



Aprisa **SR+**



User Manual

December 2023

Version 2.1.5f

Copyright

Copyright © 2023 4RF Limited. All rights reserved.

This document is protected by copyright belonging to 4RF Limited and may not be reproduced or republished in whole or part in any form without the prior written permission of 4RF Limited.

Trademarks

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

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

Disclaimer

Although every precaution has been taken preparing this information, 4RF Limited assumes no liability for errors and omissions, or any damages resulting from use of this information. This document or the equipment may change, without notice, in the interests of improving the product.

RoHS and WEEE Compliance

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

Restriction of hazardous substances (RoHS)

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

4RF has worked with its component suppliers to ensure compliance with the RoHS Directive which came into effect on the 1st July 2006.

End-of-life recycling programme (WEEE)

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

4RF has instigated a programme to manage the reuse, recycling, and recovery of waste in an environmentally safe manner using processes that comply with the WEEE Directive (EU Waste Electrical and Electronic Equipment 2002/96/EC).

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

Compliance General

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

It is the responsibility of the user, before operating the equipment, to ensure that where required the appropriate license has been granted and all conditions attendant to that license have been met.

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

Equipment authorizations sought by 4RF are based on the Aprisa SR+ radio equipment being installed at a fixed restricted access location and operated in point-to-multipoint or point-to-point mode within the environmental profile defined by EN 300 019, Class 3.4. Operation outside these criteria may invalidate the authorizations and / or license conditions.

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

Compliance Radio Equipment Directive

The Aprisa SR+ radio complies with the Radio Equipment Directive (RED) 2014/53/EU European Telecommunications Standards Institute (ETSI) specifications as follows:

	12.5 kHz Channel	25 kHz / 50 kHz Channel
Radio performance	EN 300 113	EN 302 561 ⁽¹⁾
EMC	EN 301 489-1 and 5	
Environmental	ETS 300 019 Class 3.4, IEEE 1613 Class 2 IEC 61850-3, Ingress Protection IP51	
Safety	EN 60950-1:2006 Class 1 division 2 for hazardous locations	

Frequency band	Channel size	Power input	Notified body
135-175 MHz	12.5 kHz, 25 kHz, 50 kHz	10-30 VDC	
320-400 MHz	12.5 kHz, 25 kHz, 50 kHz	10-30 VDC	
400-470 MHz	12.5 kHz, 25 kHz, 50 kHz	10-30 VDC	
450-520 MHz	12.5 kHz, 25 kHz, 50 kHz	10-30 VDC	

Note 1: At 50 kHz, TX to 256 QAM, RX to 64 QAM

Short Range Device

When operating as a short range device under EN 300 220-2 V3.2.1 for Ofcom IR2030/2/6 or IR2030/2/7:

1. The user must operate the Aprisa SR+ radio within all the applicable requirements of IR-2030
2. The transmitter power must not be set above +27 dBm

When operating as a short range device, the Aprisa SR+ radio TX power can be adjusted over the range of +10 dBm to +27 dBm (average power).

To determine the maximum power to be set on the Aprisa SR+ radio, it is necessary to take into account the feeder loss and antenna gain.

1.	ERP limit (specified in dBm, in the case of IR-2030 this is +27 dBm)	ERP _{dBm}
2.	Peak to average power ratio	Px _{dB}
	QPSK 3 dB	
	16QAM 5 dB	
	64QAM 6 dB	
	256QAM 7 dB	
	ACM 7 dB	
3.	Antenna gain specified in dBd (if given in dBi subtract 2.15 dB from the given value)	G _{dBd}
4.	Feeder coax loss between Aprisa SR+ radio and antenna (specified in dB/m)	L _{dB/m}
5.	Length of feeder coax between Aprisa SR+ radio and antenna (specified in metres)	d _m

From the above information, the power setting of the Aprisa SR+ radio (P_{dBm}) can be calculated to ensure operation within the regulatory requirements using the formula:

$$P_{dBm} = ERP_{dBm} + (d_m \times L_{dB/m}) - G_{dBd} - P_{x_{dB}}$$

Compliance United States of America FCC

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

Radio	47CFR part 24, part 27, part 90 and part 101 Private Land Mobile Radio Services
EMC	47CFR part 15 Radio Frequency Devices ^(note 1) , EN 301 489-1 and 5
Environmental	ETS 300 019 Class 3.4, IEEE 1613 Class 2 IEC 61850-3, Ingress Protection IP51
Safety	UL / EN 60950-1:2006 Class 1 division 2 for hazardous locations

Frequency Band (note 2)	Channel size	Power input	Authorization	FCC ID
135-175 MHz	15 kHz, 30 kHz	10-30 VDC	Part 90	UIPSQ135M150
215-240 MHz	12.5 kHz, 15 kHz, 25 kHz, 50 kHz	10-30 VDC	Part 90	UIPSQ215M141
400-470 MHz	12.5 kHz, 25 kHz, 50 kHz	10-30 VDC	Part 90	UIPSQ400M1311
450-520 MHz	12.5 kHz, 25 kHz	10-30 VDC	Part 90	UIPSQ450M140
757-758 MHz and 787-788 MHz (note 3)	12.5 kHz, 25 kHz, 50 kHz, 100 kHz	10-30 VDC	Part 27	UIPSQ757M160
896-902 MHz	12.5 kHz, 25 kHz, 50 kHz, 100 kHz	10-30 VDC	Part 24 / Part 90 / Part 101	UIPSQ896M141
928-960 MHz	12.5 kHz, 25 kHz, 50 kHz, 100 kHz	10-30 VDC	Part 24 / Part 90 / Part 101	UIPSQ928M141

Note 1: 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.

Note 2: The Frequency Band is not an indication of the exact frequencies approved by FCC.

Note 3: For 700 MHz FCC Part 27 compliance in the Upper A block, the following frequency range restrictions apply:

Channel Size	Low Band	High Band
12.5 kHz	757.01250 MHz to 757.98750 MHz	787.01250 MHz to 787.98750 MHz
25 kHz	757.01875 MHz to 757.98125 MHz	787.01875 MHz to 787.98125 MHz
50 kHz	757.03750 MHz to 757.96250 MHz	787.03750 MHz to 787.96250 MHz
100 kHz	757.07500 MHz to 757.92500 MHz	787.07500 MHz to 787.92500 MHz

Compliance Canada ISED

The Aprisa SR+ radio is designed to comply with Innovation, Science and Economic Development' (ISED) specifications as follows:

Radio	RSS-119 / RSS-134			
EMC	This Class A digital apparatus complies with Canadian standard ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.			
Environmental	ETS 300 019 Class 3.4, IEEE 1613 Class 2 IEC 61850-3, Ingress Protection IP51			
Safety	UL / EN 60950-1:2006 Class 1 division 2 for hazardous locations			

Frequency Band *	Channel size	Power input	Authorization	ISED
135-175 MHz	15 kHz, 30 kHz	10-30 VDC	RSS-119	6772A-SQ135M150
215-240 MHz	12.5 kHz, 15 kHz, 25 kHz, 50 kHz	10-30 VDC	RSS-119	Pending
400-470 MHz	12.5 kHz, 25 kHz, 50 kHz	10-30 VDC	RSS-119	6772A-SQ400M1311
896-902 MHz	12.5 kHz, 25 kHz, 50 kHz, 100 kHz	10-30 VDC	RSS-119 and RSS-134	6772A-SQ896M141
928-960 MHz	12.5 kHz, 25 kHz, 50 kHz, 100 kHz	10-30 VDC	RSS-119 and RSS-134	6772A-SQ928M141

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

Compliance Brazil ANATEL

This product is not suitable for use in a domestic environment, as it may cause electromagnetic interference in which the user will be required to take measures to minimize such interference.

Este produto será comercializado no Brasil com as configurações abaixo:

Faixa de frequência: 157 a 174 MHz; BW: 12,5; 25 e 50 kHz.

Faixa de frequência: 360 a 380 MHz; BW: 12,5 e 25 kHz.

Faixa de frequência: 380 a 400 MHz; BW: 12,5; 25 e 50 kHz.

Faixa de frequência: 406 a 430 e 450 a 470 MHz; BW: 12,5; 25 e 50 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. A Nationally Recognized Testing Laboratory (NRTL) listed power supply is required to power the equipment.

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

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

The following text is printed on the Aprisa SR+ where the end user is in Canada:

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

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

Les ports de service USB et le commutateur de verrouillage ne doivent pas être utilisés, à moins qu'il ne s'agisse d'un emplacement non dangereux.

Compliance IEEE 1613 class 2

Users requiring compliance to IEEE 1613 class 2 shall use screened cables and connectors to connect to the serial ports.

Compliance IEC 61850-3

Users requiring compliance to IEC 61850-3 shall use screened cables and connectors to connect to the serial ports.

Note that during certain supply voltage dips and interruptions, the alarm status may change while the unit is recovering from such an event.

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 50385:2017.

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
757	+ 37	18	3.5
788	+ 37	18	3.5
896	+ 37	28	10.0
902	+ 37	28	10.0
928	+ 37	28	9.5
960	+ 37	28	9.5

Note 1: The Peak Envelope Power (PEP) at maximum set power level is +40 dBm.

Contents

1. Getting Started	17
2. Introduction.....	19
About This Manual.....	19
What It Covers	19
Who Should Read It	19
Contact Us.....	19
3. About the Radio	20
The 4RF Aprisa SR+ Radio	20
Product Features	21
Functions	21
Security	23
Performance	24
Usability	24
Product Overview	25
Network Coverage and Capacity	25
Automatic Registration	25
Remote Messaging.....	25
Store and Forward Repeater.....	26
Repeater Packet Forwarding.....	26
Repeater Messaging	29
Peer To Peer Communication Between Remote Radios.....	30
Architecture.....	34
Product Operation.....	34
Physical Layer.....	34
Data Link Layer / MAC layer	35
Channel Access	35
Hop by Hop Transmission.....	36
Adaptive Coding and Modulation.....	36
System Gain vs FEC Coding	37
Network Layer	38
Packet Routing.....	38
Static IP Router	39
Bridge Mode with VLAN Aware	54
VLAN Bridge Mode Description	55
Terminal Server Operational in Bridge and Router Modes.....	57
Avoiding Narrow Band Radio Traffic Overloading.....	61
Interfaces.....	63
Antenna Interface	63
Ethernet Interface	63
RS-232 / RS-485 Interface.....	63
USB Interfaces	63
Protect Interface	63
Alarms Interface.....	63
Front Panel Connections	64
LED Display Panel	65
Normal Operation	65
Single Radio Software Upgrade.....	66
Network Software Upgrade	66

Test Mode	67
Network Management	68
Hardware Alarm Inputs / Outputs	69
Alarm Input to SNMP Trap.....	69
Alarm Input to Alarm Output	69
Aprisa SR Alarm Input to Aprisa SR+ Alarm Output	69
4. Implementing the Network.....	70
Network Topologies	70
Point-To-Point Network	70
Point-to-Multipoint Network.....	70
Point-to-Multipoint with Repeater 1.....	70
Point-to-Multipoint with Repeater 2.....	70
Initial Network Deployment	71
Install the Base Station.....	71
Installing the Remote radios.....	71
Install a Repeater Station	71
Network Changes	72
Adding a Repeater Station	72
Adding a Remote radio	72
5. Preparation	73
Bench Setup.....	73
Path Planning	74
Antenna Selection and Siting	74
Base or Repeater Station.....	74
Remote radio.....	75
Antenna Siting	76
Coaxial Feeder Cables	77
Linking System Plan	77
Site Requirements.....	78
Power Supply.....	78
Equipment Cooling	78
Earthing and Lightning Protection	79
Feeder Earthing.....	79
Radio Earthing	79
6. Installing the Radio	80
Mounting.....	80
Required Tools.....	80
DIN Rail Mounting	81
Rack Shelf Mounting	82
Wall Mounting.....	83
Installing the Antenna and Feeder Cable	84
Connecting the Power Supply	85
External Power Supplies.....	85
7. Managing the Radio	87
SuperVisor	87
Connecting to SuperVisor	88
Management PC Connection	89
PC Settings for SuperVisor	90
Login to SuperVisor.....	91
Logout of SuperVisor.....	94
SuperVisor Page Layout.....	95

SuperVisor Extended Network Management (EXM)	97
SuperVisor Menu	99
SuperVisor Menu	100
SuperVisor Menu Items	102
Standard Radio.....	103
Terminal	103
Radio	126
Serial	148
Ethernet	167
IP.....	177
QoS	203
Security	225
Maintenance	258
Events.....	278
Software	291
Monitoring	310
Network Status	333
Protected Station	342
Terminal	343
Radio	351
Ethernet	353
IP.....	354
Security	358
Maintenance	361
Events.....	371
Software	375
Command Line Interface	392
Connecting to the CLI via the Management Port (MGMT)	393
Connecting to the CLI via Telnet.....	395
Connecting to the CLI via SSH	395
CLI Commands	397
Viewing the CLI Terminal Summary.....	399
Changing the Radio IP Address	399
Wireshark Debug Access.....	400
8. In-Service Commissioning	401
Before You Start.....	401
What You Will Need.....	401
Antenna Alignment.....	402
Aligning the Antennas	402
9. Product Options	403
Radio Hardware Types.....	403
Hardware Software Compatibility	403
Data Interface Ports	404
Full Duplex Base Station	404
Point-To-Point Link	405
Protected Station	409
Protected Ports.....	410
Operation.....	410
Switch Over	411
Switching Criteria	411
Monitored Alarms.....	412
Configuration Management	413
Hardware Manual Lock	414

Remote Control	414
L2 / L3 Protection Operation	415
Hot-Swappable	415
Antenna and Duplexer Options	416
Installation	418
Mounting	418
Cabling	419
Power	421
Alarms	422
Maintenance	423
Changing the Protected Station IP Addresses	423
Creating a Protected Station	423
Replacing a Protected Station Faulty Radio	424
Replacing a Faulty Power Supply	425
Replacing a Faulty Protection Switch	425
Spares	426
Data Driven Protected Station	427
Operation	427
Over The Air Compatibility	427
Switch Over	428
Configuration Management	428
Power	428
Installation	429
Mounting	429
Cabling	429
Duplexer Kits	430
Radio Duplexer Kits	430
Protected Station Duplexer Kits	433
Protected Station with Duplexer Kit	437
USB RS-232 / RS-485 Serial Port	438
USB RS-232 / RS-485 operation	438
USB RS-232 Cabling Options	439
USB RS-485 Cabling Options	439
USB Retention Clip	440
10. Maintenance	441
Spare Fuses	441
Radio Spare Fuses	441
Additional Spare Fuses	442
Protected Station Spare Fuses	443
No User-Serviceable Components	444
Software Upgrade	445
Network Software Upgrade	445
Non-Protected Network Upgrade Process	445
Protected Network Upgrade Process	447
Single Radio Software Upgrade	449
File Transfer Method	449
USB Boot Upgrade Method	450
Software Downgrade	450
Protected Station Software Upgrade	451
Routine Maintenance	452
Power Supply Check	452
Temperature Test	452
Connections	452
Antenna and Feeder System	452
Transmit Power	453

Transmit Frequency.....	453
Transmit Spectrum.....	453
11. Interface Connections.....	454
RJ45 Connector Pin Assignments.....	454
Ethernet Interface Connections.....	454
RS-232 Serial Interface Connections.....	455
RS-232 Pinout	455
RS-232 Customer Cable Wiring	455
RS-232 Bit Oriented Mode Wiring	456
RS-232 RJ45 LED Indicators	456
Alarm Interface Connections	457
Protection Switch Remote Control Connections	457
12. Alarm Types and Sources.....	458
Alarm Types.....	458
Alarm Events	459
Informational Events.....	465
13. Specifications	467
RF Specifications	467
Frequency Bands	467
Channel Sizes	468
Receiver	480
Transmitter	483
Modem	484
Data Payload Security	484
Duplexer Specifications	485
Interface Specifications	486
Ethernet Interface	486
RS-232 Asynchronous Interface.....	487
Hardware Alarms Interface	488
Protection Switch Specifications.....	488
Power Specifications.....	489
Power Supply.....	489
Power Consumption.....	490
Power Dissipation	491
General Specifications.....	492
Environmental	492
Mechanical	492
Compliance.....	493
14. Product End Of Life.....	494
End-of-Life Recycling Programme (WEEE)	494
The WEEE Symbol Explained.....	494
WEEE Must Be Collected Separately	494
YOUR ROLE in the Recovery of WEEE.....	494
EEE Waste Impacts the Environment and Health	494
15. Copyrights	495

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 74
2.	Ensure that the site preparation is complete: - Power requirements - Tower requirements - Environmental considerations, for example, temperature control - Mounting space	Page 77

Phase 2:	Installing the radios	
1.	Mount the radio.	Page 80
2.	Connect earthing to the radio.	Page 79
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 79
5.	Connect the coaxial jumper cable between the lightning protection and the radio antenna port.	Page 84
6.	Connect the power to the radio.	Page 85

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 392.	Page 392
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 90
4.	Open a web browser and login to the radio.	Page 91
5.	Set or confirm the RF characteristics: • TX and RX frequencies • TX output power	Page 128
6.	Compare the actual RSSI to the expected RSSI value (from your path planning).	Page 67
7.	Align the antennas.	Page 402
8.	Confirm that the radio is operating correctly; the OK, MODE and AUX LEDs are green.	

2. Introduction

About This Manual

What It Covers

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

It specifically documents an Aprisa SR+ radio running system software version 2.1.5.

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 training and experience.

Contact Us

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

The 4RF New Zealand head office is:

4RF Limited
85 The Esplanade, Petone
PO Box 13-506
Wellington 5012
New Zealand

E-mail	support@4rf.com
Website	www.4rf.com
Telephone	+64 4 499 6000

The 4RF United States sales office is:

4RF USA, Inc.
2301 Blake Street
Denver
Colorado 80205
United States of America

E-mail	usa@4rf.com
Website	www.4rf.com
Telephone	+1 866 232-5647

3. About the Radio

The 4RF Aprisa SR+ Radio

The 4RF Aprisa SR+ is a Point-To-Multipoint (PMP) and Point-To-Point (PTP) 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 radios.

A single Aprisa SR+ is configurable as a:

- Point-To-Multipoint base station, remote radio, repeater station or a base-repeater station
- Point-To-Point local or remote radio



Product Features

Functions

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

VHF 135	135-175 MHz
VHF 220	215-240 MHz
UHF 320	320-400 MHz
UHF 400	400-470 MHz
UHF 450	450-520 MHz
UHF 700	757-758 MHz and 787-788 MHz
UHF 896	896-902 MHz
UHF 928	928-960 MHz
- Channel sizes - software selectable:

12.5 kHz
20 kHz
25 kHz
50 kHz
100 kHz
- Adaptive Coding and Modulation (ACM): QPSK (High Gain) to 256 QAM (Low gain)
- Half duplex or full duplex RF Point-To-Multipoint operation
- Full duplex RF Point-to-point operation
- Automatic Transmit Power Control (ATPC)
- Ethernet data interface and RS-232 / RS-485 asynchronous multiple port options
- Software selectable dual / single antenna port options (dual antenna port for external duplexers or filters)
- Data encryption and authentication using 128,192 and 256 bit AES and CCM security standards
- Terminal server operation for transporting RS-232 / RS-485 traffic over IP or Ethernet and converting IP packets to a local physical serial port
- Mirrored Bits ® and SLIP support for RS-232
- IEEE 802.1Q VLAN support with single and double VLAN tagged and add/remove VLAN manipulation to adapt to the appropriate RTU / PLCs
- QoS supports using IEEE 802.1p VLAN priority bits to prioritize and handle the VLAN / traffic types
- QoS per port (Ethernet, serial, management)
- L2 / L3 / L4 filtering for security and avoiding narrow band radio network overload
- L3 Gateway Router mode with standard static IP route for simple routing network integration
- L3 Router mode with per Ethernet interface IP address and subnet
- L2 Bridge mode with VLAN aware for standard Industrial LAN integration
- Ethernet header and IP/TCP / UDP ROHC header compression to increase the narrow band radio capacity
- Ethernet and serial payload compression to increase the narrow band radio capacity
- Pseudo peer to peer communication between remote radios through base-repeater or repeater stations
- SuperVisor web management support for element and sub-network (base-repeater-remotes) management

- SuperVisor Extended Network Management (EXM) extending SuperVisor management beyond the single radio network providing configuration and monitoring to other Aprisa SR family products
- SNMPv1/2/3 & encryption MIB supports for 4RF SNMP manager or third party SNMP agent network management
- SNMP context addressing for compressed SNMP access to remote radios
- SNTP for accurate wide radio network time and date
- Build-configuration / flexibility of serial and Ethernet interface ports (3+1, 2+2, 4+0)
- Radio and user interface redundancy (provided with Aprisa SR+ Protected Station)
- Protected Station fully hot swappable and monitored hot standby
- Power optimized with sleep modes
- Transparent to all common SCADA protocols; e.g. Modbus, IEC 60870-5-101/104, DNP3 or similar
- Complies with international standards, including ETSI, FCC, ISED, ACMA, EMC, safety and environmental standards

Security

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

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

The security features implemented are:

- Data encryption
 - Counter Mode Encryption (CTR) using Advanced Encryption Standard (AES) 128, 192, 256 bit, based on FIPS PUB 197 AES encryption (using Rijndael version 3.0)
- Data authentication
 - NIST SP 800-38C Cipher Block Chaining Message Authentication Code (CBC-MAC) based on RFC 3610 using Advanced Encryption Standard (AES)
- Data payload security
 - CCM Counter with CBC-MAC integrity (NIST special publication 800-38C)
- Secured management interface protects configuration
- RADIUS security for remote user authorization, authentication and accounting
- Account lockout / slowdown user account lockout mechanisms to mitigate brute force password guessing attacks
- One-time Password (OTP) recovery provides proofing mechanism that allows an Admin user access to change the Admin password if the Admin user is permanently locked out
- Events logging for auditing user access and operation
- Supported security alerts event options
- L2 / L3 / L4 Address filtering enables traffic source authorization
- Proprietary physical layer protocol and modified MAC layer protocol based on standardized IEEE 802.15.4
- Licensed radio spectrum provides recourse against interference
- Secure HTTPS access to the radio SuperVisor element management interface, i.e. secure access to the radio embedded web server
- Unique self-signed ECC-256 security certificate used for the secure HTTPS management interface
- Secure Shell (SSH) access to the radio CLI (command line interface) management interface
- SNMPv3 with Encryption for NMS secure access
- Secure remote software upgrade using HTTPS protocol
- Encrypted and signed software file to prevent the loading of non 4RF software
- Secure USB software upgrade
- Secure Ethernet port access by user of SCADA / user traffic or management traffic. This is useful to block any management access from unguarded remote sites.
- Unused ports can be disabled to prevent unauthorized access
- Key Encryption Key (KEK) based on RFC 3394, for secure Over The Air Re-keying (OTAR) of encryption keys
- User privilege allows the accessibility control of the different radio network users and the user permissions

Performance

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

Usability

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

Product Overview

Network Coverage and Capacity

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

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

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

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

Automatic Registration

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

If a remote is not able to register with base station in 5 attempts, then a 'Network Configuration Warning' alarm event will be raised indicating that a remote is not registered with the base station. If a remote radio cannot register with the base station after 30 minutes, it will automatically reboot.

If a remote radio has registered with the base station but then loses communication, it will automatically reboot 30 minutes after the 'Remote Communications Lost' alarm event. If the remote communications lost alarm is disabled, the remote will not reboot.

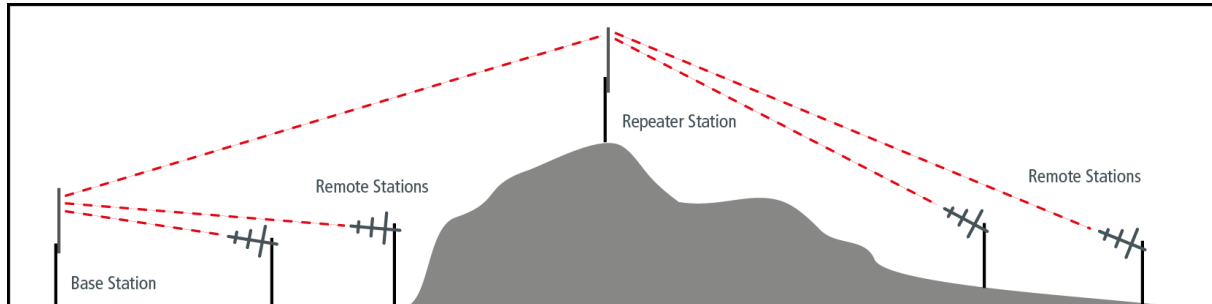
Remote Messaging

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

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

Store and Forward Repeater

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



Repeater Packet Forwarding

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

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

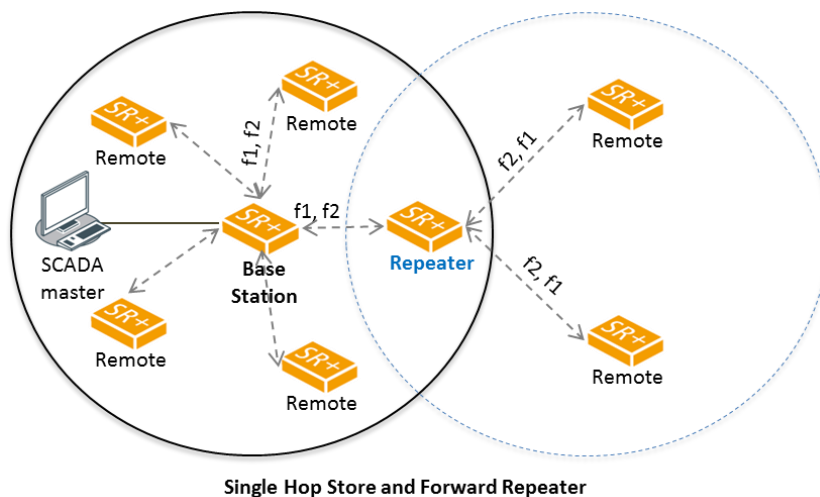
Single Hop

The Aprisa SR+ functionality allows repeaters in Bridge mode to forward Ethernet packets based on Repeater Network Segment ID. The base station translates the destination MAC address to the Repeater Network Segment ID. This improves repeater performance by forwarding the packet if the Repeater Network Segment ID belongs to the repeater branch and discards the packet if it doesn't.

Router mode supports repeater packet forwarding based on IP destination address. This improves repeater performance by forwarding the packet if the IP destination address belongs to the repeater branch and discards the packet if it doesn't.

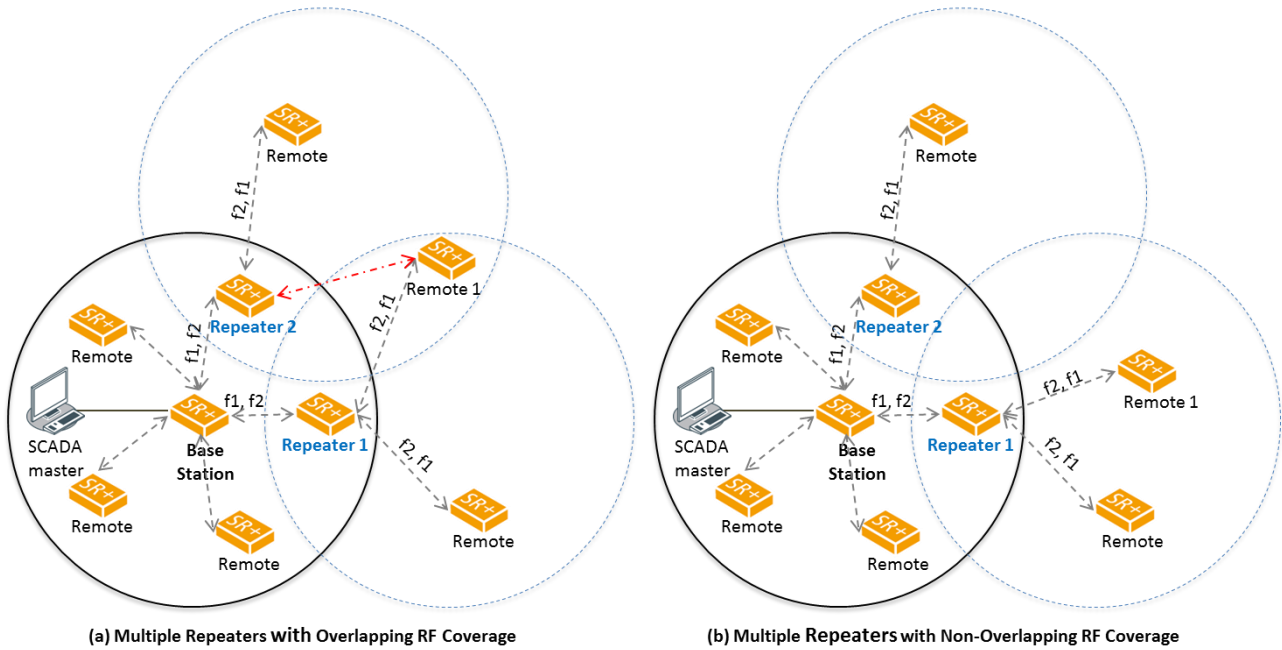
Single Repeater Single Hop

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



Multiple Repeater Single Hop

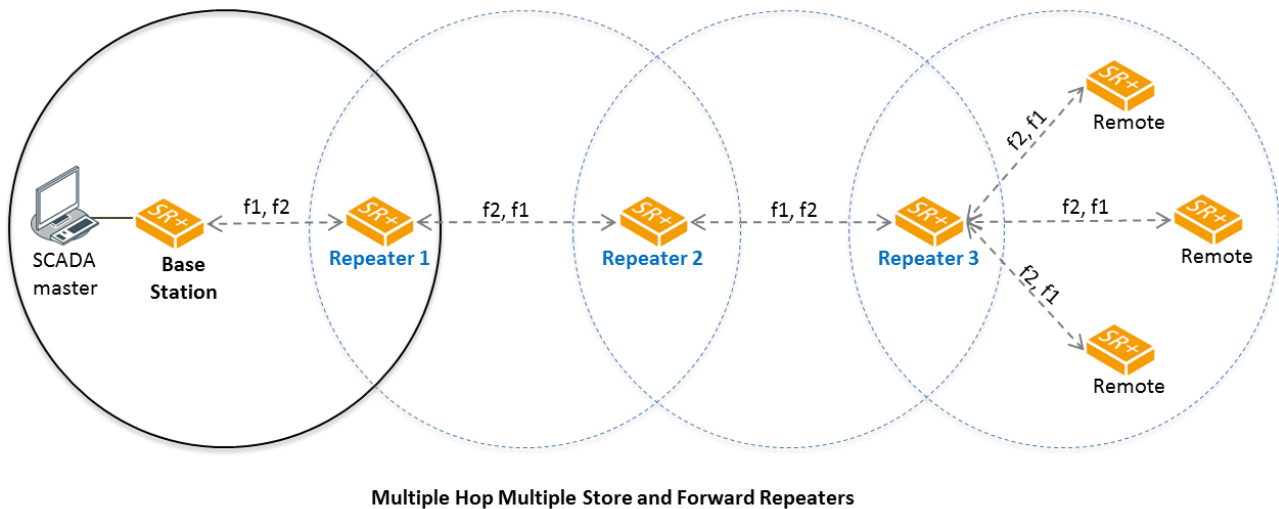
The following example depicts an Aprisa SR+ multiple repeater single hop store and forward network supporting both overlapping and non-overlapping coverage repeater networks. An overlapped RF coverage area creates radio interference and might affect network performance and reduce throughput, as show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



Multiple Hop

Multiple Repeater Multiple Hop

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



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

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

Repeater Messaging

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

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

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

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

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

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

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

Peer To Peer Communication Between Remote Radios

With the Aprisa SR+ peer to peer communication is possible between remote radios via the repeater or base-repeater. It is useful if the SCADA server or base station fails or when in some industries like the water industry, where a reservoir remote radio might send a direct message to a valve remote radio to close or open the valve without the intervention of the SCADA server.

To enable communication between remotes connected to a base station, or between remotes connected to different repeater stations, the Aprisa SR+ has a special operating mode for peer to peer communication.

The following are the settings required for all radios in bridge mode and for any traffic type (Serial or Ethernet), or all radios in all modes (bridge or router or advanced router mode) when the peer to peer traffic is serial:

1. The SuperVisor > Terminal > Operating Mode > Terminal operating mode must be set to 'Base-Repeater'. Base-Repeater operating mode does not change the Network Radius parameter as the base-repeater is considered to be like a regular base station.
2. IP Header Compression must be disabled on all radios (base, repeater, remotes) for this feature to operate correctly (see 'IP Header Compression Ratio' on page 146).
3. The Network Repeaters Proximity must be set to 'Base Repeater' on all remote radios for this feature to operate correctly (see 'Network Repeaters Proximity' on page 111).

If communication is required between remotes connected on the same repeater, implement the steps below. If Base-Repeater mode is also enabled, this can still be helpful to reduce latency for messages between remotes on the same repeater.

1. The remote radios participating in peer to peer communication must set the SuperVisor > Radio > Channel Setup > Packet Filtering to Disable. This means that when this remote receives a packet from another remote, it is processed and not discarded.
2. The repeater radio participating in peer to peer communication must also set the SuperVisor > Radio > Channel Setup > Packet Filtering to Disable. This ensures that this repeater will guarantee packets repeater from a remote will get delivered to all other remotes connected to it.

When all radios are set to router mode or gateway router mode (i.e. RM/GRM) and peer to peer traffic is Ethernet / IP, the following two alternative settings can be applied:

1. Set the **default gateway IP address** (of the base station Eth IP or Eth PVIP (i.e. virtual IP)) on remotes when all remote site traffic is destined to the SCADA master or to a distant RTU (peer-to-peer).
In RM/GRM, the base station builds a semi-automated routing table for all remotes and directly connect RTUs without any static routes on the remote radios. Thus, when the RTU sends a packet with a destination IP of the distant RTU for peer to peer, the packet is sent/routed to the default gateway IP address i.e. to the base station, which routes the packet to the destined RTU based on its semi-automated routing table. See example Figure 1 and **option without static route** table below for peer-to-peer communication between RTU-1 and RTU-2.
2. Or alternatively, set a static route on remotes when the **default gateway IP address** is not via the base station or when there is a LAN network connected to the remote radios and not all LAN traffic should be sent OTA to SCADA master or to distant remote (for peer-to-peer). The static route on the remote for peer-to-peer uses the Ethernet port IP (or Eth PVIP in case of protected station) as the next hop IP. Thus, when RTU sends the packet with a destination IP of distant RTU, the packet is sent/routed by the remote to base station based on its static route, and the base station routes the packets to the destined RTU based on its semi-automated routing table. See example Figure 1 and **option with static route** table below for peer-to-peer communication between RTU-1 and RTU-2.
3. **Note:** If there is a router between the remote radio and the RTU (i.e. RTU is not directly connected to the remote radio), then a static route must be set on the remote radio, since the base station semi-automated routing table is built only for the remote radios and their directly connected RTUs, but not for RTU devices that are ‘behind’ a router.
4. **Note:** A network with repeater will not change any of the above settings as all packets still have to go to base station for routing decision, since a repeater does not make any IP routing decision.

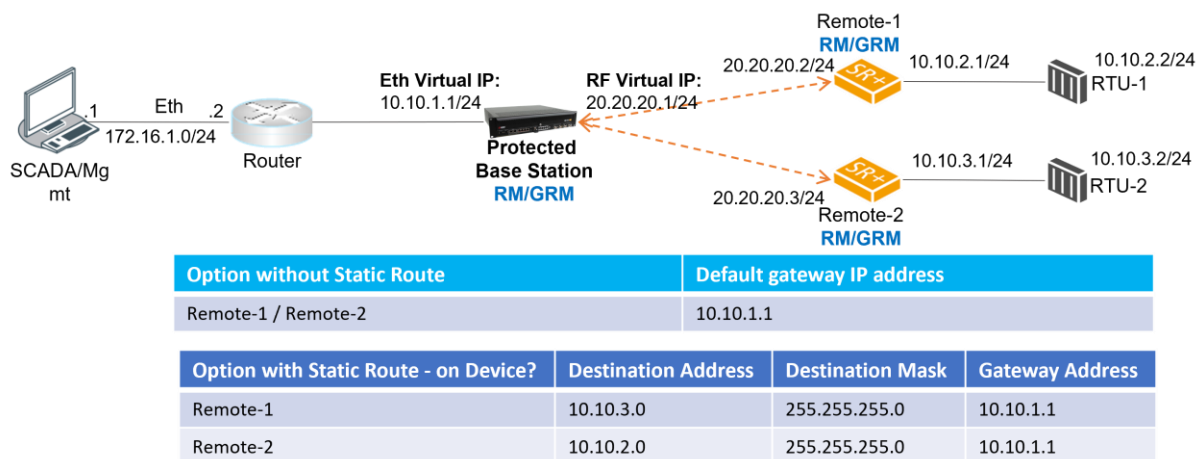
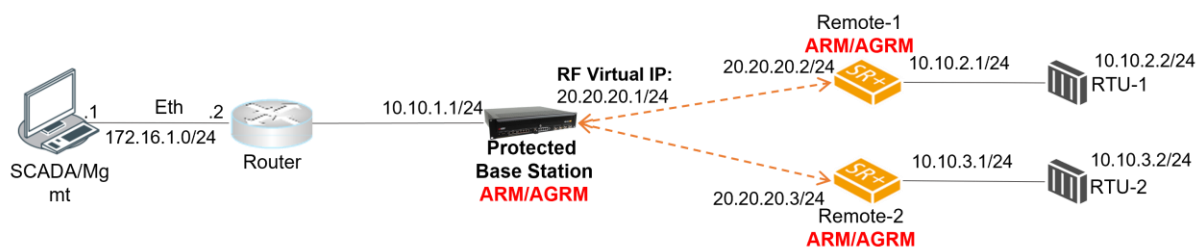


Figure 1 RM/GRM Peer-to-Peer communication options

When all radios are set to advanced router mode or advanced gateway router mode (i.e. ARM/AGRM) and peer to peer traffic is Ethernet / IP, the following two alternative settings can be applied:

1. Set the **default gateway IP address** on remotes and static route on the base station when all remote site traffic is destined to the SCADA master or to a distant RTU (peer-to-peer). Thus, when the RTU sends a packet with a destination IP of the distant RTU, the packet is sent/routed to the default gateway IP address i.e. to the base station, which routes the packets to the destined RTU IP address based on the static route setting on the base station. See example Figure 2 and **option with static route on Base but not on remote** table below for peer-to-peer communication between RTU-1 and RTU-2.
2. Set static routes on remotes and the base station when the **default gateway IP address** is not via the base station or when there is a LAN network connected to the remote radios and not all LAN traffic should be sent OTA to SCADA master or to a distant remote (for peer-to-peer). The static route for peer-to-peer uses the RF port IP (or RF PVIP in case of protected station) as the next hop IP. Thus, when the RTU sends a packet with a destination IP of distant RTU, the packet is sent/routed by the remote to the base station based on its static route, and the base station routes the packet to the destined RTU based on its static route. See example Figure 2 and **option with static route** table below for peer-to-peer communication between RTU-1 and RTU-2.
3. **Note:** A network with a repeater will not change any of the above settings as all packets still have to go to base station for routing decision, since a repeater does not make any IP routing decision.



Option with Static Route on Base but not on Remote— on Device?	Destination Address	Destination Mask	Gateway Address	Default gateway IP address
Remote-1 / Remote-2	---	---	---	20.20.20.1
Protected Base station	10.10.2.0	255.255.255.0	20.20.20.2	Router IP
Protected Base station	10.10.3.0	255.255.255.0	20.20.20.3	Router IP

Option with Static Route - on Device?	Destination Address	Destination Mask	Gateway Address
Remote-1	10.10.3.0	255.255.255.0	20.20.20.1
Remote-2	10.10.2.0	255.255.255.0	20.20.20.1
Protected Base station	10.10.2.0	255.255.255.0	20.20.20.2
Protected Base station	10.10.3.0	255.255.255.0	20.20.20.3

Figure 2 ARM/AGRM Peer-to-Peer communication options

The following example depicts peer to peer communication in bridge mode between remote radios via a base-repeater and via a repeater station where remote-1 and remote-2 communicate with each other via the base-repeater station and remote-3 and remote-4 communicate with each other via the repeater station. The repeater, remote-3 and remote-4 radios are configured with packet filtering disabled and all radios in the network are configured with IP header compression ratio disabled.

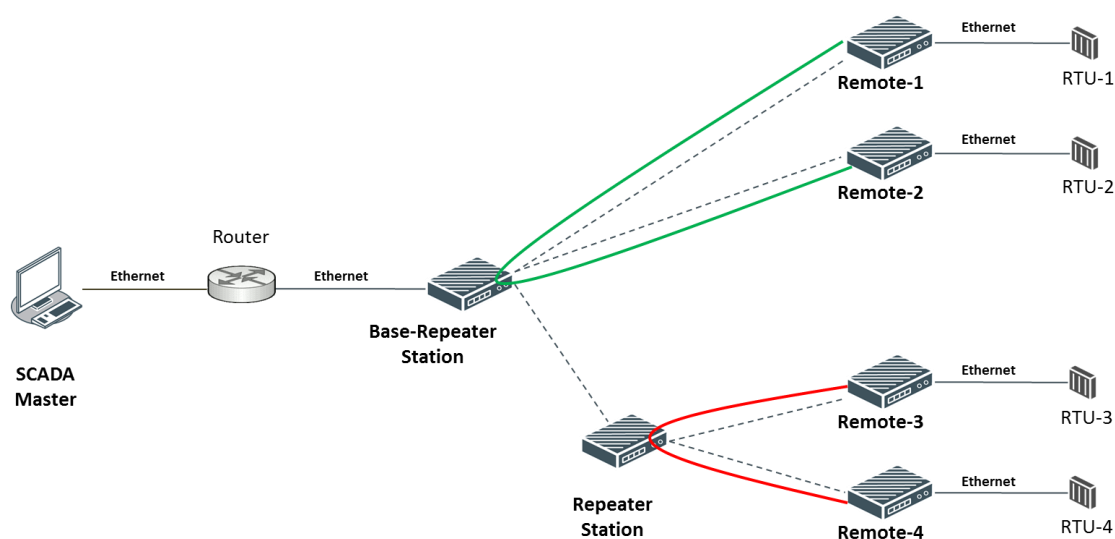


Figure 3 Peer to peer communication with repeater in bridge mode

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.

Architecture

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

- Physical
Proprietary wireless
RS-232 and Ethernet interfaces
- Link
Proprietary wireless (channel access, ARQ, segmentation)
VLAN aware Ethernet bridge
- Network
Standard IP
Proprietary automatic radio routing table population algorithm
- Transport
TCP, UDP
- Application
HTTPS web management access through base station with proprietary management application software including management of remote radios over the radio link
SNMPv1/2/3 for network management application software

Product Operation

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

Physical Layer

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

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

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

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

Data Link Layer / MAC layer

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

Channel Access

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

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

Access Request

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

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

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

Access Request - Full Duplex

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

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

This feature can be operated on full duplex hardware only (see 'Product Options' section on page 403).

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

When the Access Scheme is set to full duplex on a repeater, it is mandatory to configure the Repeater Network Segment IDs correctly (see 'Repeater Network Segment ID' on page 105).

Listen Before Send

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

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

Hop by Hop Transmission

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

Adaptive Coding and Modulation

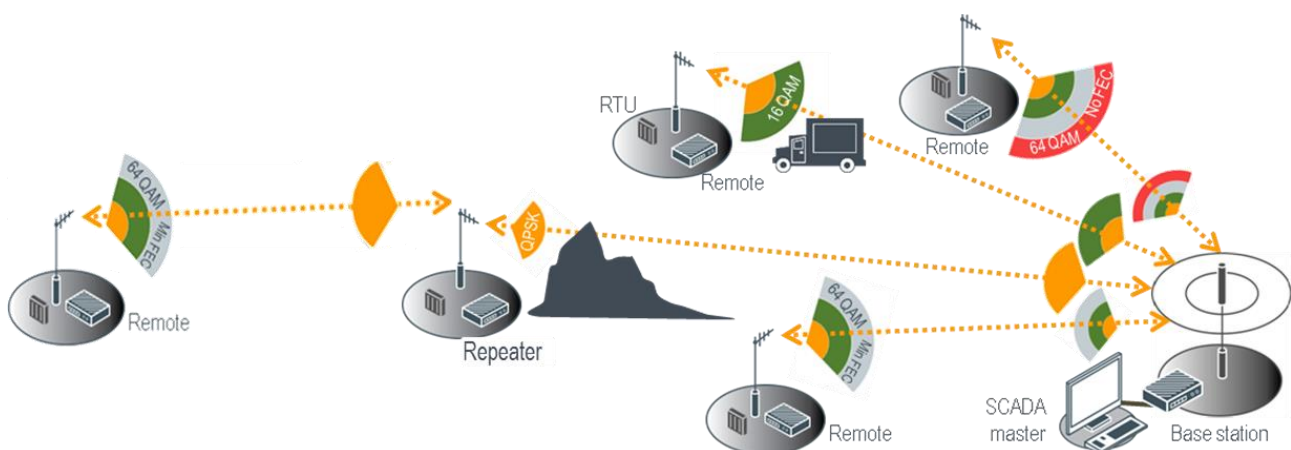
The Aprisa SR+ provides bidirectional Adaptive Coding and Modulation (ACM) which maximizes the use of the RF path on both downlink (base station/base-repeater to remote/repeater) and uplink (remote to base station/base-repeater or to repeater) to provide the highest radio capacity available.

