4RF

Aprisa SR

User Manual

August 2015

Version 1.6.5b

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 digital 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 Channel	25 kHz Channel
Radio performance	EN 300 113-2	EN 302 561
EMC	EN 301 489 Parts 1 & 5	
Environmental	EN 300 019, Class 3.4	
Safety	EN 60950-1:2006	

Frequency band	**Channel size**	**Power input**	**Notified body**
136-174 MHz	12.5 kHz, 25 kHz	12 VDC	
400-470 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 90 Private Land Mobile Radio Services
EMC	47CFR part 15 Radio Frequency Devices
Environmental	EN 300 019, Class 3.4
Safety	EN 60950-1:2006

Frequency band limits	**Channel size**	**Power input**	**Authorization**	**FCC ID**
406.1 to 454.0 MHz 456.0 to 470.0 MHz	12.5 kHz	12 VDC	Part 90	UIPSRN0400012A
136-174 MHz	6.25 kHz, 12.5 kHz, 25 kHz	12 VDC	Part 90	UIPSR135M130

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.

Compliance Industry Canada

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

Radio	RSS-GEN, RSS-119
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
Safety	EN 60950-1:2006

Frequency band limits	**Channel size**	**Power input**	**Authorization**	**IC ID**
406.1 to 430.0 MHz 450.0 to 470.0 MHz	12.5 kHz, 25 kHz	12 VDC	RSS-119	6772A-SRN400
136-174 MHz	6.25 kHz, 12.5 kHz, 25 kHz	12 VDC	RSS-119	6772A-SR135M130

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: 4-CPFSK

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.

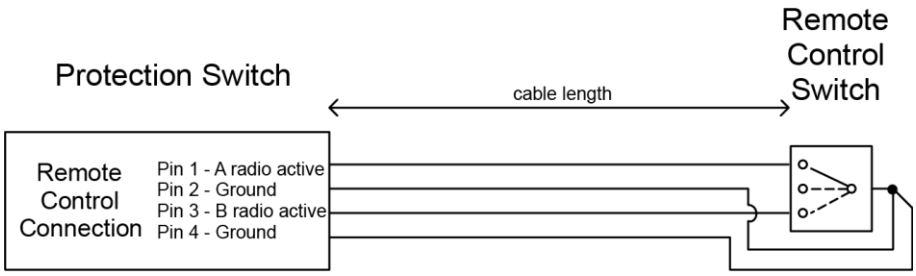
WARNING - EXPLOSION HAZARD - DO NOT REPLACE FUSE UNLESS POWER HAS BEEN SWITCHED OFF OR THE AREA IS KNOWN TO BE NON-HAZARDOUS.

AVERTISSEMENT - RISQUE D'EXPLOSION - COUPER LE COURANT OU S'ASSURER QUE L'EMPLACEMENT EST DESIGNE NON DANGEREUX AVANT DE REPLACER LE FUSIBLE.

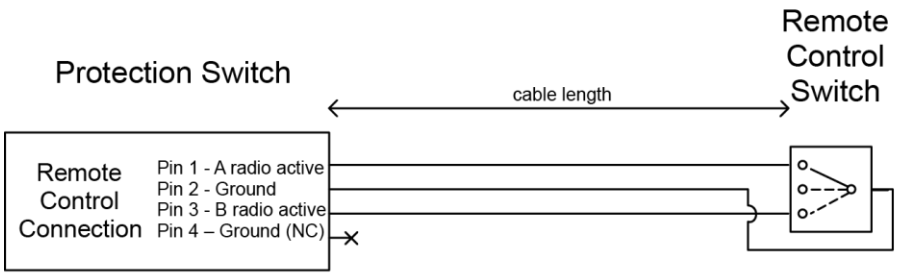
WARNING - EXPLOSION HAZARD - DO NOT DISCONNECT EQUIPMENT UNLESS POWER HAS BEEN SWITCHED OFF OR THE AREA IS KNOWN TO BE NON-HAZARDOUS.

AVERTISSEMENT - RISQUE D'EXPLOSION - AVANT DE DECONNECTER L'EQUIPEMENT, COUPER LE COURANT OU S'ASSURER QUE L'EMPLACEMENT EST DESIGNE NON DANGEREUX.

Protection switch remote control connection diagram for hazardous locations.



Vmax = 3.3 V d.c.; Imax = 1.4 A; Ca = 270 uF; La = 18 uH
Maximum cable length = 30 ft (9.1 m)



Vmax = 3.3 V d.c.; Imax = 1.4 A; Ca = 270 uF; La = 18 uH
Maximum cable length = 40 ft (12.2 m)

Title: Control Drawing
Revision: 1.0
Date: 21 May 2013

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

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 34
2.	Ensure that the site preparation is complete: • Power requirements • Tower requirements • Environmental considerations, for example, temperature control • Mounting space	Page 37

Phase 2:	**Installing the radios**	
1.	Mount the radio.	Page 40
2.	Connect earthing to the radio.	Page 39
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 39
5.	Connect the coaxial jumper cable between the lightning protection and the radio antenna port.	Page 44
6.	Connect the power to the radio.	Page 45

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 199.	Page 199
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 51
4.	Open a web browser and login to the radio.	Page 49
5.	Set or confirm the RF characteristics: • TX and RX frequencies • TX output power	Page 78
6.	Compare the actual RSSI to the expected RSSI value (from your path planning).	
7.	Align the antennas.	Page 205
8.	Confirm that the radio is operating correctly; the OK, DATA, CPU and RF LEDs are light green (the AUX LED will be off).	

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 1.6.5.

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 education 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 ‘Radio Software Upgrade’ on page 224)
- 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

In a simple point-to-multipoint network, an Aprisa SR, configured as a base station, will communicate with multiple remote units in a given coverage area. With a link range of up to 60 km, a typical deployment will have 30 – 150 remote stations operating to the base station. However, geographic features, such as hills, mountains, trees and foliage, or other path obstructions, such as buildings, tend to 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 Forward Error Correction (FEC) which greatly improves the sensitivity 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 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.

The following are the maximum number of remotes that can operate to a base station for the product configuration:

Configuration	Maximum Number Of Remotes
Non Protected Base Station	500
Protected Base Station	150

Remote Messaging

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 (RF LED flashing red) within 10 minutes, it will automatically reboot. If a remote station has registered with the base station but then loses communication, it will automatically reboot within 6 minutes.

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.

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.

Only the base station can receive the unicast messages transmitted from the remote station. Unicast messages are ignored by other remote stations which may be able to receive them.

Repeater Messaging

The Aprisa SR uses a routed protocol throughout the network whereby messages contain source and destination addresses. Upon registration, the radios populate an internal neighbor table to identify the radios in the network. The remote stations will register with a base station, or a repeater, and the repeater registers with a base station. In networks with a repeater, the repeater must register with the base station before the remotes can register with the repeater.

Additionally, all messages contain a 'message type' field in the header and messages are designated as either a 'broadcast' message, originating from a base station, or a 'unicast' message, originating from a remote station.

In a network with a repeater, or multiple repeaters, the base station broadcasts a message which contains a message type, a source address and a destination address. The repeater receives the message and recognizes it is a broadcast message, from the message type and source address and re-broadcasts the message across the network. 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 message type (unicast) a source address and a destination address (the base station). The repeater will receive this message; recognize the message type and source address and forward it to the destination address.

It is this methodology which prevents repeater-repeater loops. If there is repeater (A) which, in some circumstances, is able to pick up the RF signal from another repeater (B), it will not forward the message as it will only forward broadcast messages from the base station (recognized by the source address). For unicast messages the repeater (A) will recognize that the message (from repeater (B)) is not from a remote with which it has an association and similarly ignore the message.

Product Features

Functions

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

VHF 136	135-175 MHz
UHF 320	320-400 MHz
UHF 400	400-470 MHz

- Channel sizes:

  6.25 kHz (VHF FCC / IC only)
  12.5 kHz
  25 kHz

- Typical deployment of 30 remote stations from one base station with a practical limit of a few hundred remote stations
- Transparent to all common SCADA protocols; e.g. Modbus, IEC 60870-5-101/104, DNP3 or similar
- Dual antenna port option for external duplexers or filters (half duplex operation)
- Two Ethernet data interfaces *plus* two RS-232 asynchronous data interfaces
- Terminal server operation for transporting RS-232 traffic over IP
- Data encryption and authentication
- Layer 2 Ethernet and layer 3 IP filtering
- SNMPv2 and SNMPv3 support
- Radio and user interface redundancy (provided with Aprisa SR Protected Station)
- Complies with international standards, including ETSI RF, EMC, safety and environmental standards

Performance

- 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 with full configuration, diagnostics and monitoring functionality, including remote station configuration / diagnostics over the radio link
- LED display for on-site diagnostics
- 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
- Return Loss monitored parameter for FCC / IC VHF variants

Architecture

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 MAC layer using a proprietary implementation.

Physical Layer

The Aprisa SR PHY uses a one or two frequency ½ 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.

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.

Network Layer

Packet Routing

Packet routing is realized in the Aprisa SR by adding a network address header to the packet. This contains source and destination addresses. For the Network Layer, there are 2 addresses, the address of the originating radio and the address of the terminating radio (i.e. end to end network). This is required for routing packets across multiple hops e.g. PMP with repeaters.

The Aprisa SR uses an automated method for performing address assignment and routing information.

There are two types of packets: unicast and broadcast. Only the base station sends broadcasts which are received by all remote stations. User packets are not interpreted as the radio link is transparent.

Traffic

- Data originating on the base station is broadcast to all repeater stations and remote stations
- Data originating on a remote station is unicast to the base station only

  This can be via multiple repeater stations.
- Data originating on a repeater station is unicast to the base station only
- Data originating on a base station serial port is terminated on remote station serial ports only
- Data originating on a base station Ethernet port is terminated on remote station Ethernet ports or serial ports (Terminal Server mode)

User Traffic

User traffic is prioritized depending on the Serial and Ethernet Data Priority options (see Traffic Settings on ‘Radio > Channel Setup’ on page 83).

If the Serial and Ethernet Data Priority options are equal, then first come first served is invoked.

Repeater stations repeat traffic also on a first come first served basis.

Management Traffic

Management Traffic is prioritized relative to user traffic priority (see Traffic Settings on ‘Radio > Channel Setup’ on page 83).

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'

The security features implemented are:

- Data encryption

  Counter Mode Encryption (CTR) using Advanced Encryption Standard (AES)

- Data authentication

  Cipher Block Chaining Message Authentication Code (CBC-MAC) using Advanced Encryption Standard (AES)

- Data payload security

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

- Secured management interface protects configuration
- 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 protects against interference

Interfaces

Antenna Interface

Single Antenna Option

- 1 x TNC, 50 ohm, female connector

Dual Antenna Port Option

- 2 x TNC, 50 ohm, female connectors

Ethernet Interface

- 2 x ports 10/100 base-T Ethernet layer 2 switch using RJ45

  Used for Ethernet user traffic and product management.

RS-232 Interface

- 1x RS-232 asynchronous port using RJ45 connector
- 1x RS-232 asynchronous port using USB host port with USB to RS-232 converter

  Used for RS-232 asynchronous user traffic only.

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.

Alarms

- 2 x hardware alarm inputs on the power and alarm connector

  The alarm states can be transported over the radio link and used to generate SNMP traps.

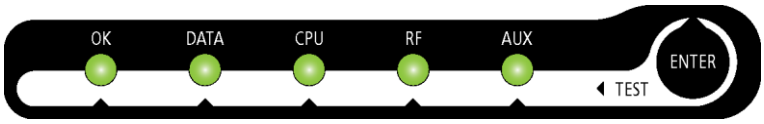
Front Panel Connections

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

Designator	Description
A1 / A2	The A1, A2 are alarm connections are used in the Protected Station.
10 - 30 VDC; 3A	+10 to +30 VDC (negative ground) DC power input using Phoenix Contact 4 pin male screw fitting connector. AC/DC and DC/DC power supplies are available as accessories. See ‘External Power Supplies’ on page 45.
ETHERNET 1	Integrated 10Base-T/100Base-TX layer-2 Ethernet switch using RJ45 connector. Used for Ethernet user traffic and product management. See ‘Ethernet > Port Setup’ on page 94.
ETHERNET 2	Integrated 10Base-T/100Base-TX layer-2 Ethernet switch using RJ45 connector. Used for Ethernet user traffic and product management. See ‘Ethernet > Port Setup’ on page 94.
MGMT	Management Port using USB micro type B connector. Used for product configuration with the Command Line Interface. See ‘Connecting to the Management Port’ on page 199.
	Host Port using USB standard type A connector. Used for software upgrade and diagnostic reporting. See ‘Radio Software Upgrade’ on page 224 and ‘Maintenance > General’ on page 120.
SERIAL	RS-232 traffic interface using a RJ45 connector. Used for RS-232 asynchronous user traffic only. See ‘Serial’ on page 88.
ANT *(Antenna connector)*	TNC, 50 ohm, female connector for connection of antenna feeder cable. See ‘Coaxial Feeder Cables’ on page 37.

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	DATA	CPU	RF	AUX
Flashing Red				*Radio not connected to a base station*	
Solid Red	Alarm present with severity Critical, Major and Minor			*RF path fail*	
Flashing Orange		*Tx Data or Rx Data on the USB management or data port*	*Device detect on the USB host port*	*RF path TX is active*	*Diagnostics Function Active*
Solid Orange	Alarm present with Warning Severity		Standby *radio in Protected Station*		
Flashing Green		*Tx Data or Rx Data on the serial port*		*RF path RX is active*	
Solid Green	*Power on and functions OK and no alarms*	*All interface ports are OK*	*Processor Block is OK and Active radio in Protected Station*	*RF path is 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 DATA LEDs
- Software upgrade completed successfully - the OK LED solid orange
- Software upgrade failed - any LED flashing red during the upgrade

Network Software Upgrade

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

Test Mode

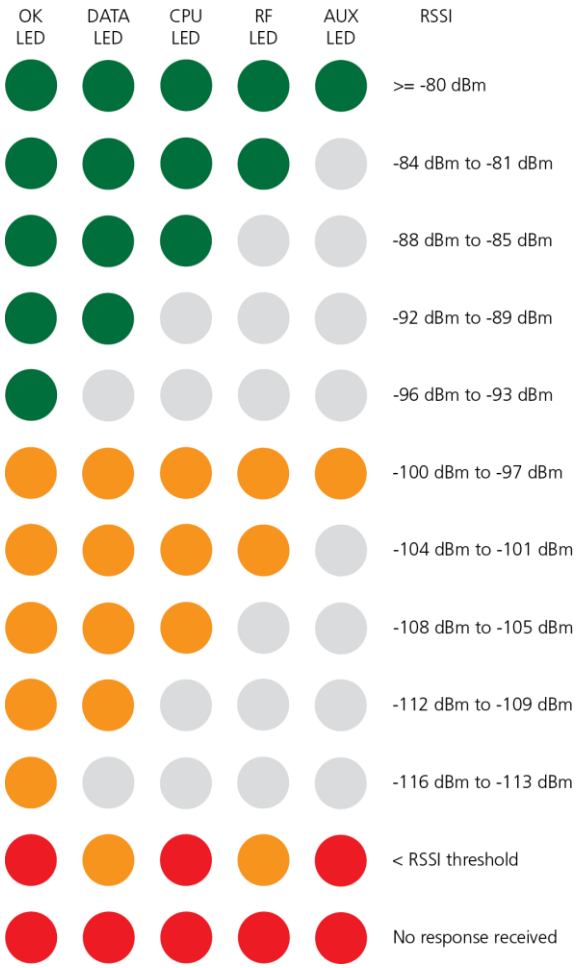
Remote station and repeater station radios have a Test Mode which presents a real time visual display of the RSSI on the LED Display panel. This can be used to adjust the antenna for optimum signal strength (see 'Maintenance > Test Mode' on page 123 for Test Mode options).

To enter Test Mode, press and hold the ENTER 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.

Note 1: Test Mode traffic has a low priority but could affect customer traffic depending on the relative priorities setup.

Note 2: The user must not activate other test modes such as PRBS, CW, Deviation or change the radio parameters such as Tx Power during test mode.

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



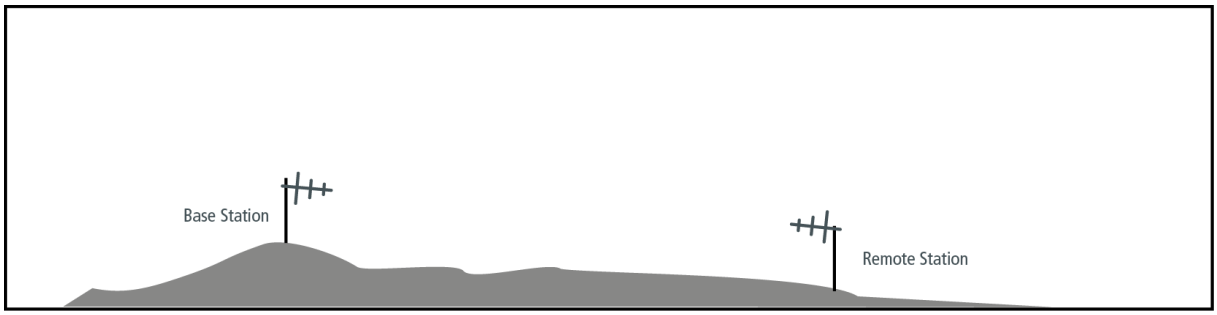
To exit Test Mode, press and hold the ENTER button until all the LEDs flash red (about 3 – 5 seconds). The RF LED will be green if the network is operating correctly.

4. Implementing the Network

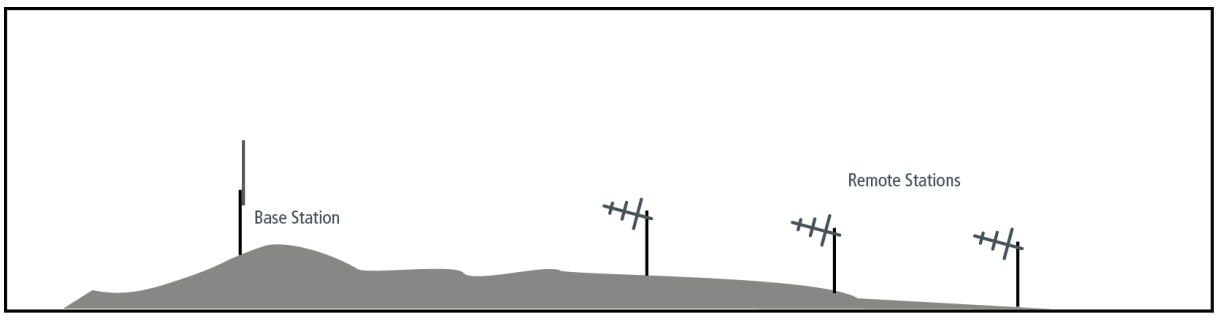
Network Topologies

The following are examples of typical network topologies:

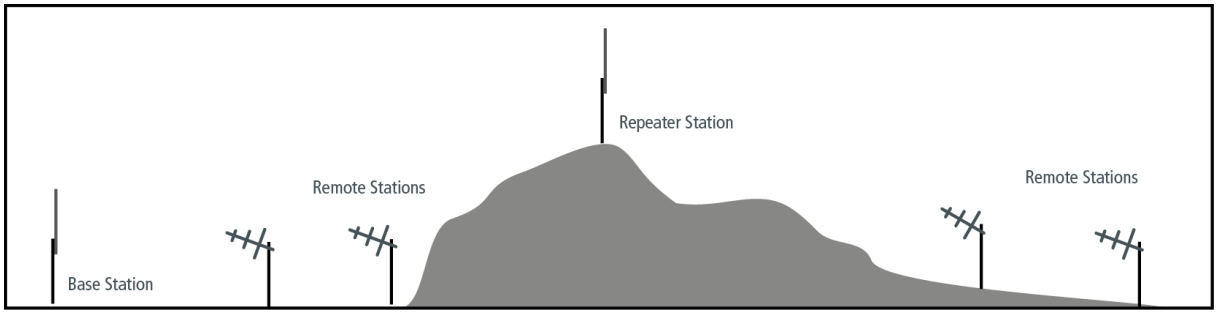
Point-To-Point Network



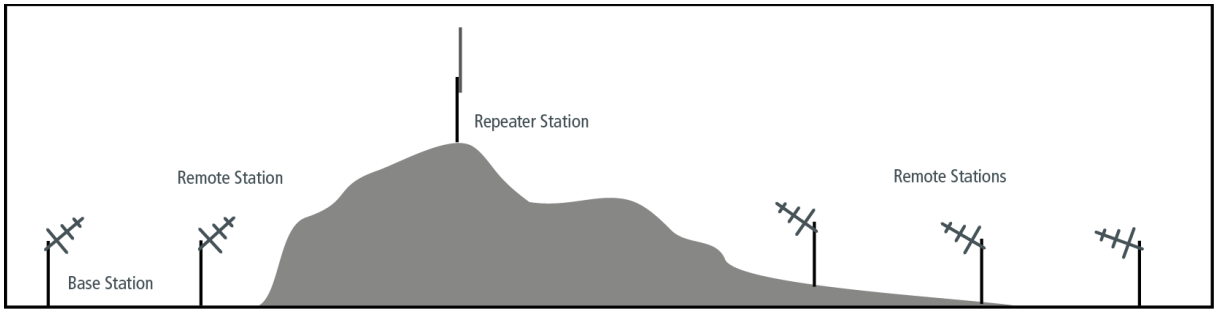
Point-to-Multipoint Network



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 40).
2. Set the radio Network ID (network) to a unique ID in your entire network (see ‘Terminal > Device’ on page 68).
3. Set the radio IP address (see ‘Terminal > Device’ on page 68).
4. Set the radio frequencies to the frequencies you wish to operate from (see ‘Radio > Radio Setup’ on page 78).
5. Set the radio operating mode to ‘base station’ (see ‘Terminal > Operating Mode’ on page 71).
6. Set the radio security settings (see ‘Security > Setup’ on page 103).

Installing the Remote Stations

To install the remote stations in your network:

1. Install the remote station radio (see ‘Installing the Radio’ on page 40).
2. Set the radio Network ID (network) to the same ID as the other stations in the network (see ‘Terminal > Device’ on page 68).
3. Set the radio IP address (see ‘Terminal > Device’ on page 68).
4. Set the radio frequencies to the base station / repeater station frequencies you wish to operate from (see ‘Radio > Radio Setup’ on page 78).
5. Set the radio operating mode to ‘remote station’ (see ‘Terminal > Operating Mode’ on page 71).
6. Set the radio security settings to the same as the base station (see ‘Security > Setup’ on page 103).

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 40).
2. Set the radio Network ID (network) to the same ID as the other stations in the network (see ‘Terminal > Device’ on page 68).
3. Set the radio IP address (see ‘Terminal > Device’ on page 68).
4. Set the radio frequencies to base station frequencies you wish to operate from (see ‘Radio > Radio Setup’ on page 78).
5. Set the radio operating mode to ‘repeater station’ (see ‘Terminal > Operating Mode’ on page 71).
6. Set the radio security settings to the same as the base station (see ‘Security > Setup’ on page 103).
7. Increase the radio network radius by one on all stations in the network (see ‘Terminal > Device’ on page 68).

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 40).
2. Set the radio Network ID (network) to the same ID as the other stations in the network (see ‘Terminal > Device’ on page 68).
3. Set the radio IP address (see ‘Terminal > Device’ on page 68).
4. Set the radio frequencies to the base station frequencies you wish to operate from (see ‘Radio > Radio Setup’ on page 78).
5. Set the radio operating mode to ‘repeater station’ (see ‘Terminal > Operating Mode’ on page 71).
6. Increase the radio network radius by one on all stations in the network (see ‘Terminal > Device’ on page 68).

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 68).

Adding a Remote Station

To add a remote station to your network:

1. Install the remote station radio (see ‘Installing the Radio’ on page 40).
2. Set the radio Network ID (network) to the same ID as the other stations in the network (see ‘Terminal > Device’ on page 68).
3. Set the radio IP address (see ‘Terminal > Device’ on page 68).
4. Set the radio frequencies to the base station / repeater station frequencies you wish to operate from (see ‘Radio > Radio Setup’ on page 78).
5. Set the radio operating mode to ‘remote station’ (see ‘Terminal > Operating Mode’ on page 71).

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

To remove a remote station from your network:

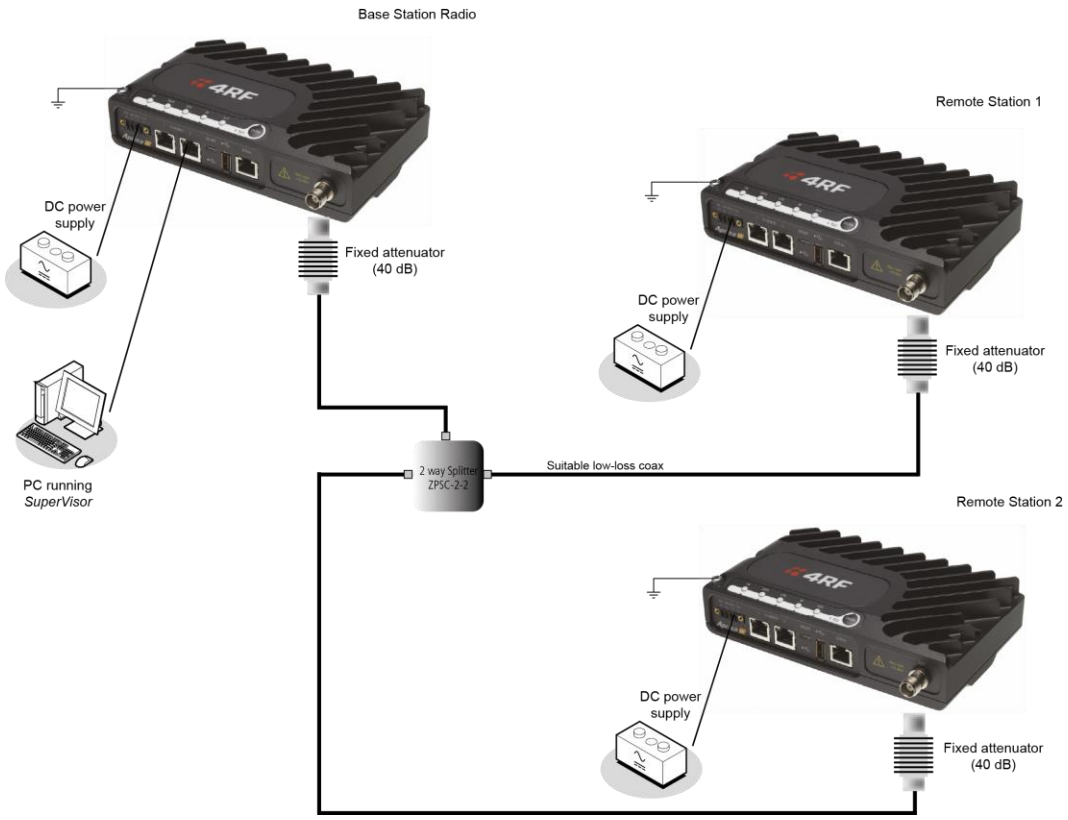
1. Turn the power off on the remote station radio you wish to remove. This is the only action that is required.

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.

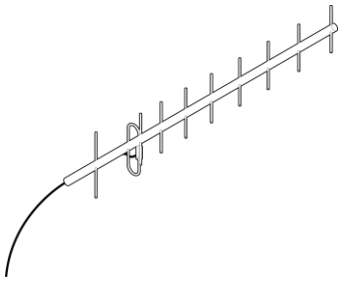
Omni Directional Collinear Antennas

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

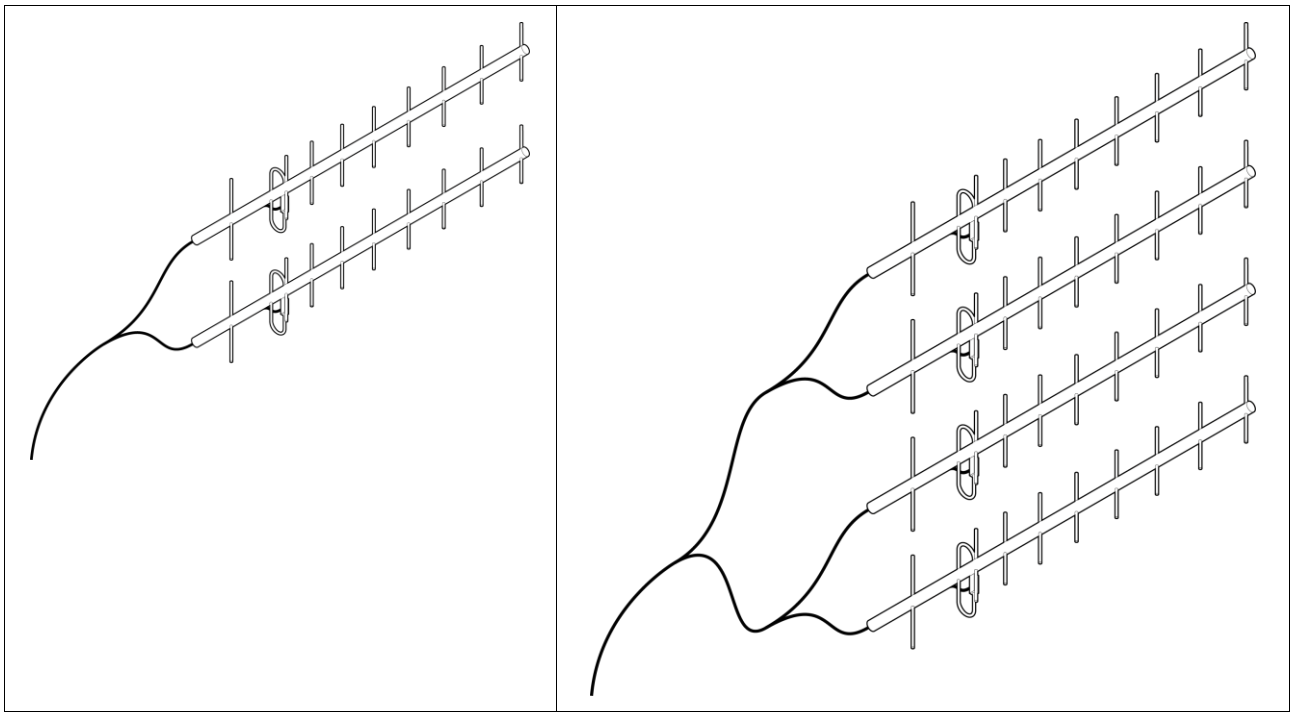
There are two main types of directional antenna that are commonly used for remote stations, Yagi and corner reflector antennas.

Yagi Antennas



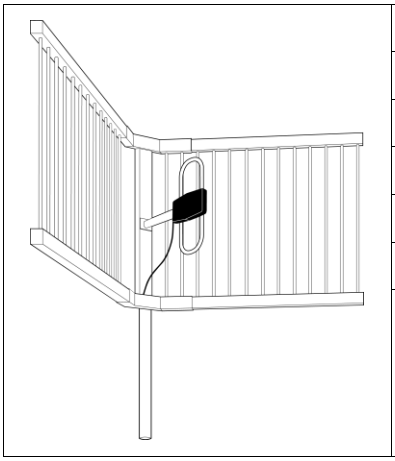
Factor	Explanation
Frequency	Often used in 350-600 MHz bands
Gain	Varies with size (typically 11 dBi to 16 dBi)
Stackable gain increase	2 Yagi antennas (+ 2.8 dB) 4 Yagi antennas (+ 5.6 dB)
Size	Range from 0.6 m to 3 m in length
Front to back ratio	Low (typically 18 to 20 dB)

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

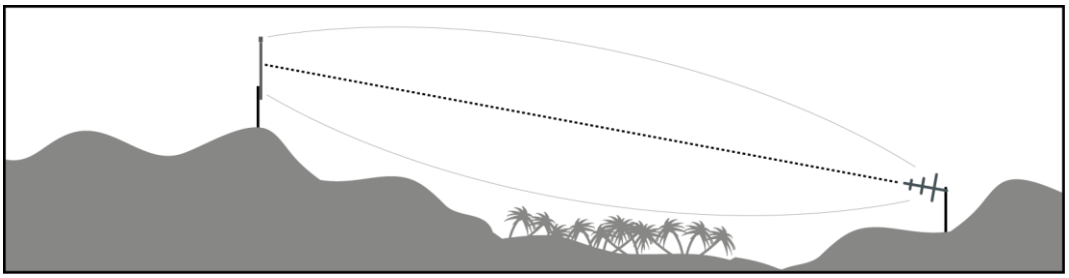


Factor	Explanation
Frequency	Often used in 330-960 MHz bands
Gain	Typically 12 dBi
Size	Range from 0.36 m to 0.75 m in length
Front to back ratio	High (typically 30 dB)
Beamwidth	Broad (up to 60˚)

Antenna Siting

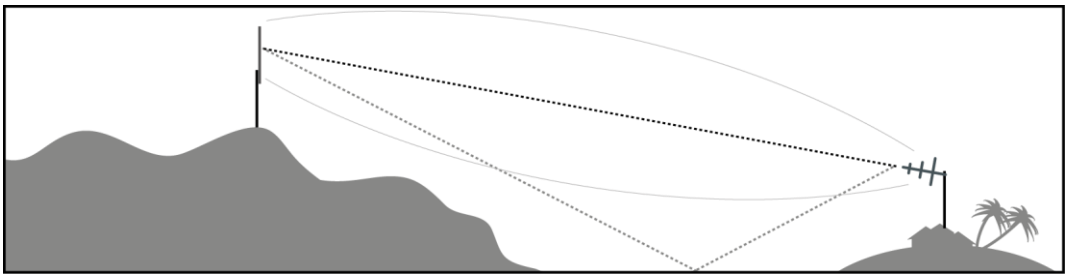
When siting antennas, consider the following points:

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 LCF78, LCF12 or CNT-400 feeder cable or equivalent:

Part Number	Part Description	Specification
RFS LCF78 50JA	Feeder Cable, 7/8', CELLFLEX, Low Loss, Std, /m, MOQ 50	Low loss 7/8' (22.2 mm) feeder cable Bending radius of 125 mm min Attenuation of 2.5 dB / 100m @ 450 MHz
RFS LCF12 50J	Feeder Cable, 1/2', CELLFLEX, Low Loss, Std, /m, MOQ 50	Low loss 0.5' (12.7 mm) feeder cable Bending radius of 125 mm min Attenuation of 4.7 dB / 100m @ 450 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 30 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 heatsink.

Earthing and Lightning Protection

WARNING:

Lightning can easily damage electronic equipment.

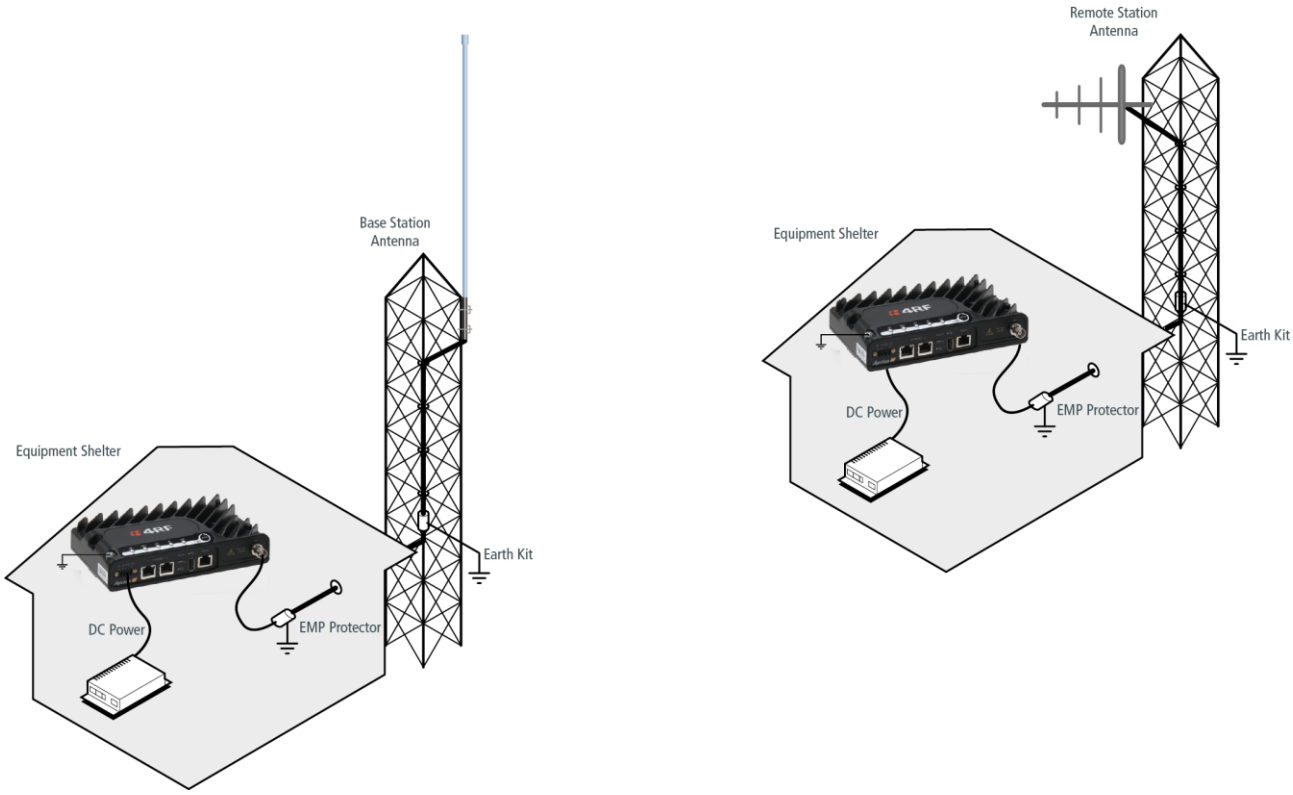
To avoid this risk, install primary lightning protection devices on any interfaces that are reticulated in the local cable network.

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 of the enclosure. A M4 8mm pan pozi machine screw and a M4 lock washer is supplied fitted to the radio. This can be used to earth the enclosure to a protection earth.

6. Installing the Radio

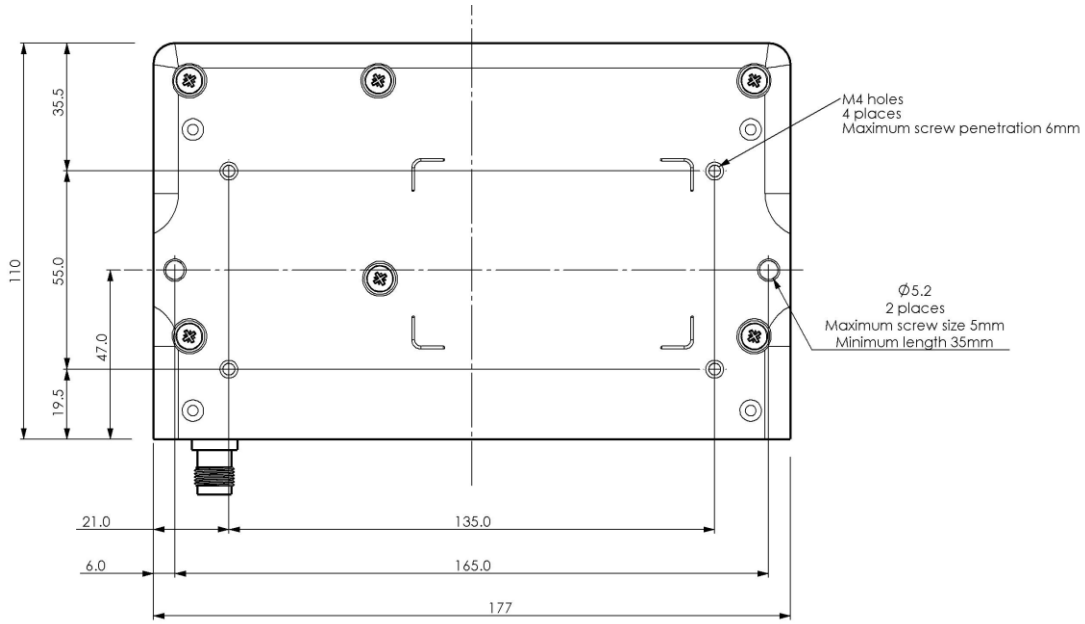
CAUTION:

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.

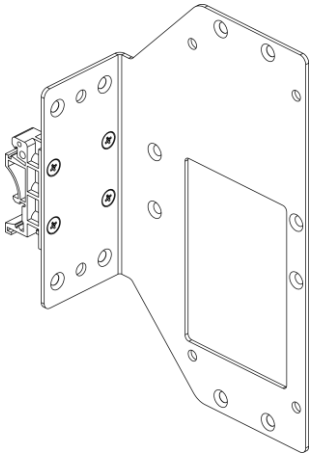
Required Tools

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:

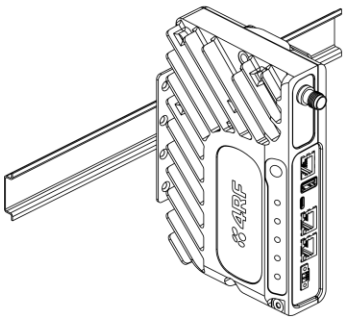
Part Number	Part Description
APSA-MBRK-DIN	4RF Aprisa SR Acc, Mounting, Bracket, DIN Rail



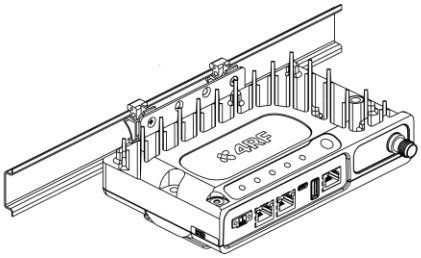
The Aprisa SR is mounted into the DIN rail mounting bracket using the four M4 threaded holes in the Aprisa SR enclosure base. Four 8 mm M4 pan pozi machine screws are supplied with the bracket.

