RF interface IP address from its own subnet.

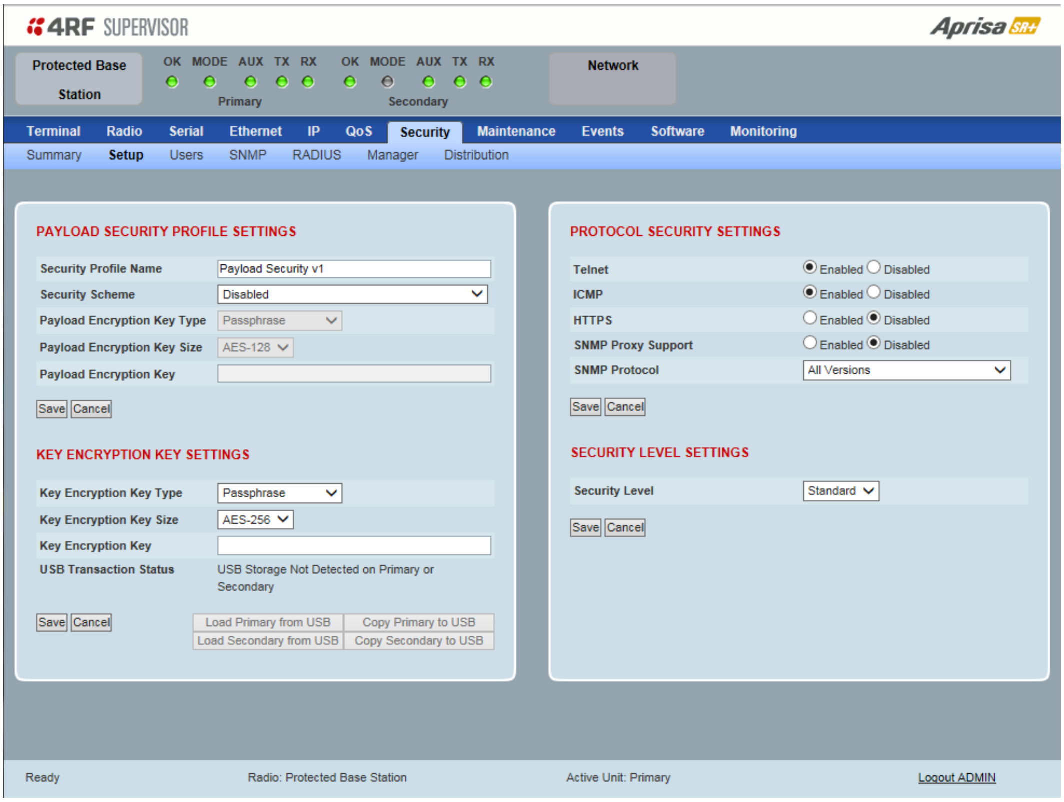
When the base radio has a host specific RF interface IP address, then all the remotes must have a host specific RF interface IP address from the same subnet.

Note 2: When a remote radio is configured for Router Mode and the base radio is changed from Bridge Mode to Router Mode and the RF interface IP address is set to AUTO IP configuration (at least the last octet of the RF interface IP address is zero), it is mandatory to configure the network topology by using the 'Decommission Node' and 'Discover Nodes' (see 'Maintenance > Advanced' on page 202).

Security

Protected Station: Security > Setup

This page displays the current settings for the Security parameters.



KEY ENCRYPTION KEY SETTINGS

USB Transaction Status

This parameter shows if a USB flash drive is plugged into the radio host port .

Option	Function
USB Storage Disconnected	A USB flash drive is not plugged into the radio host port.
USB Storage Connected	A USB flash drive is plugged into the radio host port.

Controls

These buttons are grayed out if a USB flash drive is not plugged into the radio host port.

The ‘Load Primary From USB’ button loads the Key Encryption Key settings from the primary radio USB flash drive into the primary radio.

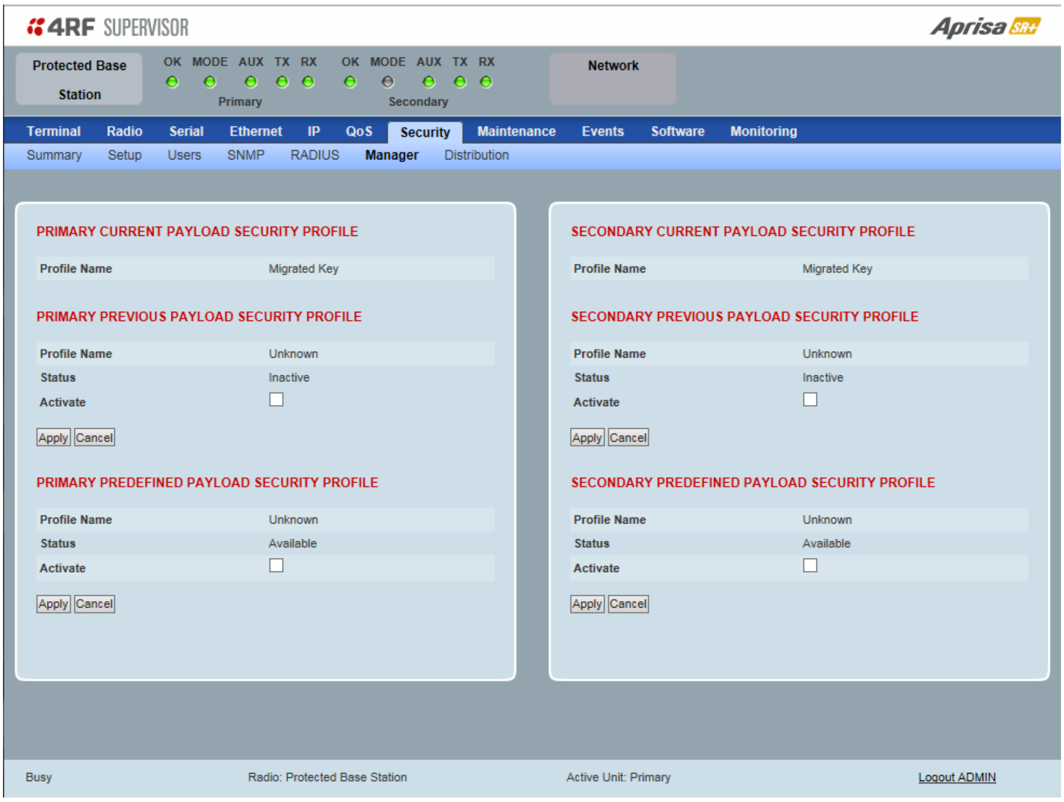
The ‘Copy To Primary USB’ button copies the Key Encryption Key settings from the primary radio to the primary radio USB flash drive.

The ‘Load Secondary From USB’ button loads the Key Encryption Key settings from the secondary radio USB flash drive into the secondary radio.

The ‘Copy To Secondary USB’ button copies the Key Encryption Key settings from the secondary radio to the secondary radio USB flash drive.

Protected Station: Security > Manager

This page provides the management and control of the Protected Station Networking Security settings.



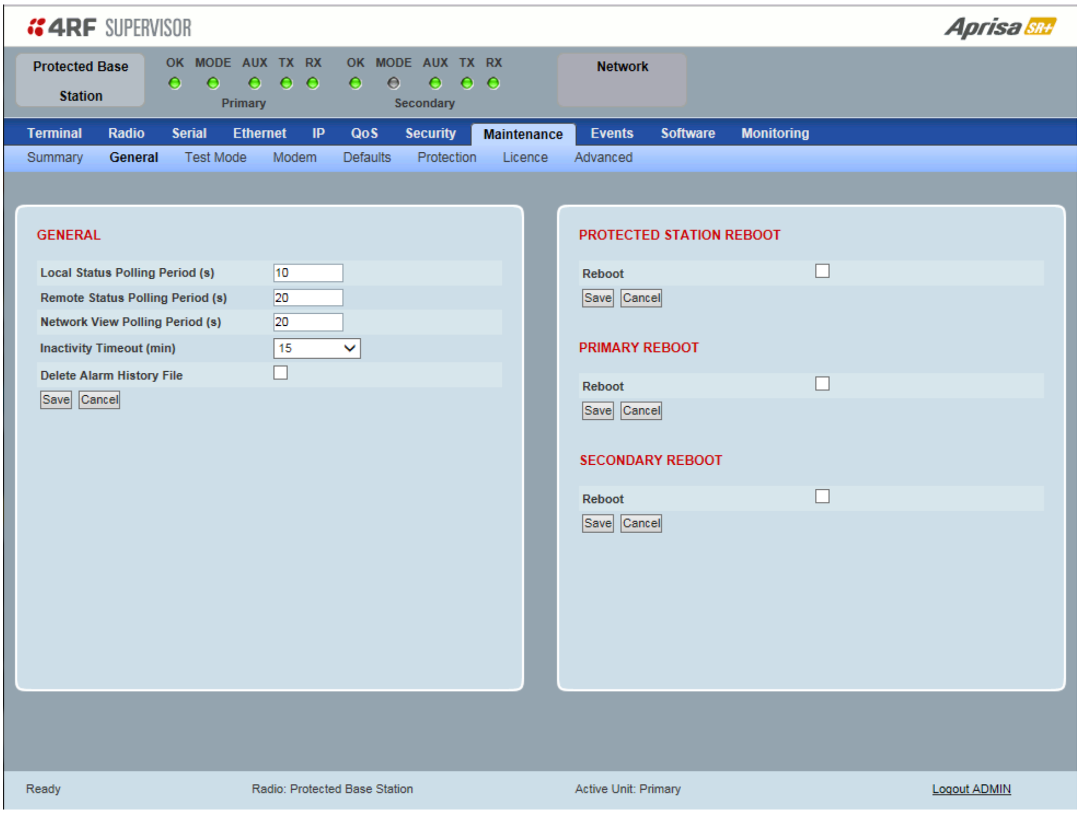
PRIMARY / SECONDARY SECURITY PROFILE

See 'Security > Manager' on page 184 for parameter details.

Maintenance

Protected Station: Maintenance > General

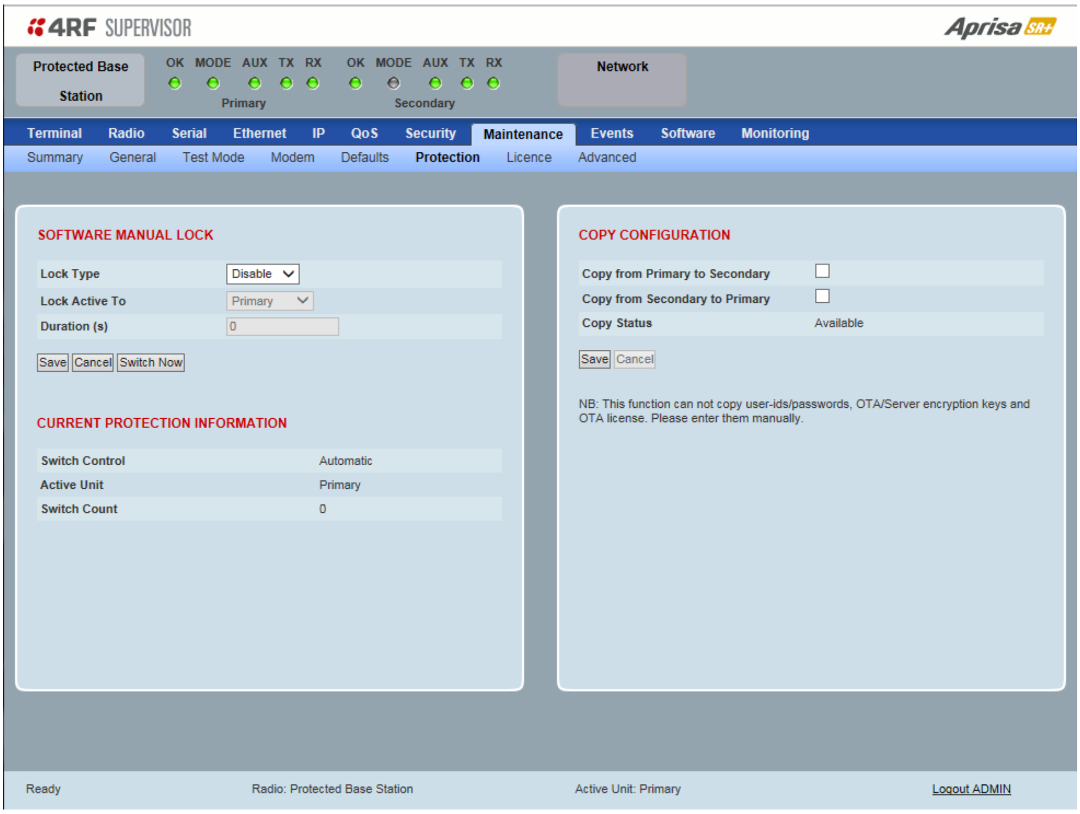
This page provides the management and control of the Protected Station Maintenance General settings.



See 'Maintenance > General' on page 193 for parameter details.

Protected Station: Maintenance > Protection

This page provides the management and control of the Protected Station Maintenance Protection settings.



SOFTWARE MANUAL LOCK

The software Manual Lock is a software implementation of the Hardware Manual Lock switch on the Protection Switch.

Lock Active To

This parameter sets the Protection Switch Software Manual Lock. The Software Manual Lock only operates if the Hardware Manual Lock is deactivated (set to the Auto position).

Option	Function
Automatic	The protection is automatic and switching will be governed by normal switching and blocking criteria.
Primary	The primary radio will become active i.e. traffic will be switched to the primary radio.
Secondary	The secondary radio will become active i.e. traffic will be switched to the secondary radio.

Duration (s)

This parameter defines the period required for manually locking to the primary or secondary radios. When this period elapses, the Lock To becomes automatic.

Switch Now Button

This button forces a switch-over independent of the state of Lock Type.

CURRENT PROTECTION INFORMATION

Switch Control

This parameter shows the status of the switch control i.e. which mechanism is in control of the protection switch.

Option	Function
Automatic	The protection is automatic and switching will be governed by normal switching and blocking criteria.
Software Manual Lock	The Software Manual Lock has control of the protection switch.
Hardware Manual Lock	The Hardware Manual Lock has control of the protection switch.

Active Unit

This parameter shows the radio which is currently active (Primary or Secondary).

Switch Count

This parameter shows the number of protection switch-overs since the last radio reboot (volatile).

Automatic Periodic Switch will occur in

If this parameter is visible, the Automatic Periodic Switch feature has been enabled and will show the period before the next automatic switch-over.

COPY CONFIGURATION

When common parameters are changed in one radio, they are automatically changed in the partner radio but if one radio has been replaced in the protected station, common parameters will need to be updated in the new radio.

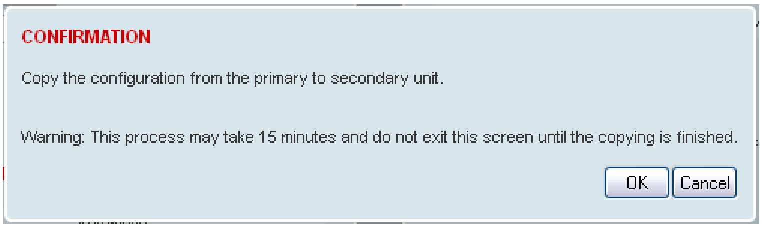
Note: This function does not copy user IDs, passwords, encryption keys or licenses. These must be entered manually.

Copy from Primary to Secondary

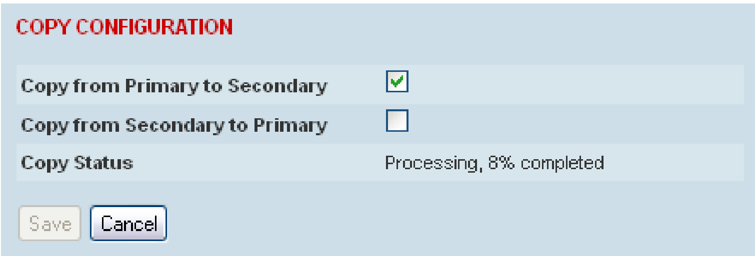
This parameter copies all common parameters from the primary to the secondary radio.

To activate copy configuration:

1. Tick the Copy from Primary to Secondary and click Save.



2. To continue, click OK.



Copy from Secondary to Primary

This parameter copies all common parameters from the secondary to the primary radio.

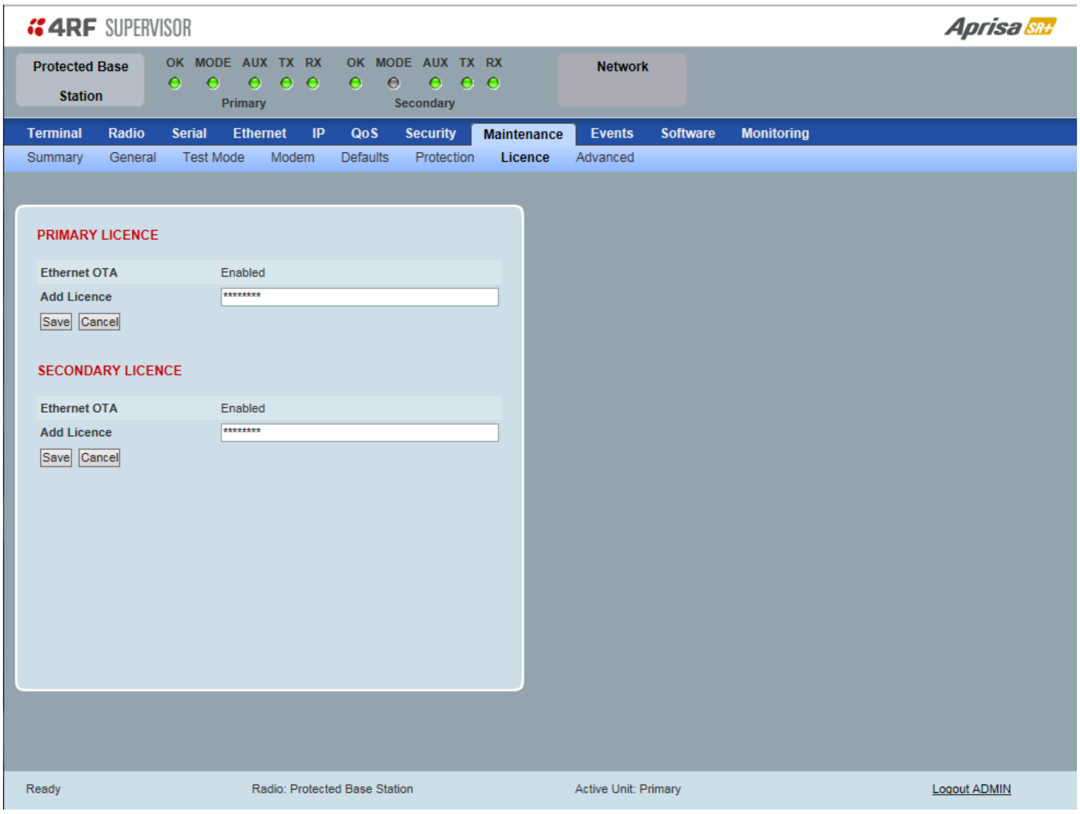
Copy Status

This parameter displays the status of the Copy Configuration.

Option	Function
Available	The Copy Configuration feature can be used (but not necessarily required).
Processing	The Copy Configuration feature is running and the % completed.

Protected Station: Maintenance > Licence

This page provides the management and control of the Protected Station Maintenance Licence settings.

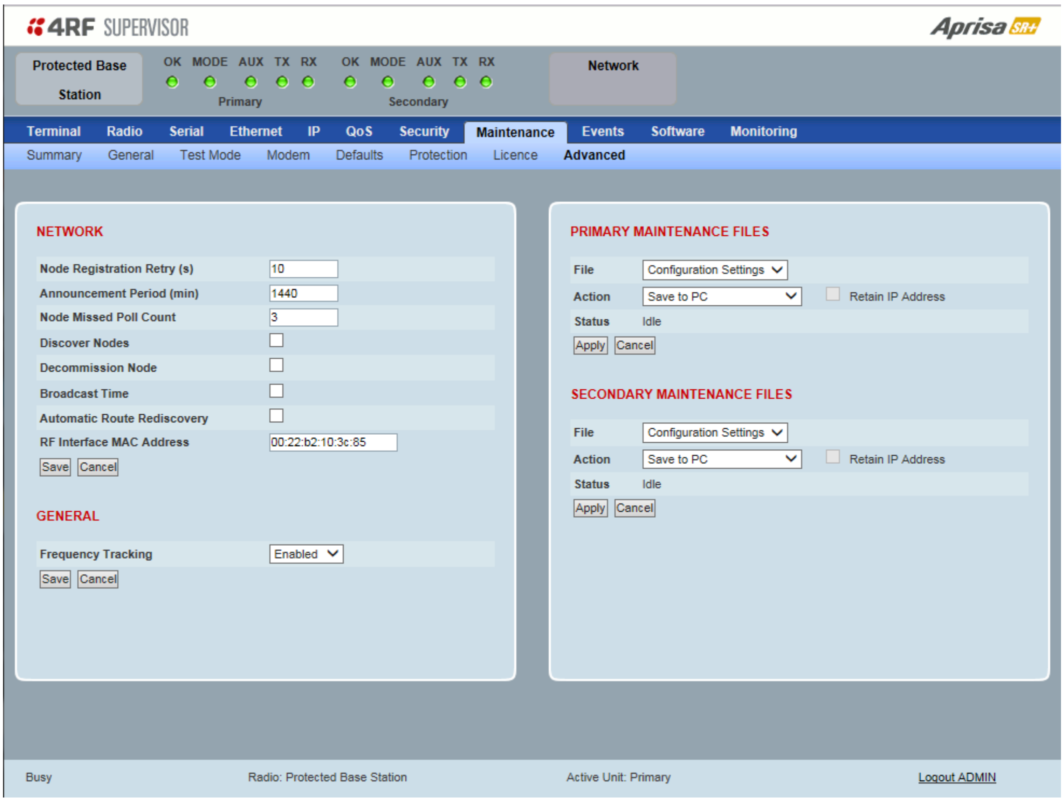


PRIMARY / SECONDARY LICENCE

See 'Maintenance > Licence' on page 201 for parameter details.