When the Modulation Type is set to Adaptive, in unicast packets, the transmitted modulation and coding will be determined by the signal quality of the link to the destination radio. Link quality for each radio is determined both concurrently and independently.

When a broadcast packet (such as broadcast IP, multicast IP, and serial) is sent from the base to a remote/repeater, or from a repeater to a remote which is received by all remote radios, the signal quality of the worst remote link is used.

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

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



System Gain vs FEC Coding

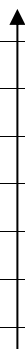
This table shows the relationship between modulation, FEC coding, system gain, capacity and coverage.

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

This table defines the modulation order based on gross capacity:

Modulation	FEC Coding	Capacity
QPSK (High Gain)	Max Coded FEC	Minimum
QPSK (Low Gain)	Min Coded FEC	
16QAM (High Gain)	Max Coded FEC	
QPSK	No FEC	
16QAM (Low Gain)	Min Coded FEC	
16QAM	No FEC	
64QAM (High Gain)	Max Coded FEC	
64QAM (Low Gain)	Min Coded FEC	
64QAM	No FEC	
256QAM (Low Gain)	Min Coded FEC	Maximum

This table defines the modulation order based on receiver sensitivity:

Modulation	FEC Coding	Coverage
QPSK (High Gain)	Max Coded FEC	Maximum
QPSK (Low Gain)	Min Coded FEC	
QPSK	No FEC	
16QAM (High Gain)	Max Coded FEC	
16QAM (Low Gain)	Min Coded FEC	
16QAM	No FEC	
64QAM (High Gain)	Max Coded FEC	
64QAM (Low Gain)	Min Coded FEC	
64QAM	No FEC	
256QAM (Low Gain)	Min Coded FEC	Minimum

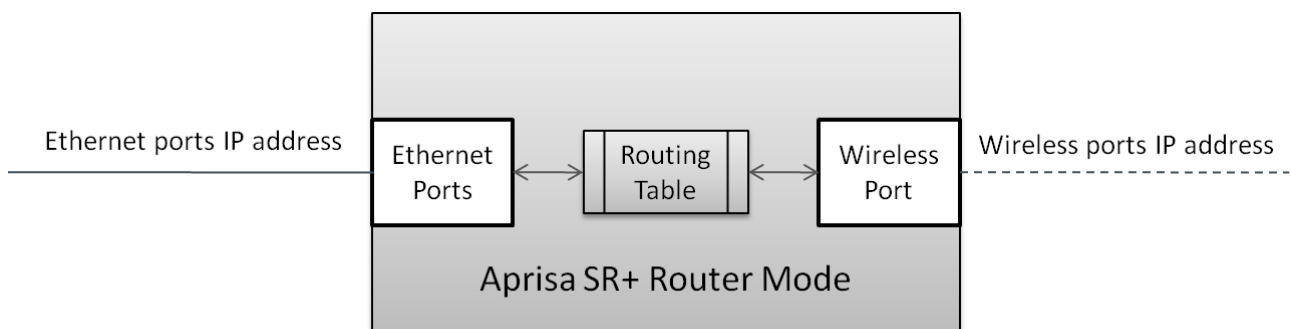
Network Layer

Packet Routing

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

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

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



Static IP Router

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

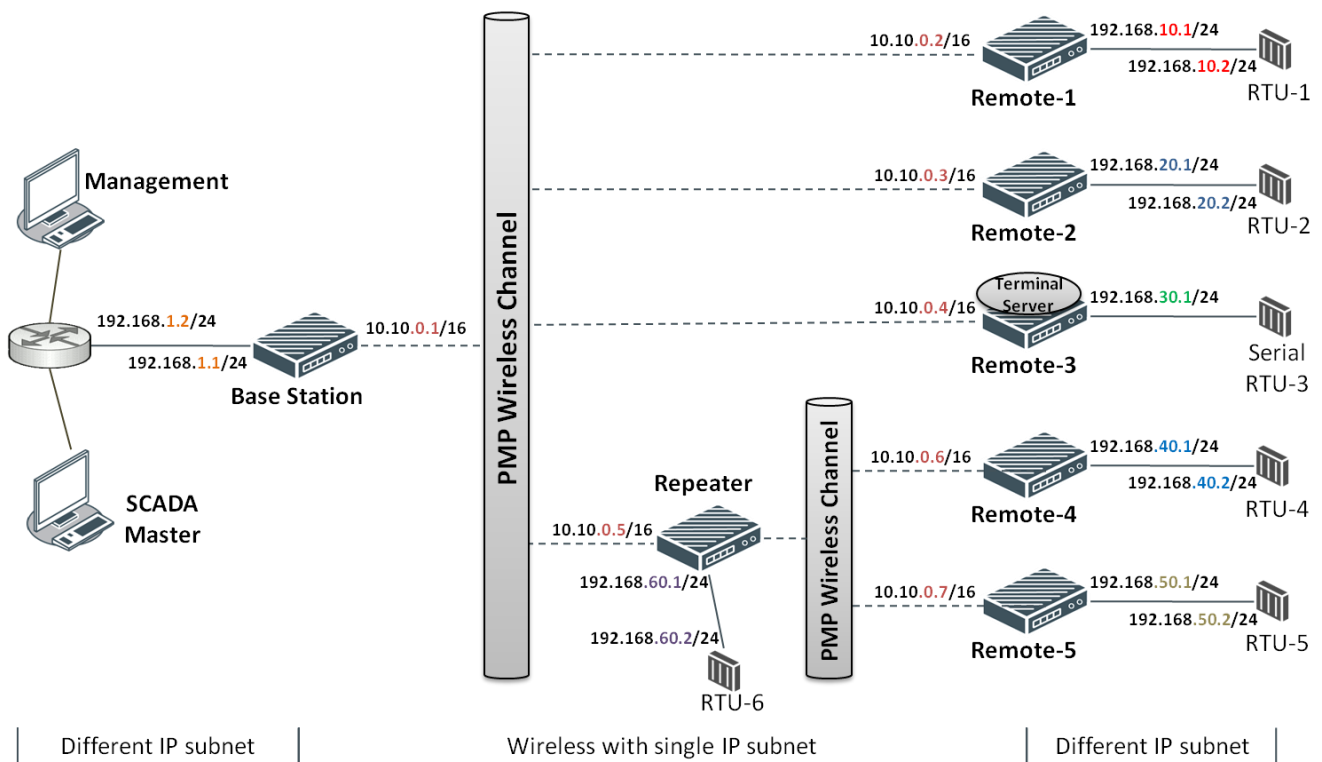
The Aprisa SR+ static router is semi-automated operation, where the routing table is automatically created in the base station and populated with routes to all remotes and repeater stations in the network during the registration process and vice versa, where the routing table is automatically created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

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

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

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

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



The Radio Network as a Gateway Router

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

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

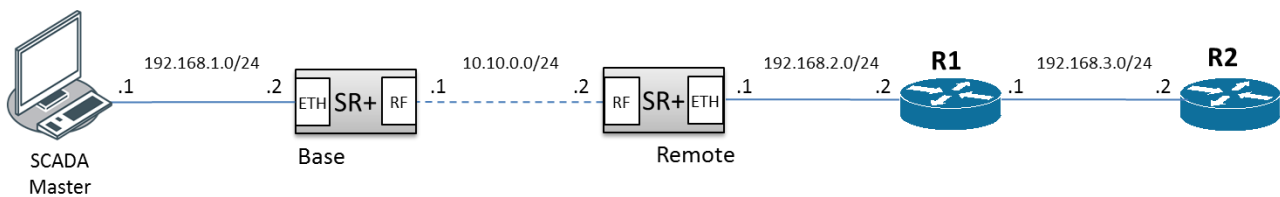
The ‘Radio interface IP address’ is used internally for the radio network and automatic routes. It is not used when setting static routes or default gateways.

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

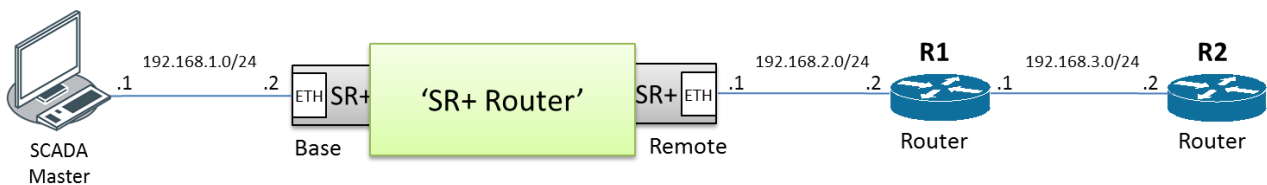
External network routers should be set with a high metric for the SR+ path, to prevent route updates being sent over the radio network.

The Radio Network as a Router - Example

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



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



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

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

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

Advanced Gateway Router Mode (AGRM) and Advanced Router Mode (ARM)

The Advanced Gateway Router Mode (AGRM) or Advanced Router Mode (ARM) are enabled when either Router or a Gateway Router mode is selected and the Advanced checkbox is ticked (see 'Terminal > Operating Mode' on page 116).

Advanced Gateway Router mode (AGRM) or Advanced Router mode (ARM) act like a true router between the Ethernet ports and the RF interface port where the next hop is either an Ethernet port or an RF port (in the non-advanced option the next hop is the Ethernet interface of the next hop radio and the RF interface are for internal use). This means that the RF Interface of the radio also becomes a public interface, so the user should be able to use this interface just like any other Ethernet interface.

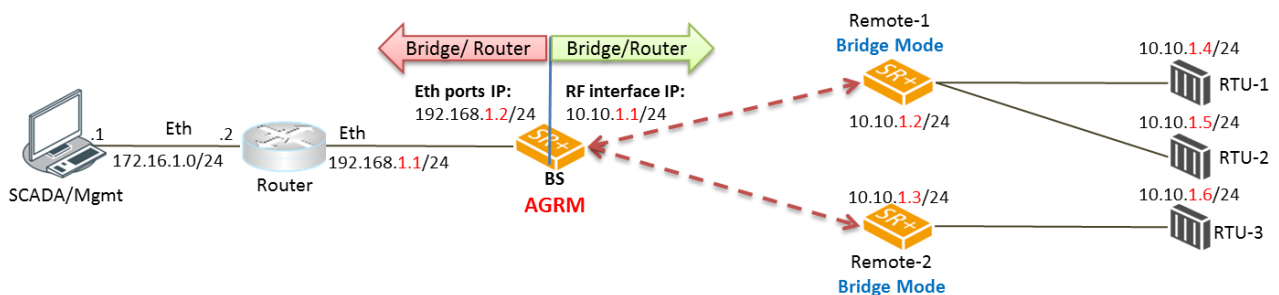
In AGRM, all Ethernet ports have the same IP address and subnet and in ARM, each Ethernet interface has a different IP address and subnet. In addition, the advanced option supports a new mix between AGRM / ARM and Bridge Mode in a radio network. The following mix of [Base Station] - [Repeater / Remote] networks are supported:

- **AGRM / ARM - Bridge network** i.e. base station AGRM / ARM and repeater and remote radios in Bridge mode.
- **Bridge - AGRM / ARM network** i.e. base station in Bridge mode and repeater and remote radios are in AGRM / ARM, where each node in the network can act as independent router without depending on other nodes in the network.
- **Bridge - Mix [AGRM / ARM and Bridge] network** i.e. base station in Bridge mode and remotes are a mix of Bridge and AGRM / ARM.
- **AGRM / ARM - Mix [AGRM / ARM and Bridge] network** i.e. base station in AGRM / ARM and remotes are a mix of Bridge and AGRM / ARM.
- **AGRM / ARM - AGRM / ARM network** i.e. base station in AGRM / ARM and repeater and remote radios are also in AGRM / ARM.

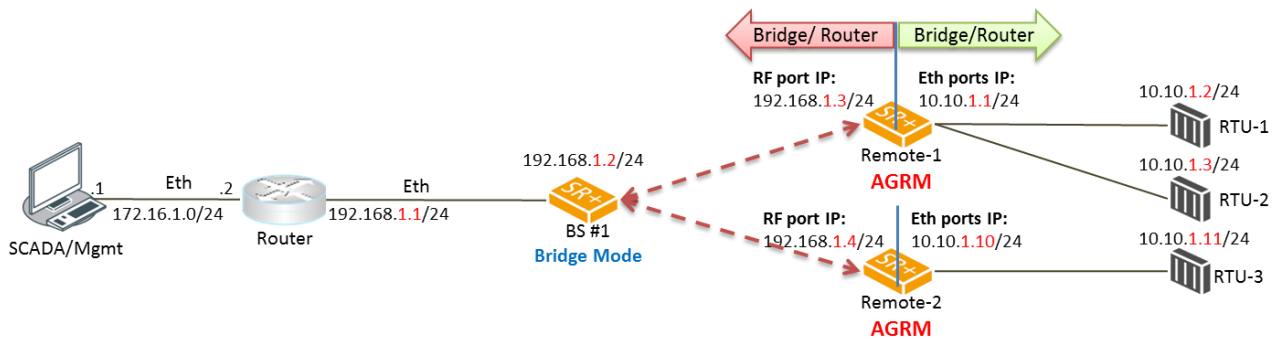
The last option is a fully routed network where it is recommended to use the standard router modes to benefit from the radio port auto IP assignment and auto static route build for all associated devices connected to the radio network.

Note: A mix between advanced router modes and standard router modes in the network is prohibited and will raise a 'network configuration warning' alarm. If a user wants to build a full routed network, use the standard router modes for the base station, repeater and remote radios.

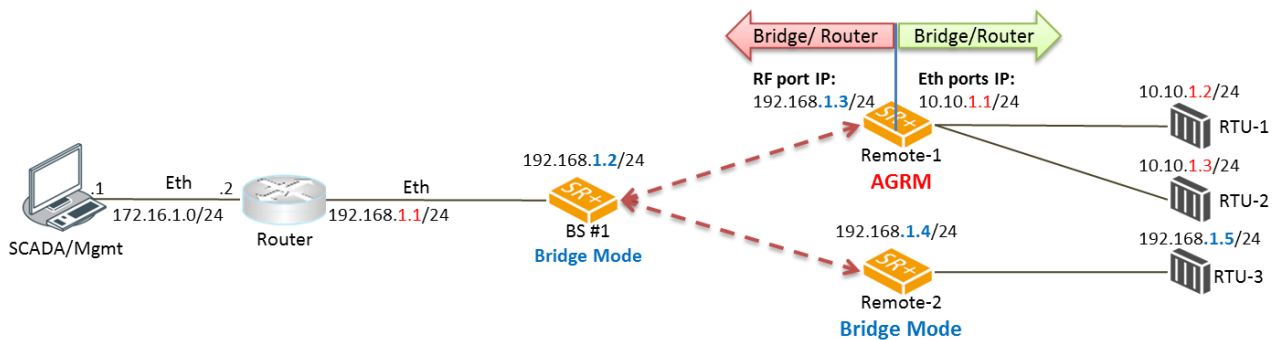
The following figures are examples of the currently supported networks as described above.



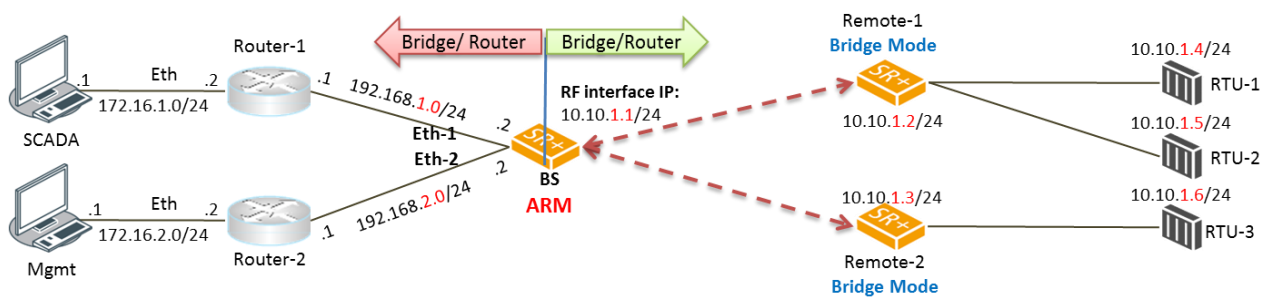
The above figure describes a mixed radio mode network (AGRM-Bridge) where base station is in Advanced Gateway Router Mode (AGRM) and the remote radios are in bridge mode (where the base station is AGRM / ARM and all remotes must be in the same bridge mode). RTUs must set their default gateway to 10.10.1.1 which is RF IP Address of base station to reach the SCADA master.



The above figure describes a mixed radio mode network (Bridge-AGRM) where the base station is in Bridge Mode and remote radios are in AGRM. To reach RTU-3 (10.10.1.11), the external router must use a next hop gateway of 192.168.1.4 which is RF Interface address of Remote-2.



The above figure describes a mixed radio mode network (Bridge-Mix [AGRM and Bridge]) where the base station is in Bridge Mode and remote radios are a mix of AGRM and Bridge mode. To reach RTU-2 (10.10.1.3), the external router must use a next hop gateway of 192.168.1.3 which is RF Interface address of Remote-1. To reach RTU-3 (192.168.1.5), the external router can send the traffic directly on the bridge subnet 192.168.1.x/24 network.



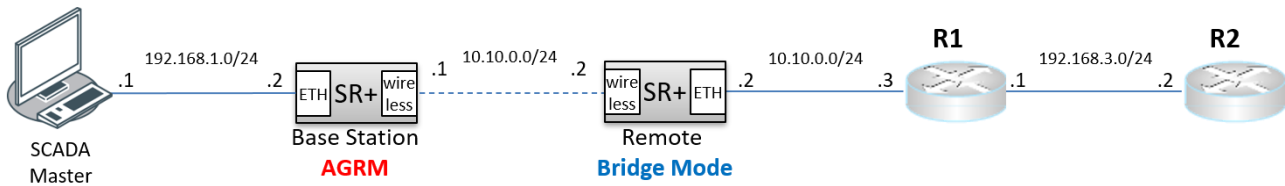
The above figure describes a mixed radio mode network (ARM-Bridge) where base station is in Advanced Router Mode (ARM) and remote radios are in bridge mode. It's the same case as the AGRM-Bridge network above, but each Ethernet interface has a different IP address and subnet at the ARM base station.

The following functions supported in AGRM / ARM is the differences between Advanced Router Mode options (AGRM / ARM) and standard Router Mode options Gateway Router Mode (GRM) / Router Mode (RM), such as AGRM vs GRM and/or ARM vs RM:

- The radio interface IP Address (RF IP Address) is associated with Ethernet MAC Address so it can be addressed like any other Ethernet Interface. The radio interface IP address will ARP respond to ARP request with his MAC address.
- The radio interface IP address can be used for radio management functions such as SNMP, ICMP and SNTP.
- External routers can use radio interface IP address as next hop / default gateway.
- The radio Interface IP address can be used as the 'Local IP Address' in terminal server.
- Auto assignment of radio interface IP address is done in a routed network of Router Mode (RM) and Gateway Router Mode (GRM) but not in AGRM / ARM. In AGRM / ARM the radio interface IP address is manually configured.
- Changes to the radio Interface IP address will be included in the remote registration or re-registration with base station, respectively.
- Both units in a protected station will share the radio Interface IP address and a protection switch will result in new active unit sending out a gratuitous ARP to advertise its ownership of radio Interface IP address.
- AGRM / ARM allows a mix with Bridge mode, so a AGRM / ARM-Bridge or Bridge-AGRM / ARM or a Bridge-Mix [AGRM / ARM and Bridge] network can be created. A network configuration warning alarm will be raised on base station if this condition is not met.
- The ARP table will report a radio interface IP address if any address is learned on this interface.

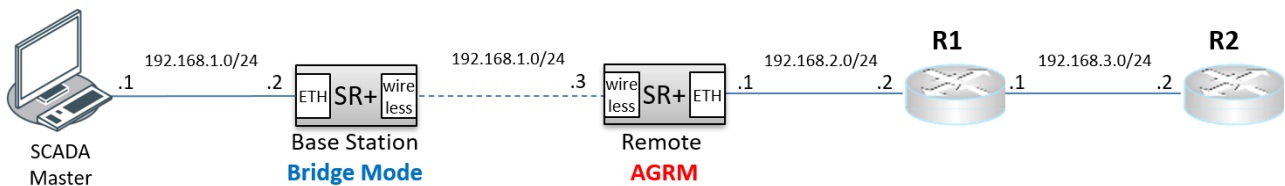
Advanced Gateway Router (AGRM) or Advanced Router Mode (ARM) Static Route - Example

The purpose of this example is to determine the static route setting for router R2 in the base station and remote radio in the following AGRM-Bridge, Bridge-AGRM networks.



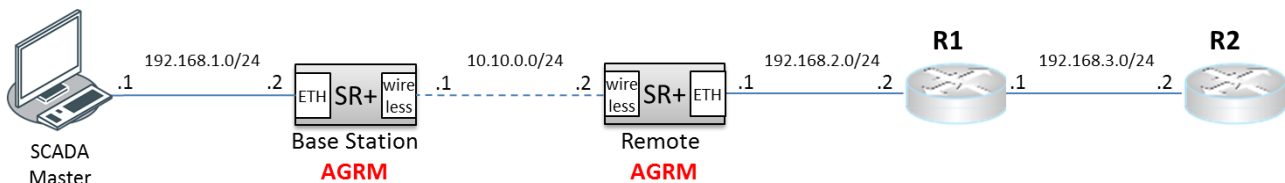
In the above figure, the static route setting for router R2 at the base radio AGRM will be:

Destination Address	Destination Mask	Gateway Address
192.168.3.0	255.255.255.0	10.10.0.3



In the above figure, the static route setting for router R2 at the remote radio AGRM will be:

Destination Address	Destination Mask	Gateway Address
192.168.3.0	255.255.255.0	192.168.2.2



In the above figure, the static route setting for router R2 at the Base Station AGRM will be:

Destination Address	Destination Mask	Gateway Address
192.168.3.0	255.255.255.0	10.10.0.2

Note: In AGRM / ARM - AGRM / ARM network scenario, automatic route build of the radio network is currently not supported. Auto route build for the associated devices to the radio network (i.e. next hop devices) is only supported in the standard router modes where the base station, repeater and remote radios are all in standard router modes.

Static IP Router - Human Error Free

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

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

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

Terminal Server - Transition to Converged Ethernet / IP Network

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

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

Network Address Translation (NAT) Router

The NAT functions are only available in Advanced Gateway Router Mode (AGRM) or Advanced Router Mode (ARM). Configuring NAT on the standard router modes will raise a 'configuration not supported' alarm.

The current implementation of One-to-One NAT and Port Forwarding NAPT supports network configurations of AGRM / ARM mode, such as AGRM / ARM - Bridge (or mix of Bridge and AGRM / ARM), Bridge - AGRM / ARM, Bridge - Mix [AGRM / ARM and Bridge] and AGRM / ARM - AGRM / ARM networks (where in AGRM / ARM - AGRM / ARM network, either base station or remote radios can be NAT enabled, not both). It is recommended reading the section about AGRM / ARM above before reading this section. The NAT is enabled in IP > NAT' on page 193.

Network Address Translation (NAT) is a method of remapping external (public) IP addresses into other local/internal (private) IP addresses and vice versa; providing transparent routing to end users/hosts via the AGRM / ARM router.

In One-to-One NAT, IP addresses in the IP address space are mapped (translated) from external / public interface IP address into other local / private interface IP address space (and vice-versa) via the AGRM / ARM router, where One-to-One IP addresses are translated (including recalculating affected fields of the header, like IP header checksum or higher-level checksum).

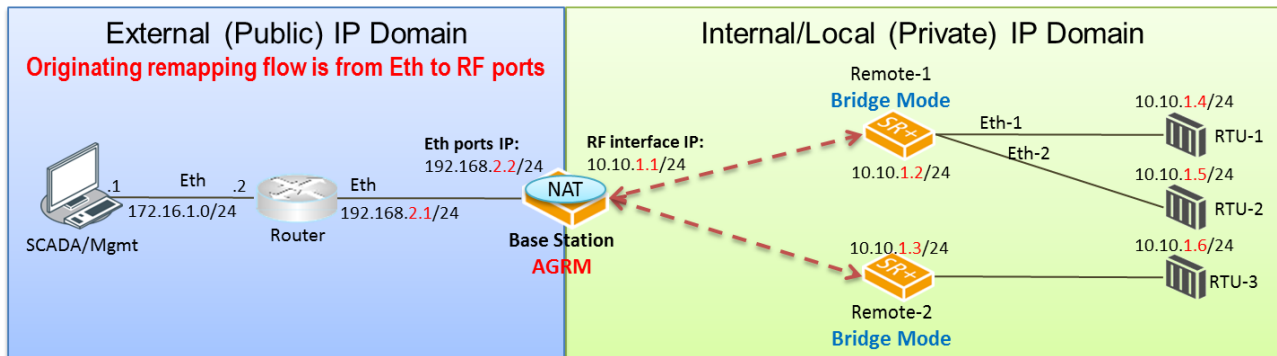
The advantage of NAT is to allow preservation of the multiple local (private) IP addresses, even if the external (public) IP addresses change. Another advantage is the security function of NAT where private / internal IP addresses are 'hidden' from the external / public IP domain behind the NAT. Also, private / internal IP addresses can be reused in different NAT routers in the radio network.

In order to easily explain the NAT function, the following terminology is used:

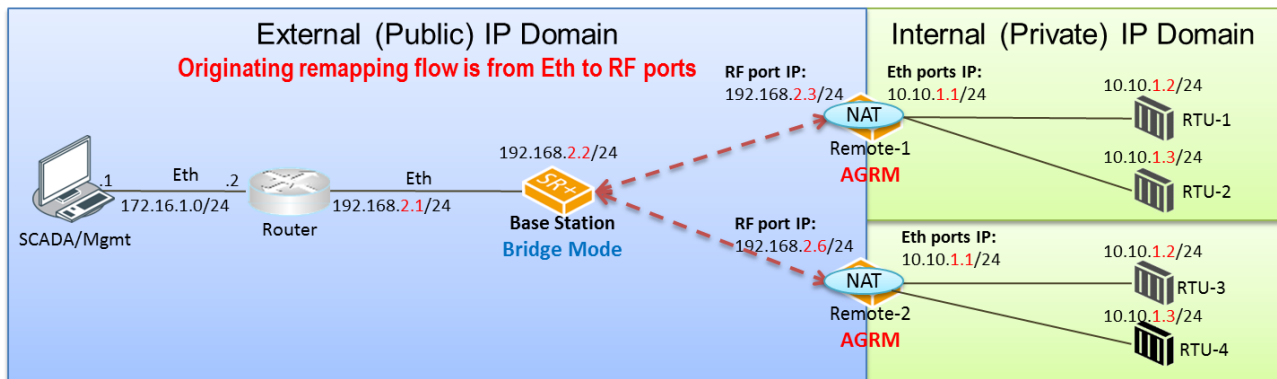
- **Session** - an IP / TCP / UDP service (identified by IP address and/or TCP / UDP port (or ICMP query ID))
- **Public (external) / Private (internal / local) IP domain** - the public / external and private / local IP network domains is used to define the NAT gating function and the inbound and outbound session NAT translation process based on NAT Address Map Table (AMP). The external / local notations used for IP address and TCP / UDP ports are as follow:
 - **Eth: eIP:ePort** - represents the external domain Ethernet port, IP address and TCP/UDP port.
 - **Eth: iIP:iPort** - represents the internal/local domain Ethernet port, IP address and TCP/UDP port.
- **Inbound / Outbound** - session originating from external to local network domain will be considered as inbound session. Session originating from internal / local to external network domain will be considered as outbound traffic. Outbound session only may for example represent report by exception. Inbound and Outbound session may for example represent poll / response.

Public (External) and Private (Internal/Local) IP Domains

The following figure describes the Public (external) and Private (internal/local) IP domains in AGRM / ARM-Bridge network. The NAT IP domains splits at the NAT function enabled device, the AGRM base station.



The following figure describes the Public (external) / Private (internal) IP domains in Bridge-AGRM / ARM network. The NAT IP domains splits at the NAT function enabled device, the AGRM remote radios.



One-to-One NAT Description

One-to-One NAT method is based on the remapping of external / public IP address space (e.g. radio IP space) into another internal / private IP space (e.g. RTUs IP space) and vice versa, by modifying the IP address. UDP / TCP ports will preserve their source / destination port numbers. NAT IP address translation function is performed before routing for inbound packets and after routing for outbound packets. NAT can translate and handle TCP, UDP, ICMP query, IP fragments and FTP packet types.

One-to-One NAT is translating inbound session packets per public interface and based on NAT Address Map Table (Address Map Table), supporting max 20 entries. Outbound session packets are translated based on the reverse table of Address Map Table. The user can configure the public port and Address Map Table in 'IP > NAT' page. NAT is translating inbound packets (IP address) originating in public network domain and destined for devices in private network domain. Outbound NAT translation refers to packets originated in private network and destined for devices in public network. Inbound or outbound packets will be dropped if it does not match any translation criteria defined for the appropriate public interface and Address Map Table configuration.

Monitoring the NAT translation sessions is available in 'Monitoring > NAT' with max 250 entries in NAT session table. Entries with a max idle time will be aged in favor of a new entry if the limit is reached. Entries are automatically removed after a period of inactivity as configured at 'IP > NAT > Settings TAB' in 'Session Idle Timeout'. NAT packet statistics of inbound and outbound sessions are also reported in the NAT session table per session basis.

NAT alarms are supported for any invalid configuration settings, including improper translation entries, invalid timeout, along with any incompatibilities with other feature settings will cause a 'configuration not supported' alarm.

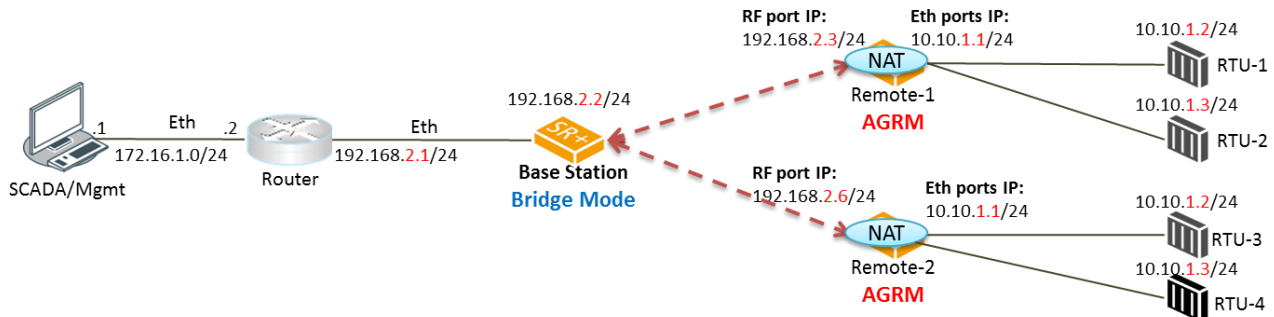
As shown in the figure of Bridge-AGRM network above, IP addresses used in one NAT internal domain can be reused by any other NAT internal domain. In the example figure above, RTUs connected to AGRM remote-1 and remote-2 reusing the same IP addresses space i.e. in this case all RTUs can have the same IP addresses space per remote radio.

NAT router radio will respond to inbound ARP requests for IP addresses in public range as define in Address Map Table with the MAC address of the public interface. Outbound ARP request for private IP range will ARP respond with MAC address of the NAT radio private/local interface.

In a protected station, all NAT configurations are shared between both the active and standby radios. The standby radio will not perform any NAT translation and routing. After a protection switch-over, NAT session table will be aged. For smooth protection switching and continuous traffic flow, the protected station automatically supports MAC address cloning for both active and standby radios NAT public interface (the cloned MAC address is presented at 'Maintenance > Advanced' page in 'RF Mac Address' field).

One-to-One NAT Operation

The following figure describes an example of a radio network with One-to-One NAT configured at remotes in AGRM mode including the user configuration of NAT Address Map Table and expected session table (a detailed in / outbound session is shown for clarity of explanation, where NAT session table in SuperVisor will show a session in one line which will include inbound / outbound transactions, session duration, statistics, etc).



NAT Address Map Table - [Remote-1, Public Interface: RF Port]					
Order	Match To...			Translate To...	Active
	Public Dest IP Address Start	Public Dest IP Address End	Protocol	Private Dest IP Address Start	
1	192.168.2.4	192.168.2.5	Any	10.10.1.2	✓

NAT Address Map Table - [Remote-2, Public Interface: RF Port]					
Order	Match To...			Translate To...	Active
	Public Dest IP Address Start	Public Dest IP Address End	Protocol	Private Dest IP Address Start	
1	192.168.2.7	192.168.2.8	Any	10.10.1.2	✓

NAT Session Table - [Remote-1]							
ID	In/Out bound	Public IP Src Addr	Public IP Dest Addr	Protocol	Private IP Src Addr	Private IP Dest Addr	Comments
1	In	172.16.1.1	192.168.2.3	Any	N/A	N/A	Management > Remote1
2	In	172.16.1.1	192.168.2.4	Any	172.16.1.1	10.10.1.2	SCADA Master > RTU-1
3	Out	192.168.2.4	172.16.1.1	Any	10.10.1.2	172.16.1.1	RTU-1 > SCADA Master
4	In	172.16.1.1	192.168.2.5	Any	172.16.1.1	10.10.1.3	SCADA Master > RTU-2
5	Out	192.168.2.5	172.16.1.1	Any	10.10.1.3	172.16.1.1	RTU-2 > SCADA Master

The configured NAT Address Map Table of remote-1 shows that NAT will translate public interface RF port IP address range 192.168.2.4 - 5 to private IP address range 10.10.1.2 - 3. NAT Address Map Table of remote-2 shows reuse of the same private IP address range where NAT will translate public IP address range 192.168.2.7 - 8 to private IP address range 10.10.1.2 - 3.

The NAT session table of remote-1 session ID #1 shows that the public interface RF port address can't be used in the NAT function or in NAT Address Map Table configuration as it is reserved for the radio access (e.g. management access, etc). This line is just for explanation purposes as in SuperVisor it will not be shown in NAT session table since no NAT translation is made as it's not part of the Address Map Table configuration table.

Session ID #2 and #3 shows the inbound and outbound session translation when the SCADA master accesses RTU-1 and vice versa. From the SCADA master perspective, RTU-1 public address is 192.168.2.4 (as it doesn't know the real address 10.10.1.2 of RTU-1 which is 'hidden' behind the NAT). As explained above, SuperVisor will not show session ID #2 and #3 in one line as these inbound / outbound transactions are considered as one session.

NAT translates the inbound session public RF port destination IP 192.168.2.4 to 10.10.1.2 on Eth port, the real private IP destination of RTU-1. The source address of SCADA master 172.16.1.1 remains unchanged during the inbound NAT translation as shown in session ID#2.

Outbound session #3 shows the response of RTU-1 to SCADA master and NAT translation of Eth port private source address 10.10.1.2 to 192.168.2.4 on RF port public source address. The destination address of SCADA master 172.16.1.1 remains unchanged during the outbound NAT translation.

Port Forwarding NAT (NAPT) Description

Port Forwarding NAT method is based on the remapping (translating) of an external / public TCP/UDP port of a single public IP addresses (e.g. BS radio Eth port-1 IP address) into multiple internal / private IP space (e.g. remote and RTUs IP address space) and vice versa, by translating public TCP/UDP ports space to the private IP space. The NAT translation function is performed before routing for inbound packets and after routing for outbound packets. NAT can translate and handle TCP, UDP, ICMP query, IP fragments and FTP packet types.

Port Forwarding NAT translates inbound session packets per public interface based on the NAT Address Map Table supporting max 20 entries. Outbound session packets are translated based on the reverse of the Address Map Table based on dynamic table entries created whenever a session is not configured in the Address Map Table (no dynamic session is allowed on inbound session). The user can configure the public port and Address Map Table in 'IP > NAT' page. NAT translates inbound packets (IP address) originating in public network domain and destined for devices in private network domain. Outbound NAT translation refers to packets originating in a private network and destined for devices in a public network. Inbound packets will be dropped if they don't match any translation criteria defined for the appropriate public interface and Address Map Table configuration.

Monitoring the NAT translation sessions is available in 'Monitoring > NAT' with max 250 entries in NAT session table. Entries with a max idle time will be aged in favour of a new entry if the limit is reached. Entries are automatically removed after a period of inactivity as configured at 'IP > NAT > Settings TAB' in 'Session Idle Timeout'. NAT packet statistics of inbound and outbound sessions are also reported in the NAT session table on a per session basis.

NAT alarms are supported for any invalid configuration settings, including improper translation entries, invalid timeout, along with any incompatibilities with other feature settings which will cause a 'configuration not supported' alarm.

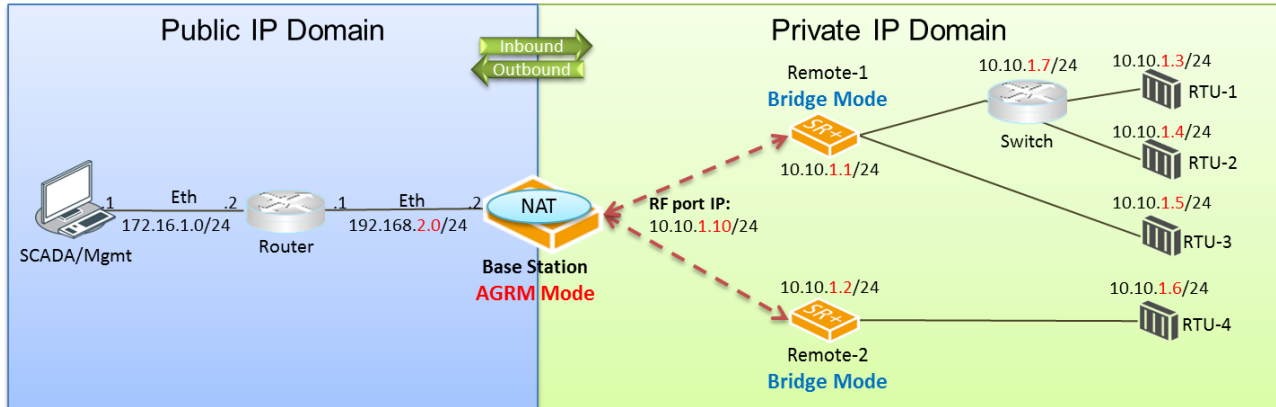
IP addresses used in one NAT internal domain can be reused by any other NAT internal domain.

A NAT router radio will respond to inbound ARP requests for IP addresses in public range as defined in the Address Map Table with the MAC address of the public interface. An outbound ARP request for a private IP range will respond with the MAC address of the NAT radio private/local interface.

In a protected station, all NAT configurations are shared between both the active and standby radios. The standby radio will not perform any NAT translation and routing. After a protection switch-over, the NAT session table will be aged. For smooth protection switching and continuous traffic flow, the public interface MAC address will be used.

Port Forwarding NAT (NAPT) Operation

The following figure describes an example of Port Forwarding used for security, hiding the private IP address from the public interface network and it can be used to preserve private IP address even if public IP network subnet might change, reducing operational risk and expense. In this example, Port Forwarding NAT is configured at the Base Station in AGRM mode including the user configuration of NAT Address Map Table and expected session table (a detailed in / outbound session is shown for clarity of explanation, where NAT session table in SuperVisor will show a session in one line which will include inbound / outbound transactions, session duration, statistics, etc).



NAT Address Map Table - [Base Station, Public Interface: Eth-1]

Order ID	Match To...				Translate To...		Active
	Public Dest IP Address Start	Public Dest Port Start	Public Dest Port End	Protocol	Private Dest IP Address Start	Private Dest Port	
1	192.168.2.2	8081	8087	Any	10.10.1.1	80	✓
2	192.168.2.2	10003	10006	Any	10.10.1.3	502	✓
3	192.168.2.2	101	107	ICMP	10.10.1.1	200	✓

NAT Session Table - [Base Station, Eth-1]

ID	In Out bound	Public IP Src Addr	Public IP Dest Addr	Public Src Port	Public Dst Port	Protocol	Private IP Src Addr	Private IP Dest Addr	Private Src Port	Private Dst Port	Comments
1	In	172.16.1.1	192.168.2.2	PPP	80	Any	N/A	N/A	N/A	N/A	Management > Base
2	In	172.16.1.1	192.168.2.2	XYZ	8081	Any	172.16.1.1	10.10.1.1	XYZ	80	Management > Remote-1
3	Out	192.168.2.2	172.16.1.1	8081	XYZ	Any	10.10.1.1	172.16.1.1	80	XYZ	Remote-1 > Management
4	In	172.16.1.1	192.168.2.2	XXX	10003	Any	172.16.1.1	10.10.1.3	XXX	502	SCADA > RTU-1 (Modbus)
5	Out	192.168.2.2	172.16.1.1	10003	XXX	Any	10.10.1.3	172.16.1.1	502	XXX	RTU-1 (Modbus) > SCADA
6	In	172.16.1.1	192.168.2.2	FFF	20000	Any	N/A	N/A	N/A	N/A	To Base CPU (and drop)
7	Out	192.168.2.2	172.16.1.1	10003	RRR	Any	10.10.1.3	172.16.1.1	502	RRR	RBE RTU-1 > SCADA
8	Out	192.168.2.2	172.16.1.1	NNN	23	Any	10.10.1.3	172.16.1.1	ZZZ	23	RTU-1 (Telnet) > SCADA
9	In	172.16.1.1	192.168.2.2	23	NNN	Any	172.16.1.1	10.10.1.3	23	ZZZ	To Base CPU (and drop)
10	In	172.16.1.1	192.168.2.2	N/A	102	ICMP	172.16.1.1	10.10.1.1	N/A	200	Ping (Req.) > Remote-2
11	Out	192.168.2.2	172.16.1.1	102	N/A	ICMP	10.10.1.1	172.16.1.1	200	N/A	Remote-2 > Ping (Resp.)

The configured NAT Address Map Table of the Base Station shows that Port Forwarding NAT will translate; NAT Address Map Table Line 1 configuration will translate public interface Eth-1 IP address 192.168.2.2 port range 8081 - 8087 to private IP address range 10.10.1.1 - 7 and port 80.

NAT Address Map Table Line 2 configuration will translate public IP address 192.168.2.2 port range 10,003 - 10,006 to private IP address range 10.10.1.3 - 6 and port 502 (Modbus).

NAT Address Map Table Line 3 configuration will translate ping messages public IP address 192.168.2.2 ping query ID 101 - 107 to private IP address range 10.10.1.1 - 7 and ping query ID 200.

The NAT session table of Base Station session ID #1 shows that the public interface Eth-1 IP address and TCP/UDP port 80 can't be used in the NAT function or in NAT Address Map Table configuration as it is reserved for the radio access (e.g. management access, etc). This line is just for explanation purposes as in SuperVisor it will not be shown in NAT session table since no NAT translation is made and it's not part of the Address Map Table configuration table.

Session ID #2 and #3 shows the inbound and outbound session translation when the Management accesses remote-1 using HTTP (port 80) and vice versa. From the Management perspective, remote-1 public address is 192.168.2.2 and port 8081 (as it doesn't know the real address 10.10.1.1 which is 'hidden' behind the NAT). As explained above, SuperVisor will not show session ID #2 and #3 in separate lines as these inbound / outbound transactions are considered as one session.

Session ID #4 and #5, are the same as sessions ID #2 and #3 and supported by NAT Address Map Table configuration ID #2.

Session ID #6 shows that an inbound session will drop packets if the session configuration is not supported in the NAT Address Map Table, or there is no outbound session initiated that can support a response of an inbound session (even if not in Address Map Table).

Session ID #7 and #8 are session initiated outbound sessions like RTU-1 RBE (Report by Exception) and Telnet session initiated from RTU-1, respectively. Initiated outbound sessions will be either translated per reverse Address Map Table configuration and if no configuration rule exists, then it will be built dynamically by the NAT function to later support a response from inbound session. Inbound session ID #9 is an example of a response to initiated outbound session ID #8, which is a dynamically created NAT translation table/session.