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

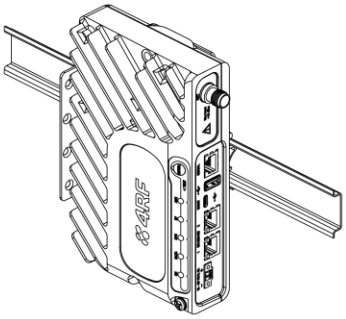
- Vertical Mount (vertical enclosure perpendicular to the mount)
- Horizontal Mount (horizontal enclosure perpendicular to the mount)
- Flat Vertical Mount (vertical enclosure parallel to the mount)
- Flat Horizontal Mount (horizontal enclosure parallel to the mount)



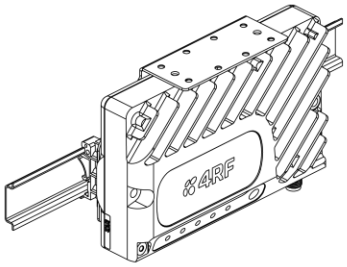
Vertical Mount



Horizontal Mount



Flat Vertical Mount

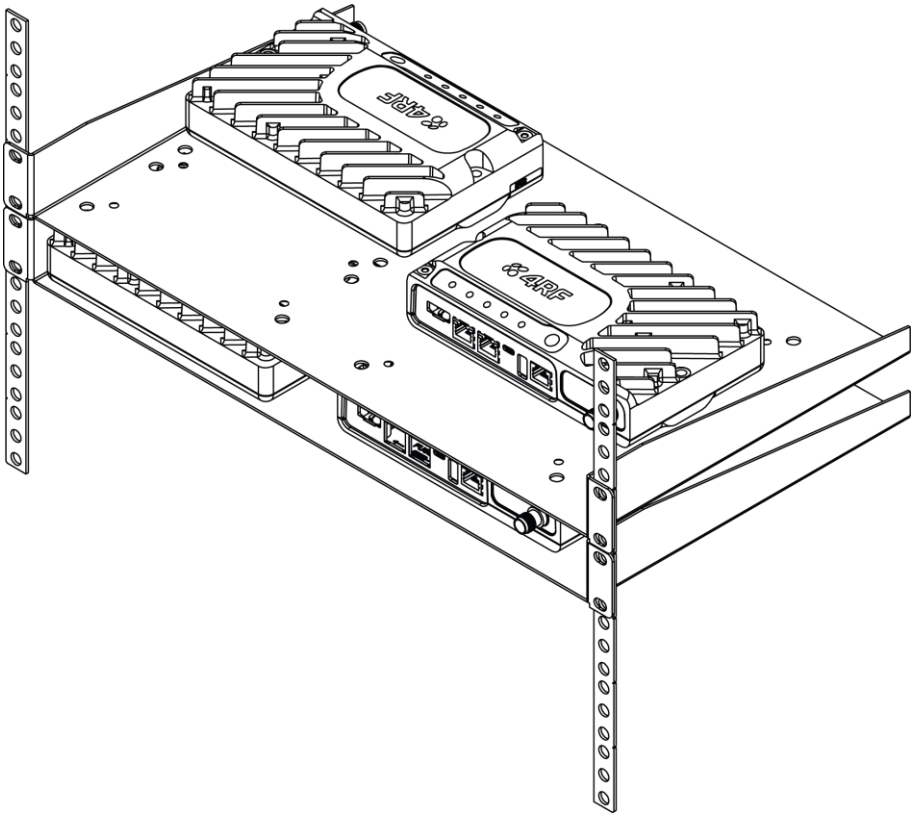


Flat Horizontal Mount

The DIN rail mounting bracket has two clips which are positioned to allow for the four mounting positions.

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 1 RU rack mounted shelves.

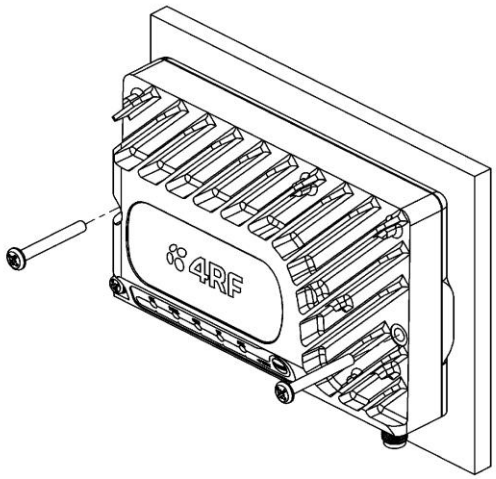


WARNING:

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.


4RF

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 39).

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 of the enclosure. A M4 8mm pan pozi machine screw and a M4 lock washer is supplied fitted to the radio. This 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 30 W.

The power connector required is a Phoenix Contact 4 pin female screw fitting part MC 1.5/ 4-STF-3.5. 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.

Additional Phoenix Contact 4 pin female power connectors can be ordered from 4RF:

Part Number	Part Description
APSA-CPH4-FEM-01	4RF Aprisa SR Acc, Connector, Phoenix 4 pin, Female, 1 item

Turn your power source on:

- All the radio LEDs will flash orange for one second and then the OK, DATA and CPU LEDs will light green, the RF LED will light orange and the AUX LED will be off
- The Aprisa SR radio is ready to operate
- The RF LED will light green 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 46 for instructions on how to locate and replace the fuses.

External Power Supplies

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

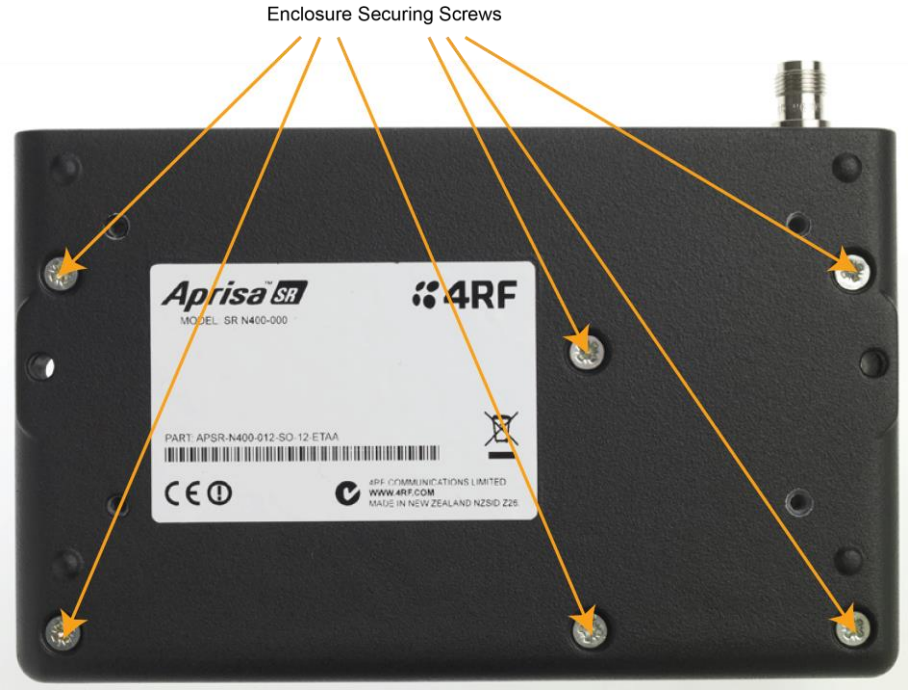
Part Number	Part Description
APSA-P230-030-24-TS	4RF Aprisa SR Acc, PSU, 230 VAC, 30W, 24 VDC, -10 to +60C
APSA-P230-048-24-TE	4RF Aprisa SR Acc, PSU, 230 VAC, 48W, 24 VDC, -20 to +75C
APSA-P230-060-24-TS	4RF Aprisa SR Acc, PSU, 230 VAC, 60W, 24 VDC, -10 to +60C
APSA-P48D-050-24-TA	4RF Aprisa SR Acc,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

Spare Fuses

The Aprisa SR PBA contains two fuses in the power input with designators F2 and F3. Both the positive and negative power connections are fused. The fuse type is a Littelfuse 0453005 with a rating of 5 A, 125 V, very fast acting.

To replace the fuses:

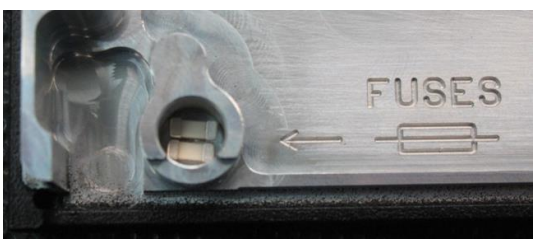
1. Remove the input power and antenna cable.
2. Unscrew the enclosure securing screws (posi 2).



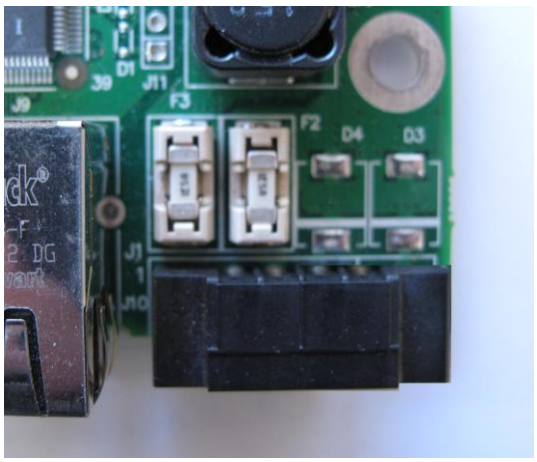
2. Separate the enclosure halves.

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
APSA-FNAN-453-05-02	4RF Aprisa SR Acc, Fuse, Nano SMF, 453 Series, 5A, 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

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 any radio in the network 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.

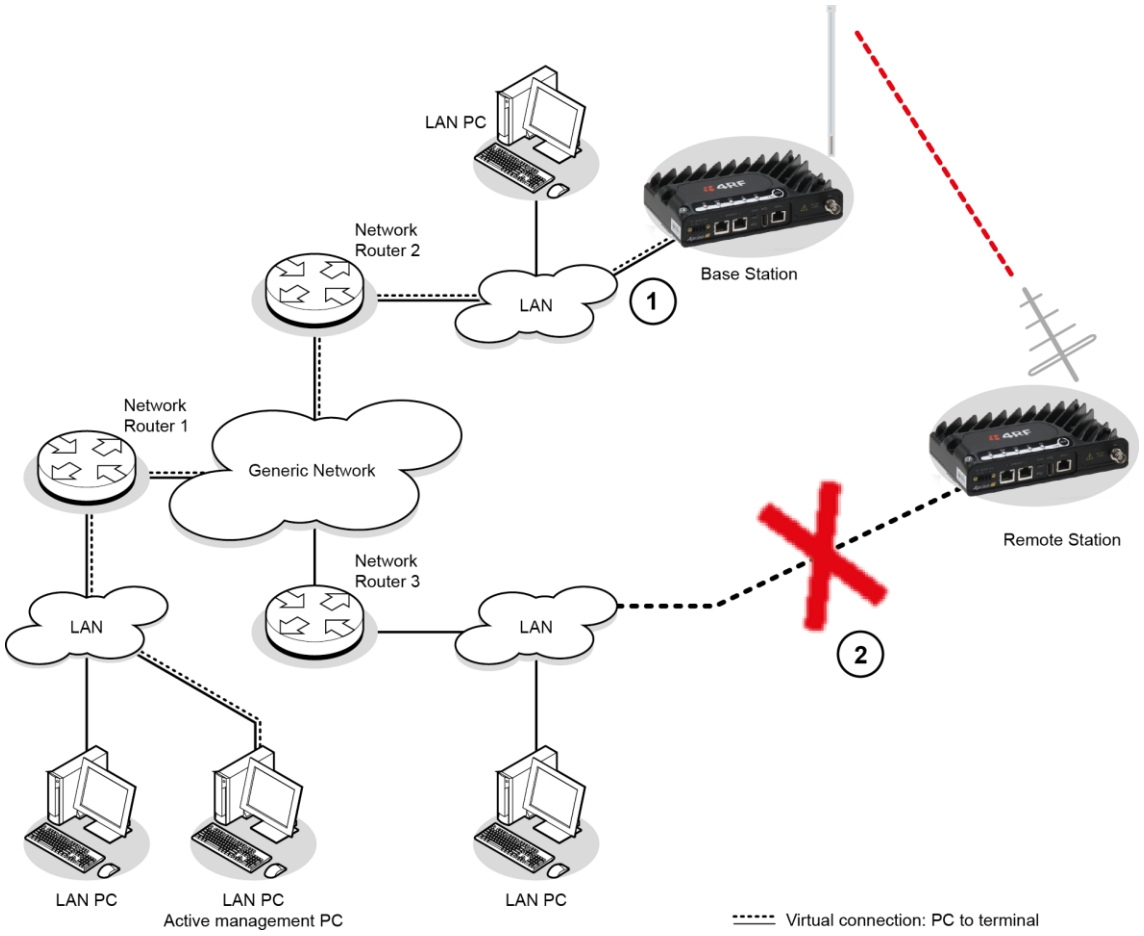
The Aprisa SR Protected Station radio A (left radio) has a factory default IP address of 169.254.50.10 and radio B (right radio) has a factory default IP address of 169.254.50.20, both with a subnet mask of 255.255.0.0.

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 http://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

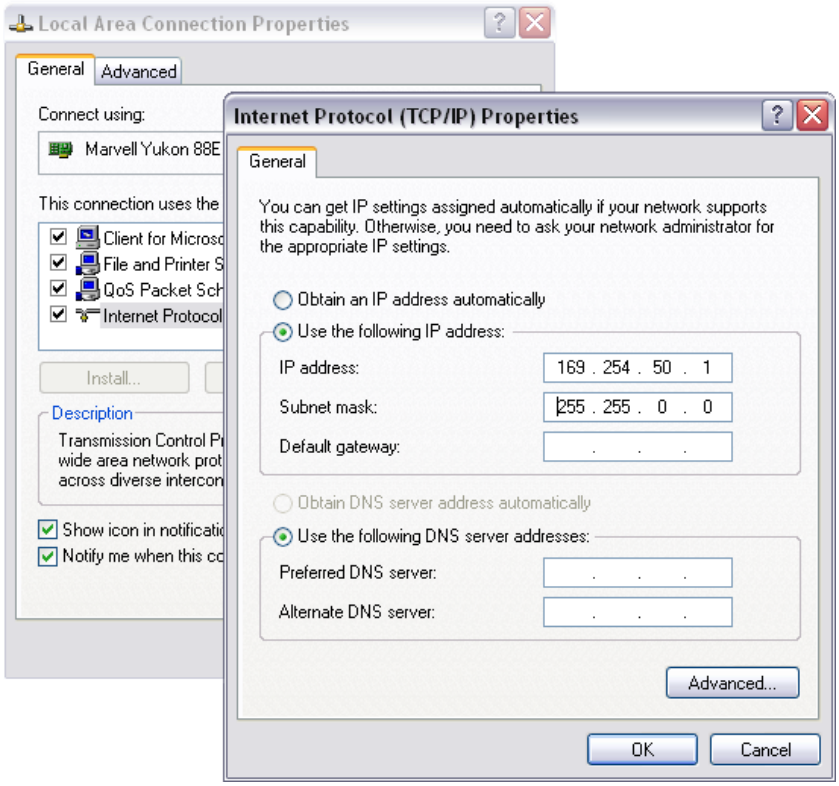
To change the PC IP address:

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).

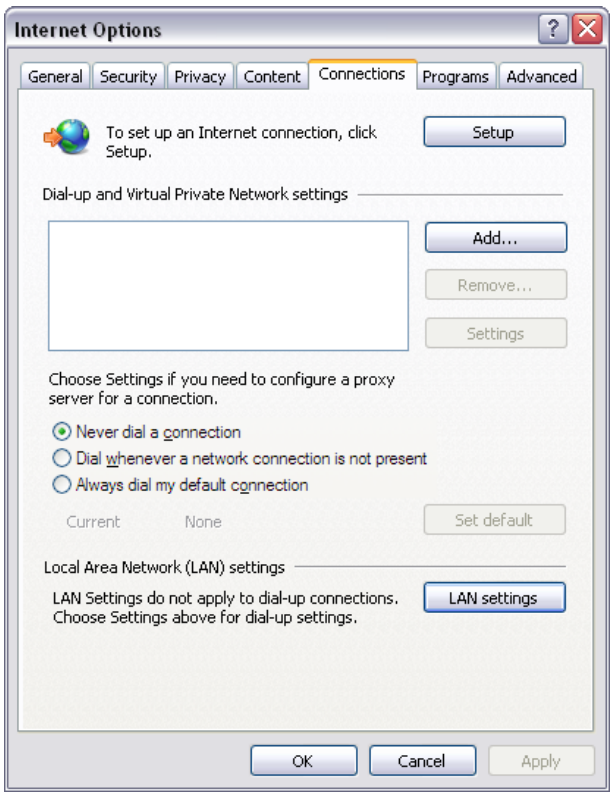


To change the PC connection type:

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.

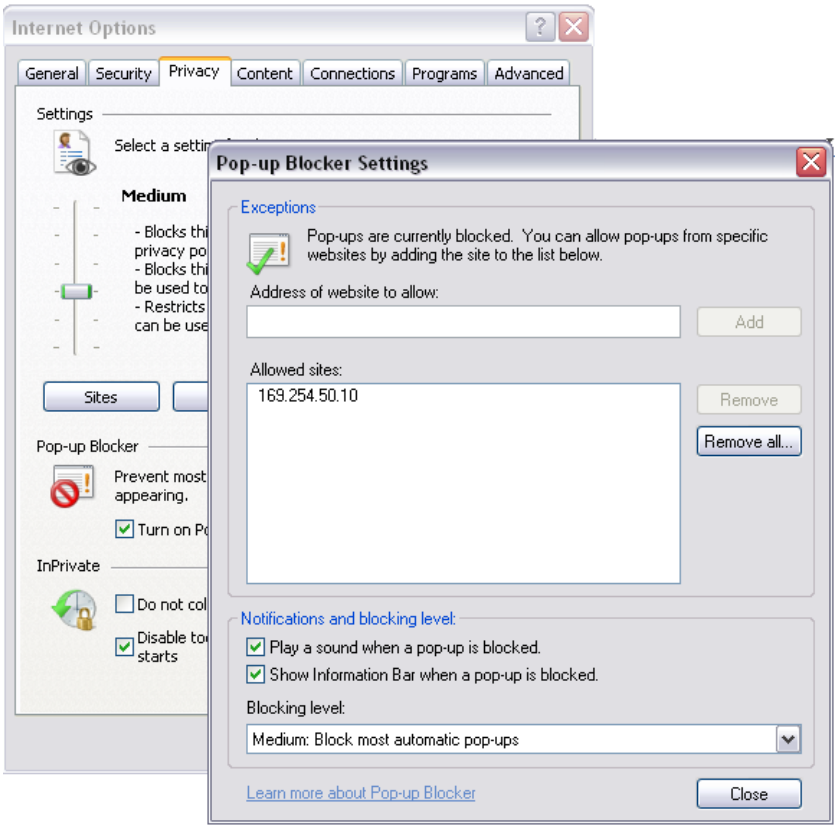


To change the PC pop-up status:

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.

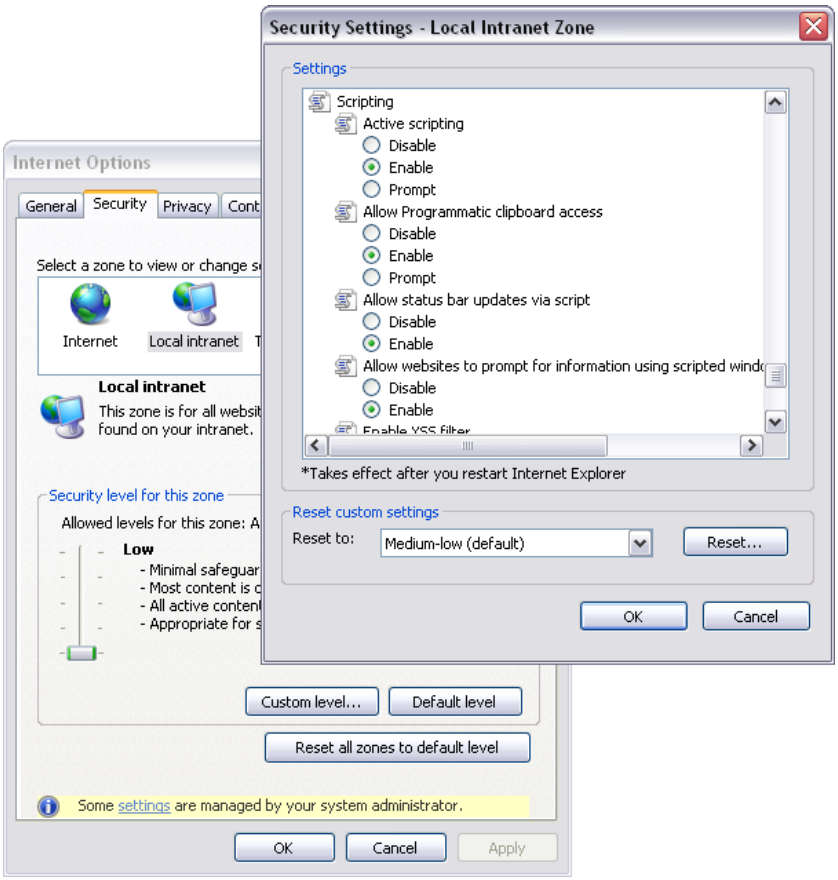


To enable JavaScript in the web browser:

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.

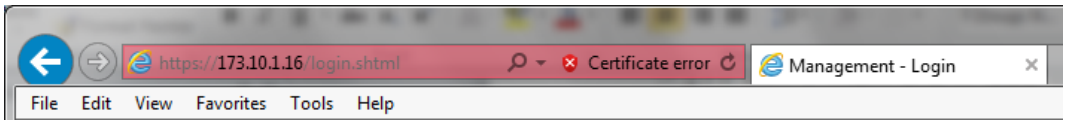
If SuperVisor is inactive for a period defined by the Inactivity Timeout option (see 'Maintenance > General' on page 120), the radio will automatically logout the user.

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 199).



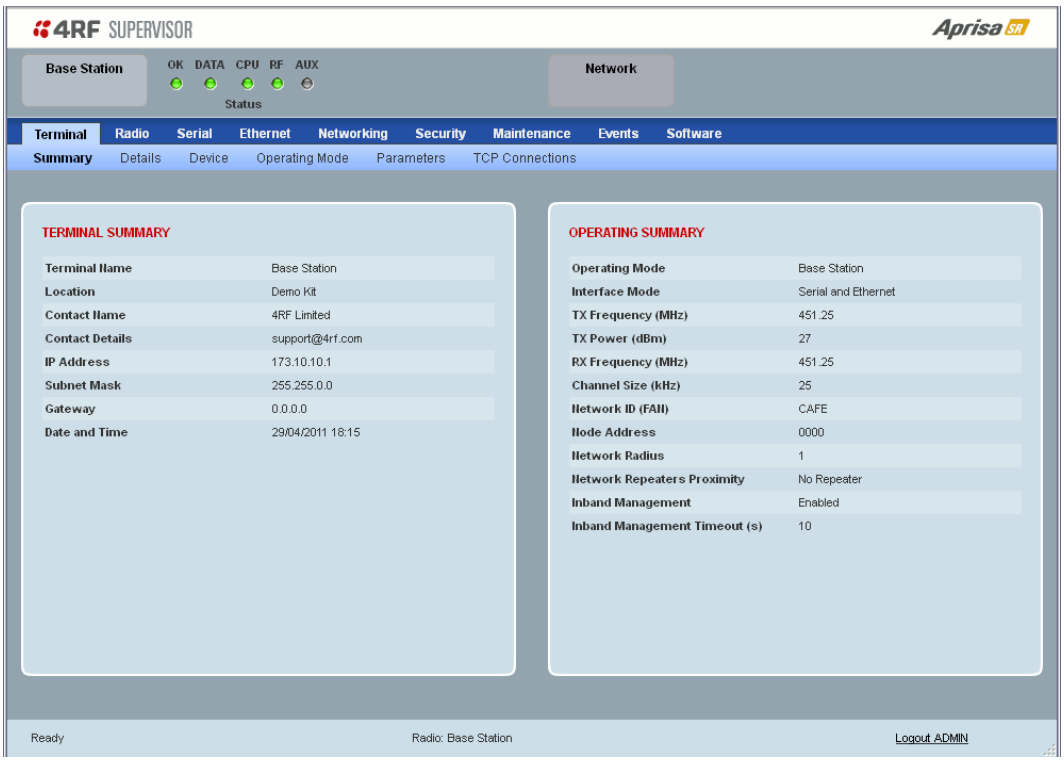
Note: The Aprisa SR has a Self Signed security certificate which may cause the browser to prompt a certificate warning. It is safe to ignore the warning and continue. The valid certificate is 'Issued By: 4RF-APRISA' which can be viewed in the browser.

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 108).

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



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.

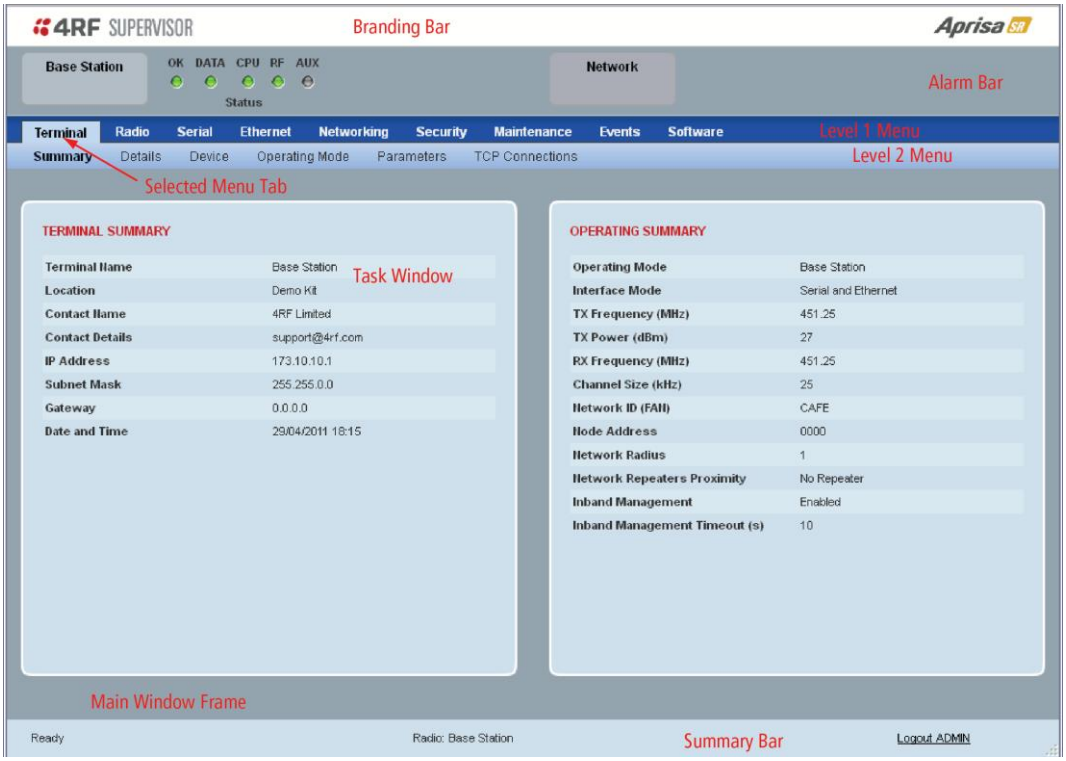
To logout of SuperVisor:

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.

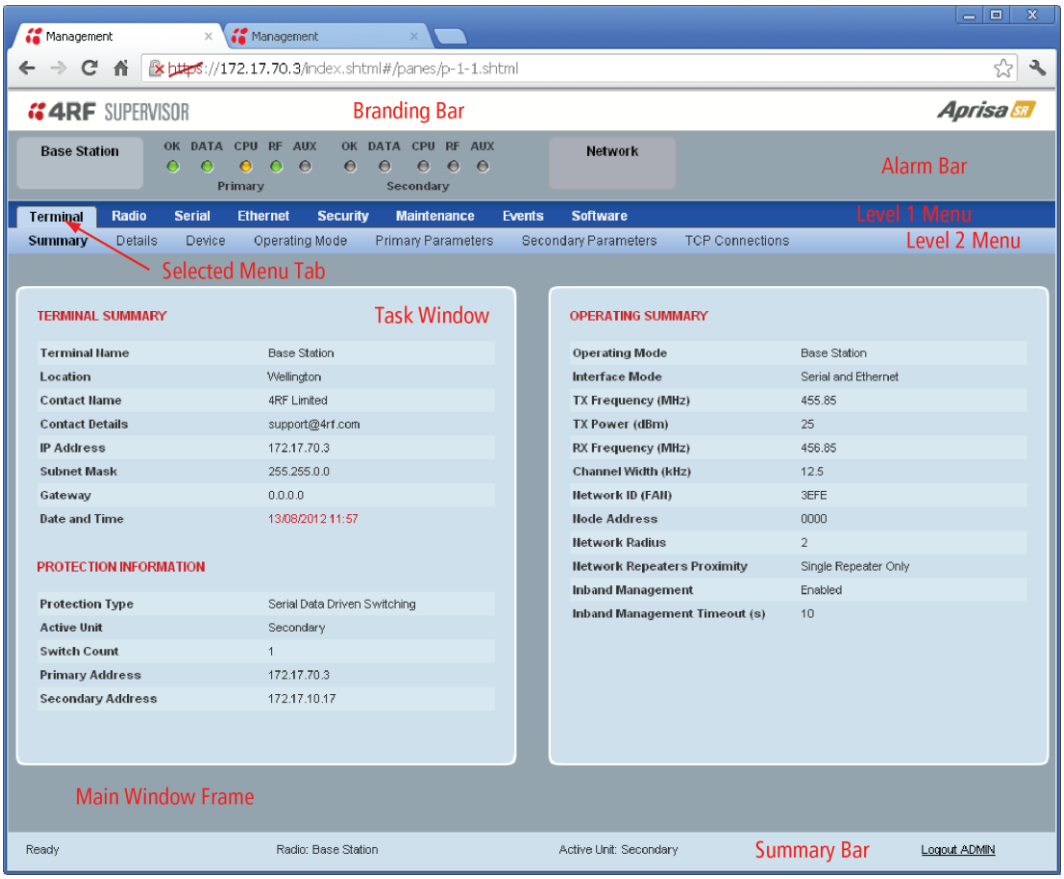
SuperVisor Summary Bar

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.

Protected Station

The following shows the components of the SuperVisor page layout for a protected station:



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 primary and secondary radios.

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 and the active radio.
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	
Networking	
Security	
Maintenance	
Events	
Software	

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 dependant 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 > Operating Mode	No Access	Read-Write	Read-Write	Read-Write
Terminal > Parameters	Read-Only	Read-Only	Read-Only	Read-Only
Terminal > Primary Parameters	Read-Only	Read-Only	Read-Only	Read-Only
Terminal > Secondary Parameters	Read-Only	Read-Only	Read-Only	Read-Only
Terminal > TCP Connections	Read-Only	Read-Only	Read-Only	Read-Only
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
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
Networking > IP Summary	Read-Only	Read-Only	Read-Only	Read-Only
Networking > IP Setup	No Access	Read-Write	Read-Write	Read-Write
Networking > L3 Filtering	No Access	No Access	Read-Write	Read-Write
Security > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Security > Users	No Access	No Access	No Access	Read-Write
Security > Settings	No Access	No Access	Read-Write	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
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 > Defaults	No Access	No Access	Read-Write	Read-Write
Software > Summary	Read-Only	Read-Only	Read-Only	Read-Only
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 > Setup	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

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:

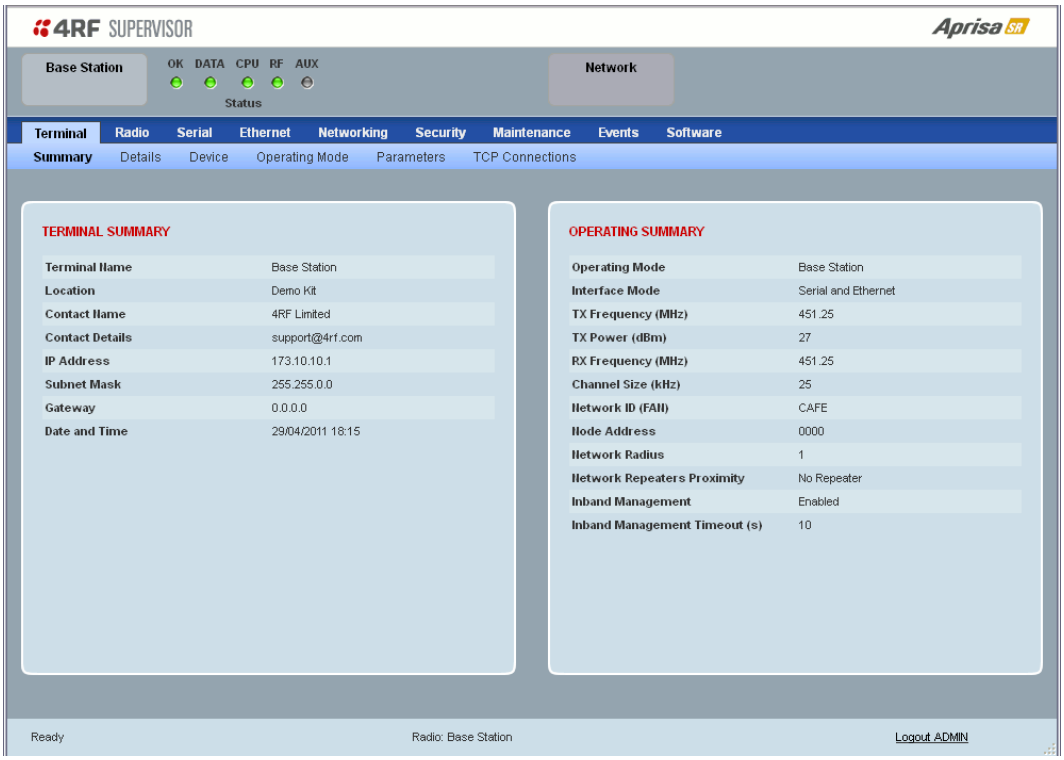
- Standard Radio
- Protected Station

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.

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.

Interface Mode

This parameter displays the Interfaces available for traffic on the radio (see ‘Maintenance > Licence’ on page 126).

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).

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.

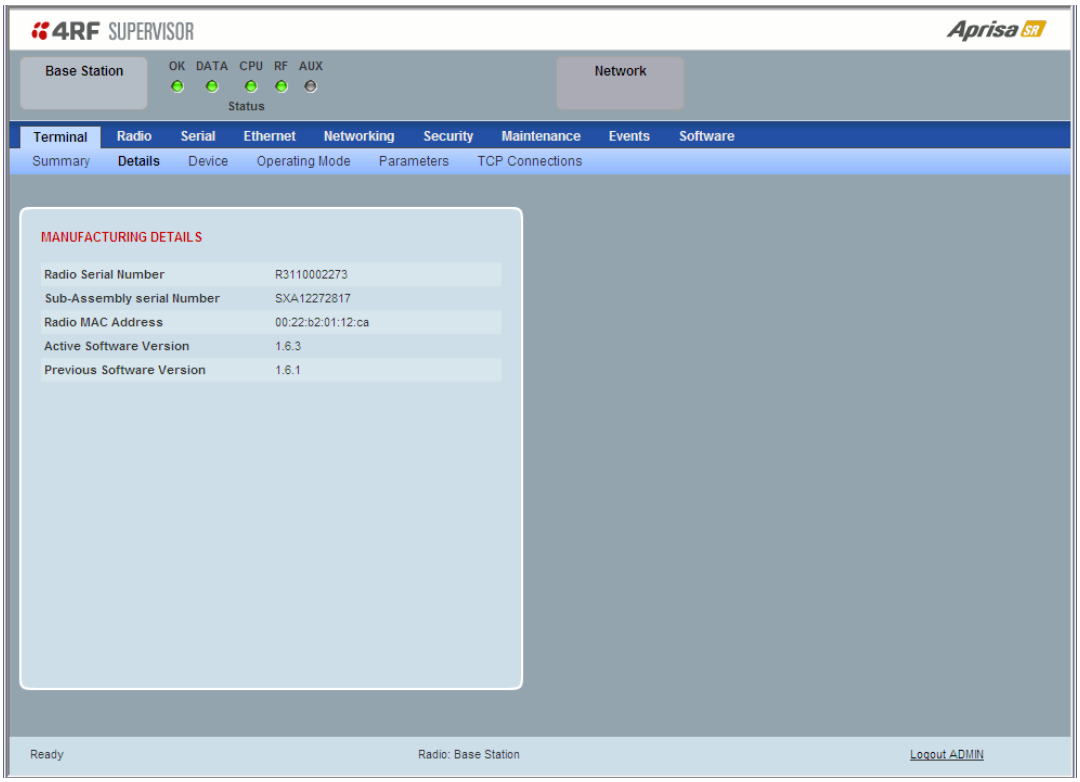
Inband Management

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).

Radio MAC Address

This parameter displays the MAC address of the radio.

Active Software Version

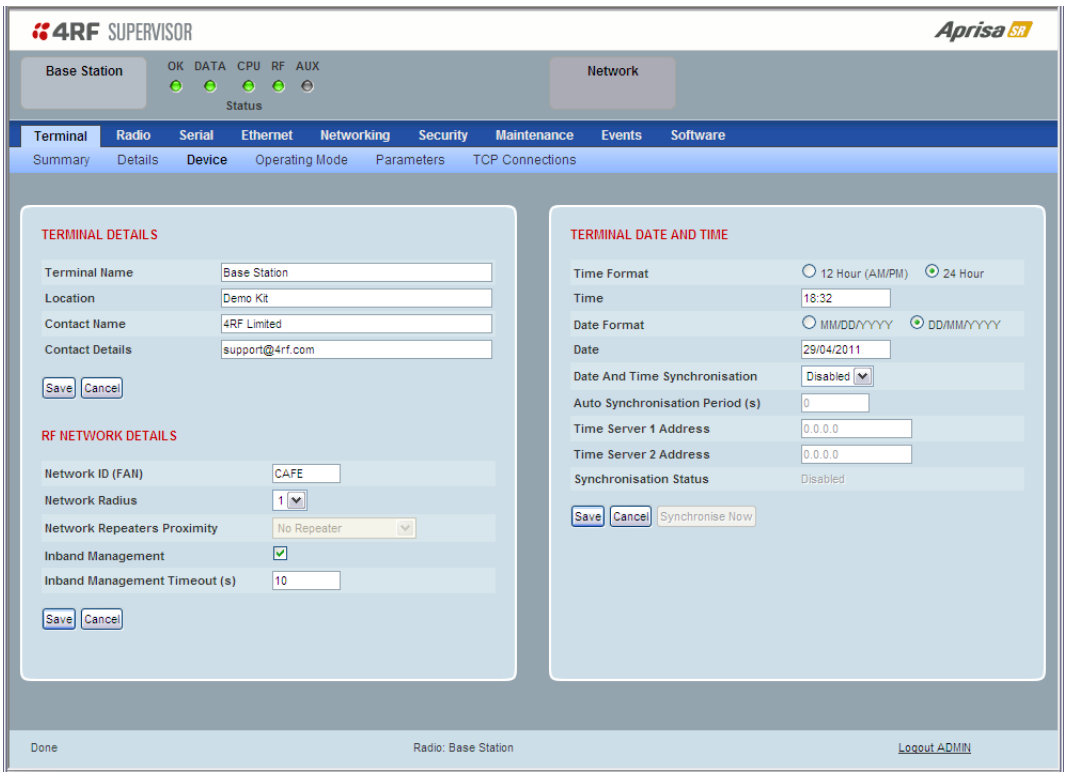
This parameter displays the version of the software currently operating the radio.

Previous Software Version

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

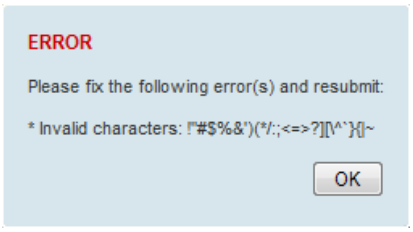
A new radio from the factory will display ‘None’ for the Previous SW Version.

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 ‘support@4RF.com’.
4. Enter the Contact Details.

RF NETWORK DETAILS

Network ID (network)

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.

Network Radius

This parameter sets the maximum number of hops in this network e.g. 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.

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

Network Repeaters Proximity

This parameter is set in base stations and repeater stations to indicate the proximity of repeaters in the network. It has no affect if the Network Radius is set to 1.

The default setting is Separated Coverage.

Option	Function
No Repeater	Use when there are no repeaters in the network.
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.

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.

TERMINAL DATE AND TIME

Set the Time Format, Time, Date Format 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.

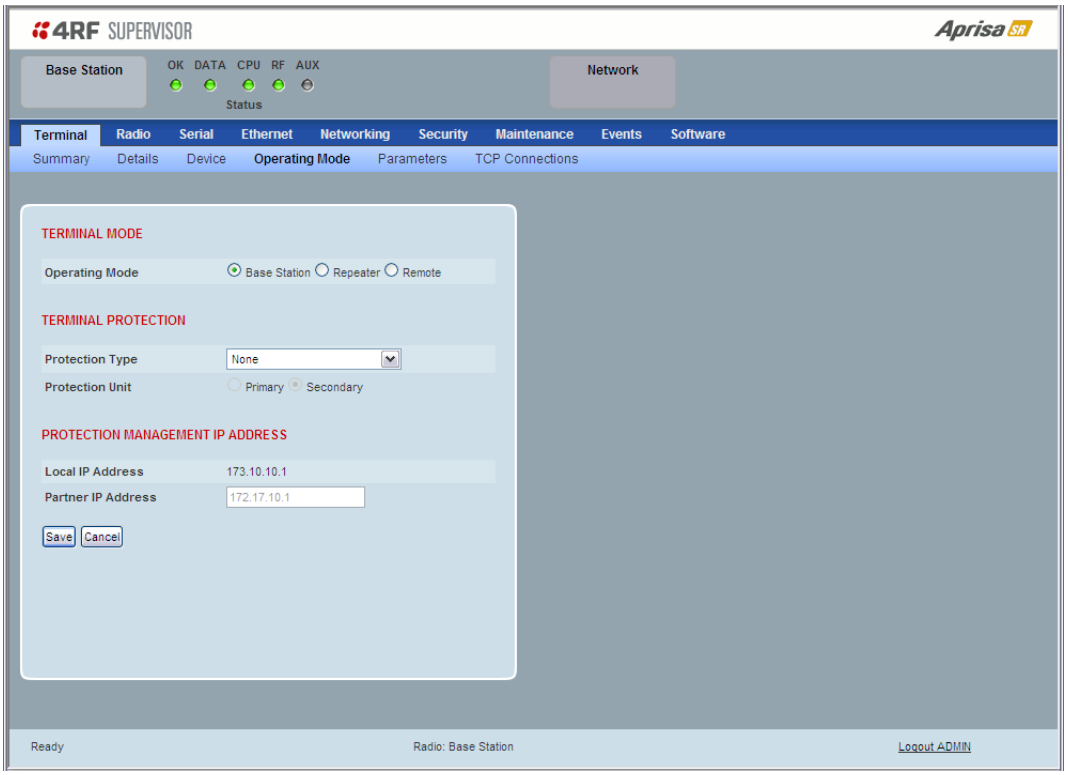
Synchronization Status

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



TERMINAL MODE

Operating Mode

The Operating Mode can be set to base station, repeater station or remote station. The default setting is remote station.

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
Serial Data Driven Switching	Set to make this SR radio part of an Aprisa SR Data Driven Protected Station. Provides radio and RS-232 serial port user interface protection for Aprisa SR radios.