Protected Station: Maintenance > Advanced

This page provides the management and control of the Protected Station Maintenance Advanced settings.



NETWORK

See 'Maintenance > Advanced' on page 202 for parameter details.

RF Interface MAC address

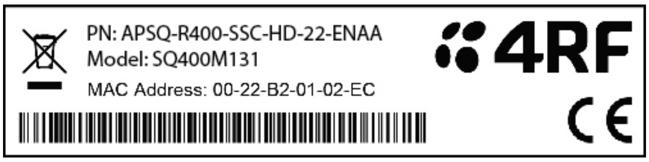
This parameter is only applicable when the radio is part of a Protected Station.

This RF Interface MAC address is used to define the MAC address of the Protection Switch. This address is entered in the factory. Both Protected Station radios read and use this MAC address.

This MAC address entry will only be used by the software if it detects that the factory MAC address set in the internal EPROM of the protected switch is corrupted for some reason, otherwise the software will ignore the MAC address entered by the user.

The RF interface MAC address is used for registration process only. For example, in a remote Protected Station, both radios share the same RF MAC address and a single entry of the remote Protected Station will be presented in network table (Network Status > Network Table).

The Protection Switch RF Interface MAC address is shown on the Protection Switch label:



PRIMARY / SECONDARY CONFIGURATION

See ‘Maintenance > Advanced’ on page 202 for parameter details.

PRIMARY / SECONDARY MAINTENANCE FILES

See ‘Maintenance > Advanced’ on page 202 for parameter details.

Events

The Events menu contains the setup and management of the alarms, alarm events and traps.

Protected Station: Events > Alarm Summary

There are two types of events that can be generated on the Aprisa SR+ radio. These are:

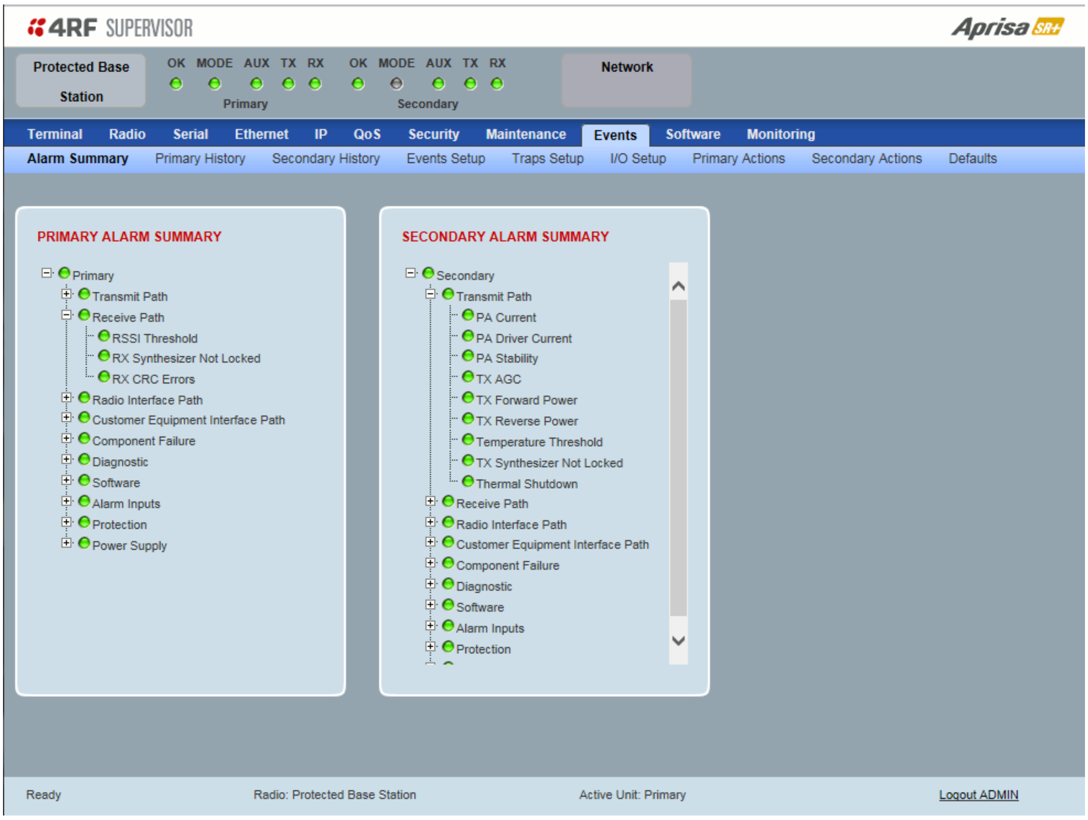
1. Alarm Events

Alarm Events are generated to indicate a problem on the radio.

2. Informational Events

Informational Events are generated to provide information on key activities that are occurring on the radio. These events do not indicate an alarm on the radio and are used to provide information only.

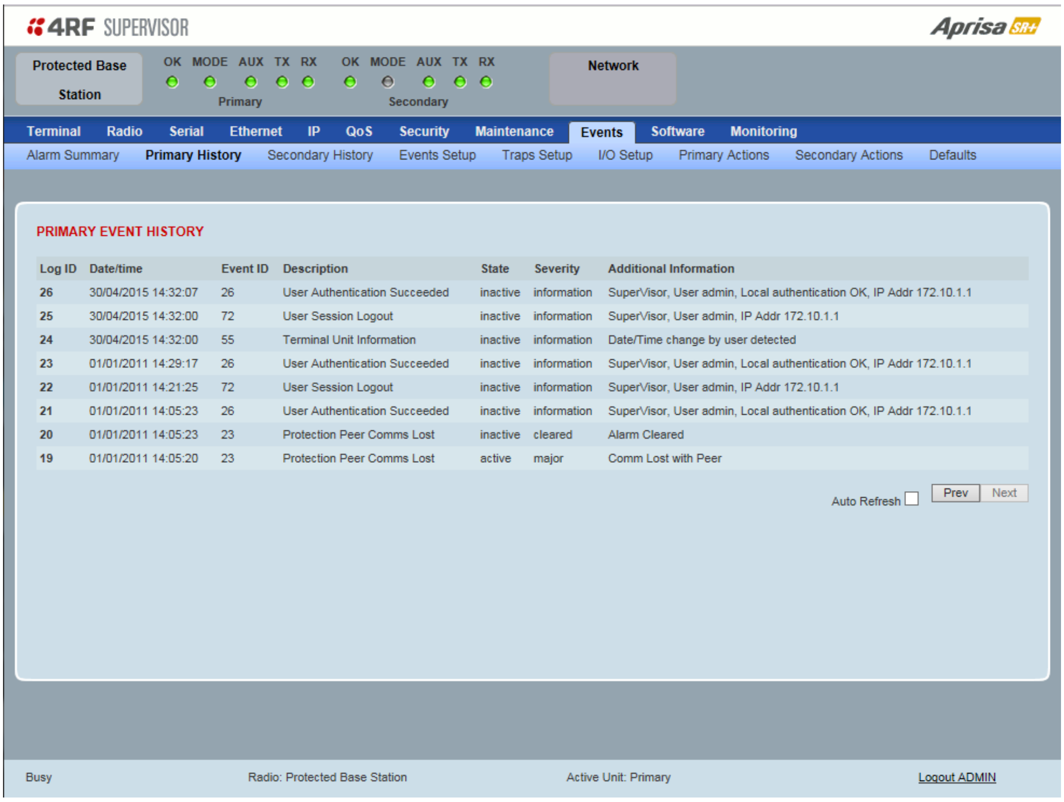
See 'Alarm Types and Sources' on page 350 for a complete list of events.



PRIMARY / SECONDARY ALARM SUMMARY

See 'Events > Alarm Summary' on page 206 for parameter details.

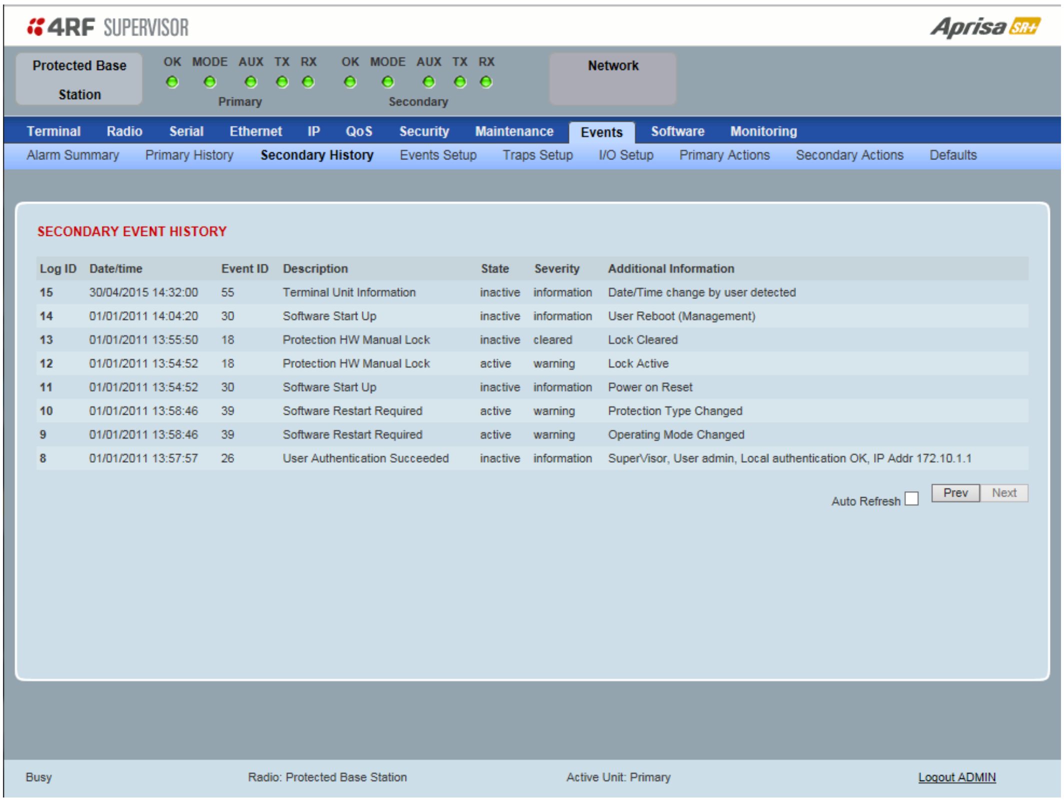
Protected Station: Events > Primary History



PRIMARY EVENT HISTORY

See 'Events > Event History' on page 207 for parameter details.

Protected Station: Events > Secondary History



SECONDARY EVENT HISTORY

See 'Events > Event History' on page 207 for parameter details.

Software

The Software menu contains the setup and management of the system software including network software distribution and activation on a protected station.

Single Radio Software Upgrade

The radio software can be upgraded on a single radio single Aprisa SR+ radio (see 'Single Radio Software Upgrade' on page 344). This process would only be used if the radio was a replacement or a new station in an existing network.

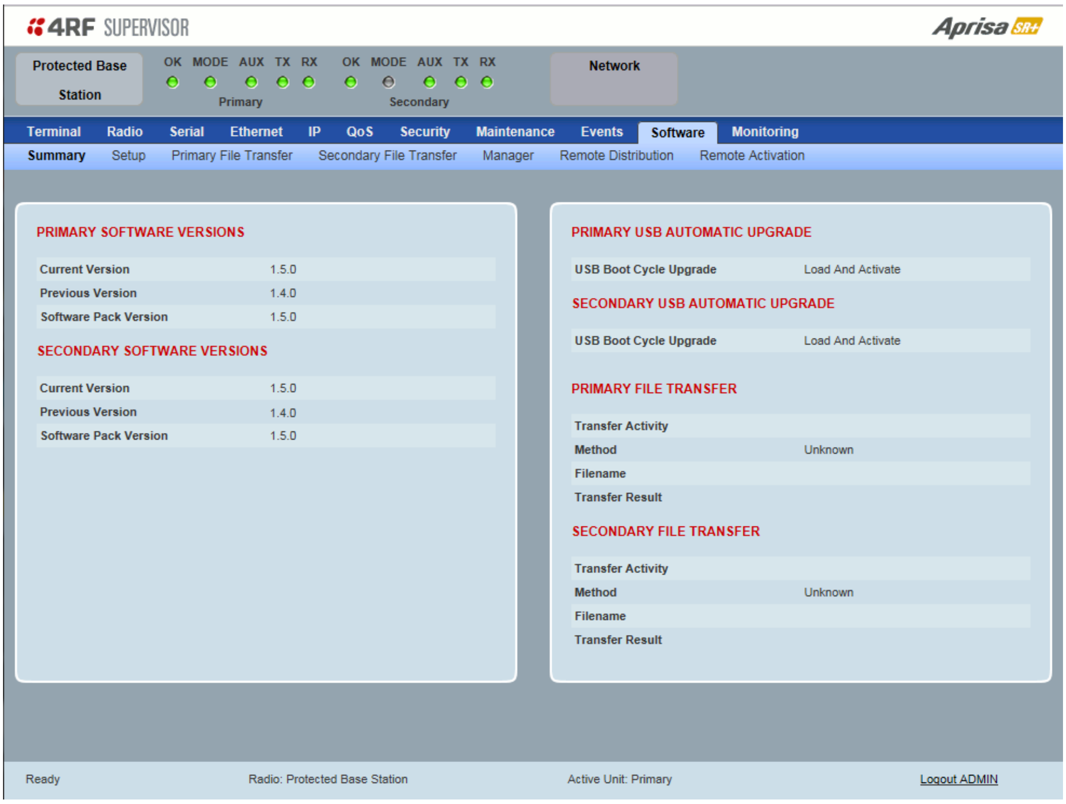
Network Software Upgrade

The radio software can be upgraded on an entire Aprisa SR+ radio network remotely over the radio link (see 'Network Software Upgrade' on page 340). This process involves the following steps:

1. Transfer the new software to base station primary radio with 'Protected Station: Software > Primary File Transfer'.
2. File Transfer the new software to base station secondary radio with 'Protected Station: Software > Secondary File Transfer'.
3. Using the Software Manual Lock, manually lock all protected remotes to the currently active radio (this is necessary to prevent automatic switching during the distribution and activation process).
4. Distribute the new software to all remote stations with 'Protected Station: Software > Remote Distribution'. Note: The software pack in the base station active radio is used for distribution.
5. Activate of the new software on remote stations with 'Protected Station: Software > Remote Activation'.
6. Finally, activate the new software on the base station primary and secondary radios. Note: activating the software will reboot the radio which will reset the Software Manual Lock to Automatic.

Protected Station: Software > Summary

This page provides a summary of the software versions installed on the radio, the setup options and the status of the File Transfers.

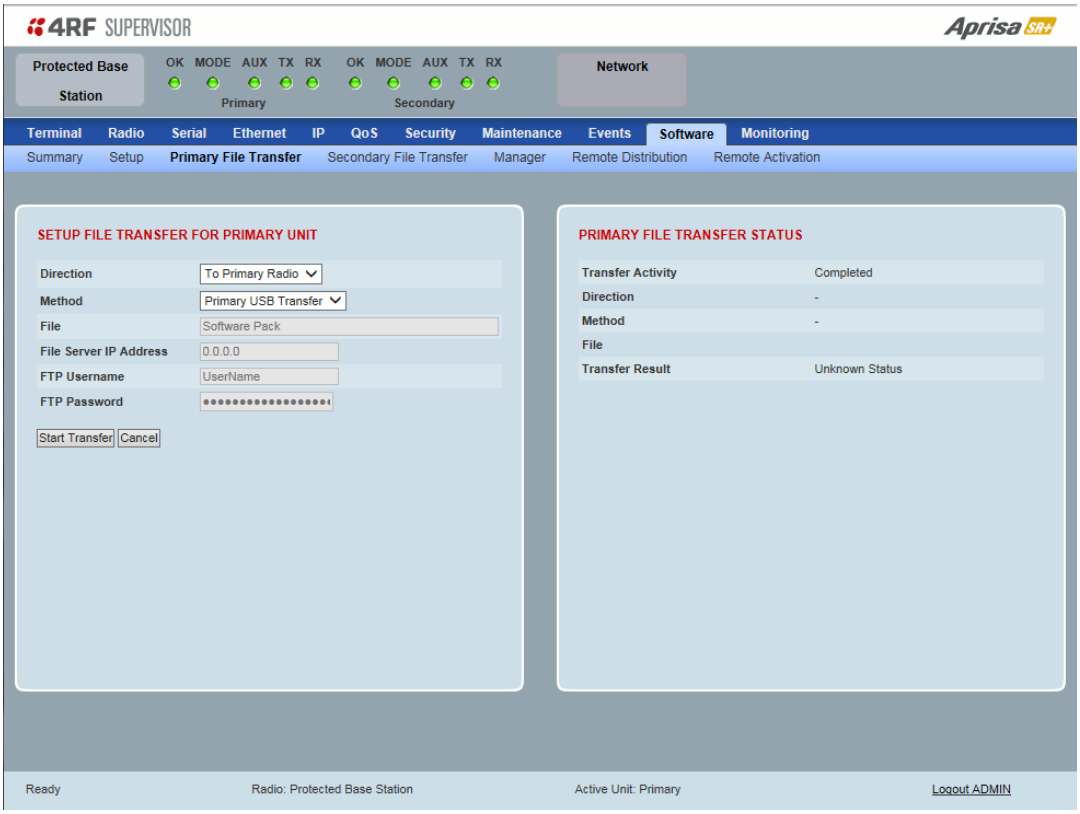


PRIMARY / SECONDARY SOFTWARE VERSIONS

See 'Protected Station: Software > Primary File Transfer' and 'Protected Station: Software > Secondary File Transfer' for parameter details.

Protected Station: Software > Primary File Transfer

This page provides the mechanism to transfer new software from a file source into the primary radio.



SETUP FILE TRANSFER FOR PRIMARY UNIT

Direction

This parameter sets the direction of file transfer. In this software version, the only choice is 'To Primary Radio'.

Method

This parameter sets the method of file transfer.

Option	Function
Primary USB Transfer	Transfers the software from the USB flash drive to the primary radio.
FTP	Transfers the software from an FTP server to the primary radio.

PRIMARY FILE TRANSFER STATUS

See 'Software > File Transfer' on page 222 for parameter details.

To transfer software into the Aprisa SR+ primary radio:

Primary USB Transfer Method

1. Unzip the software release files in to the root directory of a USB flash drive.
2. Insert the USB flash drive into the primary radio host port .
3. Click on ‘Start Transfer’.

FILE TRANSFER STATUS

Transfer Activity	In Progress
Direction	To This Radio
Method	USB Transfer
File	Software Pack
Transfer Result	In Progress (30%)

4. When the transfer is completed, remove the USB flash drive from the primary radio host port. If the SuperVisor ‘USB Boot Upgrade’ setting is set to ‘Disabled’ (see ‘USB Boot Upgrade’ on page 221), the USB flash drive doesn’t need to be removed as the radio won’t try to load from it.
5. Go to ‘Protected Station: Software > Manager’ on page 296 to activate the Software Pack. The radio will reboot automatically.

FTP Method

1. Unzip the software release files in to a temporary directory.
2. Open the FTP server and point it to the temporary directory.
3. Enter the FTP server IP address, Username and password into SuperVisor.
4. Click on ‘Start Transfer’.

FILE TRANSFER STATUS

Transfer Activity	In Progress
Direction	To This Radio
Method	FTP (172.17.10.11)
File	Software Pack
Transfer Result	In Progress (1%)

5. Go to ‘Protected Station: Software > Manager’ on page 296 to activate the Software Pack. The radio will reboot automatically.

Transfer from Secondary Unit

1. Select Transfer from Secondary Unit.
2. Click on ‘Start Transfer’.

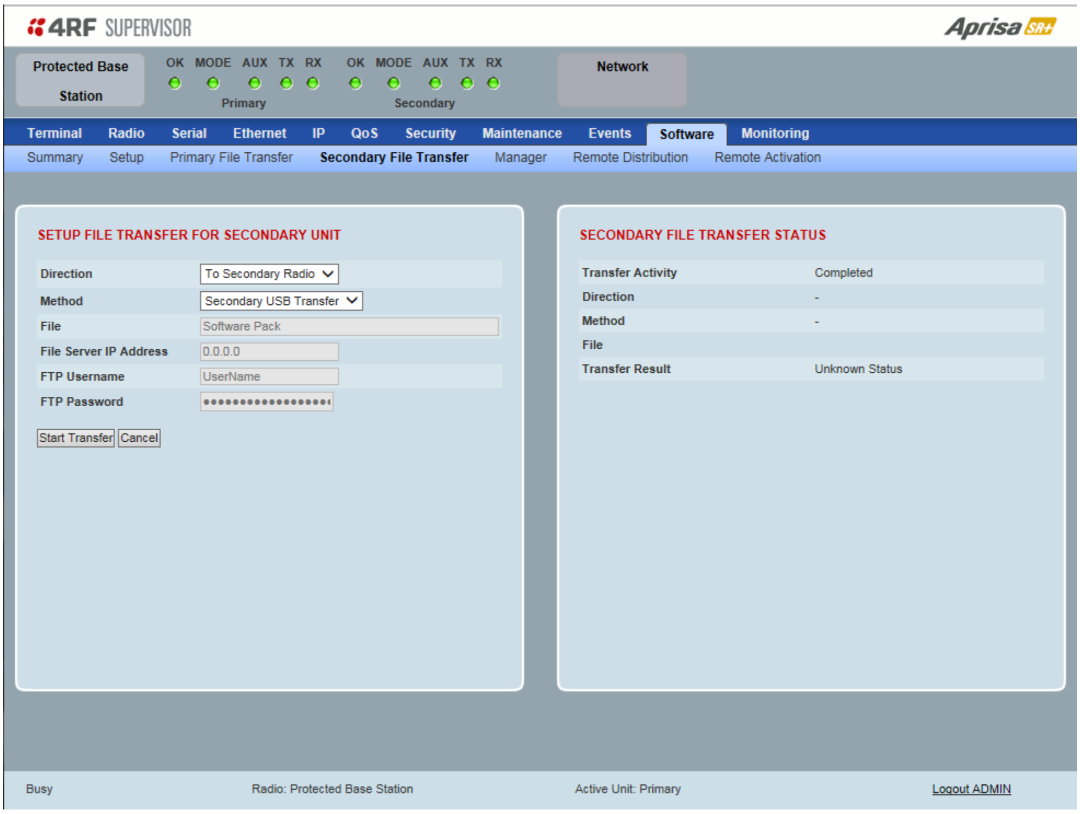
SECONDARY FILE TRANSFER STATUS	
Transfer Activity	In Progress
Direction	To This Radio
Method	Protected Partner Transfer
File	Software Pack
Transfer Result	Starting Transfer

3. Go to ‘Protected Station: Software > Manager’ on page 296 to activate the Software Pack. The radio will reboot automatically.