Session ID #10 and #11, are the same as sessions ID #2 and #3 and supported by NAT Address Map Table configuration ID #3, but this rule is set for ICMP ping. Instead of TCP/UDP port, NAT uses the ping query ID for translation. To run a ping across port forwarding NAT, user can use the hrPing.exe utility (run as admin) that can control the ping query ID value. Standard Windows ping command doesn't have the capability to control the ping query ID value.

Bridge Mode with VLAN Aware

Ethernet VLAN Bridge / Switch Overview

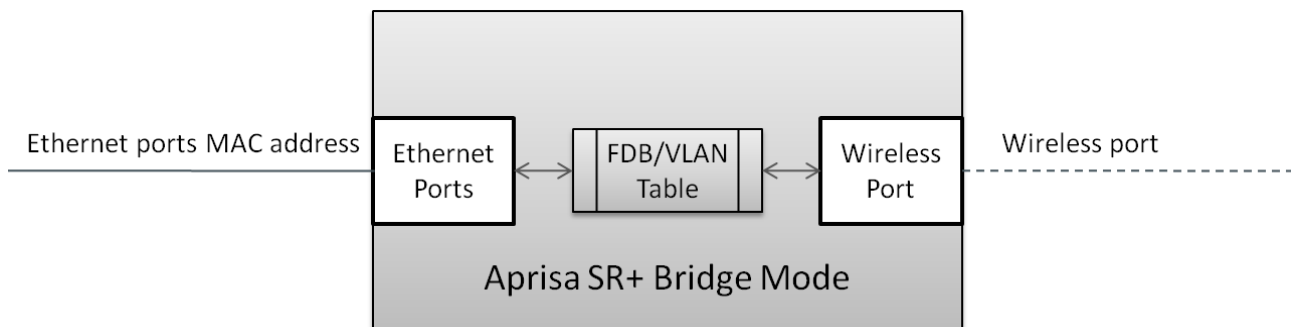
The Aprisa SR+ in Bridge mode of operation is a standard Ethernet Bridge based on IEEE 802.1d or VLAN Bridge based on IEEE 802.1q/p which forward / switch Ethernet packet based on standard MAC addresses and VLANs using FDB (forwarding database) table decisions. VLAN is short for Virtual LAN and is a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

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

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

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

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



VLAN Bridge Mode Description

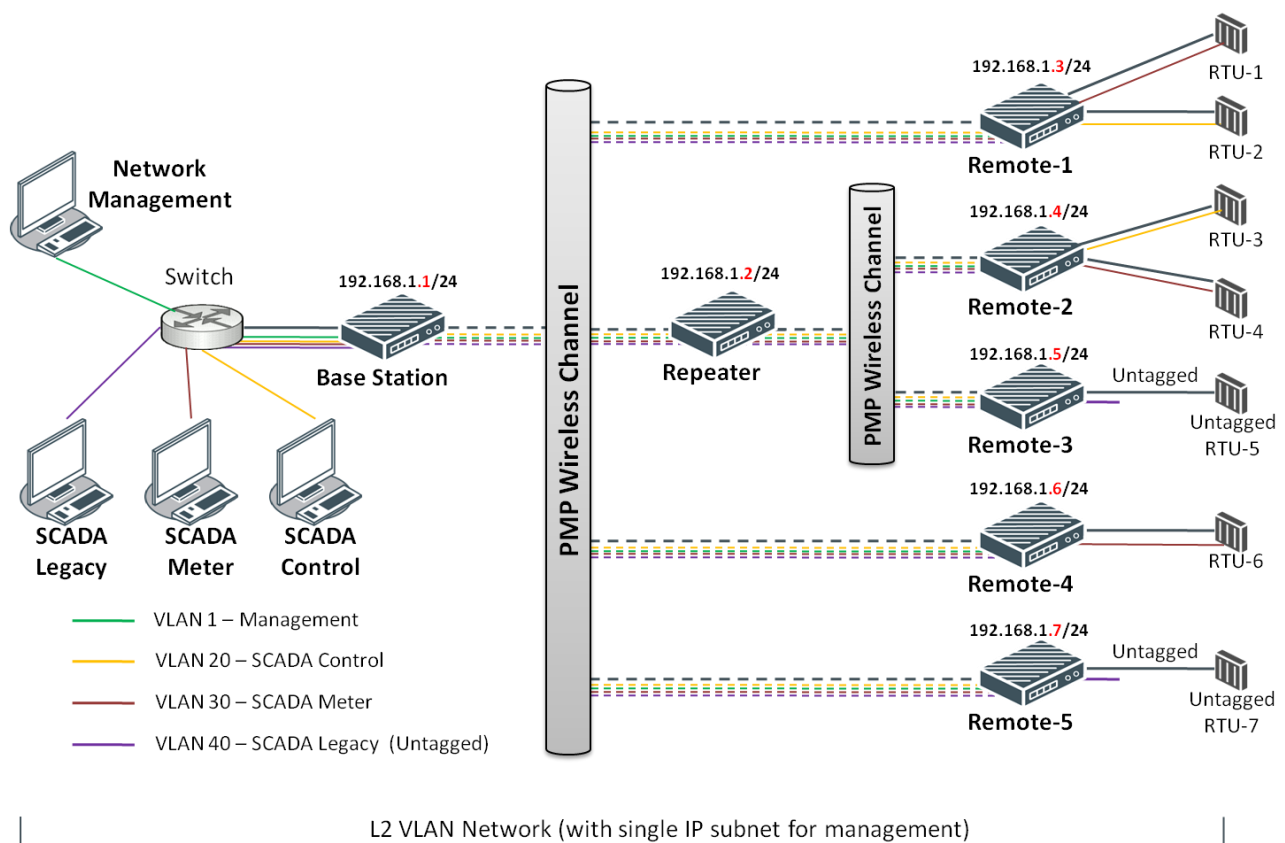
General - Aprisa SR+ VLAN Bridge

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

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

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

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



VLANs - Single, Double and Trunk VLAN ports

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

A single VLAN can be used to segregate traffic type.

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

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

VLAN Manipulation - Add / Remove VLAN Tags

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

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

QoS using VLAN

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

Terminal Server Operational in Bridge and Router Modes

VLAN and IP address Configuration per Terminal Server in Bridge Mode

In all network applications of a converged IP network where serial interfaces are part of an IP network, the remote Terminal Server or IP Terminal Server (generally configured in Base station) associated to a serial interface is part of a SCADA service and as a standalone service.

The Aprisa SR+ allows Terminal Server and IP Terminal Server service to be segregated from the management service both in VLAN, IP and QoS in Bridge mode. It allows the user:

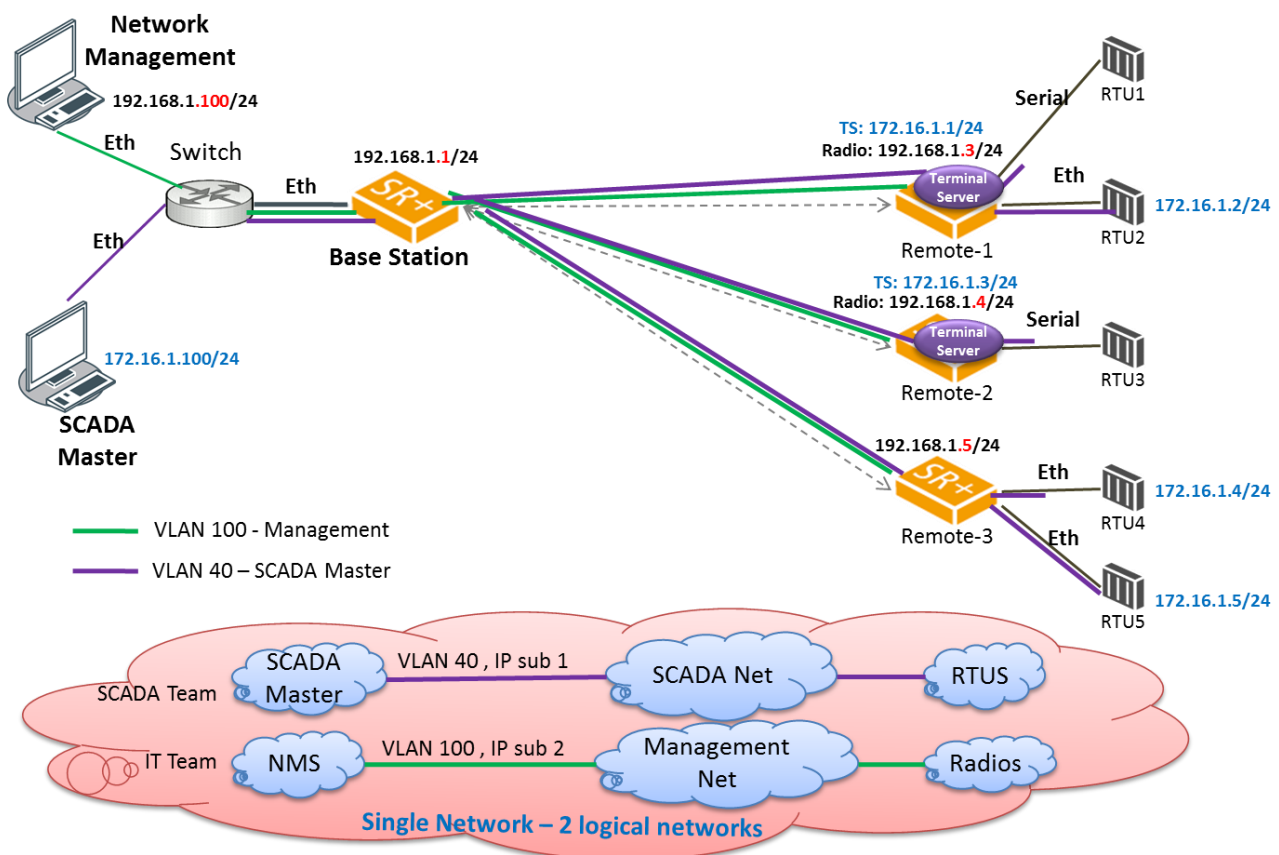
- complete separation of SCADA and management network in term of VLAN and IP subnet
- complete separation of SCADA and management network in term of VLAN
- complete separation of SCADA and management in term of IP subnet
- a unified network with single IP subnet

Since Terminal Server is part of the bridge network, it supports gratuitous ARP and ARP reply to ARP request. It also supports fixed user configuration of serial port QoS per VLAN Priority (QoS PCP bits).

The following are examples of Terminal Server and IP Terminal Server in a bridge network;

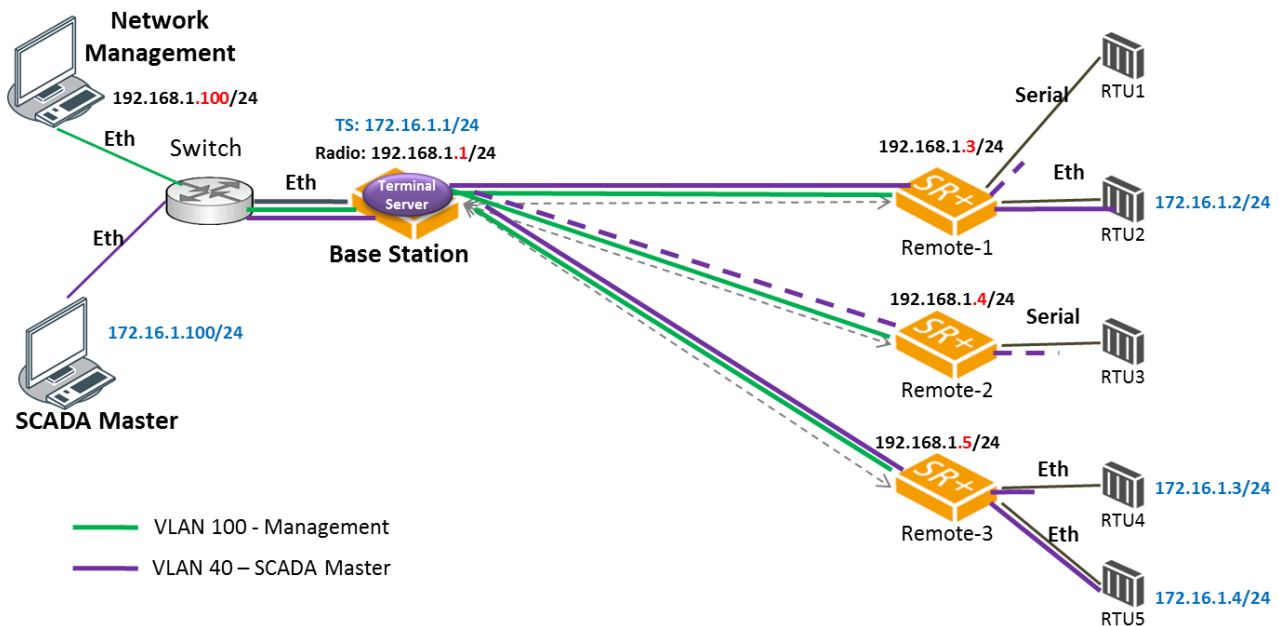
IP and VLAN segregation of remote Terminal Server and radio management

The following figure describes the IP and VLAN segregation of remote Terminal Server and radio management where the Terminal Server in remote 1 and 2 are configured with different VLANs from the management VLAN and on the same IP address subnet as the RTUs different to the IP address subnet of the radios. Thus, in fact it's two separated logical networks reside on the same physical network (as show in bottom of the figure).



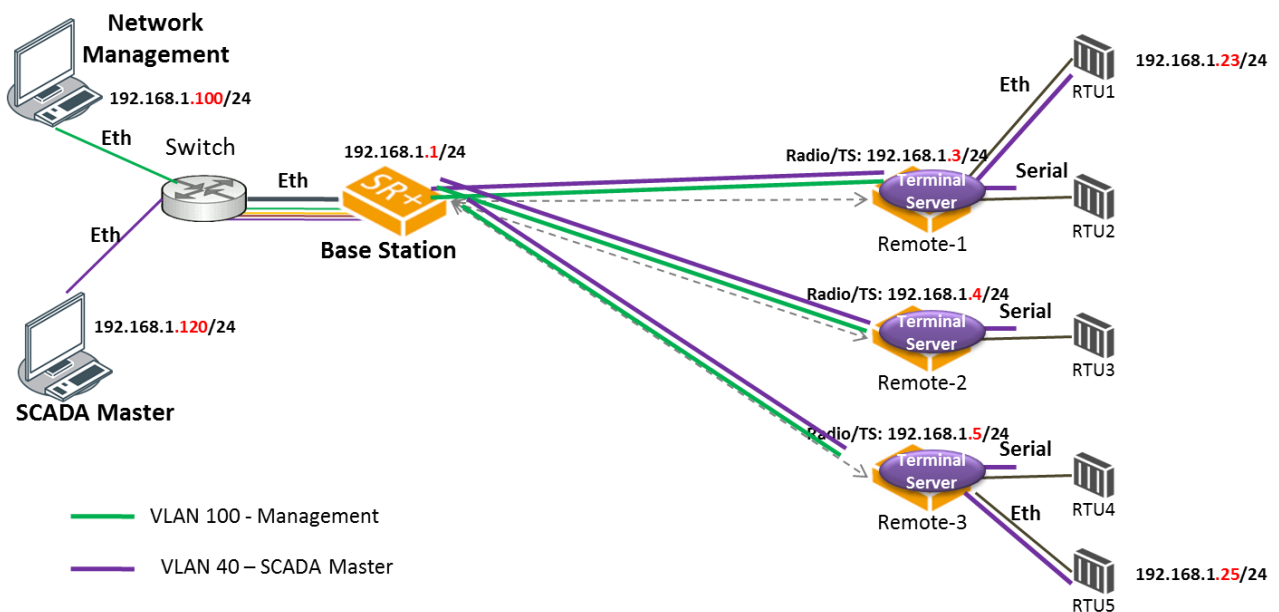
IP and VLAN segregation of IP Terminal Server and radio management

The following figure describes the IP and VLAN segregation of IP Terminal Server and radio management. It is the same as the previous example except the IP Terminal Server is configured and used in the Base station with different VLANs and IP addresses from the radio management VLAN and IP.

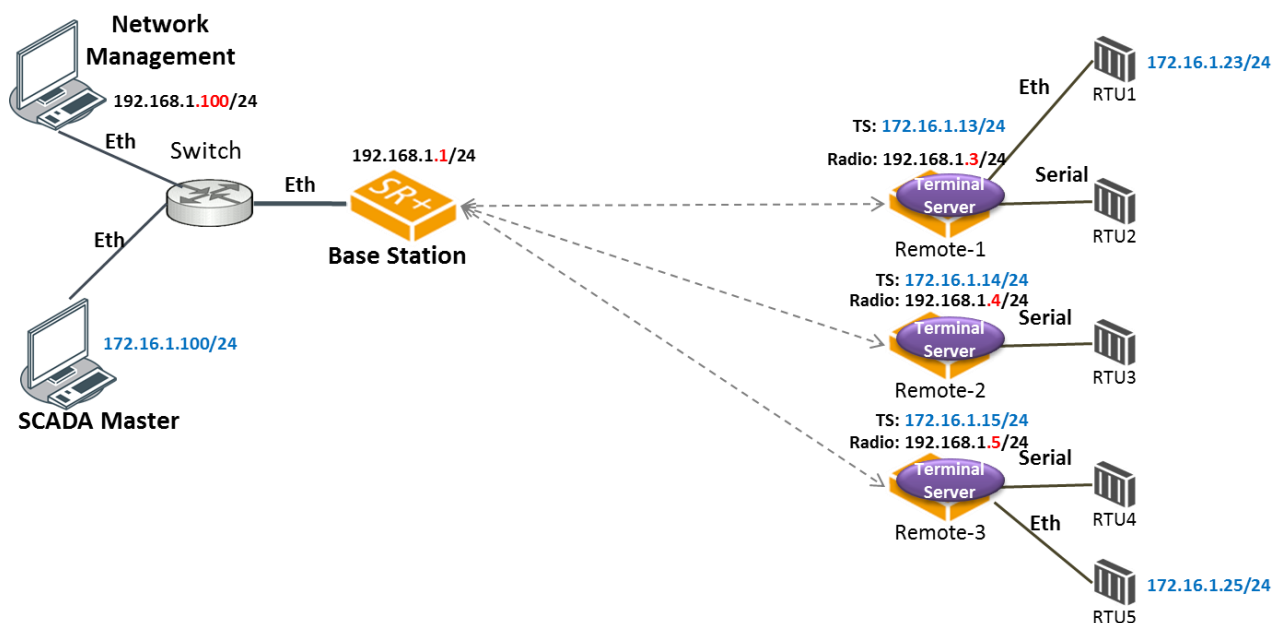
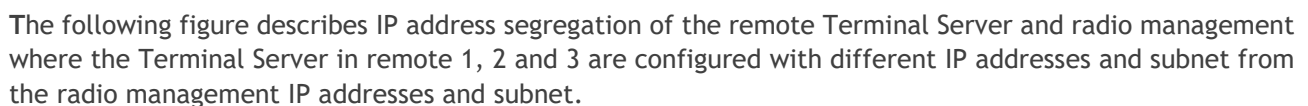


VLAN segregation of remote Terminal Server and radio management

The following figure describes VLAN segregation of the remote Terminal Server and radio management where the Terminal Server in remote 1, 2 and 3 are configured with different VLANs from the radio management VLAN and with the same IP address of the radios.

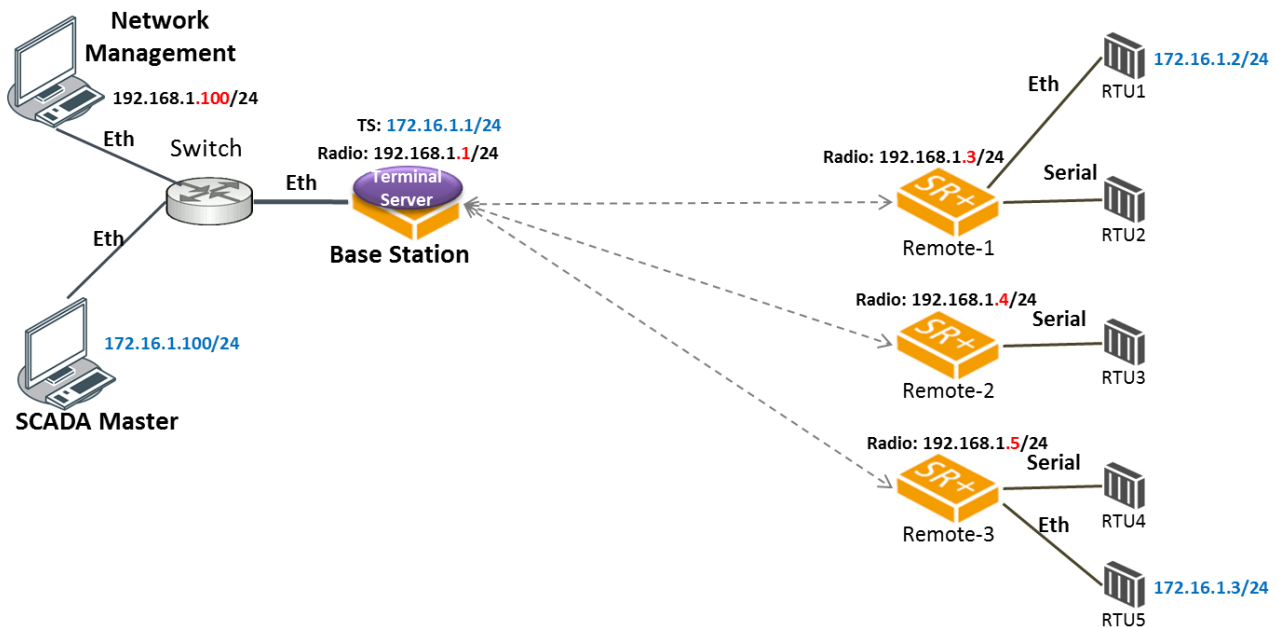


The following figure describes VLAN segregation of the IP Terminal Server and radio management where the IP-Terminal Server in base station is configured with different VLANs from the radio management VLAN and with the same IP address of the radios.



IP address segregation of IP Terminal Server and radio management

The following figure describes the IP address segregation of IP Terminal Server and radio management where the IP Terminal Server in Base station is configured with different IP address and subnet from the radio management IP addresses and subnet.



IP address Configuration per Terminal Server in Router Mode

There are minor differences in configuring the IP address of a remote Terminal Server and/or IP Terminal Server in Router mode / Gateway Router mode or Advanced mode of both options.

Router Mode / Advanced Router Mode:

- **IP Terminal Server** - the IP address must be the same as any Ethernet port IP address or PVIP of protected station.
- **Remote Terminal Server** - the IP address must be the same as Ethernet port 1 (management) IP address or PVIP of protected station.

Gateway Router Mode / Advanced Gateway Router Mode:

- **Terminal Server** - the IP address must be the same as the radio IP address or PVIP of protected station.

Avoiding Narrow Band Radio Traffic Overloading

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

1. L3/L4 Filtering

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

2. L2 Address Filtering

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

3. L2 Port VLANs Ingress Filtering and QoS

Double VLAN (Bridge Mode)

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

Single VLAN (Bridge Mode)

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

QoS using 802.1p priority bits (Bridge Mode)

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

4. Ethernet port QoS

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

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

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

6. Ethernet Packet Time to Live

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

7. Robust Header Compression (ROHC) and Payload Compression

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

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

Interfaces

Antenna Interface

- 2 x TNC, 50 ohm, female connectors

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

Ethernet Interface

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

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

RS-232 / RS-485 Interface

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

USB Interfaces

- 1 x Management port using USB micro type B connector

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

- 1 x Host port using USB standard type A connector

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

Protect Interface

- 1x Protect interface port

Used for the Protected Station operation.

Alarms Interface

- 1x Alarm port using RJ45 connector

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

Front Panel Connections



Example; 2 Ethernet ports and 2 RS-232 serial ports - see 'Data Interface Ports' on page 404 for the other interface port options.

Interface Port Option

2 Ethernet ports and 2 RS-232 serial ports

Part Number

APSQ-N400-SSC-HD-22-ENAA

All connections to the radio are made on the front panel. The functions of the connectors are:

Designator	Description
10 - 30 VDC; 4A	+10 to +30 VDC (negative ground) DC power input using Molex 2 pin male screw fitting connector. AC/DC and DC/DC power supplies are available as accessories. See 'External Power Supplies' on page 85.
ETHERNET 1 & 2	Integrated 10Base-T/100Base-TX layer-3 Ethernet switch using RJ45 connectors. Used for Ethernet user traffic and product management. See 'Ethernet > Port Setup' on page 168.
SERIAL 1 & 2	Two ports of RS-232 serial using RJ45 connectors. Used for RS-232 asynchronous user traffic. See 'Serial > Port Setup' on page 150.
	Host Port using a USB standard type A connector. Used for software upgrade and diagnostic reporting and optional: 1x RS-232 asynchronous port with USB to RS-232 converter. See 'Software Upgrade' on page 445 and 'Maintenance > General' on page 261. Also used to access the radio Command Line Interface (CLI). A USB converter to RS-232 convertor will be required to connect to a PC.
ALARM	Alarm Port using a RJ45 connector. Used for two alarm inputs and two alarm outputs. See 'Hardware Alarms Interface' on page 488.
MGMT	Management Port using a USB micro type B connector. Used to access the radio Command Line Interface (CLI). See 'Command Line Interface' on page 393.
PROTECT	Protect port. Used for Protected Station operation.
TX / ANT	TNC, 50 ohm, female connector for connection of antenna feeder cable for half duplex RF operation or the Transmit connection to an external duplexer for full duplex RF operation or to an external filter. See 'Coaxial Feeder Cables' on page 77.
RX	TNC, 50 ohm, female connector for the Receive connection to an external duplexer for full duplex RF operation or to an external filter.

LED Display Panel

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



Normal Operation

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

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

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

Single Radio Software Upgrade

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

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

Network Software Upgrade

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

Test Mode

Remote radio 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 263 for Test Mode options).

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

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

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

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

OK LED	MODE LED	AUX LED	TX LED	RX LED	RSSI
					≥ -80 dBm
					-84 dBm to -81 dBm
					-88 dBm to -85 dBm
					-92 dBm to -89 dBm
					-96 dBm to -93 dBm
					-100 dBm to -97 dBm
					-104 dBm to -101 dBm
					-108 dBm to -105 dBm
					-112 dBm to -109 dBm
					-116 dBm to -113 dBm
					< RSSI threshold
					No response received

Network Management

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

- Mozilla Firefox
- Microsoft Edge
- Google Chrome

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

The key features of SuperVisor are:

- Full element management, configuration and diagnostics
- Manage the entire network from the Base Station (remote management of elements)
- Managed network software distribution and upgrades
- Performance and alarm monitoring of the entire network, including RSSI, alarm states, time-stamped events, etc.
- View and set standard radio configuration parameters including frequencies, transmit power, channel access, serial, Ethernet port settings
- Set and view security parameters
- User management
- Operates over a secure HTTPS session on the access connection to the base station
- SuperVisor uses standard TCP/UDP port 80 for HTTP and 443 for HTTPS

SuperVisor, when connected to the base station radio allows management of all radios in the network. The Network Table displays a list of all the registered remote radios for the base station and provides management access to each of the remote radios (see 'Network Status > Network Table' on page 333).

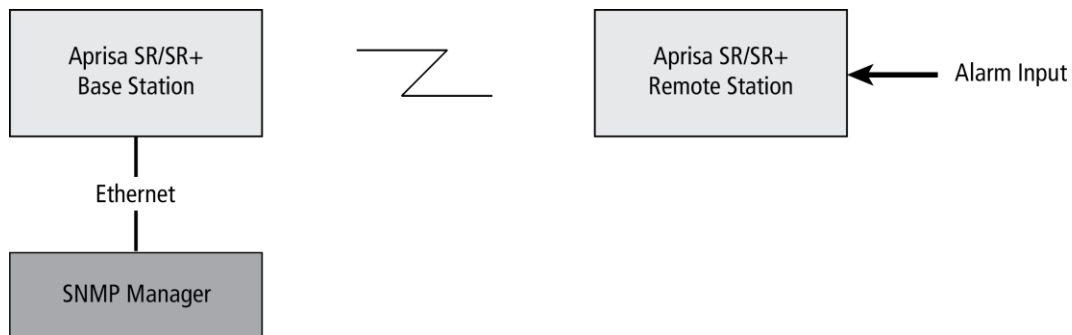
Hardware Alarm Inputs / Outputs

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

The hardware alarm inputs and outputs are part of the event system. All alarm events can be viewed in SuperVisor event history log (see ‘Events > Event History’ on page 279). These include the alarm events generated by the hardware alarm inputs.

Alarm Input to SNMP Trap

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



Alarm Input to Alarm Output

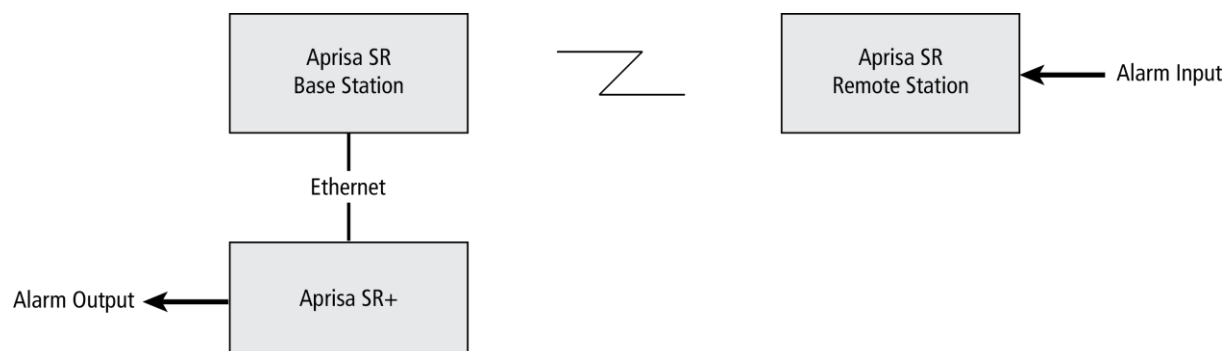
An alarm event from an Aprisa SR+ hardware alarm input can be mapped to an hardware alarm output of another SR+ using an event action setup (see ‘Events > Event Action Setup’ on page 286).



Aprisa SR Alarm Input to Aprisa SR+ Alarm Output

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

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

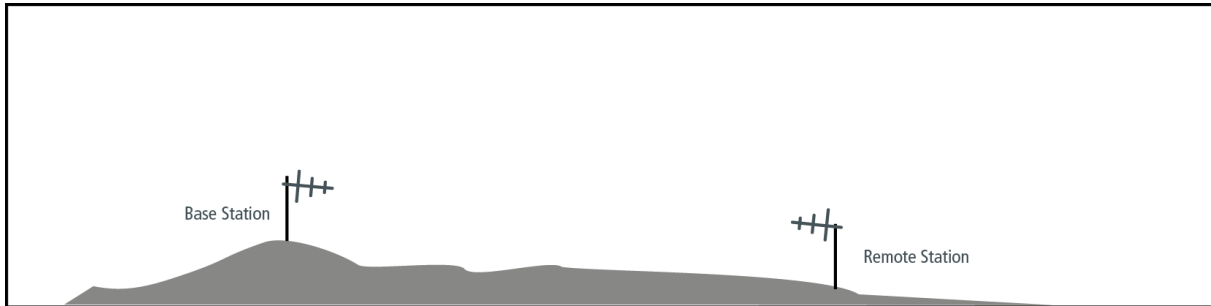


4. Implementing the Network

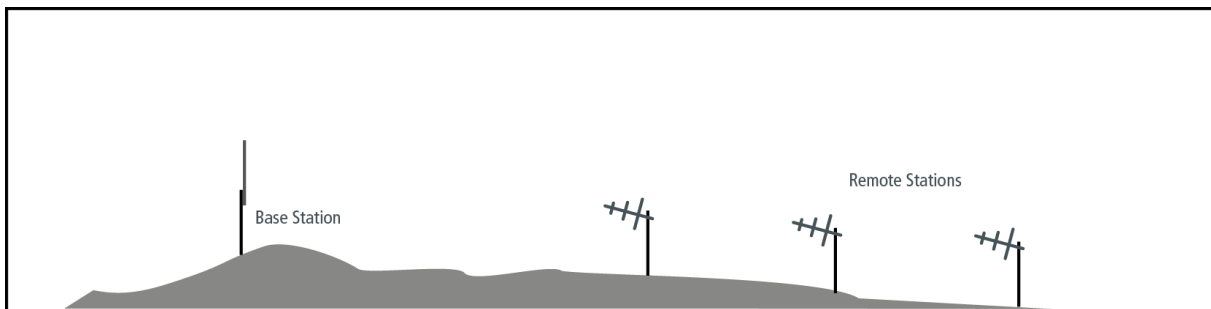
Network Topologies

The following are examples of typical network topologies:

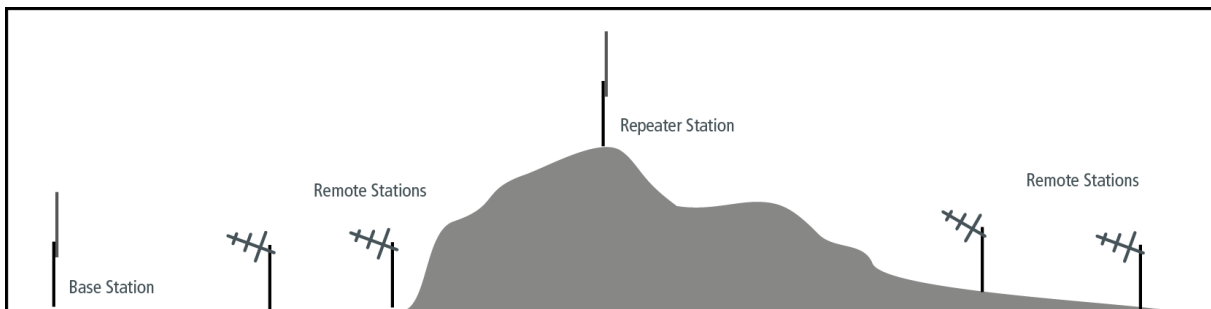
Point-To-Point Network



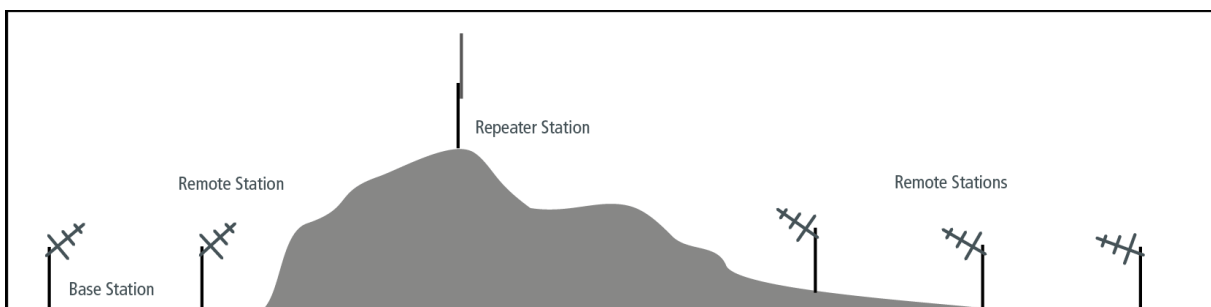
Point-to-Multipoint Network



Point-to-Multipoint with Repeater 1



Point-to-Multipoint with Repeater 2



Initial Network Deployment

Install the Base Station

To install the base station in your network:

1. Install the base station radio (see 'Installing the Radio' on page 80).
2. Set the radio Base Station ID to a unique ID in your entire network (see 'Terminal > Device' on page 108).
3. Set the radio operating mode to 'base station' (see 'Terminal > Operating Mode' on page 116).
4. Set the radio IP address (see 'IP > IP Setup > Bridge / Gateway Router Modes' on page 182).
5. Set the radio frequencies to the frequencies you wish to operate from (see 'Radio > Radio Setup' on page 128).
6. Set the radio security settings (see 'Security > Setup' on page 226).

Installing the Remote radios

To install the remote radios in your network:

1. Install the remote radio (see 'Installing the Radio' on page 80).
2. Set the radio Base Station ID to the same ID as the other stations in the network (see 'Terminal > Device' on page 108).
3. If repeater used in radius 1, set the network radius=2 on all network stations (see 'Terminal > Device' on page 108) and set the 'Repeater Network Station ID'.
4. Set the radio operating mode to 'remote radio' (see 'Terminal > Operating Mode' on page 116).
5. Set the radio IP address (see 'IP > IP Setup > Bridge / Gateway Router Modes' on page 182).
6. Set the radio frequencies to the base station / repeater station frequencies you wish to operate from (see 'Radio > Radio Setup' on page 128).
7. Set the radio security settings to the same as the base station (see 'Security > Setup' on page 226).

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

Install a Repeater Station

To install a repeater station in your network:

1. Install the repeater station radio (see 'Installing the Radio' on page 80).
2. Set the radio Base Station ID to the same ID as the other stations in the network (see 'Terminal > Device' on page 108) and set the 'Repeater Network Station ID'.
3. Increase the radio network radius by one on all stations in the network (see 'Terminal > Device' on page 108).
4. Set the radio operating mode to 'repeater station' (see 'Terminal > Operating Mode' on page 116).
5. Set the radio IP address (see 'IP > IP Setup > Bridge / Gateway Router Modes' on page 182).
6. Set the radio frequencies to base station frequencies you wish to operate from (see 'Radio > Radio Setup' on page 128).
7. Set the radio security settings to the same as the base station (see 'Security > Setup' on page 226).

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 80).
2. Set the radio Base Station ID to the same ID as the other stations in the network (see 'Terminal > Device' on page 108).
3. Set the radio IP address (see 'IP > IP Setup > Bridge / Gateway Router Modes' on page 182).
4. Set the radio frequencies to the base station frequencies you wish to operate from (see 'Radio > Radio Setup' on page 128).
5. Set the radio operating mode to 'repeater station' (see 'Terminal > Operating Mode' on page 116).
6. Increase the radio network radius by one on all stations in the network (see 'Terminal > Device' on page 108).

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 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 108).

Adding a Remote radio

To add a remote radio to your network:

1. Install the remote radio (see 'Installing the Radio' on page 80).
2. Set the radio Base Station ID to the same ID as the other stations in the network (see 'Terminal > Device' on page 108).
3. If repeater used in radius 1, set the network radius=2 on all network stations (see 'Terminal > Device' on page 108).
4. Set the radio IP address (see 'IP > IP Setup > Bridge / Gateway Router Modes' on page 182).
5. Set the radio frequencies to the base station / repeater station frequencies you wish to operate from (see 'Radio > Radio Setup' on page 128).
6. Set the radio operating mode to 'remote radio' (see 'Terminal > Operating Mode' on page 116).

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

To remove a remote radio from your network:

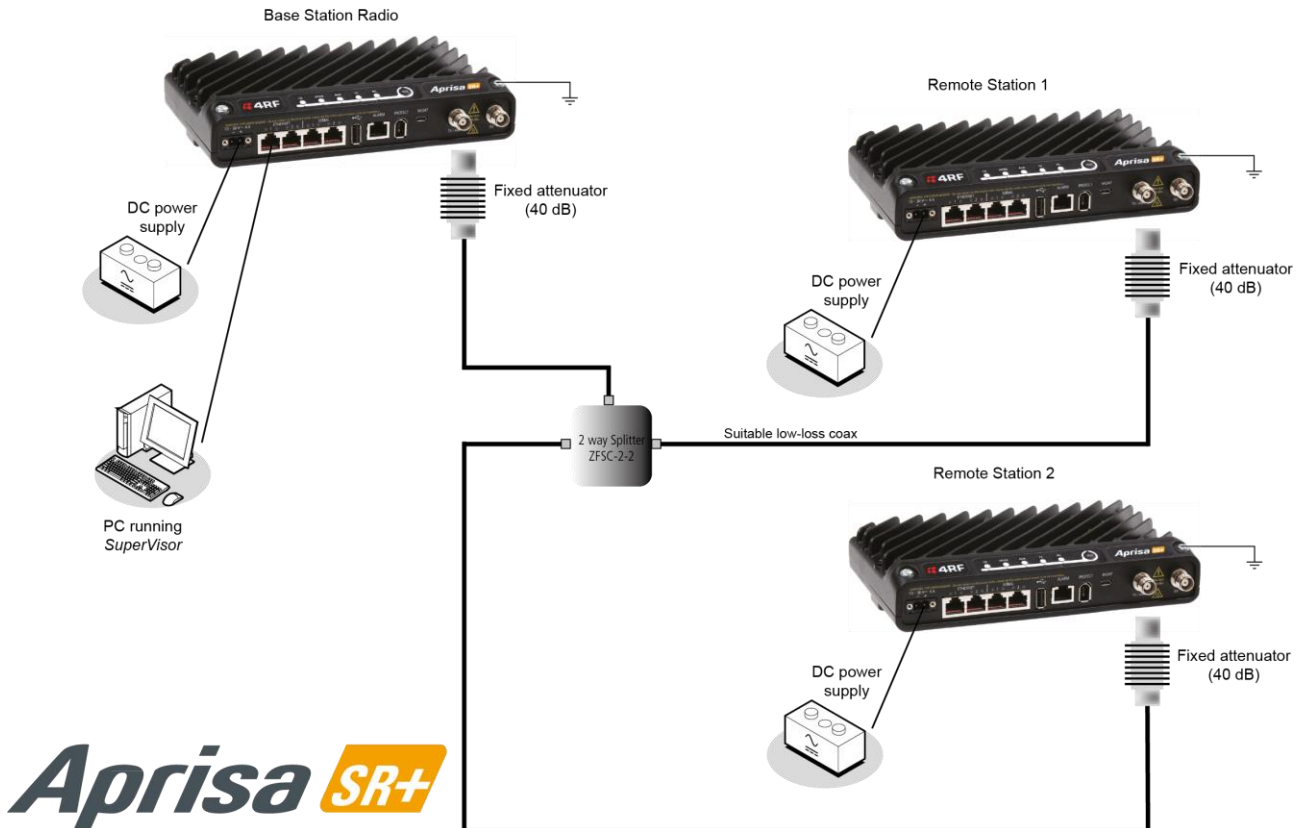
1. Turn the power off on the remote radio you wish to remove. This is the only action that is required.

Note: The remote radio 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.