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

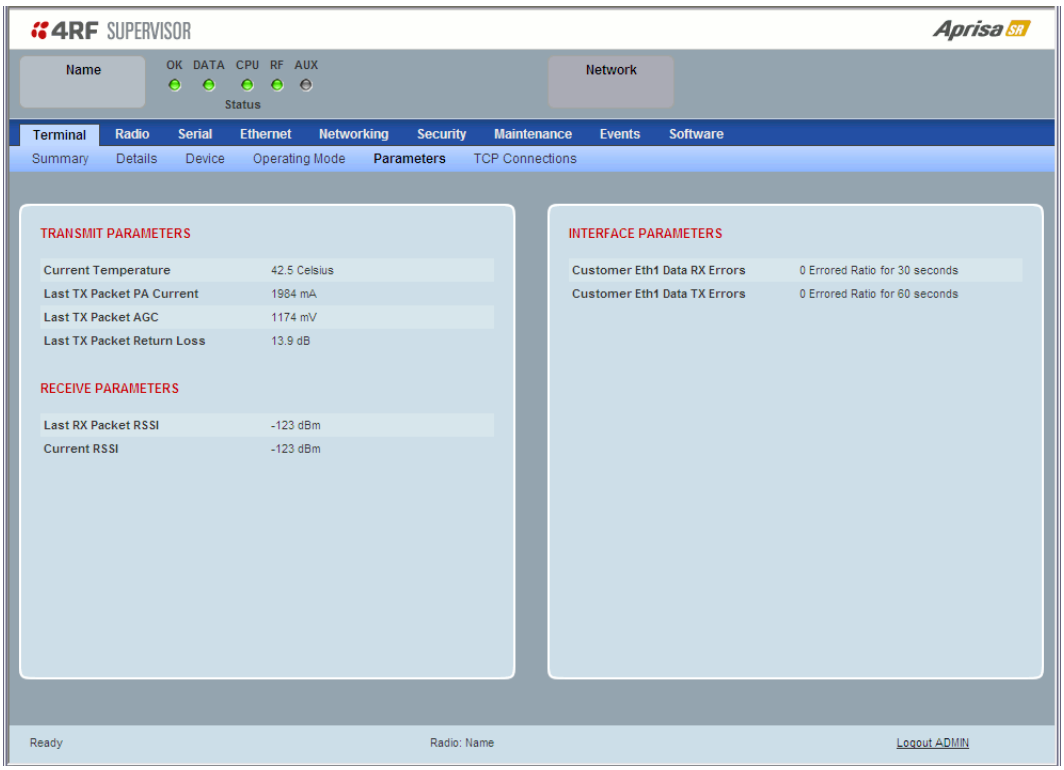
The Local IP Address shows the IP address of this radio.

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.

Terminal > Parameters

The Parameters page is a dynamic page that will display the parameters associated with the active alarms, set on 'Events > Events Setup' on page 132. The screenshot below shows a small amount of monitored alarms as an example.



The following is a list of alarm events that are monitored:

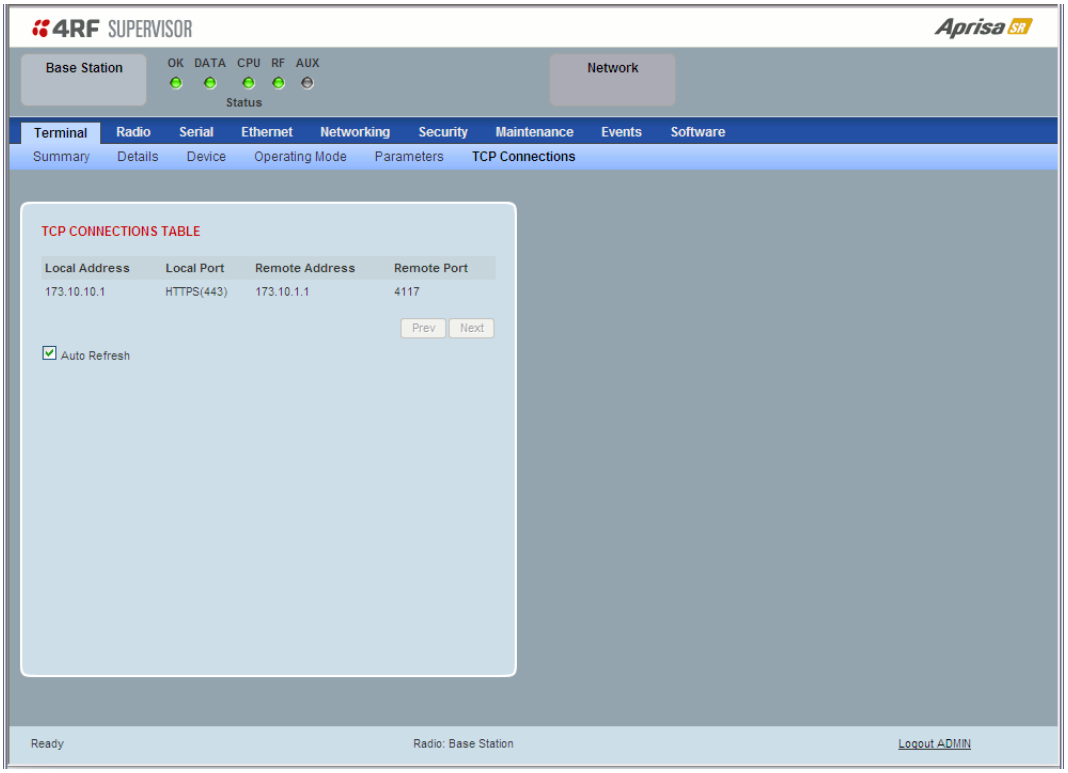
Monitored Parameter	Unit	Event ID	Event Display Text
Current Temperature	Celsius	4	Temperature Threshold
Last RX Packet RSSI	dBm	7	RSSI Threshold
Last Sample RX CRC Error	Ratio	9	RX CRC Errors
Last Sample RF RX Data	Count	34	RF No Receive Data
Last Sample Eth1 RX Data	Count	10	Port 1 Eth No Receive Data
Customer Eth1 Data RX Errors	Ratio	11	Port 1 Eth Receive Errors
Customer Eth1 Data TX Errors	Ratio	12	Port 1 Eth Transmit Errors
Last Sample Eth2 RX Data	Count	35	Port 2 Eth No Receive Data
Customer Eth2 Data RX Errors	Ratio	36	Port 2 Eth Receive Errors
Customer Eth2 Data TX Errors	Ratio	37	Port 2 Eth Transmit Errors
Last Sample Serial1 RX Data	Count	13	Port1 Serial Data No RX Data
Customer Serial1 Data RX Errors	Ratio	14	Port1 Serial Data RX Errors
Customer USB Ser Data RX Errors	Ratio	14	Port1 Serial Data RX Errors
Last Sample USB Ser RX Data	Ratio	14	USB Port Serial Data No RX Data

Monitored Parameter	Unit	Event ID	Event Display Text
Last TX Packet PA Current	mA	None	
Last TX Packet AGC	mV	None	
Last TX Packet Reverse Power	dB	None	
Last TX Packet Return Loss (VHF radios only)	dB	None	
Current RSSI	dBm	None	

If an associated alarm event occurs, the Parameters table will display the current value for that parameter. The refresh time is 12 seconds.

Terminal > TCP Connections

The TCP Connections page displays the list of active TCP connections on the radio.



TCP CONNECTIONS TABLE

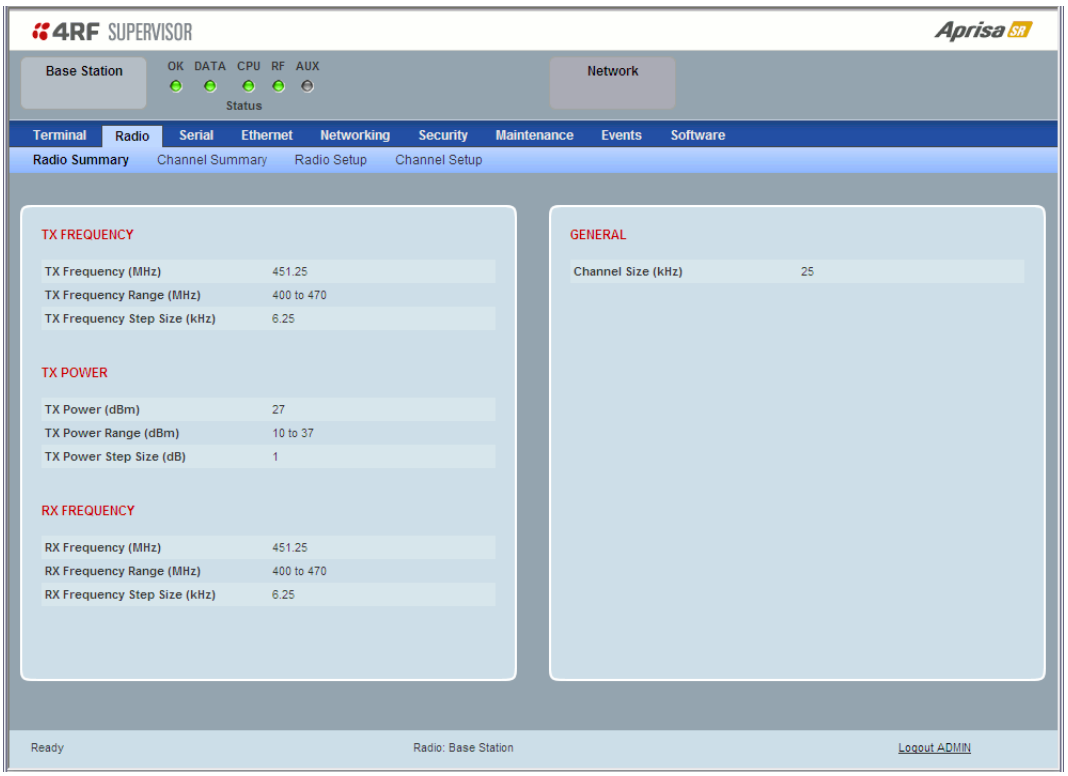
The Next button will display the next page of 8 connections and the Prev button will display the previous page of 8 connections.

If the Auto Refresh option is ticked, the TCP Connections table will refresh every 12 seconds.

Radio

Radio > Radio Summary

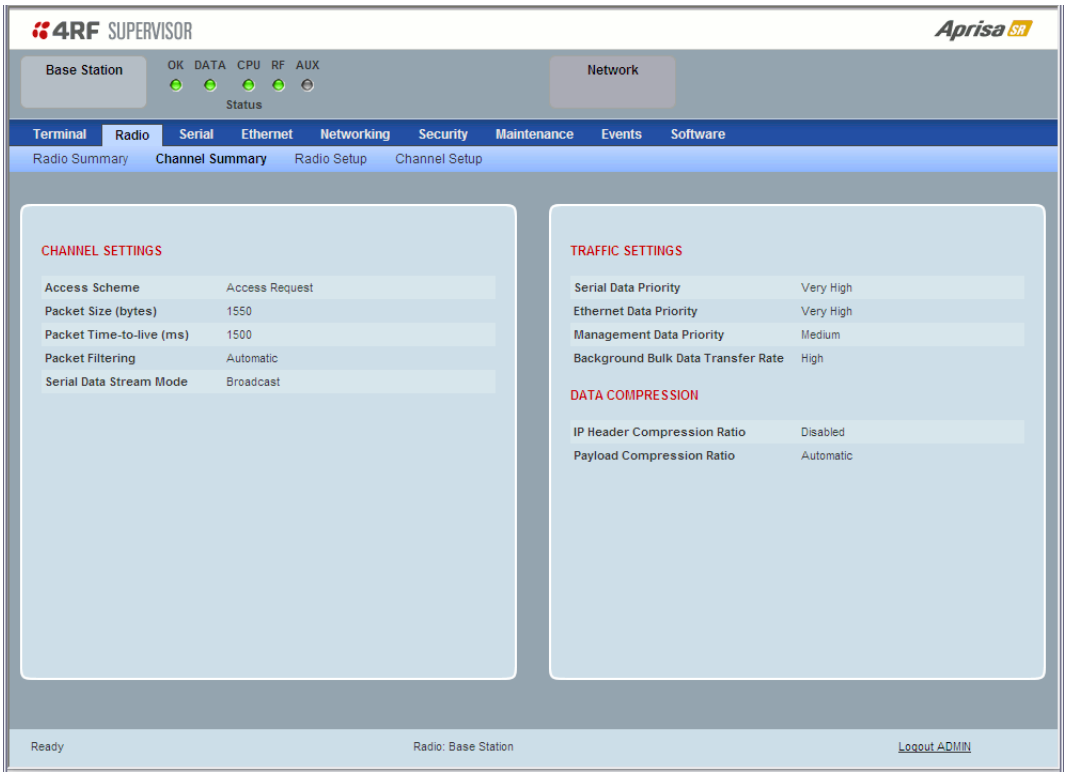
This page displays the current settings for the Radio parameters.



See ‘Radio > Radio Setup’ for setting details.

Radio > Channel Summary

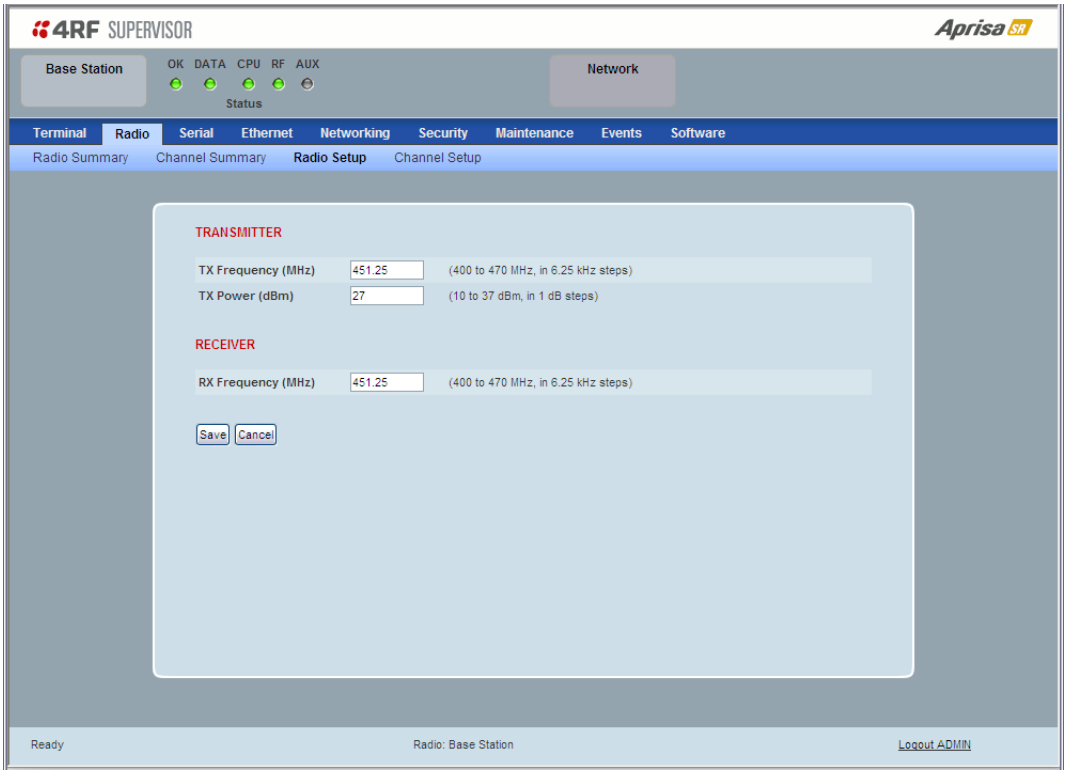
This page displays the current settings for the Channel parameters.



See ‘Radio > Channel Setup’ for setting details.

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 234).

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.

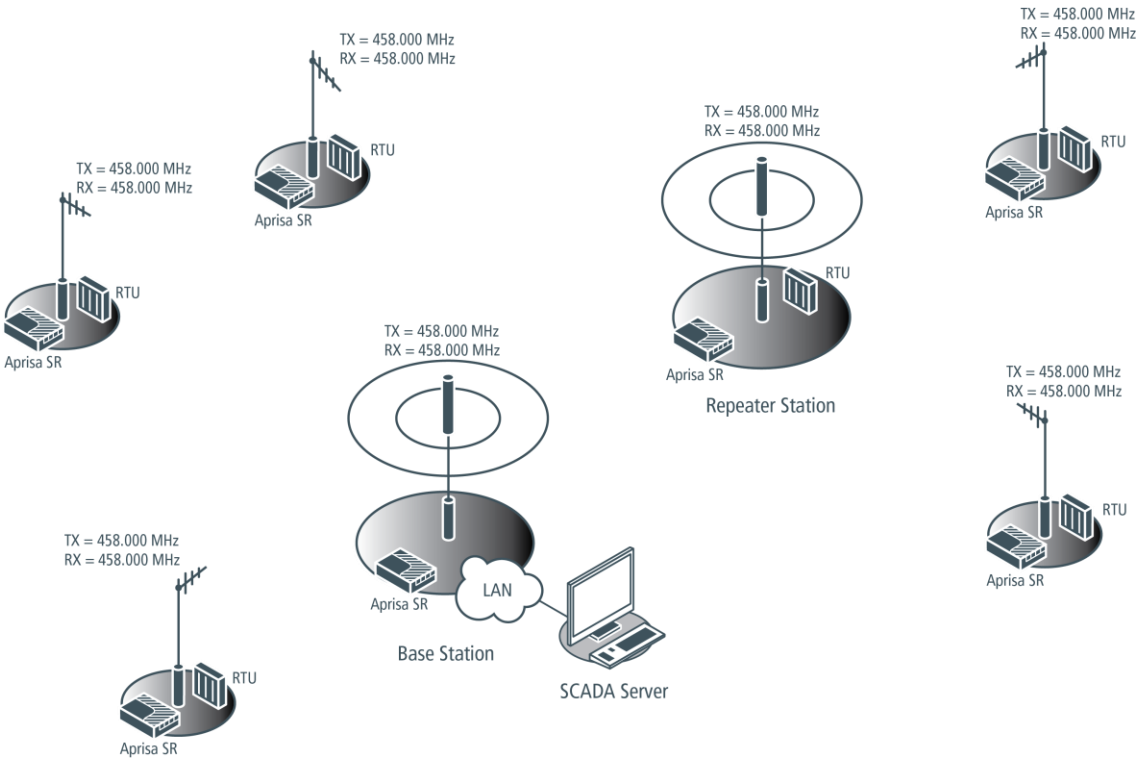
The default setting is 330 MHz for a UHF radio and 136 MHz for VHF radio.

The TX and RX frequencies can be single frequency ½ duplex or dual frequency ½ duplex. Dual frequency ½ 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.



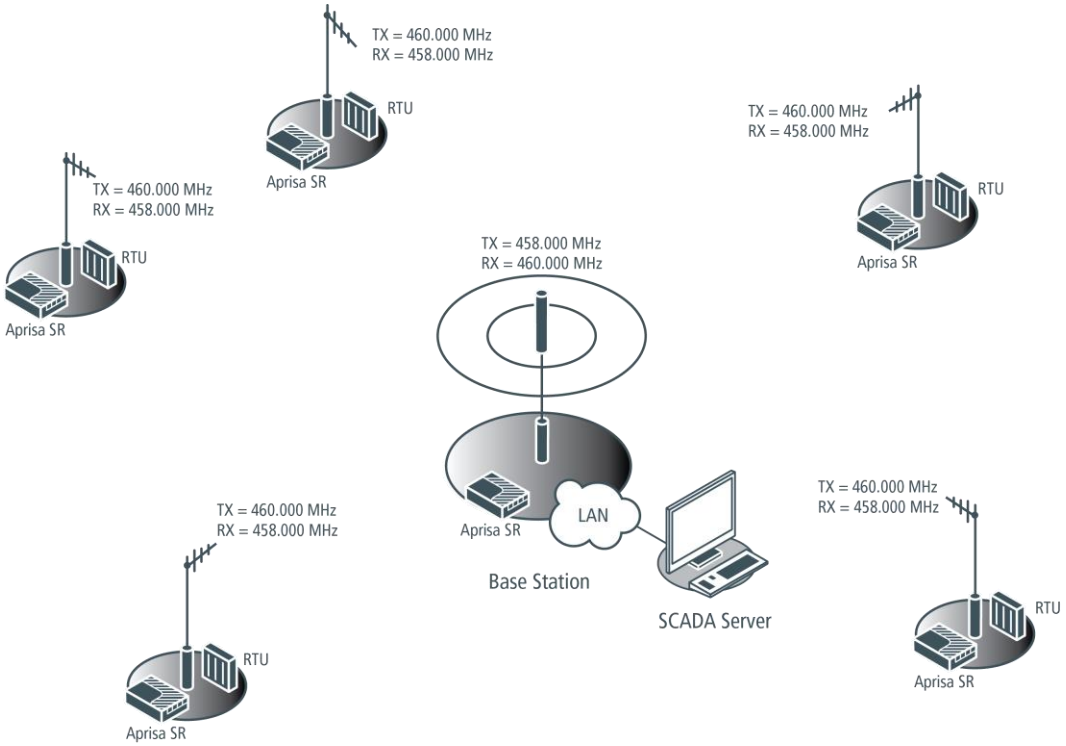
To change the TX and RX frequencies:

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.

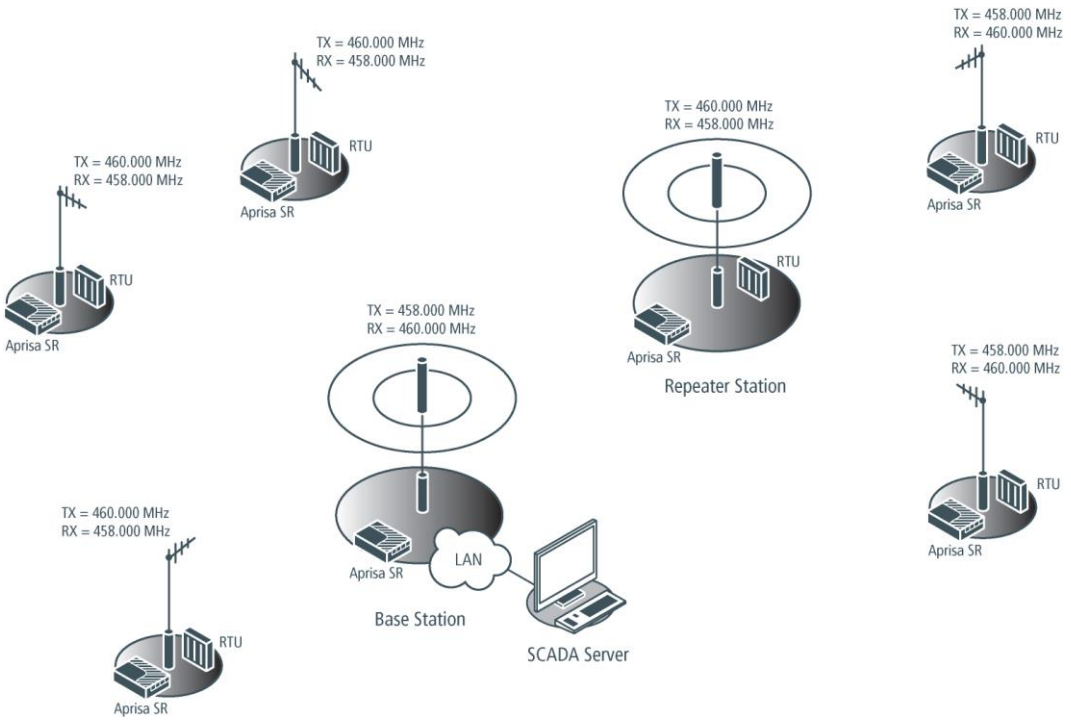
The TX frequency of the repeater station associated with the base station matches the RX frequency of the base station.

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.
3. 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 will restore.
4. For all the remote stations operating from the base station, change the TX frequency to frequency A and the RX frequency to frequency B.

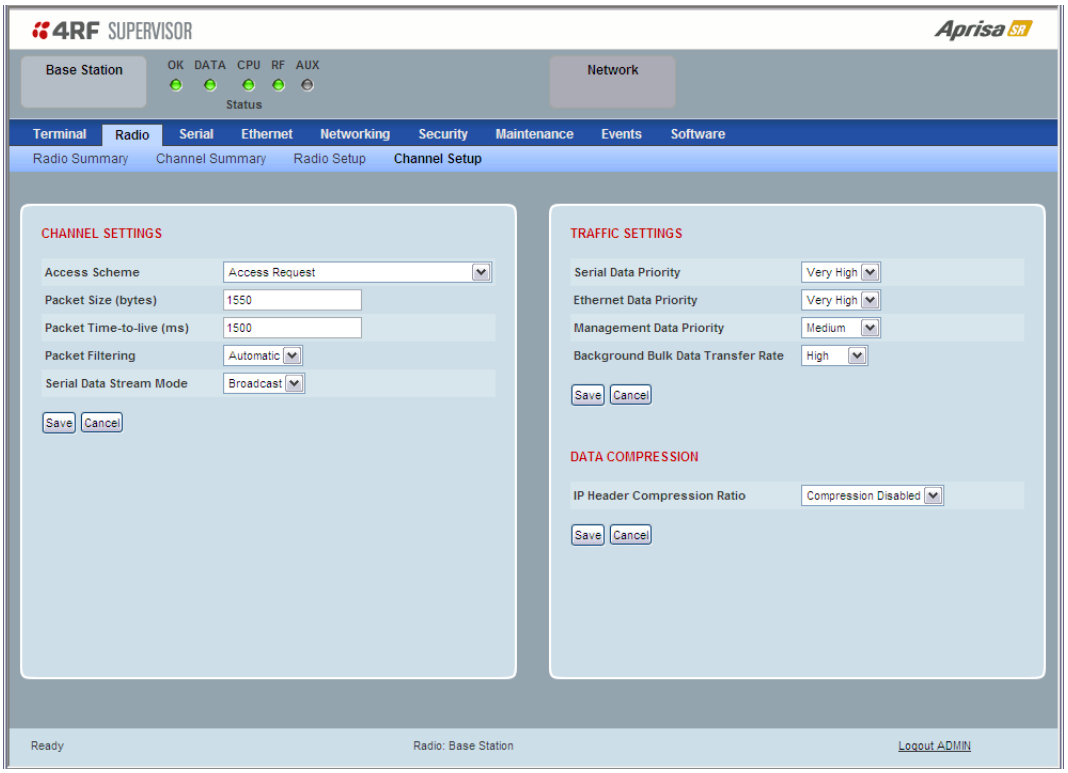
TX Power

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 (see 'Power Consumption' on page 240) and 'Save' the change.

The default setting is +37 dBm.

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

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 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. This mode is a general purpose access method for high and low load networks.
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.

The default setting is Access Request.

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 Field Access Network (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 Time to Live (ms)

This Time To Live (TTL) parameter sets the 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 a 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 which ever is the longer TTL of serial or Ethernet.

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 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 when connected to a repeater, particularly useful in the event of losing communication with a SCADA Master, assuming the Aprisa SR network is still operational.

Note: IP Header Compression must be disabled for this feature to operate correctly (see 'IP Header Compression Ratio' on page 87).

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.

The default setting is Broadcast.

TRAFFIC SETTINGS

Serial Data Priority

The Serial Data Priority controls the 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 (see 'Ethernet Data Priority' on page 86).

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

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 Data Priority

The Ethernet Data Priority controls the 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 (see 'Serial Data Priority' on page 86)

The Ethernet Data Priority can be set to Very High, High, Medium and Low. The default setting is Very High.

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, 1500 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 Management Priority

The Ethernet Management Priority controls the priority of the Ethernet management traffic relative to Ethernet customer traffic.

The Ethernet Management Priority can be set to Very High, High, Medium and Low. The default setting is Medium.

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.

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 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.

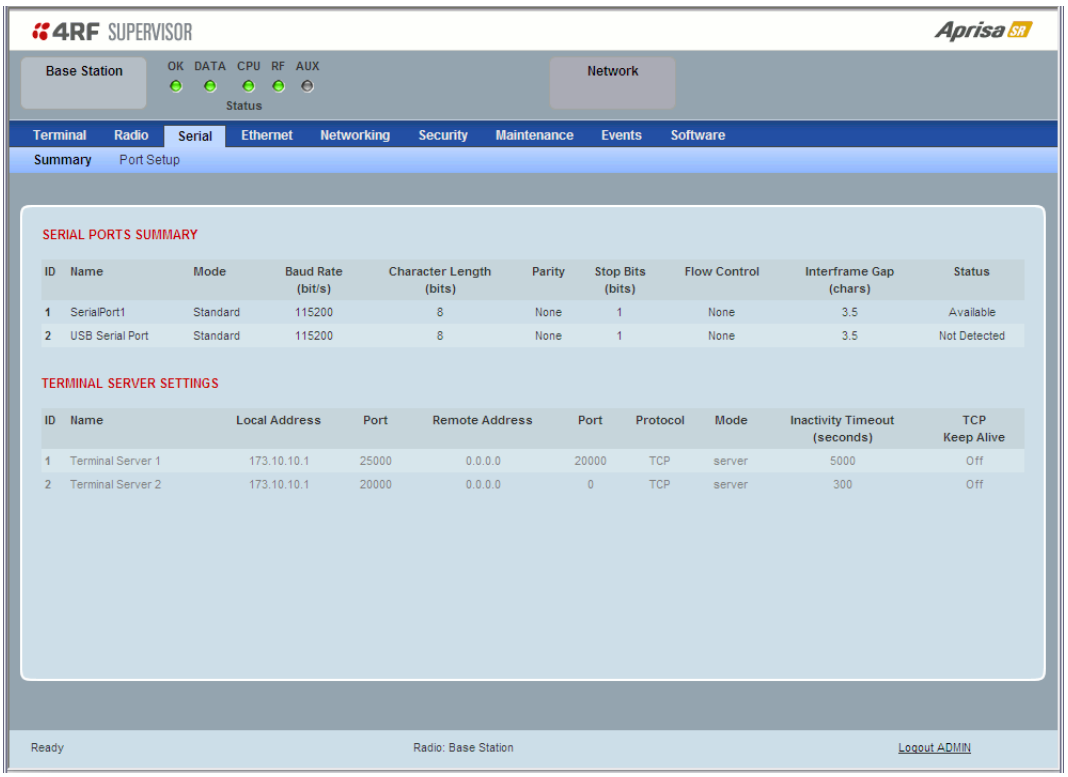
The default setting is High.

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.

Serial

Serial > Summary

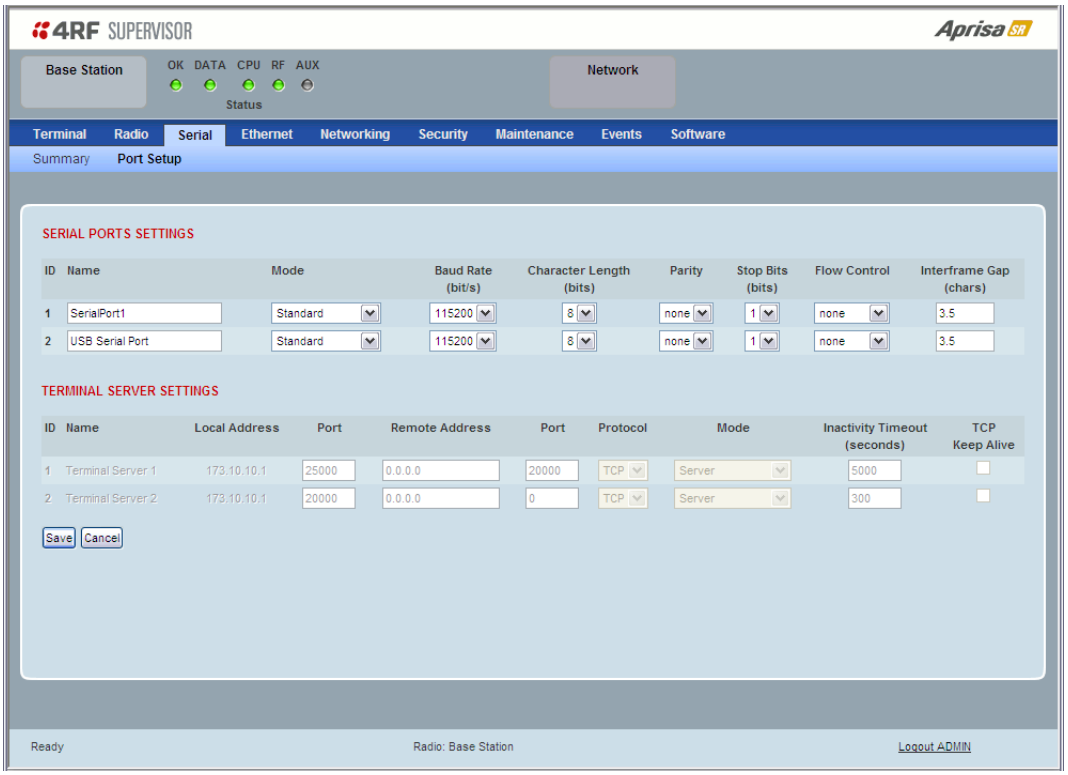
This page displays the current settings for the serial port parameters.



See ‘Serial > Port Setup’ on page 89 for configuration options.

Serial > Port Setup

This page provides the setup for the serial port settings.



SERIAL PORTS SETTINGS

Note: The current Aprisa SR has one serial port so there will be only one record.

Name

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

Option	Function
SerialPort1	This is the normal RS-232 serial port provided with the RJ45 connector.
USB Serial Port	This is the additional RS-232 serial port provided with the USB Host Port connector with a USB to RS-232 RJ45 converter cable (see 'USB RS-232 Serial Port' on page 221).

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.
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 SETTINGS on page 91).

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)

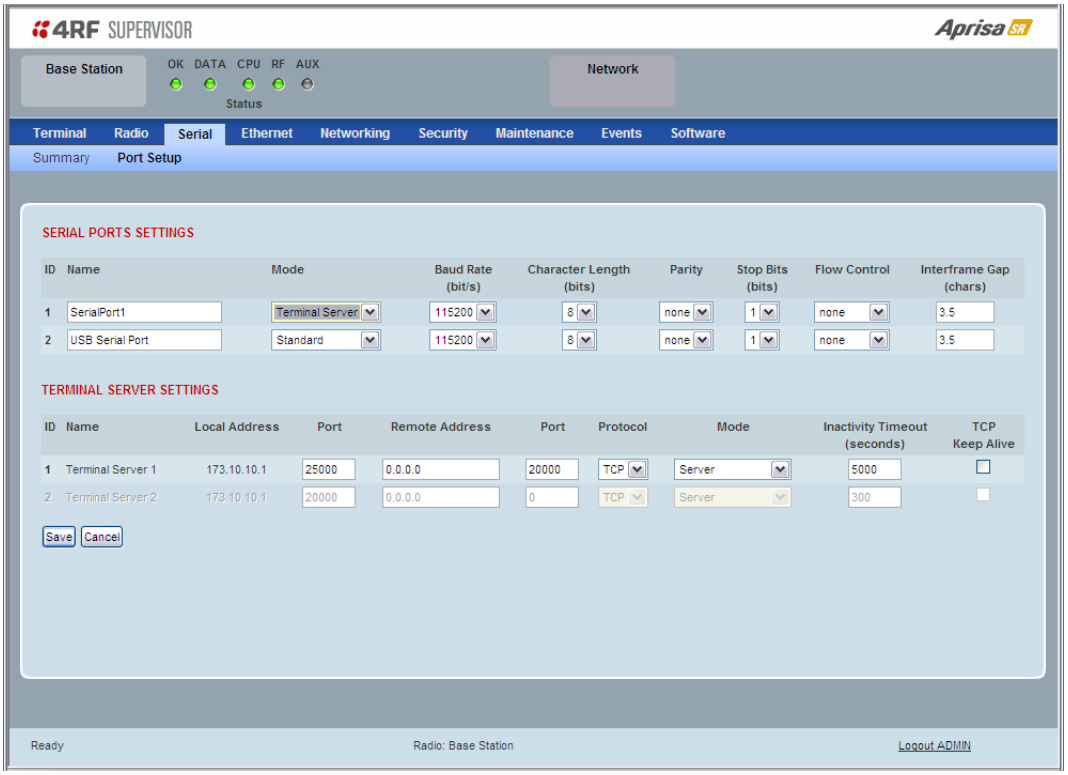
This parameter defines the gap between successive serial data frames. It is used to delimit the serial data to define the end of a packet. The Inter-Frame Gap limits are 0.5 to 16 chars. The default setting is 3.5 chars.

TERMINAL SERVER SETTINGS

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 (TCP or UDP).

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



Note: The current Aprisa SR has one serial port so there will be only one record.

Local Address

This parameter displays the IP address of this radio.

Port

This parameter sets the 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.

Port

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

Protocol

This parameter sets the 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.
Server	The radio will listen for a TCP connection on the specified local port. Data received from any client shall be forwarded to the associated serial port while data received from that serial port shall be forwarded to every client with an open TCP connection. If no existing TCP connections exist, all data received from the associated serial port shall be discarded.
Client and Server	The radio will listen for a TCP connection on the specified local port and if necessary, establish a TCP connection with the specified remote unit. Data received from any client shall be forwarded to the associated serial port while data received from that serial port shall be forwarded to every client with an open TCP connection.

Inactivity Timeout (seconds)

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

TCP Keep Alive

A TCP keepalive 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.

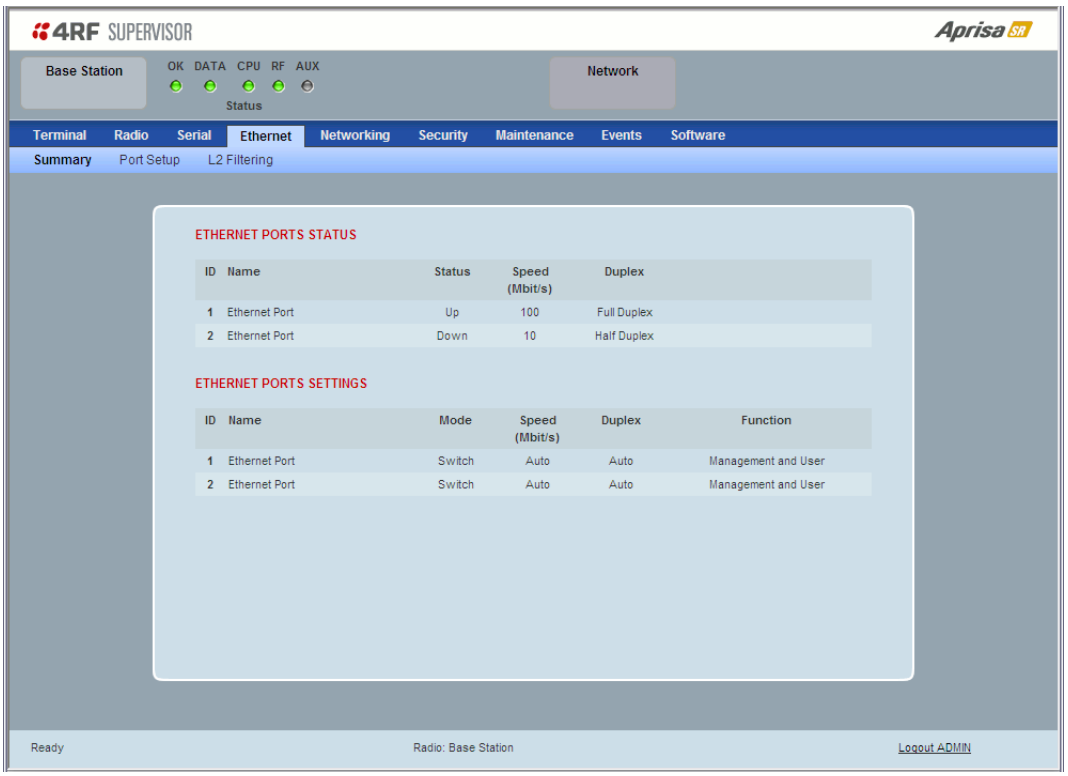
If the TCP Keep Alive is disabled, the radio relies on the Inactivity Timeout to detect a TCP connection failure. The default setting is disabled.

Note: An active TCP Keep Alive will generate a small amount of extra network traffic.

Ethernet

Ethernet > Summary

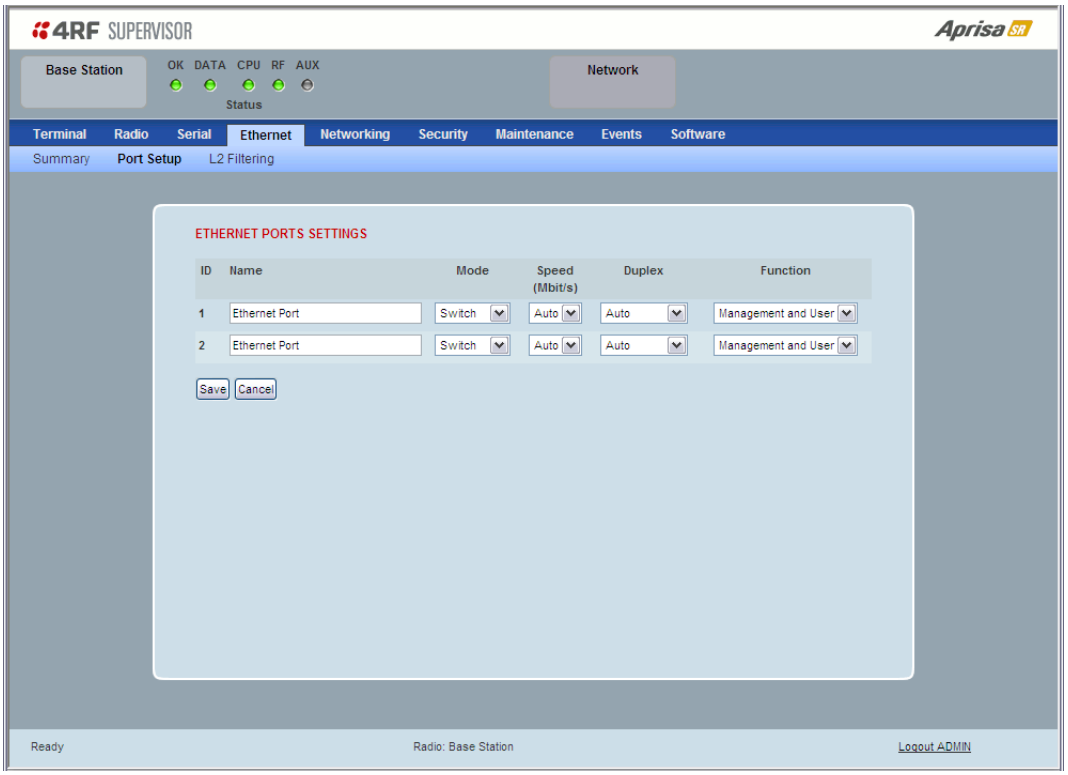
This page displays the current settings for the Ethernet port parameters and the status of the ports.



See ‘Ethernet > Port Setup’ for configuration options.

Ethernet > Port Setup

This page provides the setup for the Ethernet ports settings.



ETHERNET PORT SETTINGS

Mode

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

Option	Function
Standard	Enables Ethernet data communication over the radio link.
Switch	Ethernet traffic is switched locally between the two Ethernet ports and communicated over the radio link
Disabled	Disables Ethernet data communication over the radio link.