If the file transfer fails, check the Event History page (see ‘Protected Station: Events > Secondary History’ on page 287) for more details of the transfer.

Protected Station: Software > Secondary File Transfer

This page provides the mechanism to transfer new software from a file source into the secondary radio.



SETUP FILE TRANSFER FOR SECONDARY UNIT

Direction

This parameter sets the direction of file transfer. In this software version, the only choice is ‘To Secondary Radio’.

Method

This parameter sets the method of file transfer.

Option	Function
Secondary USB Transfer	Transfers the software from the USB flash drive to the secondary radio.
FTP	Transfers the software from an FTP server to the secondary radio.

SECONDARY FILE TRANSFER STATUS

See ‘Software > File Transfer’ on page 222 for parameter details.

To transfer software into the Aprisa SR+ secondary radio:

Secondary USB Transfer Method

1. Unzip the software release files in to the root directory of a USB flash drive.
2. Insert the USB flash drive into the secondary radio host port.
3. Click on ‘Start Transfer’.

FILE TRANSFER STATUS	
Transfer Activity	In Progress
Direction	To This Radio
Method	USB Transfer
File	Software Pack
Transfer Result	In Progress (30%)

4. When the transfer is completed, remove the USB flash drive from the secondary radio host port. If the SuperVisor ‘USB Boot Upgrade’ setting is set to ‘Disabled’ (see ‘USB Boot Upgrade’ on page 221), the USB flash drive doesn’t need to be removed as the radio won’t try to load from it.
5. Go to ‘Protected Station: Software > Manager’ on page 296 to activate the Software Pack. The radio will reboot automatically.

FTP Method

1. Unzip the software release files in to a temporary directory.
2. Open the FTP server and point it to the temporary directory.
3. Enter the FTP server IP address, Username and password into SuperVisor.
3. Click on ‘Start Transfer’.

FILE TRANSFER STATUS	
Transfer Activity	In Progress
Direction	To This Radio
Method	FTP (172.17.10.11)
File	Software Pack
Transfer Result	In Progress (1%)

4. Go to ‘Protected Station: Software > Manager’ on page 296 to activate the Software Pack. The radio will reboot automatically.

Transfer from Primary Unit

1. Select Transfer from Primary Unit.
2. Click on ‘Start Transfer’.

SECONDARY FILE TRANSFER STATUS

Transfer Activity	In Progress
Direction	To This Radio
Method	Protected Partner Transfer
File	Software Pack
Transfer Result	Starting Transfer

3. Go to ‘Protected Station: Software > Manager’ on page 296 to activate the Software Pack. The radio will reboot automatically.

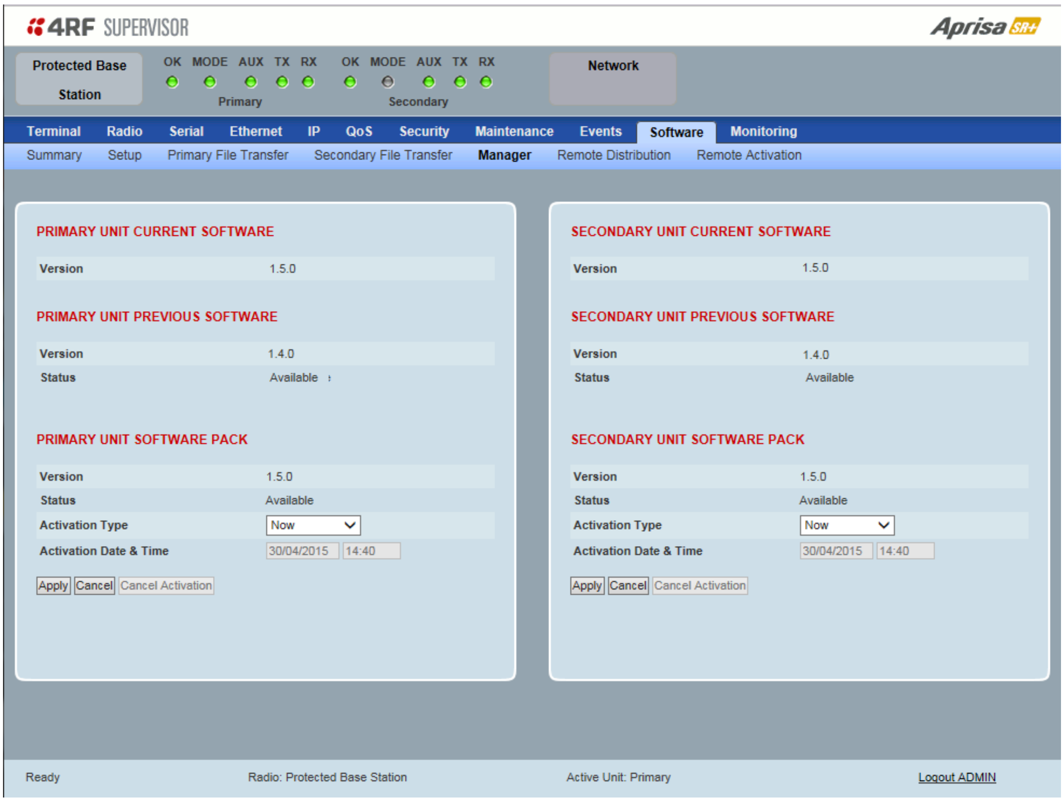
If the file transfer fails, check the Event History page (see ‘Protected Station: Events > Primary History’ on page 286) for more details of the transfer.

Protected Station: Software > Manager

This page summaries and manages the software versions available in the primary and secondary radios.

The manager is predominantly used to activate new software on single radios. Network activation is performed with ‘Protected Station: Software > Remote Activation’.

Both the previous software (if available) and Software Pack versions can be activated on each radio from this page.



PRIMARY / SECONDARY CURRENT SOFTWARE

Version

This parameter displays the software version running on the radio.

PRIMARY / SECONDARY PREVIOUS SOFTWARE

Version

This parameter displays the software version that was running on the radio prior to the current software being activated.

Status

This parameter displays the status of the software version running on the radio.

Option	Function
Active	The software is operating the radio.
Inactive	The software is not operating the radio but could be re-activated if required.

PRIMARY / SECONDARY SOFTWARE PACK

Version

This parameter displays the software pack version available for distribution on base station and activate on all stations.

Status

This parameter displays the status of the software pack version.

Option	Function
Available	On the base station, the software pack is available for distribution. On all stations, the software pack is available for activation.
Activating	The software pack is activating in the radio.
Unavailable	There is no software pack loaded into the radio.

Activate

See ‘Software > Manager’ on page 225 for the activation options.

Protected Station: Software > Remote Distribution

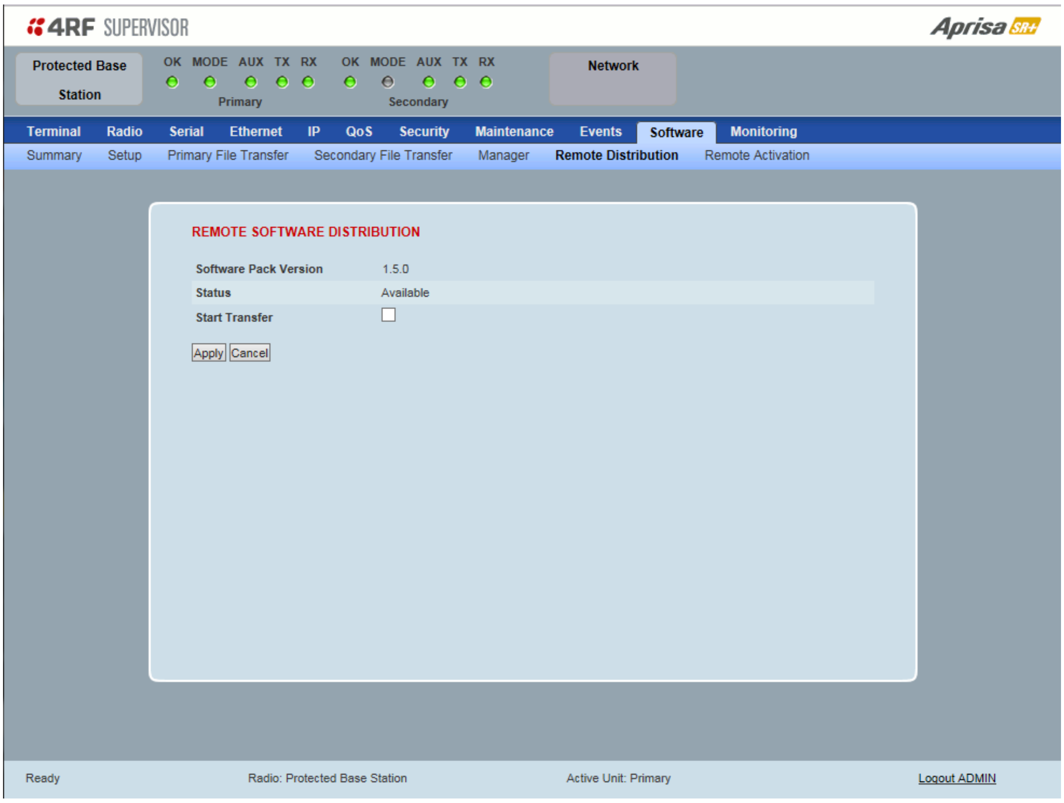
This page provides the mechanism to distribute software to all remote protected stations into the Aprisa SR+ network (network) and then activate it.

The Software Pack loaded into the base station with the file transfer process (see 'Protected Station: Software > Primary File Transfer' on page 290) is distributed via the radio link to all remote stations from the active radio.

The distribution process is monitored from this page.

When all remote stations receive the Software Pack version, the software can be remotely activated on all remote stations.

This page is only available when the radio is configured as a Base Station.



REMOTE SOFTWARE DISTRIBUTION

Software Pack Version

This parameter displays the software pack version available for distribution on base station and activate on all stations.

Status

This parameter displays the status of the software pack version.

If a Software Pack is not available, the status will display 'Unavailable' and the software distribution mechanism will not work.

Start Transfer

This parameter when activated distributes (broadcasts) the new Software Pack to all remote stations in the network.

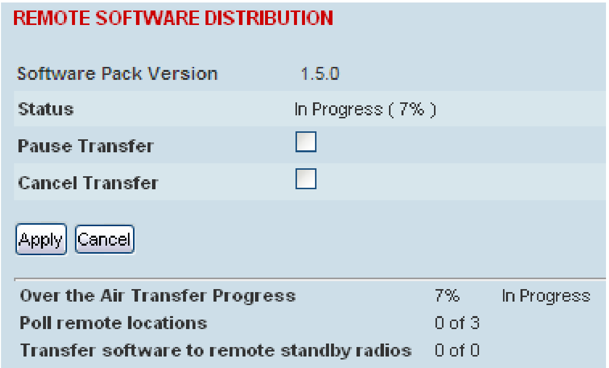
Note: The distribution of software to remote stations does not stop customer traffic from being transferred. However, due to the volume of traffic, the software distribution process may affect customer traffic.

Software distribution traffic is classified as 'management traffic' but does not use the Ethernet management priority setting. Software distribution traffic priority has a fixed priority setting of 'very low'.

To distribute software to remote stations:

This process assumes that a Software Pack has been loaded into the base station with the file transfer process (see 'Protected Station: Software > Primary File Transfer' on page 290).

1. To ensure that the Network Table is up to date, it is recommended running the node discover function (see 'Discover Nodes' on page 203).
2. Click on 'Start Transfer'.



Note: This process could take anywhere between 40 minutes and several hours depending on channel size, Ethernet Management Priority setting and the amount of customer traffic on the network.

Result	Function
Over the Air Transfer Progress	The percentage of the software pack that has been broadcast to the remote radios.
Poll Remote Locations	X is the number of radios polled to determine the number of standby radios. Y is the number of remote radios registered with the base station.
Transfer software to remote standby radios	X is the number of standby radios with the new software version. Y is the number of standby radios requiring the new software version.

3. When the distribution is completed, activate the software with the Remote Software Activation.

Pause Transfer

This parameter when activated, pauses the Over the Air Transfer Process and shows the distribution status. The distribution process will continue from where it was paused with Resume Transfer.

Cancel Transfer

This parameter when activated, cancels the Over the Air Transfer Process immediately.

During the distribution process, it is possible to navigate away from this page and come back to it to check progress. The SuperVisor session will not timeout.

Protected Station: Software > Remote Activation

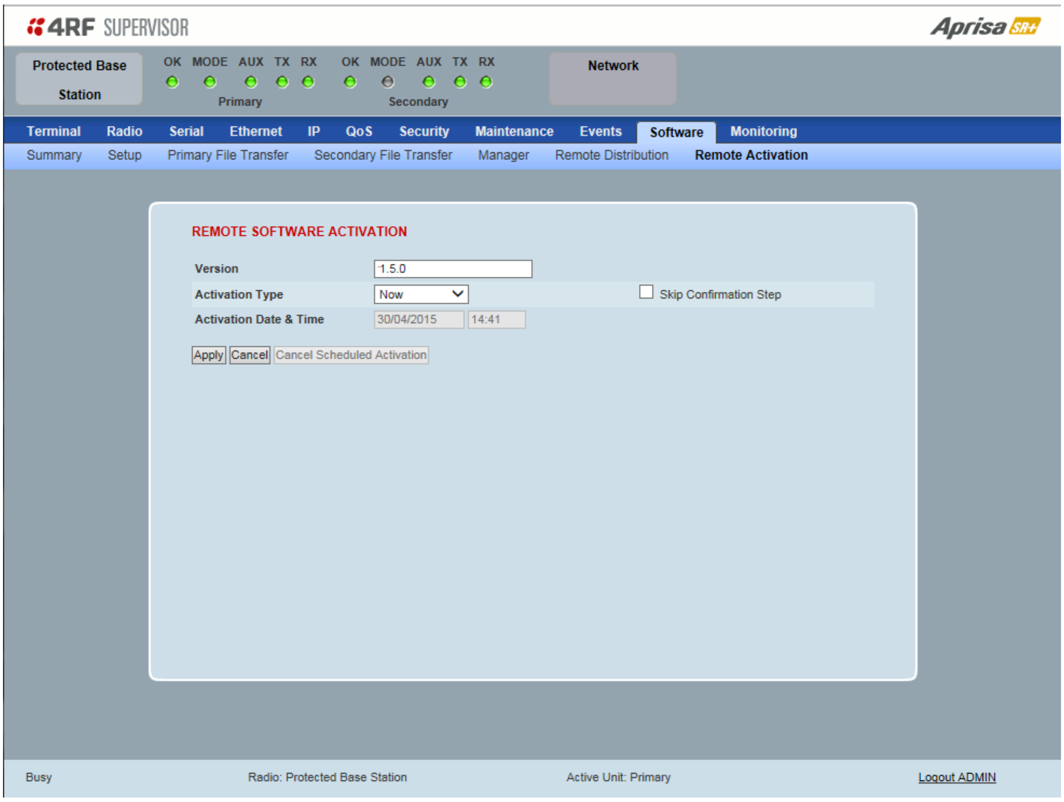
This page provides the mechanism to activate software on all remote protected stations.

The Software Pack has been loaded into the base station with the file transfer process (see 'Protected Station: Software > Primary File Transfer' on page 290) and distributed via the radio link to all remote stations from the active radio.

When all remote stations receive the Software Pack version, the software can be remotely activated on all remote stations.

The activation process is monitored by this page.

This page is only available when the radio is configured as a Base Station.



REMOTE SOFTWARE ACTIVATION

When the software pack version has been distributed to all the remote stations, the software is then activated in all the remote stations with this command. If successful, then activate the software pack in the base station to complete the network upgrade.

Version

This parameter displays the software version for activation. The default version is the software pack version but any valid software version can be entered in the format 'n.n.n'.

Activation Type

This parameter sets when the software pack activation will occur.

Option	Function
Now	Activates the software pack now.
Date & Time	Activates the software pack at the Date & Time set in the following parameter.

Activation Date & Time

This parameter sets the Date & Time when the software pack activation will occur.

This setting can be any future date and 24 hour time.

Skip Confirmation Step

This parameter when enabled skips the confirmation step during the activation process.

Normally, the confirmation step will require use intervention to accept the confirmation which will halt the activation process. Skipping the confirmation will enable the activation process to continue without use intervention.

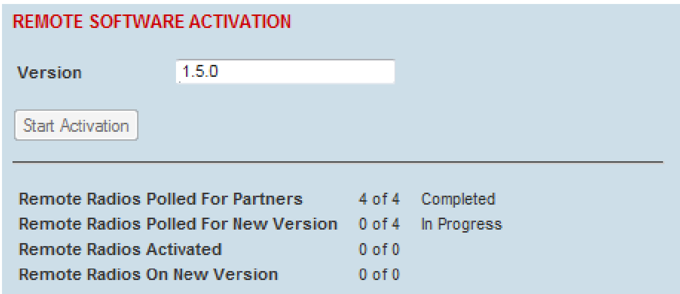
To activate software in remote stations:

This process assumes that a Software Pack has been loaded into the base station with the file transfer process (see 'Software > File Transfer' on page 222) and that distributed to all remote radios in the network.

Note: Do not navigate SuperVisor away from this page during the activation process (SuperVisor can lose PC focus).

---

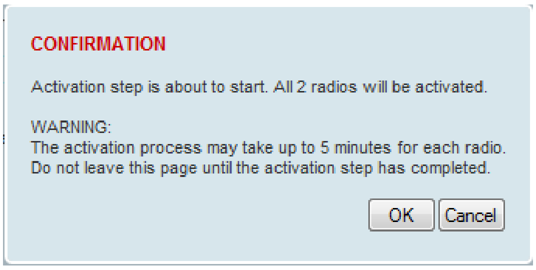
1. Enter the Software Pack version (if different from displayed version).
2. See 'Software > Manager' on page 225 for the activation options.



The remote stations will be polled to determine which radios require activation:

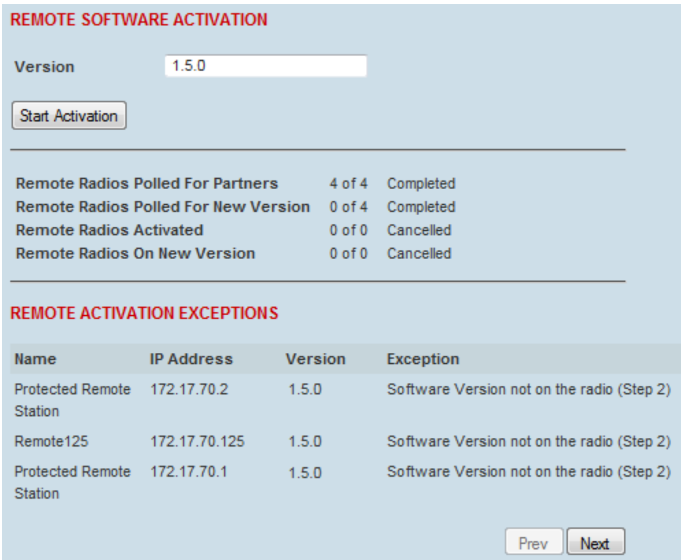
Result	Function (X of Y)
Remote Radios Polled for Partners	X is the number of radios polled to determine the number of protected stations in the network. Y is the number of remote radios registered with the base station.
Remote Radios Polled for New Version	X is the number of radios polled to determine the number of radios that contain the new software version. Y is the number of remote radios registered with the base station.
Remote Radios Activated	X is the number of radios that contain the new software version and have been activated. Y is the number of radios that contain the new software version and can be activated.
Remote Radios On New Version	X is the number of radios that has been successfully activated and now running the new version of software. Y is the number of radios that the activation command was executed on.

When the activation is ready to start:



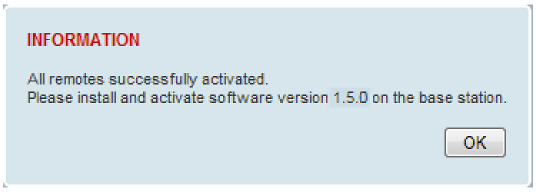
3. Click on ‘OK’ to start the activation process or Cancel to quit.

The page will display the progress of the activation.



The example shows that during the activation process there were exceptions that may need to be investigated.