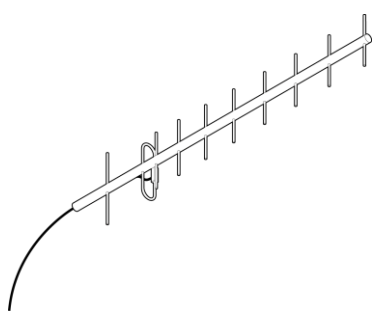
Omni Directional Collinear Antennas

	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

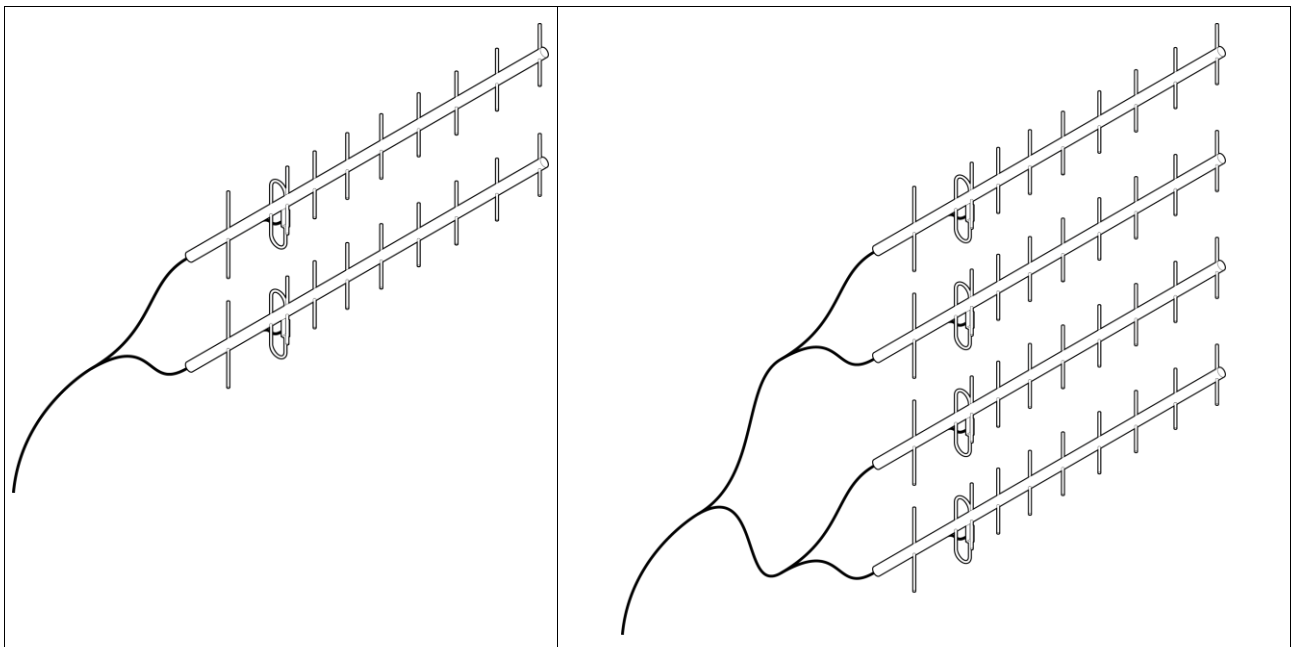
Remote radio

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

Yagi Antennas

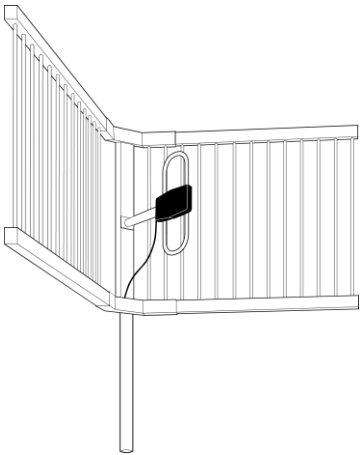
	Factor	Explanation
	Frequency	Often used in 350-600 MHz bands
	Gain	Varies with size (typically 11 dBi to 16 dBi)
	Stackable gain increase	2 Yagi antennas (+ 2.8 dB) 4 Yagi antennas (+ 5.6 dB)
	Size	Range from 0.6 m to 3 m in length
	Front to back ratio	Low (typically 18 to 20 dB)

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



Example of stacked antennas

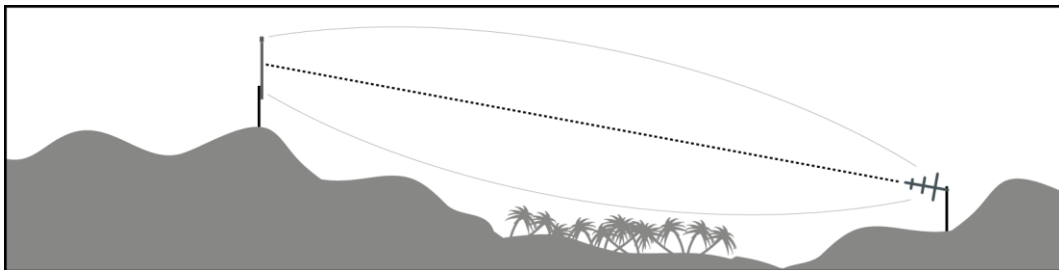
Corner Reflector Antennas

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

Antenna Siting

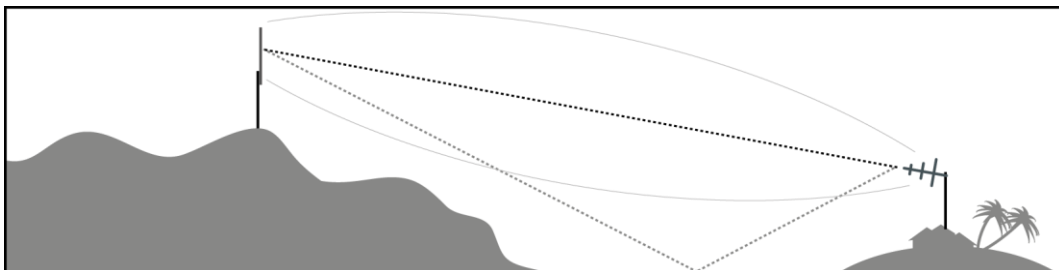
When siting antennas, consider the following points:

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



Example of a clear line-of-sight path

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



Example of a mid-path reflection path

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

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

Coaxial Feeder Cables

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

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

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

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

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

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

When running cables:

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

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

Linking System Plan

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

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

Site Requirements

Power Supply

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

The nominal input voltage for a radio is +12 VDC (negative earth) with an input voltage range of +10 to +30 VDC. The maximum power input is 35 W.



WARNING:

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

Equipment Cooling

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

The environmental operating conditions are as follows:

Operating temperature -40 to +70° C (-40 to +158° F)

Storage temperature -40 to +85° C (-40 to +185° F)

Humidity Maximum 95% non-condensing



WARNING:

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



WARNING:

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

Earthing and Lightning Protection



WARNING:

Lightning can easily damage electronic equipment.

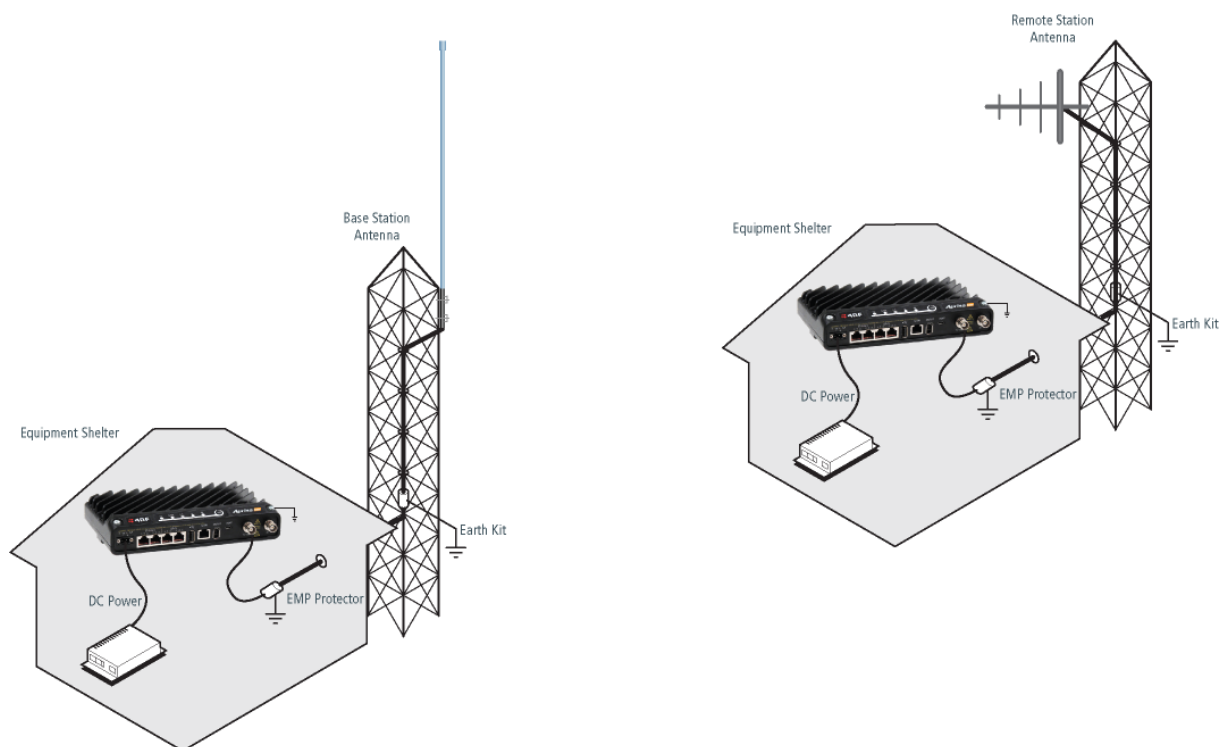
To avoid this risk, install primary lightning protection devices on any interfaces that are reticulated in the local cable network.

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

Feeder Earthing

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

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



Radio Earthing

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



6. Installing the Radio



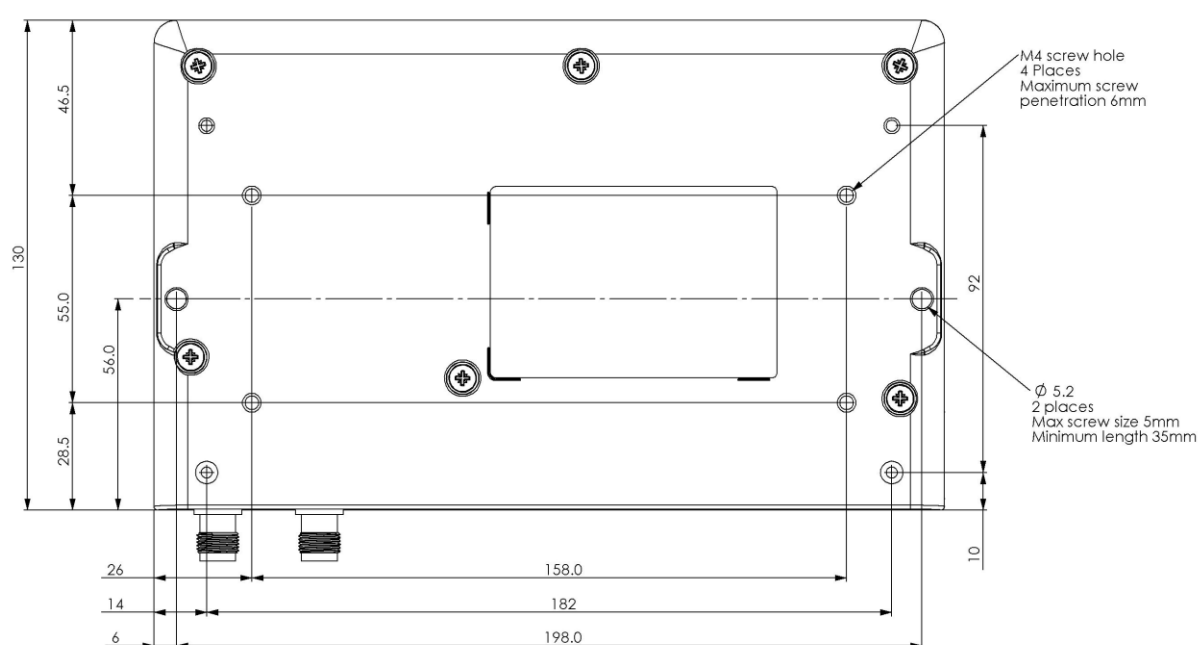
CAUTION:

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

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

Mounting

The Aprisa SR+ has four threaded holes (M4) in the enclosure base and two holes (5.2 mm) through the enclosure for mounting.



Mounting options include:

- DIN rail mounting with the 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.

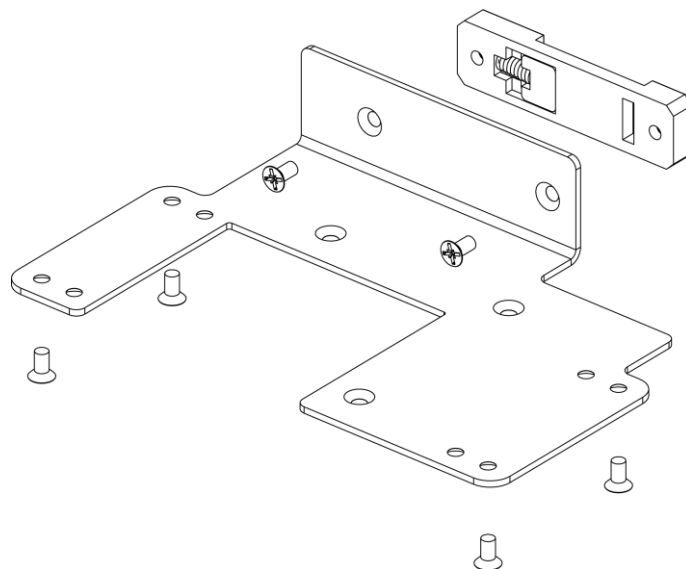
Required Tools

No special tools are needed to install the radio.

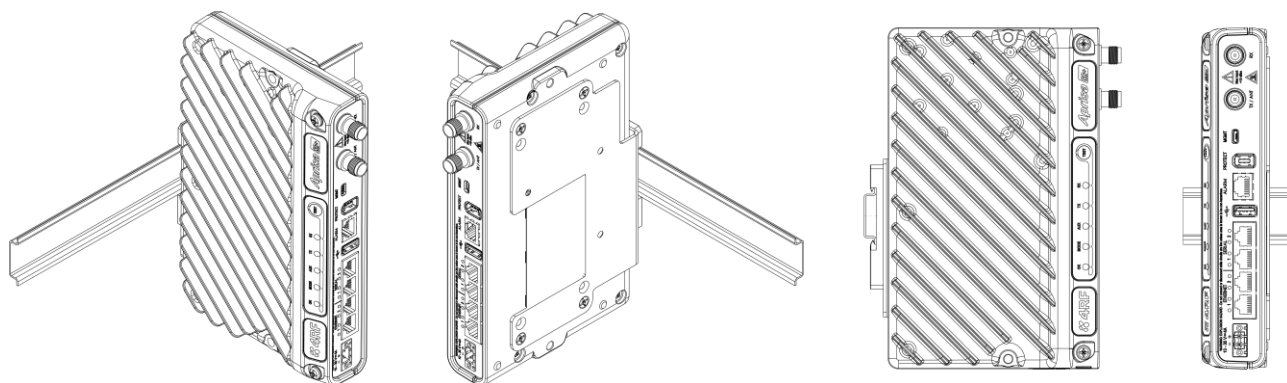
DIN Rail Mounting

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

Part Number	Part Description
APGA-MBRK-DIN	4RF 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.



Rack Shelf Mounting

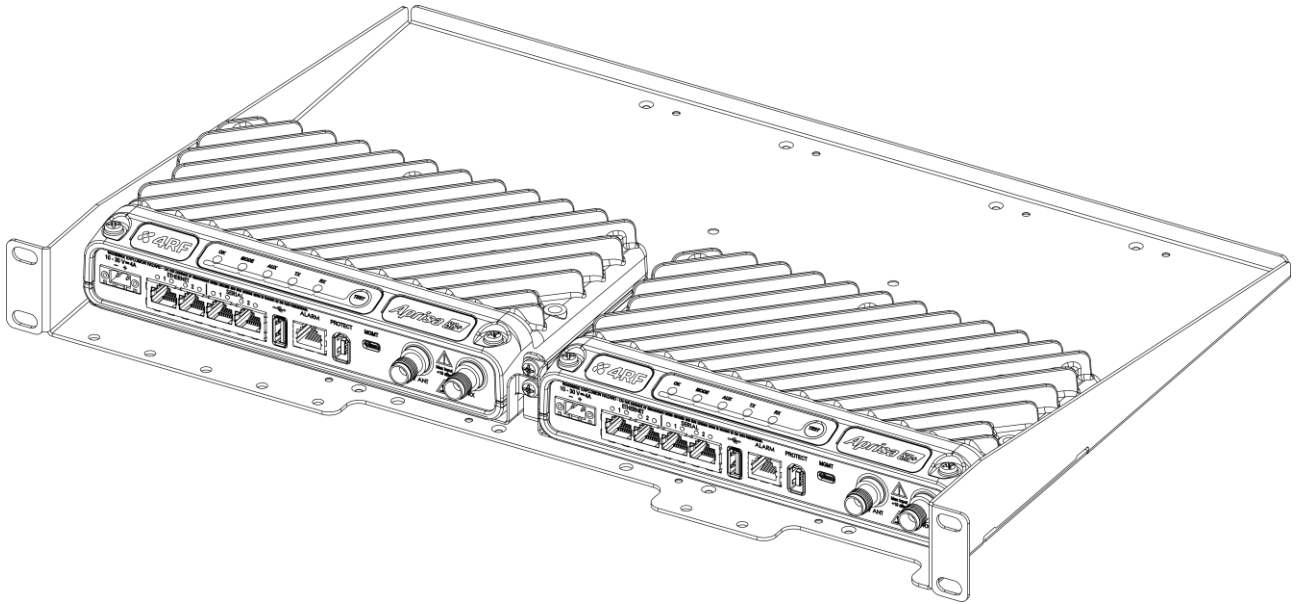
The Aprisa SR+ can be mounted on a rack mount shelf using the four M4 threaded holes in the Aprisa SR+ enclosure base. The following picture shows Aprisa SR+ mounted on a 1 RU rack mounted shelf.

Part Number

APGA-MR19-X1U

Part Description

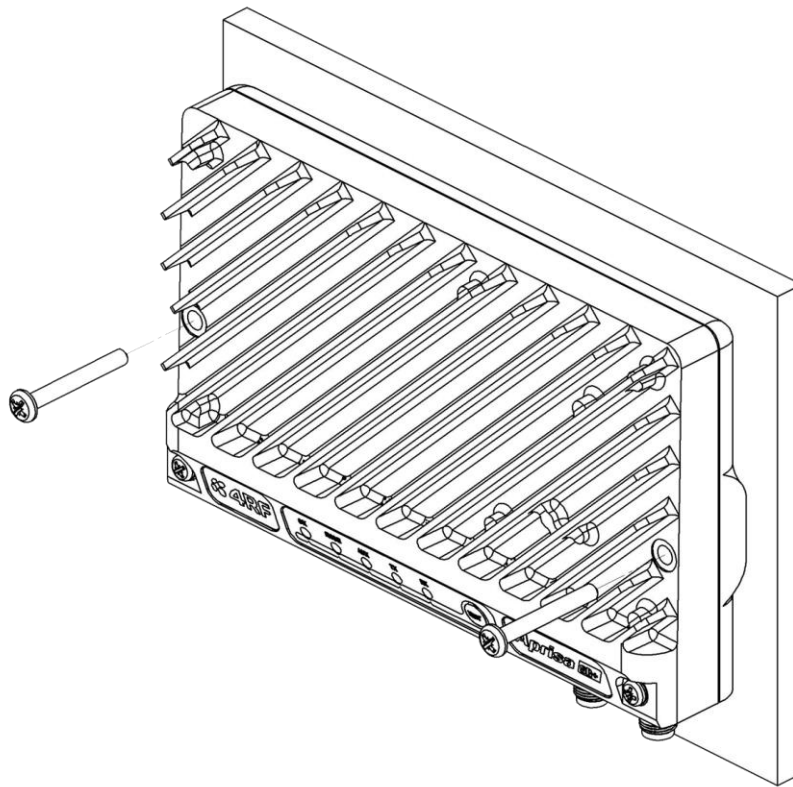
4RF Acc, Mounting, 19" Rack Mount Shelf, 1 Rack Unit

**WARNING:**

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

Wall Mounting

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



Installing the Antenna and Feeder Cable

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

Lightning protection must be incorporated into the antenna system (see 'Earthing and Lightning Protection' on page 79).



WARNING:

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

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

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

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

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

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

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

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



Connecting the Power Supply

The nominal input voltage for a radio is +12 VDC (negative earth) with an input voltage range of +10 to +30 VDC. The maximum power input is 35 W.

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



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

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

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

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

Turn your power source on:

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

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

Spare fuses are contained within the radio, see 'Spare Fuses' on page 441 for instructions on how to locate and replace the fuses.

External Power Supplies

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

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

7. Managing the Radio

SuperVisor

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

- Mozilla Firefox
- Microsoft Edge
- Google Chrome

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

The key features of SuperVisor are:

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

Connecting to SuperVisor

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

The Aprisa SR+ radio 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:

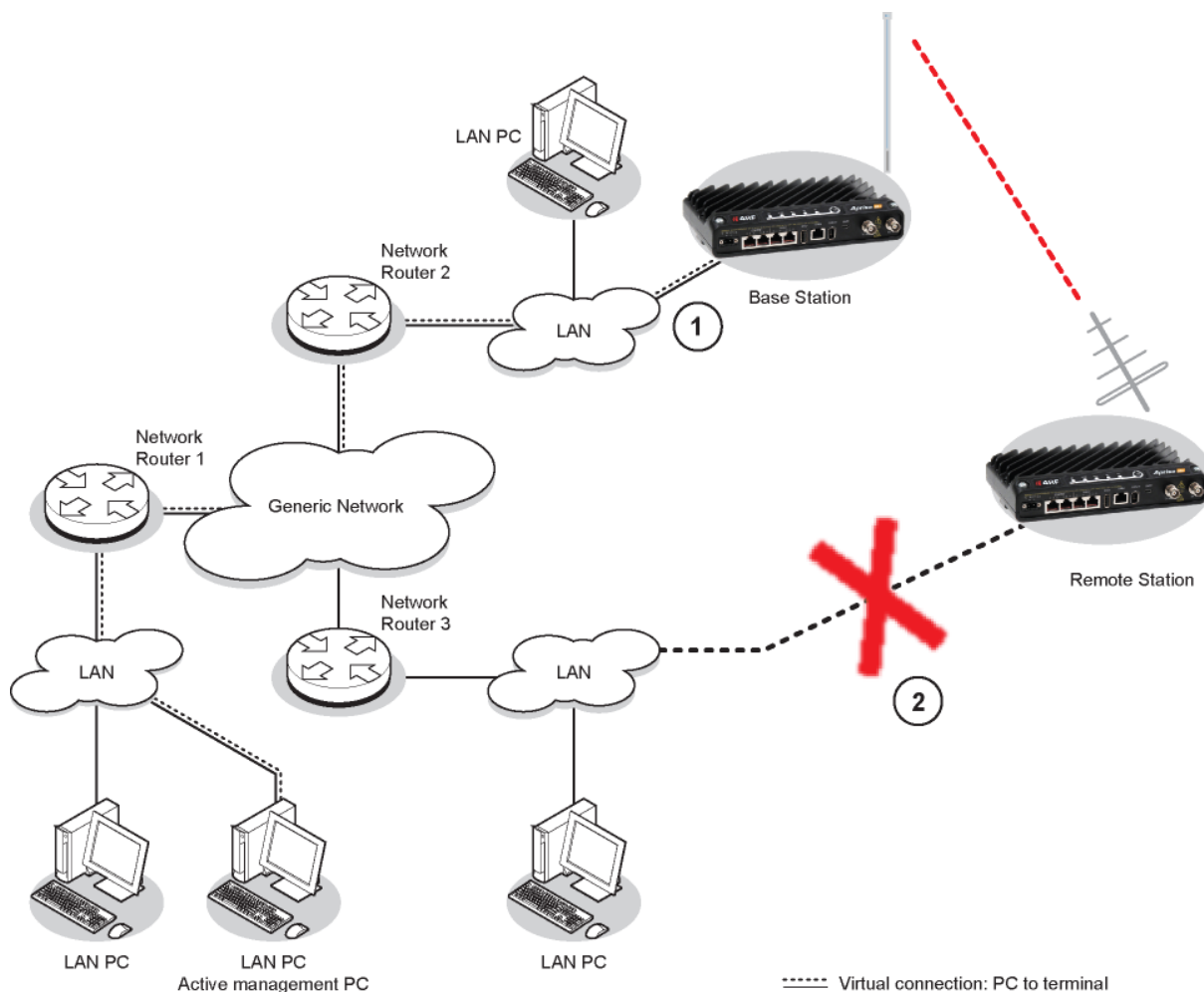
1. Set up your PC for a compatible IP address e.g. 169.254.50.1 with a subnet mask of 255.255.0.0.
2. Connect your PC network port to one of the Aprisa SR+ Ethernet ports.
3. Open a browser and enter <http://169.254.50.10>.
4. Login to the radio with the default username 'admin' and password 'admin'.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

Note 1: When the radio Ethernet Operating Mode is Router Mode or Advanced Router Modes, users must connect to SuperVisor via Ethernet Port 1 to have full management functionality when performing remote management to the other radios on the network.

Note 2: Remote management functionality requires that on networks with mixed versions of software, the base station must be running the latest version of software that is used on the network.

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 radios in the network.

If the Local Radio is a remote radio or repeater station, SuperVisor manages the remote / repeater station radio logged into, but the user can access the base station from a remote / repeater and access / retrieve the network table to manage the whole network.

If the user is at the remote radio 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

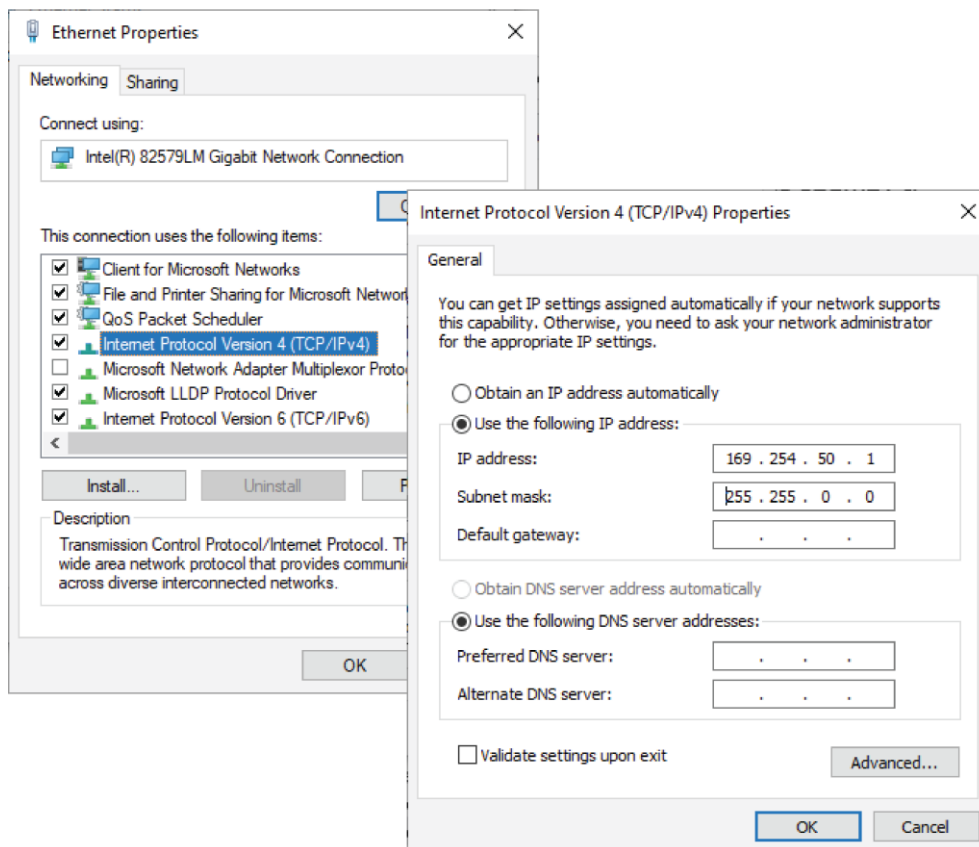
To change the PC IP address:

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 Example:

1. Open the 'Control Panel'.
2. Open the 'Network and Sharing Center', click on the 'Change Adapter Settings' and select the network.
3. On the Ethernet Status window, click 'Properties'.
4. Click on the 'Networking' tab.
5. Click on 'Internet Protocol Version 4 (TCP/IPv4)' and click on properties.
6. Enter the IP address and the subnet mask (example as shown).
7. 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).



Login to SuperVisor

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

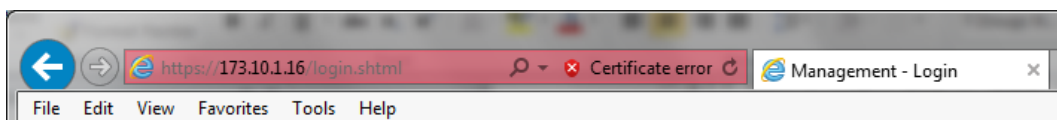
If SuperVisor is inactive for a period defined by the Inactivity Timeout option (see 'Maintenance > General' on page 261), the radio will automatically logout the user.

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.

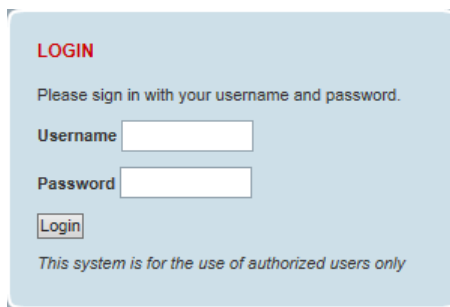
If you don't know the IP address of the radio, you can determine it using the Command Line Interface (see 'Command Line Interface' on page 392).



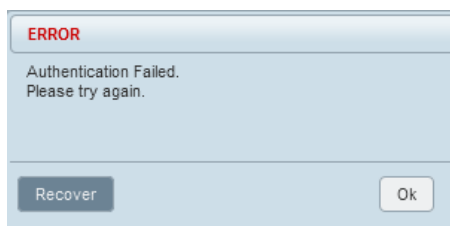
Note: The Aprisa SR+ has a randomly generated unique self-signed ECC256 security certificate which may cause the browser to prompt a certificate warning. It is safe to ignore the warning and continue. The valid certificate is 'Issued By: 4RF-APRISA' which can be viewed in the browser.

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

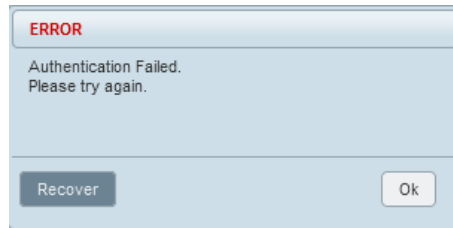
If unique usernames and passwords have not yet been configured, use the default username 'admin' and password 'admin'.



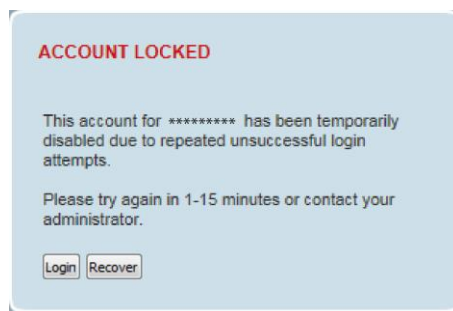
If the login fails, the pop-up will be displayed.



SuperVisor will display a warning popup upon multiple consecutive failed login attempts on the same account.

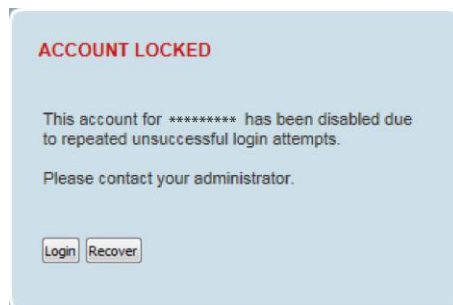


SuperVisor has login protection options which provide protection against unsuccessful login retries (see Security > Users 'Login Protection Mode' on page 239). If login protection is active and a login attempt failed due to temporary lockout of the account (Level 1 or Level 2 lockout), SuperVisor will display an 'Account Locked' message.



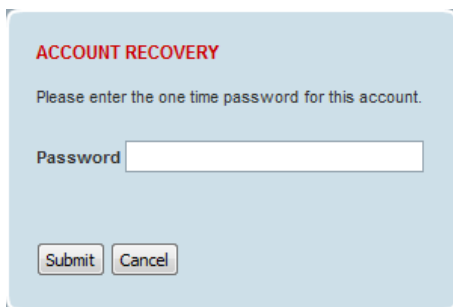
Login

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



Recover

If a login attempt failed due to permanent lockout of the account or the Admin password is unknown, click the 'Recover' button to start the recovery process.

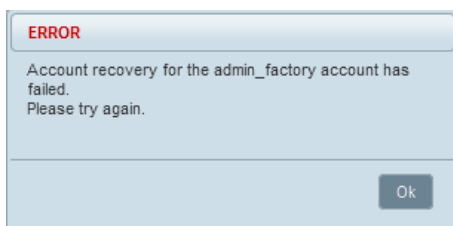


ACCOUNT RECOVERY

Please enter the one time password for this account.

Password

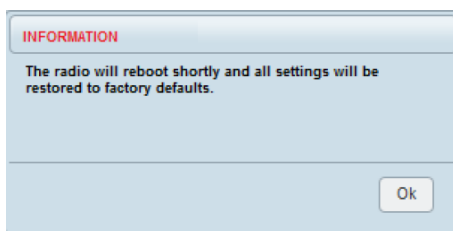
If the user account is not an ADMIN account, or if the account does not have an associated 'Standard OPT' password entered (see 'One-time Password Recovery' on page 245), SuperVisor will display an error message.



ERROR

Account recovery for the admin_factory account has failed.
Please try again.

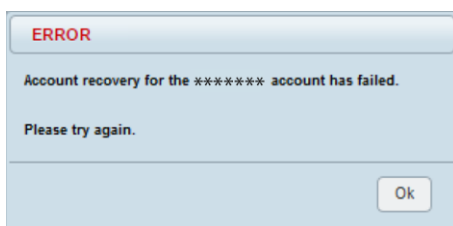
If a factory password was verified successfully during the account recover process, SuperVisor will display a message indicating that the radio will be reset to factory defaults and rebooted.



INFORMATION

The radio will reboot shortly and all settings will be restored to factory defaults.

If the submitted password for the account recovery process was invalid, SuperVisor will display a message indicating that the recovery process has failed.

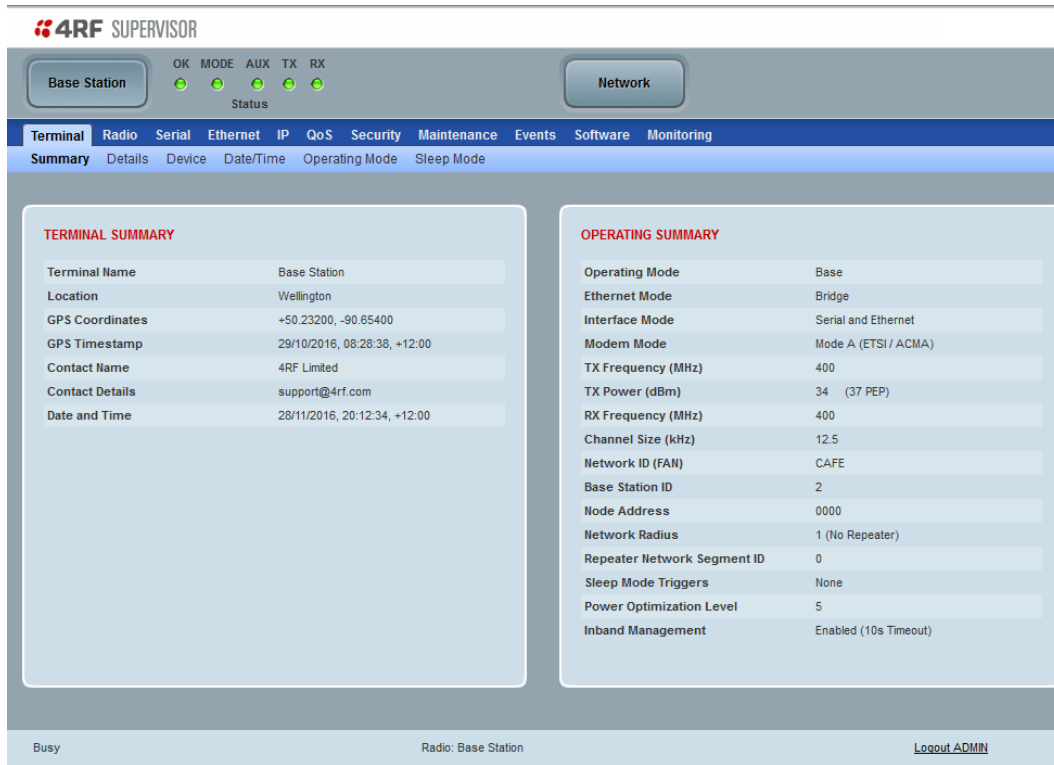


ERROR

Account recovery for the ***** account has failed.
Please try again.

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

Important: After you login for the very first time, it is recommended that you change the default admin password for security reasons (see ‘Security > Users’ on page 239).



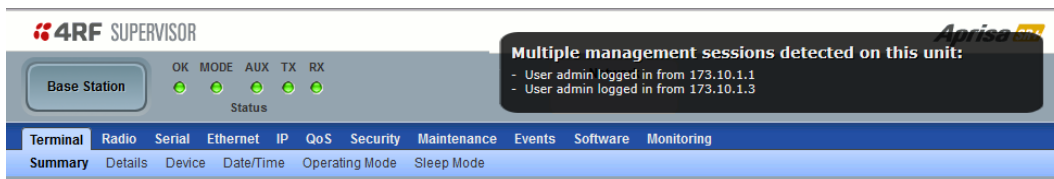
The screenshot shows the 4RF SUPERVISOR interface. At the top, there are status indicators for OK, MODE, AUX, TX, and RX, all of which are green. Below this is a navigation bar with tabs for Terminal, Radio, Serial, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring. The Terminal tab is selected, and the Summary sub-tab is active. The main content area is divided into two columns: Terminal Summary and Operating Summary.

Terminal Summary	
Terminal Name	Base Station
Location	Wellington
GPS Coordinates	+50.23200, -90.65400
GPS Timestamp	29/10/2016, 08:28:38, +12:00
Contact Name	4RF Limited
Contact Details	support@4rf.com
Date and Time	28/11/2016, 20:12:34, +12:00

Operating Summary	
Operating Mode	Base
Ethernet Mode	Bridge
Interface Mode	Serial and Ethernet
Modem Mode	Mode A (ETSI / ACMA)
TX Frequency (MHz)	400
TX Power (dBm)	34 (37 PEP)
RX Frequency (MHz)	400
Channel Size (kHz)	12.5
Network ID (FAN)	CAFE
Base Station ID	2
Node Address	0000
Network Radius	1 (No Repeater)
Repeater Network Segment ID	0
Sleep Mode Triggers	None
Power Optimization Level	5
Inband Management	Enabled (10s Timeout)

At the bottom of the interface, there is a status bar showing 'Busy' and 'Radio: Base Station'. A 'Logout ADMIN' link is visible in the bottom right corner.

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



The screenshot shows the 4RF SUPERVISOR interface with a popup message titled 'Multiple management sessions detected on this unit:'. The popup lists two users: 'User admin logged in from 173.10.1.1' and 'User admin logged in from 173.10.1.3'. The interface is otherwise identical to the previous screenshot.

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 radios in the network.



Active button; indicating the radio SuperVisor is managing a radio in this network



Inactive button; indicating a radio or network SuperVisor could manage

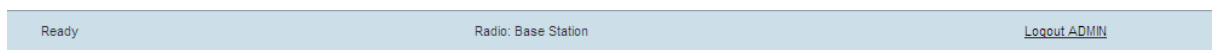


Active button; indicating the radio SuperVisor is managing a radio in the extended network radio list.

If the local radio is a remote radio 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.

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

SuperVisor Summary Bar



The summary bar at the bottom of the page shows:

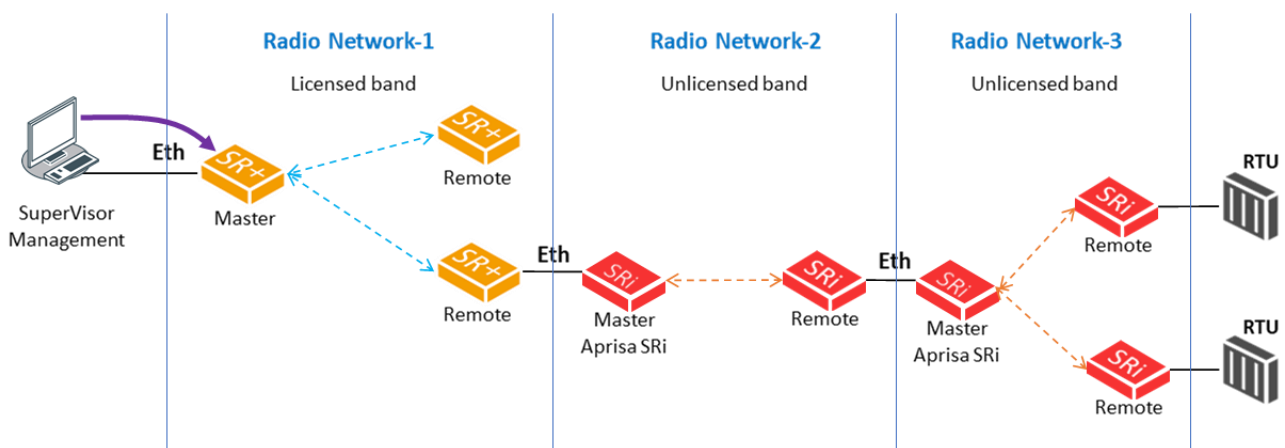
Position	Function
Left	Busy - SuperVisor is busy retrieving data from the radio that SuperVisor is logged into. Ready - SuperVisor is ready to manage the radio.
Middle	Displays the name of the radio terminal that SuperVisor is currently managing.
Right	The access level logged into SuperVisor. This label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

SuperVisor Extended Network Management (EXM)

Extended Network Management (EXM) extends SuperVisor management beyond the single radio network providing configuration and monitoring to other Aprisa SR family products down the RF path from the radio logged into. All radios that are then managed from one login become part of the extended network radio list.

A typical use of this new feature is where an Aprisa SRi radio network is connected to the ‘tail end’ of an Aprisa SR+ radio network where the Aprisa SRi base station is cable connected to the Ethernet port of an Aprisa SR+ remote radio. The connection between the Network Operations Centre (NOC) to the Aprisa SRi base station would be via the Over-The-Air path of the Aprisa SR+ base station’s network.

Note: Extended Network Management functionality requires that on networks with mixed versions of software, the radio that is used to extend the management capabilities must be running the latest version of software that is used on the network.



Extended Network Management Example

Benefits Of EXM

Some of the benefits that will be seen from this enhancement include:

- Ability to use SuperVisor to manage any 4RF compatible radio units via the ‘closest radio station’
- A user can now simply establish a local connection with the closest radio and navigate to manage another radio down the RF path from the radio logged into.
- Ability to use SuperVisor to perform ‘inverse remote management’ - i.e. to manage the base station from any of its remote radios
- When on site at a remote location, the user can now login to the remote radio and navigate to manage its base station
- A user can now add any IP connectable radio to a SuperVisor session and utilize the Network Status monitoring feature to monitor radios network wide
- SuperVisor can be left running long term on the ‘Network Status > Summary’ page to have a summarized status view of the whole monitored network

The EXM feature will not be suitable for customers who use Port forwarding NAT configuration or One to One NAT in their existing setup.

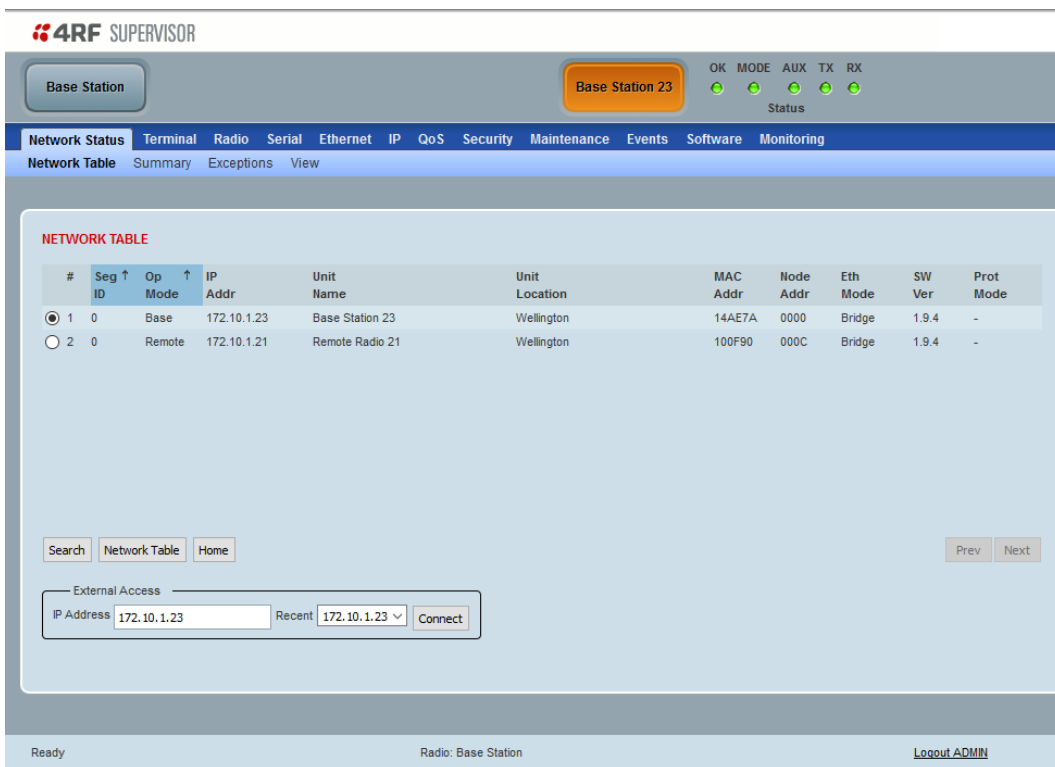
Extended Network Management (EXM) Setup

1. Enable Network Extension Mode on all radios required in the extended network radio list including the radio logged into, the remote radio being used to extend management, the destination base station and any remote radios off that base station requiring management. See 'Security > Setup' on page 226 for the Network Extension Mode setting.
2. Ensure that the Network ID is the same on all radios in the extended network radio list (see 'Network ID' on page 110).
3. Ensure that the Key Encryption Key Type, Key Encryption Key Size and the Key Encryption Key are the same on all radios in the extended network radio list (see 'Security > Setup' on page 226).
4. Click on the Network button on SuperVisor Alarm Bar (see 'Network Status > Network Table' on page 333).
5. In the External Access box, enter the IP address of the external radio and click the Connect button.