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

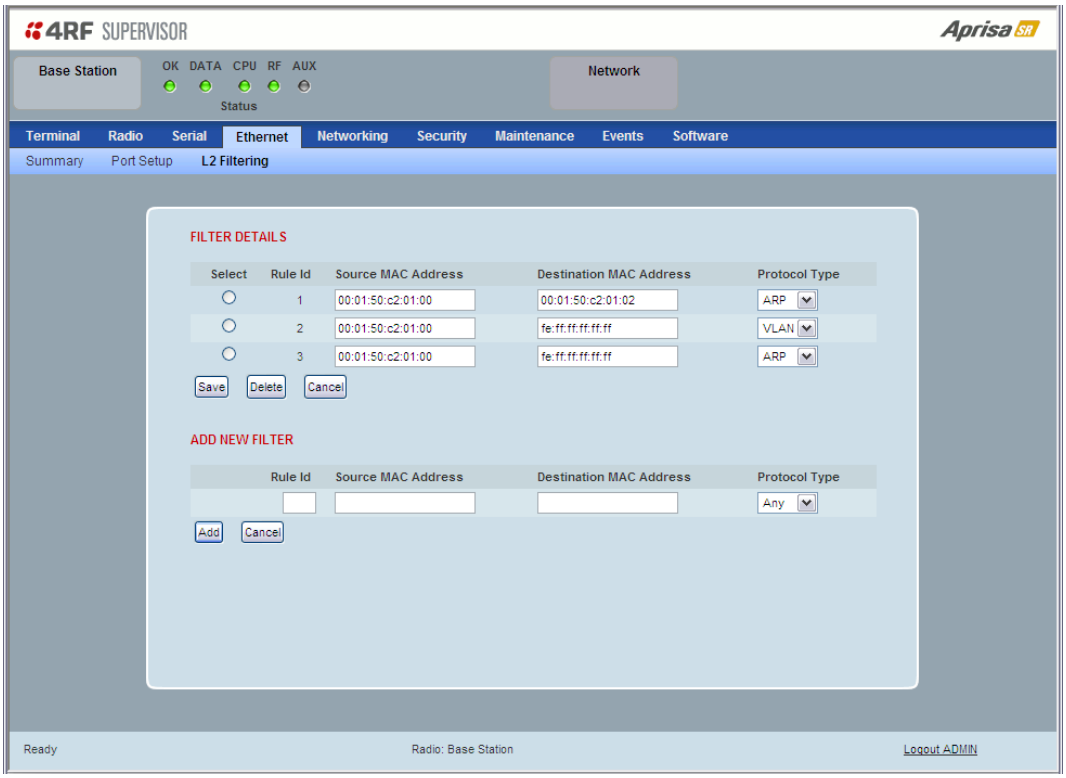
Function

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 126).



FILTER DETAILS

L2 Filtering provides the ability to filter radio link traffic based on specified Layer 2 MAC addresses.

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.

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

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 Ethernet Type accepted ARP, VLAN, IPv4, IPv6 or Any type.

Example:

In the screen shot, the rules are configured in the base station which controls the radio link traffic from base station to remote / repeater stations.

Traffic from a device with the MAC address 00:01:50:c2:01:00 is forwarded over the radio link if it meets the criteria:

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

Special L2 Filtering Rules:

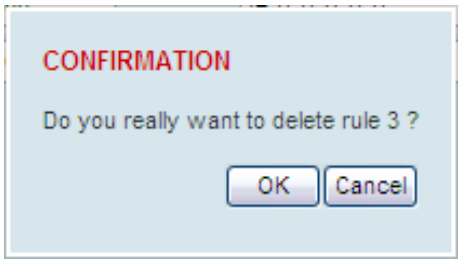
Unicast Only Traffic

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

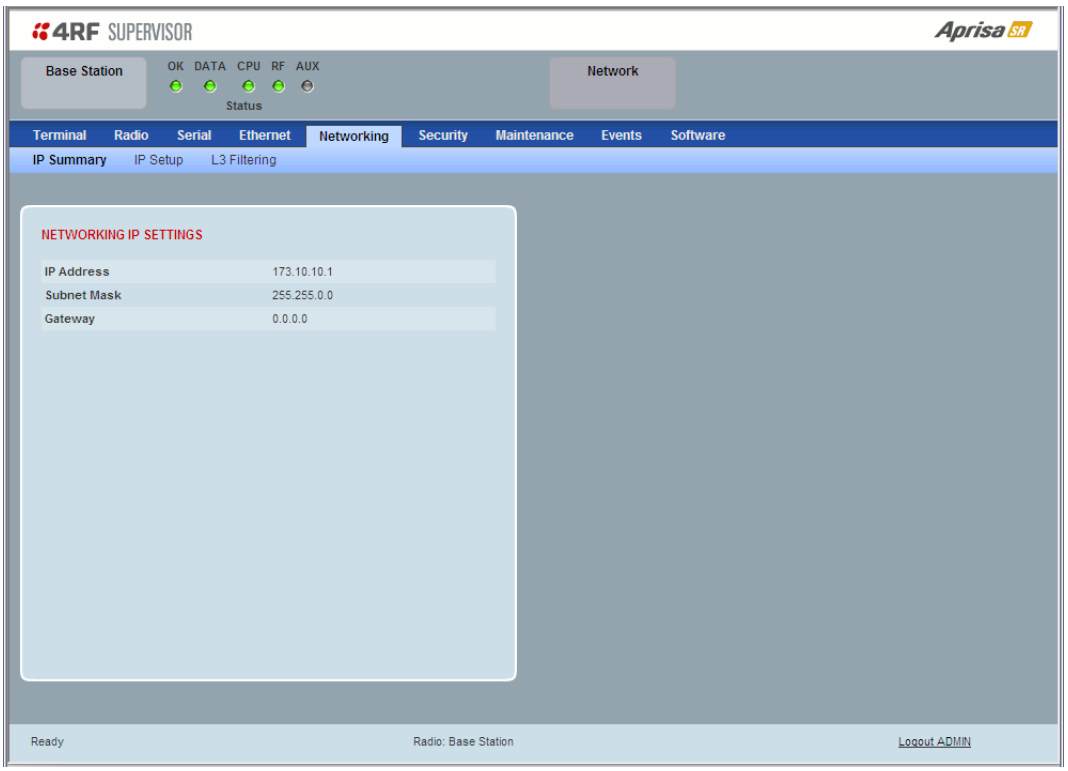
To add a L2 Filter:

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.

Networking

Networking > IP Summary

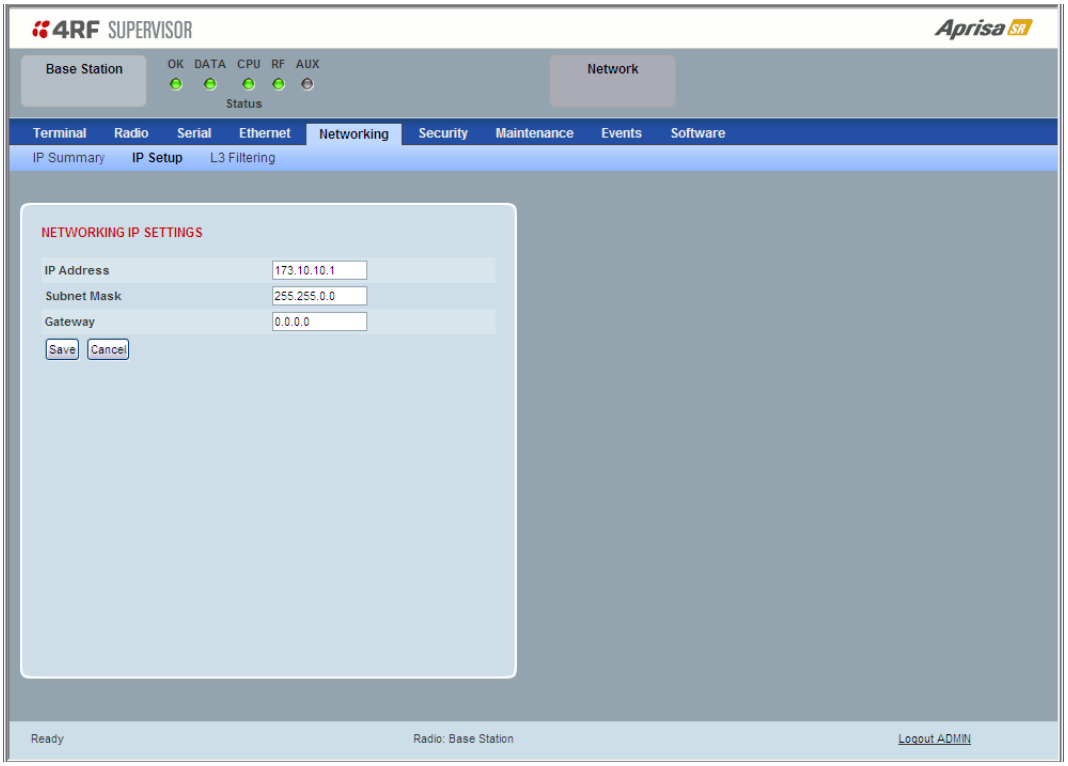
This page displays the current settings for the Networking IP Settings.



See ‘Networking > IP Setup’ for configuration options.

Networking > IP Setup

This page provides the setup for the Networking IP Settings.



NETWORKING IP SETTINGS

IP Address

Set the static IP Address of the 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.

Subnet Mask

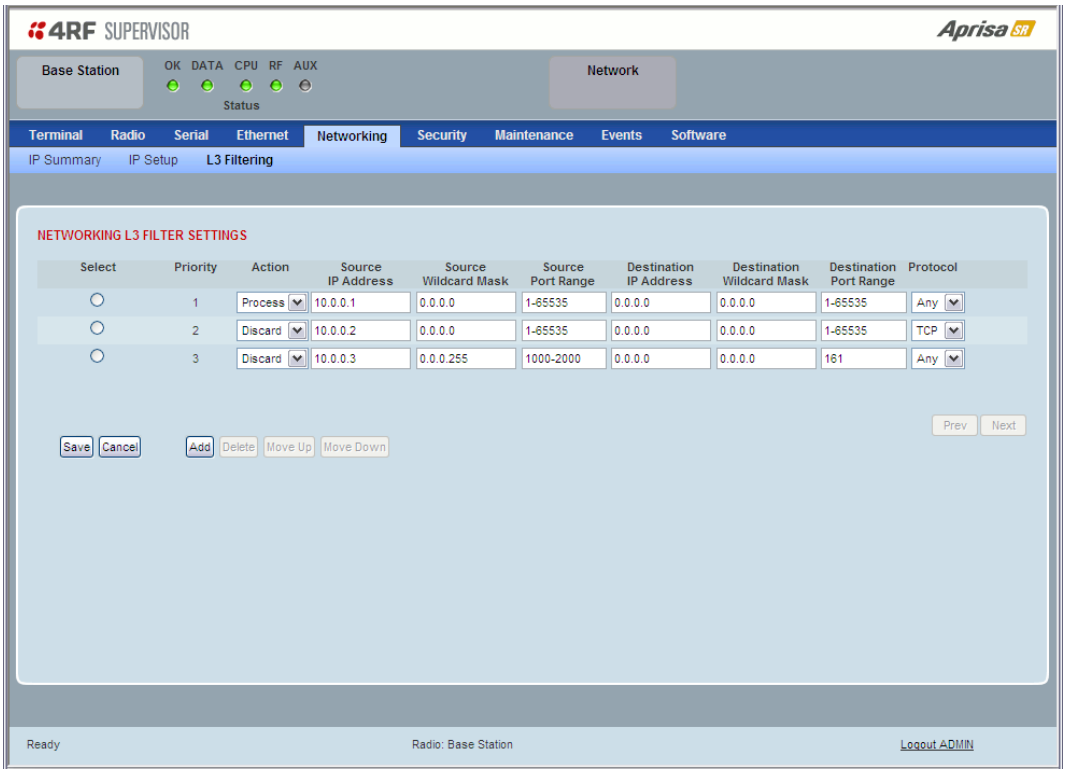
Set the Subnet Mask of the radio using the standard format xxx.xxx.xxx.xxx. The default subnet mask is 255.255.0.0.

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.

Networking > L3 Filtering

This page is only available if the Ethernet traffic option has been licensed (see 'Maintenance > Licence' on page 126).



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.

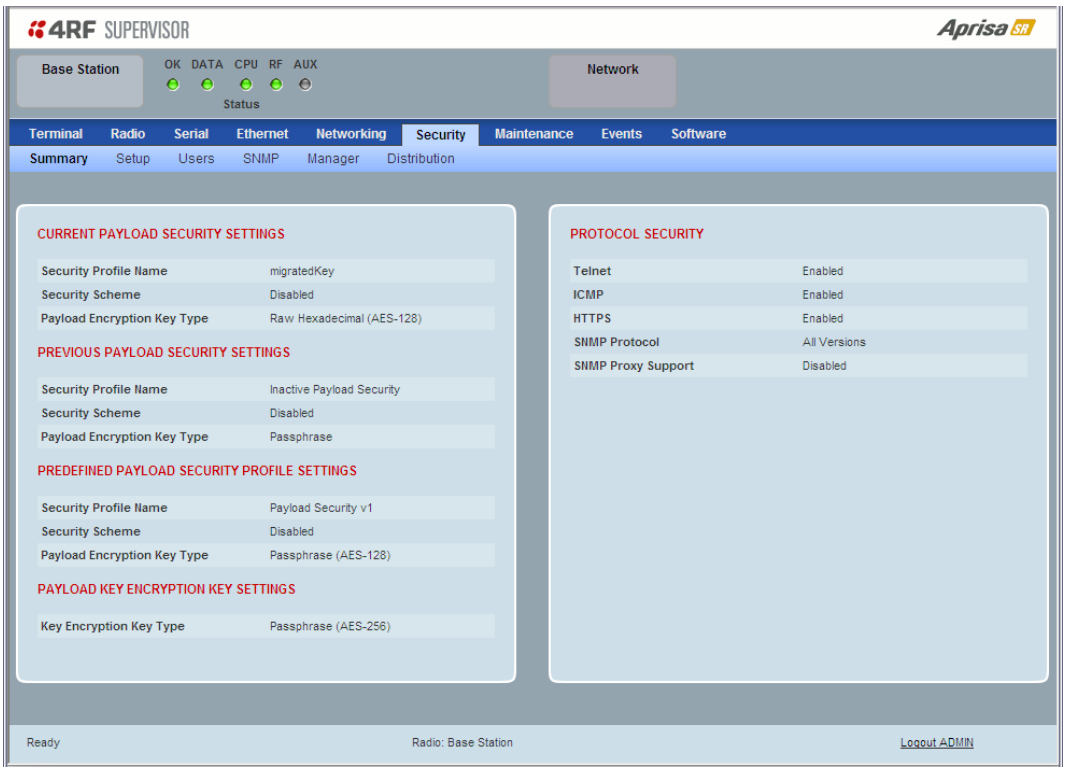
The Move Up button moves the selected entry above the entry above it increasing it’s process priority.

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

Security

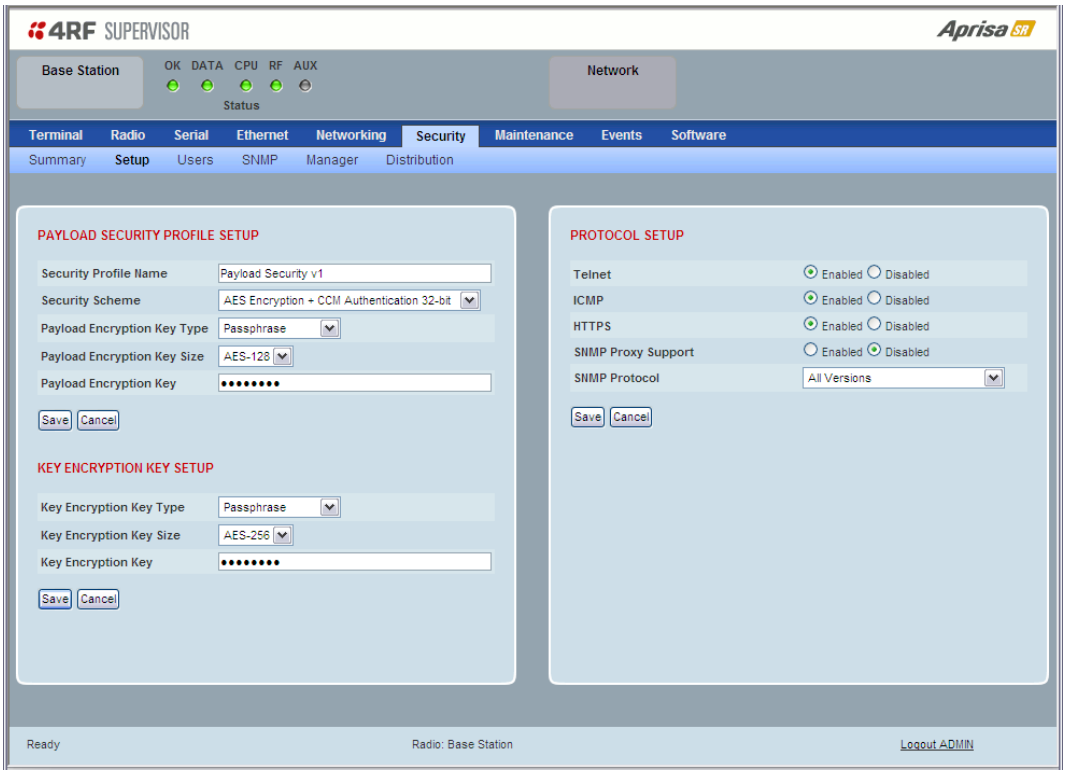
Security > Summary

This page displays the current settings for the Security parameters.



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

Security > Setup



PAYLOAD SECURITY PROFILE SETUP

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 Level
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 Hexidecimal	Use the Raw Hexidecimal password 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.

Pass Phrase

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

Raw Hexidecimal

The Raw Hexidecimal password 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 SETUP

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 Hexidecimal	Use the Raw Hexidecimal password 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 password. This is used to encrypt the payload encryption key.

PROTOCOL SETUP

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	Authentication Type	Context Name	Authentication Passphrase
noAuthUser	-	noAuth	noAuthUser
authUserMD5	MD5	auth	authUserMD5
authUserSHA	SHA	auth	authUserSHA

SNMPv3 Authentication Passphrase

The Authentication Passphrases can be changed via SNMP (not SuperVisor).

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

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

To change a user authentication passphrase:

1. SET the usmUserStatus object for that user to 'Not In Service'
2. GET the usmUserSpinLockobject
3. SET the usmUserSpinLockobject with the value that was just GOT in the previous step
4. SET the usmUserAuthKeyChange to the new Authentication key string
5. SET the usmUserPrivKeyChangeto the new Privacy key string
6. SET the usmUserStatus object for that user to 'Active'

Note that the key string for steps 4 and 5 are 32 octet hexadecimal values. This string is generated based on the 'old passphrase' and 'new passphrase' as specified in RFC2274.

The utility 'encode_keychange.exe', available from NET-SNMP open source applications, can be used to generate this string.

An example command to generate a new Authentication key string for the default desUserMD5 is:

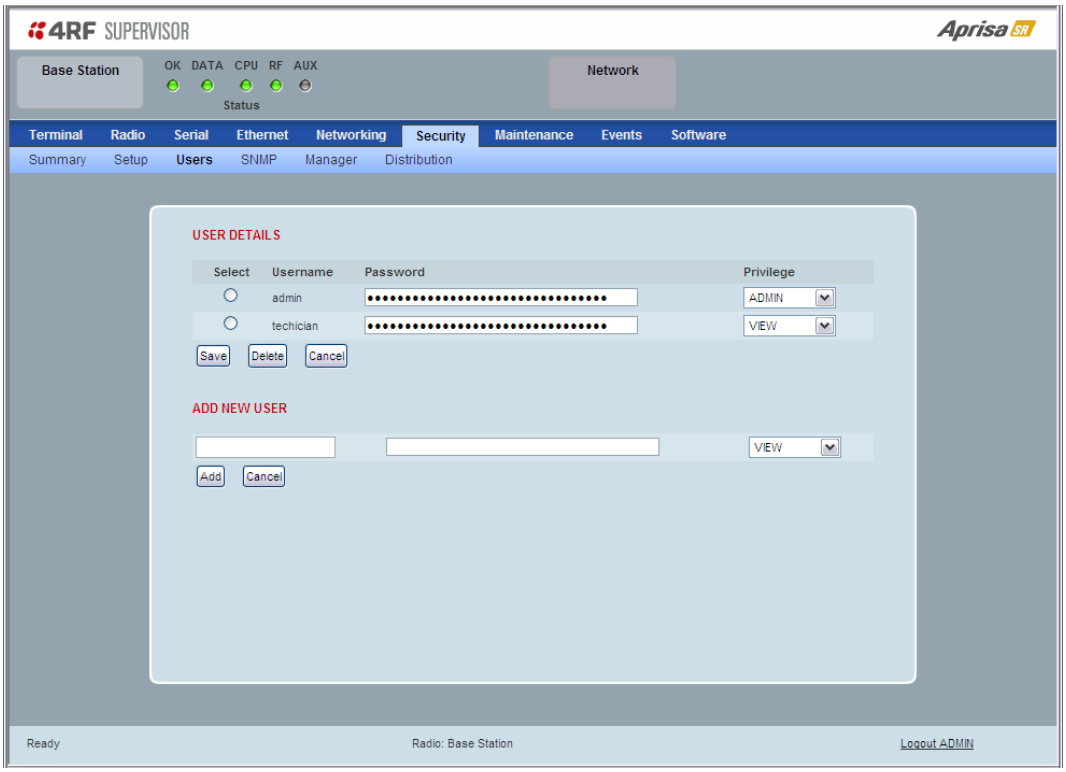
encode_keychange -t md5 -O "desUserMD5" -N "desUserMD5Auth" -E 0x0100DC

An example command to generate a new Privacy key string for the default desUserMD5 is:

encode_keychange -t md5 -O "desUserMD5" -N "desUserMD5Priv" -E 0x0100DC

These command executions will return a 32 Octet Hexadecimal string that can be used in steps 4 and 5 above.

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 characters but cannot contain back slashes, forward slashes, spaces, tabs, single or double quotes. 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 62 for the list of SuperVisor menu items versus user privileges.

4. Click ‘Add’

To delete a user:

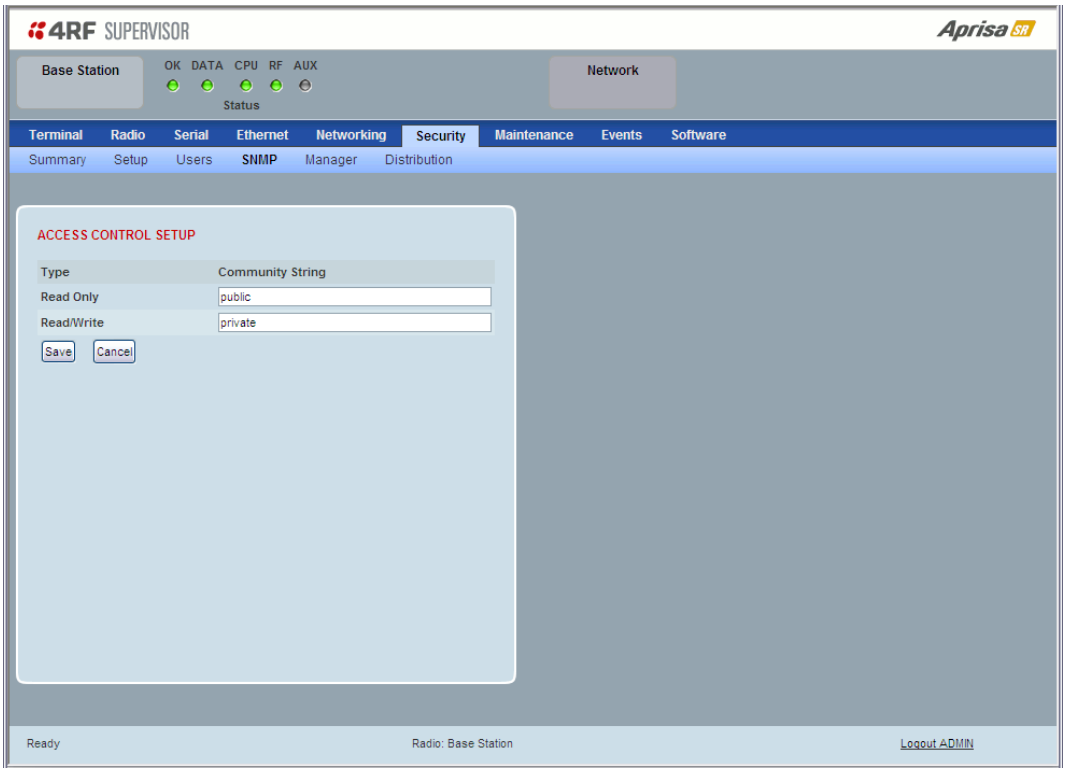
1. Select Terminal Settings > Security > Users
2. Click on the Select button for the user you wish to delete.
3. Click ‘Delete

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). 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 110).

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:

cccccccccc:bbbbbb

Where:

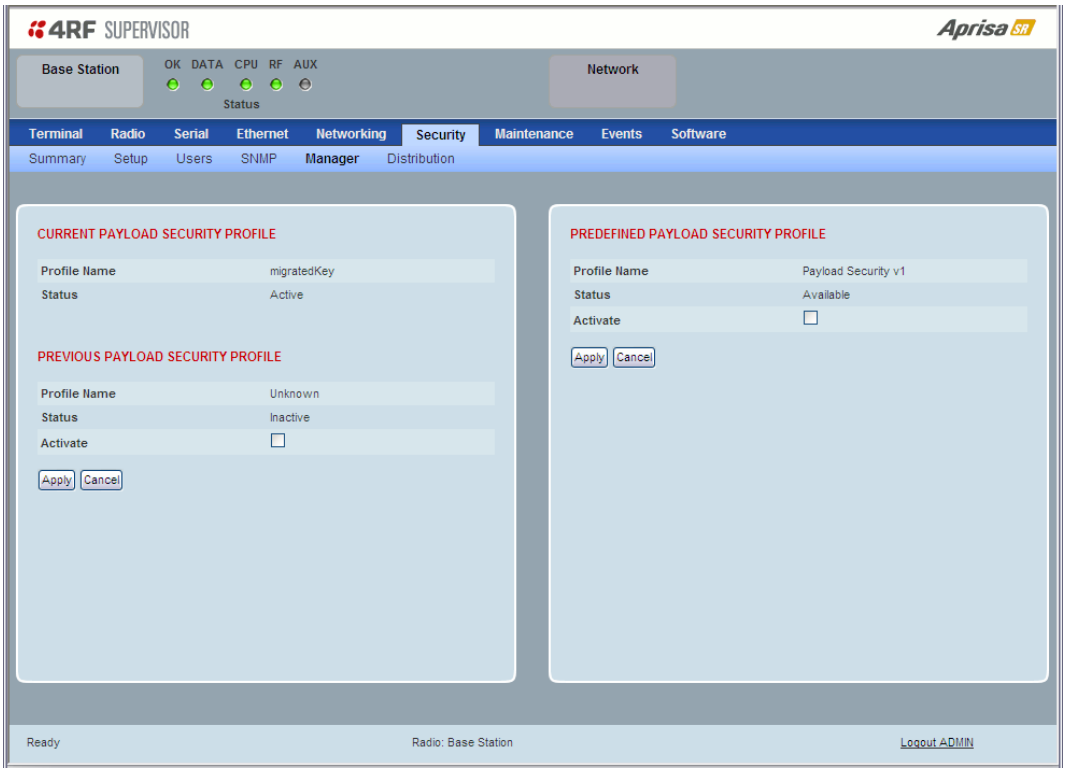
cccccccccc is the community string of the base station

and

bbbbbb is the last 3 bytes of the remote station MAC address (see 'Network Status > Network Table' on page 153) for the remote station MAC address.

The SNMP Proxy Support must be enabled for this method of SNMP access to operate (see 'SNMP Proxy Support' on page 106).

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

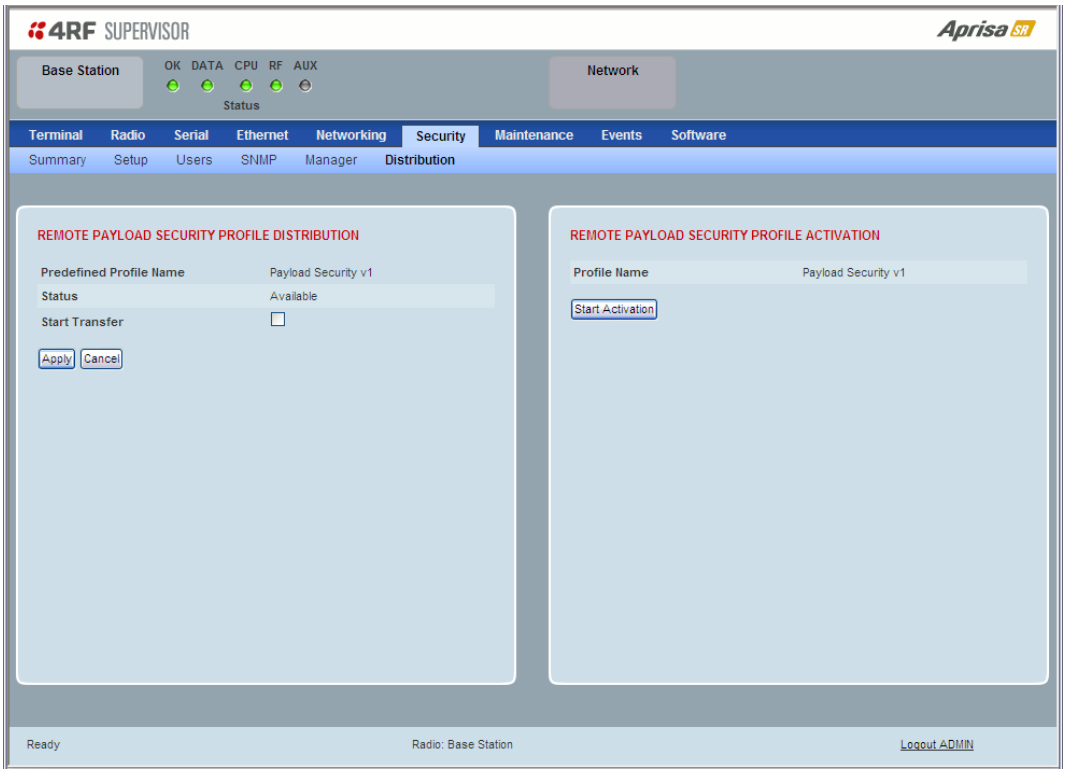
This parameter displays the new security profile that could be activated on the radio or distributed to all remote radios with Security > Distribution.

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 103.
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.

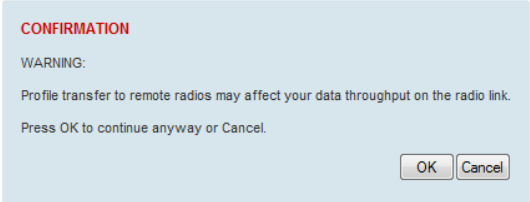
Note: The distribution of the payload security profile to remote stations does not stop customer traffic from being transferred.

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 103).

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.

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 103) 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).

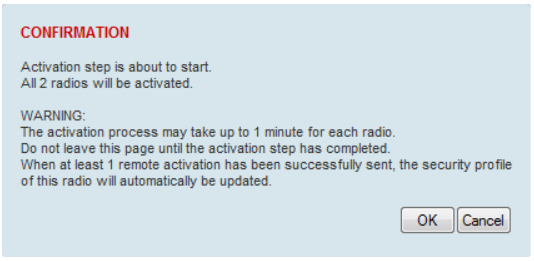
---

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:

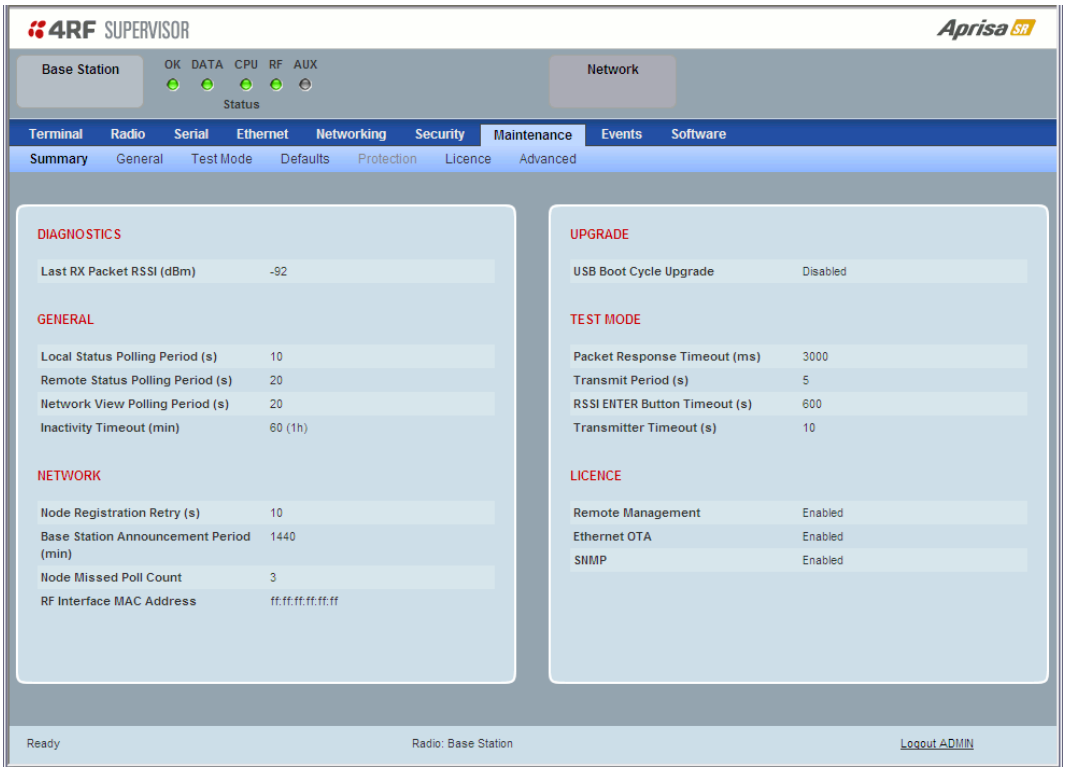


3. Click on 'OK' to start the activation process or Cancel to quit.

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.

Inactivity Timeout (min)

This parameter displays the period of user inactivity before SuperVisor automatically logs out of the radio.

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.

RF Interface MAC address

This parameter displays the RF Interface MAC address when the radio is part of a Protected Station.

UPGRADE

USB Boot Cycle Upgrade

This parameter shows the type of USB Boot Cycle upgrade defined in 'Software Setup > USB Boot Upgrade' on page 141.

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.

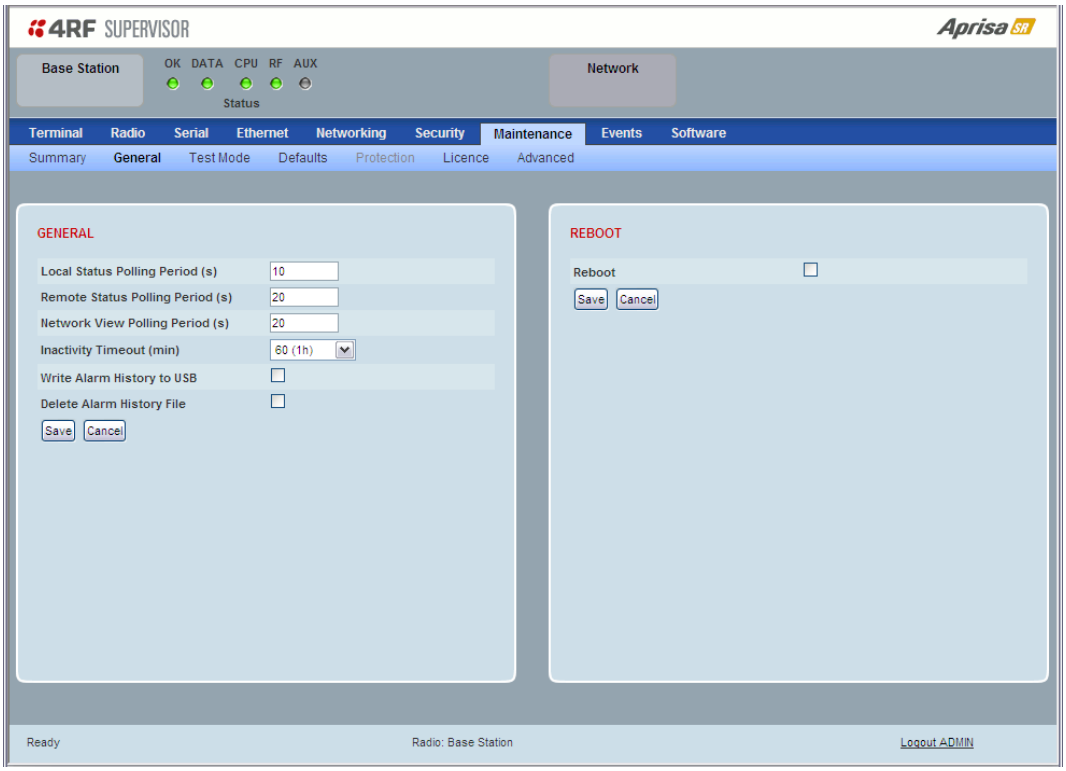
Ethernet OTA (over the air)

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 126).

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 68). 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.

Write Alarm History to USB

This parameter when enabled writes the alarm history file to a USB flash drive into the Host Port .

The file is a space delimited text file with a file name in the format 'alarm_ipaddress_date,time' e.g. 'alarm_172.17.10.17_2000-01-13,17.13.45.txt'.

The maximum number of event entries that can be stored is 1500 alarms.

The following table is an example of the alarm history file generated:

Index	Event Name	Severity	State	Time	Additional Information
1	softwareStartUp	information	0	2011-05-08,12:26:31.0	Power on Reset
2	softwareStartUp	information	0	2011-05-08,12:56:33.0	Power on Reset
3	protPeerCommunicationsLost	major	1	2011-05-08,12:56:39.0	Ethernet Comm Lost with Peer
4	protSwitchOccurred	information	0	2011-05-08,12:56:39.0	Keepalive missed from Active
5	protPeerCommunicationsLost	cleared	2	2011-05-08,12:56:40.0	Alarm Cleared
6	rfNoReceiveData	warning	1	2011-05-08,12:56:53.0	RF No Rx Data for 6 seconds
7	eth2NoRxData	warning	1	2011-05-08,12:57:03.0	ETH2 has not received data for 21 seconds
8	rfNoReceiveData	cleared	2	2011-05-08,12:57:05.0	
9	rfNoReceiveData	warning	3	2011-05-08,12:57:12.0	RF No Rx Data for 6 seconds
10	rfNoReceiveData	cleared	4	2011-05-08,12:57:23.0	
11	serialNoRxData	warning	1	2011-05-08,12:57:25.0	Serial has not received data for 44 seconds
12	rfNoReceiveData	warning	5	2011-05-08,12:57:29.0	RF No Rx Data for 6 seconds
13	rfNoReceiveData	cleared	6	2011-05-08,12:57:59.0	

State

The State column is an indication of whether the event is active or not. An even number indicates an inactive state while an odd number indicates an active state.

The AUX LED will flash orange while the file is copying to the USB flash drive.

Delete Alarm History file

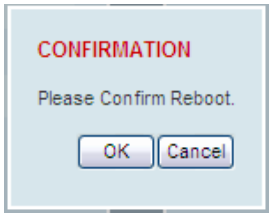
This parameter when activated deletes the alarm history file stored in the radio.

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.

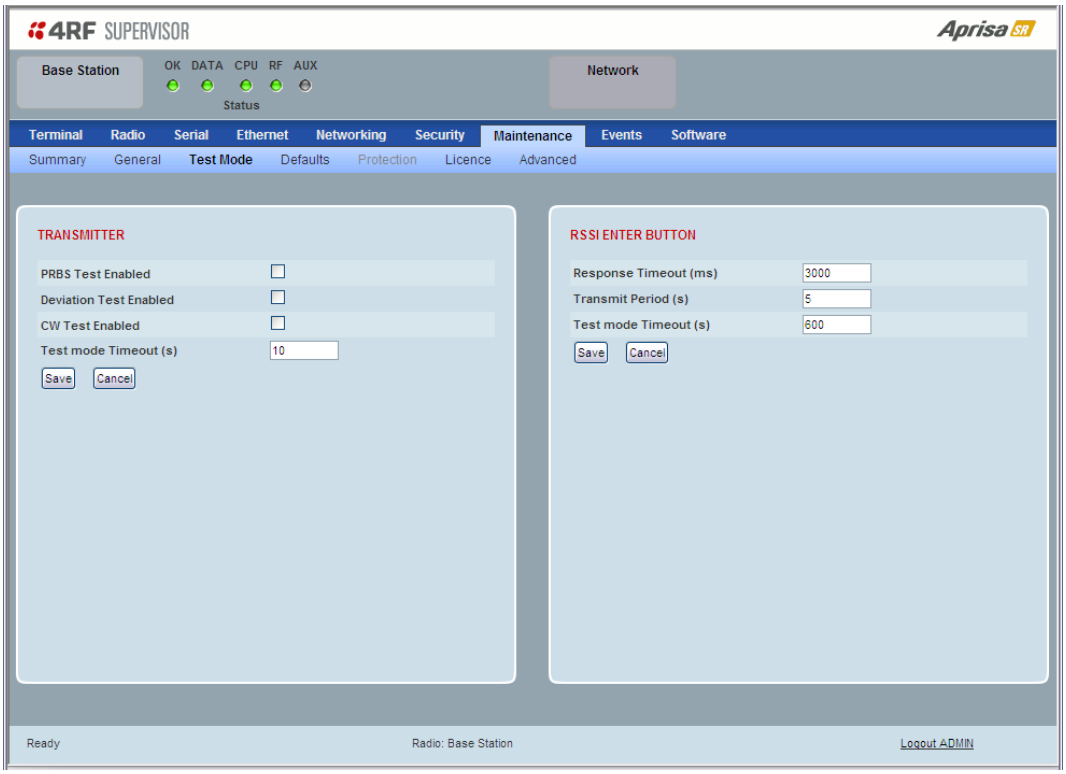
All the radio LEDS will flash repeatedly for 1 second.

The radio will be operational again in about 10 seconds.

The OK, DATA, and CPU LEDS will light green and the RF LED will be green 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 ENTER 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.