When all the remote radios have been activated, the base station radio must now be activated with (see ‘Software > Manager’ on page 225).



4. Click on ‘OK’ to start the activation on the base station.

Command Line Interface

The Aprisa SR+ has a Command Line Interface (CLI) which provides basic product setup and configuration. This can be useful if you need to confirm the radio's IP address, for example.

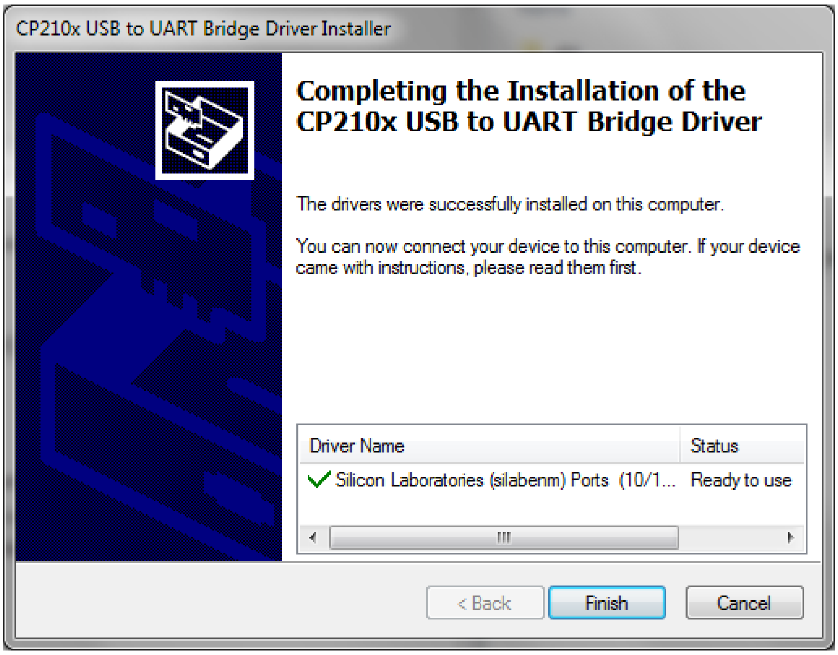
You can password-protect the Command Line Interface to prevent unauthorized users from modifying radio settings.

This interface can be accessed via an Ethernet Port (RJ45), the Management Port (USB micro type B) or the USB host port with a USB converter to RS-232 convertor.

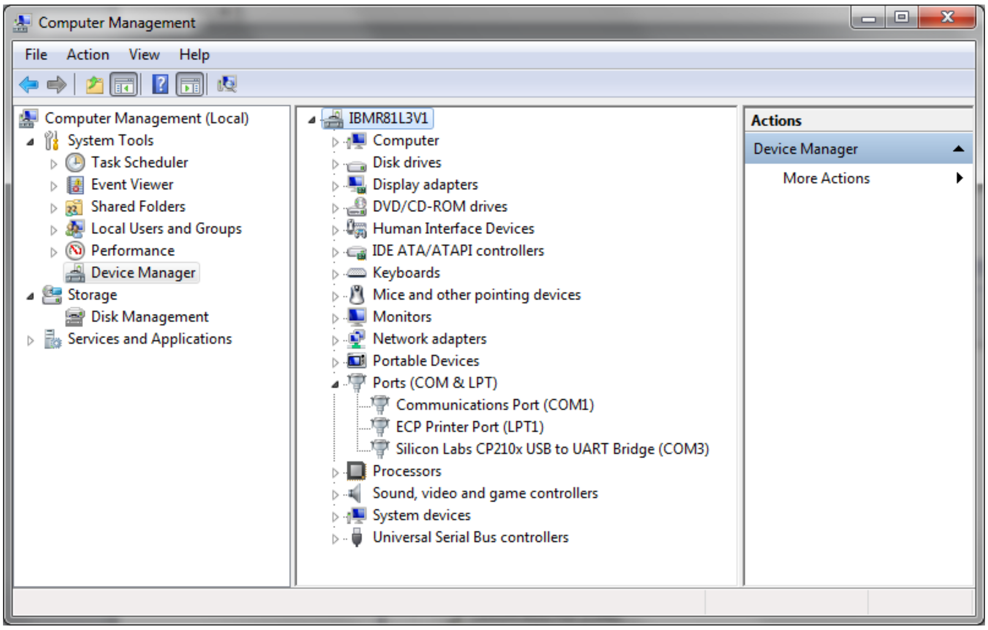
Connecting to the Management Port

A USB Cable USB A to USB micro B, 1m is provided with each radio.

1. Connect the USB A to your computer USB port and the USB micro B to the management port of the Aprisa SR+ (MGMT).
2. Unzip the file 'USB Serial Driver CP210x_VCP_Windows.zip' to a temporary location and install the appropriate driver on your computer. This file is on the Information and setup CD supplied with the radio.



3. Go to your computer device manager (Win 7: Control Panel > Administrative Tools > Computer Management > Device Manager)
4. Click on ‘Ports (COM & LPT)’
5. Make a note of the COM port which has been allocated to the ‘Silicon Labs CP210x USB to UART Bridge’ (COM3 in the example below)



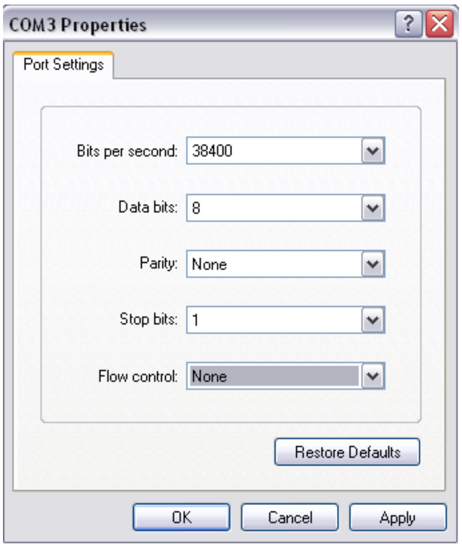
6. Open HyperTerminal or an alternative type of terminal Emulator program e.g. TeraTerm or Putty.

<u>HyperTerminal Example</u>

7. Enter a name for the connection (Aprisa SR+ CLI for example) and click OK.

8. Select the COM port from the Connect Using drop-down box that was allocated to the UART USB.

9. Set the COM port settings as follows:

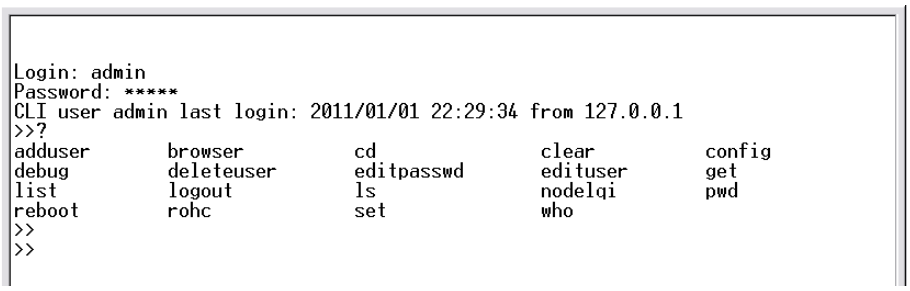


10. Click OK. The HyperTerminal window will open.

11. Press the Enter key to initiate the session.

12. Login to the Aprisa SR+ CLI with a default Username ‘admin’ and Password ‘admin’.

The Aprisa SR+ CLI menu is shown:



CLI Commands

To enter a CLI command:

1. Type the first few characters of the command and hit Tab. This auto completes the command.
2. Enter the command string and enter.

Note: All CLI commands are case sensitive.

The top level CLI command list is displayed by typing a ? at the command prompt.

The following is a list of the top level CLI commands and their usage:

CLI Command	Usage
adduser	adduser [-g <password aging>] [-a <account aging>] [-i <role>] <userName> <userPassword>
browser	browser <state(STR)>
cd	cd <changeMode(STR)>
clear	Clears the screen
config	config userdefault save restore factorydefault restore
debug	set subsystem param(INT) level param(INT) get clear subsystem param(INT) level param(INT) help log dump clear
deleteuser	deleteuser <userName>
editpasswd	editpasswd <oldpassword> <newpassword>
edituser	edituser [-p <password>] [-g <password aging>] [-a <account aging>] [-i]
get	get [-m <mib name>] [-n <module name>] <attribute name> [indexes]
list	list <tablename>
logout	Logs out from the CLI
ls	Displays the next level menu items
pwd	Displays the current working directory
reboot	Reboots the radio
rohc	stats show clear
set	set [-m <mib name>] [-n <module name>] <attribute name> <attribute set value> [indexes]
who	Shows the users currently logged into the radio

Viewing the CLI Terminal Summary

At the command prompt, type:

cd APRISASR-MIB-4RF

MPA APRISASR-MIB-4RF >>ls Terminal

```
>>cd APRISASR-MIB-4RF
MPA APRISASR-MIB-4RF >>ls Terminal
+------------------------------------------------------------+
|S.NO|ATTRIBUTE NAME                  |ATTRIBUTE VALUE       |
+------------------------------------------------------------+
|1   |termName                        |Base Station          |
|2   |termLocation                    |Wellington            |
|3   |termContactName                 |4RF Limited           |
|4   |termContactDetails              |support@4rf.com       |
|5   |termTimeFormat                  |time24h (1)           |
|6   |termDateFormat                  |ddmmyyyy (1)          |
|7   |termDateTime                    |2013-9-12,19:22:43.0|
|8   |termEthController1IpAddress     |173.10.10.1           |
|9   |termEthController1SubnetMask    |255.255.0.0           |
|10  |termEthController1Gateway       |0.0.0.0               |
|11  |termRfNwkPanId                  |CAFE                  |
|12  |termRfNwkRadius                 |1                     |
|13  |termInbandManagementEnabled     |true (1)              |
|14  |termInbandManagementTimeoutSec|10                      |
|15  |termRfNwkRepeaterProximity      |noRepeater (0)        |
+------------------------------------------------------------+
```

Changing the Radio IP Address with the CLI

At the command prompt, type 'set termEthController1IpAddress xxx.xxx.xxx.xxx'

```
+------------------------------------------------------------+
|1   |termName                        |Base Station          |
|2   |termLocation                    |Wellington            |
|3   |termContactName                 |4RF Limited           |
|4   |termContactDetails              |support@4rf.com       |
|5   |termTimeFormat                  |time24h (1)           |
|6   |termDateFormat                  |ddmmyyyy (1)          |
|7   |termDateTime                    |2013-9-12,19:25:19.0|
|8   |termEthController1IpAddress     |173.10.10.1           |
|9   |termEthController1SubnetMask    |255.255.0.0           |
|10  |termEthController1Gateway       |0.0.0.0               |
|11  |termRfNwkPanId                  |CAFE                  |
|12  |termRfNwkRadius                 |1                     |
|13  |termInbandManagementEnabled     |true (1)              |
|14  |termInbandManagementTimeoutSec|10                      |
|15  |termRfNwkRepeaterProximity      |noRepeater (0)        |
+------------------------------------------------------------+

MPA APRISASR-MIB-4RF >>set termEthController1IpAddress 173.10.10.1
termEthController1IpAddress     =       173.10.10.1

MPA APRISASR-MIB-4RF >>
```

Connected 0:06:07 | ANSIW | 38400 8-N-1 | SCROLL | CAPS | NUM | Capture | Print echo

8. In-Service Commissioning

Before You Start

When you have finished installing the hardware, RF and the traffic interface cabling, the system is ready to be commissioned. Commissioning the radio is a simple process and consists of:

1. Powering up the radios.
2. Configuring all radios in the network using SuperVisor.
3. Aligning the antennas.
4. Testing that the links are operating correctly.
5. Connecting up the client or user interfaces.

What You Will Need

- Appropriately qualified commissioning staff at both ends of each link.
- Safety equipment appropriate for the antenna location at both ends of each link.
- Communication equipment, that is, mobile phones or two-way radios.
- SuperVisor software running on an appropriate laptop, computer, or workstation at the base station radio.
- Tools to facilitate loosening and re-tightening the antenna pan and tilt adjusters.
- Predicted receiver input levels and fade margin figures from the radio link budget.

Antenna Alignment

A base station omni-directional collinear antenna has a vertical polarization. The remote station yagi antennas must also have vertical polarization.

Aligning the Antennas

Align the remote station yagi antennas by making small adjustments while monitoring the RSSI. The Aprisa SR+ has a Test Mode which presents a real time visual display of the RSSI on the front panel LEDs. This can be used to adjust the antenna for optimum signal strength (see 'Test Mode' on page 43).

Note: Low gain antennas need less adjustment in elevation as they are simply aimed at the horizon. They should always be panned horizontally to find the peak signal.

1. Press and hold the TEST button on the radio LED panel until all the LEDs flash green (about 3 - 5 seconds).

   Note: The time for the LEDs to display the RSSI result is variable, depending on the network traffic, and can be up to 5 seconds. Small antenna adjustments should be made and then wait for the display to refresh.

   The RSSI poll refresh rate can be set with the SuperVisor command 'Transmit Period' (see 'Maintenance > Test Mode' on page 195).

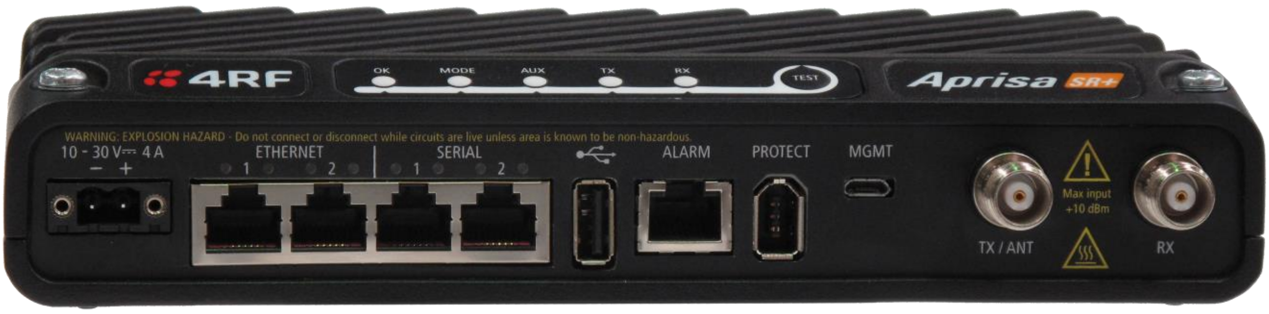
2. Move the antenna through a complete sweep horizontally (pan). Note down the RSSI reading for all the peaks in RSSI that you discover in the pan.
3. Move the antenna to the position corresponding to the maximum RSSI value obtained during the pan. Move the antenna horizontally slightly to each side of this maximum to find the two points where the RSSI drops slightly.
4. Move the antenna halfway between these two points and tighten the clamp.
5. If the antenna has an elevation adjustment, move the antenna through a complete sweep (tilt) vertically. Note down the RSSI reading for all the peaks in RSSI that you discover in the tilt.
6. Move the antenna to the position corresponding to the maximum RSSI value obtained during the tilt. Move the antenna slightly up and then down from the maximum to find the two points where the RSSI drops slightly.
7. Move the antenna halfway between these two points and tighten the clamp.
8. Recheck the pan (steps 2-4) and tighten all the clamps firmly.
9. To exit Test Mode, press and hold the TEST button until all the LEDs flash red (about 3 – 5 seconds).

9. Product Options

Data Interface Ports

The standard Aprisa SR+ provides multiple interface port options for combinations of Ethernet and RS-232 serial for a total of four interface ports i.e. port options of 2E2S, 3E1S or 4E0S, where E=Ethernet, S=Serial port.

The product shown below is the two Ethernet ports plus two RS-232 serial ports.



Interface Port Option	Part Number
4 Ethernet ports and no RS-232 serial ports	APSQ-N400-SSC-HD-40-ENAA
3 Ethernet ports and 1 RS-232 serial port	APSQ-N400-SSC-HD-31-ENAA
2 Ethernet ports and 2 RS-232 serial ports	APSQ-N400-SSC-HD-22-ENAA

Note: The optional serial interface is always available via the USB to serial converter.

Full Duplex Base Station

The Aprisa SR+ supports Full Duplex base / master station hardware. This option works with half duplex repeater / remote radios. The base / master station can transmit while simultaneously receiving from the repeater /remote radios.

Example of an 400 MHz full duplex Aprisa SR+.

Part Number	Part Description
APSQ-N400-SSC-FD-22-ENAA	4RF SR+, BR, 400-470 MHz, SSC, Full Duplex, 2E2S, EN, STD

Protected Station

The Aprisa SR+ Protected Station is fully monitored hot-standby and fully hot-swappable product providing radio and user interface protection for Aprisa SR+ radios. The RF ports and interface ports from the active radio are switched to the standby radio if there is a failure in the active radio.

Option Example

Part Number	Part Description
APSQ-R400-SSC-HD-22-ENAA	4RF SR+, PS, 400-470 MHz, SSC, Half Duplex, 2E2S, EN, STD

The Aprisa SR+ Protected Station is comprised of an Aprisa SR+ Protection Switch and two standard Aprisa SR+ radios mounted in a 2U rack mounting chassis.

All interfaces (RF, data, etc.) are continually monitored on both the active and standby radio to ensure correct operation. The standby radio can be replaced without impacting traffic flow on the active radio.

The Aprisa SR+ radios can be any of the currently available Aprisa SR+ radio frequency bands, channel sizes or interface port options.

The Aprisa SR+ Protected Station can operate as a base station, repeater station or remote station. The protection behaviour and switching criteria between the active and standby radios is identical for the three configurations.

By default, the Aprisa SR+ Protected Station is configured with the left hand radio (A) designated as the primary radio and the right hand radio (B) designated as the secondary radio.

Each radio is configured with its own unique IP and MAC address and the address of the partner radio.

On power-up, the primary radio will assume the active role and the secondary radio will assume the standby role. If, for some reason, only one radio is powered on it will automatically assume the active role.

Protected Ports

The protected ports are located on the protected station front panel. Switching occurs between the active radio ports and the standby radio ports based on the switching criteria described below.

The protected ports include:

- Antenna ports ANT/TX and RX (if dual antenna ports used)
- Ethernet ports (depending on interface port option purchased)
- Serial ports (depending on interface port option purchased)

Operation

In hot-standby normal operation, the active radio carries all RS-232 serial and Ethernet traffic over the radio link and the standby radio transmit is on with its transmitter connected to an internal load. Both radios are continually monitored for correct operation including the transmitter and receiver and alarms are raised if an event occurs.

The active radio sends regular 'keep alive' messages to the standby radio to indicate it is operating correctly. In the event of a failure on the active radio, the RF link and user interface traffic is automatically switched to the standby radio.

The failed radio can then be replaced in the field without interrupting user traffic.

Switch Over

The switch-over to the standby radio can be initiated automatically, on fault detection, or manually via the Hardware Manual Lock switch on the Protection Switch or the Software Manual Lock from SuperVisor.

Additionally, it is possible to switch-over the radios remotely without visiting the station site, via the remote control connector on the front of the Protection Switch.

On detection of an alarm fault the switch-over time is less than 0.5 seconds. Some alarms may take up to 30 seconds to be detected depending on the configuration options selected.

The Protection Switch has a switch guard mechanism to prevent protection switch oscillation. If a switch-over has occurred, subsequent switch-over triggers will be blocked if the guard time has not elapsed.

The guard time starts at 20 seconds and doubles each switch-over to a maximum of 320 seconds and halves after a period of two times the last guard time with no protection switch-overs.

Switching Criteria

The Protected Station will switch-over operation from the active to the standby radio if any of the configurable alarm events occur, or if there is a loss of the 'keep alive' signal from the active radio.

It is possible to configure the alarm events which will trigger the switch-over. It is also possible to prevent an alarm event triggering a switch-over through the configuration of blocking criteria.

Any of the following alarm events can be set to trigger or prevent switching from the active radio to the standby radio (see 'Events > Events Setup' on page 208).

PA current	
Tx reverse power	Tx AGC
Temperature threshold	Thermal shutdown
RSSI Threshold	RX Synthesizer Not Locked
Rx CRC errors	RF no receive data
Port 1 Eth no receive data	Port 2 Eth no receive data
Port 1 Eth data receive errors	Port 2 Eth data receive errors
Port 1 Eth data transmit errors	Port 2 Eth data transmit errors
Port 3 Eth no receive data	Port 4 Eth no receive data
Port 3 Eth data receive errors	Port 4 Eth data receive errors
Port 3 Eth data transmit errors	Port 4 Eth data transmit errors
Port 1 Serial Data No RX Data	Port 2 Serial Data RX Data
Port 1 Serial Data RX Errors	Port 2 Serial Data RX Errors
USB Port Serial Data No RX Data	USB Port Serial Data RX Errors
Component failure	Calibration failure
Configuration not supported	Protection Hardware Failure
Alarm Input 1	Alarm Input 2

It will not attempt to switch-over to a standby radio which has power failure.

It will also not switch over to a standby radio with an active alarm event which has been configured as a 'blocking criteria'.

Switch-over will be initiated once either of these conditions is rectified, i.e. power is restored or the alarm is cleared.

Monitored Alarms

The following alarms are monitored by default on the active / standby radio. The monitored alarms are dependent on the Protection Type selected.