If this connection is successful:

- The Network Button will show the name of the radio connected to
- The LEDs next to the Network button will display the status of the radio connected to
- Clicking any top level menu after the connection is established will open the page for the radio connected to

The Network Table shows the radio connected to. To see the complete Network Table of the radio connected to, click the Network Table button.



The screenshot shows the 4RF SUPERVISOR web interface. At the top, there's a 'Base Station' button and a 'Base Station 23' button with status LEDs for OK, MODE, AUX, TX, and RX. Below this is a navigation bar with tabs: Network Status, Terminal, Radio, Serial, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring. The 'Network Status' tab is active, showing a 'Network Table' with columns: #, Seg ID, Op Mode, IP Addr, Unit Name, Unit Location, MAC Addr, Node Addr, Eth Mode, SW Ver, and Prot Mode. The table contains two entries: a selected 'Base Station 23' (IP 172.10.1.23) and a 'Remote Radio 21' (IP 172.10.1.21). Below the table is an 'External Access' section with a 'Search' button, a 'Network Table' button, and a 'Home' button. It also includes a text input for 'IP Address' (172.10.1.23), a 'Recent' dropdown (172.10.1.23), and a 'Connect' button. At the bottom, there's a status bar showing 'Ready', 'Radio: Base Station', and a 'Logout ADMIN' link.

#	Seg ID	Op Mode	IP Addr	Unit Name	Unit Location	MAC Addr	Node Addr	Eth Mode	SW Ver	Prot Mode
1	0	Base	172.10.1.23	Base Station 23	Wellington	14AE7A	0000	Bridge	1.9.4	-
2	0	Remote	172.10.1.21	Remote Radio 21	Wellington	100F90	000C	Bridge	1.9.4	-

SuperVisor Menu

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

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

SuperVisor Parameter Settings

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

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

SuperVisor Menu

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

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

Terminal Settings Menu Items

Menu Item	View	Technician	Engineer	Admin
Terminal > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Terminal > Details	Read-Only	Read-Only	Read-Only	Read-Only
Terminal > Device	No Access	Read-Write	Read-Write	Read-Write
Terminal > Date / Time	Read-Only	Read-Write	Read-Write	Read-Write
Terminal > Operating Mode	No Access	Read-Write	Read-Write	Read-Write
Terminal > Sleep Mode	No Access	Read-Write	Read-Write	Read-Write
Radio > Radio Summary	Read-Only	Read-Only	Read-Only	Read-Only
Radio > Channel Summary	Read-Only	Read-Only	Read-Only	Read-Only
Radio > Radio Setup	No Access	Read-Write	Read-Write	Read-Write
Radio > Channel Setup	No Access	Read-Write	Read-Write	Read-Write
Radio > Advanced Setup	No Access	Read-Write	Read-Write	Read-Write
Serial > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Serial > Port Setup	No Access	Read-Write	Read-Write	Read-Write
Ethernet > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Ethernet > Port Setup	No Access	Read-Write	Read-Write	Read-Write
Ethernet > L2 Filtering	No Access	No Access	Read-Write	Read-Write
Ethernet > VLAN	No Access	No Access	Read-Write	Read-Write
IP > IP Summary	Read-Only	Read-Only	Read-Only	Read-Only
IP > Terminal Server Summary	Read-Only	Read-Only	Read-Only	Read-Only
IP > IP Setup	No Access	Read-Write	Read-Write	Read-Write
IP > Terminal Server Setup	No Access	Read-Write	Read-Write	Read-Write
IP > L3 Filtering	No Access	No Access	Read-Write	Read-Write
IP > IP Routes	No Access	No Access	Read-Write	Read-Write
IP > NAT	No Access	No Access	Read-Write	Read-Write
QoS > Summary	Read-Only	Read-Only	Read-Only	Read-Only
QoS > Traffic Priority	No Access	No Access	Read-Write	Read-Write
QoS > Traffic Classification	No Access	No Access	Read-Write	Read-Write
Security > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Security > Setup	No Access	No Access	Read-Write	Read-Write
Security > Users	No Access	No Access	No Access	Read-Write
Security > RADIUS	No Access	No Access	No Access	Read-Write
Security > SNMP	No Access	No Access	No Access	Read-Write
Security > Manager	No Access	No Access	Read-Write	Read-Write
Security > Distribution	No Access	No Access	Read-Write	Read-Write
Maintenance > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Maintenance > General	No Access	Read-Write	Read-Write	Read-Write

Menu Item	View	Technician	Engineer	Admin
Maintenance > Test Mode	No Access	Read-Write	Read-Write	Read-Write
Maintenance > Modem	No Access	Read-Write	Read-Write	Read-Write
Maintenance > Defaults	No Access	No Access	No Access	Read-Write
Maintenance > RF	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 > SCADA	No Access	No Access	Read-Write	Read-Write
Maintenance > Files	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 > Event Action Setup	No Access	No Access	Read-Write	Read-Write
Events > Syslog	No Access	No Access	Read-Write	Read-Write
Events > Defaults	No Access	No Access	Read-Write	Read-Write
Software > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Software > Setup	No Access	No Access	Read-Write	Read-Write
Software > File Transfer	No Access	No Access	Read-Write	Read-Write
Software > File Primary Transfer	No Access	No Access	Read-Write	Read-Write
Software > File Secondary Transfer	No Access	No Access	Read-Write	Read-Write
Software > Manager	No Access	No Access	Read-Write	Read-Write
Software > Remote Distribution	No Access	No Access	Read-Write	Read-Write
Software > Remote Activation	No Access	No Access	Read-Write	Read-Write
Monitoring > Terminal	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Serial	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Ethernet	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Radio	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Interface	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > User Selected	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > TCP Connections	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Routing Table	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Address Tables	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > NAT	Read-Only	Read-Only	Read-Only	Read-Only

Network Settings Menu Items

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

SuperVisor Menu Items

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

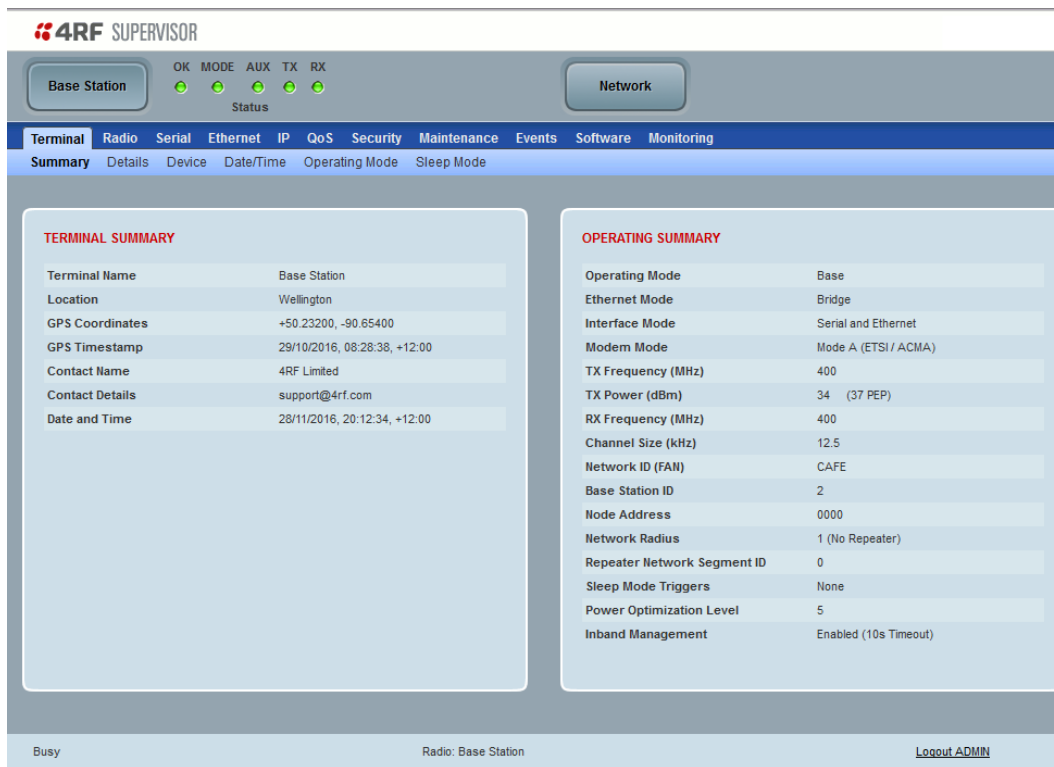
- Standard Radio
- Protected Station

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

Standard Radio

Terminal

Terminal > Summary



4RF SUPERVISOR

Base Station OK MODE AUX TX RX Status Network

Terminal Radio Serial Ethernet IP QoS Security Maintenance Events Software Monitoring

Summary Details Device Date/Time Operating Mode Sleep Mode

TERMINAL SUMMARY

Terminal Name	Base Station
Location	Wellington
GPS Coordinates	+50.23200, -90.65400
GPS Timestamp	29/10/2016, 08:28:38, +12:00
Contact Name	4RF Limited
Contact Details	support@4rf.com
Date and Time	28/11/2016, 20:12:34, +12:00

OPERATING SUMMARY

Operating Mode	Base
Ethernet Mode	Bridge
Interface Mode	Serial and Ethernet
Modem Mode	Mode A (ETSI / ACMA)
TX Frequency (MHz)	400
TX Power (dBm)	34 (37 PEP)
RX Frequency (MHz)	400
Channel Size (kHz)	12.5
Network ID (FAN)	CAFE
Base Station ID	2
Node Address	0000
Network Radius	1 (No Repeater)
Repeater Network Segment ID	0
Sleep Mode Triggers	None
Power Optimization Level	5
Inband Management	Enabled (10s Timeout)

Busy Radio: Base Station Logout ADMIN

TERMINAL SUMMARY

This page displays the current settings for the Terminal parameters. See ‘Terminal > Details’ on page 106, ‘Terminal > Device’ on page 108 and ‘Terminal > Operating Mode’ on page 116 for setting details.

OPERATING SUMMARY

Operating Mode

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

Interface Mode

This parameter displays the Interfaces available for traffic on the radio such as Ethernet and Serial. For Ethernet availability on the radio see ‘Maintenance > Licence’ on page 270.

Modem Mode

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

TX Frequency (MHz)

This parameter displays the current Transmit Frequency in MHz.

TX Power (dBm)

This parameter displays the current Transmit Power in dBm.

RX Frequency (MHz)

This parameter displays the current Receive Frequency in MHz.

Channel Size (kHz)

This parameter displays the current Channel Size in kHz.

Network ID

This parameter is the network ID of this base station node and its remote / repeater stations in the network. The entry is four alphanumeric characters.

Base Station ID

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

It is especially important to set different values for each network when two or more networks using the same frequencies are operating with some overlapping coverage. The entry is an integer from 1 to 32.

Node Address

The Node Address of the base station is 0000.

If the Node Address shown is FFFE, this radio is a remote radio 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 radios. This address can be between 000B to 01FE.

Network Radius

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

Network Repeaters Proximity

This parameter displays the proximity of repeaters in the network.

Repeater Network Segment ID

This parameter identifies the repeater network segment this radio belongs to. This allows a remote to communicate only with the correct base/repeater for improved reliability, and also allows improved performance by only forwarding through a repeater when a packet is destined for that repeater segment.

The base station and each repeater should be assigned a unique value between 1 and 31. Each remote radio should be assigned the same number as the base station or repeater that it is connected to.

A Repeater Network Segment ID of 0 means that the radio will communicate with any repeater, which in some overlapping coverage scenarios can reduce reliability. Using a Repeater Network Segment ID of 0 also disables the improved performance.

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

4RF SUPERVISOR

Base Station

OK MODE AUX TX RX

Status

Network

Terminal

Radio

Serial

Ethernet

IP

QoS

Security

Maintenance

Events

Software

Monitoring

Summary

Details

Device

Date/Time

Operating Mode

Sleep Mode

MANUFACTURING DETAILS

Radio Serial Number	R1310000522
Sub-Assembly Serial Number	13092449
HW Frequency Band	400 - 470MHz
HW Type	B
RF Interface MAC Address	00:22:b2:10:09:a1
Ethernet Port 1 MAC Address	00:22:b2:10:09:9c
Ethernet Port 2 MAC Address	00:22:b2:10:09:9d
Active Software Version	1.9.4
Previous Software Version	1.9.1

Busy

Radio: Base Station

Logout ADMIN

MANUFACTURING DETAILS

Radio Serial Number

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



Sub-Assembly Serial Number

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



HW Frequency Band

This parameter displays the hardware radio frequency operating range.

HW Type

This parameter displays the radio hardware type (see 'Radio Hardware Types' on page 403).

Radio MAC Address

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

Active Software Version

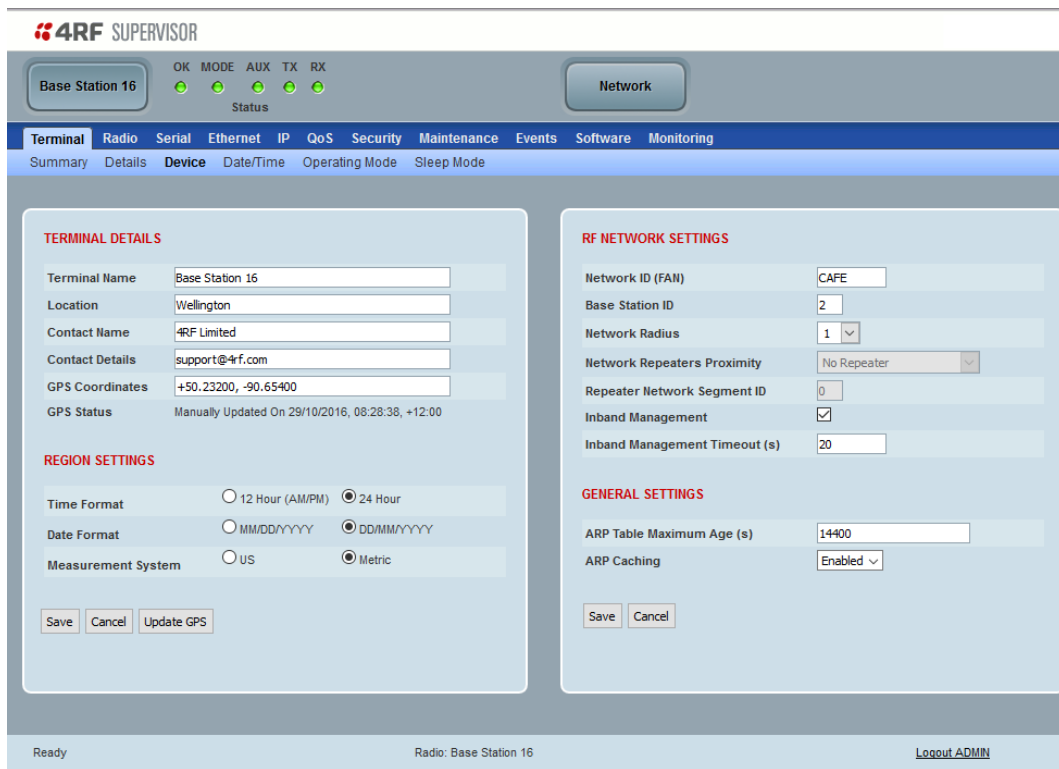
This parameter displays the version of the software currently operating the radio.

Previous Software Version

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

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

Terminal > Device



The screenshot shows the 4RF SUPERVISOR web interface. At the top, there's a status bar for 'Base Station 16' with indicators for OK, MODE, AUX, TX, and RX. Below this is a navigation menu with tabs for Terminal, Radio, Serial, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring. The 'Terminal' tab is active, and within it, the 'Device' sub-tab is selected. The main content area is divided into two panels: 'TERMINAL DETAILS' and 'RF NETWORK SETTINGS'.

TERMINAL DETAILS

- Terminal Name: Base Station 16
- Location: Wellington
- Contact Name: 4RF Limited
- Contact Details: support@4rf.com
- GPS Coordinates: +50.23200, -90.65400
- GPS Status: Manually Updated On 29/10/2016, 08:28:38, +12:00

REGION SETTINGS

- Time Format: ☐ 12 Hour (AM/PM) ☒ 24 Hour
- Date Format: ☐ MM/DD/YYYY ☒ DD/MM/YYYY
- Measurement System: ☐ US ☒ Metric

Buttons: Save, Cancel, Update GPS

RF NETWORK SETTINGS

- Network ID (FAN): CAFE
- Base Station ID: 2
- Network Radius: 1
- Network Repeaters Proximity: No Repeater
- Repeater Network Segment ID: 0
- Inband Management: ☒
- Inband Management Timeout (s): 20

GENERAL SETTINGS

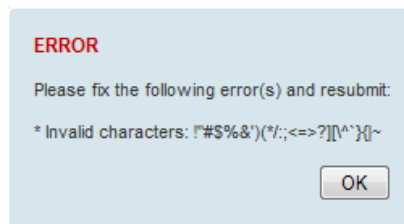
- ARP Table Maximum Age (s): 14400
- ARP Caching: Enabled

Buttons: Save, Cancel

Footer: Ready, Radio: Base Station 16, Logout ADMIN

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:



ERROR

Please fix the following error(s) and resubmit:

* Invalid characters: !"#\$%&'()*+,-./:;<=>?[^\`{}|]~

OK

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

GPS Coordinates

This parameter sets the GPS Coordinates for the radio location. It can be manually entered and saved or if the radio is fitted with a GPS Receiver, it can be set by clicking on the Update GPS button. The entry is two values of latitude and longitude comma delimited;

- The Latitude value must be a decimal number anywhere from -90 to 90
- The Longitude value must be a decimal number anywhere from -180 to 180

GPS Status

This field displays the status of the GPS Receiver if enabled (see 'GPS Receiver' on page 166).

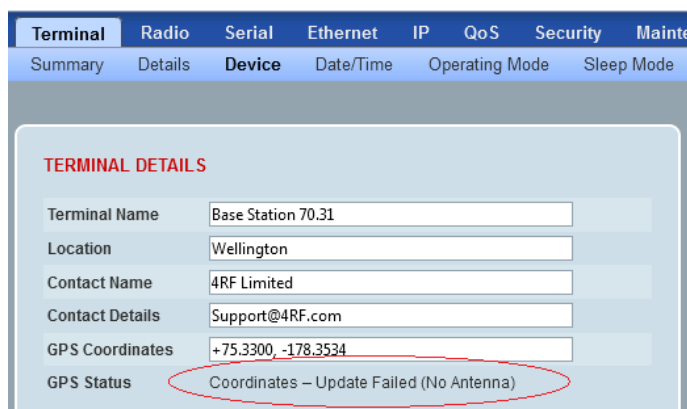
The GPS Horizontal Dilution Of Precision (HDOP) information provides a GPS signal quality rating;

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

Controls

The Update GPS button updates the GPS Coordinates field from the installed USB GPS Receiver.

If the GPS Receiver is enabled but is not operating or not receiving a valid GPS signal, the GPS Status will show 'Update Failed'.



The screenshot shows the 'Terminal' tab selected in the top navigation bar. Below it, the 'Details' sub-tab is active. The 'Device' section is expanded, showing 'TERMINAL DETAILS'. The fields are as follows:

- Terminal Name: Base Station 70.31
- Location: Wellington
- Contact Name: 4RF Limited
- Contact Details: Support@4RF.com
- GPS Coordinates: +75.3300, -178.3534
- GPS Status: Coordinates - Update Failed (No Antenna)

The 'GPS Status' field is circled in red, indicating the failure state.

REGION SETTINGS

Time Format

This parameter sets the time format for all time based results.

The default setting is 24 Hours.

Date Format

This parameter sets the date format for date based results.

The default setting is DD/MM/YYYY.

Measurement System

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

The default setting is Metric.

RF NETWORK DETAILS

Network ID

This parameter sets the network ID of this base station node and its remote / repeater stations in the network. The entry is four alphanumeric characters.

The default setting is CAFE.

Base Station ID

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

It is especially important to set different values for each network when two or more networks using the same frequencies are operating with some overlapping coverage. The entry is an integer from 1 to 32.

Note: starting with release 2.0.0, the Base Station ID has been extended to support up to 32 (instead up to 8). If a Base Station ID of greater than 8 is selected and if the software is downgraded, the previous valid Base Station ID from 1 - 8 will be reinstated. If other radios in the network are still operating with Base Station IDs greater than 8, then this will cause a mismatch and the units will not be able to associate.

Network Radius

This parameter sets the maximum number of hops in this network e.g. in a network with base station, repeater and remotes communicating via the repeater, the Network Radius should be set to 2. If the Network Radius is set to 2, a message from that node will only pass 2 hops before it is blocked. The default setting is 1.

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

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

Network Repeaters Proximity

Network Radius > 1

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

Option	Function
No Repeater	Use when there is no repeater in the network.
Single Repeater Only	Use when there is only one repeater in the network and remotes may communicate through repeater or directly with the base station.
Single Repeater Only (no base remotes)	Use this when there is only one repeater in the network and all remotes communicate through the repeater. This setting allows increased performance compared with Single Repeater Only proximity.
Overlapping Coverage	Use for multiple one hop repeaters where the remote radio 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 radio 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.

Network Radius = 1

This parameter is set in remote radios to indicate the proximity of repeaters in the network when the Network Radius is set to 1. All remote radios in the network must be set the same.

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

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

Operating Mode	Network Radius	Options	Default
Base	1	No Repeater	No Repeater
Base	2	All (except No Repeater)	Single Repeater Only
Remote or Repeater	1	No Repeater, Base Repeater	No Repeater
Remote or Repeater	2	All (except No Repeater)	Single Repeater Only
Base Repeater	1	Base Repeater	No Repeater
Base Repeater	2	All (except No Repeater)	Single Repeater Only

Repeater Network Segment ID

This parameter identifies the repeater network segment this radio belongs to. This allows a remote to communicate only with the correct base/repeater for improved reliability, and also allows improved performance by only forwarding through a repeater when a packet is destined for that repeater segment.

The base station and each repeater should be assigned a unique value between 1 and 31. Each remote radio should be assigned the same number as the base station or repeater that it is connected to.

A Repeater Network Segment ID of 0 means that the radio will communicate with any repeater, which in some overlapping coverage scenarios can reduce reliability. Using a Repeater Network Segment ID of 0 also disables the improved 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.

GENERAL SETTINGS

ARP Table Maximum Age

This parameter sets the maximum time that an ARP entry can be present in the ARP table.

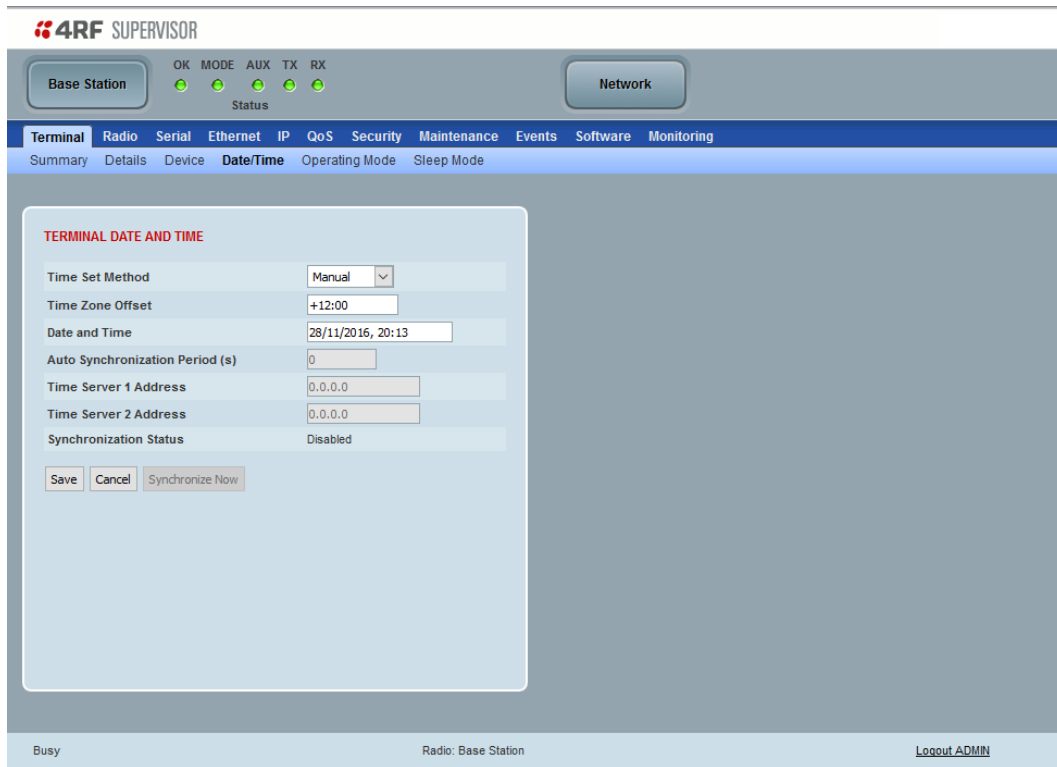
The default setting is 14400 seconds.

ARP Caching

This parameter enables ARP caching. The default setting is Enabled.

Option	Function
Disabled	ARP requests for remote devices are always sent OTA
Enabled	Allows the local radio to respond to ARP requests from its own cache instead of forwarding the request OTA

Terminal > Date / Time



The screenshot shows the 4RF SUPERVISOR web interface. At the top, there's a status bar with 'Base Station' and 'Network' buttons, and a row of status indicators (OK, MODE, AUX, TX, RX) with green lights. Below this is a navigation menu with 'Terminal' selected. Under 'Terminal', there's a sub-menu with 'Summary', 'Details', 'Device', 'Date/Time' (selected), 'Operating Mode', and 'Sleep Mode'. The main content area is titled 'TERMINAL DATE AND TIME' and contains the following fields:

- Time Set Method:** A dropdown menu set to 'Manual'.
- Time Zone Offset:** A text input field containing '+12:00'.
- Date and Time:** A text input field containing '28/11/2016, 20:13'.
- Auto Synchronization Period (s):** A text input field containing '0'.
- Time Server 1 Address:** A text input field containing '0.0.0.0'.
- Time Server 2 Address:** A text input field containing '0.0.0.0'.
- Synchronization Status:** A dropdown menu set to 'Disabled'.

At the bottom of the form are three buttons: 'Save', 'Cancel', and 'Synchronize Now'. The footer of the interface shows 'Busy', 'Radio: Base Station', and a 'Logout ADMIN' link.

TERMINAL DATE AND TIME

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

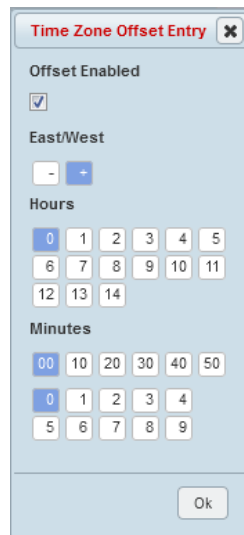
Time Set Method

This parameter sets the method for setting the Date and Time. The default setting is Manual.

Option	Function
Manual	Manual entry of Date and Time. If a remote is in Manual mode, base announcement messages from the base will update the Date and Time of the remote.
SNTP	Date and Time Synchronization feature allows a radio to synchronize its date and time from an SNTP server. Using the SNTP feature will ensure that all radios in the network has the same date and time required for accurate network diagnostics. Configure SNTP on the base station which then sends the date and time to all the remote radios. It can be configured on a remote radio if required but not on all remotes as SNTP requests could overload the network. For high availability time/date synchronization, SNTP can be synchronized from two SNTP servers for server backup. If a remote is in SNTP mode: - if an automated announcement message is sent from the base (controlled by the Announcement Period), the remote will disregard the message and not update its Date and Time - if the Synchronize Now is clicked, a manual message is sent from the base and the remote will accept the message and update its Date and Time

Time Zone Offset

The Time Zone Offset is the number of hours / minutes offset from UTC time. The default setting is 'No Offset'. Clicking the Time Zone Offset field brings up a pop-up to enter the offset.



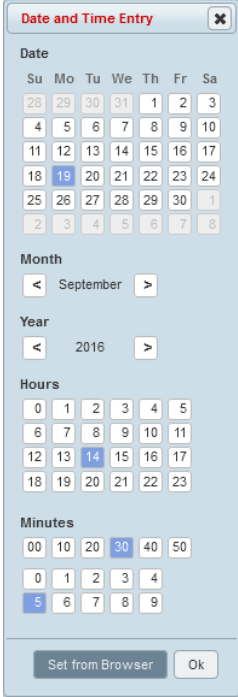
The dialog box is titled "Time Zone Offset Entry" with a close button (X) in the top right corner. It contains the following fields and controls:

- Offset Enabled:** A checkbox that is currently checked.
- East/West:** Two buttons, a minus sign (-) and a plus sign (+), for selecting the direction of the offset.
- Hours:** A grid of buttons for selecting the hour offset. The buttons are arranged in three rows: the first row contains 0, 1, 2, 3, 4, 5; the second row contains 6, 7, 8, 9, 10, 11; and the third row contains 12, 13, 14. The button "0" is currently selected.
- Minutes:** Two rows of buttons for selecting the minute offset. The first row contains 00, 10, 20, 30, 40, 50. The second row contains 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. The button "00" is currently selected.
- Ok:** A button at the bottom right to confirm the selection.

After selecting the offset, review the current date and time before saving the changes.

Date and Time

This sets the radio Date and Time. Clicking the Date and Time field brings up a pop-up to enter the date and time.



The 'Date and Time Entry' dialog box is shown. It contains the following sections:

- Date:** A calendar grid showing the month of September 2016. The date 19 is selected.
- Month:** A dropdown menu showing 'September'.
- Year:** A dropdown menu showing '2016'.
- Hours:** A grid of numbers from 0 to 23. The number 14 is selected.
- Minutes:** A grid of numbers from 00 to 50 in increments of 10. The number 30 is selected.
- Buttons:** 'Set from Browser' and 'Ok'.

The 'Set from Browser' button sets the date and time directly from the browser date and time.

If the Set from Browser button is used and the offset for the browser and the radio are different, then SuperVisor will adjust the time displayed in the text box to be the local time for the radio e.g. clicking 5pm in Sydney (+10:00) will put 3 pm in the text box for a Perth based radio (+08:00).

Auto Synchronization Period (s)

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

The base station sends a broadcast message to the remote radios to synchronize the radio date and time at a rate controlled by the Announcement Period (see page 276).

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.

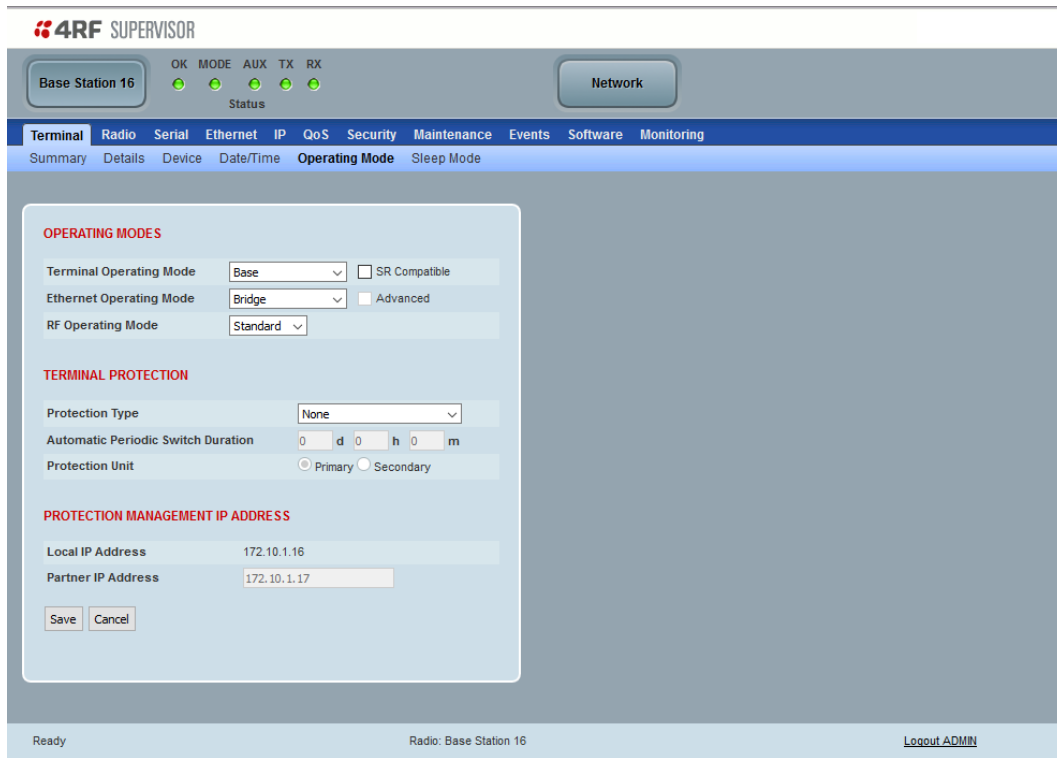
Synchronization Status

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 of the remote radios.

Terminal > Operating Mode



4RF SUPERVISOR

Base Station 16 OK MODE AUX TX RX Status Network

Terminal Radio Serial Ethernet IP QoS Security Maintenance Events Software Monitoring

Summary Details Device Date/Time **Operating Mode** Sleep Mode

OPERATING MODES

Terminal Operating Mode: Base ☐ SR Compatible

Ethernet Operating Mode: Bridge ☐ Advanced

RF Operating Mode: Standard

TERMINAL PROTECTION

Protection Type: None

Automatic Periodic Switch Duration: 0 d 0 h 0 m

Protection Unit: ☒ Primary ☐ Secondary

PROTECTION MANAGEMENT IP ADDRESS

Local IP Address: 172.10.1.16

Partner IP Address: 172.10.1.17

Save Cancel

Ready Radio: Base Station 16 Logout ADMIN

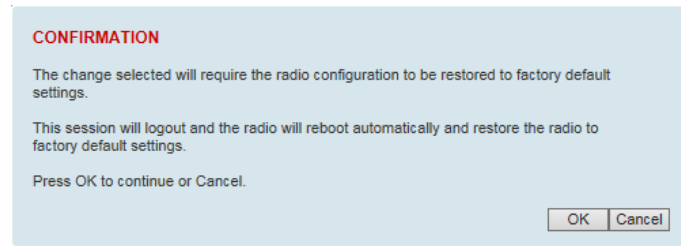
OPERATING MODES

Terminal Operating Mode

The Terminal Operating Mode defines the radio mode of operation. The default setting is Remote.

Option	Function
Base	The Base operating mode manages all traffic activity between itself, repeaters, and remotes. It is the center-point of network where in most cases will be connected to a SCADA master.
Base Repeater	The Base Repeater operating mode has the same function as the base (and repeater station) but used when peer to peer connections between remotes is required via the base station.
Base MMS	The Base MMS operating mode has the same function as the base operating mode but used with a Migration Station (see Aprisa SR+ MMS User Manual).
Repeater	The Repeater operating mode forwards packets coming from base station and other repeaters e.g. in daisy chain LBS mode and /or remote radios.
Repeater MMS	The Repeater MMS operating mode has the same function as the repeater operating mode but used with a Migration Station (see Aprisa SR+ MMS User Manual).
Remote	The Remote operating mode in most cases is used as the end-point of the SCADA network connected to an RTU or PLC device for SCADA network control and monitoring.
Point To Point	The Point To Point operating mode configures a full duplex radio for Point-to-point (PTP) operation. Changing from PMP or PTP or vice versa requires the radio to be 'restored to factory default settings' which will clear <u>all</u> previous radio setup and configuration. See 'Point-To-Point' section on page 405.

When the Terminal Operating Mode is changed from PMP to PTP or vice versa, the following popup will warn of the 'restore to factory default settings'.



SR Compatible

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

When the 'SR Compatible' option is activated on a Aprisa SR+ base station, the base station can operate with a mixture of SR+ and SRx remote radios.

In a mixed network when a Aprisa SR+ base station is working with SR+ and SRx remotes, the SR+ remote is not set to 'SR Compatible' mode to allow the remote SR+ work in the highest performance modulation. The SR+ base must be set to 'SR Compatible' mode to allow operation with SRx remotes, but it will not restrict the SR+ base to Tx packet at modulations higher than QPSK when the destination is a SR+ remote radio. Thus, the SR+ base station modulation can be set to a modulation higher than QPSK.

Ethernet Operating Mode

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

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

Advanced

Enabled for Gateway Router and Router modes only. The default setting is unticked.

To enable Advanced routing, select the operating mode; Router or Gateway Router and tick the Advanced checkbox.

Advanced Gateway Router mode (AGRM) or Advanced Router mode (ARM) act like a true router between the Ethernet ports and RF interface port where the next hop is one of these ports. This means that the RF interface is a public interface exposed to the user with IP and MAC address like the Ethernet interface.

In AGRM mode, all Ethernet interfaces have the same IP address and subnet.

In ARM mode, each Ethernet interface has a different IP address and subnet.

See 'Advanced Gateway Router Mode (AGRM) and Advanced Router Mode (ARM)' on page 41 for a detailed explanation of advanced router modes.

Note 1: The Network Address Translation feature works only in Advanced Router or Advanced Gateway Router operating mode (see 'IP > NAT' on page 193).

Note 2: When the radio Ethernet Operating Mode is Router Mode or Advanced Router Modes, users must connect to SuperVisor via Ethernet Port 1 to have full management functionality when performing remote management to the other radios on the network.

RF Operating Mode

The RF Operating Mode defines the operation of the RF over-the-air. The default setting is Standard.

Option	Function
Standard	The radio operates normally.
Disabled	Disables all RF over-the-air communications from the RF port and turns off the transmitter and receiver to save power. This enables a radio to be used as a Terminal Server without RF.

TERMINAL PROTECTION

Protection Type

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

Option	Function
None	The SR+ radio is stand-alone radio (not part of an Aprisa SR+ Protected Station).
Redundant (Protected Station)	Set to make this SR+ radio part of an Aprisa SR+ Protected Station. The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio.
Monitored Hot Standby (Protected Station)	Set to make this SR+ radio part of an Aprisa SR+ Protected Station. The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio. The standby radio is monitored to ensure its correct operation should a switch-over be required. See 'Monitored Alarms' on page 412 for the list of monitored alarms.
Serial Data Driven Switching	Set to make this SR+ radio part of an Aprisa SR+ Data Driven Protected Station.

Automatic Periodic Switch Duration

The Automatic Periodic Switch Duration sets the time interval for automatic switch-over from the active radio to the standby radio.

This feature will automatically switch over from the active radio to the standby radio if there are no alarms preventing the switch-over to the standby radio. It can be used to provide confidence that the standby radio is still operational, maybe after many days of standby operation.

The maximum number of days that can be set is 49 days.

The default setting is 0 which disables the automatic switch-over feature.

Protection 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 > Sleep Mode

Sleep Mode is a feature of Type B Aprisa SR+ radios. This page is only visible when the radio is of Type B hardware see 'Radio Hardware Types' on page 403.

4RF SUPERVISOR

Base Station 16 OK MODE AUX TX RX Status Network

Terminal Radio Serial Ethernet IP QoS Security Maintenance Events Software Monitoring

Summary Details Device Date/Time Operating Mode **Sleep Mode**

SLEEP MODE SETTINGS

Sleep Mode: Automatic

Awake Duration for ABB Totalflow®: ☒ (automatic) (ms)

Serial Port 1 DTR Input Trigger: Disabled

Serial Port 2 DTR Input Trigger: Disabled

Alarm Input 1 Trigger: Disabled

Wake Up Transmit Delay: ☒ (automatic) (ms)

OPERATING VOLTAGE SETTINGS

Current Input Voltage (V): 12.220

Minimum Turn On Input voltage (V): 10

Minimum Turn Off Input voltage (V): 9.5

Save Cancel

RECEIVE IDLE SETTINGS

Power Optimization: 5

High power consumption (Low initial packet latency) Low power consumption (High initial packet latency)

Inactivity Period Before Idle (ms): 4000

Save Cancel

Ready Radio: Base Station 16 Logout ADMIN

SLEEP MODE SETTINGS

Sleep mode allows the radio to be put to sleep where it consumes very little power (< 0.5 watts with all Ethernet ports disabled) but allows rapid wake up. Once awake, remote devices will typically re-associate with the SR+ network within 3 seconds, but this depends on signal conditions.

The sleep and wake up is controlled from the Alarm Input 1 or serial port DTR triggers. The Aprisa SR+ will be in sleep mode if one or more of the Alarm Input 1 or serial port DTR triggers are set to Enabled, and one or more of the enabled sleep triggers are active. If sleep mode is enabled for serial port DTR trigger and the customer serial interface is not connected, the radio will sleep.

When radio is in sleep mode, the OK LED pulses once per second at a colour depending on the current state of the OK LED before sleep mode was entered and the other LEDs will be OFF.

Sleep mode will be disabled and sleeping radio will be woken up while a management user is logged into the radio or when a USB CLI cable is inserted in the management port.

Sleep mode will be disabled and sleeping radio will be woken up when an Ethernet cable is inserted into an enabled Ethernet port configured for 'management and user data', however 60 seconds after insertion, the radio will be allowed to enter sleep unless the user has logged into SuperVisor.

Pressing the radio 'test' button and holding for 1 second will also wake up a sleeping radio for 5 minutes.

Sleep Mode

The Sleep Mode parameter sets how sleep mode is controlled. The default setting is Automatic.

Option	Function
Automatic	If this radio is a remote, it uses the setting from the base station. If this radio is the base station, the external triggers control the radio sleep mode state.
Standard	The external triggers control the radio sleep mode state.
ABB Totalflow ®	The external trigger wakes up the radio for up to the maximum duration set in the 'Awake Duration' or indefinitely if data is sent to the RTU.

Awake Duration for ABB Totalflow ®

The Awake Duration sets the radio awake duration when there is no data being sent to the RTU.

Triggers

The triggers when enabled cause the radio to sleep or wake up. For the radio to sleep, all the enabled triggers must be OFF i.e. if only one enabled trigger goes ON, the radio will wake up.

Serial Port 1 / 2 DTR Trigger

The Serial Port 1 / 2 DTR Trigger controls the radio sleep and wake up. The default setting is Disabled.

Option	Function
Disabled	The Serial Port DTR has no effect on sleep mode.
Active Low (sleep when input is low)	The Serial Port DTR ON state causes the radio to wake up and the DTR OFF state allows the radio to sleep.

The Aprisa SR+ valid control states are:

- ON state = +2.7 to +20 volts
- OFF state = -20 to +0.6 volts

Alarm Input 1 Trigger

The Alarm Input 1 Trigger controls the radio sleep and wake up. The default setting is Disabled.

Option	Function
Disabled	The Alarm Input 1 has no effect on sleep mode.
Active Low (sleep when input is low)	The Alarm Input 1 high (ON) state causes the radio to wake up and the low (OFF) state allows the radio to sleep (see 'Alarm Inputs' on page 488 for alarm input specification). Note: If the alarm input is disconnected (e.g. alarm cable unplugged), the radio will go to sleep.

Wake Up Transmit Delay (ms)

The Wake Up Transmit Delay (ms) sets the maximum time to check if the channel is clear before the radio attempts to transmit. The transmitter will wait for either;

- a packet to be received from the base station or
- the expiry of the Wake Up Transmit Delay

The default setting is Ticked (Automatic) which automatically calculates the best case for this delay for the current radio settings. This value will be between 0.4 second and 2 seconds depending on channel size and compliance mode.

The following are the default Wake Up Transmit delays;

Channel Size	Wake Up Transmit Delay (seconds)
12.5 kHz	1.6
20 kHz	1.1
25 kHz	0.8
50 kHz	0.41

Maximum Power Savings

If the Ethernet ports are not required for customer traffic, maximum power savings can be achieved by disabling them. This will however prevent SuperVisor management with Ethernet. The Ethernet ports can only be restored using SNMP or the CLI.

To enable Ethernet ports from the CLI:

1. Connect the radio management port (MGMT) to your PC with a USB A to USB micro B cable. This will wake a radio that is sleeping.
2. Login to the CLI. The default login is Login: 'admin' Password: 'admin'
3. At the CLI prompt >> type 'cd APRISASR-MIB-4RF' enter
4. At the CLI prompt >> type 'set ethPort1Enabled 1' enter (for port 1)

OPERATING VOLTAGE SETTINGS

Power supply input voltage thresholds are used to trigger Aprisa SR+ sleep mode to reduce power consumption.

The difference between the two thresholds Turn On and Turn Off defines the detection hysteresis.