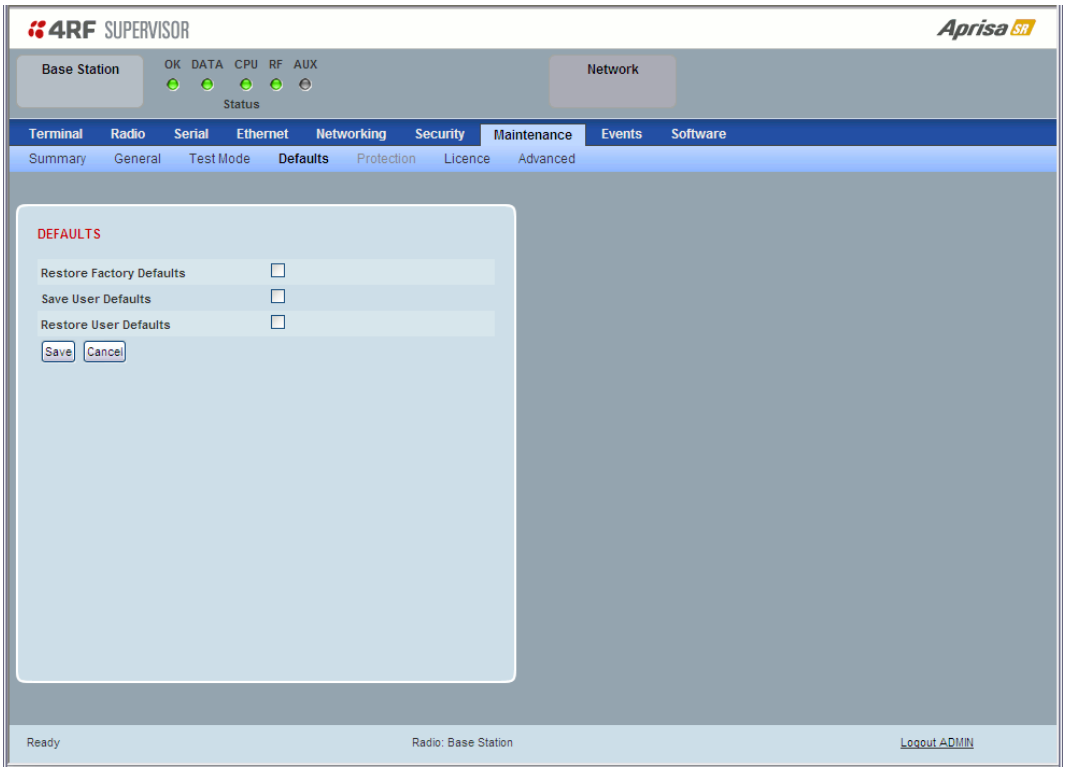
Transmit Period (sec)

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 > Defaults

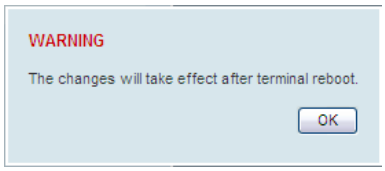


DEFAULTS

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.

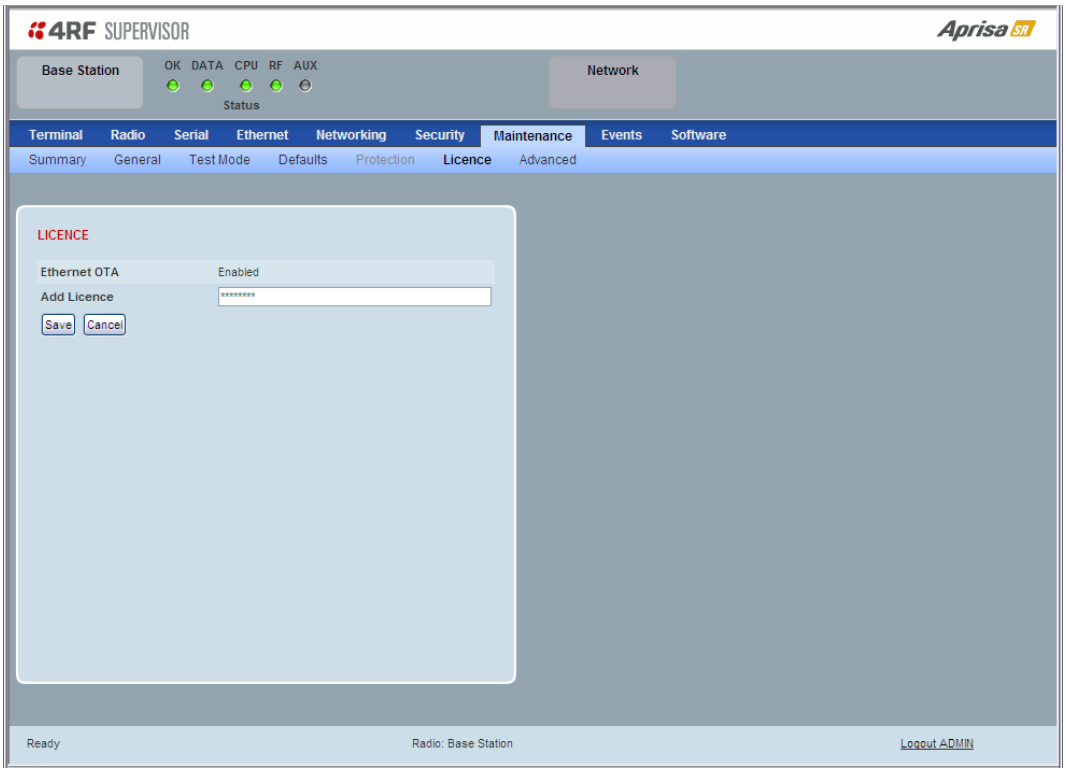
Save User Defaults

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
APSR-N400-012-SO-12-ETAA	4RF Aprisa SR, BR, 400-470 MHz, 12.5 kHz, SO, 12 VDC, ET, AA

Serial Only Radio

If a Serial Only Aprisa SR radio is purchased (indicated by the A1), Ethernet Traffic is not enabled.

Part Number	Part Description
APSR-N400-012-SO-12-ETA1	4RF Aprisa SR, BR, 400-470 MHz, 12.5 kHz, SO, 12 VDC, ET, A1

Feature Licences

Feature Licences can be purchased to enable features if they were not purchased initially.

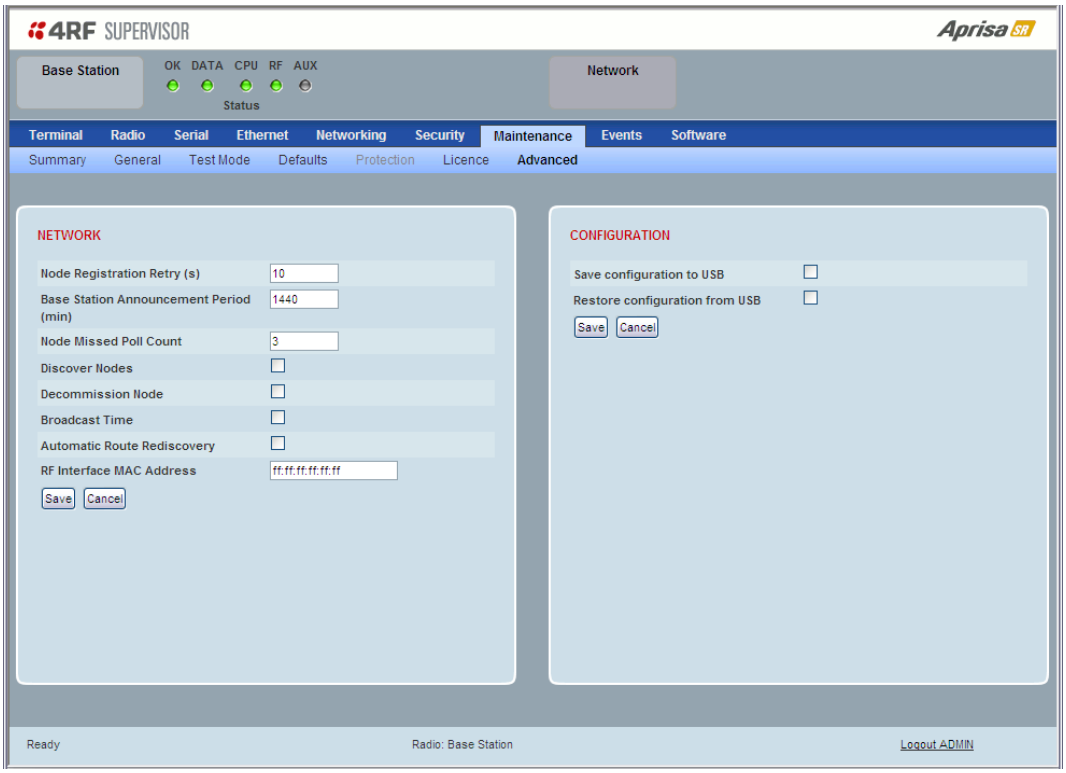
One license key is required per feature and per radio serial number.

Part Number	Part Description
APSA-LSRF-FET	4RF Aprisa SR Acc, Licence, Feature, Ethernet Traffic

When Ethernet traffic is enabled, the Ethernet port status must be set to enabled to allow Ethernet data communication over the radio link (see ‘Ethernet > Port Setup’ on page 94).

In this software version, Remote Management 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

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.

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 into both Protected Station radios in the factory.

If a replacement Protection Switch is installed, the replacement unit MAC address must be entered in both radios (see ‘Replacing a Faulty Protection Switch’ on page 215).

The Protection Switch RF Interface MAC address is shown on the Protection Switch label:

CONFIGURATION

Save Configuration to USB

This parameter saves all user configuration settings to a binary encrypted file on the USB root directory with filename of asrcfg_1.6.5. Some parameters are not saved e.g. security passwords, licence keys etc.

Restore Configuration from USB

This parameter restores all user configuration settings from a binary encrypted file on the USB root directory with filename of asrcfg_1.6.5.

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).

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:

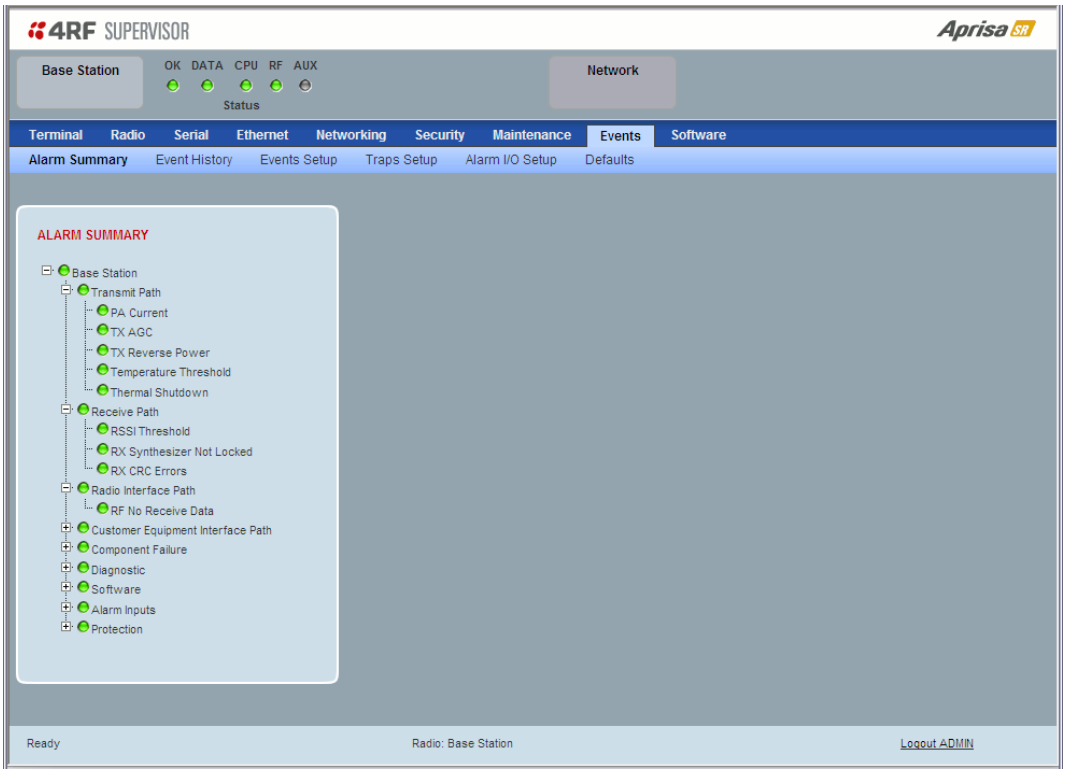
1. Alarm Events

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 230 for a complete list of events.

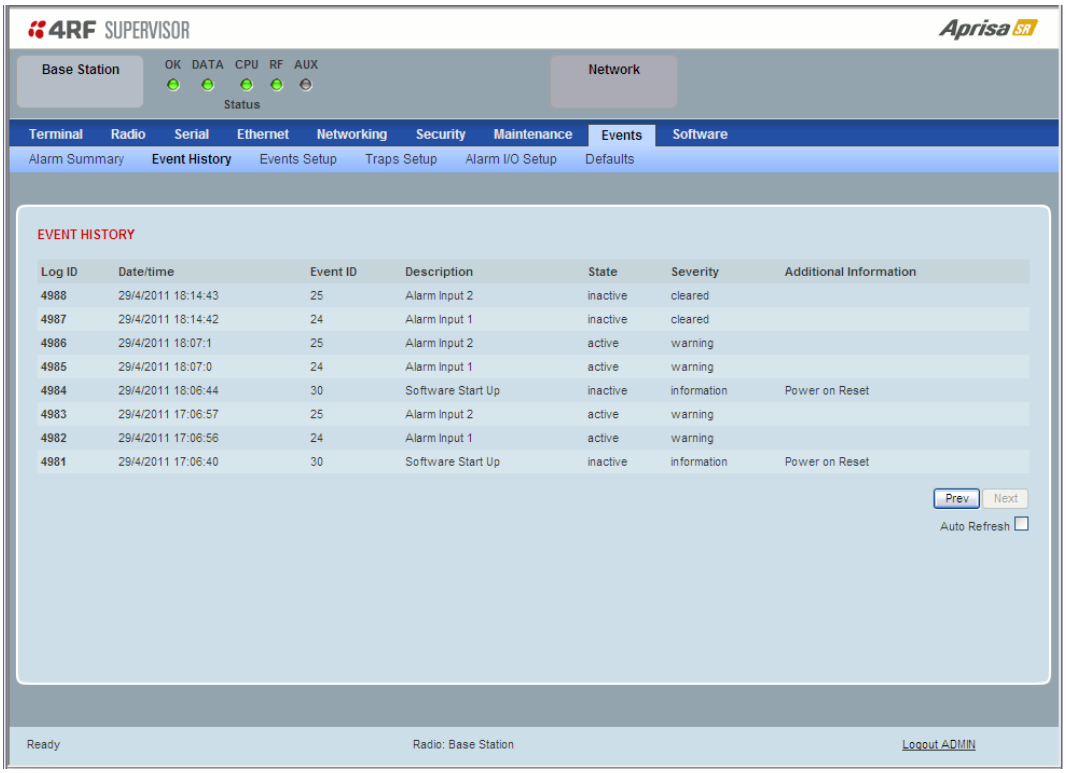


ALARM SUMMARY

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



EVENT HISTORY

The last 1500 events are stored in the radio. The complete event list can be downloaded to a USB flash drive (see 'Write Alarm History to USB' on page 121).

The Event History can display the last 50 events stored in the radio in blocks of 8 events.

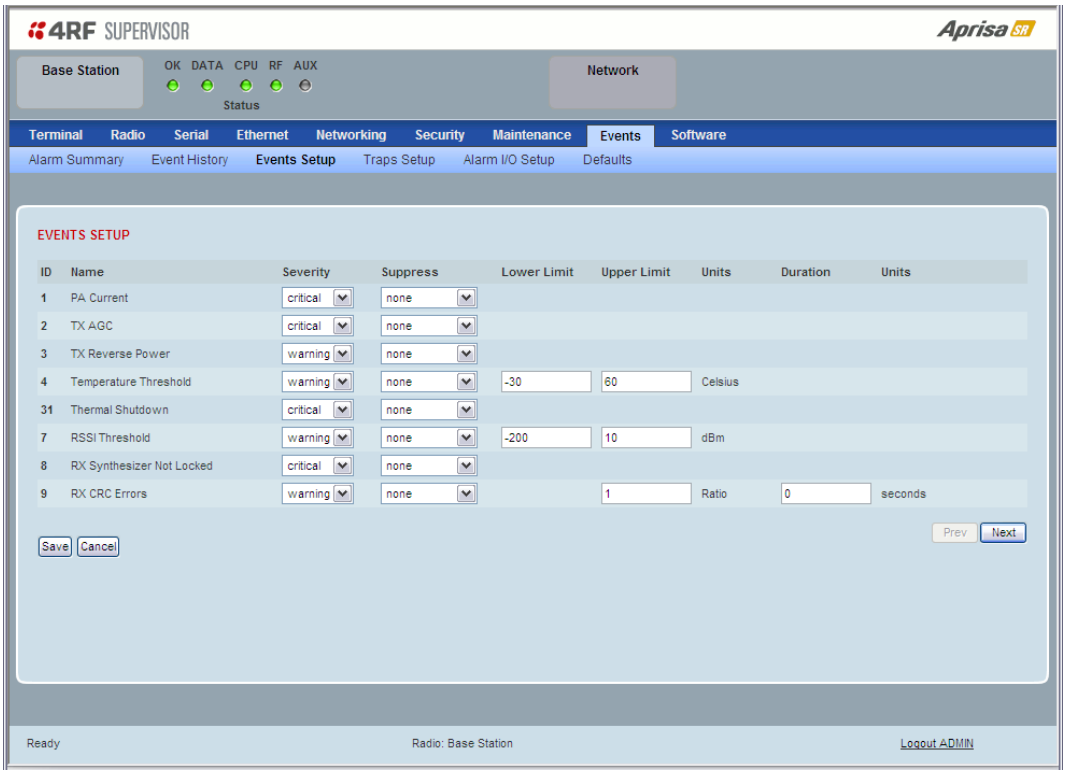
The Next button will display the next page of 8 events and the Prev button will display the previous page of 8 events. Using these buttons will disable Auto Refresh to prevent data refresh and page navigation contention.

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 230).

All active alarms for configured alarm events will be displayed on the Parameters page (see 'Terminal > Parameters' on page 73). 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.

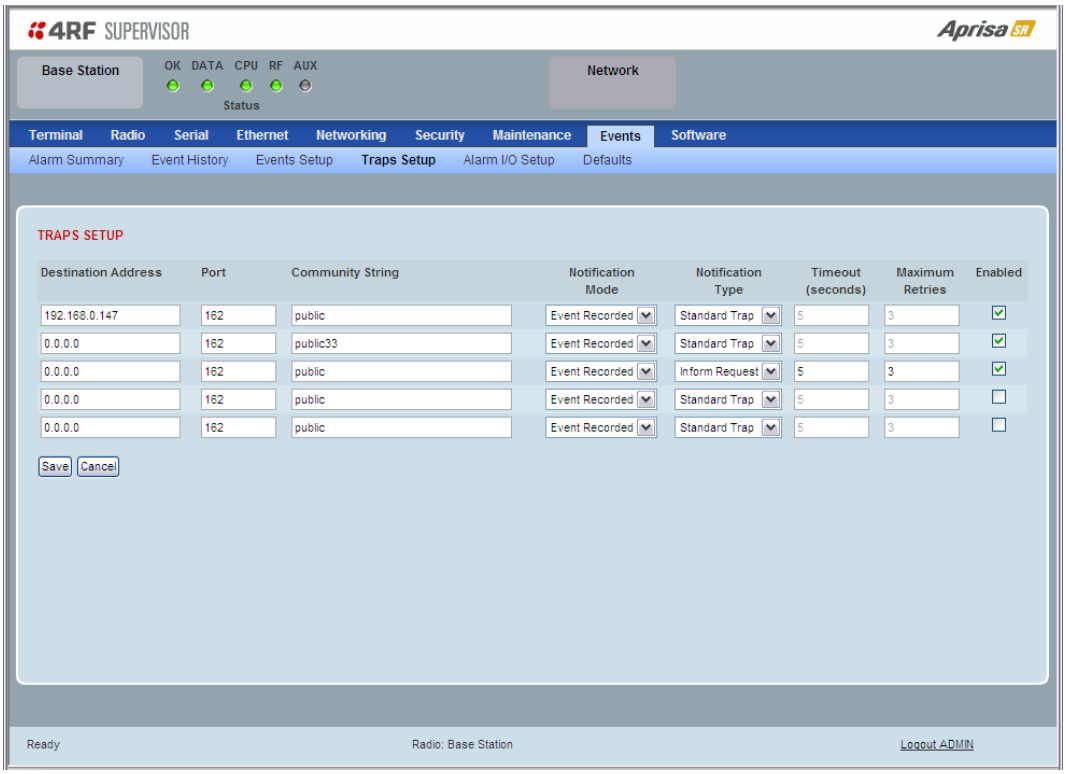
Block

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.

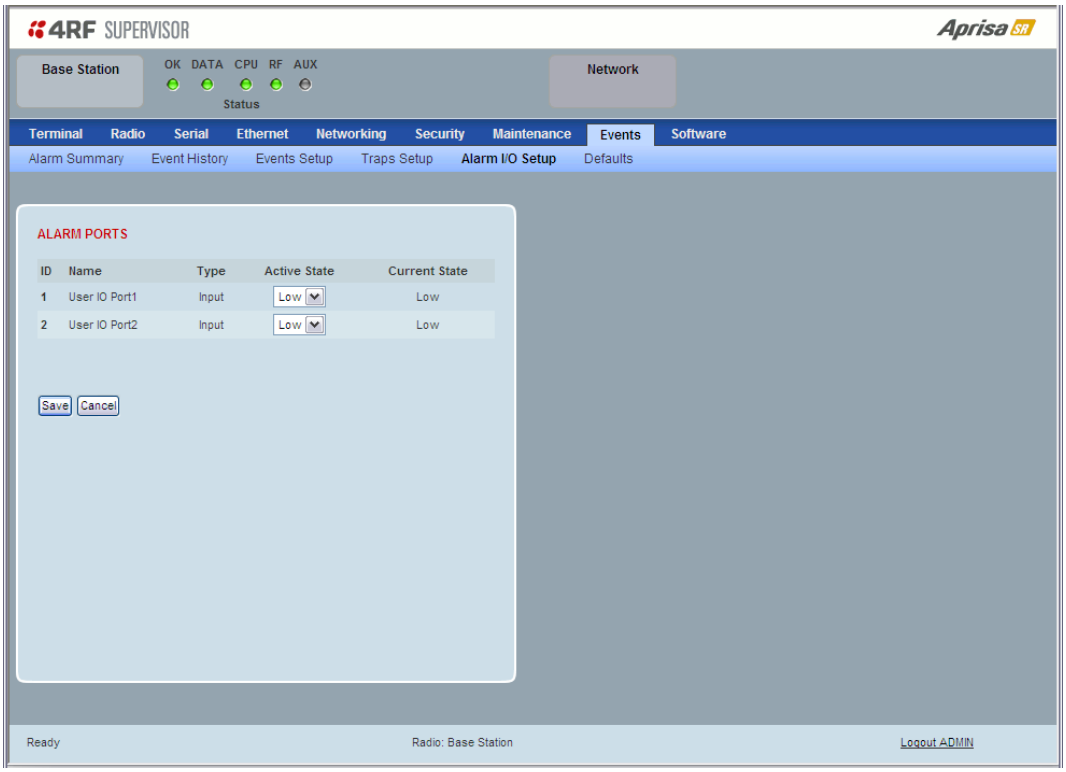
Maximum Retries

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

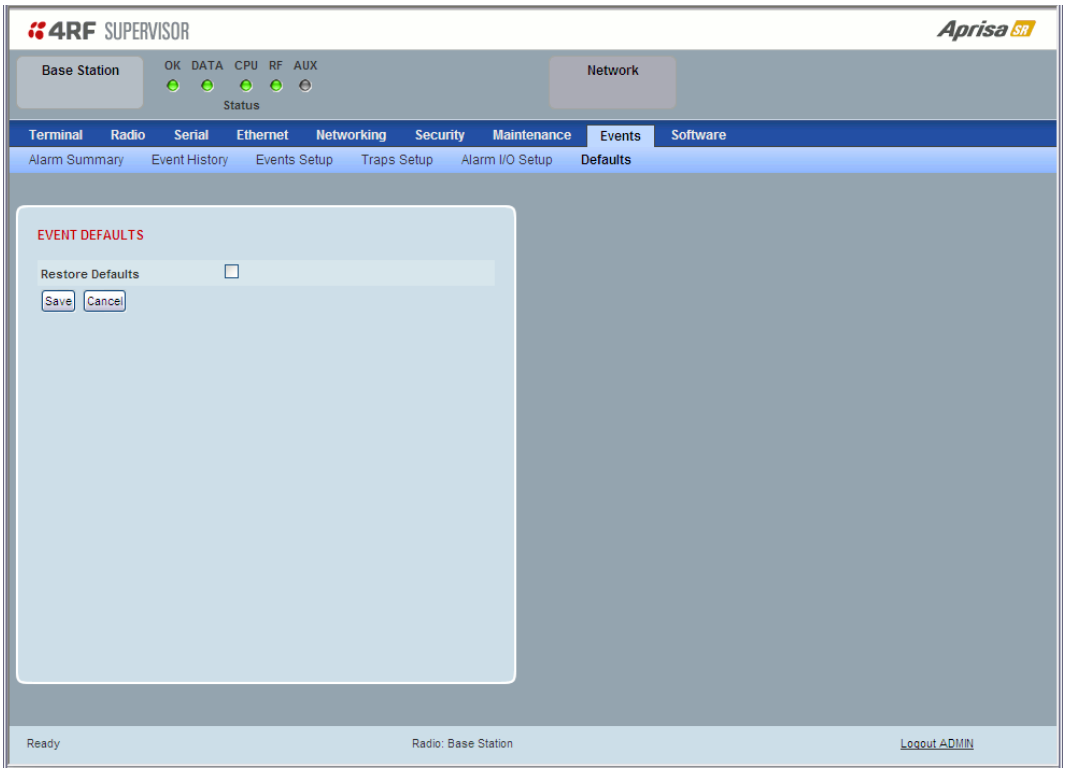


ALARM PORTS

This page provides control of the two hardware alarm inputs provided on the power and alarm connector. These alarms are only available when the station is non protected (see 'Hardware Alarms Connections' on page 229).

Option	Function
Low	The alarm is active low i.e. a logic 0 on the port will cause an alarm state
High	The alarm is active high i.e. a logic 1 on the port will cause an alarm state

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.

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 225). This process would only be used if the radio was a replacement or a new station in an existing network.

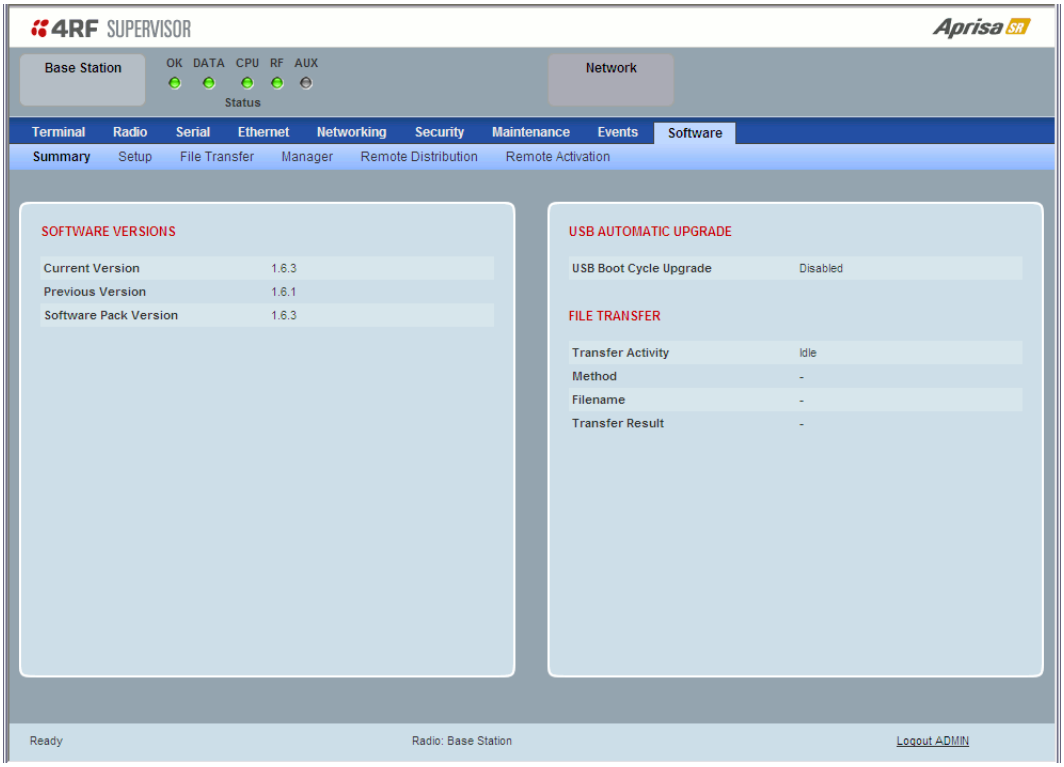
Network Software Upgrade

The radio software can be upgraded on an entire Aprisa SR radio network remotely over the radio link (see ‘Network Software Upgrade’ on page 224). 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 141.

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.

File

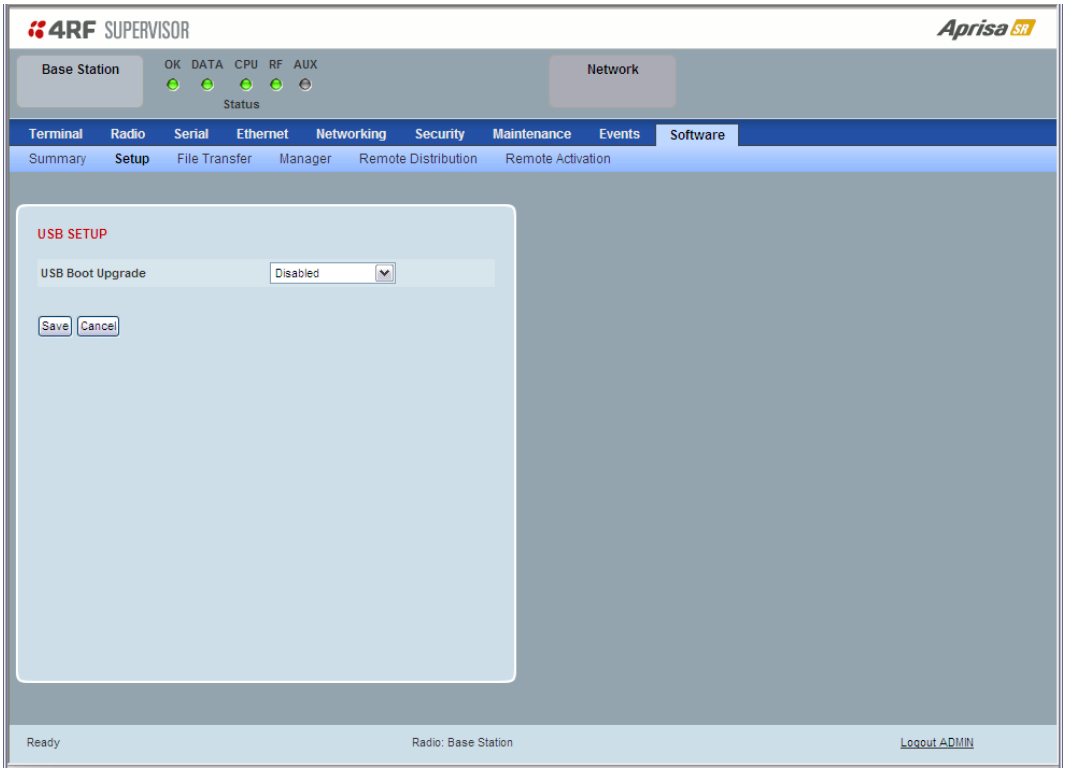
This parameter shows the software file source.

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

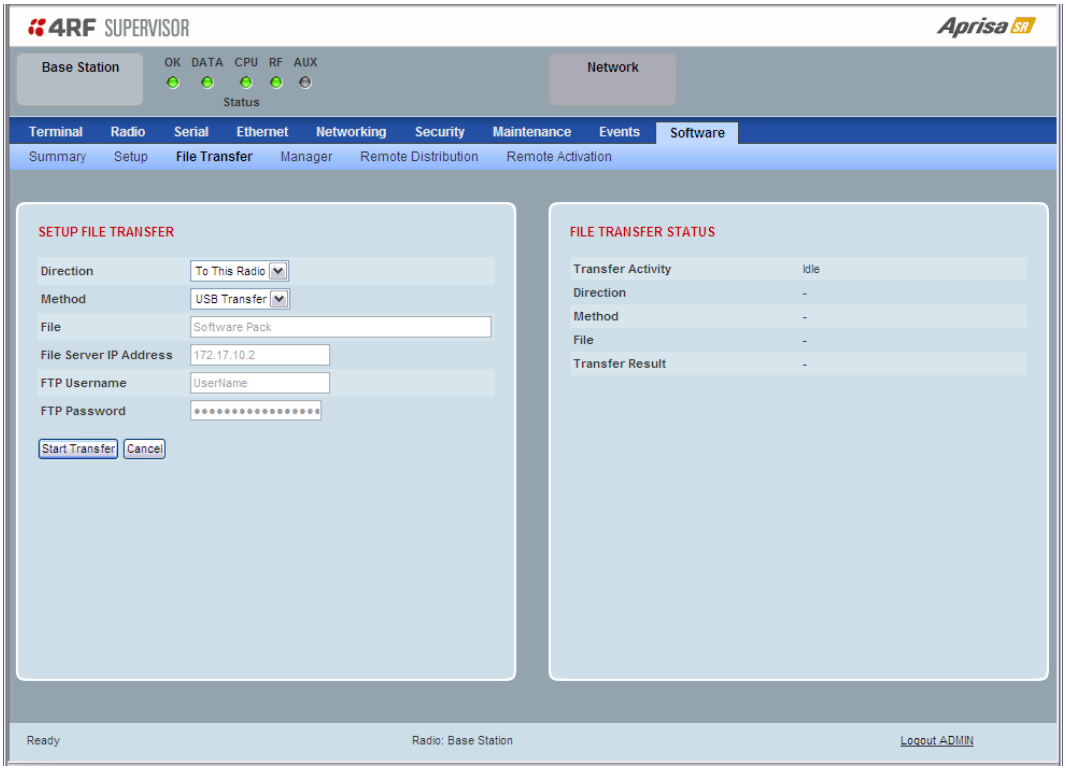
This parameter determines the action taken when the radio power cycles and finds a USB flash drive in the Host port. The default setting is 'Load and Activate'.

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 145).
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

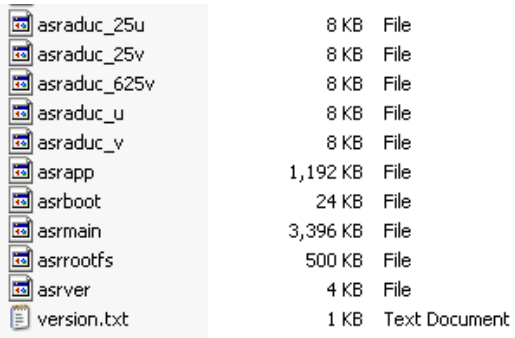
This parameter shows the file transfer method.

File

This parameter shows the software file source.

Transfer Result

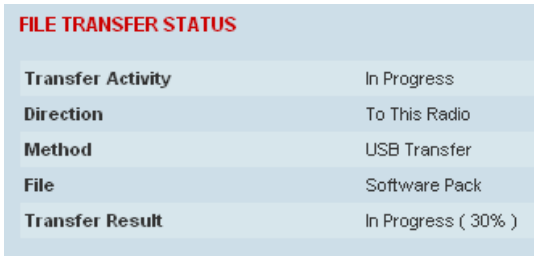
This parameter shows the progress of the transfer:

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;  asraduc_25u 8 KB File asraduc_25v 8 KB File asraduc_625v 8 KB File asraduc_u 8 KB File asraduc_v 8 KB File asrapp 1,192 KB File asrboot 24 KB File asrmain 3,396 KB File asrrootfs 500 KB File asrver 4 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'.



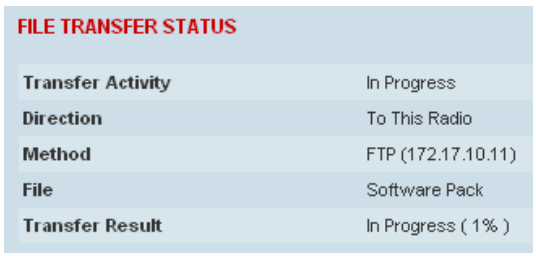
4. When the transfer is completed, remove the USB flash drive from the Host Port. If the SuperVisor 'USB Boot Upgrade' setting is set to 'Disabled' (see 'USB Boot Upgrade' on page 141), the USB flash drive doesn't need to be removed as the radio won't try to load from it.

Go to Supervisor > Software > Manager and activate the Software Pack (see 'Software > Manager' on page 145). The radio will reboot automatically.

If the file transfer fails, check the Event History page (see 'Events > Event History' on page 131) 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'.



Go to Supervisor > Software > Manager and activate the Software Pack (see 'Software > Manager' on page 145). The radio will reboot automatically.

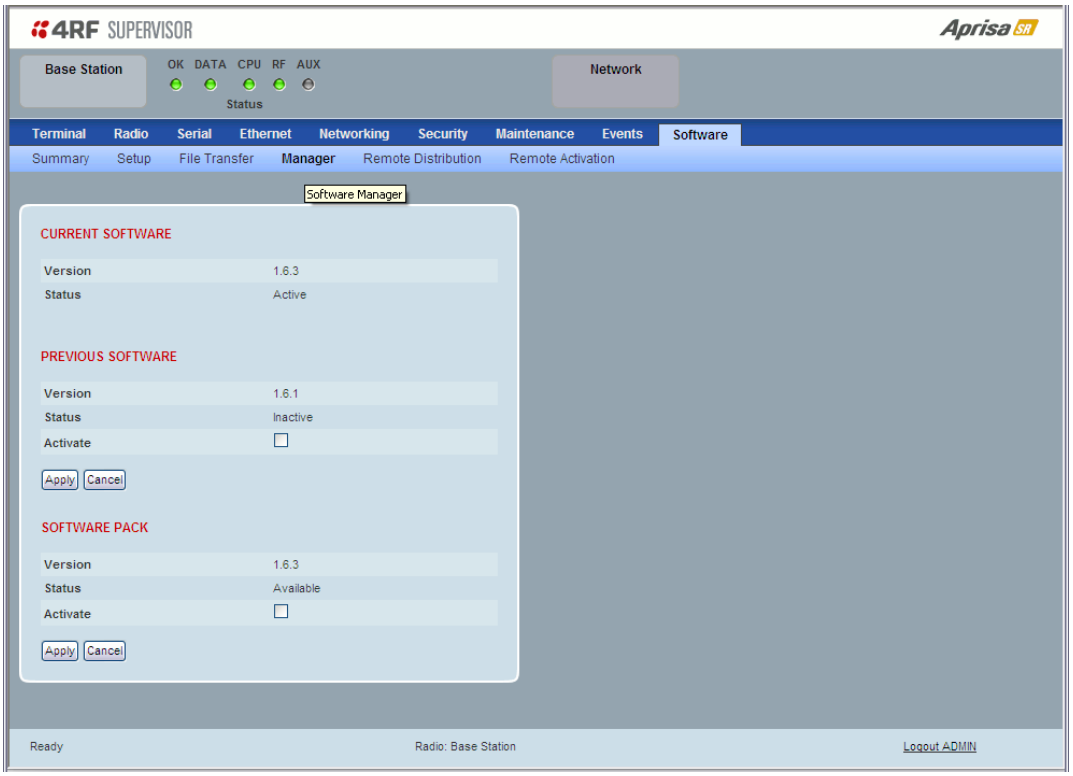
If the file transfer fails, check the Event History page (see 'Events > Event History' on page 131) for more details of the transfer.

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.

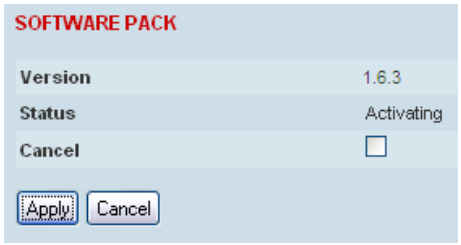
Activate

This parameter activates the software pack.

The Aprisa SR will automatically reboot after activation.

To activate a software version:

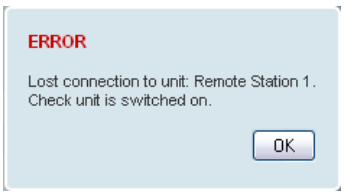
1. Tick the software version required to be activated (previous software or software pack).
2. Click ‘Apply’.



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.

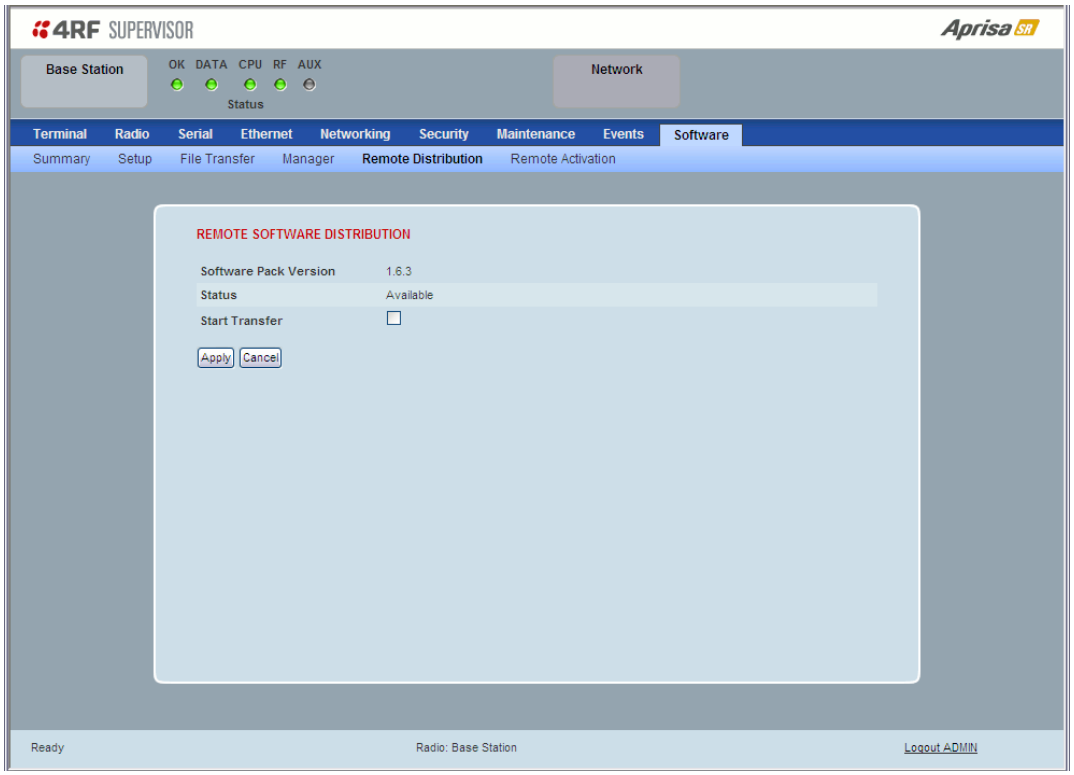
Software > Remote Distribution

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 142) 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.

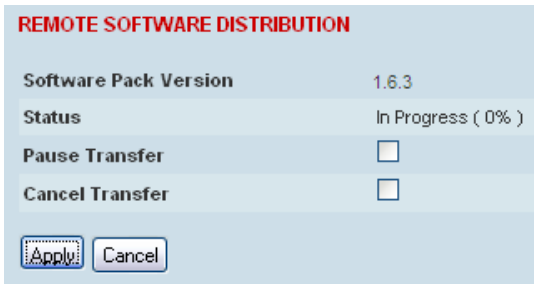
Note: The distribution of software to remote stations does not stop customer traffic from being transferred. However, due to the volume of traffic, the software distribution process may affect customer traffic.

Software distribution traffic is classified as 'management traffic' but does 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 'Software > File Transfer' on page 142).

1. To ensure that the Network Table is up to date, it is recommended running the node discover function (see 'Discover Nodes' on page 128).
2. Click on 'Start Transfer'.