Protection Type	All Protection Types	Redundant	Monitored Hot Standby	
Alarm Type	Monitored on Active Radio	Monitored on Standby Radio	Monitored on Standby Radio TX	Monitored on Standby Radio RX
PA Current	☑		☑	
PA Driver Current	☑		☑	
PA Stability	☑		☑	
TX AGC	☑			
TX Forward Power	☑		☑	
TX Reverse Power	☑		☑	
Temperature Threshold	☑	☑	☑	☑
TX Synthesizer Not Locked	☑		☑	
Thermal Shutdown	☑			
RSSI Threshold	☑			☑
RX Synthesizer Not Locked	☑			☑
RX CRC Errors	☑			☑
RF No Receive Data	☑			☑
Port1 ETH No Receive Data	☑			
Port1 ETH Data Receive Errors	☑			
Port1 ETH Data Transmit Errors	☑			
Port2 ETH No Receive Data	☑			
Port2 ETH Data Receive Errors	☑			
Port2 ETH Data Transmit Errors	☑			
Port3 ETH No Receive Data	☑			
Port3 ETH Data Receive Errors	☑			
Port3 ETH Data Transmit Errors	☑			
Port4 ETH No Receive Data	☑			
Port4 ETH Data Receive Errors	☑			
Port4 ETH Data Transmit Errors	☑			
Port1 Serial Data No RX Data	☑			
Port1 Serial Data RX Errors	☑			
Port2 Serial Data No RX Data	☑			
Port2 Serial Data RX Errors	☑			
USB Port Serial Data No RX Data	☑			
USB Port Serial Data No RX Errors	☑			
Component Failure	☑	☑	☑	☑
Protection SW Manual Lock	☑			
Protection HW Manual Lock	☑			

Protection Type	All Protection Types	Redundant	Monitored Hot Standby	
Alarm Type	Monitored on Active Radio	Monitored on Standby Radio	Monitored on Standby Radio TX	Monitored on Standby Radio RX
Modem FEC Disable	☑			
Modem ACM Lock	☑			
Alarm Input 1	☑	☑	☑	☑
Alarm Input 2	☑	☑	☑	☑
Protection Peer Comms Lost	☑			
Protection Hardware Failure	☑			
VDC Power Supply	☑	☑	☑	☑
3.3 Volts Power Supply	☑	☑	☑	☑
5.0 Volts Power Supply	☑	☑	☑	☑
7.2 Volts Power Supply	☑			
15.0 Volts Power Supply	☑	☑	☑	☑

Configuration Management

The Primary and Secondary radios are managed with the embedded web-based management tool, SuperVisor, by using either the Primary or Secondary IP address. Configuration changes in one of the radios will automatically be reflected in the partner radio.

To ensure all remote stations are registered to the correct (active) base station, changes to the Network Table are automatically synchronized from the active radio to the standby radio. The Network Table is only visible on the active radio. This synchronization does not occur if the Hardware Manual Lock is active.

Hardware Manual Lock

The Hardware Manual Lock switch on the Protection Switch provides a manual override of the active / standby radio.

When this lock is activated, the selected radio (A or B) becomes the active radio regardless of the Software Manual Lock and the current switching or block criteria.

When the lock is deactivated (set to the Auto position), the protection will become automatic and switching will be governed by normal switching and blocking criteria.

The state of the switch is indicated by the three LEDs on the Protection Switch:

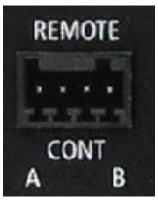
A LED	B LED	Locked LED	State
Green	Off	Off	Auto - Radio A is active
Off	Green	Off	Auto - Radio B is active
Green	Off	Orange	Manual Lock to radio A
Off	Green	Orange	Manual Lock to radio B

The Protection Switch also has a Software Manual Lock. The Hardware Manual Lock takes precedence over Software Manual Lock if both diagnostic functions are activated i.e. if the Software Manual Lock is set to 'Primary' and the Hardware Manual Lock set to 'Secondary', the system will set the Secondary radio to Active.

When a Hardware Manual Lock is deactivated (set to the Auto position), the Software Manual Lock is re-evaluated and locks set appropriately.

Remote Control

The switch-over to the standby radio can be initiated via the Remote Control connector on the front of the Protection Switch. This control will only operate if the Hardware Manual Lock switch is set to the Auto position.



The inputs are logic inputs with 4700 Ω pullup to +3.3 VDC. They require a pull down to ground to activate the control. The ground potential is available on the connector (see 'Protection Switch Remote Control Connections' on page 349).

L2 / L3 Protection Operation

The Aprisa SR+ Protected Station has selectable L2 Bridge or L3 Router modes, with VLAN, QoS and L2/3/4 address filtering attributes. Each Radio is configured with its own unique IP and MAC address and partner radio address. On switch-over failure, the new active radio sends out a gratuitous ARP to update the MAC learning tables / ARP tables of upstream bridge/router for appropriate traffic flow.

Hot-Swappable

The two Aprisa SR+ radios are mounted on a pull-out tray to making it possible to replace a failed radio without interrupting user traffic.

Antenna and Duplexer Options

Option 1 - single antenna without a duplexer

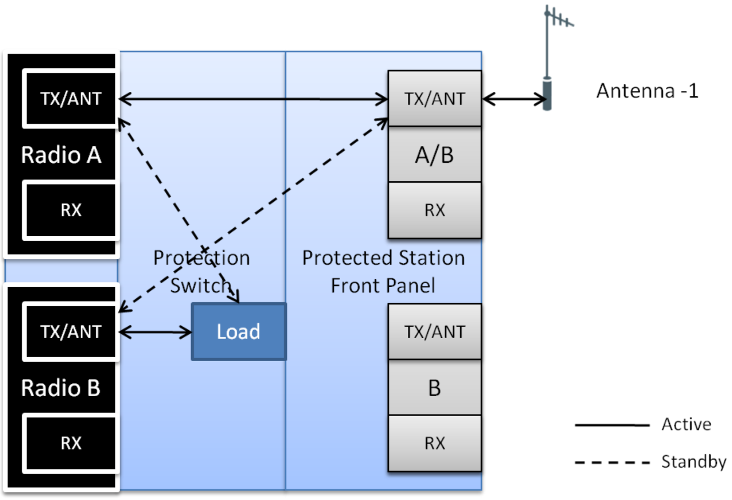
In this configuration, a single antenna is used and connected directly to the Aprisa SR+ Protected Station TX/ANT (A/B side) TNC port on the front panel. In this option Protected Station can operate in:

- Half duplex RF operation only

If single frequency used, standby radio TX is OFF/Mute (as RX/TX on same connector).

If dual frequency used, standby radio TX is ON, transmit to internal load for fault monitoring.

Only the active radio receives the signal (single RX path) from the antenna.



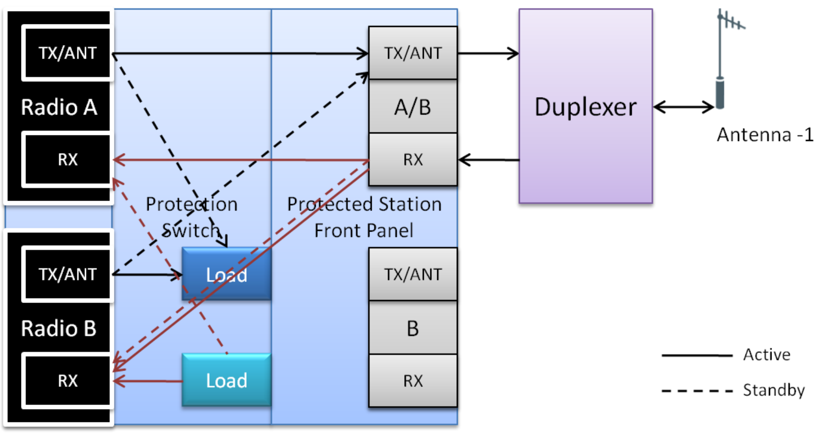
Option 2 - single antenna with a single duplexer

In this configuration, a single antenna is used with a duplexer which is connected to the Aprisa SR+ Protected Station TX/ANT and RX (A/B side) TNC ports on the front panel. In this option, the Protected Station can operate in:

- Half or full duplex RF operation
- Only dual frequency supported, where standby radio TX is ON, transmits to internal load for fault monitoring

When the 'Protection Type' is set to 'monitored hot standby' (Terminal > Operating Mode), the standby radio RX/TX can be fault monitored. This mode has a 4 dB loss in RX sensitivity.

When the 'Protection Type' is set to 'redundant', the standby radio RX/TX will not be fault monitored. This mode has 1 dB loss in RX sensitivity.



Option 3 - dual antenna without a duplexer

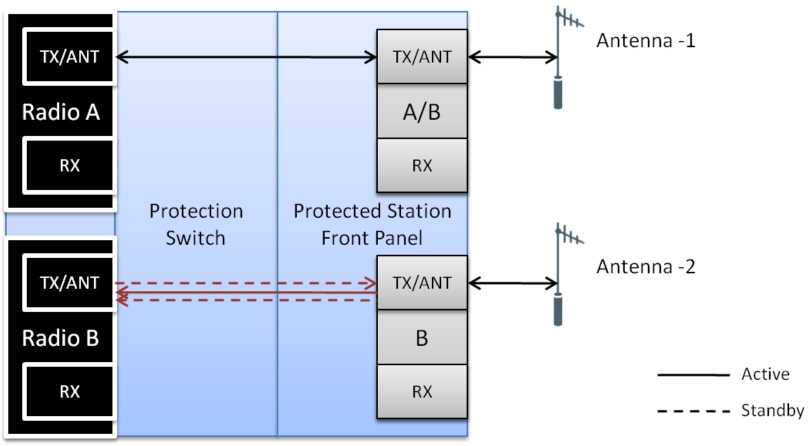
In this configuration, antenna redundancy is supported with dual antennas connected to the Aprisa SR+ Protected Station TX/ANT (A/B side) and TX/ANT (B side) TNC ports on the front panel. In this option, the Protected Station can operate in:

- Half duplex RF operation only

If single frequency used, standby radio RX (TX is off) can't be monitored as it will receive the active TX.

If dual frequency used, and the 'Protection Type' is set to 'monitored hot standby' (Terminal > Operating Mode), the standby radio RX/TX can be fault monitored. This mode has a 1 dB loss in RX sensitivity.

If dual frequency used, and the 'Protection Type' is set to 'redundant', the standby radio RX/TX will not be fault monitored.



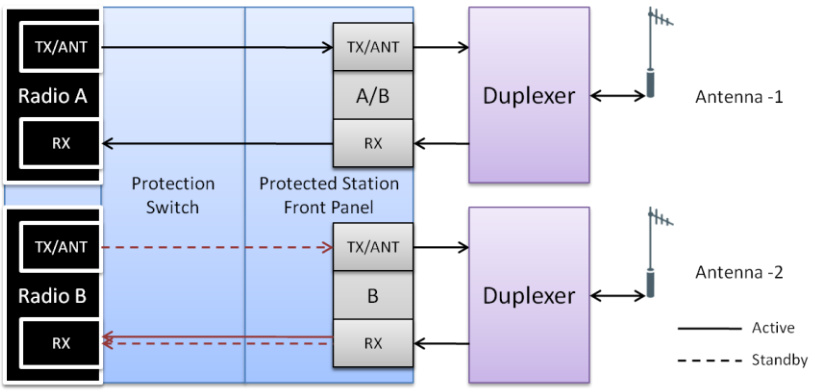
Option 4 - dual antenna with dual duplexers

In this configuration, antenna redundancy is supported with dual antennas connected via dual duplexers to the Aprisa SR+ Protected Station TX/ANT and RX (A/B side) TNC ports and TX/ANT and RX (B side) TNC ports on the front panel. In this option, the Protected Station can operate in:

- Half or full duplex RF operation
- Only dual frequency

When the 'Protection Type' is set to 'monitored hot standby' (Terminal > Operating Mode), the standby radio RX/TX can be fault monitored. This mode has a 1 dB loss in RX sensitivity.

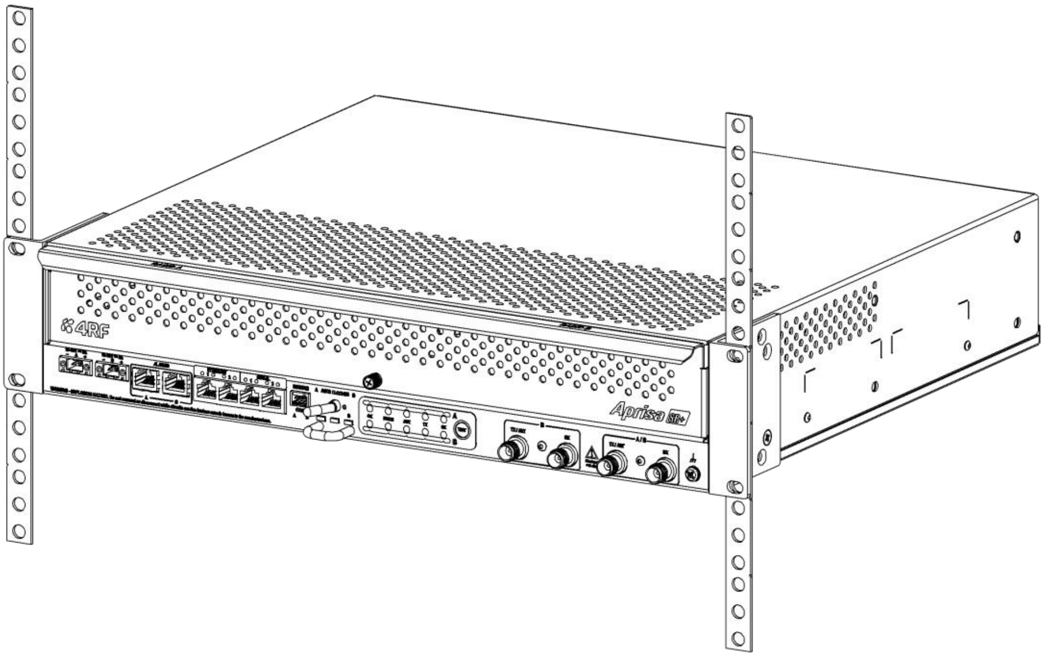
When the 'Protection Type' is set to 'redundant', the standby radio RX/TX will not be fault monitored.



Installation

Mounting

The Aprisa SR+ Protected Station is designed to mount in a standard 19 inch rack.



Cabling

The Aprisa SR+ Protected Station is delivered pre-cabled with power, interface, management and RF cables.

There are two options for the pre-cabled Protected Station (see 'Antenna and Duplexer Options'):

1. Standard Protected Station- suitable for options #1 and #2 (single antenna operation)

Part Number	Part Description
APSQ-R400-SSC-HD-22-ENAA	4RF SR+, PS, 400-470 MHz, SSC, Half Duplex, 2E2S, EN, STD

2. Dual Antenna Protected Station- suitable for options #3 and #4 (dual antenna operation)

Part Number	Part Description
APSQ-R400-SSC-HD-22-ENDA	4RF SR+, PS, 400-470 MHz, SSC, Half Duplex, 2E2S, EN, Dual Ant

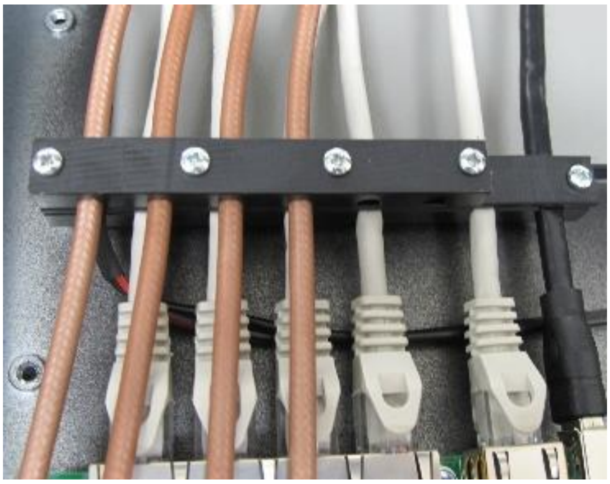
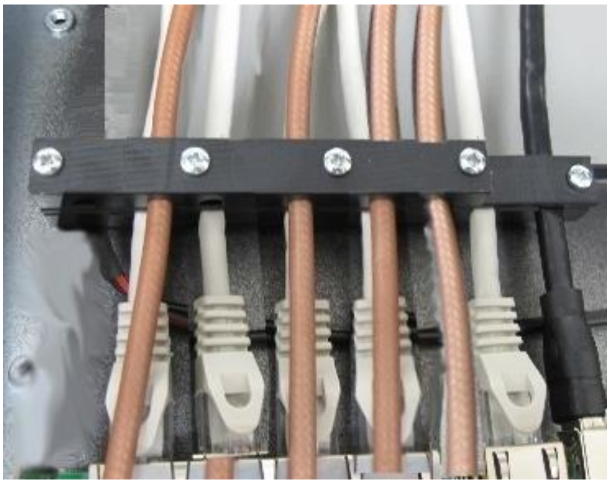
Each option (per ordered part number) is pre-cable configured as the following:

Protected Station Wiring	Internal pre-cabled Protected Station wiring setting	
	Radio / TNC Port	**RF Switch Port**
Standard Protected Station (single antenna operation)	Radio A TX/ANT	TX/ANTA
	Radio A RX	RXA
	Radio B TX/ANT	TX/ANTB
	Radio B RX	RXB
Dual Antenna Protected Station (dual antenna operation)	Radio A TX/ANT	TX/ANTA
	Radio A RX	RXA
	Radio B TX/ANT	TXB2
	Radio B RX	RXB2

Users can change an existing Protected Station from one option to the other option by following the procedure:

To change a pre-cabled Protected Station from one option to the other option:

1. Disconnect the power supply, antenna/s, interface cables and any other connections
2. Remove the Protected Station shelf from the rack
3. Turn the Protected Station shelf upside down
4. Remove the securing screws and remove the bottom panel
5. Unscrew the four coaxial cable clamp screws
6. Swap the two cables and position them in the appropriate connector ports
7. Refit the coaxial cable clamp and tighten the four clamp screws
8. Refit the bottom panel and tighten the two screws
9. Replace the shelf in the rack

Single Antenna Operation	Dual Antenna Operation
	
	

Power

The external power source must be connected to both the A and B Molex 2 pin male power connectors located on the protected station front panel. The A power input powers the A radio and the B power input powers the B radio.

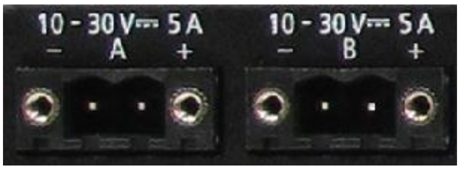
The protection switch is powered from the A power input or the B power input (whichever is available).

The maximum combined power consumption is 35 Watts.

The Aprisa SR+ Protected station has two DC power options, 12 VDC and 48 VDC.

12 VDC

The 13.8 VDC nominal external power source can operate over the voltage range of +10.5 to +30 V DC (negative earth).

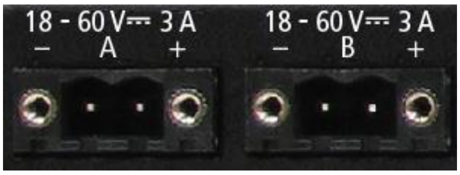


An example of the 12 VDC option part number is:

Part Number	Part Description
APSQ-R400-SSC-HD-22-ENAA	4RF SR+, PS, 400-470 MHz, SSC, Half Duplex, 2E2S, EN, STD

48 VDC

The 48 VDC nominal external power source can operate over the voltage range of 18 to 60 V DC (floating).

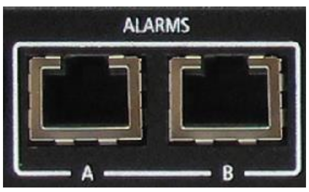


An example of the 48 VDC option part number is:

Part Number	Part Description
APSQ-R400-SSC-HD-22-ENAB	4RF SR+, PS, 400-470 MHz, SSC, Half Duplex, 2E2S, EN, 48VDC

Alarms

The protection switch provides access to both the A radio and B radio Alarm Interfaces (see 'Alarm Interface Connections' on page 348 for the connector pinout).



Maintenance

Changing the Protected Station IP Addresses

To change the IP address of a Protected Station radio:

1. Change the IP address of either or both the Primary Radio and Secondary radio (see ‘Protected Station: IP > IP Setup’ on page 272). Changes in these parameters are automatically changed in the partner radio.

Creating a Protected Station

When a Protected Station is ordered from 4RF, it will be delivered complete with radios installed, pre-cabled and pre-configured for Redundant operation. The following process will not be required.

This process is to create a protected station from two individual SR+ radios and a new spare Aprisa SR+ Protection Switch. It assumes that the SR+ radios are currently setup for non-protected operation.

1. Set the protection type and partner IP address of the SR+ radio A with SuperVisor 'Terminal > Operating Mode'. Set this radio Protection Unit to primary.
2. Set the protection type and partner IP address of the secondary SR+ radio B with SuperVisor Terminal > Operating Mode'. Set this radio Protection Unit to secondary.
3. Switch off the radios and place the two radios in the new spare Aprisa SR+ Protection Switch.
4. Ensuring that the cables are not crossed over, plug in the interface port cables, the Alarm and Protect port cables and the power connector to both the radios. Secure the power connectors with the two screws.
5. Power on the Protected Station.
6. Connect to either one of the radios via SuperVisor. This will start up SuperVisor in Single Session Management mode.
7. The user can now configure the Protected Station as required.

Replacing a Protected Station Faulty Radio

Replacing a faulty radio in a Protected Station can be achieved without disruption to traffic.