In sleep mode, the main CPU goes into sleep mode and all the ports shut down.

Note: To prevent a 48V Protected Station always going into low power mode, set the 'Minimum Turn On Input Voltage' to 10 V and the 'Minimum Turn Off Input Voltage' to 9.5 V.

Minimum Turn On Input Voltage:

The SR+ will not turn on when input supply voltage remains lower than this threshold. While voltage is lower than this threshold, but higher than minimum operating voltage of the Aprisa SR+, the OK led will flash once every 5 seconds. The valid values are from 10.0 V and 27.0 V but the value must always be higher than Minimum Turn Off Input Voltage.

The default value is 10 V.

Minimum Turn Off Input Voltage:

The SR+ will turn off when the input supply voltage is lower than this threshold. The valid values are from 9.5 V to 26.5 V but the value must always be lower than Minimum Turn On Input Voltage.

The default value is 9.5 V.

Note: There must also be a 0.3 V difference between the 'Minimum Turn On Input Voltage' and the 'Minimum Turn Off Input Voltage'.

RECEIVE IDLE SETTINGS

Radio power consumption in idle mode is lowered by turning off the receiver when remote radios know that packet reception is not possible. This feature only works with the Access Request MAC as the Listen Before Send MAC cannot know that packet reception is not possible.

The base station receiver never goes into idle mode and is always on.

When a remote radio's receiver is in idle mode, the base station must send a series of idle exit packets before it can send a data packet or allow a remote to send a data packet. This is to ensure that all remotes can receive the data packet.

Power Optimization Level

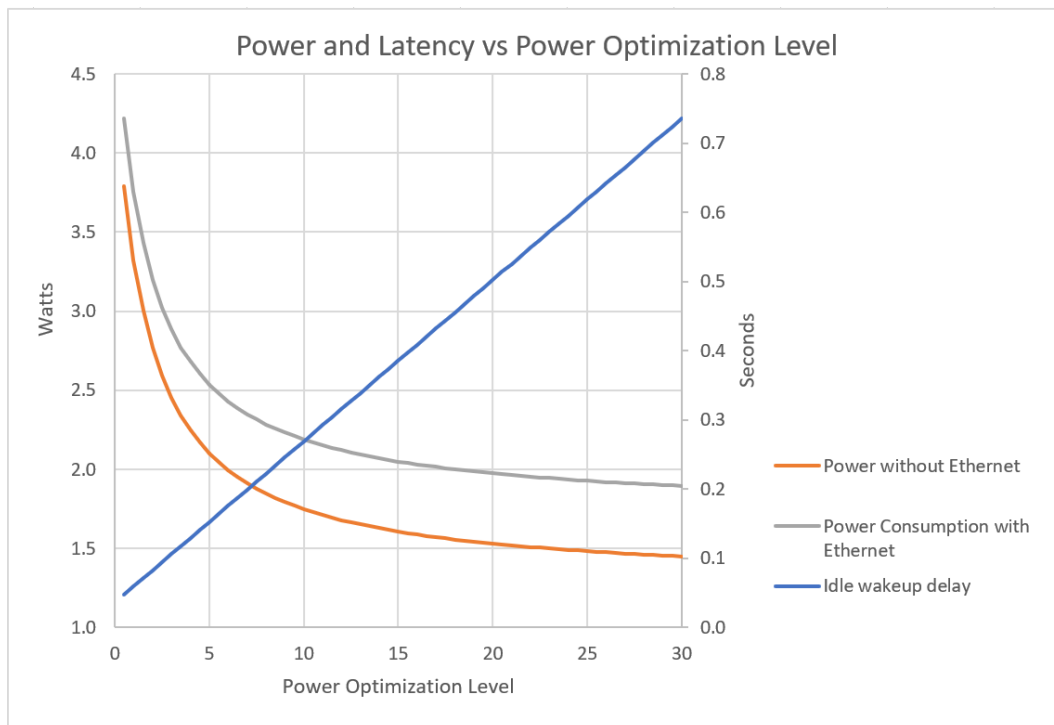
The Power Optimization Level sets the remote radio receiver on/off ratio between 0 (no power saving) and 30 (maximum power saving).

The longer the receiver is off for, the less the idle power consumption but the higher the initial packet latency.

The shorter the receiver is off for, the more the idle power consumption but the lower the initial packet latency.

All radios in an Aprisa SR+ network must use the same Power Optimization Level setting.

The default setting is 5.



Inactivity Period Before Idle (ms)

The Inactivity Period Before Idle (ms) sets the delay remote radios configured for Access Request MAC will wait before entering a power saving 'idle' state.

All radios in an Aprisa SR+ network must use the same Inactivity Period Before Idle setting.

The default setting is 4000 ms.

Radio

Radio > Radio Summary

This page displays the current settings for the Radio parameters.

4RF SUPERVISOR

Base Station

OK

MODE

AUX

TX

RX

Status

Network

Terminal

Radio

Serial

Ethernet

IP

QoS

Security

Maintenance

Events

Software

Monitoring

Radio Summary

Channel Summary

Radio Setup

Channel Setup

Advanced Setup

RADIO PATH

	TX Frequency (MHz)	TX Power (dBm)	PEP (dBm)	RX Frequency (MHz)	ATPC	Status	Active
1	787.5	37	40	757.5	Disabled	Enabled	✔
2	787	35	38	757	Enabled	Disabled	

RADIO HARDWARE

TX Frequency Range (MHz)	757 to 758, and 787 to 788
TX Frequency Step Size (kHz)	6.25
TX Power Range (dBm)	10 to 37
TX Power Step Size (dB)	1
RX Frequency Range (MHz)	757 to 758, and 787 to 788
RX Frequency Step Size (kHz)	6.25

GENERAL

Modem Mode	Mode A (FCC)
Enhanced Noise Rejection Mode	Disabled
Channel Size (kHz)	50
Modulation Type	Adaptive
ACM Control	Standard
Antenna Port Configuration	Single Antenna Single Port
RX Path Attenuation (dB)	0

ADAPTIVE CODING MODULATION

Current Modulation Type	QPSK (Low Gain)
Default Modulation	QPSK (Low Gain)

Ready

Radio: Remote

[Logout ADMIN](#)

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

Radio > Channel Summary

This page displays the current settings for the Channel parameters.



4RF SUPERVISOR

Base Station OK MODE AUX TX RX Status Network

Terminal Radio Serial Ethernet IP QoS Security Maintenance Events Software Monitoring

Radio Summary **Channel Summary** Radio Setup Channel Setup Advanced Setup

CHANNEL SETTINGS

Access Scheme	Access Request
Maximum Packet Size (bytes)	1550
Packet Filtering	Disabled
Serial Data Stream Mode	Segregate
Packet Aggregation	Enabled

DATA COMPRESSION

IP Header Compression Ratio	Disabled
Payload Compression Ratio	Automatic

TRAFFIC SETTINGS

Background Bulk Data Transfer Rate	High
Network Traffic Type	User Defined

ADVANCED SETTINGS

Default Packet Time-to-live (ms)	2500
Serial Packet Time-to-live (ms)	2500
Ethernet Packet Time-to-live (ms)	2500

Busy Radio: Base Station Logout ADMIN

See 'Radio > Channel Setup' for setting details.

DATA COMPRESSION

IP Header Compression Ratio

See 'IP Header Compression Ratio' on page 146.

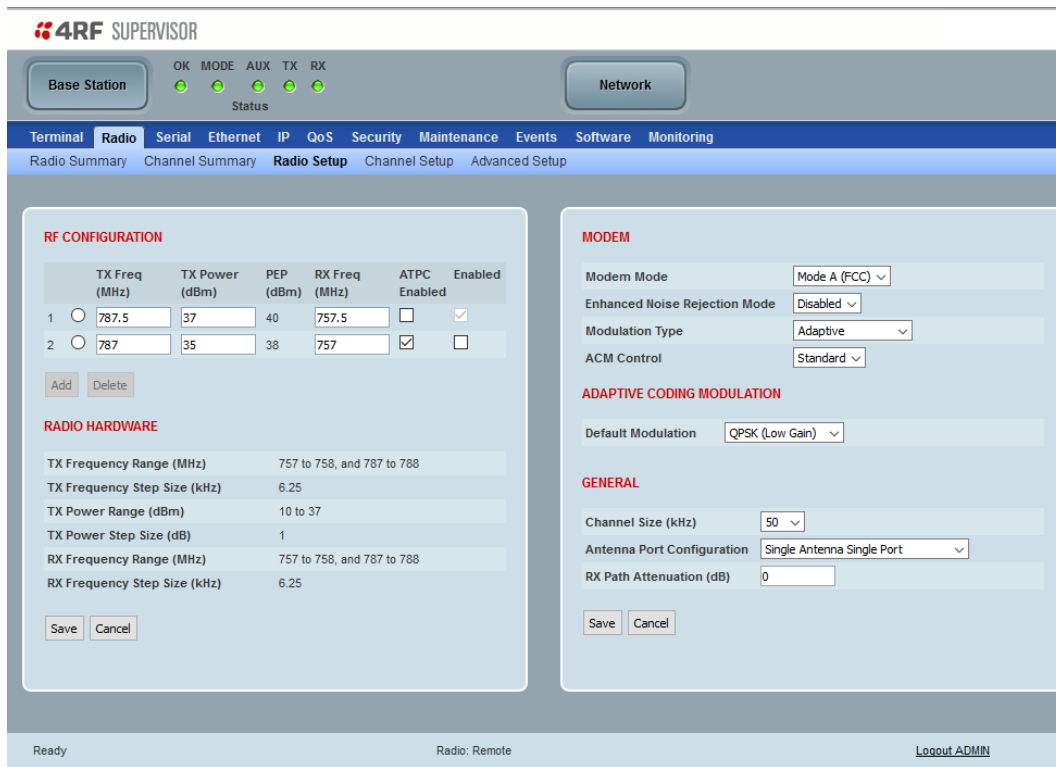
Payload Compression Ratio

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

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

Radio > Radio Setup

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



4RF SUPERVISOR

Base Station OK MODE AUX TX RX Status Network

Terminal Radio Serial Ethernet IP QoS Security Maintenance Events Software Monitoring

Radio Summary Channel Summary **Radio Setup** Channel Setup Advanced Setup

RF CONFIGURATION

	TX Freq (MHz)	TX Power (dBm)	PEP (dBm)	RX Freq (MHz)	ATPC Enabled	Enabled
1	☐ 787.5	37	40	757.5	☐	☒
2	☐ 787	35	38	757	☒	☐

Add Delete

RADIO HARDWARE

TX Frequency Range (MHz) 757 to 758, and 787 to 788

TX Frequency Step Size (kHz) 6.25

TX Power Range (dBm) 10 to 37

TX Power Step Size (dB) 1

RX Frequency Range (MHz) 757 to 758, and 787 to 788

RX Frequency Step Size (kHz) 6.25

Save Cancel

MODEM

Modem Mode Mode A (FCC) ▾

Enhanced Noise Rejection Mode Disabled ▾

Modulation Type Adaptive ▾

ACM Control Standard ▾

ADAPTIVE CODING MODULATION

Default Modulation QPSK (Low Gain) ▾

GENERAL

Channel Size (kHz) 50 ▾

Antenna Port Configuration Single Antenna Single Port ▾

RX Path Attenuation (dB)

Save Cancel

Ready Radio: Remote Logout ADMIN

RF CONFIGURATION

RF configuration profiles allows for two sets of TX Frequency, RX Frequency, TX Power and ATPC. The switch-over between the two profiles can be manual controlled (see Maintenance > RF on page 268) or automatically controlled by alarm events (see Events > Event Action Setup on page 286).

ATPC Enabled

This parameter enables the radio Automatic Transmit Power Control (ATPC). ATPC reduces the TX power to the minimum required while still providing reliable link capacity and performance at the remote radio. ATPC considers margins for fading and multi path to achieve high availability.

The benefits of ATPC are:

- Enhanced frequency use and reduced interference
- Input power saving

ATPC will dynamically adjust both the base station and remote station transmitter power to maximise the frequency reuse and reduce power consumption in the network.

A remote radio transmitter will adjust its transmitter power based on the RSSI being received at the base station. As long as the SNR being received is greater than 30dB and the RSSI is above the current set point, then the base station will send a recommendation for the remote radio to change its transmitter power. This recommendation is sent every minute and is based on the lowest RSSI received during this period. The transmitter power recommendations are a minimum of +/-1dBm up to a maximum change of +/-5dBm. The SNR limit is used to prevent interference from limiting the throughput of the system.

The RSSI set point is set per channel size to maintain enough fade margin for typical operation. If there is a change in the RSSI level of >10dB received at the base station, then the remote radio will be instructed to increase its level immediately and not wait the one minute. This is done to counter any fast fading or fault conditions that would want the transmitter power to increase quickly.

The base station transmitter will adjust its transmitter power based on the lowest received RSSI and SNR from all the remote radios in the network. The remote radios will send this information at the end of data packets so to minimize the impact of throughput on the network. Again, if the RSSI drops by more than 10dB then the base station will be instructed to increase its transmitter power level immediately.

ACM will continue to operate independently of ATPC. Any SNR fluctuations or packet errors will cause ACM to change modulations.

The monitored parameter 'Last TX Packet Forward Power' displays the current TX power setting (see 'Monitoring > Radio' on page 320).

Enabled

This parameter enables the active radio RF configuration profile.

RADIO HARDWARE

The radio hardware displays the radio TX Frequency, RX Frequency and TX Power specifications.

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 467).

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 1.250 kHz.

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

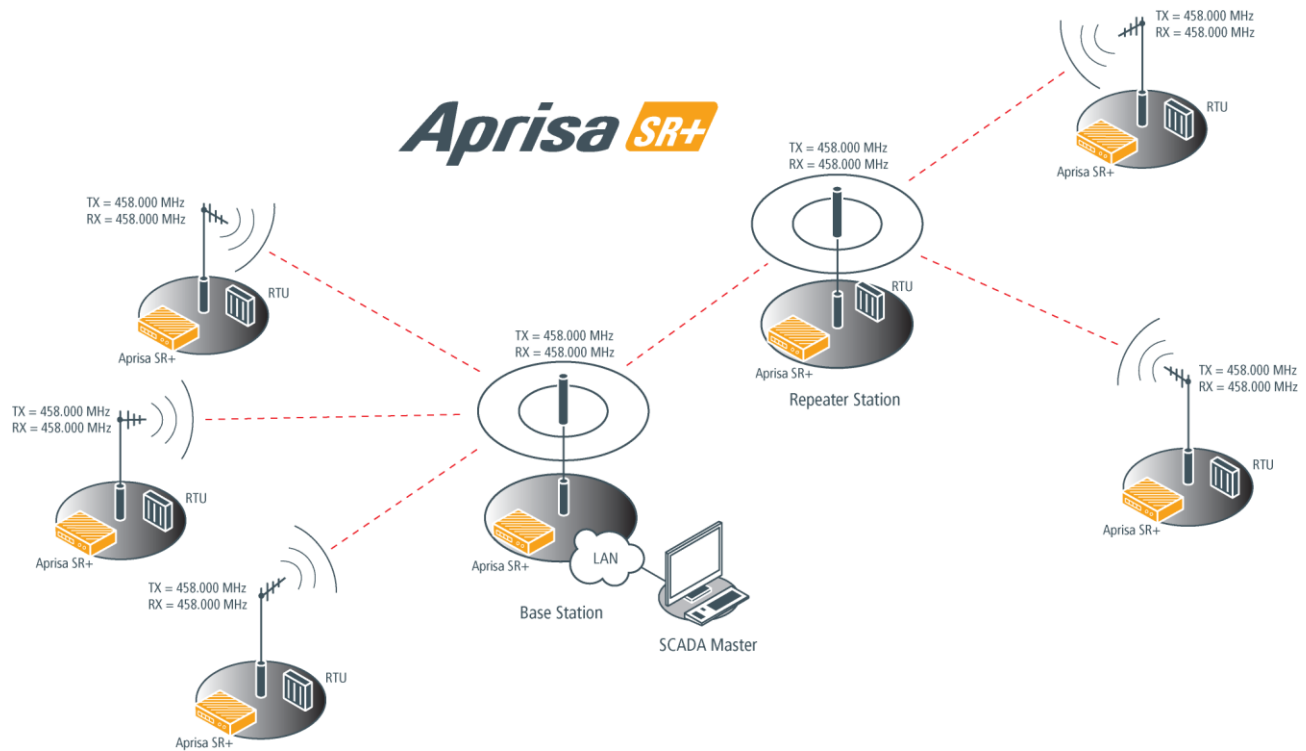
- Channel Planning
- Network Efficiencies
- Regulatory rules

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 radios.
-

Single Frequency Operation

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



To change the TX and RX frequencies:

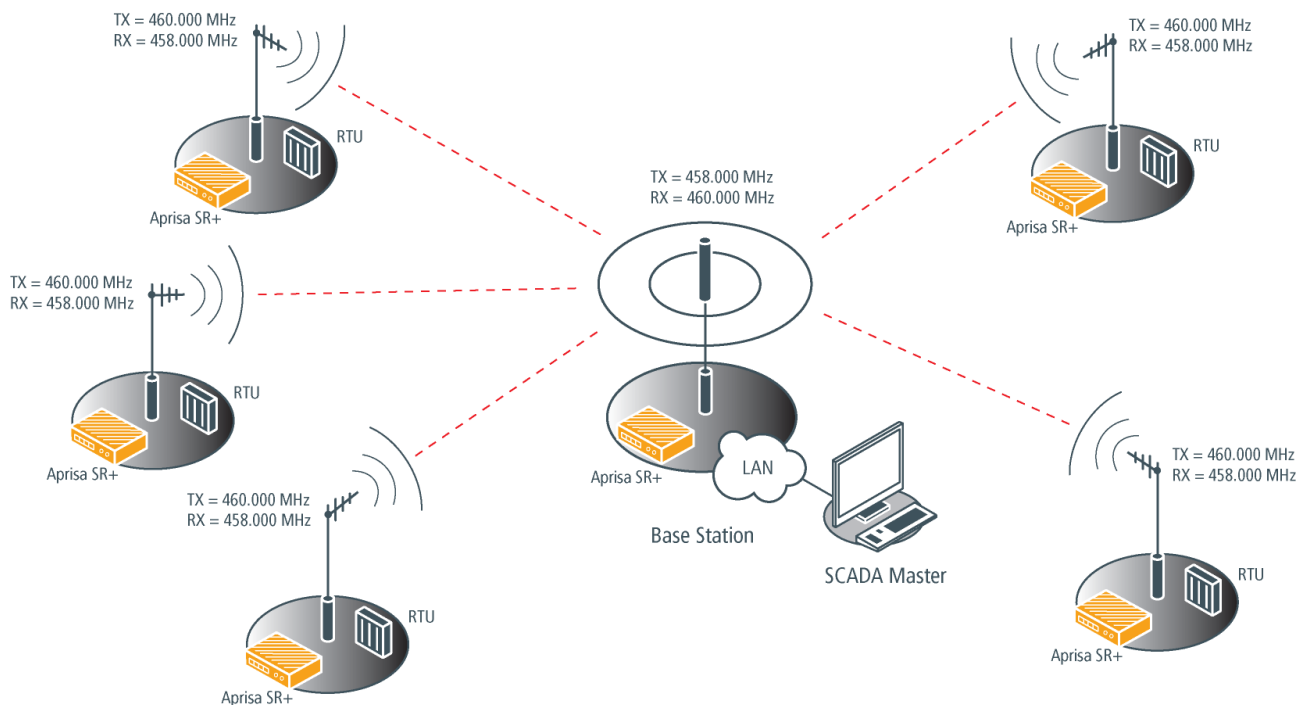
1. Change the TX and RX frequencies of the remote radios operating from the repeater station to the new frequency. The radio links to these remote radios will fail.
2. Change the TX and RX frequencies of the repeater station operating from the base station to the new frequency. The radio links to the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

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

Aprisa SR+



To change the TX and RX frequencies:

1. For all the remote radios, change the RX frequency to frequency A and the TX frequency to frequency B. The radio links to the remote radios 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 radios will restore.

Dual Frequency with Repeater

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

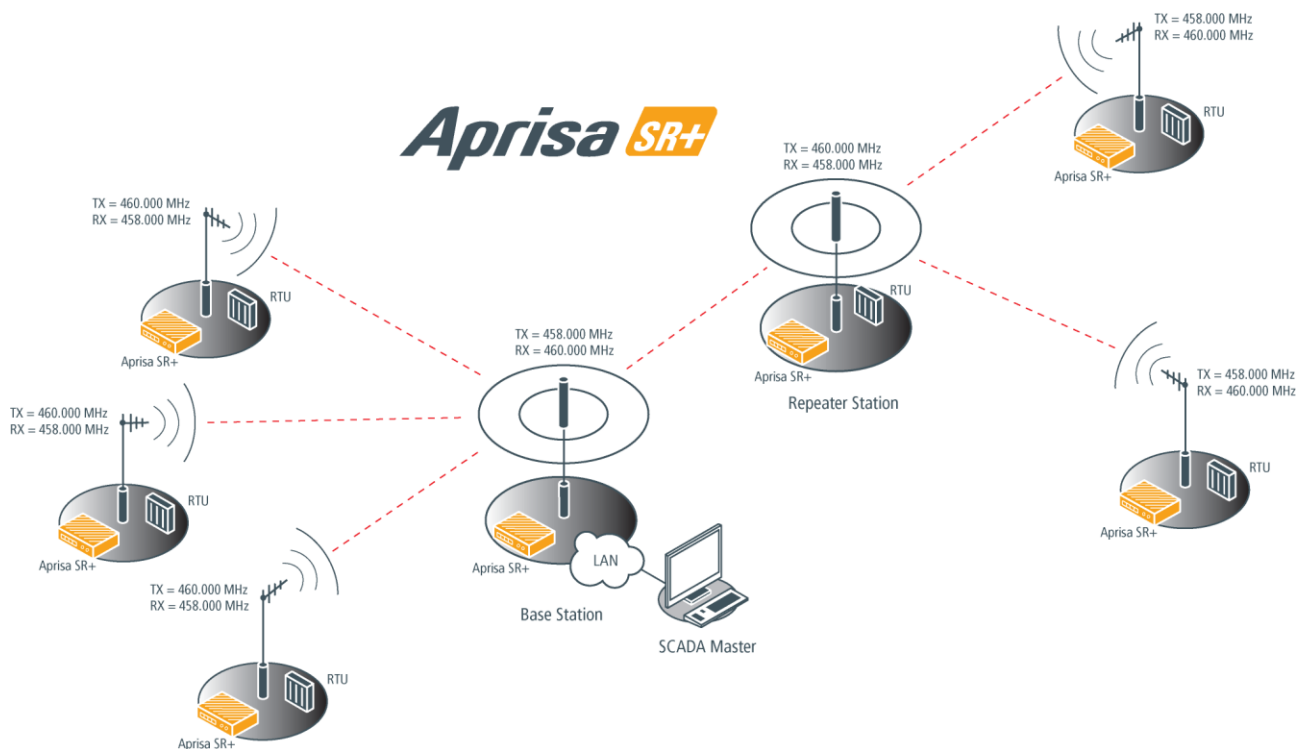
The TX frequency of the repeater station associated with the base station matches the RX frequency of the base station.

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

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

TX Power

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

The default setting is +37 dBm.

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

The Peak Envelope Power (PEP) is calculated based on current configured TX power settings and modulation:

- QPSK PEP = TX Power Setting + 3 dBm
- 16 QAM PEP = TX Power Setting + 5 dBm
- 64 QAM PEP = TX Power Setting + 6 dBm
- 256 QAM PEP = TX Power Setting + 7 dBm

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

MODEM

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

Modem Mode

This parameter sets the Modem Mode in the radio. The Modem Mode option list is dependent on the radio hardware frequency band variant (see 'Terminal > Details' on page 106).

HW Variant	Option	Channel Size kHz	Symbol Rate ksps
135 MHz	Mode A (FCC / ISSED)	50	36
		30	16
		15	9
	Mode B (ETSI / ACMA)	50	36
		25	20
		12.5	10
	Mode C	50	36
		25	20
		12.5	8
220 MHz	Mode A (FCC / ISSED)	50	36
		25	16
		15	10
		12.5	9
320 MHz	Mode A (ETSI / ACMA)	50	36
		25	20
		20	14
		12.5	10
400 MHz	Mode A (ETSI / ACMA)	50	36
		25	20
		20	14
		12.5	10
	Mode B (FCC / ISSED)	50	36
		25	16
		12.5	9
	Mode C	50	36
		25	20
		12.5	8
450 MHz	Mode A (ETSI / ACMA)	50	36
		25	20
		12.5	10
	Mode B (FCC)	50	36
		25	16
		12.5	9
700 MHz	Mode A (FCC Part 27)	100	72
		50	40
		25	20
		12.5	10

HW Variant	Option	Channel Size kHz	Symbol Rate ksps
896 MHz	Mode A (FCC / ISSED)	100	72
		50	36
		25	16
		12.5	10
	Mode B (FCC Part 24)	100	72
		50	36
		25	16
		12.5	8
	Mode C (ISSED RSS-134)	100	72
		50	36
		25	16
		12.5	8
928 MHz	Mode A (FCC)	100	72
		50	36
		25	16
		12.5	8
	Mode B (ISSED)	100	72
		50	36
		25	16
		12.5	8
	Mode C (FCC Part 24)	100	72
		50	36
		25	16
		12.5	9
	Mode D (ISSED RSS-134)	100	72
		50	36
		25	16
		12.5	10

Enhanced Noise Rejection Mode

All radios in an Aprisa SR+ network must use the same setting.

Option	Function
Disable	This feature is disabled.
Noise Rejection	Improves co-channel interference performance at strong receiver signal levels.
Channel Reuse & Noise Rejection	Packets with RSSI lower than that of the registered network will be discarded during frame sync.

The default setting is Disabled.

Modulation Type

This parameter sets the TX Modulation Type for the radio.

Option	Function
Adaptive	Sets the transmit modulation to Adaptive Coding Modulation (ACM).
QPSK (High Gain)	Sets the modulation to QPSK with Max Coded FEC.
QPSK (Low Gain)	Sets the modulation to QPSK with Min Coded FEC.
QPSK	Sets the modulation to QPSK with no FEC.
16QAM (High Gain)	Sets the modulation to 16 QAM with Max Coded FEC.
16QAM (Low Gain)	Sets the modulation to 16 QAM with Min Coded FEC.
16QAM	Sets the modulation to 16 QAM with no FEC.
64QAM (High Gain)	Sets the modulation to 64 QAM with Max Coded FEC.
64QAM (Low Gain)	Sets the modulation to 64 QAM with Min Coded FEC.
64QAM	Sets the modulation to 64 QAM with no FEC.
256QAM (Low Gain)	Sets the modulation to 256 QAM with Min Coded FEC.

The default setting is Adaptive.

When the Modulation Type is set to Adaptive, the transmitted modulation and coding will be determined by the signal quality of the link to the destination radio. Link quality for each radio is determined both concurrently and independently.

The link quality used for each packet depends on the destination;

- Remote to base, remote to repeater and repeater to base uses the quality of that link only
- Unicast base to remote and base to repeater packets use the quality of that link only
- Unicast repeater to remote packets use the lowest of either the repeater-remote link or the repeater-base link
- Broadcast base to remote, base to repeater and repeater to remote packets (serial or broadcast IP or multicast IP) use the slowest link quality of all destinations

Adaptive Modulation is available in all Terminal Operating Modes and all Channel Access Schemes except Listen Before Send.

ACM Control

This parameter enables / disables Adaptive Coding Modulation in the receive direction.

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

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

The default setting is Fast.

ADAPTIVE CODING MODULATION

Default Modulation

This parameter is used when the Modulation Type is set to Adaptive, but the far end of the link has ACM Control set to 'Disabled'.

The default setting is QPSK (Low Gain).

Option	Function
QPSK (High Gain)	Sets the modulation to QPSK with Max Coded FEC.
QPSK (Low Gain)	Sets the modulation to QPSK with Min Coded FEC.
QPSK	Sets the modulation to QPSK with no FEC.
16QAM (High Gain)	Sets the modulation to 16 QAM with Max Coded FEC.
16QAM (Low Gain)	Sets the modulation to 16 QAM with Min Coded FEC.
16QAM	Sets the modulation to 16 QAM with no FEC.
64QAM (High Gain)	Sets the modulation to 64 QAM with Max Coded FEC.
64QAM (Low Gain)	Sets the modulation to 64 QAM with Min Coded FEC.
64QAM	Sets the modulation to 64 QAM with no FEC.
256QAM (Low Gain)	Sets the modulation to 256 QAM with Min Coded FEC.

GENERAL

Channel Size (kHz)

This parameter sets the Channel Size for the radio (see ‘Channel Sizes’ on page 468 for Radio Capacities). The default setting is 12.5 kHz.

Antenna Port Configuration

This parameter sets the Antenna Port Configuration for the radio.

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

The default setting is Single Antenna Single Port.

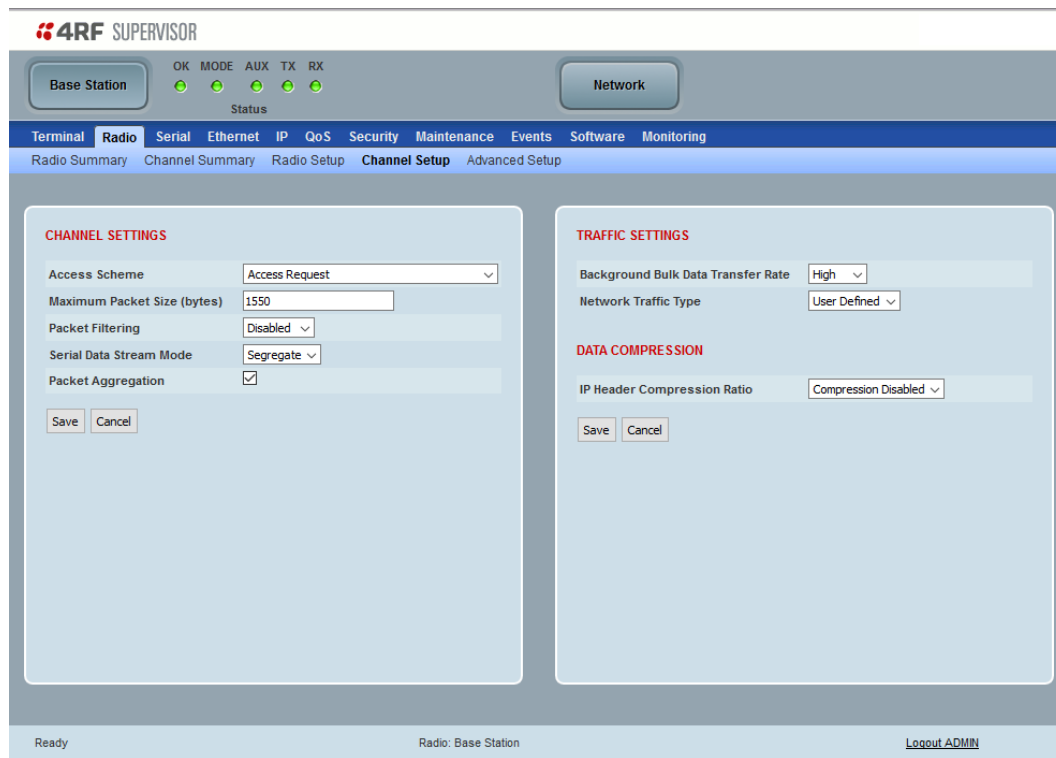
RX Path Attenuation (dB)

This parameter sets the receiver front end variable attenuator. The attenuator can be set from 0 to 30.5 dB in 0.5 dB steps. This attenuator can be used to protect the receiver from strong out of band interference.

The default setting is 0 dB.

This feature is only available on 700 MHz radios.

Radio > Channel Setup



CHANNEL SETTINGS

Access Scheme

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

Option	Function
Access Request	Channel access scheme where the base station controls the communication on the channel. Remotes ask for access to the channel, and the base station grants access if the channel is not occupied. This mode is a general purpose access method for high and low load networks.
Access Request (full duplex)	Used on a network with full duplex base or repeater station hardware and half duplex remotes. A full duplex version of Access Request channel access scheme where the base station controls the communication on the channel. Remotes ask for access to the channel, and the base station grants access if the channel is not occupied. If no repeaters are present, this allows the base station to send traffic during remote transmission and when used in a repeater network, this allows repeaters to forward traffic while it is being received.
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 optimized 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 optimized for low load networks and repeated networks. With Acknowledgement, unicast requests from the remote radio are acknowledged by the base station to ensure that the transmission has been successful. If the remote radio does not receive an acknowledgement, then random back-offs are used to reschedule the next transmission. Enabling acknowledgments increases reliability of transport but reduces available channel capacity so if application has the capability to handle lost or duplicate messages, the Access Scheme should be set to Listen Before Send without Acknowledgement.
Point To Point (Half Duplex)	Channel access scheme for Point-to-point links using half duplex radios. This is the preferred access scheme for mirrored bits ®.

The default setting is Access Request.

Maximum Packet Size (Bytes)

This parameter sets the maximum over-the-air packet size in bytes. A smaller maximum Packet Size is beneficial when many remote radios or repeater stations are trying to access the channel, and smaller high priority packets must not be delayed by larger low priority packets sent by other radios.

This benefit comes at the cost of preventing some packet aggregation from occurring and / or reduced overall throughput.

The default setting is 1570 bytes.

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

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

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

Packet Filtering

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

Normally all packets sent by remotes and repeaters are only received at the base station. Setting packet filtering to disabled can provide the ability for remote radios to communicate with each other (peer to peer communication) when connected to a repeater station, particularly useful in the event of losing communication with a SCADA Master, assuming the Aprisa SR+ network is still operational.

In a network without repeaters, this setting only affects packets from base to remote (causing IP packets for devices at one remote to be sent out ethernet ports of all remotes with packet filtering disabled).

When repeaters exist in the network, setting this to disabled on both the repeater and its immediately connected remotes allows devices connected to those remotes to communicate with each other and with the repeater.

With base-repeater mode, this setting is not usually required as the base station changes the destination from itself to broadcast when it retransmits a packet. However, if base-repeater is used in conjunction with repeaters, then it can still be useful to disable packet filtering to reduce message latency between distant remotes.

Note: For correct PTP link operation, the Packet Filtering parameter should not be changed from the default setting of 'automatic'.

Note: Packet filtering will remain enabled for IP packets regardless of this setting unless IP Header Compression is disabled (see 'IP Header Compression Ratio' on page 146).

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

The default setting is Automatic.

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

Serial Data Stream Mode

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

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

The default setting is Broadcast.

Segregated Port Directions

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

2E2S Port Number		2E2S Port Number
1	↔	1
2	↔	2
USB	↔	USB

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

2E2S Port Number		3E1S Port Number
1	↔	1
2	→ X	NA
USB	↔	USB

Packet Aggregation

This parameter when active enhances OTA performance by increasing throughput and reducing latency at all modulations. This feature can only be enabled when the Network Radius=1 PMP networks (i.e. network without repeaters) for both half duplex and full duplex base station modes.

Packets will be aggregated as long as the combined size is less than the Maximum Packet Size setting, and the destination radios are all receiving packets at the same modulation.

The default setting is enabled.

TRAFFIC SETTINGS

Background Bulk Data Transfer Rate

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

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

The default setting is high.

Network Traffic Type

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

Option	Function
User Defined	Allows the user to define the channel settings (see ‘Radio > Advanced Setup’ on page 147). INFORMATION For “User Defined” network traffic type, more parameters are available for configuration in the Advanced Setup menu. OK
Serial Only	Optimizes the channel settings for the predominantly serial traffic.
Ethernet Only	Optimizes the channel settings for the predominantly Ethernet traffic.
Mixed	Optimizes the channel settings for a mix of Ethernet and serial traffic.

The default setting is Mixed.

DATA COMPRESSION

IP Header Compression Ratio

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

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

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

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

The default setting is High.

Radio > Advanced Setup

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

ADVANCED CHANNEL SETTINGS

Default Packet Time to Live (ms)

This parameter sets the time a default packet is allowed to live in the system before being dropped if it cannot be transmitted over the air. This applies to packets that are neither Serial nor Ethernet such as registration, inter-unit messaging, firmware distribution etc. The default setting is 1500 ms. The default parameter should work for most situations.

Serial Packet Time to Live (ms)

This parameter sets the time a serial packet is allowed to live in the system before being dropped if it cannot be transmitted over the air. The default setting is 2500 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'.

Ethernet Packet Time to Live (ms)

This parameter sets the time an Ethernet packet is allowed to live in the system before being dropped if it cannot be transmitted over the air. The default setting is 2500 ms.

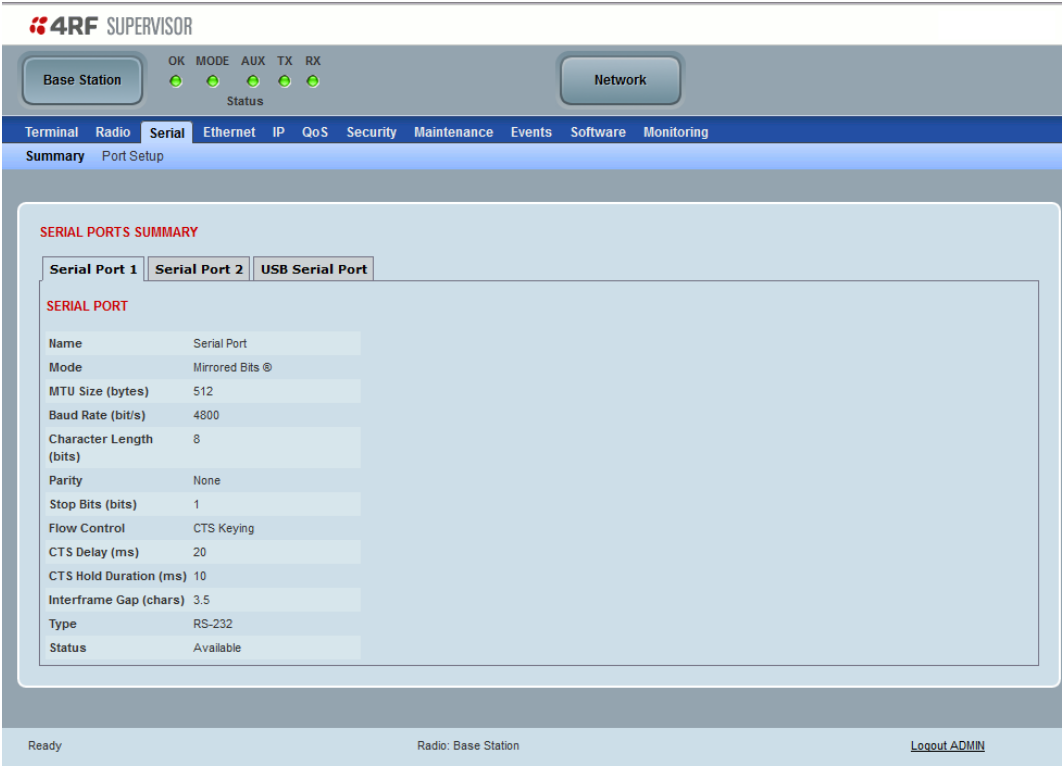
Serial

Serial > Summary

RS-232 Hardware Ports

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

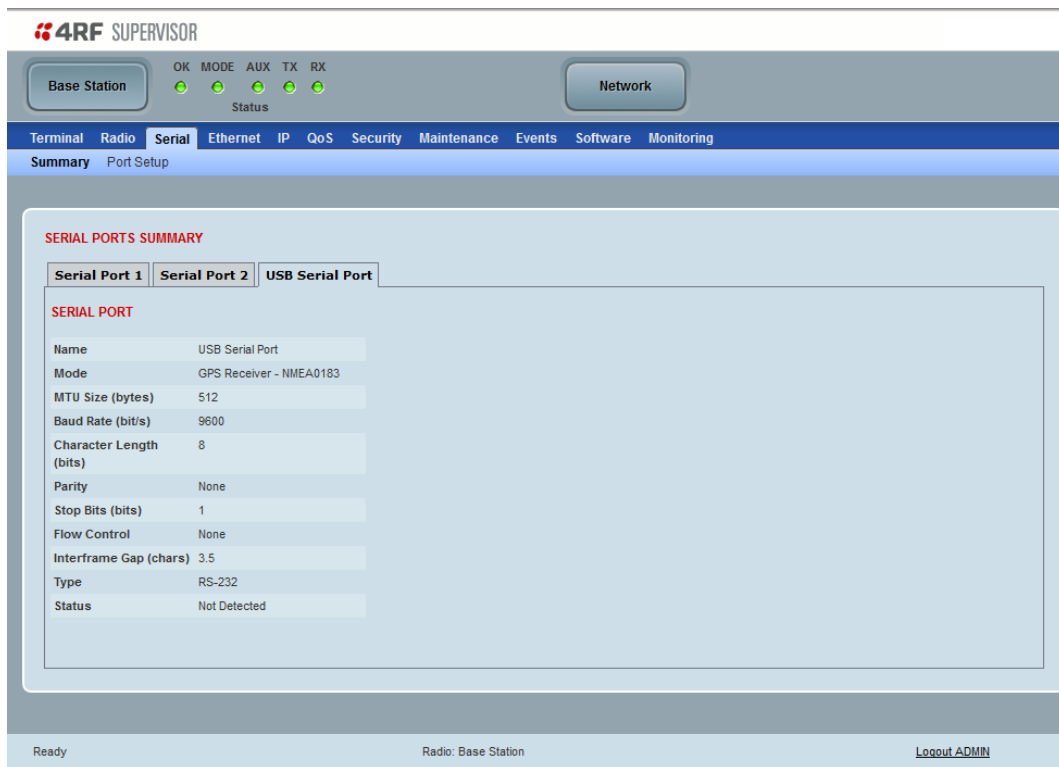
Note: This screen is dependent on the Data Port product option purchased (see ‘Data Interface Ports’ on page 404). The Data Port product option shown is a 2E2S - two Ethernet ports and two Serial ports



See ‘Serial > Port Setup’ on page 150 for configuration options.

USB Serial Ports

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



Type

This parameter displays the Serial Port interface type.

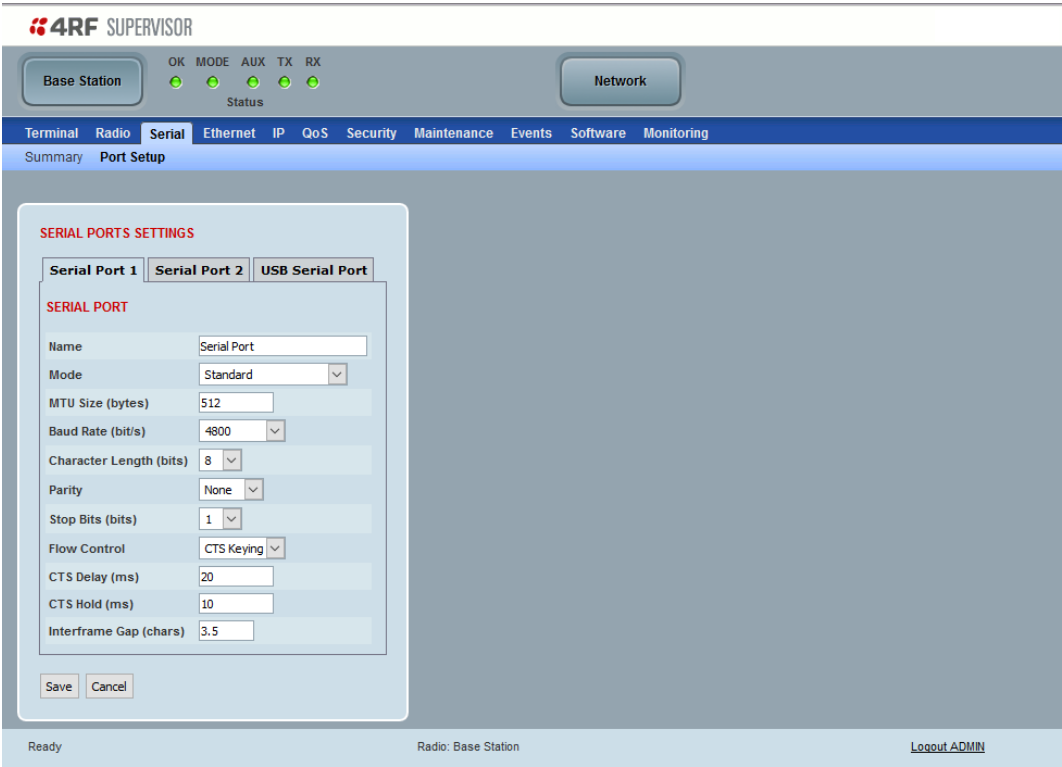
If the Name is USB Serial Port:

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

Serial > Port Setup

RS-232 Hardware Ports

This page provides the setup for the serial port settings.