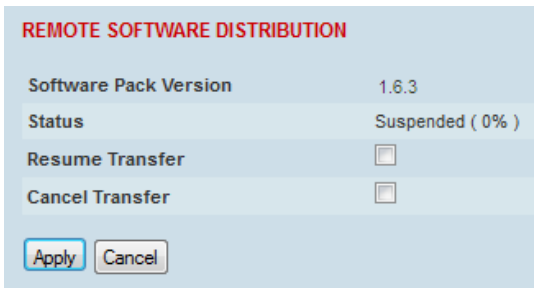
Note: This process could take anywhere between 40 minutes and several hours depending on channel size, Ethernet Management Priority setting and the amount of customer traffic on the network.

---

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.

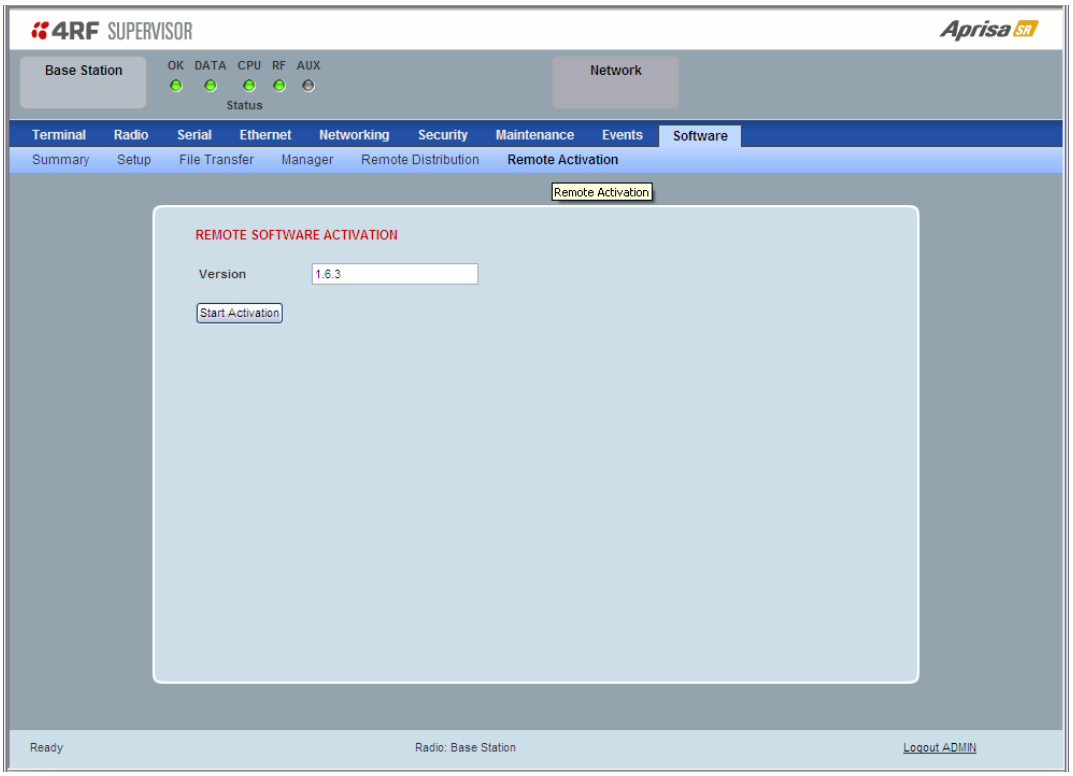
Software > Remote Activation

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 142) 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'.

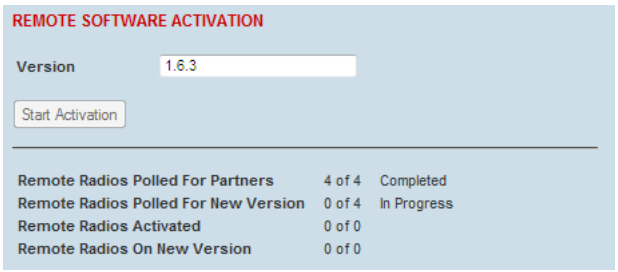
To activate software in remote stations:

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 142) 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).

---

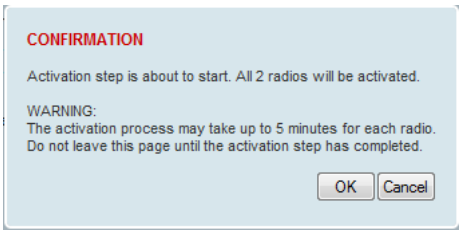
1. Enter the Software Pack version (if different from displayed version).
2. Click on 'Start Activation'.



The remote stations will be polled to determine which radios require activation:

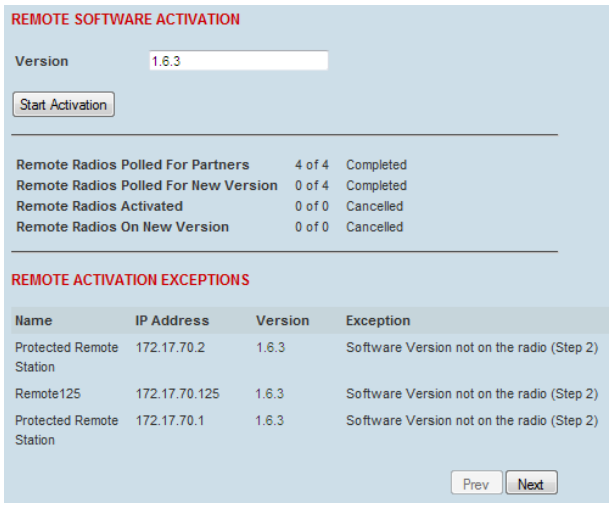
Result	Function (X of Y)
Remote Radios Polled for Partners	X is the number of radios polled to determine the number of protected stations in the network. Y is the number of remote radios registered with the base station.
Remote Radios Polled for New Version	X is the number of radios polled to determine 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:



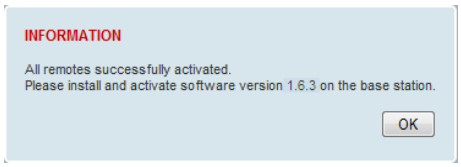
3. Click on 'OK' to start the activation process or Cancel to quit.

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 145).

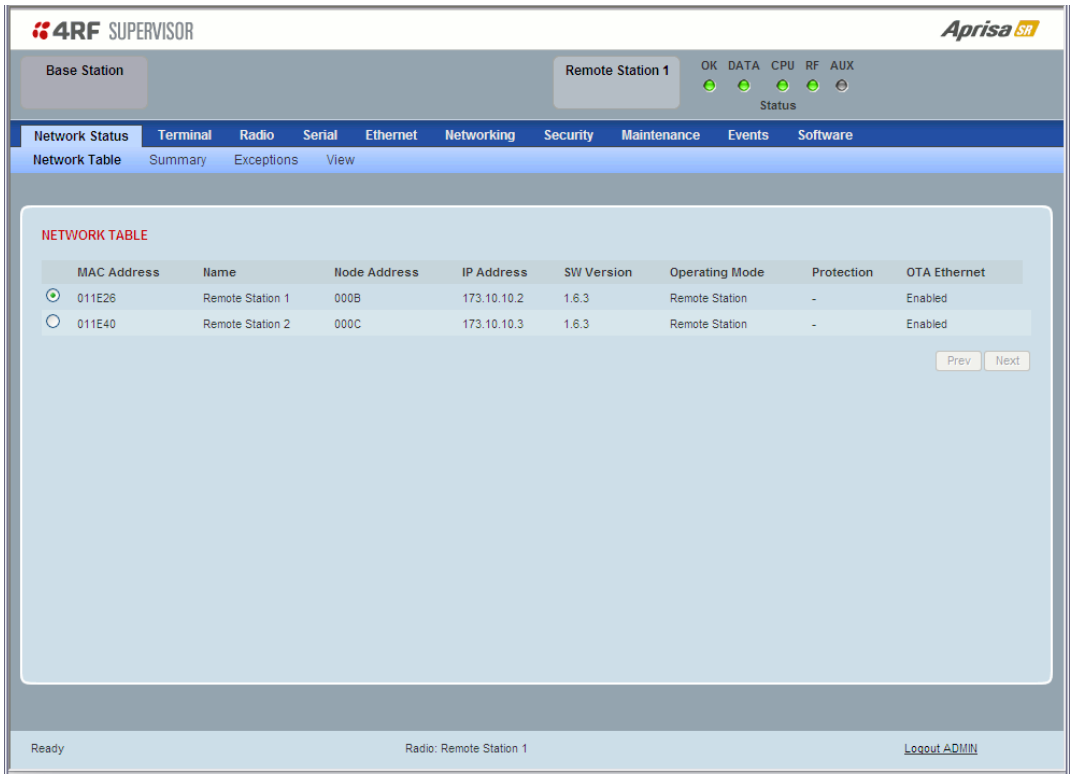


4. Click on ‘OK’ to start the activation on the base station.

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.

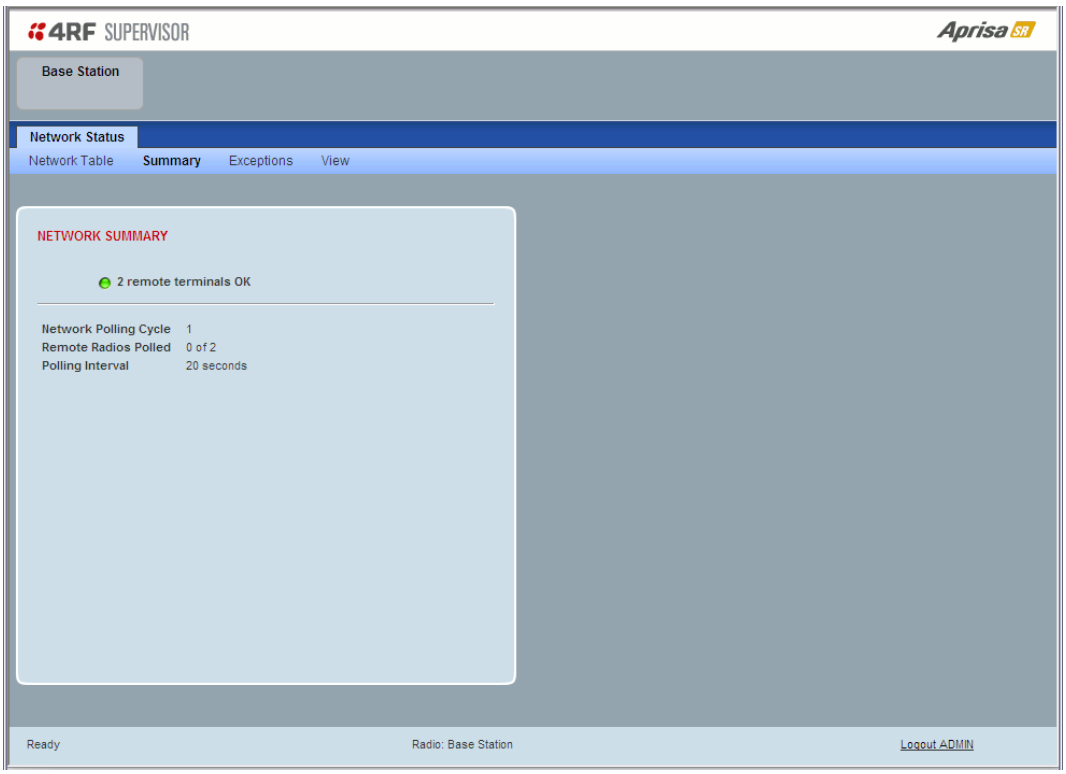
To manage a remote / repeater station with SuperVisor:

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.



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.

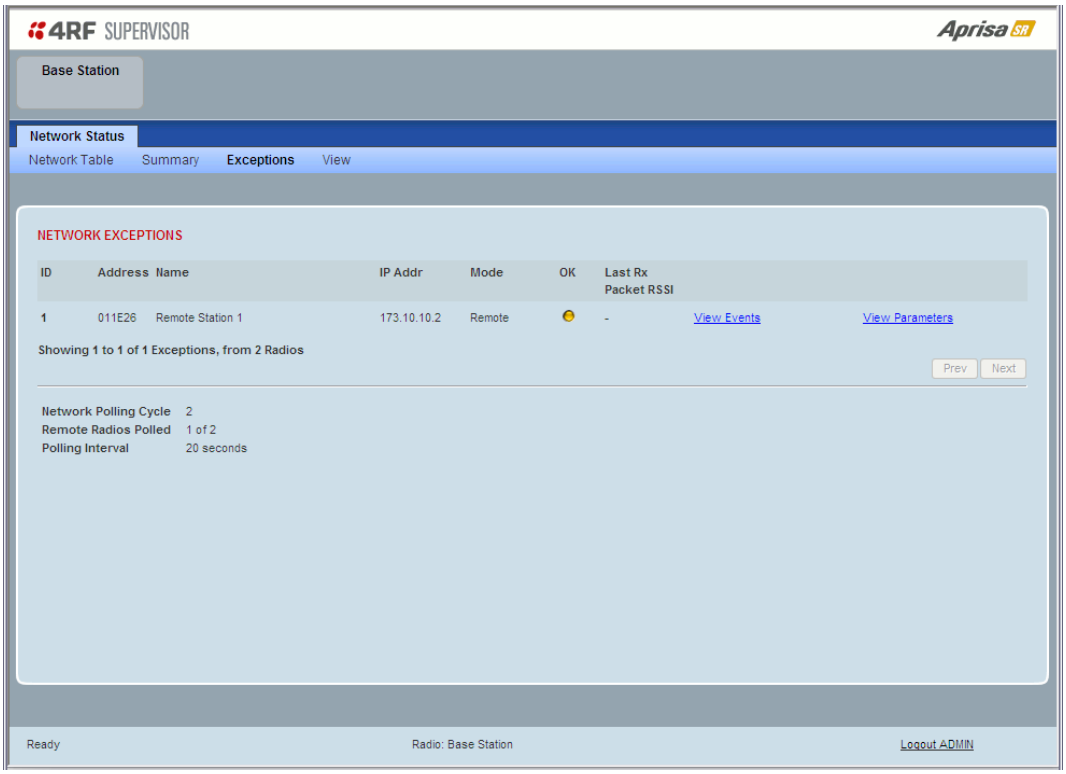
Network Summary Example:

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 120.

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 120.

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

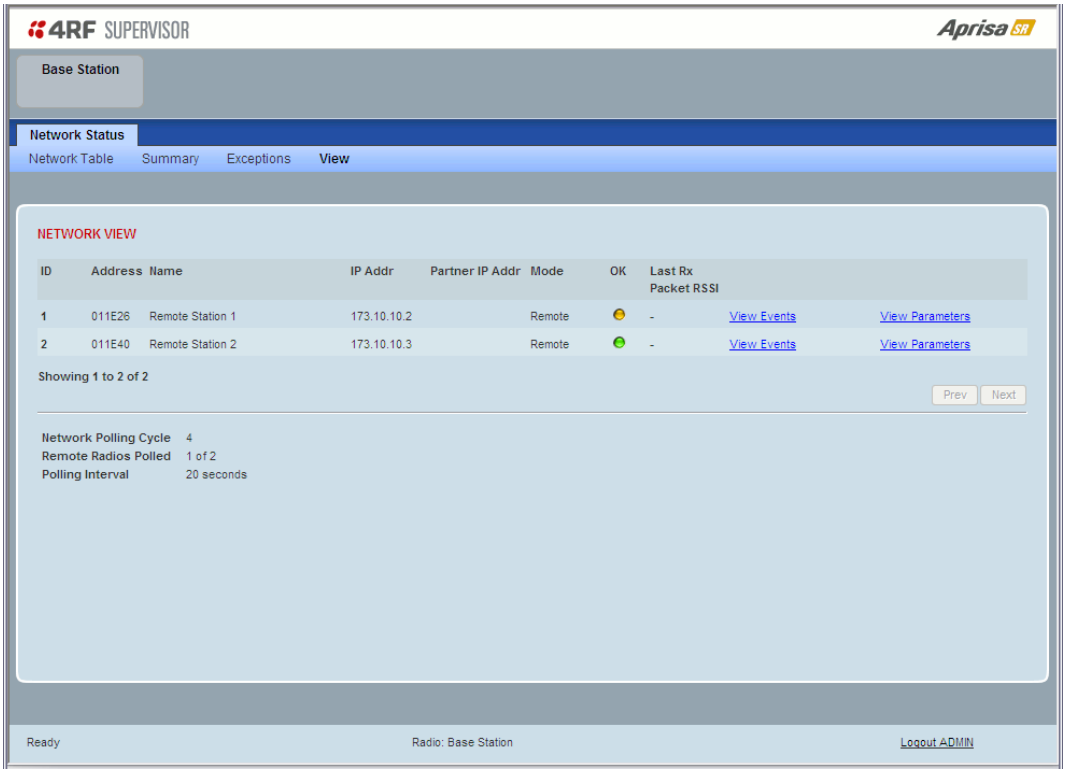
Clicking on View Events navigates to the Events page (see ‘Events’ on page 130) for the specific remote radio where the radio events will be displayed.

View Parameters

Clicking on View Parameters navigates to Terminal > Parameters page (see ‘Terminal > Parameters’ on page 73) 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 120. 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 130) for the specific remote radio where the radio events will be displayed.

View Parameters

Clicking on View Parameters navigates to Terminal > Parameters page (see 'Terminal > Parameters' on page 73) 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.

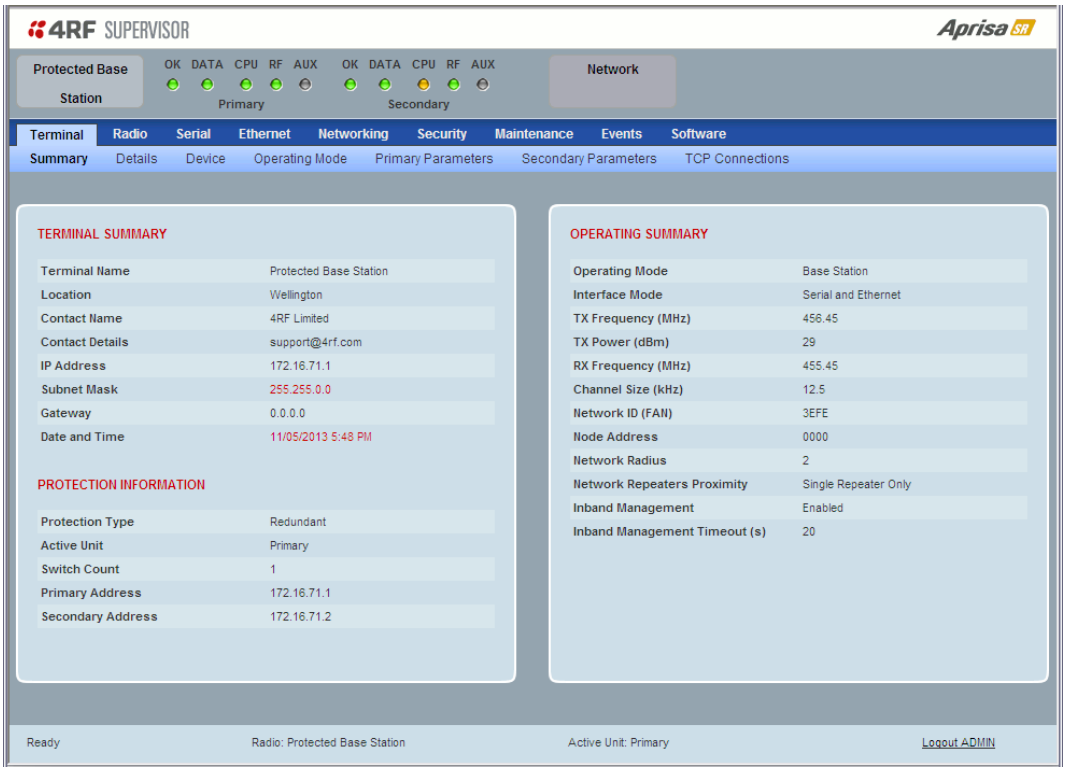
Parameter Errors

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 161 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.
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).

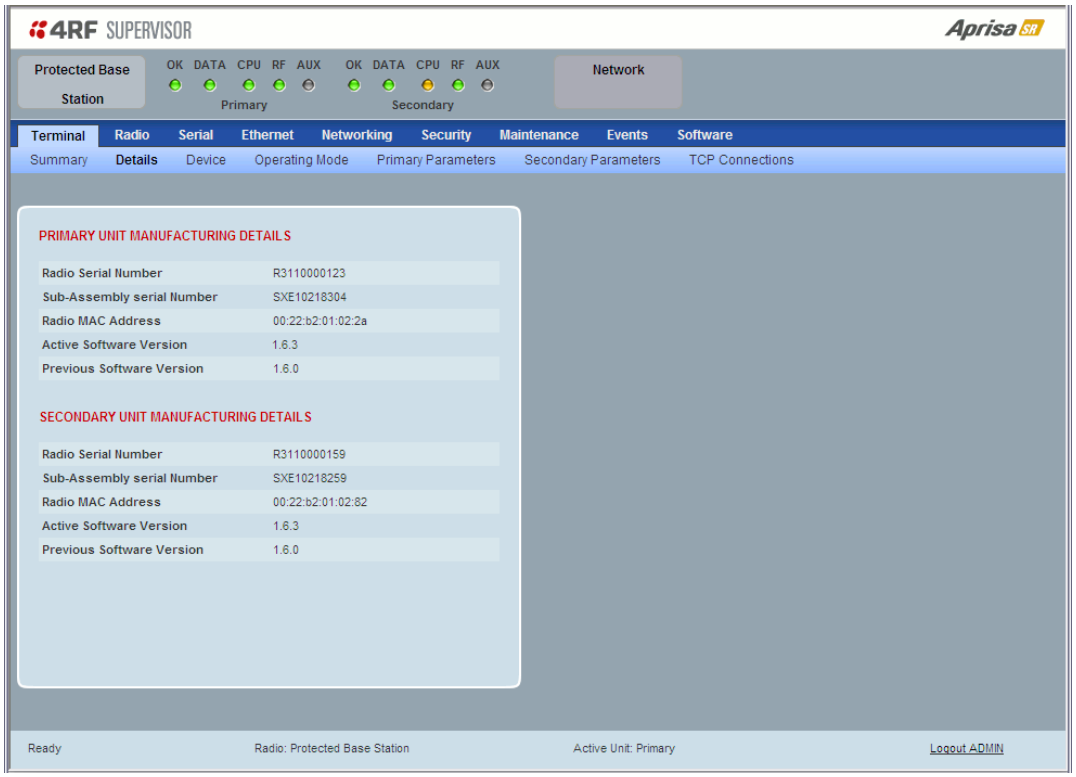
Secondary Address

This parameter shows the IP address of the secondary radio (usually the right side radio B).

OPERATING SUMMARY

See ‘Terminal > Summary’ on page 64 for parameter details.

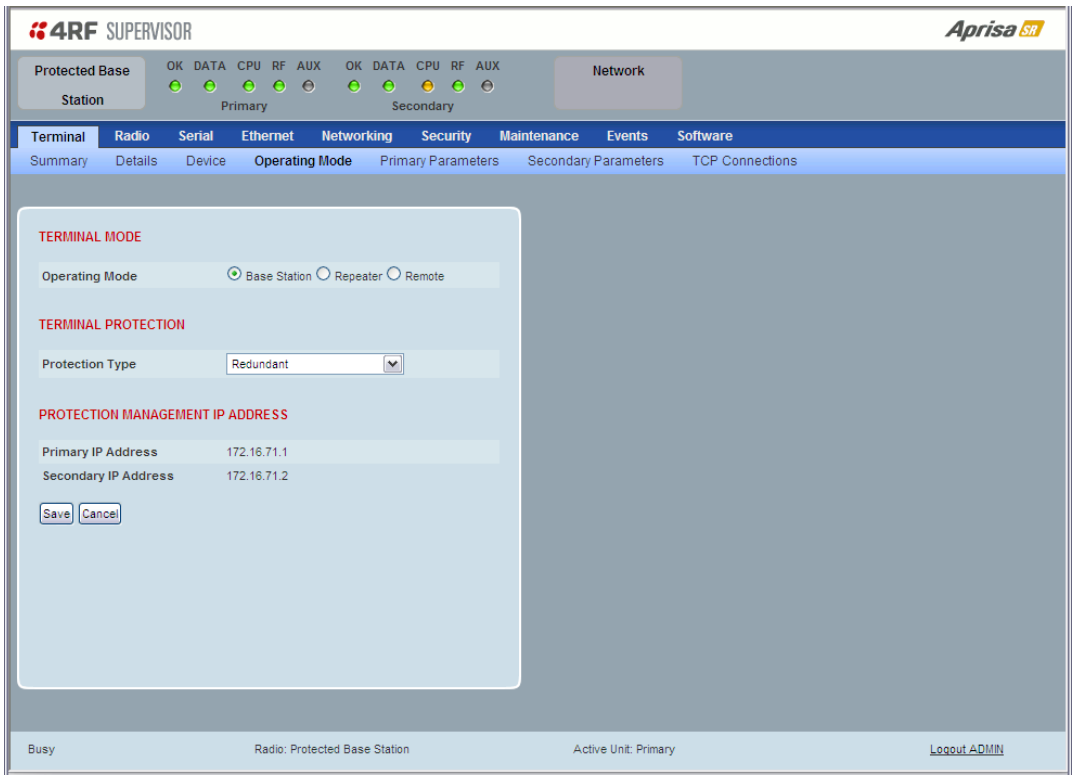
Protected Station: Terminal > Details



PRIMARY UNIT / SECONDARY UNIT MANUFACTURING DETAILS

See ‘Terminal > Details’ on page 66 for parameter settings.

Protected Station: Terminal > Operating Mode



TERMINAL MODE

Operating Mode

The Operating Mode can be set to base station, repeater station or remote station. The default setting is remote station.

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)	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
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.

PROTECTION MANAGEMENT IP ADDRESS

Primary Address

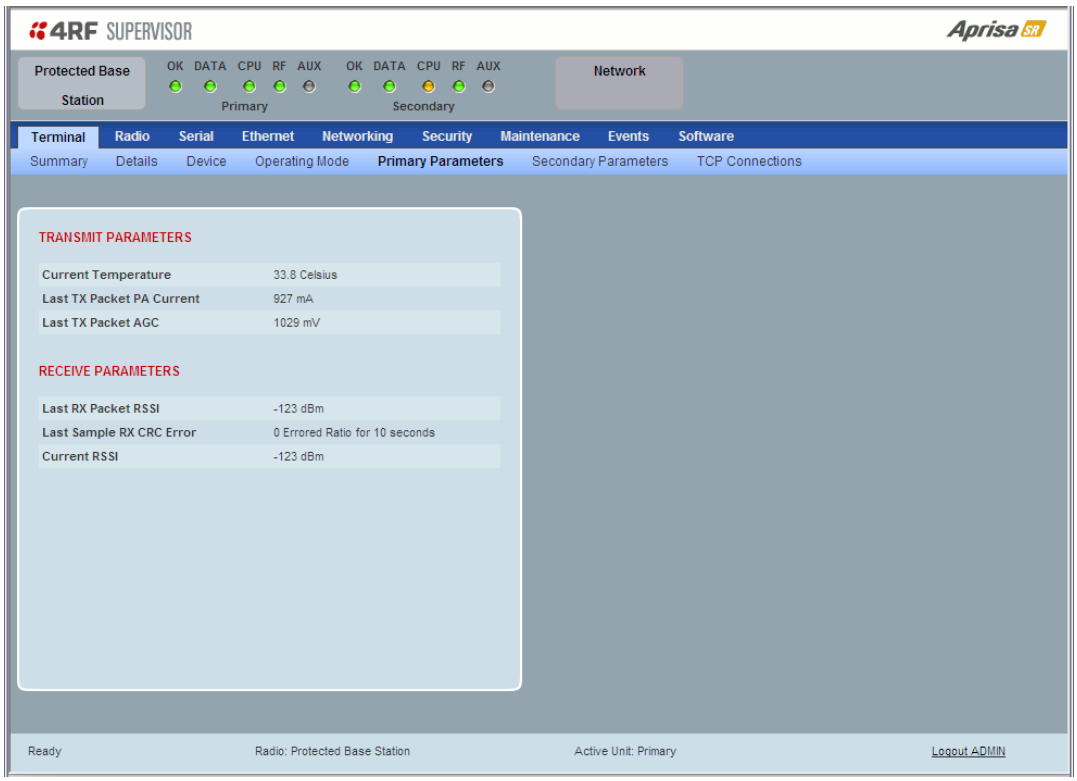
This parameter shows the IP address of the primary radio (usually the left side radio A).

Secondary Address

This parameter shows the IP address of the secondary radio (usually the right side radio B).

Protected Station: Terminal > Primary Parameters

The Parameters page is a dynamic page that will display the parameters associated with the active alarms, set on 'Events > Events Setup' on page 132. The screenshot below shows a small amount of monitored alarms as an example.



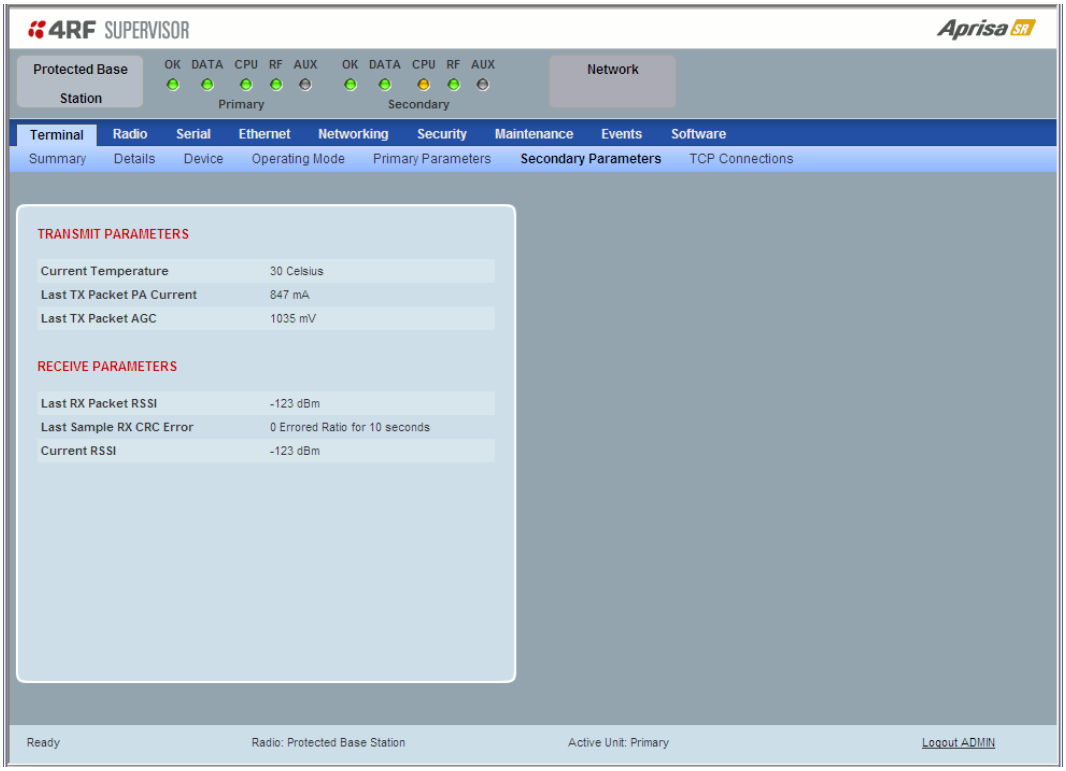
TRANSMIT / RECEIVE PARAMETERS

This parameter displays the parameters of the Primary radio.

See 'Terminal > Parameters' on page 73 for parameter details.

Protected Station: Terminal > Secondary Parameters

The Parameters page is a dynamic page that will display the parameters associated with the active alarms, set on 'Events > Events Setup' on page 132. The screenshot below shows a small amount of monitored alarms as an example.



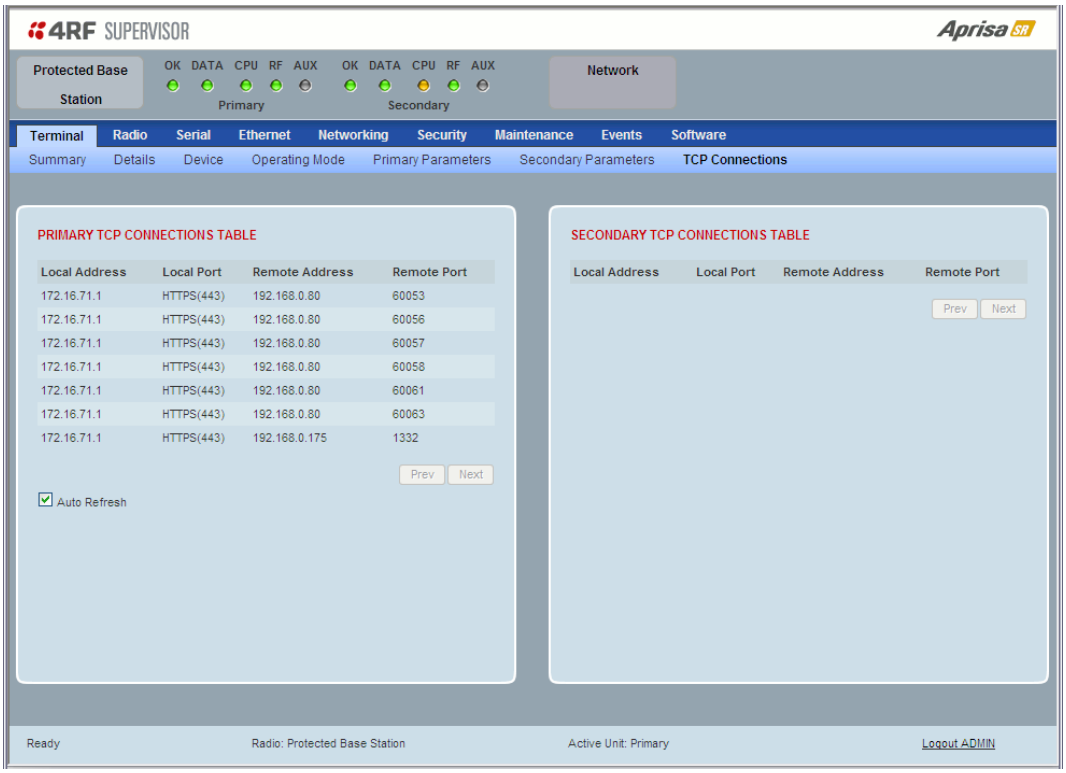
TRANSMIT / RECEIVE PARAMETERS

This parameter displays the parameters of the Secondary radio.

See 'Terminal > Parameters' on page 73 for parameter details.

Protected Station: Terminal > TCP Connections

The TCP Connections page displays the list of active TCP connections on the radio.



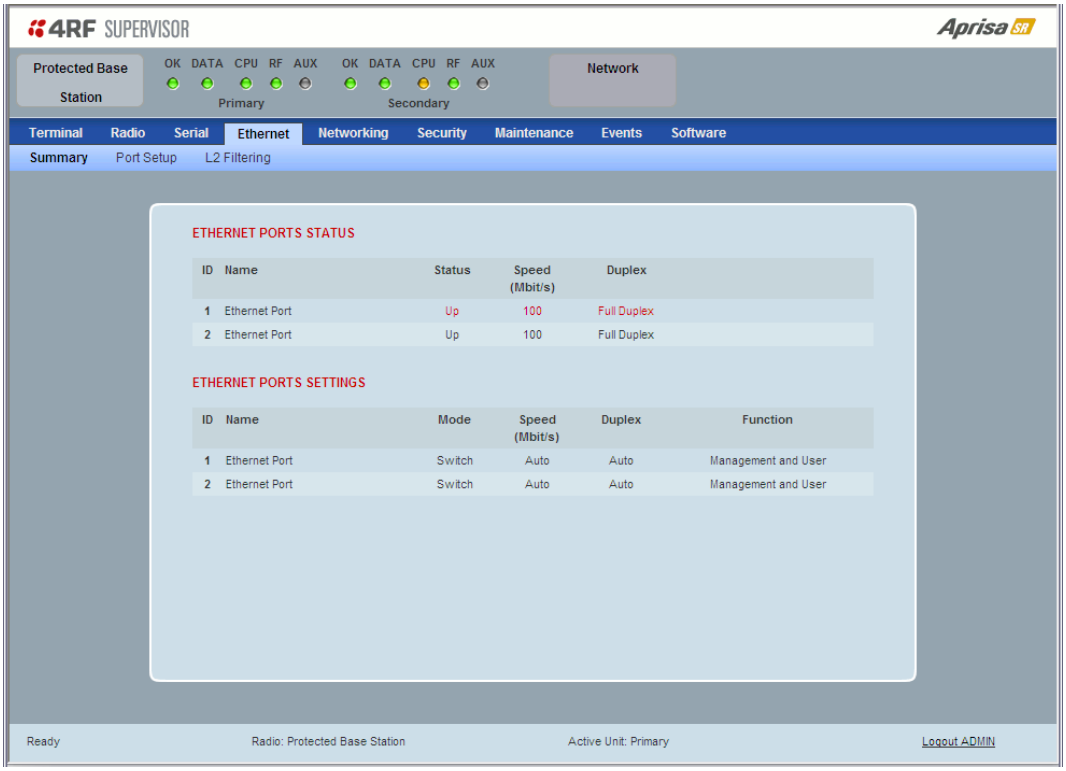
PRIMARY / SECONDARY TCP CONNECTIONS TABLE

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.

Protected Station: Ethernet > Summary

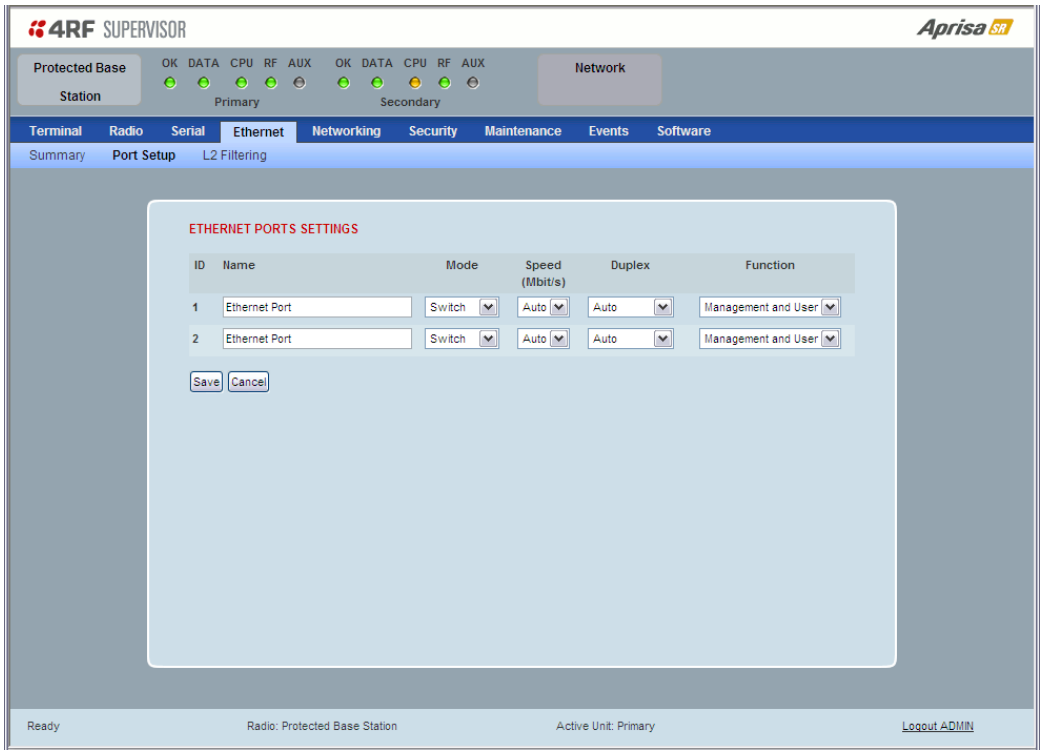
This page displays the current settings for the Protected Station Ethernet port parameters.



See ‘Protected Station: Ethernet > Port Setup’ for configuration options.

Protected Station: Ethernet > Port Setup

This page provides the setup for the Protected Station Ethernet ports settings.



ETHERNET PORT SETTINGS

Mode

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

Option	Function
Standard	Enables Ethernet data communication over the radio link.
Switch	Ethernet traffic is switched locally between the two Ethernet ports and communicated over the radio link
Disabled	Disables Ethernet data communication over the radio link.

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

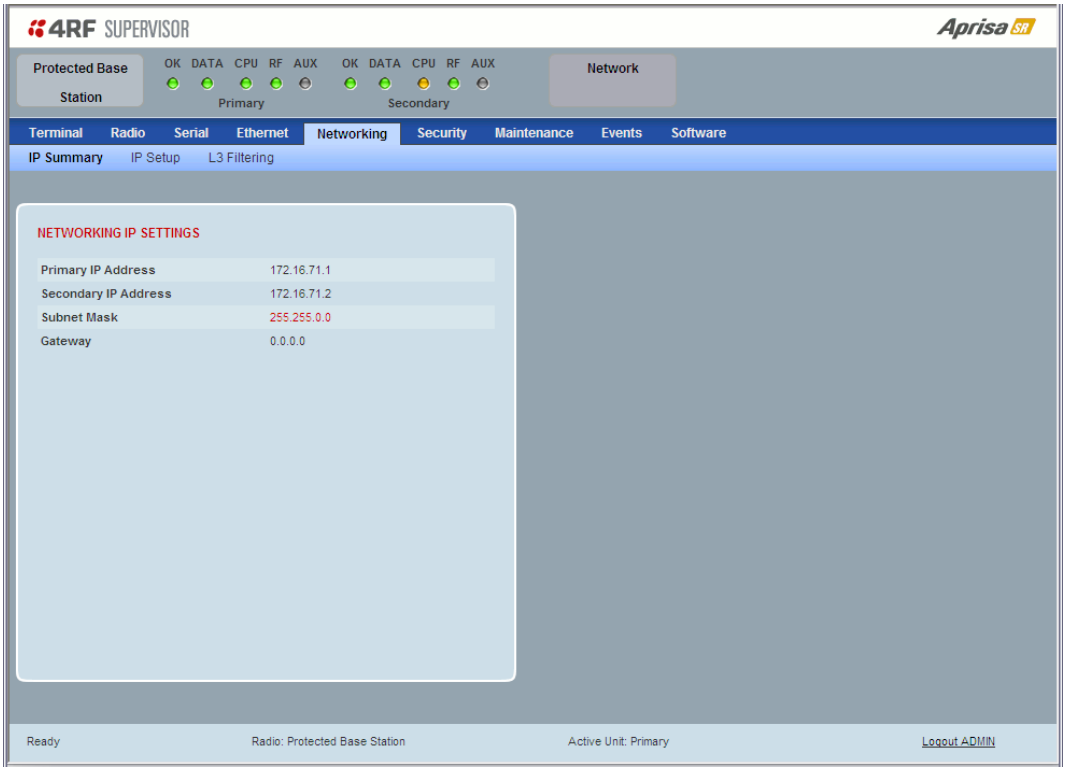
Function

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.