Assuming that the primary radio is active and the secondary radio is faulty and needs replacement:

1. Ensure the replacement radio has the same version of software installed as the primary radio. If necessary, upgrade the software in the replacement radio.
2. Set the RF Interface MAC Address (see ‘Protected Station: Maintenance > Advanced’ on page 283). This MAC address is present on chassis label.
3. Using SuperVisor > Maintenance > Advanced ‘Save Configuration to USB’ and ‘Restore Configuration from USB’ operation, clone the primary radio’s configuration to the replacement radio.
4. Configure the replacement radio as the secondary radio and setup the IP address and other protection parameters (see ‘Terminal > Operating Mode’ on page 91).
5. Set the Hardware Manual Lock switch to make the primary radio active.
6. Unplug the interface port cables, the Alarm and Protect port cables and the power connector from the faulty radio being replaced. The two screws securing the power connector will need to be undone.
7. Carefully remove the faulty radio from the protection switch.
8. Install the replacement radio into the protection switch.
9. Ensuring that the cables are not crossed over, plug in the interface port cables, the Alarm and Protect port cables and the power connector to the replacement radio. Secure the power connector with the two screws.
10. Power on the replacement radio and wait for it to become standby.
11. Set the Hardware Manual Lock switch to the Auto position.

Replacing a Faulty Power Supply

Replacing one of the power supplies can be achieved without disruption to traffic.

If a power supply has failed, the associated radio will have failed which will have caused the protection switch to switch-over to the other radio. It will not have switched back unless the power was restored and another problem occurred which caused a switch-over.

1. If the A power supply is faulty, ensure that the B radio is active (whether it be the primary or secondary radio).

   If the B power supply is faulty, ensure that the A radio is active (whether it be the primary or secondary radio).
2. Replace the faulty power supply.

Replacing a Faulty Protection Switch

Note: Replacing a faulty Protection Switch will disrupt traffic.

Move the radios, the interface cables and the power cables to the replacement Protection Switch.

On both Protected Station radios:

1. Power on the radio and wait for it to become ready.
2. Using SuperVisor > Maintenance > Advanced, enter the RF Interface MAC address shown on the Protection Switch label (see ‘Protected Station: Maintenance > Advanced’ on page 283).
3. Using SuperVisor > Maintenance > Advanced, Decommission the node (see ‘Decommission Node’ on page 203) and then Discover the Nodes (see ‘Discover Nodes’ on page 203).

Ensure that the Hardware Manual Lock switch is set to the Auto position.

The Aprisa SR+ Protected Station is now ready to operate.

Spares

The Aprisa SR+ Protection Switch is available as spare parts for the three radio interface port options:

Part Number	Part Description
APST-XPSW-X22	4RF SR+ Spare, Protection Switch, 2E2S
APST-XPSW-X31	4RF SR+ Spare, Protection Switch, 3E1S
APST-XPSW-X40	4RF SR+ Spare, Protection Switch, 4E0S

Data Driven Protected Station

The Aprisa SR+ Data Driven Protected Station provides radio and RS-232 serial port user interface protection for Aprisa SR+ radios.

Example Part:

Part Number	Part Description
APSQ-D400-SSC-HD-22-ENAA	4RF SR+, PD, 400-470 MHz, SSC, Half Dup, 2E2S, EN, STD

The Aprisa SR+ Data Driven Protected Station shown is comprised of two standard Aprisa SR+ setup as 'dual antenna port', 'half duplex' radios and two external duplexers mounted on 19" rack mounting shelves.

The Aprisa SR+ radios can be any of the currently available Aprisa SR+ radio frequency band options.

By default, the Aprisa SR+ Data Driven Protected Station is configured with the left hand radio (A) designated as the primary radio and the right hand radio (B) designated as the secondary radio.

Each radio is configured with its own unique IP and MAC address and the address of the partner radio.

On power-up, the primary radio will assume the active role and the secondary radio will assume the standby role. If, for some reason, only one radio is powered on it will automatically assume the active role.

Operation

The active radio is determined explicitly by which radio receives data on its RS-232 serial port input from the interface.

The active radio carries all RS-232 serial traffic over its radio link and the standby radio is unused with its transmitter turned off.

If data is received on the RS-232 serial port interface input of the standby radio, it will immediately become the active radio and the radio which was active will become the standby radio.

Over The Air Compatibility

If the Aprisa SR+ Data Driven Protected Station is to be used in a network of New Aprisa SR radios, the 'SR Compatible' option must be enabled (see 'SR Compatible' on page 92).

Switch Over

The active radio is determined explicitly by which radio receives data on its RS-232 serial port.

The switching and blocking criteria used for the standard Protected Station do not apply. This means that events and alarms on the unit are not used as switching criteria.

Configuration Management

The Primary and Secondary radios are managed with the embedded web-based management tool, SuperVisor (see 'Managing the Radio' on page 65) by using either the Primary or Secondary IP address. Configuration changes in one of the radios will automatically be reflected in the partner radio.

Changes to the Network Table are automatically synchronized from the active radio to the standby radio but the Network Table is only visible on the active radio.

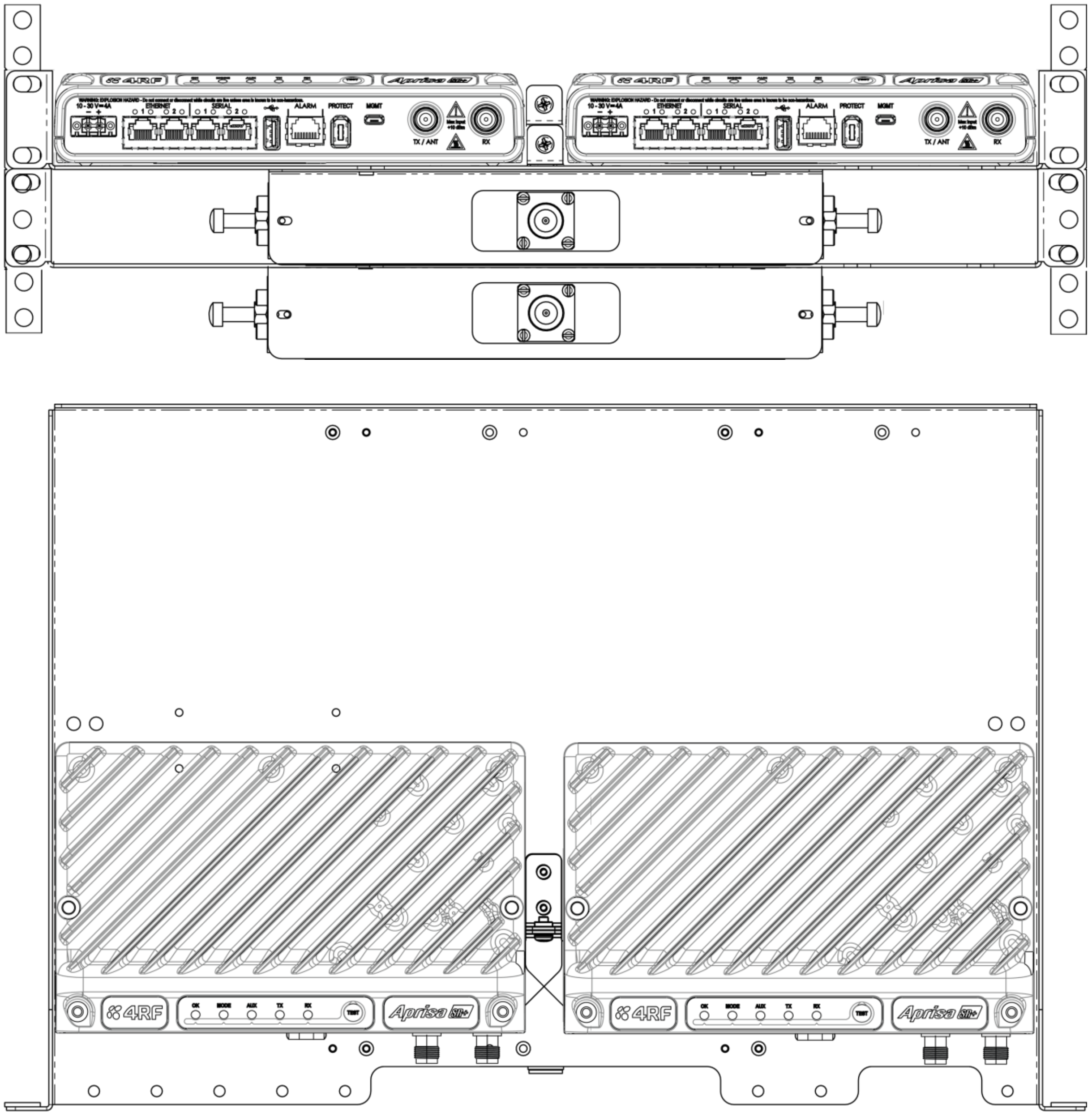
Power

A +10.5 to +30 V DC external power source must be connected to both the A and B Phoenix Contact 2 pin male power connectors. The maximum combined power consumption is 32.0 W for 1 W transmit power.

Installation

Mounting

The Aprisa SR+ Data Driven Protected Station is designed to mount in a standard 19” rack on two 1U rack mounting shelves (total of 3RU).



Cabling

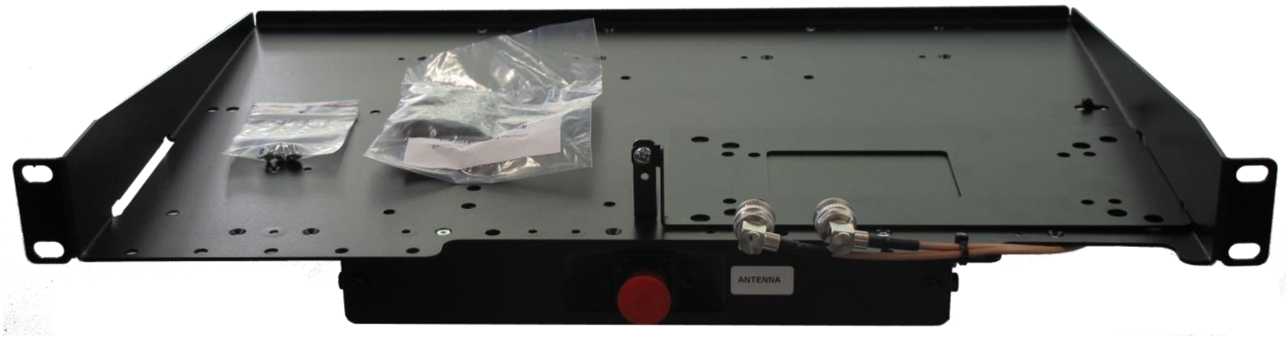
The Aprisa SR+ Data Driven Protected Station is delivered with the radios, duplexers, rack mounting shelves and interconnect cables. The set of interconnect cables is available as a spare part.

Part Number	Part Description
APST-XPSC-ST6	4RF SR+ Spare, Protection Switch Cables, Set Of 6

Duplexer Kits

The Aprisa SR+ product range contains Duplexer Kit accessories for use with Aprisa SR+ radios configured for Single Antenna Dual Port operation.

Radio Duplexer Kits



Example of part number: APSB-KDUP-400-B1-BR

Part Number	Description
APSB-KDUP-135-N0-BR	Aprisa SR+ Duplexer Kit for a SR+ Radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x N0 Duplexer 135 MHz, s4.6 MHz, p0.5 MHz 2x TNC to SMA right angle 640mm cables
APSB-KDUP-320-A1-BR	Aprisa SR+ Duplexer Kit for a Aprisa SR+ radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x A1 Duplexer 300 MHz, s 5 MHz, p 0.5 MHz 2x TNC to SMA right angle 640mm cables
APSB-KDUP-400-B1-BR	Aprisa SR+ Duplexer Kit for a SR+ Radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x B1 Duplexer 400 MHz, s 5 MHz, p 0.5 MHz 2x TNC to SMA right angle 640mm cables
APSB-KDUP-450-M0-BR	Aprisa SR+ Duplexer Kit for a SR+ radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x M0 Duplexer 450 MHz, s 5 MHz, p 0.5 MHz 2x TNC to SMA right angle 640mm cables
APSB-KDUP-450-P0-BR	Aprisa SR+ Duplexer Kit for a SR+ radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1 or 2 Aprisa SR+ radios and 1 duplexer 1x P0 Duplexer 450 MHz, s 3 MHz, p 0.5 MHz 2x TNC to SMA right angle 640mm cab

Part Number	Description
APSB-KDUP-928-G0-BR	Aprisa SR+ Duplexer Kit for a SR+ radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x G0 Duplexer 900 MHz, s 40 MHz, p 7 MHz 2x TNC to SMA right angle 640mm cables
APSB-KDUP-928-G2-BR-MM	Aprisa SR+ Duplexer Kit for a SR+ radio containing: 1x 1U 19" rack mid mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x G2 Duplexer 900 MHz, s 9 MHz, p 1 MHz 2x TNC to SMA right angle 640mm cables
APSB-KDUP-928-G2-BR	Aprisa SR+ Duplexer Kit for a SR+ radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x G2 Duplexer 900 MHz, s 9 MHz, p 1 MHz 2x TNC to SMA right angle 640mm cables
APSB-KDUP-928-G3-BR	Aprisa SR+ Duplexer Kit for a SR+ radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x G3 Duplexer 900 MHz, s5.5 MHz, p0.5 MHz 2x TNC to SMA right angle 640mm cables
APSB-KDUP-928-G3-BR-MM	Aprisa SR+ Duplexer Kit for a SR+ radio containing: 1x 1U 19" rack mid mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x G3 Duplexer 900 MHz, s5.5 MHz, p0.5 MHz 2x TNC to SMA right angle 640mm cables

Protected Station Duplexer Kits

Example of part number: APSB-KDUP-928-G2-PS

Part Number	Description
APSB-KDUP-135-N0-PS	Aprisa SR+ Duplexer Kit for a SR+ Protected Station containing: 1x N0 Duplexer 135 MHz, s4.6 MHz, p0.5 MHz 2x right angle TNC to SMA right angle 640mm cables Rack front mounted
APSB-KDUP-135-N0-PS-DA	Aprisa SR+ Duplexer Kit for a dual antenna SR+ Protected Station containing: 2x N0 Duplexer 135 MHz, s4.6 MHz, p0.5 MHz 4x right angle TNC to SMA right angle 640mm cables Rack front mounted
APSB-KDUP-320-A1-PS	Aprisa SR+ Duplexer Kit for a Aprisa SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x A1 Duplexer 300 MHz, s 5 MHz, p 0.5 MHz 2x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-320-A1-PS-DA	Aprisa SR+ Duplexer Kit for a dual antenna Aprisa SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 2x A1 Duplexer 300 MHz, s 5 MHz, p 0.5 MHz 4x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-400-B1-PS-DA	Aprisa SR+ Duplexer Kit for a dual antenna SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 2x B1 Duplexers 400 MHz, s 5 MHz, p 0.5 MHz 4x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-400-B1-PS	Aprisa SR+ Duplexer Kit for a SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x B1 Duplexer 400 MHz, s 5 MHz, p 0.5 MHz 2x right angle TNC to SMA right angle 640mm cables

Part Number	Description
APSB-KDUP-450-M0-PS	Aprisa SR+ Duplexer Kit for a SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x M0 Duplexer 450 MHz, s 5 MHz, p 0.5 MHz 2x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-450-M0-PS-DA	Aprisa SR+ Duplexer Kit for a dual antenna SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 2x M0 Duplexer 450 MHz, s 5 MHz, p 0.5 MHz 4x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-450-P0-PS	Aprisa SR+ Duplexer Kit for a SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x P0 Duplexer 450 MHz, s 3 MHz, p 0.5 MHz 2x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-450-P0-PS-DA	Aprisa SR+ Duplexer Kit for a dual antenna SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 2x P0 Duplexer 450 MHz, s 3 MHz, p 0.5 MHz 4x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-928-G0-PS	Aprisa SR+ Duplexer Kit for a SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x G0 Duplexer 900 MHz, s 40 MHz, p 7 MHz 2x TNC to SMA right angle 590mm cables
APSB-KDUP-928-G2-PS	Aprisa SR+ Duplexer Kit for a SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x G2 Duplexer 900 MHz, s 9 MHz, p 1 MHz 2x TNC to SMA right angle 590mm cables
APSB-KDUP-928-G2-PS-MM	Aprisa SR+ Duplexer Kit for a SR+ Protected Station containing: 1x 1U 19" rack mid mount shelf with duplexer mounting brackets and screws 1x G2 Duplexer 900 MHz, s 9 MHz, p 1 MHz 2x TNC to SMA right angle 590mm cables
APSB-KDUP-928-G3-PS-MM	Aprisa SR+ Duplexer Kit for a SR+ Protected Station containing: 1x 2U 19" rack mid mount shelf with duplexer mounting brackets and screws 1x G3 Duplexer 900 MHz, s5.5 MHz, p0.5 MHz 2x TNC to SMA right angle 640mm cables
APSB-KDUP-928-G3-PS	Aprisa SR+ Duplexer Kit for a SR+ Protected Station containing: 1x 2U 19" rack front mount shelf with duplexer mounting brackets and screws 1x G3 Duplexer 900 MHz, s5.5 MHz, p0.5 MHz 2x TNC to SMA right angle 640mm cables

USB RS-232 / RS-485 Serial Port

The Aprisa SR+ USB host port is predominantly used for software upgrade and diagnostic reporting. However, it can also be used to provide an additional RS-232 DCE or RS-485 serial port for customer traffic.

This is accomplished with a USB to RS-232 / RS-485 serial converter cable. This plugs into the USB host port connector and can be terminated with the required customer connector.

This additional RS-232 / RS-485serial port is enabled with the SuperVisor mode setting in Serial Port Settings (see ‘Serial > Port Setup’ on page 117).

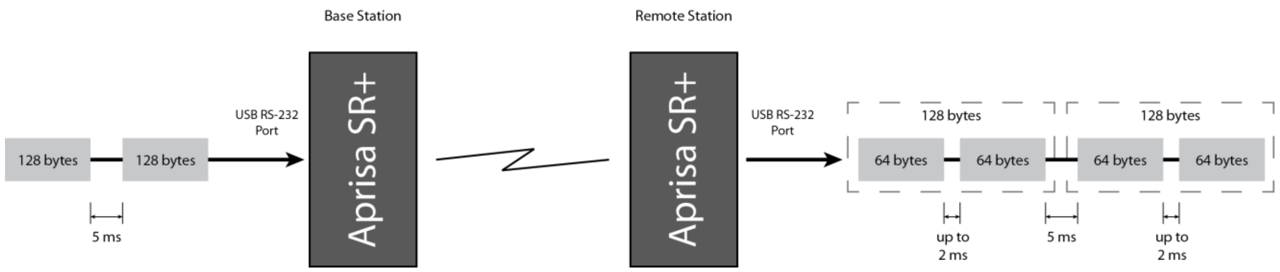
The Aprisa SR+ USB port has driver support for these USB serial converters. Other USB serial converters may not operate correctly.

USB RS-232 / RS-485 operation

The USB serial converter buffers the received data frames into 64 byte blocks separated by a small inter-frame gap.

For the majority of applications, this fragmentation of egress frames is not an issue. However, there are some applications that may be sensitive to the inter-frame gap, therefore, these applications need consideration.

A 5 ms inter-frame is recommended for the applications that are sensitive to inter-frame gap timings.



On a USB RS-232 port, Modbus RTU can operate up to 9600 bit/s with all packet sizes and up to 115200 bit/s if the packet size is less than 64 bytes. The standard RS-232 port is fully compatible with Modbus RTU at all baud rates.

USB RS-232 Cabling Options

The following converter cables are available as Aprisa SR+ accessories to provide the customer interface. The kit contains a USB connector retention clip (see 'USB Retention Clip' on page 338).

1. USB Converter to 1.8 metre multi-strand cable 6 wire for termination of customer connector

Part Number	Part Description
APSB-KFCA-USB-23-MS-18	4RF SR+ Acc, Kit, Interface, USB Conv, RS-232, Multi-strand, 1.8m

2. USB converter to RJ45 female kit for USB to RS-232 DCE conversion.

Part Number	Part Description
APSB-KFCA-USB-23-45-MF18	4RF SR+ Acc, Kit, Interface, USB Conv, RS-232, RJ45, Female, 1.8m

3. USB converter to DB9 female kit for USB to RS-232 DCE conversion.

Part Number	Part Description
APSB-KFCA-USB-23-D9-MF18	4RF SR+ Acc, Kit, Interface, USB Conv, RS-232, DB9, Female, 1.8m

USB RS-485 Cabling Options

The following converter cable is available as an Aprisa SR+ accessory to provide the customer interface RS-485 2 wire. The kit contains a USB connector retention clip (see 'USB Retention Clip' on page 338).

1. USB Converter to 1.8 metre multi-strand cable 6 wire for termination of customer interface

Part Number	Part Description
APSB-KFCA-USB-48-MS-18	4RF SR+ Acc, Kit, Interface, USB Conv, RS-485, Multi-strand, 1.8m

USB Retention Clip

The USB Retention Clip attaches to the underside of the Aprisa SR+ enclosure adjacent to the USB connector.

To attach the USB Retention Clip:

1. Clean the enclosure surface where the retention clip will attach with an alcohol based cleaner e.g. Isopropanol.
2. Peel off the retention clip protective backing.
3. Stick the clip onto the Aprisa SR+ enclosure ensuring that it aligns to the middle of the radio USB connector.

10. Maintenance

No User-Serviceable Components

There are no user-serviceable components within the radio.

All hardware maintenance must be completed by 4RF or an authorized service centre.

Do not attempt to carry out repairs to any boards or parts.

Return all faulty radios to 4RF or an authorized service centre.

For more information on maintenance and training, please contact 4RF Customer Services at support@4rf.com.

CAUTION: Electro Static Discharge (ESD) can damage or destroy the sensitive electrical components in the radio.

Software Upgrade

A software upgrade can be performed on a single Aprisa SR+ radio or an entire Aprisa SR+ network.

Network Software Upgrade

This process allows customers to upgrade their Aprisa SR+ network from the central base station location without need for visiting remote sites.

The Software Pack is loaded into the base station with the file transfer process (see 'Software > File Transfer' on page 222) and distributed via the radio link to all remote stations.

When all remote stations receive the Software Pack version, the software can be remotely activated on all remote stations.