SERIAL PORTS SETTINGS

Note: This screen is dependent on the Data Port product option purchased (see ‘Data Interface Ports’ on page 404). The Data Port product option shown is a 2E2S - two Ethernet ports and two Serial ports

Name

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

Option	Function
Serial Port	This is the normal RS-232 serial ports provided with the RJ45 connector.
USB Serial Port	This is the optional RS-232 / RS-485 serial port provided with the USB host port connector with a USB to RS-232 / RS-485 RJ45 converter cable (see ‘USB RS-232 / RS-485 Serial Port’ on page 438).

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.
Standard (Streaming)	This mode when used with a small MTU setting provides reduced latency without introducing gaps in the serial stream by taking exclusive control of the radio channel.
Bit Oriented	This mode allows support for legacy protocols that are not compatible with standard UARTs (see 'Bit Oriented' on page 153).
Bit Oriented (Streaming)	This mode allows support for legacy protocols that are not compatible with standard UARTs (see 'Bit Oriented' on page 153). It includes Streaming which when used with a small MTU setting provides reduced latency without introducing gaps in the serial stream by taking exclusive control of the radio channel.
Mirrored Bits ®	Mirrored Bits® is a serial communications protocol used to exchange internal logic status messages directly between relays and devices used in line protection, remote control and monitoring, relay remote tripping, sectionalizing and other such applications. The protocol is often described as a relay-to-relay communications technology.
Terminal Server	A base station Ethernet port can communicate with both Ethernet ports and serial ports on remote radios. RS-232 traffic is encapsulated in IP packets (see 'Serial > Port Setup' Terminal Server on page 159).
SLIP	IP packets are encapsulated over RS-232 interface port (see 'Serial > Port Setup' Serial Line Interface Protocol (SLIP)' on page 162).

MTU Size (bytes)

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

Baud Rate (bit/s)

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

Character Length (bits)

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

Parity

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

Stop Bits (bits)

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

Flow Control

This parameter sets the flow control of the serial port. The default setting is None.

Option	Function
None	The Aprisa SR+ radio port (DCE) CTS is in a permanent ON (+ve) state. If radio enters sleep state, then CTS goes OFF.
CTS-RTS	CTS / RTS hardware flow control between the DTE and the Aprisa SR+ radio port (DCE) is enabled. The CTS state follows the RTS state. If the Aprisa SR+ buffer is full or the Aprisa SR+ is in sleep state, the CTS goes OFF.
CTS-Keying	CTS Keying is needed when working with devices that require to be keyed before sending data; - Driving legacy modems that use the CTS signal as a key-up signal. - Driving RS485 serial links, where the CTS signal is used as a Tx enable - Used to enable interfacing between SR+ running bit-oriented protocol with an OSI MEU device. The CTS signal is wired to the OSI MEU CD input in this case, as the MEU uses the CD as a receiver enable signal in bit-oriented mode.

CTS Delay ms

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

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

CTS Hold Duration ms

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

Inter-Frame Gap (chars)

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

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

The Inter-Frame Gap limits are 0 to 9999 chars in steps of 0.1 char. The default setting is 3.5 chars.

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

Bit Oriented

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

This mode allows support for legacy protocols that are not compatible with standard UARTs. Examples are VANCOMM, REDAC, CONITEL, and CDC, although others will work as well.

Bit Oriented (Streaming) may be used to reduce latency of BOP. If this mode is selected, an MTU value of 8 is recommended. When streaming mode is used, other traffic is blocked during a BOP packet, so this mode is only recommended when the radio network is used exclusively for BOP traffic.

The limitations of this mode are:

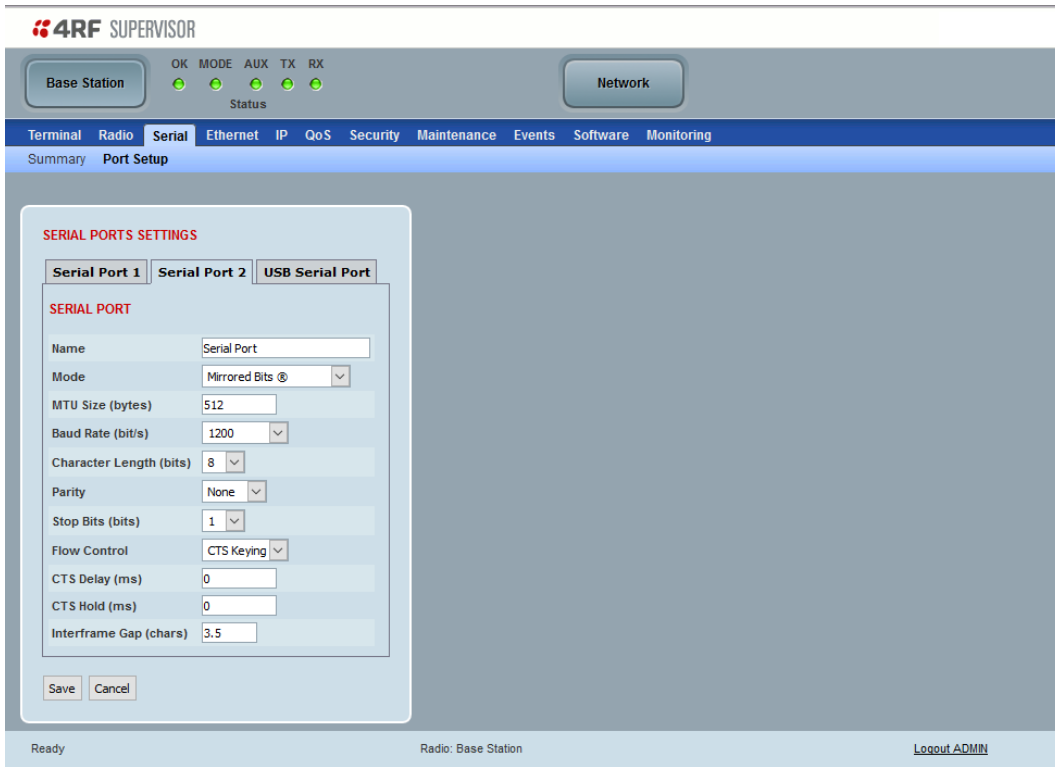
- The MTU must be configured larger than the inter-frame gap.
- The maximum baud rate is 4800 bit/s.
- The inter-frame gap must be configured to the length of a packet in the protocol being used. Tested values known to work are:

Protocol	Inter-Frame Gap
VANCOMM	14
REDAC	4
CONITEL	4
CDC TYPE I (at base station)	4
CDC TYPE I (at remote radio)	31

- Only supported on one serial port at a time.
- Not supported on a USB serial port.
- CTS-RTS Flow Control is not supported. The RTS input (RJ45 Pin 1) to Aprisa SR+ must be tied to the TX input (RJ45 Pin 3).
- CTS Keying can be used to enable interfacing between SR+ running bit-oriented protocol with an OSI MEU device. The CTS signal is wired to the OSI MEU CD input in this case, as the MEU uses the CD as a receiver enable signal in bit-oriented mode.

Mirrored Bits®

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



The screenshot shows the 4RF SUPERVISOR web interface. At the top, there are status indicators for Base Station, OK, MODE, AUX, TX, and RX. Below this is a navigation bar with tabs for Terminal, Radio, Serial, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring. The 'Serial' tab is selected, and the 'Port Setup' sub-tab is active. The main content area displays the 'SERIAL PORTS SETTINGS' for 'Serial Port 1'. The settings include:

- Name: Serial Port
- Mode: Mirrored Bits® (selected)
- MTU Size (bytes): 512
- Baud Rate (bit/s): 1200
- Character Length (bits): 8
- Parity: None
- Stop Bits (bits): 1
- Flow Control: CTS Keying
- CTS Delay (ms): 0
- CTS Hold (ms): 0
- Interframe Gap (chars): 3.5

At the bottom of the settings panel are 'Save' and 'Cancel' buttons. The footer of the interface shows 'Ready', 'Radio: Base Station', and a 'Logout ADMIN' link.

Introduction

Mirrored Bits® is a serial communications protocol used to exchange internal logic status messages directly between relays and devices used in line protection, remote control and monitoring, relay remote tripping, sectionalizing and other such applications.

The protocol relies on near constant transmission of status bytes between the devices. It can only tolerate small delays between receipts of packets.

The protocol provides alarms states to monitor and report on radio channel performance. If a receiving device does not receive a status packet within a predefined time then it asserts an 'instantaneous channel monitor' error (ROK), this error clears as soon as the next status packet is received.

There are two more significant errors RBAD (ROK dropout for settable time) and CBAD (long term channel unavailability exceeding a settable threshold) that will be asserted if more extensive delays occur or the communications channel is lost.

The trigger or time period for asserting ROK varies between devices. Typically the ROK error state is asserted if a receiving device does not receive a packet for a period > than 3 x the period taken to transmit a packet.

When optimizing for Mirrored Bits® operation the target is to present a radio channel that does not result in ROK triggers occurring. Individual networks may be tolerant to occasional ROK alarms states if configured to make use of the more significant alarms

Optimization

Typically Full Duplex radio communications are required however Aprisa SR+ has been optimized to support Mirrored Bits® in a narrow channel licensed Half Duplex radio channel.

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

Under some scenarios limited Ethernet transport may be supported without impacting Mirrored Bits® operation. If the network can tolerate occasional ROK errors Ethernet support may be increased. The level of impact on Mirrored Bits® is related to radio settings and the specifics of the Ethernet traffic including size and frequency of the Ethernet packets.

When attempting to configure the radios to support new devices or varying network requirements a standard configuration is used for the radios and the following two key serial data parameters are adjusted:

- Inter-Frame Gap (IFG) - used to detect new packets on the serial input to the radio
- Maximum Transmission Unit (MTU) - used to define the over the air (OTA) packet size

To date, 4RF has lab tested and confirmed operation with the follow SEL Mirrored Bits® devices. Contact 4RF for preferred configuration:

- 2411 PAC (Programmable Automation Controller)
- 2505 series remote I/O modules
- 321 series relays

4RF is working with customers to confirm support for other devices as they are identified. The remainder of this document details the configuration settings and general process to optimize the radio to support additional devices, in addition to listing expected latencies under different configurations.

General Configuration

The configurations and process are aligned with a 2505 series remote I/O module device with serial baud rate of 9600. As a 'fast' Mirrored Bits® device it is considered a good start point for optimization. For other baud rates please refer to the table in Initial Setup for Mirrored Bits® Support on page 157 for initial MTU and IFG settings.

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

Recommended RF configurations are:

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

Serial data port variable parameters

Two key serial port parameters will be adjusted during optimization. The following initial values have been determined as a suitable for the SEL 2505 device which is the fastest device 4RF has lab tested. It is a suitable start point to carry out optimization for other devices.

Inter-Frame Gap - initially set to 0.2

- IFG is dependent on serial line baud rate only
- The Mirrored Bits® protocol is essentially timed to a base clock, the slower the baud rate the longer the period to transmit a packet resulting in less time between packets
- A low baud rate is ideal as it increase the time period before a ROK error will occur as this is dependent on serial packet transmission time
- The minimum baud rate currently proven to provide reliable communications is 9600 bit, with this rate an IFG of 0.2 is required to be used
- With the 2505 device the IFG increases with increases in serial baud rate, while easier to detect gaps the ROK error period is reduced

MTU - initially set to 32 bytes

- Dependent on serial line baud rate, channel size, modulation, security settings, intended traffic mix and all other settings that influence OTA speed and capacity available for external traffic
- MTU affects latency, if a large MTU then the radio will 'wait' for the number of bytes before sending the packet OTA
- Ideally a low MTU will be used - the minimum needs to support the various settings above and intended mix of traffic
- MTU can be changed in steps of +/- 8 when trying different configurations
- Refer table in section 5 for start point of MTU based on channel size, modulation and serial baud rate, this assumes the general radio settings as above
- Increase by 8 for new devices or in attempt to support some Ethernet or other services

Initial Setup for Mirrored Bits® Support

The MTU can be adjusted up or down in steps of 8 bytes

- Increase by 8 bytes if Mirrored Bits® is not running without alarms or ROK assertions
- Decrease by 8 bytes if Mirrored Bits® is running error free, the target is to find the smallest MTU for reliable transport

If reliable Mirrored Bits® communications cannot be achieved after increasing the MTU by 10 steps or 80 bytes, then the following CLI commands can be used to extract low level packet information from the radio.

This information can be forwarded to 4RF to determine what is occurring and identify alternate configurations.

- Configure Radio / Mirrored Bits® equipment for 9600 baud rate
- Connect Mirrored Bits® equipment to one of the serial ports and start traffic
- Ensure no management traffic or other services are connected to the Ethernet or Serial ports
- Login to the radio CLI as 'admin' and execute 'debug set 2 5' -> there will be continuous scrolling information
- Screen capture one page of the scrolling information to send to 4RF
- Remove serial cable and execute 'debug clear 2 5' via the CLI to clear the debug routine, alternatively reboot the radio
- Note if the serial baud rate intended to be used is not 9600 then repeat for each different rate and clearly identify the screen prints by baud rate before forwarding to 4RF

Note there are additional low level configurations which can improve performance. 4RF will detail these if required based on the information received.

Additional Setup for Improved Latency or Additional Services

Once reliable Mirrored Bits® communications has been achieved, experimentation can be undertaken to reduce latencies or provide support for additional services such as Ethernet based SCADA polling.

Increasing the MTU will impact latency for each packet (refer to table in section 4). A point may be reached where the gaps between individual packets are too high and the Mirrored Bits® ROK or other alarms will assert.

Increasing the MTU allows some 'space' in each packet for additional data from the second serial port or the Ethernet ports.

Support for Ethernet is highly dependent on the size and frequency of packets being sent. A level of trial and error is required. At the very narrow channel sizes and OTA data rates support may be limited however with wider channels and higher OTA data rates some services may be supported (such as polling).

It should be noted that if the Mirrored Bits® devices or network manager can accept occasional ROK assertions then there is more flexibility for other services.

Baud rate and Latency Table

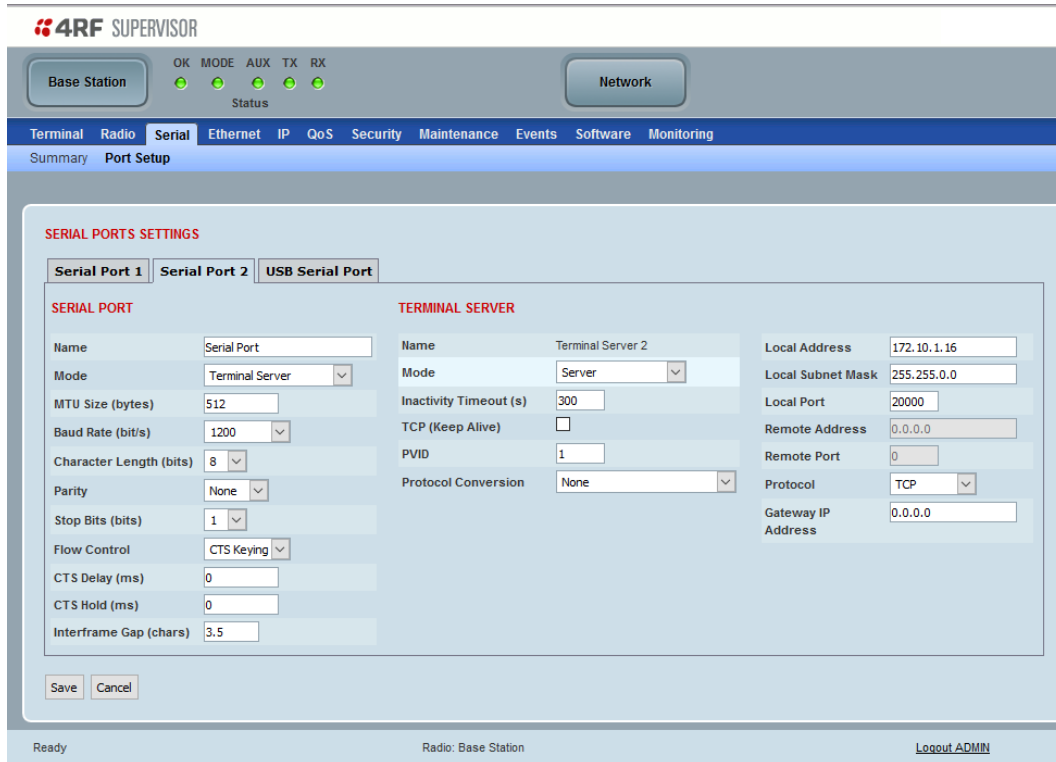
The following table is arranged by serial baud rate followed by Aprisa SR+ channel size and modulation. It lists the optimized MTU and IFG and resulting latency for the SEL 2505 device, one of the faster devices available so serves as an ideal starting point when introducing new devices. It is recommended that initial testing is carried out with one step size higher (8) on MTU.

Serial Baud Rate	Modulation	Channel Size	Minimum MTU Size	IFG SEL 2505	One Way Latency (ms)
9600	64 QAM Low	50	8	0.2	20.0
9600	16 QAM Low	50	16	0.2	-
9600	QPSK	50	16	0.2	-
9600	QPSK Low	50	24	0.2	42.5
9600	64 QAM Low	25	16	0.2	40.0
9600	16 QAM Low	25	24	0.2	-
9600	QPSK	25	24	0.2	-
9600	QPSK Low	25	32	0.2	62.5
9600	64 QAM Low	12.5	24	0.2	60.0
9600	16 QAM Low	12.5	40	0.2	-
9600	QPSK	12.5	40	0.2	-
9600	QPSK Low	12.5	64	0.2	125.0
19200	64 QAM Low	50	16	0.5	25.0
19200	16 QAM Low	50	24	0.5	-
19200	QPSK	50	24	0.5	-
19200	QPSK Low	50	24	0.5	-
19200	64 QAM Low	25	32	0.5	50.0
19200	16 QAM Low	25	48	0.5	-
19200	QPSK	25	56	0.5	-
19200	QPSK Low	25	56	0.5	-
19200	64 QAM Low	12.5	56	0.5	85.0
19200	16 QAM Low	12.5	88	0.5	-
19200	QPSK	12.5	not supported	0.5	-
19200	QPSK Low	12.5	not supported	0.5	-
38400	64 QAM Low	50	24	3	40.0
38400	16 QAM Low	50	24	3	-
38400	QPSK	50	32	3	-
38400	QPSK Low	50	40	3	62.5
38400	64 QAM Low	25	40	3	62.5
38400	16 QAM Low	25	72	3	-
38400	QPSK	25	76	3	-
38400	QPSK Low	25	not supported	3	-
38400	64 QAM Low	12.5	82	3	112.5
38400	16 QAM Low	12.5	not supported	3	-
38400	QPSK	12.5	not supported	3	-
38400	QPSK Low	12.5	not supported	3	-

Terminal Server

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

The Terminal Server operating mode provides encapsulation of serial data from a local serial port into an IP packet (over TCP or UDP). This function is typically used for connecting a legacy serial RTU at a remote radio to an Ethernet SCADA server.



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 address when data is presented on the serial port.
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. Generally, this setting is used for the remote radio but it should be used carefully as two connections might be established to the remote address. Data received from any client shall be forwarded to the associated serial port while data received from that serial port shall be forwarded to every client with an open TCP connection.

Inactivity Timeout (seconds)

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

TCP Keep Alive

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

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

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

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

PVID

This parameter sets the PVID (port VLAN ID) for each of the terminal servers on the radio.

Protocol Conversion

This parameter defines the mode of operation of the terminal server connection. The default setting is None.

Option	Function
None	No terminal server Protocol Conversion
Modbus TCP to Modbus RTU	The radio provides a gateway between Modbus TCP to Modbus RTU.
Modbus TCP to Modbus ASCII	The radio provides a gateway between Modbus TCP to Modbus ASCII.

Local Address

This parameter sets the serial Terminal Server local IP address.

Bridge Mode

The local IP address can be the same as the radio's configured IP address or the Virtual IP address for protected stations. If it is not the above, then it must be an IP address from a network different from the radio's network.

Note that the Terminal Server local IP address settings can be the same for other terminal servers in the radio.

Router Mode

The local IP address must be the same as port 1 (management IP address) of the radio's configured port IP addresses or the Virtual IP address for protected stations.

Gateway Router Mode

The local IP address must be the same as the radio's configured IP address or the Virtual IP address for protected stations.

Local Port

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

The valid port number range is less than or equal to 49151 but with exclusions of 0, 20, 21, 23, 80, 161, 162, 443, 5445, 6445, 9930 or 9931. The default setting is 20000.

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

Remote Address

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

Remote Port

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

Protocol

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

Gateway IP Address

This Terminal Server parameter sets the Gateway IP address of a router in the network that serves as the forwarding router to other networks when no other route specification matches the destination IP address of a packet.

This is useful when default gateway IP address of the radio and the Terminal Server Gateway IP Address are on different IP subnet networks.

When all radios are in router mode (GRM / RM) or advanced router mode (AGRM / ARM), the default gateway IP address of the radio and Gateway IP Address of the Terminal Server are the same, leaving the Gateway IP Address on the default value of 0.0.0.0 will serve the purpose. Only when the radio and Terminal Server are with different IP subnets and are connected to different router gateway IP addresses, the default value shall be set to the appropriate gateway IP address.

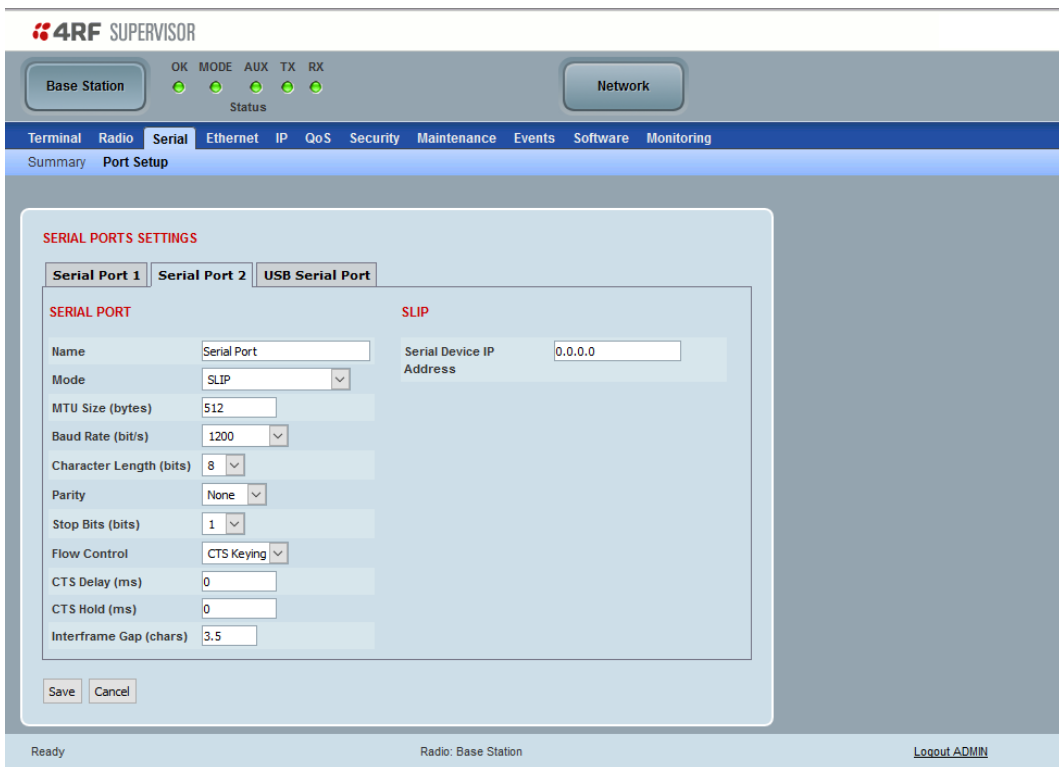
Serial Line Interface Protocol (SLIP)

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

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

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

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



The screenshot shows the 4RF SUPERVISOR web interface. At the top, there's a status bar with 'Base Station' and 'Network' buttons, and a row of status indicators (OK, MODE, AUX, TX, RX). Below this is a navigation menu with tabs: Terminal, Radio, Serial (selected), Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring. Under the 'Serial' tab, there's a sub-menu with 'Summary' and 'Port Setup' (selected). The main content area is titled 'SERIAL PORTS SETTINGS' and has three sub-tabs: 'Serial Port 1' (selected), 'Serial Port 2', and 'USB Serial Port'. The 'Serial Port 1' tab is divided into two sections: 'SERIAL PORT' and 'SLIP'. The 'SERIAL PORT' section contains fields for Name (Serial Port), Mode (SLIP), MTU Size (bytes) (512), Baud Rate (bit/s) (1200), Character Length (bits) (8), Parity (None), Stop Bits (bits) (1), Flow Control (CTS Keying), CTS Delay (ms) (0), CTS Hold (ms) (0), and Interframe Gap (chars) (3.5). The 'SLIP' section contains a field for Serial Device IP Address (0.0.0.0). At the bottom of the form are 'Save' and 'Cancel' buttons. The footer of the interface shows 'Ready', 'Radio: Base Station', and a 'Logout ADMIN' link.

Serial Device IP Address

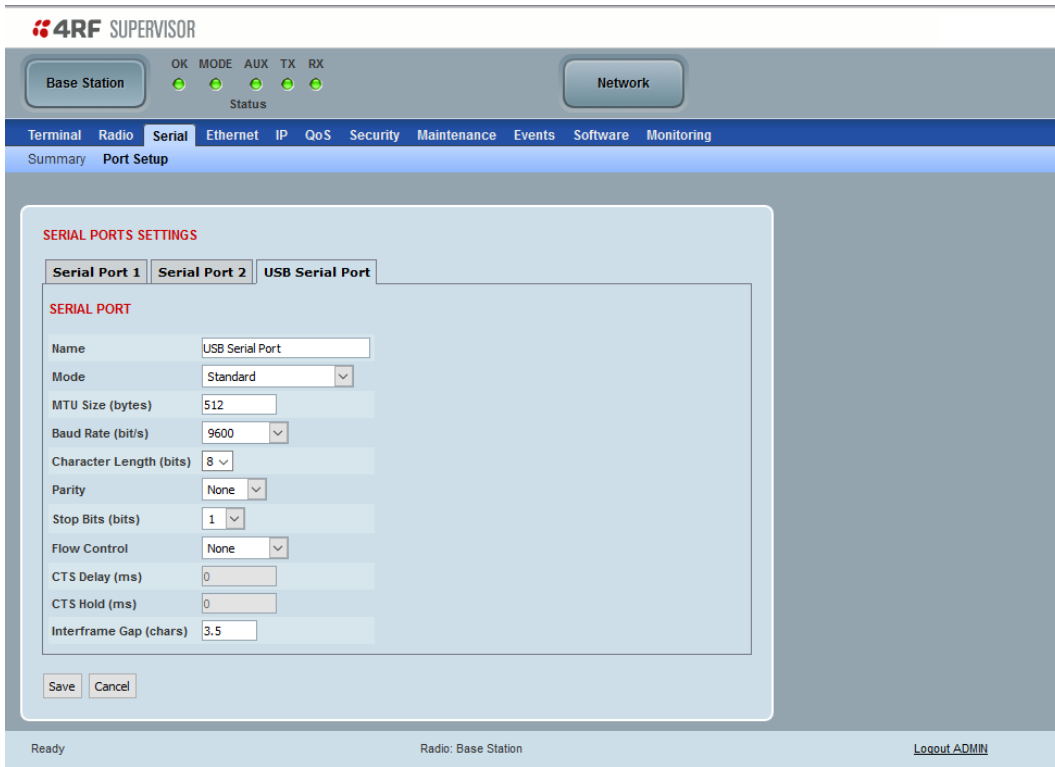
This parameter sets the IP address of the RTU connected on the configured serial port.

Baud Rate (bit/s)

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

USB Serial Ports

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



SERIAL PORTS SETTINGS

Mode

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

Option	Function
Disabled	The serial port is not required.
Standard	The serial port is communicating with serial ports on other stations.
Standard (Streaming)	This mode when used with a small MTU setting provides reduced latency without introducing gaps in the serial stream by taking exclusive control of the radio channel.
Terminal Server	A base station Ethernet port can communicate with both Ethernet ports and serial ports on remote radios. RS-232 traffic is encapsulated in IP packets (see 'Serial > Port Setup' Terminal Server on page 159).
CLI Management	The USB host port can be used to access the radio Command Line Interface (CLI). A USB converter to RS-232 convertor will be required to connect to a PC.
GPS Receiver - NMEA0183	Set if a GPS receiver device is plugged into the radio USB port (see 'GPS Receiver' on page 166).

MTU Size (bytes)

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

Baud Rate (bit/s)

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

Character Length (bits)

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

Parity

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

Stop Bits (bits)

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

Flow Control

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

Option	Function
None	The Aprisa SR+ radio port (DCE) CTS is in a permanent ON (+ve) state.
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, otherwise CTS is ON.
CTS-Keying	CTS Keying is needed when working with devices that require to be keyed before sending data; - Driving legacy modems that use the CTS signal as a key-up signal. - Driving RS485 serial links, where the CTS signal is used as a Tx enable - Used to enable interfacing between SR+ running bit-oriented protocol with an OSI MEU device. The CTS signal is wired to the OSI MEU CD input in this case, as the MEU uses the CD as a receiver enable signal in bit-oriented mode.

CTS Delay ms

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

CTS Hold Duration ms

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

Inter-Frame Gap (chars)

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

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

The Inter-Frame Gap limits are 0 to 9999 chars in steps of 0.1 char. The default setting is 3.5 chars.

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

GPS Receiver

This menu item is only applicable if a GPS Receiver device is plugged into the radio USB port.

The radio USB port supports NMEA 0183 - a combined electrical and data specification for communication between electronics systems and GPS receivers.

The currently supported GNSS Receiver devices are;

Part Number	Part Description
APSB-GREC-T01-UA	GNSS receiver and mushroom antenna Working mode GPS, GLONASS dual-mode Protocols NMEA,0183 Binary Waterproof grade: IPX67 Connector USB A Cable length 15 metres Antenna dimensions H=150mm, DIA=100mm

MTU Size (bytes)

This parameter is not required for GPS Receiver device.

Baud Rate (bit/s)

Set to 4800 bit/s for both supported GPS Receiver devices above.

Character Length (bits)

Set to 8 bits.

Parity

Set to None.

Stop Bits (bits)

Set to 1 bit.

Flow Control

Set to Disabled.

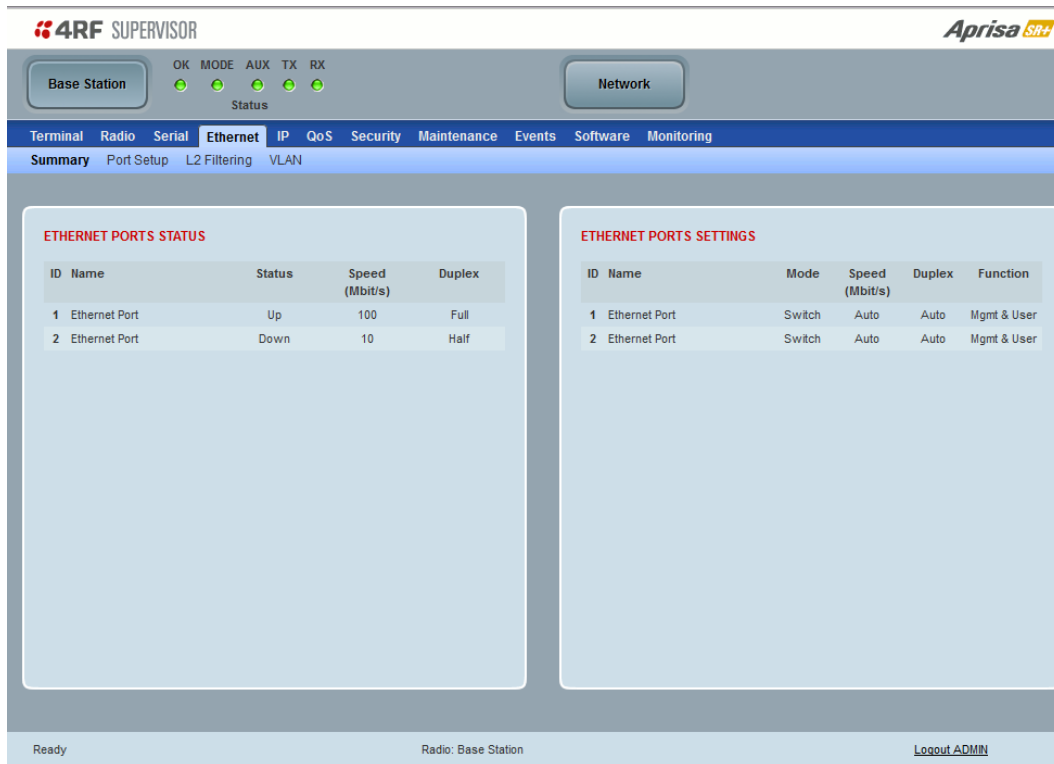
Inter-Frame Gap (chars)

This parameter is not required for GPS Receiver device.

Ethernet

Ethernet > Summary

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



ETHERNET PORTS STATUS

ID	Name	Status	Speed (Mbit/s)	Duplex
1	Ethernet Port	Up	100	Full
2	Ethernet Port	Down	10	Half

ETHERNET PORTS SETTINGS

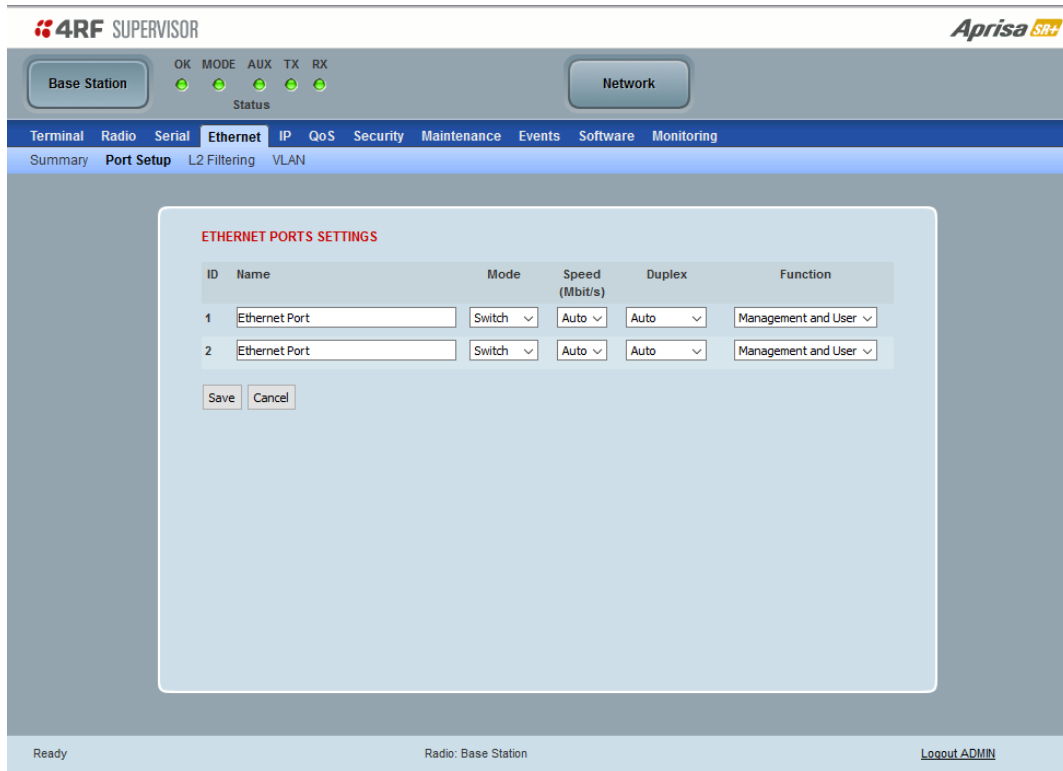
ID	Name	Mode	Speed (Mbit/s)	Duplex	Function
1	Ethernet Port	Switch	Auto	Auto	Mgmt & User
2	Ethernet Port	Switch	Auto	Auto	Mgmt & User

Ready Radio: Base Station [Logout ADMIN](#)

See 'Ethernet > Port Setup' for configuration options.

Ethernet > Port Setup

This page provides the setup for the Ethernet ports settings.



ID	Name	Mode	Speed (Mbit/s)	Duplex	Function
1	Ethernet Port	Switch	Auto	Auto	Management and User
2	Ethernet Port	Switch	Auto	Auto	Management and User

Save Cancel

ETHERNET PORT SETTINGS

Note: This screen is dependent on the Data Port product option purchased (see ‘Data Interface Ports’ on page 404). The Data Port product option shown is a 2E2S - two Ethernet ports and two Serial ports

Mode

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

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

Speed (Mbit/s)

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

Option	Function
Auto	Provides auto selection of Ethernet Port Speed 10/100 Mbit/s
10	The Ethernet Port Speed is manually set to 10 Mbit/s
100	The Ethernet Port Speed is manually set to 100 Mbit/s

Duplex

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

Option	Function
Auto	Provides auto selection of Ethernet Port duplex setting.
Half Duplex	The Ethernet Port is manually set to Half Duplex.
Full Duplex	The Ethernet Port is manually set to Full Duplex.

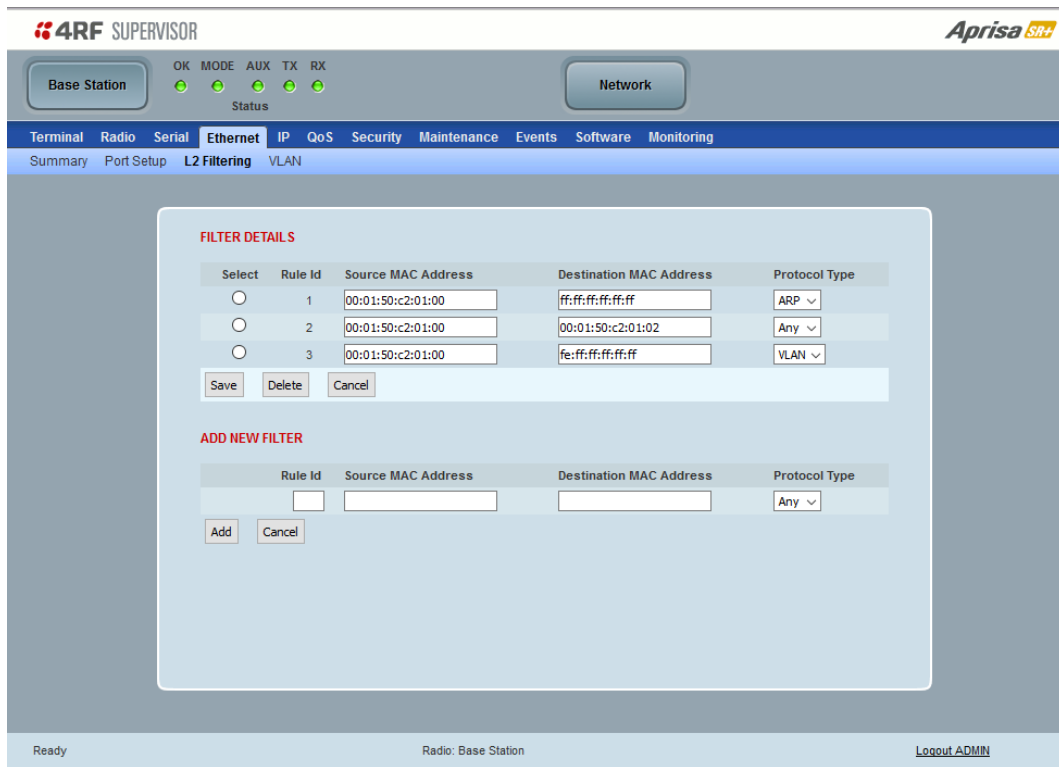
Function

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

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

Ethernet > L2 Filtering

This page is only available if the Ethernet traffic option has been licensed (see ‘Maintenance > Licence’ on page 270).



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Status Network

Terminal Radio Serial **Ethernet** IP QoS Security Maintenance Events Software Monitoring

Summary Port Setup **L2 Filtering** VLAN

FILTER DETAILS

Select	Rule Id	Source MAC Address	Destination MAC Address	Protocol Type
☐	1	00:01:50:c2:01:00	ff:ff:ff:ff:ff:ff	ARP ▾
☐	2	00:01:50:c2:01:00	00:01:50:c2:01:02	Any ▾
☐	3	00:01:50:c2:01:00	fe:ff:ff:ff:ff:ff	VLAN ▾

Save Delete Cancel

ADD NEW FILTER

Rule Id	Source MAC Address	Destination MAC Address	Protocol Type
			Any ▾

Add Cancel

Ready Radio: Base Station Logout ADMIN

FILTER DETAILS

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

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

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

Management traffic to the radio will never be blocked.

Source MAC Address

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

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

Destination MAC Address

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

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

Protocol Type

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

Example:

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

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

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

Special L2 Filtering Rules:

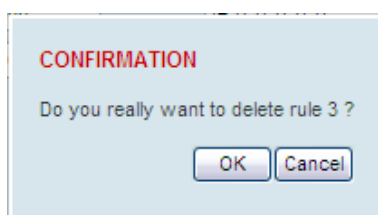
Unicast Only Traffic

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

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

To delete a L2 Filter:

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



3. Click on OK.

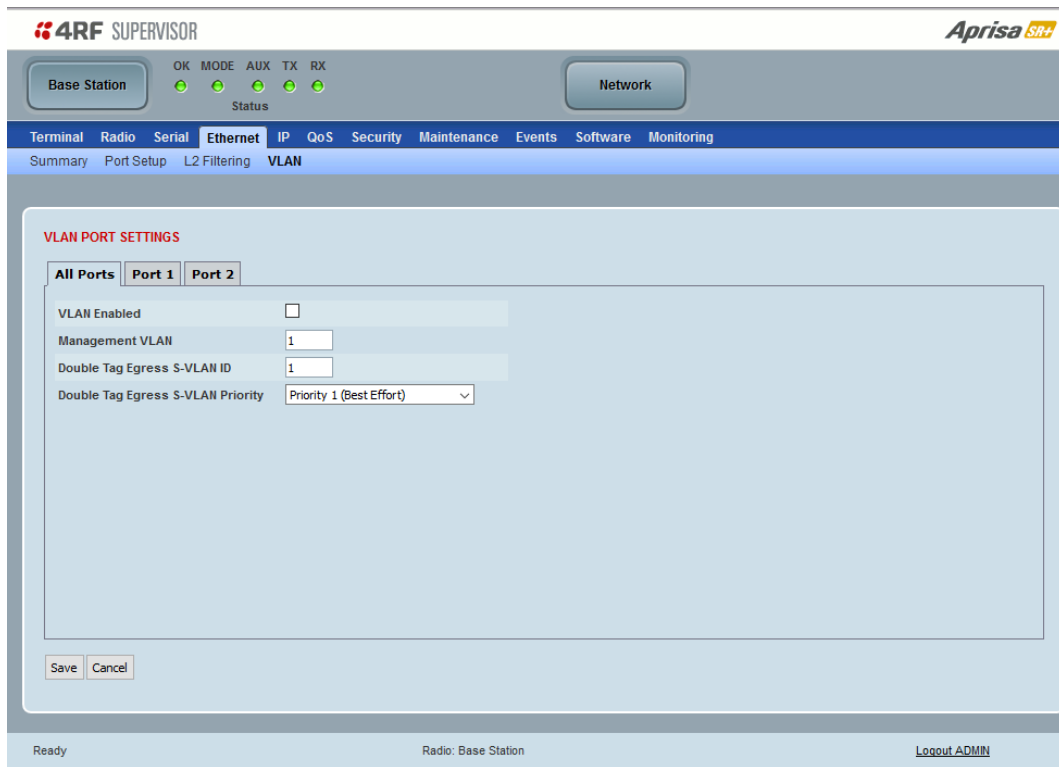
ADD NEW FILTER

To add a L2 Filter:

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

Ethernet > VLAN

This page is only available if the Ethernet traffic option has been licensed (see 'Maintenance > Licence' on page 270).