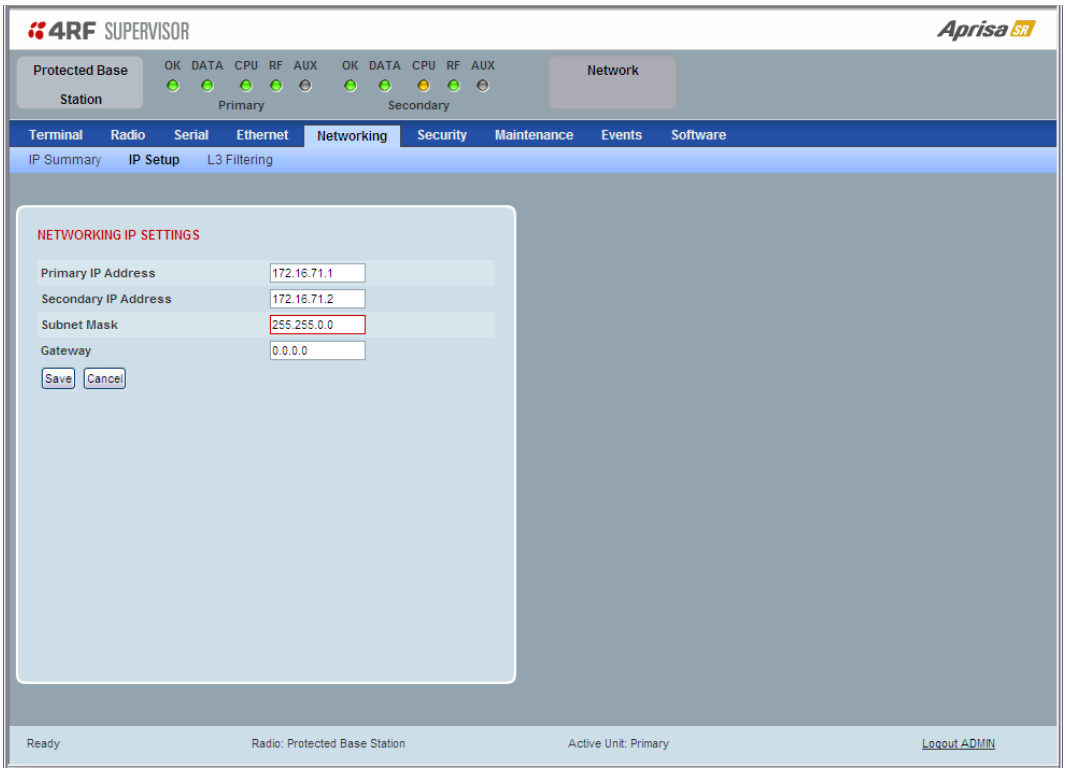
Protected Station: Networking > IP Summary

This page displays the current settings for the Protected Station Networking IP settings.



Protected Station: Networking > 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.

Subnet Mask

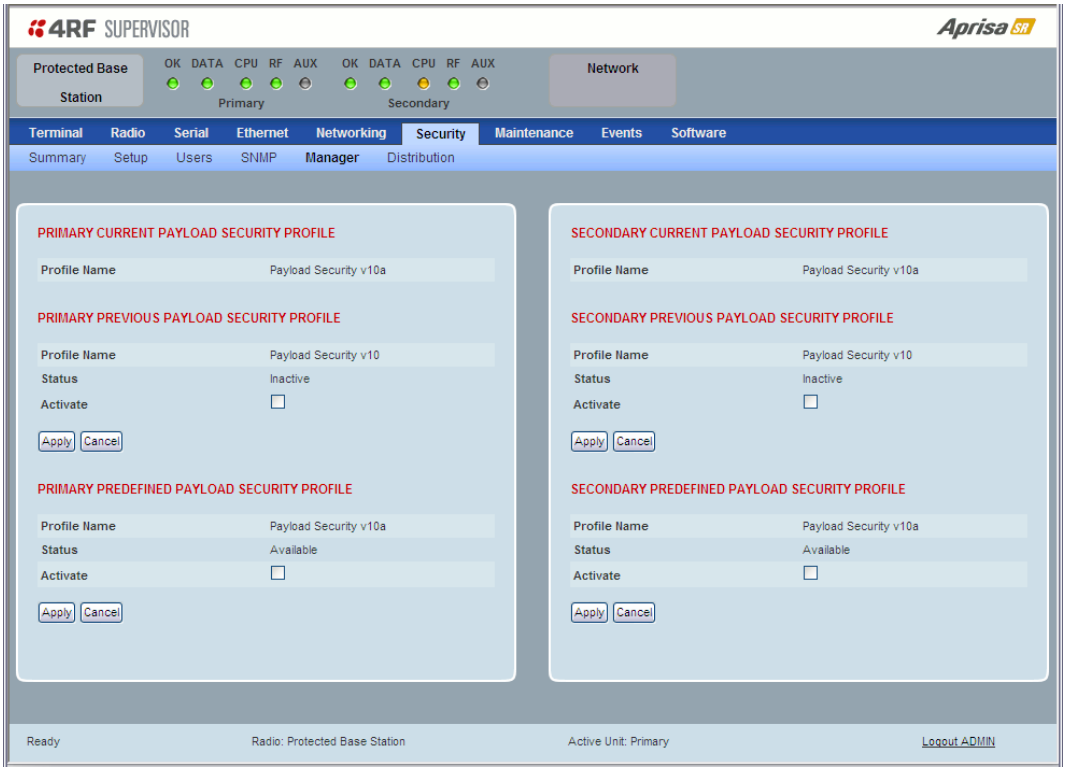
Set the Subnet Mask of the radio using the standard format xxx.xxx.xxx.xxx. The default subnet mask is 255.255.0.0.

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.

Protected Station: Security > Manager

This page provides the management and control of the Protected Station Networking Security settings.

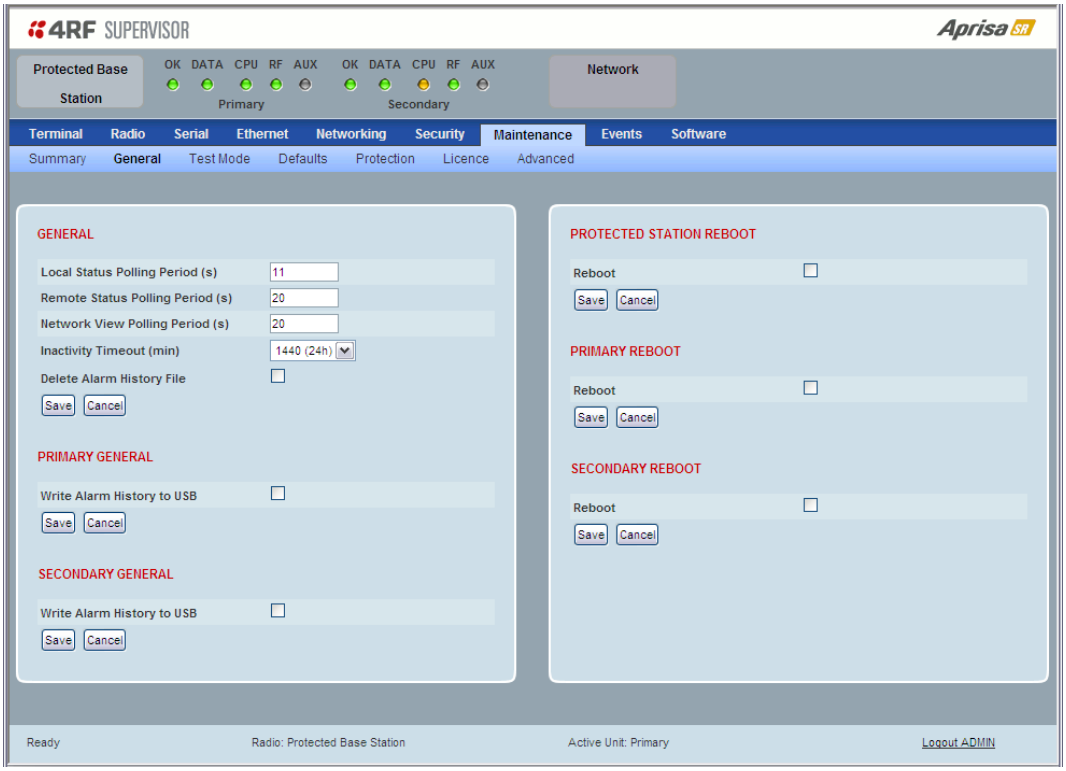


PRIMARY / SECONDARY SECURITY PROFILE

See ‘Security > Manager’ on page 112 for parameter details.

Protected Station: Maintenance > General

This page provides the management and control of the Protected Station Maintenance General settings.

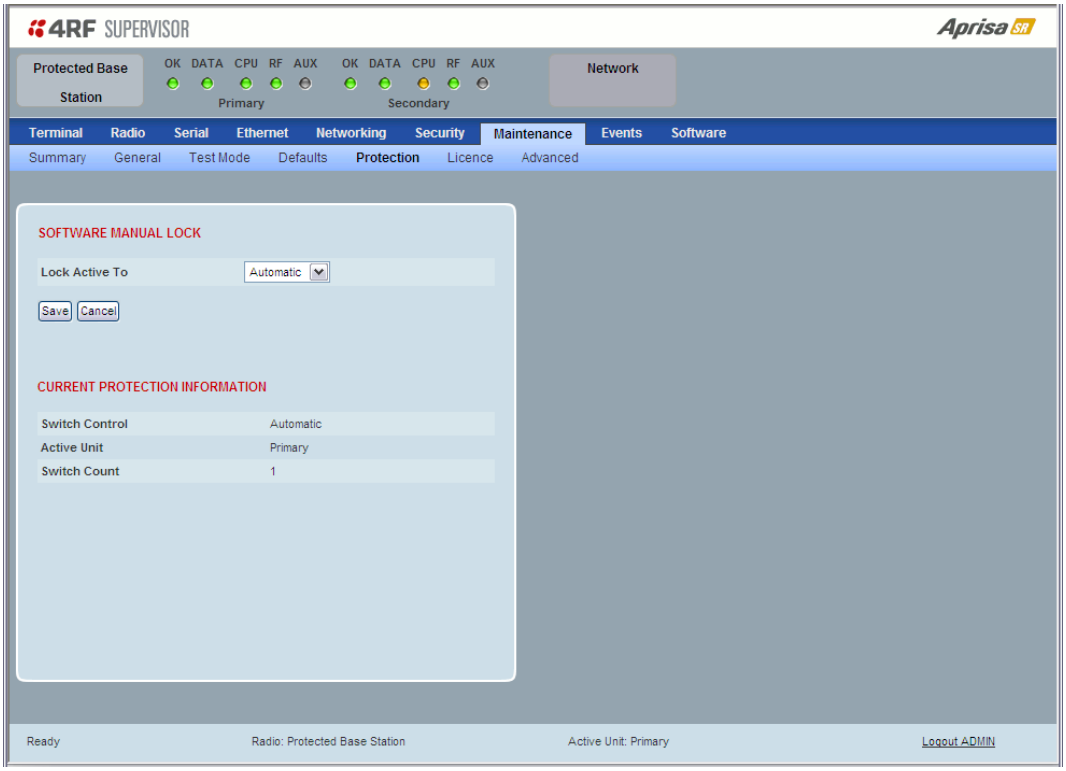


See ‘Maintenance > General’ on page 120 for parameter details.

Maintenance

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.

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

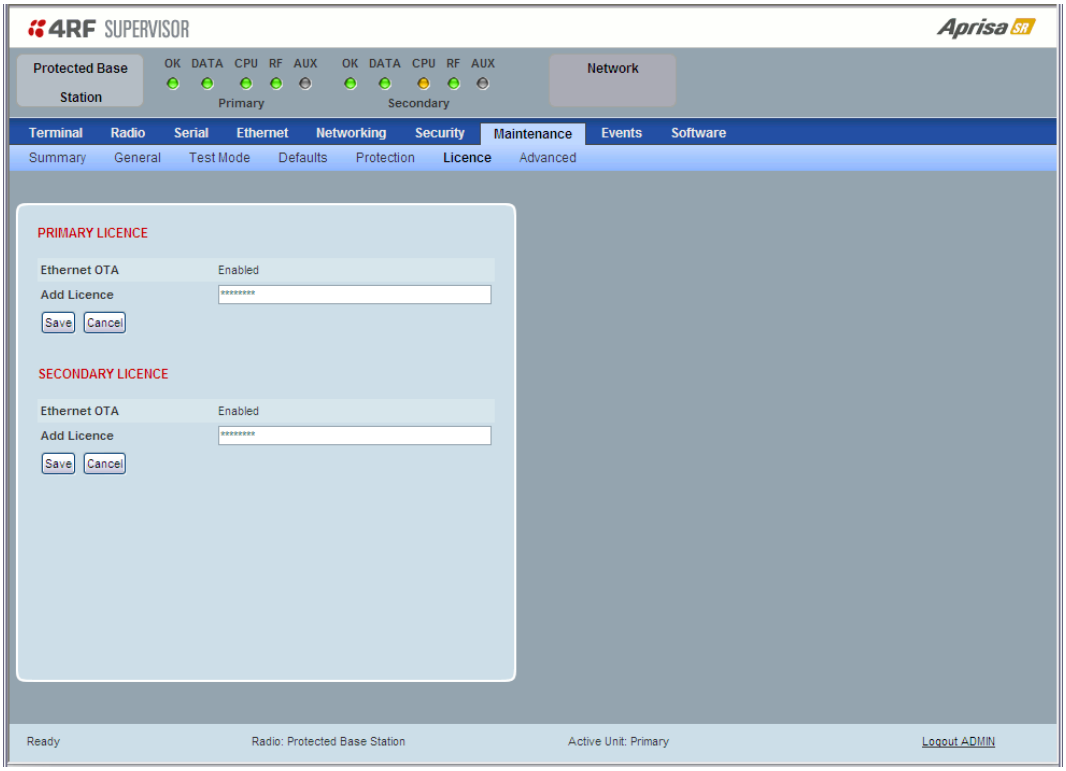
This parameter shows the radio which is currently active (Primary or Secondary).

Switch Count

This parameter shows the number of protection switch-overs since the last radio reboot (volatile).

Protected Station: Maintenance > Licence

This page provides the management and control of the Protected Station Maintenance Licence settings.

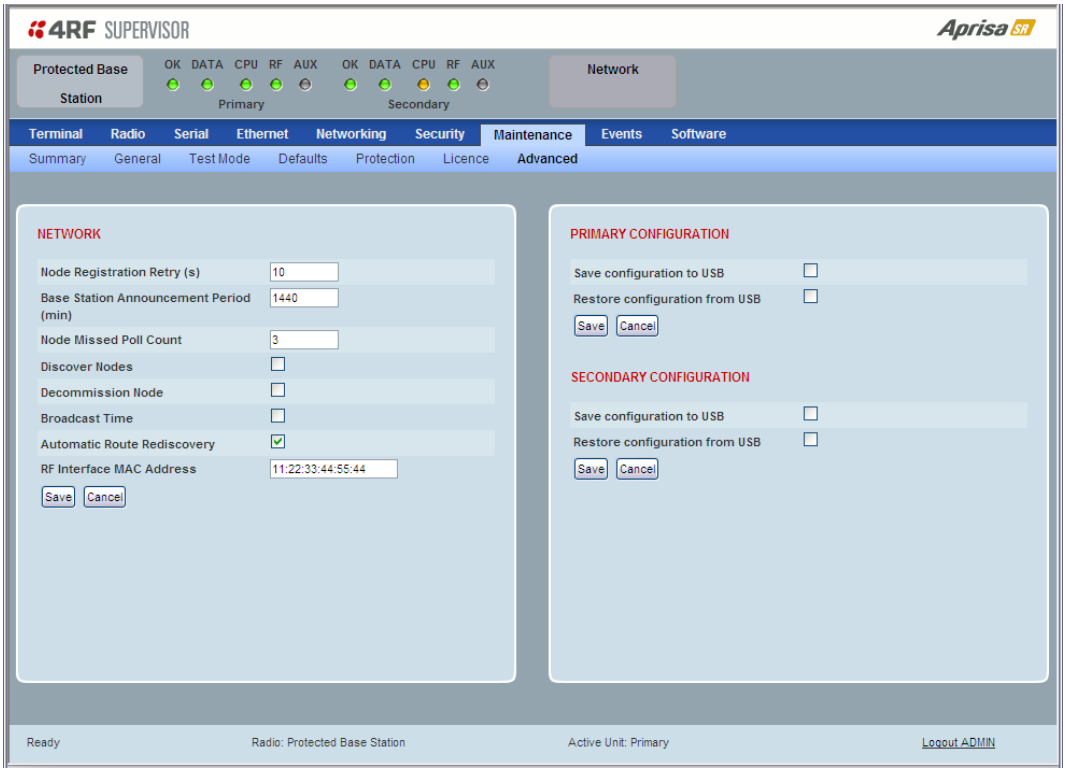


PRIMARY / SECONDARY LICENCE

See ‘Maintenance > Licence’ on page 126 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 127 for parameter details.

PRIMARY / SECONDARY CONFIGURATION

See ‘Maintenance > Advanced’ on page 127 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:

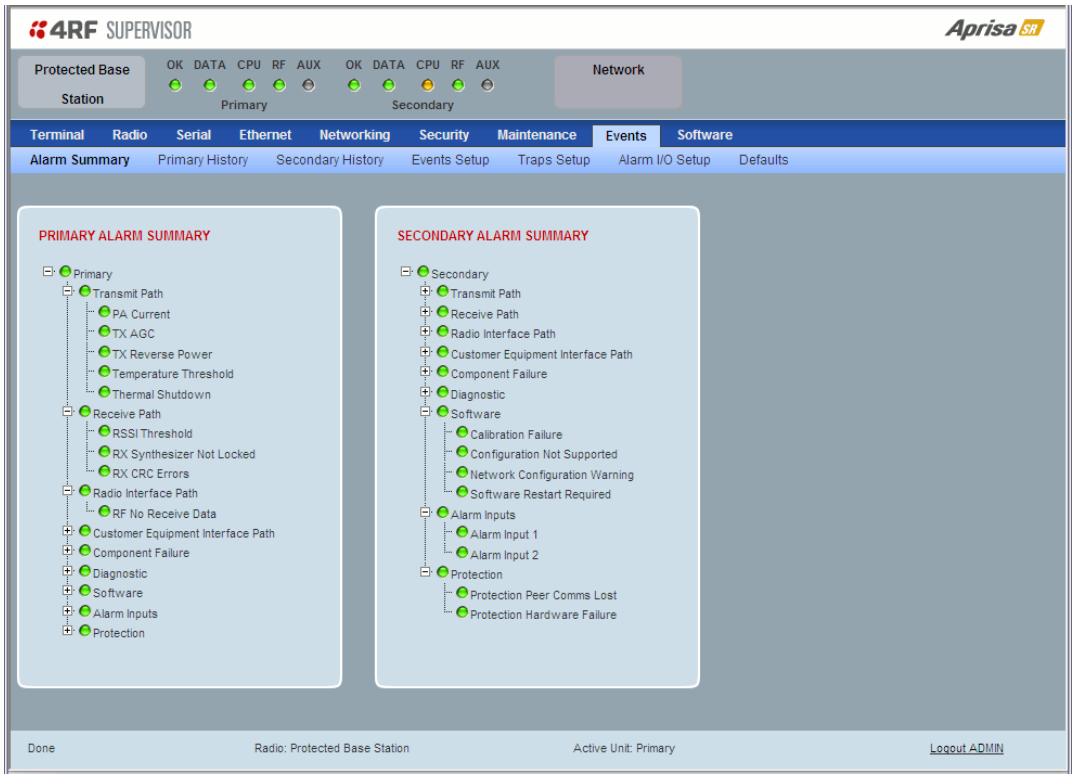
1. Alarm Events

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.

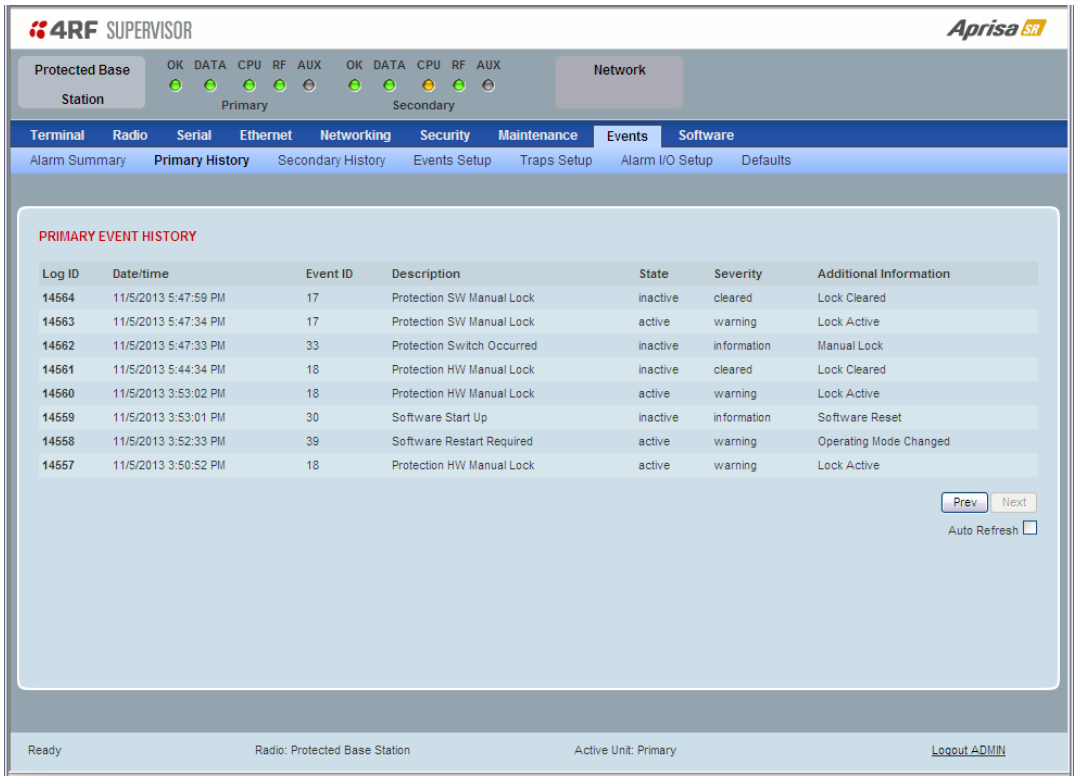
See ‘Alarm Types and Sources’ on page 230 for a complete list of events.



PRIMARY / SECONDARY ALARM SUMMARY

See ‘Events > Alarm Summary’ on page 130 for parameter details.

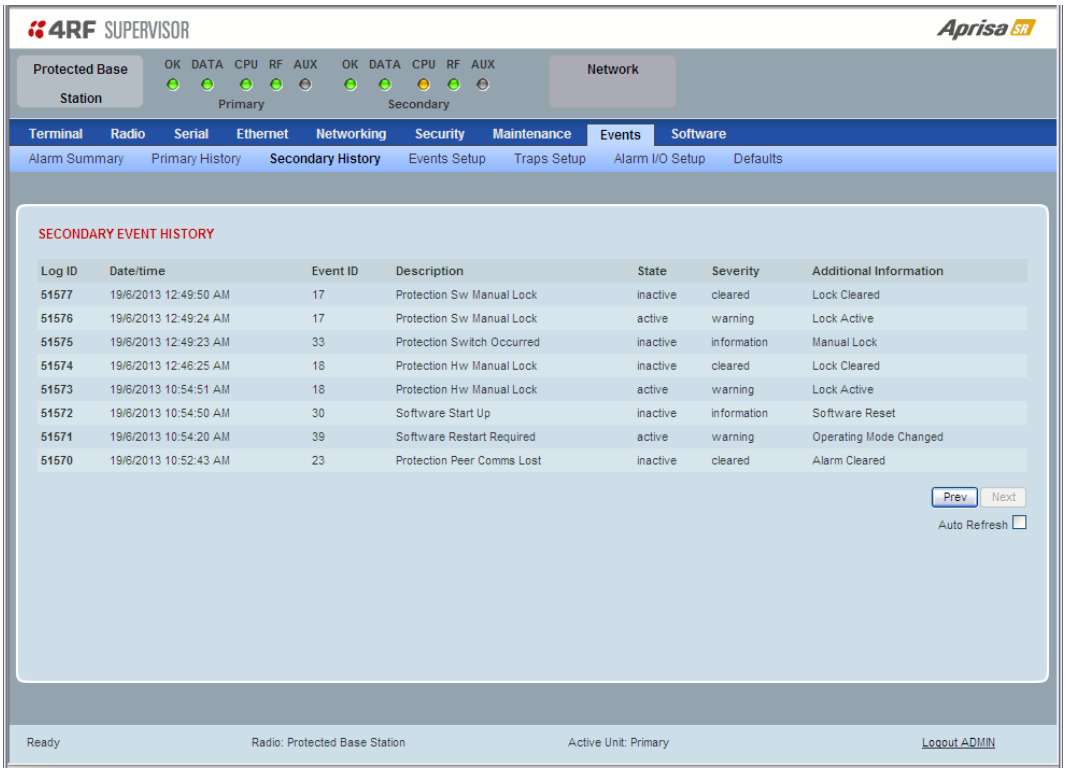
Protected Station: Events > Primary History



PRIMARY EVENT HISTORY

See ‘Events > Event History’ on page 131 for parameter details.

Protected Station: Events > Secondary History



SECONDARY EVENT HISTORY

See ‘Events > Event History’ on page 131 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 225). This process would only be used if the radio was a replacement or a new station in an existing network.

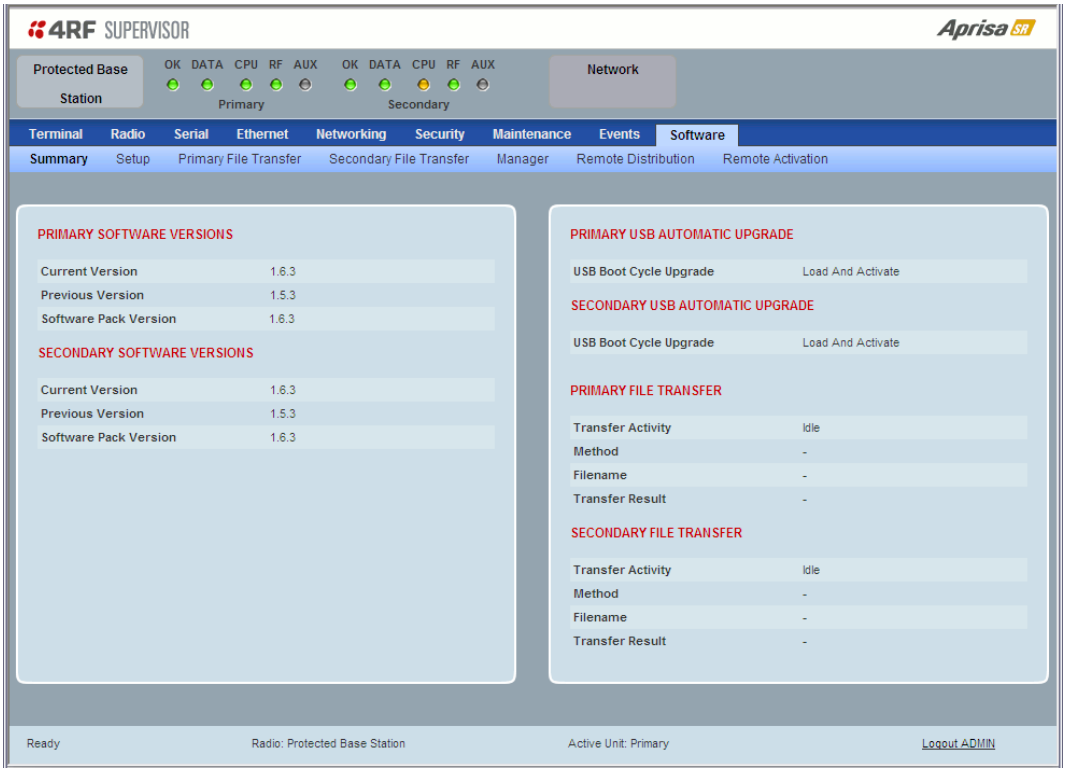
Network Software Upgrade

The radio software can be upgraded on an entire Aprisa SR radio network remotely over the radio link (see ‘Network Software Upgrade’ on page 224). 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.

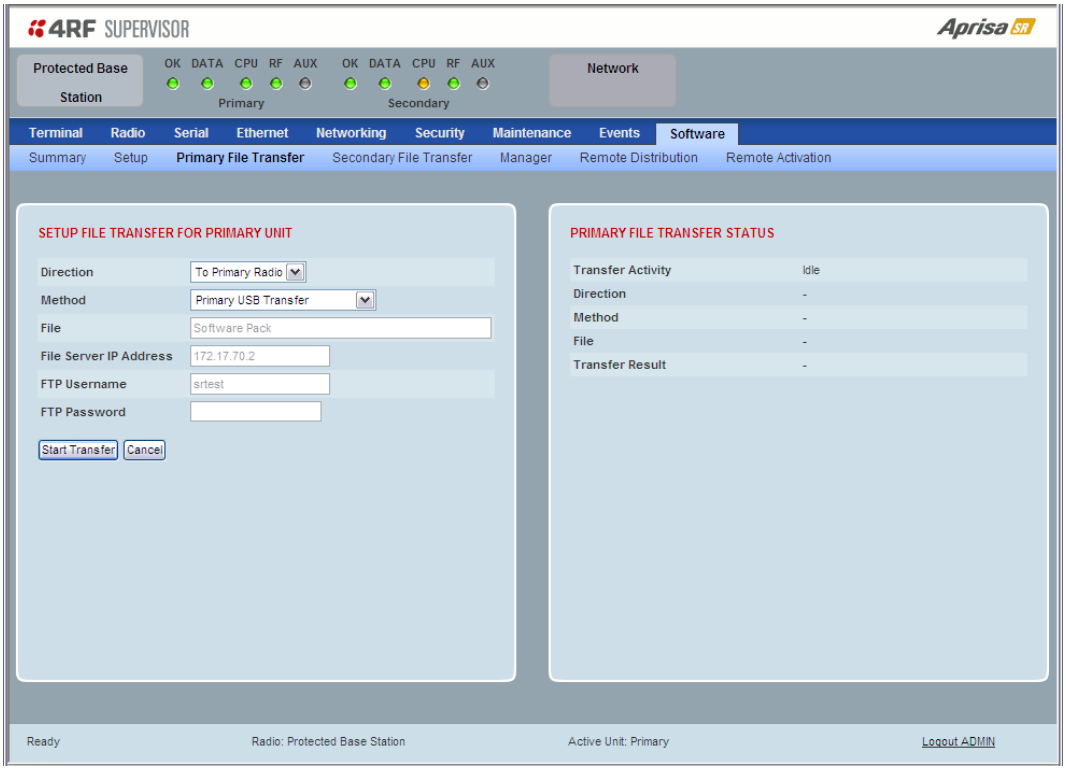


PRIMARY / SECONDARY SOFTWARE VERSIONS

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.
Transfer from Secondary Unit	Transfers the software from the secondary radio to the primary radio.

PRIMARY FILE TRANSFER STATUS

See 'Software > File Transfer' on page 142 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 141), 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 191 to activate the Software Pack. The radio will reboot automatically.

FTP Method

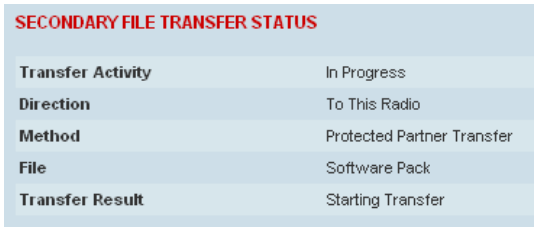
1. Unzip the software release files in to a temporary directory.
2. Open the FTP server and point it to the temporary directory.
3. Enter the FTP server IP address, Username and password into SuperVisor.
4. Click on 'Start Transfer'.

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 191 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’.

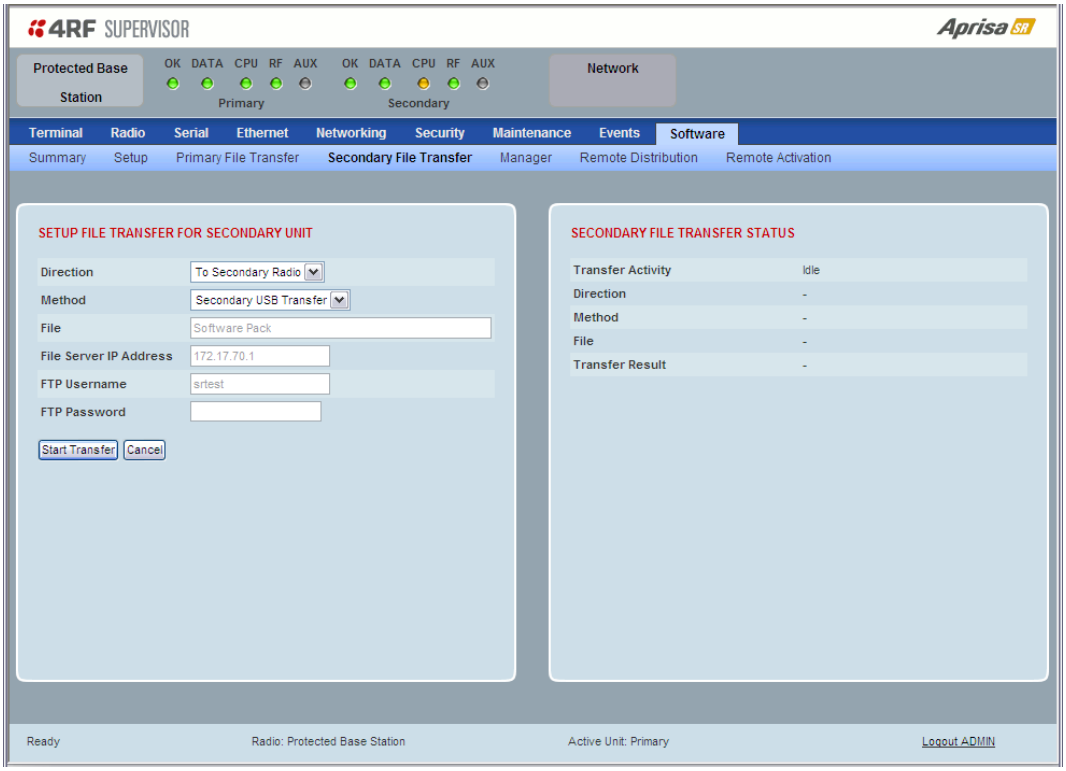


3. Go to ‘Protected Station: Software > Manager’ on page 191 to activate the Software Pack. The radio will reboot automatically.

If the file transfer fails, check the Event History page (see ‘Protected Station: Events > Secondary History’ on page 182) 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.
Transfer from Primary Unit	Transfers the software from the primary radio to the secondary radio.

SECONDARY FILE TRANSFER STATUS

See 'Software > File Transfer' on page 142 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 141), 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 191 to activate the Software Pack. The radio will reboot automatically.

FTP Method

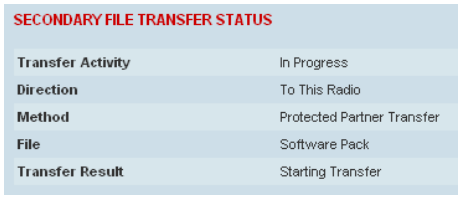
1. Unzip the software release files in to a temporary directory.
2. Open the FTP server and point it to the temporary directory.
3. Enter the FTP server IP address, Username and password into SuperVisor.
3. Click on 'Start Transfer'.

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 191 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’.



3. Go to ‘Protected Station: Software > Manager’ on page 191 to activate the Software Pack. The radio will reboot automatically.

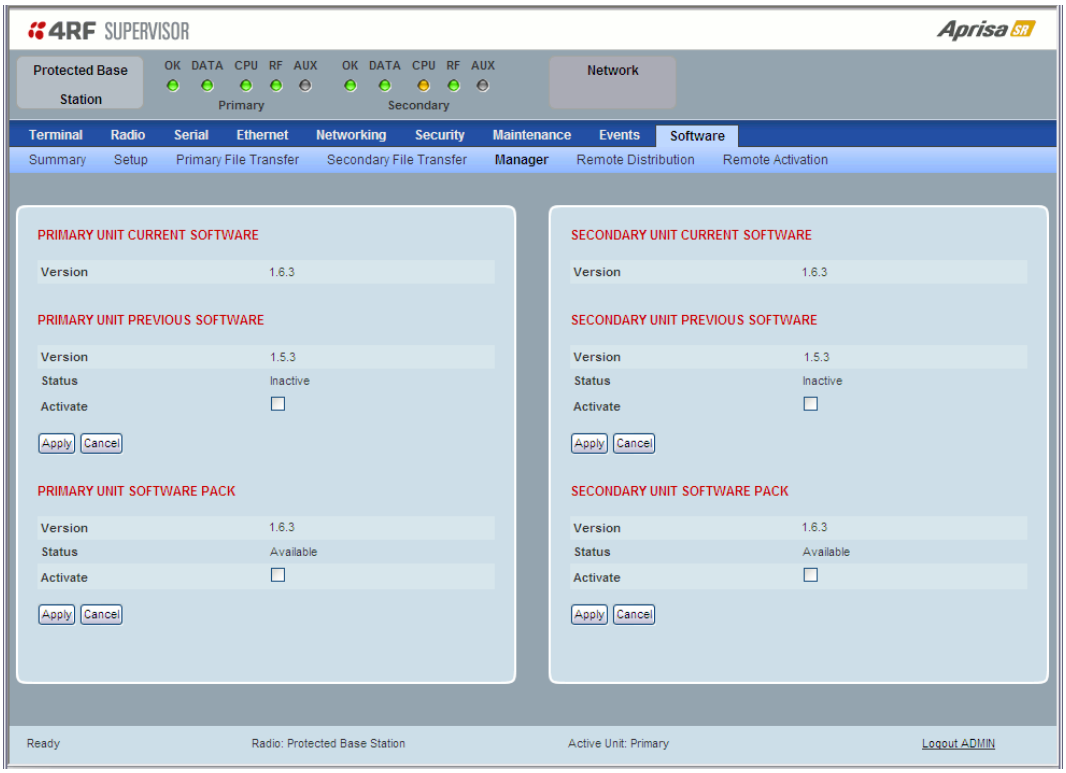
If the file transfer fails, check the Event History page (see ‘Protected Station: Events > Primary History’ on page 181) for more details of the transfer.

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

This parameter activates the software pack.

The Aprisa SR will automatically reboot after activation.

Protected Station: Software > Remote Distribution

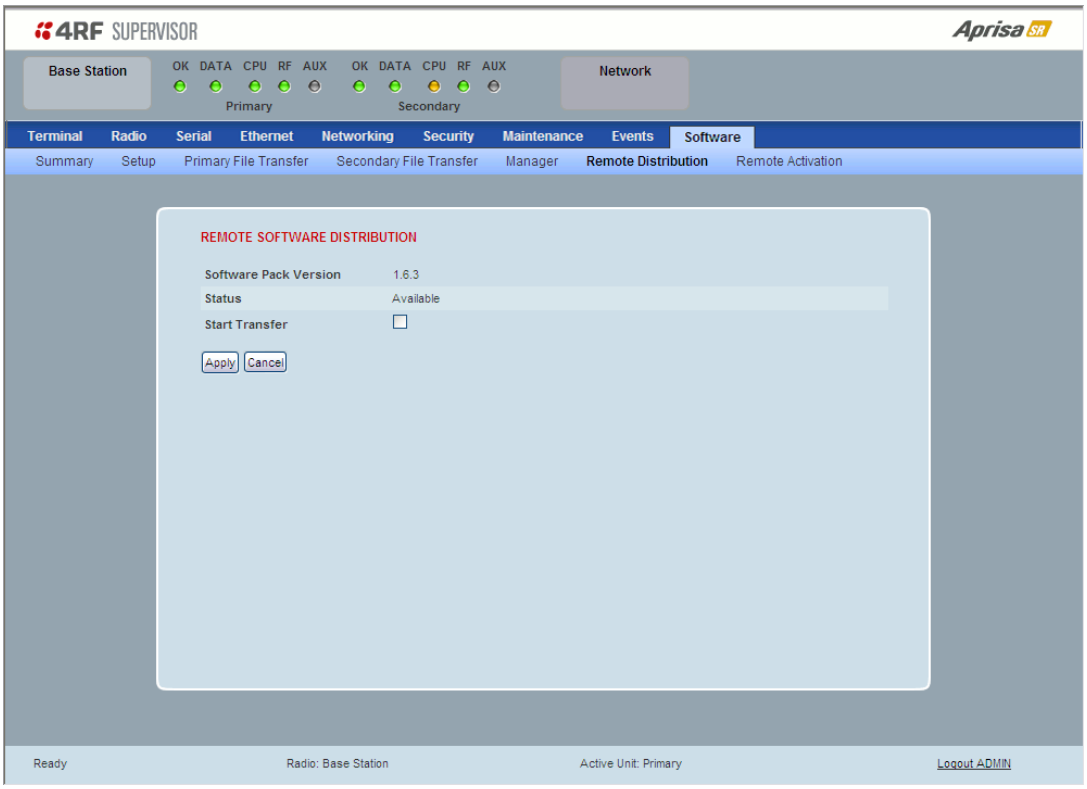
This page provides the mechanism to distribute software to all remote protected stations into the Aprisa SR network (network) and then activate it.

The Software Pack loaded into the base station with the file transfer process (see 'Protected Station: Software > Primary File Transfer' on page 185) 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.

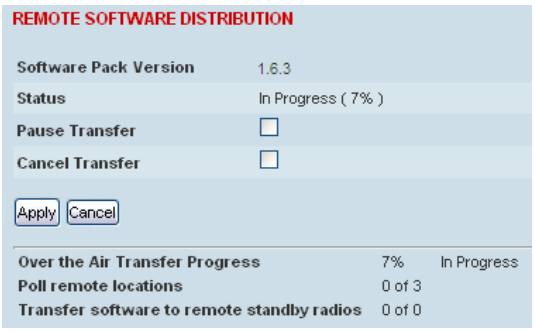
Note: The distribution of software to remote stations does not stop customer traffic from being transferred. However, due to the volume of traffic, the software distribution process may affect customer traffic.

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 185).