Non-Protected Network Upgrade Process

This upgrade process is for upgrading the software on an entire Aprisa SR+ network from a non-protected base station. If there are protected remotes in the network, they must be locked to the current active radio.

To upgrade the entire Aprisa SR+ network software:

1. Using File Transfer, load the software pack into the base station (see 'Software > File Transfer' on page 222). The software can be transferred to the radio via an FTP transfer or from a USB flash drive.

   The Aprisa SR+ network file transfer operation is indicated in base station and remote stations by a flashing orange AUX LED.

2. Distribute the software to the entire network of remote radios (see 'Software > Remote Distribution' on page 229). Note that the distribution process over the air will take some time, depending on RF and Transfer rate settings.

   The Aprisa SR+ network software distribution operation is indicated in base station and remote stations by a flashing orange MODE LED.

   Note: The distribution of software to remote stations does not stop customer traffic from being transferred. However, due to the volume of traffic, the software distribution process may affect customer traffic.

   Software distribution traffic is classified as 'management traffic' but does not use the Ethernet management priority setting. Software distribution traffic priority has a fixed priority setting of 'very low'.

3. Activate the software on the entire network of remote radios (see 'Software > Remote Activation' on page 231).

   Note: When the new software activates on the remote radios, all link communication from the base station to the remote will be lost. The base station will attempt to re-establish connectivity to the remote radios for the new version verification but this will fail. However, when the new software activates on the remote radios, the remote radio will reboot automatically and link communication will restore when the base station software is activated.

   When the Remote Activation process gets to the 'Remote Radios On New Version' step, don't wait for this to complete but proceed to step 4.

4. Activate the software on the base station radio (see ‘Software > Manager’ on page 225).
5. When the new software has been activated, remote stations will re-register with the base station. The remote stations software version can verified with ‘Network Status > Network Table’ on page 254.
6. When the base station restarts with the new software, rediscover the nodes (see ‘Discover Nodes’ on page 203).
7. Check that all remote radios are now running on the new software (see ‘Network Status > Network Table’ on page 254).

Note: The following steps will only be necessary if for some reason steps 1-7 did not operate correctly or if software activation is attempted before the distribution process ends or the remote radio was off during steps 1-7 and turns on later. Thus, the following steps will most likely not be required.

8. If step 7 shows that not all remote radios are running the latest software version, restore the base / master station to the previous software version (see ‘Software > Manager’ on page 225).
9. Attempt to re-establish connectivity to the remote radios that have failed to upgrade by navigating to and remotely managing the remote radios individually.
10. Navigate to the remote radio history log and review the logs to determine the reason for the failure to activate the new software version.
11. Take appropriate actions to address the reported issue. If connectivity restores with the failed remotes, repeat steps 2-7 if required.

Protected Network Upgrade Process

This upgrade process is for upgrading the software on an entire Aprisa SR+ network from a protected base station. This software upgrade can be achieved without disruption to traffic.

Transferring the new software to the radios

The software can be transferred to the radio via an FTP transfer or from a USB flash drive.

1. Using the Hardware Manual Lock switch (see ‘Hardware Manual Lock’ on page 318), or the Software Manual Lock (see ‘Lock Active To’ on page 279), force the secondary radio to active
2. Using File Transfer, load the software pack into the secondary radio (see ‘Protected Station: Software > Secondary File Transfer’ on page 293).
3. Confirm that the transfer is successful (see ‘Protected Station: Software > Manager’ on page 296).
4. Using the Hardware Manual Lock switch (see ‘Hardware Manual Lock’ on page 318), or the Software Manual Lock (see ‘Lock Active To’ on page 279), force the primary radio to active.
5. Using File Transfer, load the software pack into the primary radio (see ‘Protected Station: Software > Primary File Transfer’ on page 290).
6. Confirm that the transfer is successful (see ‘Protected Station: Software > Manager’ on page 296).
7. Distribute the software to the entire network of remote radios (see ‘Protected Station: Software > Remote Distribution’ on page 298). If there are protected remotes in the network, they must be locked to the current active radio.

   Note that the distribution process over the air will take some time, depending on RF and Transfer rate settings.

Activating the new software on the radios

1. Activate the software on the entire network of remote radios (see ‘Protected Station: Software > Remote Activation’ on page 301).
2. Monitor the progress of the activation process until the stage where activation of all remote radios has been confirmed.

   When the new software has been activated, remote stations will re-register with the base station. The remote stations software version can verified with ‘Network Status > Network Table’ on page 254.
3. If the new software version is not over the air compatible with the version currently operating on the radio, there is no need to wait as all link communication from the base station to the remote will be lost so the verification of the new version on the remote radio will fail.
4. Activate the new version software pack of the secondary radio (see ‘Protected Station: Software > Manager’ on page 296).
5. Immediately after that, activate the new version software pack of the primary radio (see ‘Protected Station: Software > Manager’ on page 296).

   Note that the activation process will take a few minutes.

Confirm that the new software version is now running on the radios

1. Re-login into the Protection Station and navigate to SuperVisor > Software>Summary.
2. Confirm that the Primary and Secondary radio current software version is now up to date
3. Confirm that the list of remote radios are now running the latest software version with ‘Network Status > Network Table’ on page 254.
4. When the upgrade process is complete, if the Hardware Manual Lock switch has been used, set it to the Auto position. The software manual lock will release automatically.

Single Radio Software Upgrade

This upgrade process is for upgrading the software on a single Aprisa SR+ radio.

Note: If a radio has been configured for a Protection Type of 'Redundant', and that radio is no longer part of a Protected Station, the Protection Type must be changed to 'None' before the radio software upgrade can be achieved.

File Transfer Method

The Software Pack is loaded into the radio with the file transfer process (see 'Software > File Transfer' on page 222) and activated (see 'Software > Manager' on page 225).

The Aprisa SR+ upgrade operation is indicated by a flashing orange AUX LED.

To upgrade the Aprisa SR+ radio software:

1. Unzip the software release files in to the root directory of a USB flash drive.
3. Insert the USB flash drive into the host port .
4. Using File Transfer, load the software pack into the radio (see 'Software > File Transfer' on page 222).
5. Remove the USB flash drive from the host port ..
6. Activate the software on the radio (see 'Software > Manager' on page 225).

USB Boot Upgrade Method

A single Aprisa SR+ radio can also be upgraded simply by plugging a USB flash drive containing the new software into the USB A host port on the Aprisa SR+ front panel and power cycling the radio.

To upgrade the Aprisa SR+ radio software:

1. Unzip the software release files in to the root directory of a USB flash drive.
2. Check that the SuperVisor USB Boot Upgrade setting is set to 'Load and Activate' (see 'Software > Setup' on page 221).
3. Power off the Aprisa SR+ and insert the USB flash drive into the host port .
4. Power on the Aprisa SR+.
5. The software upgrade process is complete when the OK LED flashes green. This can take about 2 minutes.

   The software will have loaded in to the radio current software version.
6. Remove the USB flash drive from the host port .
7. Power cycle the Aprisa SR.

Login to the radio being upgraded and go to SuperVisor 'Software > Manager' on page 225.

The version of the uploaded software will be displayed in the Software Pack 'Version' field and the current software version.

If the upgrade process did not start, the Aprisa SR+ could already be operating on the version of software on the USB flash drive. This will be indicated by flashing OK LED and then the OK, MODE and AUX will light steady green.

If the radio is not operating on the new software (after the power cycle), it could be caused by the SuperVisor 'USB Boot Upgrade' setting set to 'Load Only' (see 'Software > Setup' on page 221).

In this case, go to SuperVisor see 'Software > Manager' on page 225 and tick the Software Pack 'Activate' checkbox and click 'Apply'.

If any Display Panel LED flashes red or is steady red during the upgrade process, it indicates that the upgrade has failed. This could be caused by incorrect files on the USB flash drive or a radio hardware failure.

Software Downgrade

Radio software can also be downgraded if required. This may be required if a new radio is purchased for an existing network which is operating on an earlier software release.

The downgrade process is the same as the upgrade process.

Protected Station Software Upgrade

This upgrade process is for upgrading the software on a single Aprisa SR+ Protected Station.

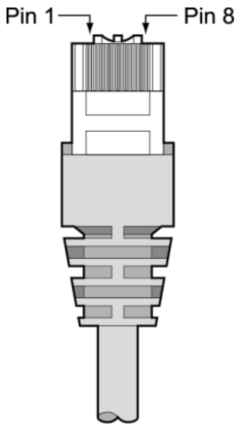
USB Boot Upgrade Method

Assuming the Primary radio is active and the Secondary radio is standby

1. Using the Hardware Manual Lock switch, force the primary radio to active.
2. Insert the USB flash drive with the new software release into the secondary radio host port .
3. Power cycle the secondary radio. The radio will be upgraded with the new software.
4. When the secondary radio upgrade is completed, remove the USB flash drive, power cycle the secondary radio and wait for it to become standby.
5. Using the Hardware Manual Lock switch, force the secondary radio to active.
6. Insert the USB flash drive with the new software release into the primary radio host port .
7. Power cycle the primary radio. The radio will be upgraded with the new software.
8. When the primary radio upgrade is completed, remove the USB flash drive, power cycle the primary radio and wait for it to become standby.
9. When the upgrade process is complete, set the Hardware Manual Lock switch to the Auto position. The secondary radio will remain active and the primary radio will remain standby. To set the primary radio to active, use the hardware lock switch to select the primary radio and wait for it to become active, then set the hardware manual lock switch to the Auto position.

11. Interface Connections

RJ45 Connector Pin Assignments



RJ45 pin numbering

Ethernet Interface Connections

Pin Number	Pin Function	Direction	TIA-568A Wire Colour	TIA-568B Wire Colour
1	Transmit	Output	Green/white	Orange/white
2	Transmit	Output	Green	Orange
3	Receive	Input	Orange/white	Green/white
4	Not used		Blue	Blue
5	Not used		Blue/white	Blue/white
6	Receive	Input	Orange	Green
7	Not used		Brown/white	Brown/white
8	Not used		Brown	Brown

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

RJ45 connector LED indicators		
LED	**Status**	**Explanation**
Green	On	Ethernet signal received
Orange	Flashing	Data traffic present on the interface

Note: Do not connect Power over Ethernet (PoE) connections to the Aprisa SR+ Ethernet ports as this will damage the port.

RS-232 Serial Interface Connections

RS-232 Pinout

The Aprisa 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 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

RS-232 RJ45 LED Indicators

LED	Status	Explanation
Green	On	RS-232 device connected
Orange	Flashing	Data present on the interface

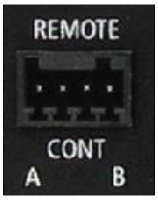
Alarm Interface Connections

RJ45 Pin Number	Pin Function	Direction	TIA-568A Wire Colour	TIA-568B Wire Colour
1	Alarm 1 Input	Input	Green / white	Orange/white
2	Ground		Green	Orange
3	Alarm 2 Input	Input	Orange / white	Green/white
4	Ground		Blue	Blue
5	Alarm 1 Output	Output	Blue / white	Blue/white
6	Ground		Orange	Green
7	Alarm 2 Output	Output	Brown / white	Brown/white
8	Ground		Brown	Brown

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

Protection Switch Remote Control Connections

1 2 3 4



Pin Number	1	2	3	4
Function	A radio active	Ground	B radio active	Ground

12. Alarm Types and Sources

Alarm Types

There are three types of alarm event configuration types:

1. Threshold Type

These alarm events have lower and upper limits. An alarm is raised if current reading is outside the limits.

Note: the limits for PA Current, TX AGC, TX Reverse Power and Thermal shutdown are not user configurable.

2. Error Ratio Type

This is the ratio of bad packets vs total packets in the defined sample duration.

For Serial, it is the ratio of bad characters vs total characters in the duration seconds. An alarm is raised if current error ratio is greater than the configured ratio. The error ratio is configured in ‘Upper Limit’ field and accepts value between 0 and 1. Monitoring of these events can be disabled by setting the duration parameter to 0.

3. Sample Duration Type

Used for No Receive data events type. An alarm is raised if no data is received in the defined sample duration. Monitoring of these events can be disabled by setting the duration parameter to 0.

See ‘Events > Events Setup’ on page 208 for setup of alarm thresholds / sample durations etc.

Alarm Events

Transmitter Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
1	PA Current	critical(1)	Threshold Type	Alarm to indicate that the current drawn by the transmitter power amplifier is outside defined limits.	Check antenna is not open or shorted, check duplexer correctly connected and tuned, if OK replace radio.
61	PA Driver Current	critical(1)	Threshold Type	Alarm to indicate that the current drawn by the transmitter power amplifier driver is outside defined limits.	Check antenna is not open or shorted, check duplexer correctly connected and tuned, if OK replace radio.
62	PA Stability	warning(4)	Threshold Type	Alarm to indicate that the power amplifier is oscillating which may cause corruption of the TX signal	Check antenna is not open or shorted, check duplexer correctly connected and tuned, if OK replace radio.
2	TX AGC	critical(1)	Threshold Type	Alarm to indicate that the variable gain control of the transmitter is outside defined limits.	Check antenna is not open or shorted, check duplexer correctly connected and tuned, if OK replace radio.
3	TX Reverse Power	warning(4)	Threshold Type	Alarm to indicate that the antenna is not connected to the radio	Check antenna is not open or shorted, check duplexer correctly connected and tuned, and confirm VSWR at TX port is less than 2:1. If OK replace radio.
60	TX Forward Power	warning(4)	Threshold Type	Alarm to indicate that the transmitter power is outside the selected TX power setting.	Check antenna is not open or shorted, check duplexer correctly connected and tuned, and confirm VSWR at TX port is less than 2:1. If OK replace radio.
4	Temperature Threshold	warning(4)	Threshold Type	Alarm to indicate that the transmitter temperature is outside defined limits.	Check ambient temperature and for airflow obstructions.
5	TX Synthesizer Not Locked	critical(1)	Threshold Type	Alarm to indicate that the transmitter synthesizer is not locked.	Power off radio and restart. If condition persists replace radio.
31	Thermal Shutdown	critical(1)	Threshold Type	Alarm to indicate that the transmitter has shutdown due to excessively high temperature.	Check ambient temperature and for airflow obstructions.

Receiver Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
7	RSSI Threshold	warning(4)	Threshold Type	Alarm to indicate that the receiver RSSI reading taken on the last packet received is outside defined limits.	Check antenna is not open or shorted. If the antenna is directional check for off-pointing.
8	RX Synthesizer Not Locked	critical(1)	Not Configurable	Alarm to indicate that the receiver Synthesizer is not locked on the RF received signal.	Power off radio and restart. If condition persists replace radio.
9	RX CRC Errors	warning(4)	Error Ratio Type	Alarm to indicate that the data received on the RF path contains errors at a higher rate than the defined error rate threshold.	Check antenna is not open or shorted. Check duplexer is correctly tuned. If the antenna is directional check for off-pointing. Power off radio and restart. If condition persists replace radio.

Radio Interface Path Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
34	RF No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that there is no data received on the RF path in the defined duration period.	Check master is operational. If new deployment check set-up, frequencies, and duplexer (if used). Check antenna is not open or shorted. If the antenna is directional check for off-pointing. Power off radio and restart. If condition persists replace radio.

Modem Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
68	Modem FEC disable	warning(4)	Not Configurable	Alarm to indicate that FEC has been disabled. This could be a permanent event or a timed event.	Alarm to indicate that FEC has been disabled. This could be a permanent event or a timed event.
70	Modem ACM locked	warning(4)	Not Configurable	Alarm to indicate that the ACM has been locked to a fixed coding and modulation. This could be a permanent event or a timed event.	Alarm to indicate that the ACM has been locked to a fixed coding and modulation. This could be a permanent event or a timed event.

Customer Equipment Interface Path Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
10	Port 1 Eth No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that Ethernet port 1 has no received input signal in the defined duration period.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
11	Port 1 Eth Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 1 received input signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
12	Port 1 Eth Data Transmit Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 1 transmitted output signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
35	Port 2 Eth No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that Ethernet port 2 has no received input signal in the defined duration period.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
36	Port 2 Eth Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 2 received input signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
37	Port 2 Eth Data Transmit Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 2 transmitted output signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
44	Port 3 Eth No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that Ethernet port 3 has no received input signal in the defined duration period.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
45	Port 3 Eth Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 3 received input signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
46	Port 3 Eth Data Transmit Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 3 transmitted output signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
48	Port 4 Eth No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that Ethernet port 4 has no received input signal in the defined duration period.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
49	Port 4 Eth Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 4 received input signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
50	Port 4 Eth Data Transmit Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 4 transmitted output signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
13	Port 1 Serial Data No Receive Data	warning(4)	Sample Duration Type	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.
14	Port 1 Serial Data Receive Errors	warning(4)	Error Ratio Type	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.
52	Port 2 Serial Data No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that the RS-232 port 2 has no received input signal in the defined duration period.	Check serial ports settings, check serial cable and connector.
53	Port 2 Serial Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that the RS-232 port 2 received input signal contains errors at a higher rate than the defined error rate threshold.	Check serial ports settings, check serial cable and connector.
63	USB Port Serial Data No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that the USB port has no received input signal in the defined duration period.	Check serial ports settings, check USB serial cable and adapter, check serial connector.
64	USB Port Serial Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that the USB port received input signal contains errors at a higher rate than the defined error rate threshold.	Check serial ports settings, check USB serial cable and adapter, check serial connector.

Component Failure Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
16	Component Failure	major(2)	Not Configurable	Alarm to indicate that a hardware component has failed.	Power off and restart radio. If fault persists replace radio.

Hardware Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
56	VDC Power Supply	warning(4)	Not Configurable	Alarm to indicate that the input power source is outside the operating limits of 10 to 30 VDC	Check DC connection to radio. Replace power supply.
57	3.3 Volts Power Supply	warning(4)	Not Configurable	Alarm to indicate that the 3.3 volt power rail is outside defined limits.	Power off and restart radio. If fault persists replace radio.
58	5.0 Volts Power Supply	warning(4)	Not Configurable	Alarm to indicate that the 5.0 volt power rail is outside defined limits.	Power off and restart radio. If fault persists replace radio.
59	7.2 Volts Power Supply	warning(4)	Not Configurable	Alarm to indicate that the 7.2 volt power rail is outside defined limits.	Power off and restart radio. If fault persists replace radio.
71	15 Volts Power Supply	warning(4)	Not Configurable	Alarm to indicate that the 15 volt power rail is outside defined limits.	Power off and restart radio. If fault persists replace radio.

Software Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
20	Calibration Failure	major(2)	Not Configurable	Alarm to indicate that the RF calibration has failed.	Power off and restart radio. If fault persists replace radio.
21	Configuration Not Supported	major(2)	Not Configurable	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(4)	Not Configurable	Alarm to indicate a network configuration problem e.g. remote not registered.	Check for invalid parameters. Audit network settings.
73	Radio Network	warning(4)	Not Configurable	Alarm to indicate that there is an alarm in the radio network e.g. a remote radio has not registered or duplicate IP address.	Check for duplicate or invalid parameters. Audit network settings.
39	Software Restart Required	warning(4)	Not Configurable	Alarm to indicate that a configuration has changed that requires a software reboot.	Reboot radio.

Hardware Alarm Input Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
24	Alarm Input 1	warning(4)	Not Configurable	Alarm to indicate that there is an active alarm on hardware alarm input 1	Action depends on nature of third-party alarm.
25	Alarm Input 2	warning(4)	Not Configurable	Alarm to indicate that there is an active alarm on hardware alarm input 2	Action depends on nature of third-party alarm.

Protected Station Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
17	Protection Sw Manual Lock	warning(4)	Not Configurable	Alarm to indicate that the Protection Switch Software Manual Lock has been activated.	Information only.
18	Protection Hw Manual Lock	warning(4)	Not Configurable	Alarm to indicate that the Protection Switch Hardware Manual Lock has been activated.	Remember to unlock the Hardware Manual Lock for normal operation
23	Protection Peer Comms Lost	major(2)	Not Configurable	Alarm to indicate that the standby radio has lost communication with the active radio.	Check that the partner radio is powered on and the 'Protect' cable is plugged from the switch to both radios. Check that the radios have been setup for protected operation.
54	Protection Hardware Failure	major(2)	Not Configurable	Alarm to indicate that there is a failure in the protection switch hardware.	Check that the cables are connecting the switch to both radios. Check that the switch and both radios are the same Data interface port options e.g. 2E2S

Informational Events

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
26	User authentication succeeded	information (5)	Event to indicate that a user is successfully authenticated on the radio during login. The information on the user that was successfully authenticated is provided in the eventHistoryInfo object of the Event History Log.	Information No action required unless unexpected
27	User authentication failed	information (5)	Event to indicate that a user has failed to be authenticated on the radio during login. The information on the user that was unsuccessfully authenticated is provided in the eventHistoryInfo object of the Event History Log.	Check for possible intrusion attempt. If unexpected follow cyber incident report procedure.
28	Protection switch failed	information (5)	Event to indicate that a protection switch-over cannot occur for some reason. The reason for the failure to switch is described in the eventHistoryInfo object of the Event History Log.	Investigate reason for switch over and take remedial action.
29	Software System Check	information (5)	Event to indicate that the software has done a system check on the radio. Any information relevant to the cause of the event is provided in the eventHistoryInfo object of the Event History Log.	Information No action required unless unexpected
30	Software Start Up	information (5)	Event to indicate that the radio software has started. Any information relevant to the software start up is provided in the eventHistoryInfo object of the Event History Log.	Information No action required unless unexpected
33	Protection Switch Occurred	information (5)	Event to indicate that a protection switch-over occurs for some reason. The reason for the switch-over is described in the eventHistoryInfo object of the Event History Log.	Investigate reason for switch over and take remedial action.
41	File Transfer Activity	information (5)	Event to indicate that a data file is being transferred to or from the radio.	Information No action required unless unexpected
42	Software Management Activity	information (5)	Event to indicate that software is being distributed to remote radios.	Information No action required unless unexpected
43	Terminal Server TCP Activity	information (5)	Event to indicate TCP packets are being transferred from the terminal server.	Information No action required unless unexpected
55	Terminal Unit Information	information (5)	Event to indicate a miscellaneous activity occurring on the radio	Information no action required unless unexpected.
65	Event Action Activity	information (5)	Event to indicate an event action occurring on the radio	Information No action required unless unexpected
72	User SuperVisor Session Logout	information (5)	Event to indicate that a user has logged out or the user session has timed out	Information No action required unless unexpected

13. Specifications

RF Specifications

Blocking (desensitization), intermodulation, spurious response rejection, and adjacent channel selectivity values determined according to the methods introduced in V1.7.1 of ETSI standards EN 300 113-1.

Frequency Bands

ETSI Compliant

Broadcast Band	Frequency Band	Frequency Tuning Range	Synthesizer Step Size
UHF	320 MHz	320-400 MHz	6.250 kHz

ETSI / FCC / IC Compliant

Broadcast Band	Frequency Band	Frequency Tuning Range	Synthesizer Step Size
VHF	135 MHz (1)	135-175 MHz	1.25 kHz
UHF	400 MHz	400-470 MHz	6.250 kHz

ETSI / FCC Compliant

Broadcast Band	Frequency Band	Frequency Tuning Range	Synthesizer Step Size
UHF	450 MHz	450-520 MHz	6.250 kHz

FCC / IC Compliant

Broadcast Band	Frequency Band	Frequency Tuning Range	Synthesizer Step Size
UHF	220 MHz	215-240 MHz	1.25 kHz
UHF	896 MHz	896-902 MHz	6.250 kHz
UHF	928 MHz	928-960 MHz	6.250 kHz

Note 1: Please consult 4RF for availability.

The Frequency Tuning Range is not an indication of the exact frequencies approved by FCC / IC.

Channel Sizes

ETSI Compliant

ETSI: 320 / 450 MHz Bands

No Forward Error Correction

Channel Size	Gross Radio Capacity			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s	9.6 kbit/s
20 kHz	84.0 kbit/s	56.0 kbit/s	28.0 kbit/s	9.6 kbit/s
25 kHz	120.0 kbit/s	80.0 kbit/s	40.0 kbit/s	19.2 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s	8.4 kbit/s
20 kHz	72.7 kbit/s	32.4 kbit/s	16.2 kbit/s	8.4 kbit/s
25 kHz	103.9 kbit/s	46.2 kbit/s	23.1 kbit/s	16.7 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s	4.1 kbit/s
20 kHz	63.8 kbit/s	24.2 kbit/s	12.1 kbit/s	4.1 kbit/s
25 kHz	91.2 kbit/s	34.6 kbit/s	17.3 kbit/s	8.3 kbit/s

ETSI: 400 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s	9.6 kbit/s
20 kHz	84.0 kbit/s	56.0 kbit/s	28.0 kbit/s	9.6 kbit/s
25 kHz	120.0 kbit/s	80.0 kbit/s	40.0 kbit/s	19.2 kbit/s
50 kHz (1)	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s	38.4 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s	8.4 kbit/s
20 kHz	72.7 kbit/s	32.4 kbit/s	16.2 kbit/s	8.4 kbit/s
25 kHz	103.9 kbit/s	46.2 kbit/s	23.1 kbit/s	16.7 kbit/s
50 kHz (1)	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s	33.4 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s	4.1 kbit/s
20 kHz	63.8 kbit/s	24.2 kbit/s	12.1 kbit/s	4.1 kbit/s
25 kHz	91.2 kbit/s	34.6 kbit/s	17.3 kbit/s	8.3 kbit/s
50 kHz (1)	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s	16.5 kbit/s

Note 1: It is the responsibility of the user to check for country regulatory of 50 kHz availability in this frequency band.

ETSI: 320 MHz Band in Austria

No Forward Error Correction

Channel Size	Gross Radio Capacity			
	64 QAM	16 QAM	QPSK	4-CPFSK
20 kHz	84.0 kbit/s	56.0 kbit/s	28.0 kbit/s	9.6 kbit/s
50 kHz	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s	38.4 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC			
	64 QAM	16 QAM	QPSK	4-CPFSK
20 kHz	72.7 kbit/s	32.4 kbit/s	16.2 kbit/s	8.4 kbit/s
50 kHz	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s	33.4 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC			
	64 QAM	16 QAM	QPSK	4-CPFSK
20 kHz	63.8 kbit/s	24.2 kbit/s	12.1 kbit/s	4.1 kbit/s
50 kHz	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s	16.5 kbit/s

FCC / IC Compliant

FCC / IC: 400 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	54.0 kbit/s	36.0 kbit/s	18.0 kbit/s	9.6 kbit/s
25 kHz	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s	19.2 kbit/s
50 kHz (1)	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s	38.4 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	46.8 kbit/s	20.8 kbit/s	10.4 kbit/s	8.4 kbit/s
25 kHz	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s	16.7 kbit/s
50 kHz (1)	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s	33.4 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	41.0 kbit/s	15.6 kbit/s	7.8 kbit/s	4.1 kbit/s
25 kHz	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s	8.3 kbit/s
50 kHz (1)	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s	16.5 kbit/s

Note 1: It is the responsibility of the user to check for country regulatory of 50 kHz availability in this frequency band.

FCC / IC: 450 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	54.0 kbit/s	36.0 kbit/s	18.0 kbit/s	9.6 kbit/s
25 kHz	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s	19.2 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	46.8 kbit/s	20.8 kbit/s	10.4 kbit/s	8.4 kbit/s
25 kHz	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s	16.7 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	41.0 kbit/s	15.6 kbit/s	7.8 kbit/s	4.1 kbit/s
25 kHz	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s	8.3 kbit/s

FCC / IC: 220 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	54.0 kbit/s	36.0 kbit/s	18.0 kbit/s	9.6 kbit/s
15 kHz	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s	9.6 kbit/s
25 kHz	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s	19.2 kbit/s
50 kHz	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s	38.4 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	46.8 kbit/s	20.8 kbit/s	10.4 kbit/s	8.4 kbit/s
15 kHz	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s	8.4 kbit/s
25 kHz	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s	16.7 kbit/s
50 kHz	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s	33.4 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	41.0 kbit/s	15.6 kbit/s	7.8 kbit/s	4.1 kbit/s
15 kHz	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s	4.1 kbit/s
25 kHz	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s	8.3 kbit/s
50 kHz	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s	16.5 kbit/s

FCC / IC: 896 / 928 MHz Bands

No Forward Error Correction

Channel Size	Gross Radio Capacity			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s	9.6 kbit/s
25 kHz	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s	19.2 kbit/s
50 kHz	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s	38.4 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s	8.4 kbit/s
25 kHz	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s	16.7 kbit/s
50 kHz	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s	33.4 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC			
	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s	4.1 kbit/s
25 kHz	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s	8.3 kbit/s
50 kHz	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s	16.5 kbit/s

Receiver

ETSI / FCC / IC Compliant Receiver Sensitivity

			12.5 kHz	25 kHz	50 kHz
BER < 10^{-2}	64 QAM	Max coded FEC	-106 dBm	-102 dBm	-99 dBm
BER < 10^{-2}	64 QAM	Min coded FEC	-105 dBm	-101 dBm	-98 dBm
BER < 10^{-2}	64 QAM	No FEC	-103 dBm	-99 dBm	-96 dBm
BER < 10^{-2}	16 QAM	Max coded FEC	-113 dBm	-110 dBm	-107 dBm
BER < 10^{-2}	16 QAM	Min coded FEC	-112 dBm	-109 dBm	-106 dBm
BER < 10^{-2}	16 QAM	No FEC	-109 dBm	-106 dBm	-103 dBm
BER < 10^{-2}	QPSK	Max coded FEC	-118 dBm	-115 dBm	-112 dBm
BER < 10^{-2}	QPSK	Min coded FEC	-117 dBm	-114 dBm	-111 dBm
BER < 10^{-2}	QPSK	No FEC	-115 dBm	-112 dBm	-109 dBm
BER < 10^{-2}	4-CPFSK	Max coded FEC	NA	NA	NA
BER < 10^{-2}	4-CPFSK	Min coded FEC	-117 dBm	-114 dBm	-111 dBm
BER < 10^{-2}	4-CPFSK	No FEC	-115 dBm	-112 dBm	-109 dBm
BER < 10^{-6}	64 QAM	Max coded FEC	-103 dBm	-99 dBm	-96 dBm
BER < 10^{-6}	64 QAM	Min coded FEC	-101 dBm	-97 dBm	-94 dBm
BER < 10^{-6}	64 QAM	No FEC	-96 dBm	-92 dBm	-89 dBm
BER < 10^{-6}	16 QAM	Max coded FEC	-110 dBm	-107 dBm	-104 dBm
BER < 10^{-6}	16 QAM	Min coded FEC	-108 dBm	-105 dBm	-102 dBm
BER < 10^{-6}	16 QAM	No FEC	-102 dBm	-99 dBm	-96 dBm
BER < 10^{-6}	QPSK	Max coded FEC	-115 dBm	-112 dBm	-109 dBm
BER < 10^{-6}	QPSK	Min coded FEC	-113 dBm	-110 dBm	-107 dBm
BER < 10^{-6}	QPSK	No FEC	-108 dBm	-105 dBm	-102 dBm
BER < 10^{-6}	4-CPFSK	Max coded FEC	NA	NA	NA
BER < 10^{-6}	4-CPFSK	Min coded FEC	-113 dBm	-110 dBm	-107 dBm
BER < 10^{-6}	4-CPFSK	No FEC	-108 dBm	-105 dBm	-102 dBm

ETSI / FCC / IC Compliant Adjacent Channel Selectivity

		12.5 kHz	25 kHz	50 kHz
Adjacent channel selectivity		> -47 dBm	> -37 dBm	> -37 dBm
BER < 10^{-2}	64 QAM	> 43 dB	> 53 dB	> 53 dB
BER < 10^{-2}	16 QAM	> 43 dB	> 53 dB	> 53 dB
BER < 10^{-2}	QPSK	> 48 dB	> 58 dB	> 58 dB
BER < 10^{-2}	4-CPFSK	> 55 dB	> 65 dB	> 65 dB

ETSI / FCC / IC Compliant Co-Channel Rejection

		12.5 kHz	25 kHz	50 kHz
BER < 10^{-2}	64 QAM	> -23 dB	> -23 dB	> -23 dB
BER < 10^{-2}	16 QAM	> -19 dB	> -19 dB	> -19 dB
BER < 10^{-2}	QPSK	> -12 dB	> -12 dB	> -12 dB
BER < 10^{-2}	4-CPFSK	> -17 dB	> -17 dB	> -17 dB

ETSI / FCC / IC Compliant Intermodulation Response Rejection

		12.5 kHz	25 kHz	50 kHz
Intermodulation response rejection		> -35 dBm	> -35 dBm	> -35 dBm
BER < 10^{-2}	64 QAM	> 55 dB	> 55 dB	> 55 dB
BER < 10^{-2}	16 QAM	> 55 dB	> 55 dB	> 55 dB
BER < 10^{-2}	QPSK	> 60 dB	> 60 dB	> 60 dB
BER < 10^{-2}	4-CPFSK	> 65 dB	> 65 dB	> 65 dB

ETSI / FCC / IC Compliant Blocking or Desensitization

		12.5 kHz	25 kHz	50 kHz
Blocking or desensitization		> -17 dBm	> -17 dBm	> -17 dBm
BER < 10^{-2}	64 QAM	> 73 dB	> 73 dB	> 73 dB
BER < 10^{-2}	16 QAM	> 73 dB	> 73 dB	> 73 dB
BER < 10^{-2}	QPSK	> 78 dB	> 78 dB	> 78 dB
BER < 10^{-2}	4-CPFSK	> 85 dB	> 85 dB	> 85 dB

ETSI / FCC / IC Compliant Spurious Response Rejection

		12.5 kHz	25 kHz	50 kHz
Spurious response rejection		> -32 dBm	> -32 dBm	> -32 dBm
BER < 10^{-2}	64 QAM	> 58 dB	> 58 dB	> 58 dB
BER < 10^{-2}	16 QAM	> 58 dB	> 58 dB	> 58 dB
BER < 10^{-2}	QPSK	> 63 dB	> 63 dB	> 63 dB
BER < 10^{-2}	4-CPFSK	> 70 dB	> 70 dB	> 70 dB

ETSI / FCC / IC Compliant Receiver Spurious Radiation

	12.5 kHz	25 kHz	50 kHz
Receiver spurious radiation	> -57 dBm	> -57 dBm	> -57 dBm

Transmitter

Average Power output Note: The Peak Envelope Power (PEP) at maximum set power level is +41 dBm.	64 QAM	0.01 to 2.5 W (+10 to +34 dBm, in 1 dB steps)
	16 QAM	0.01 to 3.2 W (+10 to +35 dBm, in 1 dB steps)
	QPSK	0.01 to 5.0 W (+10 to +37 dBm, in 1 dB steps)
	4-CPFSK [Note 1]	0.01 to 10.0 W (+10 to +40 dBm, in 1 dB steps)

Note 1: Please consult 4RF for availability

Note: The Aprisa SR+ transmitter contains power amplifier protection which allows the antenna to be disconnected from the antenna port without product damage.

Adjacent channel power	< - 60 dBc
Transient adjacent channel power	< - 60 dBc
Spurious emissions	< - 37 dBm
Attack time	< 1.5 ms
Release time	< 0.5 ms
Data turnaround time	< 2 ms
Frequency stability	± 1.0 ppm
Frequency aging	< 1 ppm / annum

Modem

Forward Error Correction	Variable length concatenated Reed Solomon plus convolutional code
Adaptive Burst Support	Adaptive FEC Adaptive Coding Modulation

Data Payload Security

Data payload security	CCM* Counter with CBC-MAC
Data encryption	Counter Mode Encryption (CTR) using Advanced Encryption Standard (AES) 128, 192 or 256
Data authentication	Cipher Block Chaining Message Authentication Code (CBC-MAC) using Advanced Encryption Standard (AES) 128, 192 or 256

Interface Specifications

Ethernet Interface

The Aprisa SR+ radio features an integrated 10Base-T/100Base-TX layer-2 Ethernet switch.

To simplify network setup, each port supports auto-negotiation and auto-sensing MDI/MDIX. Operators can select from the following preset modes:

- Auto negotiate
- 10Base-T half or full duplex
- 100Base-TX half or full duplex

The Ethernet ports are IEEE 802.3-compatible. The L2 Bridge (Switch) is IEEE 802.1d/q/p compatible, and supports VLANs and VLAN manipulation of add/remove VLANs.

General	Interface	RJ45 x 2 (Integrated 2-port switch)
	Cabling	CAT-5/6 UTP, 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 radio link capacity.
	Maximum transmission unit	Option setting of 1522 or 1536 octets
	Address table size	1024 MAC addresses
	Ethernet mode	10Base-T or 100Base-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 SR+ Ethernet ports as this will damage the port.

RS-232 Asynchronous Interface

The Aprisa SR+ radio'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

Hardware Alarms Interface

The hardware alarms interface supports two alarm inputs and two alarms outputs.

Alarm Inputs

The alarm connector provides two hardware alarm inputs for alarm transmission to the other radios in the network.

Interface	RJ45 connector
Detector type	Non-isolated ground referenced voltage detector
Detection voltage - on	> +10 VDC
Detection voltage - off	< +4 VDC
Maximum applied input voltage	30 VDC
Maximum input current limit	10 mA

Alarm Outputs

The alarm connector provides two hardware alarm outputs for alarm reception from other radios in the network.

Interface	RJ45 connector
Output type	Non-isolated ground referenced open collector output
Maximum applied voltage	30 VDC
Maximum drive current	100 mA
Overload protection	Thermally resettable fuse

Protect Interface

The Protect interface is used to connect the radios to the protection switch within a Protected Station. It is not a customer interface.

Protection Switch Specifications

RF Insertion Loss	< 0.5 dB (switch and connecting cables)
Remote Control inputs	Logic 4700 ohms pullup to +3.3 VDC

Power Specifications

Power Supply

Aprisa SR+ Radio

Nominal voltage	+13.8 VDC (negative earth)
Absolute input voltage range	+10 to +30 VDC
Maximum power input	35 W
Connector	Molex 2 pin male screw fitting 39526-4002

Aprisa SR+ Protected Station

Power Input	13.8 VDC	48 VDC
Nominal voltage	+13.8 VDC (negative earth)	48 VDC (floating)
Absolute input voltage range	+10 to +30 VDC	18 to 60 VDC
Maximum power input	35 W	
Connector	2x Molex 2 pin male screw fitting 39526-4002	

Power Consumption

Note: The radio power consumption is very dependent on transmitter power, the type of traffic and network activity.

Aprisa SR+ Radio

Mode	Power Consumption (10 W radio with 4-CPFSK modulation)
Transmit / Receive	< 35 W for 10 W transmit power
	< 25.0 W for 1 W transmit power
Receive only	< 7 W

Aprisa SR+ Protected Station and Aprisa SR+ Data Driven Protected Station

Mode	Power Consumption (10 W radios with 4-CPFSK modulation)
Transmit / Receive	< 42 W for 10 W transmit power
	< 32.0 W for 1 W transmit power
Receive only	< 15 W

Power Dissipation

Aprisa SR+ Radio

Transmit Power	Power Dissipation (10 W radio with 4-CPFSK modulation)
10 W transmit power	< 25 W
1 W transmit power	< 24 W

Aprisa SR+ Protected Station and Aprisa SR+ Data Driven Protected Station

Transmit Power	Power Dissipation (10 W radios with 4-CPFSK modulation)
10 W transmit power	< 32 W
1 W transmit power	< 31 W

General Specifications

Environmental

Operating temperature range	-40 to +70˚ C (-40 to +158˚ F)
Storage temperature range	-40 to +80˚ C (-40 to +176˚ F)
Operating humidity	Maximum 95% non-condensing
Acoustic noise emission	No audible noise emission

Mechanical

Aprisa SR+ Radio

Dimensions	Width 210 mm (8.27”) Depth 130 mm (5.12”) and 146 mm (5.748”) with TNC connectors Height 41.5 mm (1.63”)
Weight	1.25 kg (2.81 lbs)
Colour	Matt black
Mounting	Wall (2 x M5 screws) Rack shelf (2 x M4 screws) DIN rail bracket

Aprisa SR+ Protected Station

Dimensions	Width 432.6 mm (17”) Depth 372 mm (14.6”) and 388 mm (15.276”) with TNC connectors Height 2U plus external duplexer (if used)
Weight	12 kg (27 lbs) (includes the 2 radios)
Colour	Matt black
Mounting	Rack mount (2 x M6 screws)

Compliance

ETSI

Radio	EN 300 113-2
EMI / EMC	EN 301 489 Parts 1 & 5
Safety	EN 60950-1:2006 Class 1 div 2 for hazardous locations
Environmental	ETS 300 019 Class 3.4 Ingress Protection code IP51

FCC

Radio	47CFR part 24, part 90 and part 101 Private Land Mobile Radio Services
EMC	47CFR part 15 Radio Frequency Devices, EN 301 489 Parts 1 & 4
Safety	EN 60950-1:2006 Class 1 div 2 for hazardous locations
Environmental	ETS 300 019 Class 3.4 Ingress Protection code IP51

IC

Radio	RSS-119 / RSS-134
EMC	This Class A digital apparatus complies with Canadian standard ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.
Safety	EN 60950-1:2006 Class 1 div 2 for hazardous locations
Environmental	ETS 300 019 Class 3.4 Ingress Protection code IP51

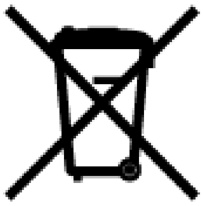
14. Product End Of Life

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.

4RF 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 SR+ radio, contact us (on page 15).

15. Copyrights

Mirrored Bits® is a registered trademark of Schweitzer Engineering Laboratories, Inc

16. Abbreviations

AES	Advanced Encryption Standard
AGC	Automatic Gain Control
BER	Bit Error Rate
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC integrity
DCE	Data Communications Equipment
DTE	Data Radio Equipment
EMC	Electro-Magnetic Compatibility
EMI	Electro-Magnetic Interference
ESD	Electro-Static Discharge
ETSI	European Telecommunications Standards Institute
FW	Firmware
HW	Hardware
IF	Intermediate Frequency
IP	Internet Protocol
I/O	Input/Output
ISP	Internet Service Provider
kbit/s	Kilobits per second
kHz	Kilohertz
LAN	Local Area Network
LED	Light Emitting Diode
mA	Milliamps
MAC	Media Access Control
MAC	Message Authentication Code
Mbit/s	Megabits per second
MHz	Megahertz
MIB	Management Information Base
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
ms	milliseconds
NMS	Network Management System
PC	Personal Computer
PCA	Printed Circuit Assembly
PLL	Phase Locked Loop
ppm	Parts Per Million
PMR	Public Mobile Radio
RF	Radio Frequency
RoHS	Restriction of Hazardous Substances
RSSI	Received Signal Strength Indication
RX	Receiver
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
SWR	Standing Wave Ratio
TCP/IP	Transmission Control Protocol/Internet Protocol
TCXO	Temperature Compensated Crystal Oscillator
TFTP	Trivial File Transfer Protocol
TMR	Trunk Mobile Radio
TX	Transmitter
UTP	Unshielded Twisted Pair
VAC	Volts AC
VCO	Voltage Controlled Oscillator
VDC	Volts DC
WEEE	Waste Electrical and Electronic Equipment

17. Index

S

T

U

W