1. To ensure that the Network Table is up to date, it is recommended running the node discover function (see 'Discover Nodes' on page 128).
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

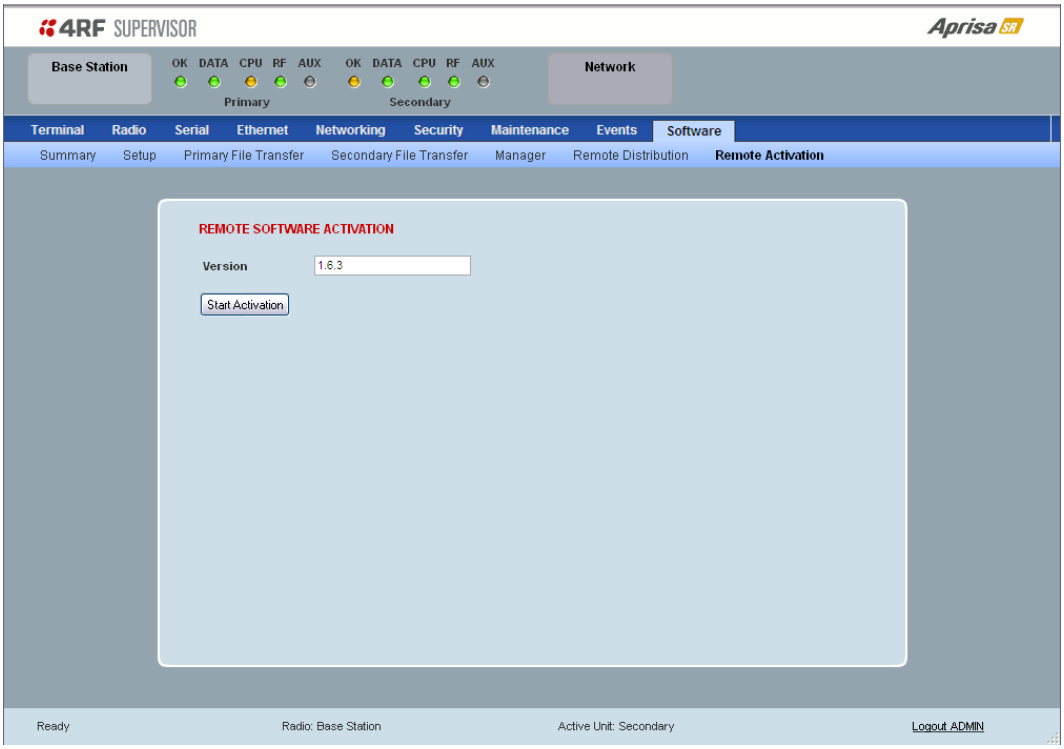
This page provides the mechanism to activate software on all remote protected stations.

The Software Pack has been loaded into the base station with the file transfer process (see 'Protected Station: Software > Primary File Transfer' on page 185) 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'.

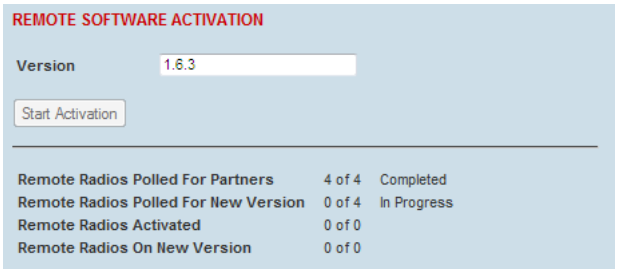
To activate software in remote stations:

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 142) 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).

---

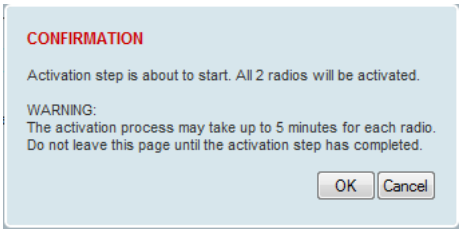
1. Enter the Software Pack version (if different from displayed version).
2. Click on 'Start Activation'.



The remote stations will be polled to determine which radios require activation:

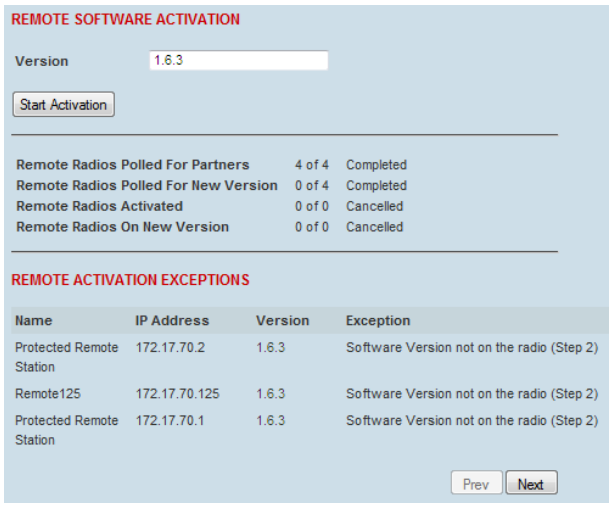
Result	Function (X of Y)
Remote Radios Polled for Partners	X is the number of radios polled to determine the number of protected stations in the network. Y is the number of remote radios registered with the base station.
Remote Radios Polled for New Version	X is the number of radios polled to determine 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:



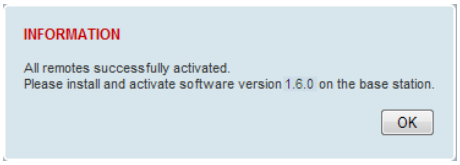
3. Click on 'OK' to start the activation process or Cancel to quit.

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 145).



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.

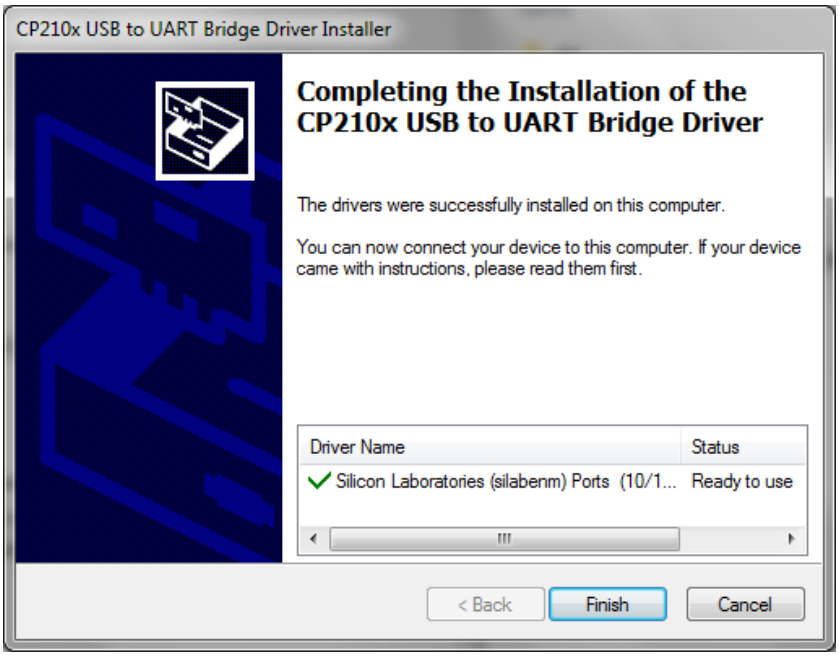
You can password-protect the Command Line Interface to prevent unauthorized users from modifying radio settings.

This interface can be accessed via an Ethernet Port (RJ45) or the Management Port (USB micro type B).

Connecting to the Management Port

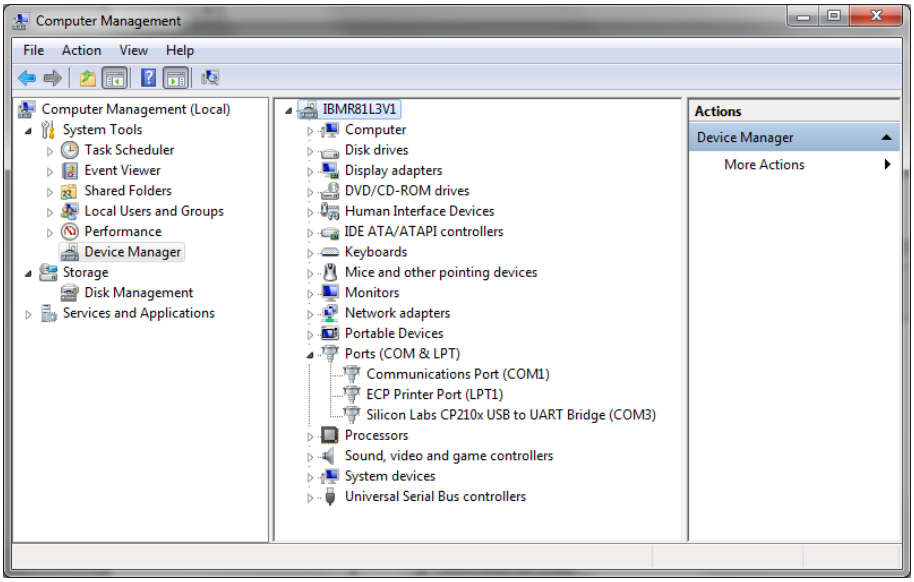
A USB Cable USB A to USB micro B, 1m is provided with each radio.

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 and install the USB Serial Driver CP210x_VCP_Win2K_XP_S2K3.zip on your computer. This file is on the Information and setup CD supplied with the radio.



3. Go to your computer device manager (Control Panel > System > Hardware > Device Manager)
4. Click on 'Ports (COM & LPT)'

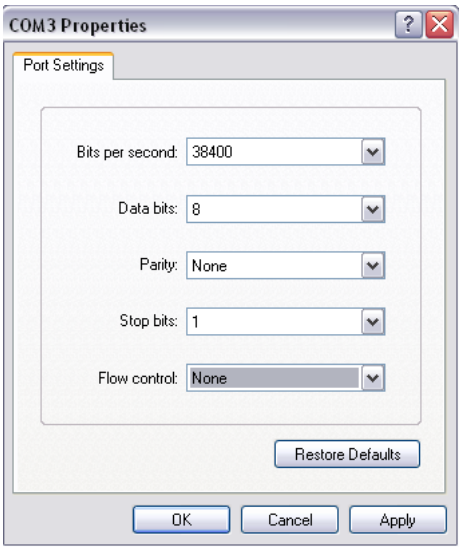
5. Make a note of the COM port which has been allocated to the 'Silicon Labs CP210x USB to UART Bridge' (COM3 in the example below)



6. Open HyperTerminal Session (Start > All Programs > Accessories > Communications > HyperTerminal)
7. Enter a name for the connection (Aprisa SR CLI for example) and click OK.

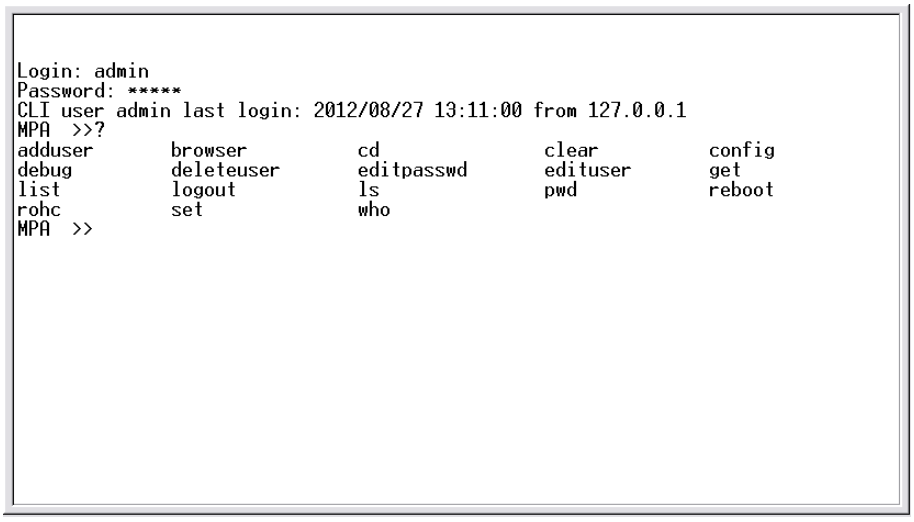
8. Select the COM port from the Connect Using drop-down box that was allocated to the UART USB.

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 MIB 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 v]
who	Shows the users currently logged into the radio

Viewing the CLI Terminal Summary

At the command prompt, type:

MPA >>cd APRISASR-MIB-4RF

MPA APRISASR-MIB-4RF >>ls Terminal

```
MPA APRISASR-MIB-4RF >>ls Terminal
+-----------------------------------------------------------+
|S.NO|ATTRIBUTE NAME                 |ATTRIBUTE VALUE       |
+-----------------------------------------------------------+
|1   |termName                       |Base Station          |
|2   |termLocation                   |Wellington            |
|3   |termContactName                |4RF Communications Ltd|
|4   |termContactDetails             |support@4rf.com       |
|5   |termTimeFormat                 |time24h (1)           |
|6   |termDateFormat                 |ddmmyyyy (1)          |
|7   |termDateTime                   |2011-1-1,15:21:21.0   |
|8   |termEthController1IpAddress    |172.17.10.2           |
|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                     |
+-----------------------------------------------------------+

MPA APRISASR-MIB-4RF >>
```

Changing the Radio IP Address with the CLI

At the command prompt, type ‘set termEthController1IpAddress xxx.xxx.xxx.xxx’

```
MPA APRISASR-MIB-4RF >>ls Terminal
+-----------------------------------------------------------+
|S.NO|ATTRIBUTE NAME                 |ATTRIBUTE VALUE       |
+-----------------------------------------------------------+
|1   |termName                       |RemoteStation1        |
|2   |termLocation                   |Location              |
|3   |termContactName                |4RF Support           |
|4   |termContactDetails             |Contact Details       |
|5   |termTimeFormat                 |time24h (1)           |
|6   |termDateFormat                 |ddmmyyyy (1)          |
|7   |termDateTime                   |2010-3-23,11:39:39.0  |
|8   |termEthController1IpAddress    |172.17.40.41          |
|9   |termEthController1SubnetMask   |255.255.0.0           |
|10  |termEthController1Gateway      |172.17.0.4            |
|11  |termRfNwkPanId                 |dddd                  |
|12  |termRfNwkRadius                |1                     |
|13  |termInbandManagementEnabled    |true (1)              |
+-----------------------------------------------------------+

MPA APRISASR-MIB-4RF >>set termEthController1IpAddress 172.17.40.41
termEthController1IpAddress     =       172.17.40.41

MPA APRISASR-MIB-4RF >>_
```

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 28).

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 ENTER 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 123).

   ---

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 ENTER button until all the LEDs flash red (about 3 – 5 seconds).

Antenna Matching

If the radio is a VHF variant, SuperVisor has a monitored parameter that will display the 'Last TX Packet Return Loss' in dB.

This can be used to determine the degree of match between the radio Antenna port and the feeder cable / antenna. Adjust the antenna system for best match.

To test the transmit return loss:

Remote or Repeater Station

Active the Test Mode (see 'Test Mode' on page 28) and monitor the Last TX Packet Return Loss (see 'Terminal > Parameters' on page 73).

Base Station

As Test Mode is not available on a base station, send Serial or Ethernet traffic to the base station and monitor the Last TX Packet Return Loss (see 'Terminal > Parameters' on page 73).

The following table provides an indicator of the significance of the return loss result:

Return Loss Result	Significance	Reverse Power (based on +37dBm TX Power)	Mismatch Loss VSWR
20 dB	Ideal situation	17 dBm (50 mW)	1.20 dB
12 dB	Normal operation	25 dBm (0.3 W)	1.67 dB
8 dB	Should be investigated	29 dBm (0.8 W)	2.32 dB
4 dB	Defective antenna, feeder, or connectors	33 dBm (2.0 W)	4.42 dB

A low return loss result is not always an indication of poor performance but is an indicator of a possible installation problem.

9. Product Options

Dual Antenna Port

The standard Aprisa SR uses a one or two frequency ½ 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. The transmission remains half duplex.

Example Part:

Part Number	Part Description
APSR-N400-012-DO-12-ETAA	4RF SR, BR, 400-470 MHz, 12.5 kHz, DO, 12 VDC, ET, AA

Protected Station

The Aprisa SR Protected Station provides radio and user interface protection for Aprisa SR radios. 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.

Example Part:

Part Number	Part Description
APSR-R400-012-SO-12-ETAA	4RF SR, PS, 400-470 MHz, 12.5 kHz, SO, 12 VDC, ET, AA

The Aprisa SR Protected Station is comprised of an Aprisa SR Protection Switch and two standard Aprisa SR radios. This configuration provides the ability to 'hot-swap' a failed radio without interrupting user traffic on the active radio. Additionally, retains the full temperature range specification of a single radio.

The Aprisa SR radios can be any of the currently available Aprisa SR radio frequency bands, channel sizes or single / dual antenna port options.

The Aprisa SR Protected Station can operate as a base station, repeater station or remote station. The protection behavior 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 1 and 2
- Serial port

Operation

In normal operation, the active radio carries all RS-232 serial and Ethernet traffic over the radio link and the standby radio is unused with its transmitter turned off. Both radios are continually monitored for correct operation and alarms are raised if an event occurs.

Both the active and standby radios send regular ‘keep alive’ messages to each other to indicate if they are 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 (see ‘Replacing a Protected Station Faulty Radio’ on page 214).

Configuration Management

The Primary and Secondary radios are managed with the embedded web-based management tool, SuperVisor (see ‘Managing the Radio’ on page 49) 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.

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 5 seconds to be detected.

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 132).

PA current	Tx AGC
Tx reverse power	Thermal shutdown
Temperature threshold	Thermal shutdown
RSSI Threshold	RX Synthesizer Not Locked
Rx CRC errors	RF no receive data
Port1 Eth no receive data	Port2 Eth no receive data
Port1 Eth data receive errors	Port2 Eth data receive errors
Port1 Eth data transmit errors	Port2 Eth data transmit errors
Port1 Serial Data No RX Data	Port1 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.

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 (see ‘Protected Station: Maintenance > Protection’ on page 176). 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

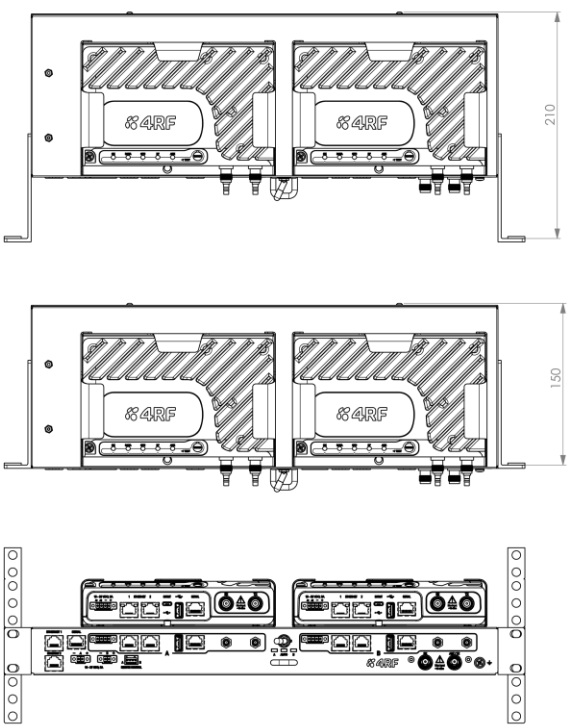
The switch over to the standby radio can be initiated via the Remote Control connector on the front of the Protection Switch. This control will only operate if the Hardware Manual Lock switch is set to the Auto position.

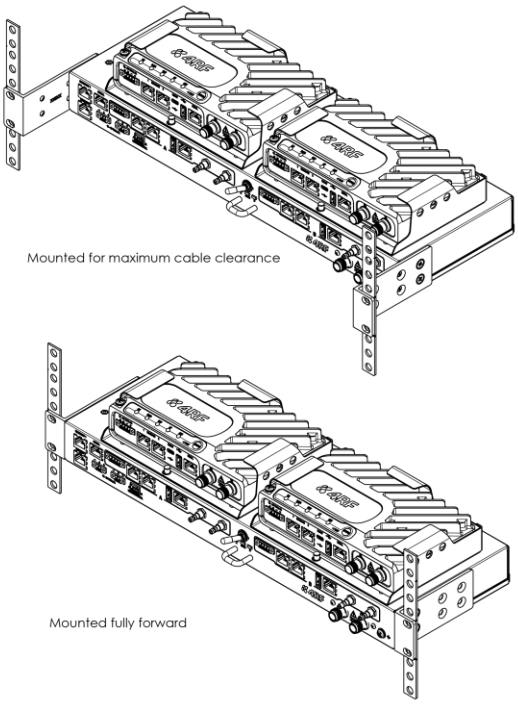
The inputs are logic inputs with 4700 Ω pullup to +3.3 VDC. They require a pull down to ground to activate the control. The ground potential is available on the connector (see ‘Protection Switch Remote Control Connections’ on page 229).

Installation

Mounting

The Aprisa SR Protected Station is designed to mount in a standard 19 inch rack.





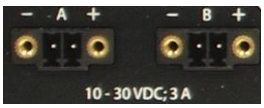
Cabling

The Aprisa SR Protected Station is delivered pre-cabled with power, interface, management and RF cables.

The set of interconnect cables is available as a spare part (see ‘Spares’ on page 215).

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 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 (which ever is available). The maximum combined power consumption is 35 Watts.



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: ’ on page 172). Changes in these parameters are automatically changed in the partner radio.

Protected Station Software Upgrade

The Protected Station software upgrade can be achieved without disruption to traffic.

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 142) 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.

Single Radio Software Upgrade

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. 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.

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 ‘Maintenance > Advanced’ on page 127). 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 71).
5. Set the Hardware Manual Lock switch to make the primary radio active.
6. Carefully remove the faulty radio from the protection switch and install the replacement radio.
7. Power on the replacement radio and wait for it to become standby.
8. Set the Hardware Manual Lock switch to the Auto position.

Spares

The Aprisa SR Protection Switch is available as a spare part. This spare includes the protection switch and two sets of Protection Switch interconnect cables (one set is 6 cables).

Part Number	Part Description
APSP-SRPSW	4RF Spare, Aprisa SR, Protection Switch

The set of interconnect cables is available as a spare part (set of 6 cables).

Part Number	Part Description
APSP-SRPSC-ST6	4RF Spare, Aprisa SR, Protection Switch Cables, Set Of 6

Replacing a Faulty Protection Switch

Note: Replacing a faulty Protection Switch will disrupt traffic.

Move the radios, the interconnect cables, 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 ‘RF Interface MAC address’ on page 128).
3. Using SuperVisor > Maintenance > Advanced, Decommission the node (see ‘Decommission Node’ on page 128) and then Discover the Nodes (see ‘Discover Nodes’ on page 128).

Ensure that the Hardware Manual Lock switch is set to the Auto position.

The Aprisa SR Protected Station is now ready to operate.

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
APSR-D400-012-DO-12-ETAA	4RF SR, PD, 400-470 MHz, 12.5 kHz, DO, 12 VDC, ET, AA

The Aprisa SR Data Driven Protected Station shown is comprised of two standard Aprisa SR dual antenna port option 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 bands, channel sizes or single / dual antenna port 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.

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

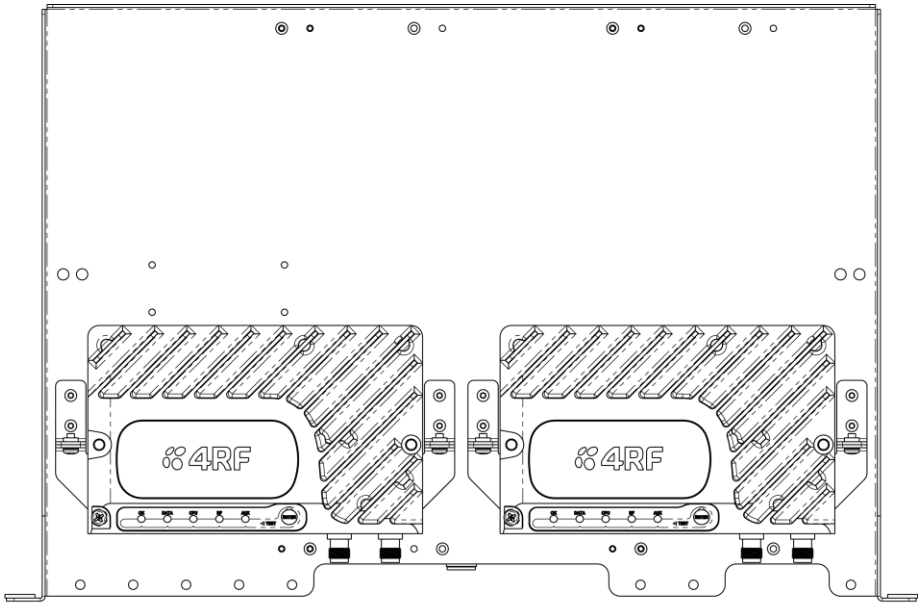
The Primary and Secondary radios are managed with the embedded web-based management tool, SuperVisor (see ‘Managing the Radio’ on page 49) by using either the Primary or Secondary IP address. Configuration changes in one of the radios will automatically be reflected in the partner radio.

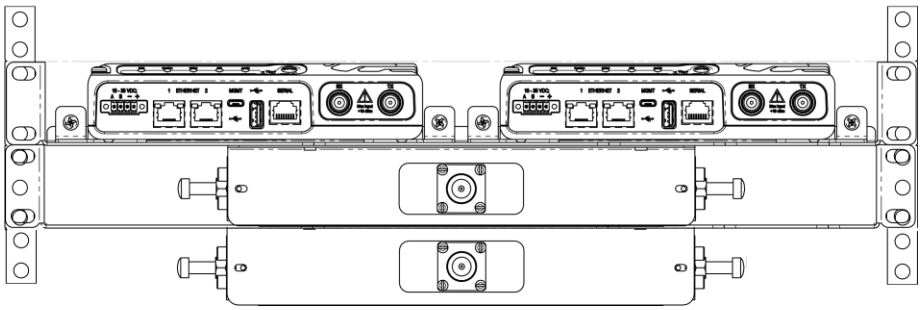
Changes to the Network Table are automatically synchronized from the active radio to the standby radio but the Network Table is only visible on the active radio.

Installation

Mounting

The Aprisa SR Data Driven Protected Station is designed to mount in a standard 19” rack on two 1U rack mounting shelves.





Cabling

The Aprisa SR Data Driven Protected Station is delivered with the radios, duplexers, rack mounting shelves and RF cables.

The picture demonstrates the RF cabling but the product is delivered with the cables separately packaged.

The set of interconnect cables is available as a spare part.

Power

A +10.5 to +30 V DC external power source must be connected to both the A and B Phoenix Contact 4 pin male power connectors. The maximum combined power consumption is 35 Watts.

Duplexer Kits

The Aprisa SR product range contains Duplexer Kit accessories for use with the Dual Antenna port Aprisa SR radios.

Radio Duplexer Kits

The Aprisa SR Radio Duplexer Kit contains:

- 1x 1U 19" rack mount shelf, black powder coated with duplexer and mounting brackets and screws to mount 1 or 2 Aprisa SR radios
- 1x Duplexer
- 2x right angle TNC to SMA right angle 590 mm cables

Part Number	Part Number
APSA-KDUP-135-N0-BR	4RF SR Acc, Kit, Dupl, 135-175 MHz, s4.6 MHz, p0.5 MHz, BR
APSA-KDUP-400-B1-BR	4RF SR Acc, Kit, Dupl, 400-470 MHz, s5 MHz, p0.5 MHz, BR

Protected Station Duplexer Kits

The Aprisa SR Protected Station Single Antenna Duplexer Kit contains:

- 1x 1U 19" rack mount shelf, black powder coated, to mount one duplexer
- 1x duplexer
- 2x right angle TNC to SMA right angle 640 mm cables

Part Number	Part Number
APSA-KDUP-135-N0-PS	4RF SR Acc, Kit, Dupl, 135-175 MHz, s4.6 MHz, p0.5 MHz, PS
APSA-KDUP-400-B1-PS	4RF SR Acc, Kit, Dupl, 400-470 MHz, s5 MHz, p0.5 MHz, PS

USB RS-232 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 serial port for customer traffic.

This is accomplished with a USB to RS-232 serial converter cable. This plugs into the USB host port connector and can be terminated with the required customer connector.

This additional RS-232 serial port is enabled with the SuperVisor mode setting in Serial Port Settings (see 'Serial > Port Setup' on page 89).

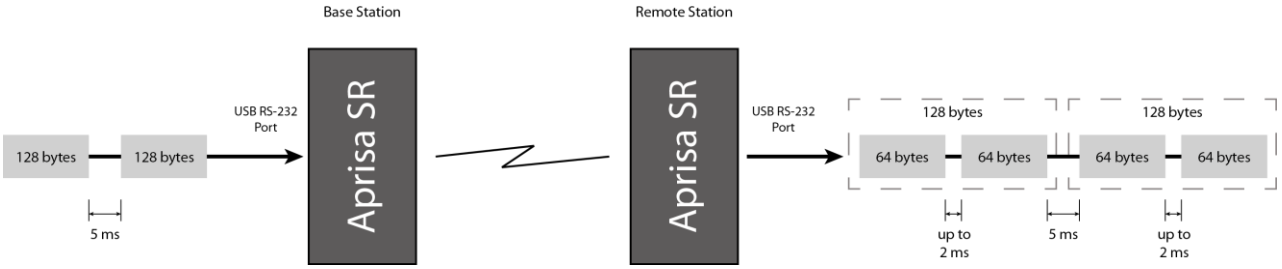
The Aprisa SR USB port has driver support for these USB serial converters. Other USB serial converters may not operate correctly.

USB RS-232 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 baud with all packet sizes and up to 115200 if the packet size is less than 64 bytes. The standard RS-232 port is fully compatible with Modbus RTU at all baud rates.

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 below):

1. USB Converter to 1.8 metre multi-strand cable 6 wire for termination of customer connector

Part Number	Part Number
APSA-IFCA-USB-MS-18	4RF SR Acc, Cable, Interface, USB Converter, Multi-strand, 1.8m

2. USB converter to RJ45 female kit for USB to RS-232 DCE conversion.

Part Number	Part Number
APSA-KFCA-USB-45-MF-18	4RF SR Acc, Kit, Interface, USB Converter, RJ45, Female, 1.8m

3. USB converter to DB9 female kit for USB to RS-232 DCE conversion.

Part Number	Part Number
APSA-KFCA-USB-D9-MF-18	4RF SR Acc, Kit, Interface, USB Converter, DB9, Female, 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 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.

Radio Software Upgrade

A software upgrade can be performed on a single radio or an entire Aprisa SR network (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 142) 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.

Upgrade Process

The Aprisa SR network upgrade operation is indicated in base station and remote stations by a flashing orange AUX LED.

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 142).
2. Distribute the software to the entire network of remote radios (see 'Software > Remote Distribution' on page 148).

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 150).

   Where 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 153.

4. Activate the software on the base station radio (see 'Software > Manager' on page 145).

Single Radio Software Upgrade

The software upgrade procedure is different for an Aprisa SR Protected Station (see 'Protected Station Software Upgrade' on page 213).

Note: If a radio has been configured for a Protection Type of 'Redundant' (see 'Protected Station: Terminal > Operating Mode' on page 164), 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

This process allows customers to upgrade a single Aprisa SR radio.

The Software Pack is loaded into the radio with the file transfer process (see 'Software > File Transfer' on page 142) and activated (see 'Software > Manager' on page 145).

Upgrade Process

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.
2. Check that the SuperVisor USB Boot Upgrade setting is set to 'Disabled' (see 'Software > Setup' on page 141).
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 142).
5. Activate the software on the radio (see 'Software > Manager' on page 145).

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.

Upgrade Process

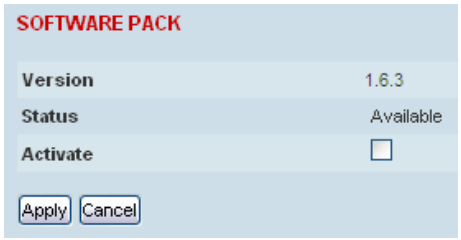
To upgrade the Aprisa SR radio software:

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 141).
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 lights solid orange. This can take about 2 minutes.

   The software will have loaded in to the radio Software Pack location.
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 145.

The version of the uploaded software will be displayed in the Software Pack 'Version' field.



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, DATA and CPU 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 141).

In this case, go to SuperVisor see ‘Software > Manager’ on page 145 and tick the Software Pack ‘Activate’ checkbox and click ‘Appy’.

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.

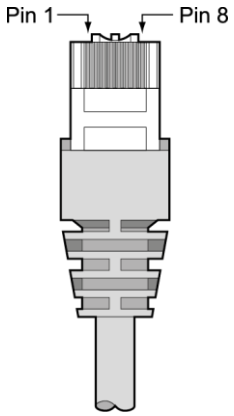
Software Downgrade

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.

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

RJ45 connector LED indicators		
LED	**Status**	**Explanation**
Green	On	Ethernet signal received
Green	Flashing	Indicates 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

The RS-232 Serial Interface is always configured as a DCE:

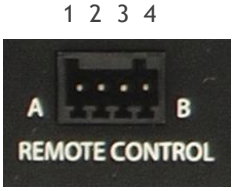
RJ45 Pin Number	Pin Function	Direction	TIA-568A Wire Colour	TIA-568B Wire Colour
1	RTS	Input	Green / white	Orange/white
2	DTR	Input	Green	Orange
3	TXD	Input	Orange / white	Green/white
4	Ground		Blue	Blue
5	DCD	Output	Blue / white	Blue/white
6	RXD	Output	Orange	Green
7	DSR	Output	Brown / white	Brown/white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

Hardware Alarms Connections

The power and alarm connector provides two hardware alarm inputs for alarm transmission to the other radios in the network.

Pin Number	1	2	3	4
Function	Alarm Port 1	Alarm Port 2	Power Negative	Power Positive

Protection Switch Remote Control Connections



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 132 for setup of alarm thresholds / sample durations etc.

Alarm Events

Transmitter Alarms

Event ID	Event Display Text	Default Severity	Configuration Type	Function
1	PA Current	critical(1)	Threshold Type	Alarm to indicate that the current drawn by the transmitter power amplifier is outside defined limits.
2	TX AGC	critical(1)	Threshold Type	Alarm to indicate that the variable gain control of the transmitter is outside defined limits.
3	TX Reverse Power	warning(4)	Threshold Type	Alarm to indicate that the antenna is not connected to the radio
4	Temperature Threshold	warning(4)	Threshold Type	Alarm to indicate that the transmitter temperature is outside defined limits.
31	Thermal Shutdown	critical(1)	Threshold Type	Alarm to indicate that the transmitter has shutdown due to excessively high temperature.

Receiver Alarms

Event ID	Event Display Text	Default Severity	Configuration Type	Function
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.
8	RX Synthesizer Not Locked	critical(1)	Not Configurable	Alarm to indicate that the receiver Synthesizer is not locked on the RF received signal.
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.

Radio Interface Path Alarms

Event ID	Event Display Text	Default Severity	Configuration Type	Function
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.

Customer Equipment Interface Path Alarms

Event ID	Event Display Text	Default Severity	Configuration Type	Function
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.
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.
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.
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.
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.
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.
13	Serial Data No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that the RS-232 port has no received input signal in the defined duration period.
14	Serial Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that the RS-232 port received input signal contains errors at a higher rate than the defined error rate threshold.

Component Failure Alarms

Event ID	Event Display Text	Default Severity	Configuration Type	Function
16	Component Failure	major(2)	Not Configurable	Alarm to indicate that a hardware component has failed.

Diagnostic Alarms

Event ID	Event Display Text	Default Severity	Configuration Type	Function
17	Protection Sw Manual Lock	warning(4)	Not Configurable	Alarm to indicate that the Protection Switch Software Manual Lock has been activated.
18	Protection Hw Manual Lock	warning(4)	Not Configurable	Alarm to indicate that the Protection Switch Hardware Manual Lock has been activated.

Software Alarms

Event ID	Event Display Text	Default Severity	Configuration Type	Function
20	Calibration Failure	major(2)	Not Configurable	Alarm to indicate that the RF calibration has failed.
21	Configuration Not Supported	major(2)	Not Configurable	Alarm to indicate that a configuration has entered that is invalid.
32	Network Configuration Warning	warning(4)	Not Configurable	Alarm to indicate a network configuration problem e.g. duplicate IP address.
39	Software Restart Required	warning(4)	Not Configurable	Alarm to indicate that a configuration has changed that requires a software reboot.

Protection Alarms

Event ID	Event Display Text	Default Severity	Configuration Type	Function
23	Protection Peer Comms Lost	major(2)	Not Configurable	Alarm to indicate that the standby radio has lost communication with the active radio.
54	Protection Hardware Failure	major(2)	Not Configurable	Alarm to indicate that there is a failure in the protection switch hardware.

Informational Events

Event ID	Event Display Text	Default Severity	Function
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.
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.
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.
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.
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.
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.

13. Specifications

RF Specifications

Frequency Bands

ETSI

Broadcast Band	Frequency Band	Frequency Tuning Range	Synthesizer Step Size
VHF	136 MHz	135-175 MHz	6.250 kHz
UHF	320 MHz (1)	320-400 MHz	6.250 kHz
UHF	400 MHz	400-470 MHz	6.250 kHz

FCC / IC

Broadcast Band	Frequency Band	Frequency Tuning Range	Synthesizer Step Size
VHF	136 MHz	135-175 MHz	2.5 kHz
UHF	400 MHz	400-470 MHz	6.250 kHz

Channel Sizes

ETSI

Channel Size	Gross Radio Capacity
12.5 kHz	9.6 kbit/s
12.5 kHz	14.4 kbit/s (1)
25 kHz	19.2 kbit/s

FCC / IC

Channel Size	Gross Radio Capacity
6.25 kHz (2)	4.8 kbit/s
12.5 kHz	9.6 kbit/s
12.5 kHz	19.2 kbit/s (1)
25 kHz	19.2 kbit/s

Note 1: Please consult 4RF for availability.

Note 2: VHF frequency band only.

Transmitter

Transmit Power output	0.01 to 5.0 W (+10 to +37 dBm, in 1 dB steps)
Adjacent channel power	< -60 dBc
Transient adjacent channel power	< -50 dBc
Spurious emissions	< -37 dBm
Attack time	< 1.5 ms
Release time	< 1.5 ms
Data turnaround time	< 10 ms
Frequency stability	± 1 ppm
Frequency aging	< 1 ppm / annum
Synthesizer lock time	< 1.5 ms (5 MHz step)

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

Receiver

Receiver sensitivity BER < 10^{-6}

Radio Capacity	Channel Size		
	6.25 kHz	12.5 kHz	25 kHz
4.8 kbit/s	-115 dBm		
9.6 kbit/s		-113 dBm	
14.4 kbit/s		-108 dBm	
19.2 kbit/s		TBD	-110 dBm

Adjacent channel selectivity

Radio Capacity	Channel Size		
	6.25 kHz	12.5 kHz	25 kHz
4.8 kbit/s	> -47 dBm [> 60 dB]		
9.6 kbit/s		> -47 dBm [> 60 dB]	
14.4 kbit/s		> -47 dBm [> 55 dB]	
19.2 kbit/s		TBD	> -37 dBm [> 65 dB]

Co-channel rejection

Radio Capacity	Channel Size		
	6.25 kHz	12.5 kHz	25 kHz
4.8 kbit/s	> -12 dB		
9.6 kbit/s		> -12 dB	
14.4 kbit/s		> -17 dB	
19.2 kbit/s		TBD	> -12 dB

Intermodulation response rejection

Radio Capacity	Channel Size		
	6.25 kHz	12.5 kHz	25 kHz
4.8 kbit/s	> -37 dBm [> 70 dB]		
9.6 kbit/s		> -37 dBm [> 70 dB]	
14.4 kbit/s		> -37 dBm [> 65 dB]	
19.2 kbit/s		TBD	> -37 dBm [> 65 dB]

Blocking or desensitization

Radio Capacity	Channel Size		
	6.25 kHz	12.5 kHz	25 kHz
4.8 kbit/s	> -17 dBm [> 90 dB]		
9.6 kbit/s		> -17 dBm [> 90 dB]	
14.4 kbit/s		> -17 dBm [> 85 dB]	
19.2 kbit/s		TBD	> -17 dBm [> 85 dB]

Spurious response rejection

Radio Capacity	Channel Size		
	6.25 kHz	12.5 kHz	25 kHz
4.8 kbit/s	> -32 dBm [> 75 dB]		
9.6 kbit/s		> -32 dBm [> 75 dB]	
14.4 kbit/s		> -32 dBm [> 70 dB]	
19.2 kbit/s		TBD	> -32 dBm [> 70 dB]

Receiver spurious radiation

Radio Capacity	Channel Size		
	6.25 kHz	12.5 kHz	25 kHz
All	< -57 dBm	< -57 dBm	< -57 dBm

Note: The receiver figures are shown in typical fixed interference dBm values and dB values [in brackets] relative to the sensitivity.

Modem

Modulation	4-CPFSK
Forward Error Correction	¾ trellis code

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 bit
Data authentication	Cipher Block Chaining Message Authentication Code (CBC-MAC) using Advanced Encryption Standard (AES) 128, 192 or 256 bit

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 switch is IEEE 802.3-compatible. It passes VLAN tagged traffic.

General	Interface	RJ45 x 2 (Integrated 2-port switch)
	Cabling	CAT-5 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 Green LED	Off: Indicates no data traffic present on the interface Flashing: Indicates 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 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
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

Hardware Alarms Interface

Alarm Inputs

The power and alarm connector provides two hardware alarm inputs for alarm transmission to the other radios in the network.

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

Protection Switch Specifications

RF Insertion Loss	< 0.5 dB
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	30 W
Connector	Phoenix Contact 4 pin male screw fitting MC 1.5/ 4-GF-3.5

Aprisa SR Protected Station

Nominal voltage	+13.8 VDC (negative earth)
Absolute input voltage range	+10 to +30 VDC
Maximum power input	35 W
Connector	2x Phoenix Contact 2 pin male screw fitting MC 1.5/ 2-GF-3.5

Aprisa SR Data Driven Protected Station

Nominal voltage	+13.8 VDC (negative earth)
Absolute input voltage range	+10 to +30 VDC
Maximum power input	35 W
Connector	2x Phoenix Contact 4 pin male screw fitting MC 1.5/ 2-GF-3.5

Power Consumption

Aprisa SR Radio

Mode	Power Consumption
Transmit / Receive	< 22.5 W for 5W transmit power
	< 15.0 W for 1W transmit power
Receive only	< 6 W full Ethernet traffic activity
	< 4.5 W no Ethernet traffic activity

Aprisa SR Protected Station and Aprisa SR Data Driven Protected Station

Mode	Power Consumption
Transmit / Receive	< 31 W for 5W transmit power
	< 23.5 W for 1W transmit power
Receive only	< 14.5 W full Ethernet traffic activity
	< 11.5 W no Ethernet traffic activity

Power Dissipation

Aprisa SR Radio

Transmit Power	Power Dissipation
1W transmit power	< 14.0 W
5W transmit power	< 17.5 W

Aprisa SR Protected Station and Aprisa SR Data Driven Protected Station

Transmit Power	Power Dissipation
1W transmit power	< 22.5 W
5W transmit power	< 26.0 W

General Specifications

Environmental

Operating temperature range	- 40 to + 70˚ C
Storage temperature range	- 40 to + 80˚ C
Operating humidity	Maximum 95% non-condensing
Acoustic noise emission	No audible noise emission

Mechanical

Aprisa SR Radio

Dimensions	Width 177 mm Depth 110 mm (126 mm with TNC connector) Height 41.5 mm
Weight	720 g
Colour	Matt black
Mounting	Wall (2 x M5 screws) Rack shelf (2 x M4 screws) DIN rail bracket

Aprisa SR Protected Station

Dimensions	Width 430 mm Depth 220 mm (incl interconnect cables) Height 90 mm
Weight	4.46 kg
Colour	Matt black
Mounting	Rack mount (2 x M4 screws)

Compliance

	12.5 kHz	25 kHz
Radio	EN 300 113-2	EN 302 561
EMI / EMC	EN 301 489 Parts 1 & 5	
Safety	EN 60950	
Environmental	ETS 300 019 Class 3.4	

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. 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

16. Index

S

T

U

W