VLAN PORT SETTINGS - All Ports

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

VLAN Enabled

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

Management VLAN

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

Double Tag Egress S-VLAN ID

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

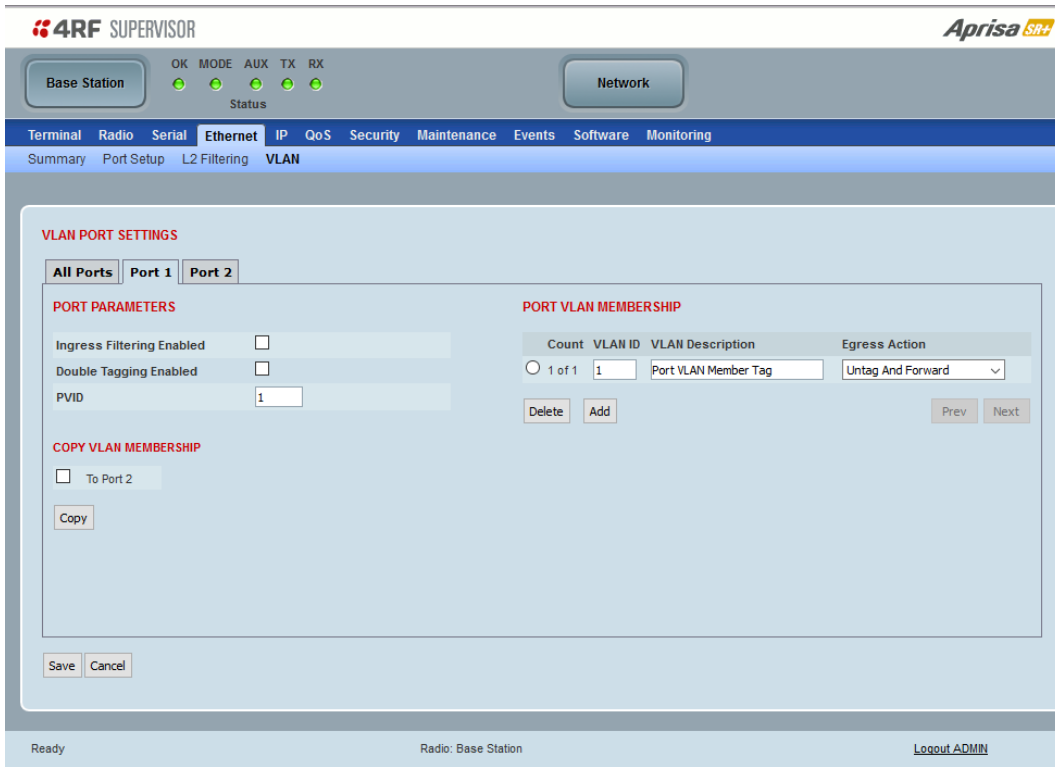
Double Tag Egress S-VLAN Priority

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

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

VLAN PORT SETTINGS - Port 1

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



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Network

Status

Terminal Radio Serial **Ethernet** IP QoS Security Maintenance Events Software Monitoring

Summary Port Setup L2 Filtering **VLAN**

VLAN PORT SETTINGS

All Ports Port 1 Port 2

PORT PARAMETERS

Ingress Filtering Enabled ☐

Double Tagging Enabled ☐

PVID

COPY VLAN MEMBERSHIP

☐ To Port 2

PORT VLAN MEMBERSHIP

Count	VLAN ID	VLAN Description	Egress Action
1 of 1	1	Port VLAN Member Tag	Untag And Forward

Ready Radio: Base Station [Logout ADMIN](#)

PORT PARAMETERS

Ingress Filtering Enabled

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

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

Double Tagging Enabled

This parameter enables double tagging on this specific port. When enabled, if the ingress traffic is double tagged, the Aprisa SR+ will check and validate that the S-VLAN ID matches the S-VLAN defined in 'Double Tag Egress S-VLAN ID' in the 'all ports' tab. If there is a match, the packet will be forwarded into the Bridge and the S-VLAN outer tag will be removed, thus the radio network will only forward a single VLAN. If there isn't a matching S-VLAN, the packet will be discarded. On egress, the outer tag (S-VLAN) is appended with the 'Double Tag Egress S-VLAN ID' defined in the 'all ports' tab (see page 172). The default is disabled.

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

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

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

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

PVID (Port VLAN ID)

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

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

COPY VLAN MEMBERSHIP

To Port

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

PORT VLAN MEMBERSHIP

VLAN ID

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

VLAN Description

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

Egress Action

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

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

Controls

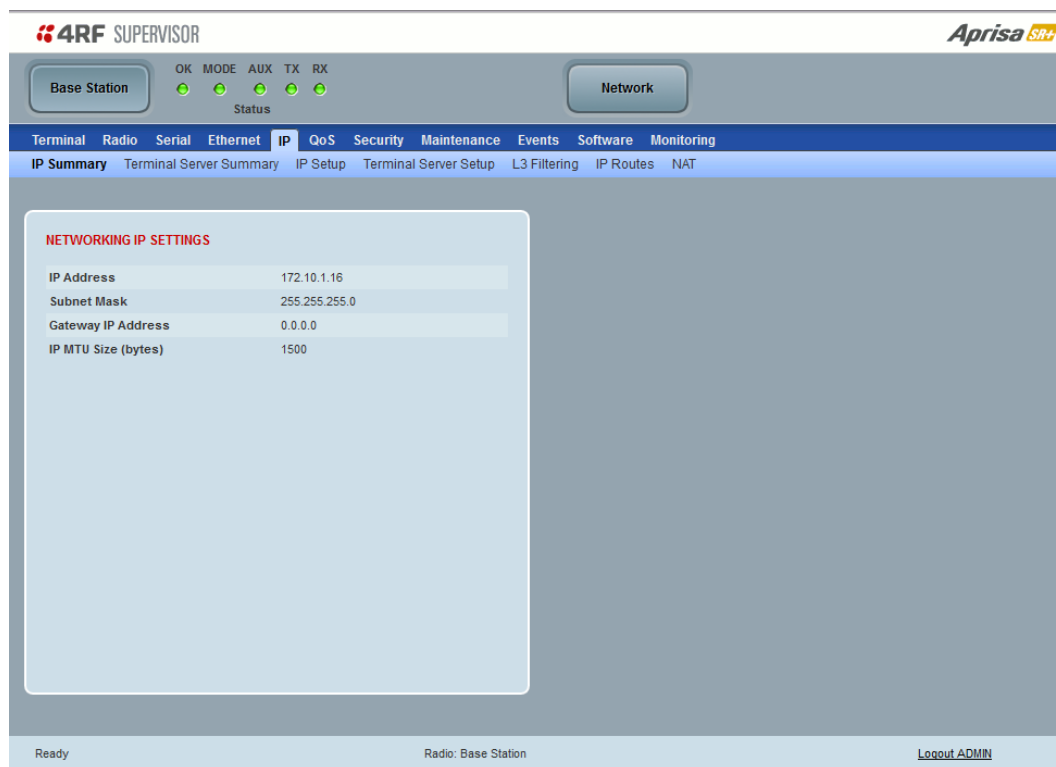
The Add button adds the selected entry.

The Delete button deletes the selected entry.

IP

IP > IP Summary > Bridge / Gateway Router Modes

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



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Status Network

Terminal Radio Serial Ethernet **IP** QoS Security Maintenance Events Software Monitoring

IP Summary Terminal Server Summary IP Setup Terminal Server Setup L3 Filtering IP Routes NAT

NETWORKING IP SETTINGS

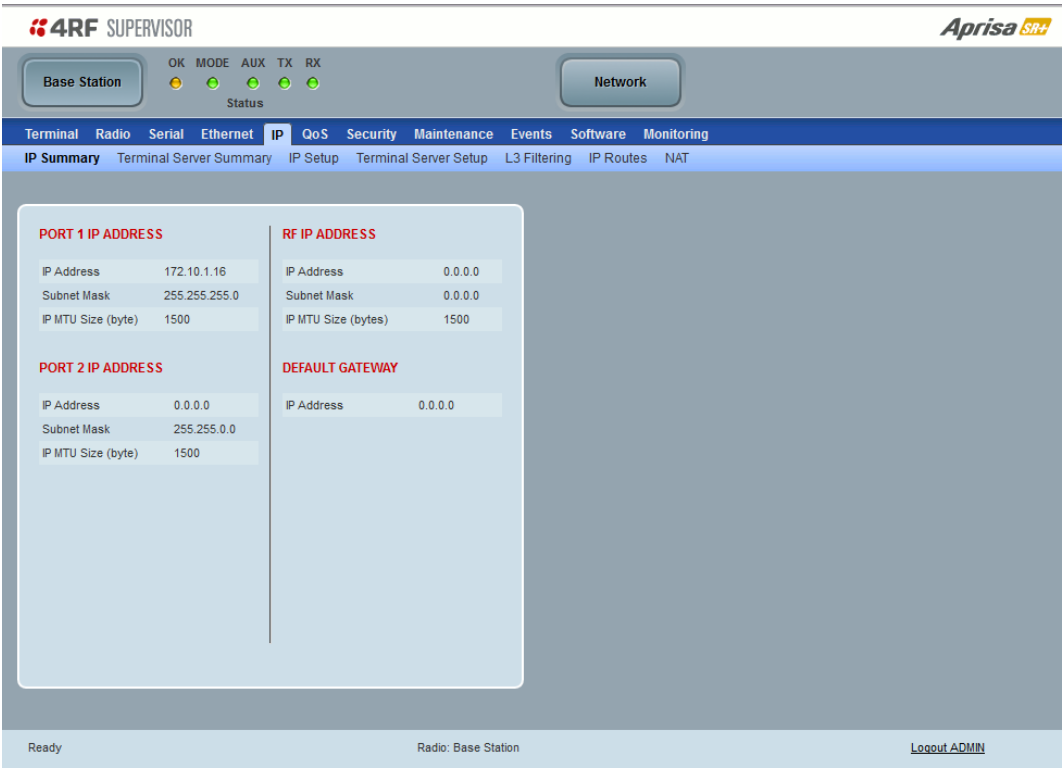
IP Address	172.10.1.16
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
IP MTU Size (bytes)	1500

Ready Radio: Base Station [Logout ADMIN](#)

See ‘IP > IP Setup > Bridge / Gateway Router Modes’ on page 182 for configuration options.

IP > IP Summary > Router Mode

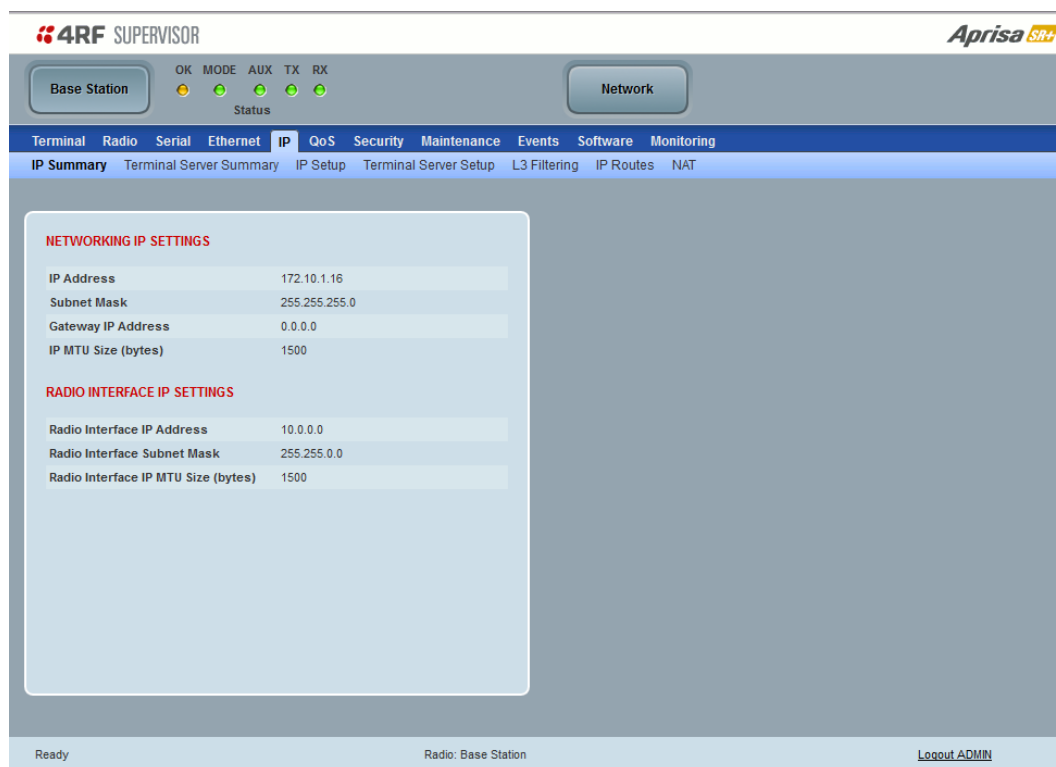
This page displays the current settings for the Networking IP Settings for an Ethernet Operating Mode of ‘Router’.



See ‘IP > IP Setup > Router Mode’ on page 183 for configuration options.

IP > IP Summary > Advanced Gateway Router Mode

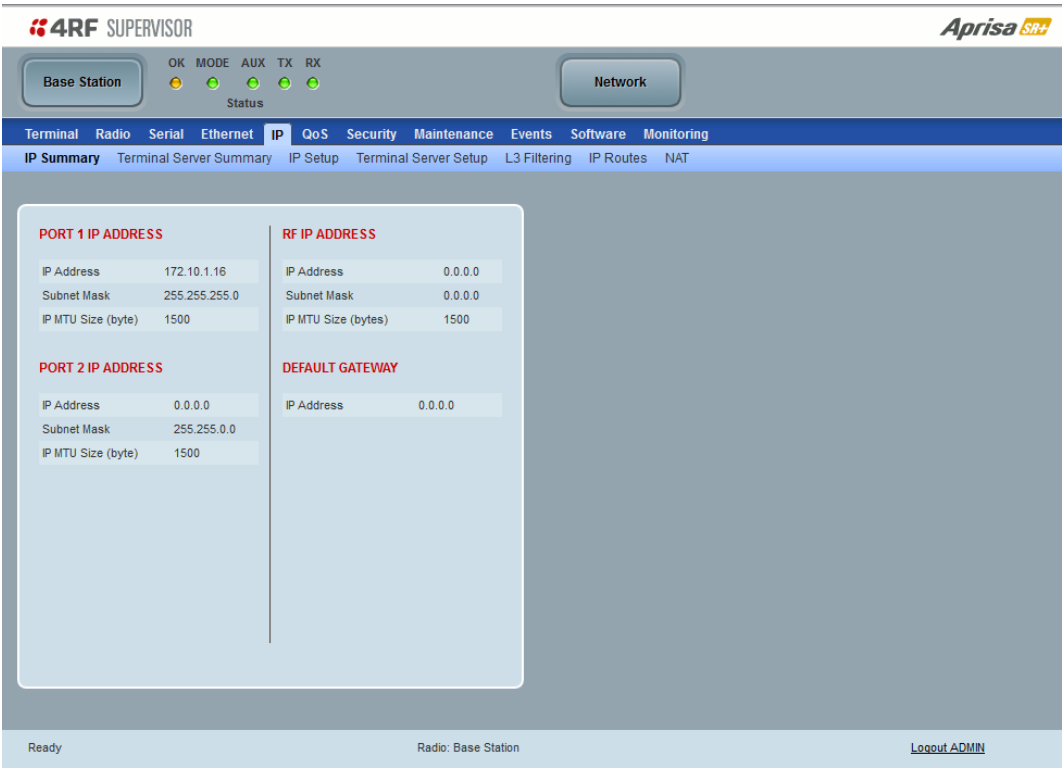
This page displays the current settings for the Networking IP Settings for an Ethernet Operating Mode of ‘Gateway Router’ with Advanced.



See ‘Advanced Gateway Router Mode (AGRM) and Advanced Router Mode (ARM)’ on page 41 for a detailed explanation of advanced router modes.

IP > IP Summary > Advanced Router Mode

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



See ‘Advanced Gateway Router Mode (AGRM) and Advanced Router Mode (ARM)’ on page 41 for a detailed explanation of advanced router modes.

IP > Terminal Server Summary

This page displays the current IP Terminal Server settings.



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Network

Status

Terminal Radio Serial Ethernet **IP** QoS Security Maintenance Events Software Monitoring

IP Summary **Terminal Server Summary** IP Setup Terminal Server Setup L3 Filtering IP Routes NAT

TERMINAL SERVER SUMMARY

Terminal Server 1	Terminal Server 2	Terminal Server 3	
Terminal Server	Disabled	Local Address	172.10.1.16
Name	IP Terminal Server 1	Local Subnet Mask	255.255.0.0
Serial Port	Serial Port 1	Port	20000
Mode	Server	Remote Address	0.0.0.0
Inactivity Timeout (sec)	300	Port	0
TCP (Keep Alive)	Off	Protocol	TCP
PVID	1	Gateway IP Address	0.0.0.0
Protocol Conversion	None		

Ready Radio: Base Station [Logout ADMIN](#)

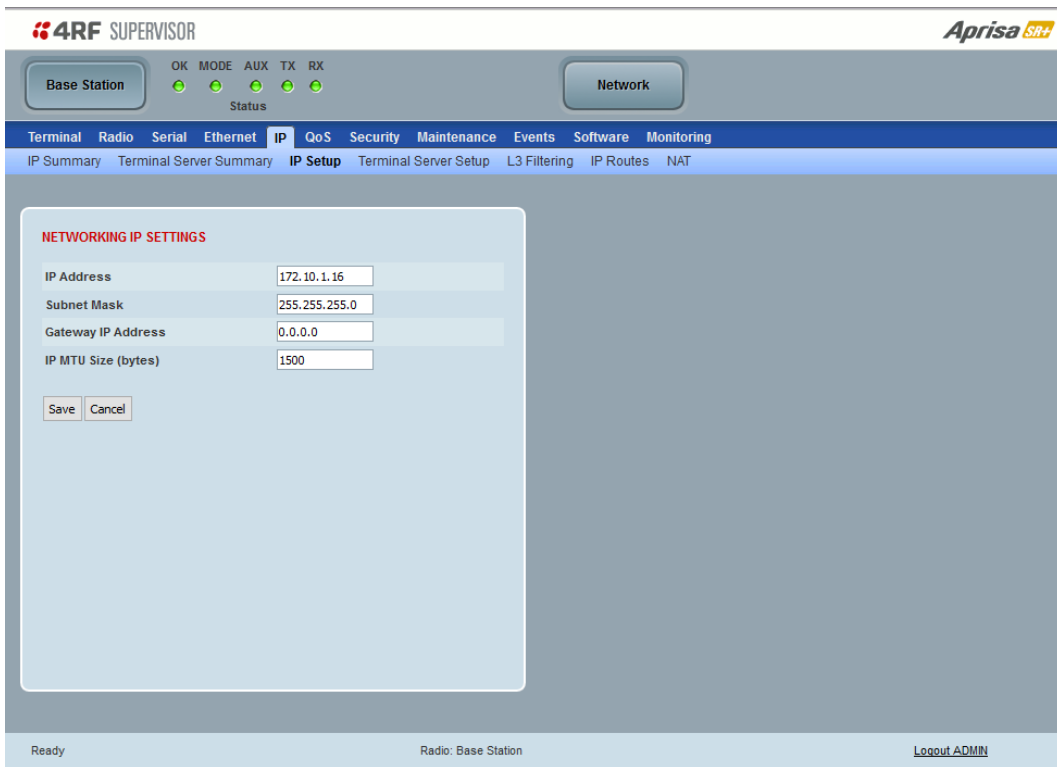
TERMINAL SERVER SUMMARY

IP Terminal Server converts local incoming IP packets to a local physical serial port and to OTA serial packets. This function is typically used on a base station to convert traffic to serial OTA for transmission to all remote radios.

See 'IP > Terminal Server Setup' for configuration options.

IP > IP Setup > Bridge / Gateway Router Modes

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



NETWORKING IP SETTINGS

IP Address

Set the static IP Address of the radio (Management and Ethernet ports) assigned by your site network administrator using the standard format xxx.xxx.xxx.xxx. This IP address is used both in Bridge mode and in Router mode. The default IP address is in the range 169.254.50.10.

Subnet Mask

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

Gateway

Set the Gateway address of the radio, if required, using the standard format xxx.xxx.xxx.xxx.

A default gateway is the node on the network that traffic is directed to when an IP address does not match any other routes in the routing table. It can be the IP address of the router or PC connected to the base station. The default gateway commonly connects the internal radio network and the outside network. The default Gateway is 0.0.0.0.

IP MTU Size (bytes)

Sets the IP Maximum Transmission Unit (MTU).

The IP MTU can be configured on each IP interface to improve compatibility and/or performance when integrating with devices using smaller than standard MTU sizes. The default setting is 1500.

IP > IP Setup > Router Mode

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

4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Network

Status

Terminal Radio Serial Ethernet **IP** QoS Security Maintenance Events Software Monitoring

IP Summary Terminal Server Summary **IP Setup** Terminal Server Setup L3 Filtering IP Routes NAT

PORT 1 IP SETTINGS

IP Address: 172.10.1.16

Subnet Mask: 255.255.255.0

IP MTU Size (bytes): 1500

PORT 2 IP SETTINGS

IP Address: 0.0.0.0

Subnet Mask: 255.255.0.0

IP MTU Size (bytes): 1500

Save Cancel

RADIO INTERFACE IP SETTINGS

IP Address: 10.0.0.0

Subnet Mask: 255.255.0.0

IP MTU Size (bytes): 1500

GATEWAY IP SETTINGS

IP Address: 0.0.0.0

Ready Radio: Base Station [Logout ADMIN](#)

PORT SETTINGS - port (n)

Note: This screen is dependent on the Data Port product option purchased (see 'Data Interface Ports' on page 404). The Data Port product option shown is a 2E2S - two Ethernet ports and two Serial ports

IP Address

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

Subnet Mask

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

Gateway

Set the Gateway address of the radio Ethernet port (n), if required, using the standard format xxx.xxx.xxx.xxx.

A default gateway is the node on the network that traffic is directed to when an IP address does not match any other routes in the routing table. It can be the IP address of the router or PC connected to the base station. The default gateway commonly connects the internal radio network and the outside network. The default Gateway is 0.0.0.0.

IP MTU Size (bytes)

Sets the IP Maximum Transmission Unit (MTU).

The IP MTU can be configured on each IP interface to improve compatibility and/or performance when integrating with devices using smaller than standard MTU sizes. The default setting is 1500.

RADIO INTERFACE IP SETTINGS

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

Radio Interface IP Address

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

Radio Interface Subnet Mask

Set the Subnet Mask of the RF interface using the standard format xxx.xxx.xxx.xxx. The default subnet mask is 255.255.254.0 (/23) (see Note 2 below).

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

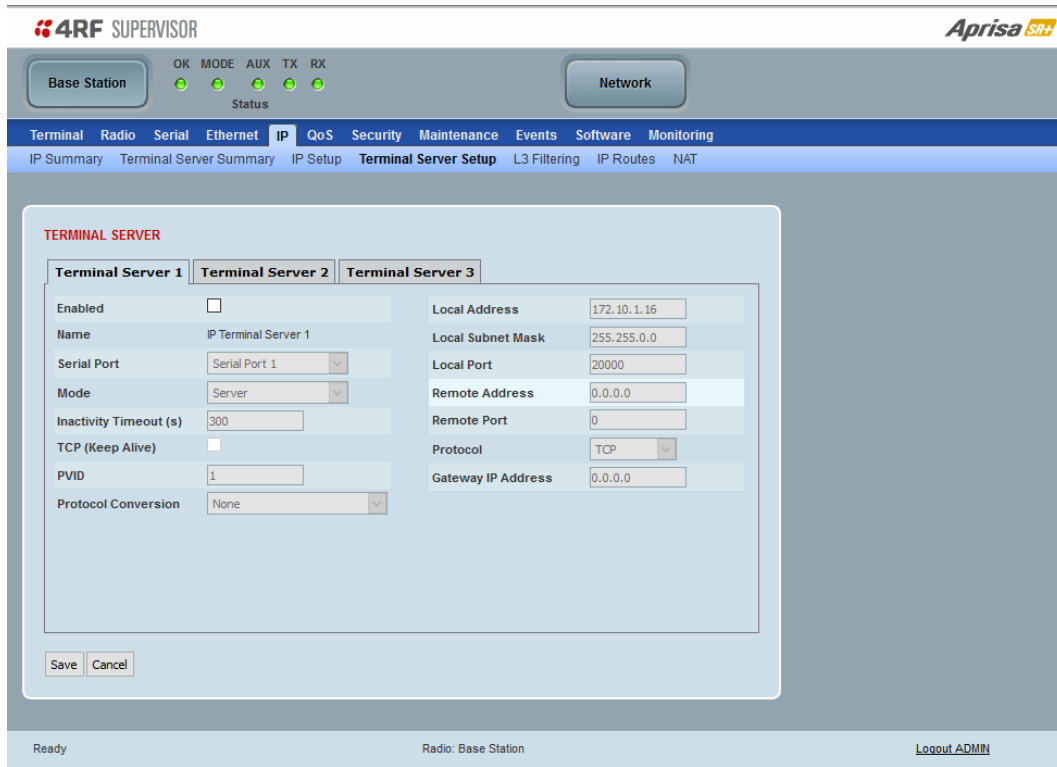
When the base radio has a host specific RF interface IP address, then all the remotes must have a host specific RF interface IP address from the same subnet.

Note 2: If the user sets the RF interface IP address to a network IP address for Auto IP assignment, then the radio will ignore the Radio Interface Subnet Mask setting and use a /23 network subnet ignoring the last two octets.

Note 3: When a remote radio is configured for Router Mode and the base radio is changed from Bridge Mode to Router Mode and the RF interface IP address is set to Auto IP configuration (at least the last octet of the RF interface IP address is zero), it is mandatory to configure the network topology by using the 'Decommission Node' and 'Discover Nodes' (see 'Maintenance > Advanced' on page 276).

IP > Terminal Server Setup

This page provides the setup for the IP Terminal Server settings.



TERMINAL SERVER

Enabled

This parameter enables IP terminal server.

IP terminal server converts local incoming IP packets to a local physical serial port and to OTA serial packets as well. This function is typically used on a base station to convert traffic to serial OTA for transmission to all remote radios.

The serial terminal server traffic can be prioritized separately. For QoS, the priority of the serial terminal server traffic is that of the configured priority for its associated serial port (see 'QoS > Traffic Priority' on page 204).

Name

This parameter displays the IP terminal server port name.

Serial Port

This parameter selects the serial port to use IP terminal server.

Option	Function
Serial Port	This is the normal RS-232 serial ports provided with the RJ45 connector.
USB Serial Port	This is the optional RS-232 / RS-485 serial port provided with the USB host port connector with a USB to RS-232 / RS-485 RJ45 converter cable (see 'USB RS-232 / RS-485 Serial Port' on page 438).

Mode

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

Option	Function
Client	The radio will attempt to establish a TCP connection with the specified remote unit. Generally, this setting is for the base station with an Ethernet connection to the SCADA master.
Server	The radio will listen for a TCP connection on the specified local port. Generally, this setting is for the remote radio with a serial connection to the RTU. Data received from any client shall be forwarded to the associated serial port while data received from that serial port shall be forwarded to every client with an open TCP connection. If no existing TCP connections exist, all data received from the associated serial port shall be discarded.
Client and Server	The radio will listen for a TCP connection on the specified local port and if necessary, establish a TCP connection with the specified remote unit. Generally, this setting is used for the remote radio but it should be used carefully as two connections might be established with the base station. Data received from any client shall be forwarded to the associated serial port while data received from that serial port shall be forwarded to every client with an open TCP connection.

Inactivity Timeout (seconds)

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

TCP Keep Alive

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

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

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

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

PVID

This parameter sets the PVID (port VLAN ID) for each of the terminal servers on the radio.

Protocol Conversion

This parameter defines the mode of operation of the terminal server connection. The default setting is None.

Option	Function
None	No terminal server Protocol Conversion
Modbus TCP to Modbus RTU	The radio provides a gateway between Modbus TCP to Modbus RTU.
Modbus TCP to Modbus ASCII	The radio provides a gateway between Modbus TCP to Modbus ASCII.

Local Address

This parameter sets the Terminal Server local IP address.

Bridge Mode

The local IP address can be the same as the radio's configured IP address or the Virtual IP address for protected stations. If it is not the above, then it must be an IP address from a network different from the radio's network.

Note that the Terminal Server local IP address settings can be the same for other terminal servers in the radio.

Router Mode

The local IP address must be the same as any one of the radio's configured port IP addresses or the Virtual IP address for protected stations.

Gateway Router Mode

The local IP address must be the same as the radio's configured IP address or the Virtual IP address for protected stations.

Local Port

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

The valid port number range is less than or equal to 49151 but with exclusions of 0, 20, 21, 23, 80, 161, 162, 443, 5445, 6445, 9930 or 9931. The default setting is 20000.

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

Remote Address

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

Remote Port

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

Protocol

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

Gateway IP Address

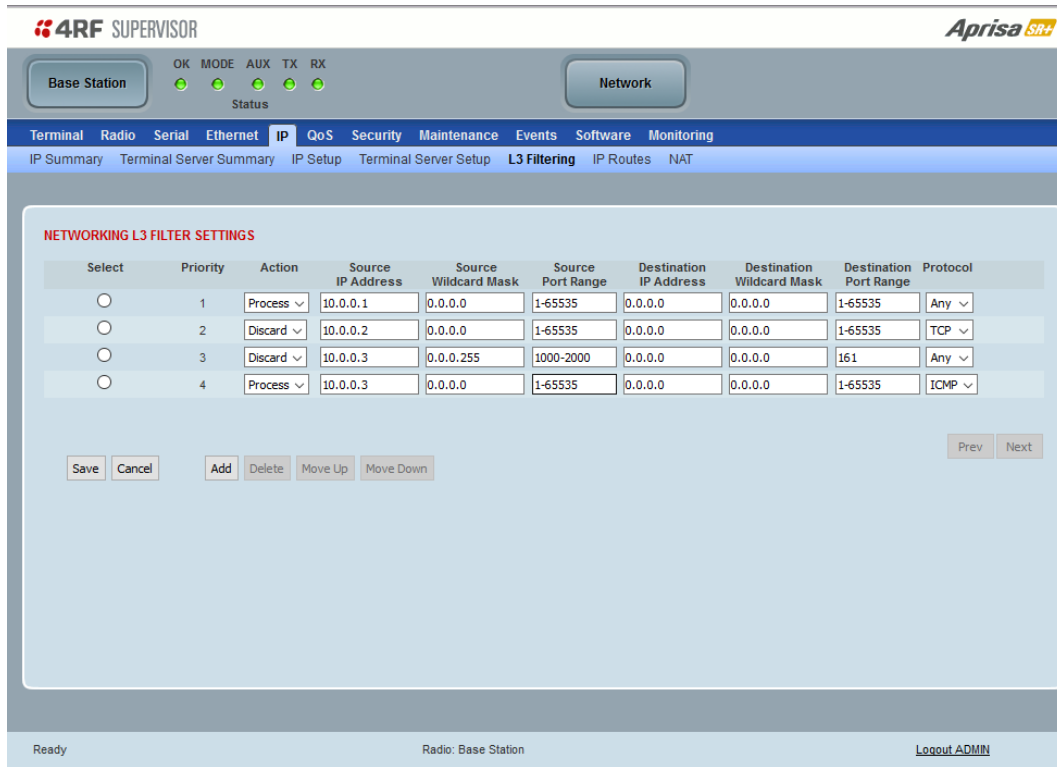
This Terminal Server parameter sets the Gateway IP address of a router in the network that serves as the forwarding router to other networks when no other route specification matches the destination IP address of a packet.

This is useful when default gateway IP address of the radio and the Terminal Server Gateway IP Address are on different IP subnet networks.

When all radios are in router mode (GRM / RM) or advanced router mode (AGRM / ARM), the default gateway IP address of the radio and Gateway IP Address of the Terminal Server are the same, leaving the Gateway IP Address on the default value of 0.0.0.0 will serve the purpose. Only when the radio and Terminal Server are with different IP subnets and are connected to different router gateway IP addresses, the default value shall be set to the appropriate gateway IP address.

IP > L3 Filtering

This page is only available if the Ethernet traffic option has been licensed (see 'Maintenance > Licence' on page 270). The filter operates in either Bridge Mode or Router Mode (see 'Terminal > Operating Mode' on page 116).



Select	Priority	Action	Source IP Address	Source Wildcard Mask	Source Port Range	Destination IP Address	Destination Wildcard Mask	Destination Port Range	Protocol
☐	1	Process	10.0.0.1	0.0.0.0	1-65535	0.0.0.0	0.0.0.0	1-65535	Any
☐	2	Discard	10.0.0.2	0.0.0.0	1-65535	0.0.0.0	0.0.0.0	1-65535	TCP
☐	3	Discard	10.0.0.3	0.0.0.255	1000-2000	0.0.0.0	0.0.0.0	161	Any
☐	4	Process	10.0.0.3	0.0.0.0	1-65535	0.0.0.0	0.0.0.0	1-65535	ICMP

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 of field will automatically enter the wildcard values when the data is saved.

Priority

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

Action

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

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

Source IP Address

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

Source Wildcard Mask

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

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

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

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

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

Source Port Range

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

Destination IP Address

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

Destination Wildcard Mask

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

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

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

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

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

Destination Port Range

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

Protocol

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

Controls

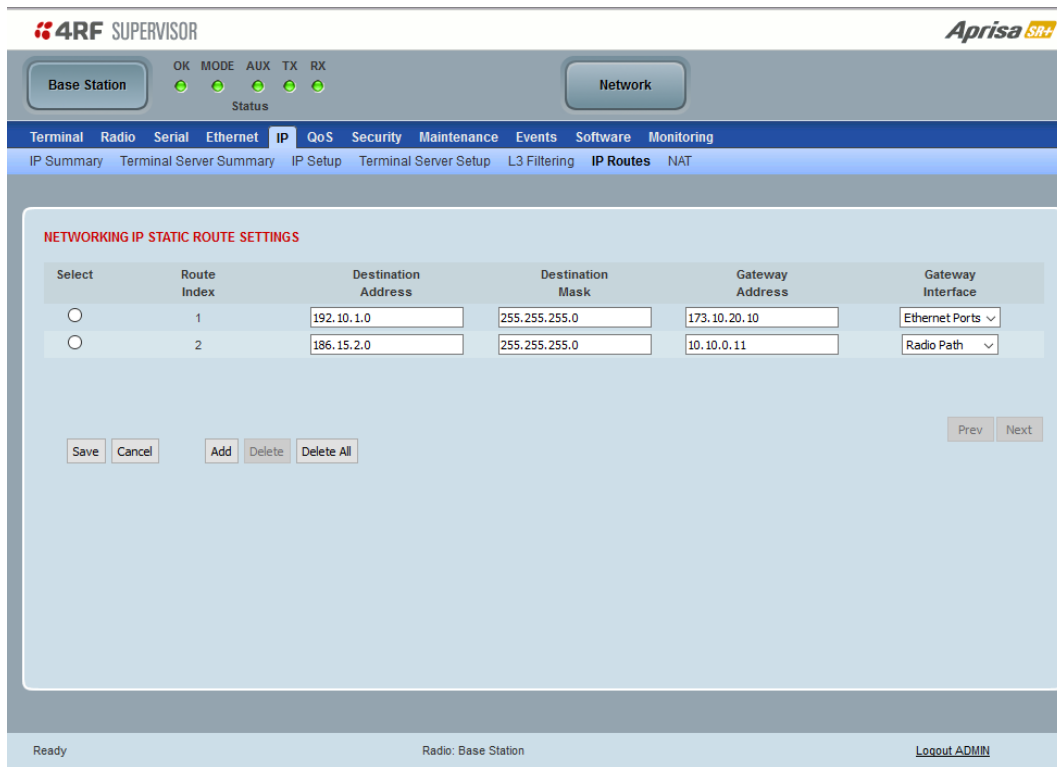
The Delete button deletes the selected entry.

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

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

IP > IP Routes

This page is only available if the Ethernet traffic option has been licensed (see 'Maintenance > Licence' on page 270).



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Status Network

Terminal Radio Serial Ethernet **IP** QoS Security Maintenance Events Software Monitoring

IP Summary Terminal Server Summary IP Setup Terminal Server Setup L3 Filtering **IP Routes** NAT

NETWORKING IP STATIC ROUTE SETTINGS

Select	Route Index	Destination Address	Destination Mask	Gateway Address	Gateway Interface
☐	1	192.10.1.0	255.255.255.0	173.10.20.10	Ethernet Ports
☐	2	186.15.2.0	255.255.255.0	10.10.0.11	Radio Path

Save Cancel Add Delete Delete All Prev Next

Ready Radio: Base Station Logout ADMIN

NETWORKING IP STATIC ROUTE SETTINGS

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

Route Index

This parameter shows the route index.

Destination Address

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

Destination Mask

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

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

If the destination subnet mask is set to 255.255.0.0, the first 2 octets of the Destination IP Address will be evaluated for the route criteria.

Gateway Address

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

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

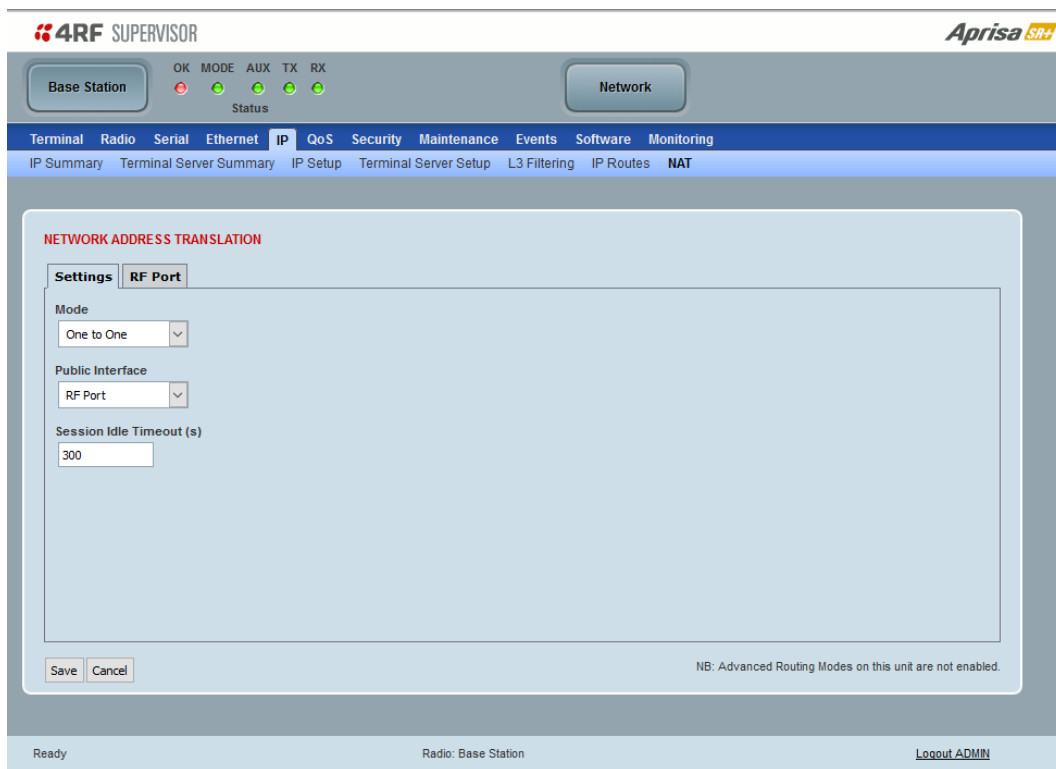
Gateway Interface

This parameter sets the destination interface.

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

IP > NAT

This page is only available if the Ethernet traffic option has been licensed (see 'Maintenance > Licence' on page 270) and Router Mode selected. It is not valid for Bridge Mode (see 'Terminal > Operating Mode' on page 116).



NETWORK ADDRESS TRANSLATION

Mode

Option	Function
Disabled	No Network Address Translation
One to One	NAT mapping (translating) of public interface IP address space into another private interfaces IP address space and vice versa via AGRM/ARM router.
Port Forwarding	NAT mapping (translating) of public TCP/UDP port (or ICMP query ID) of a single public IP addresses into multiple private IP address space and vice versa via AGRM/ARM router.

One To One

The One-to-One Network Address Translation (NAT) remaps one public interface IP address space into another private interface IP address space and vice versa by modifying the IP network address information in IP datagram packet headers.

The NAT function is only available in Advanced Gateway Router Mode (AGRM) or Advanced Router Mode (ARM).

The current implementation of One-to-One NAT supports network configurations supported in AGRM / ARM mode, such as AGRM / ARM-Bridge, Bridge-AGRM / ARM and Bridge-Mix [AGRM / ARM and Bridge] i.e. other network configuration options are not supported by NAT, such as AGRM / ARM-AGRM / ARM network). For more detailed information about NAT see section 'Network Address Translation (NAT) Router' on page 46.

Public Interface

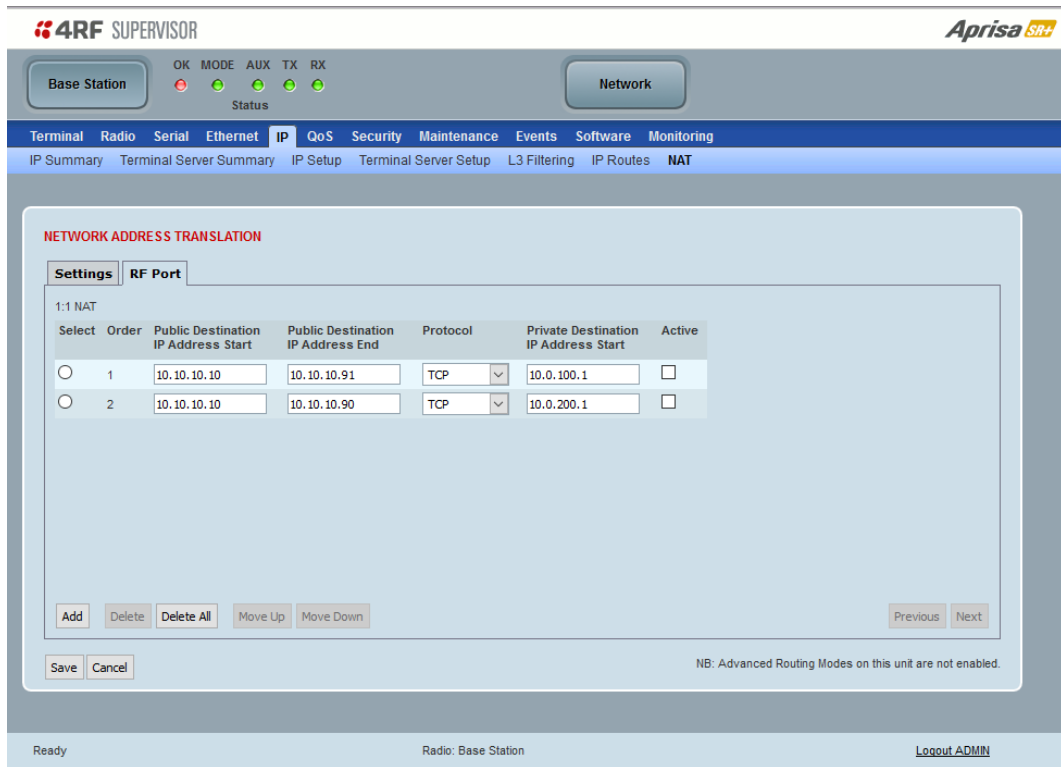
This parameter sets the Global external / public interface.

Option	Function
Radio Port	The public interface for NAT is the radio port.
Ethernet Port (n)	The public interface for NAT is Ethernet port n.

Session Idle Timeout

This time defines the NAT session period in the NAT session table. The session will be automatically removed once the idle timer expires. The Time is common for 'ANY' protocol. This timer will be reset to 0 in session table when a matching packet hits the NAT rule.

One To One > RF Port



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Network

Status

Terminal Radio Serial Ethernet **IP** QoS Security Maintenance Events Software Monitoring

IP Summary Terminal Server Summary IP Setup Terminal Server Setup L3 Filtering IP Routes **NAT**

NETWORK ADDRESS TRANSLATION

Settings **RF Port**

1:1 NAT

Select	Order	Public Destination IP Address Start	Public Destination IP Address End	Protocol	Private Destination IP Address Start	Active
☐	1	10.10.10.10	10.10.10.91	TCP	10.0.100.1	☐
☐	2	10.10.10.10	10.10.10.90	TCP	10.0.200.1	☐

Add Delete Delete All Move Up Move Down Previous Next

Save Cancel

NB: Advanced Routing Modes on this unit are not enabled.

Ready Radio: Base Station Logout ADMIN

The RF Port configures the inbound NAT translation rules (public to private interface translation direction) for the selected public interface which in this case is the RF port. NAT will perform the IP address translation on the inbound direction whenever there is a matching rule in the public IP address and protocol fields translating it to the private IP address. Outbound NAT translation function (private to public interface translation direction) will perform the IP address translation whenever there is a matching rule in the private IP address and protocol fields translating it to the public IP address.

Public Destination IP Address Start

The start of the public destination IP address range.

Public Destination IP Address End

The end of the public destination IP address range.

Protocol

The matching protocol where NAT should perform the IP address translation function. Supports ICMP, TCP, UDP or Any (Any means one among the list; ICMP, TCP, UDP).

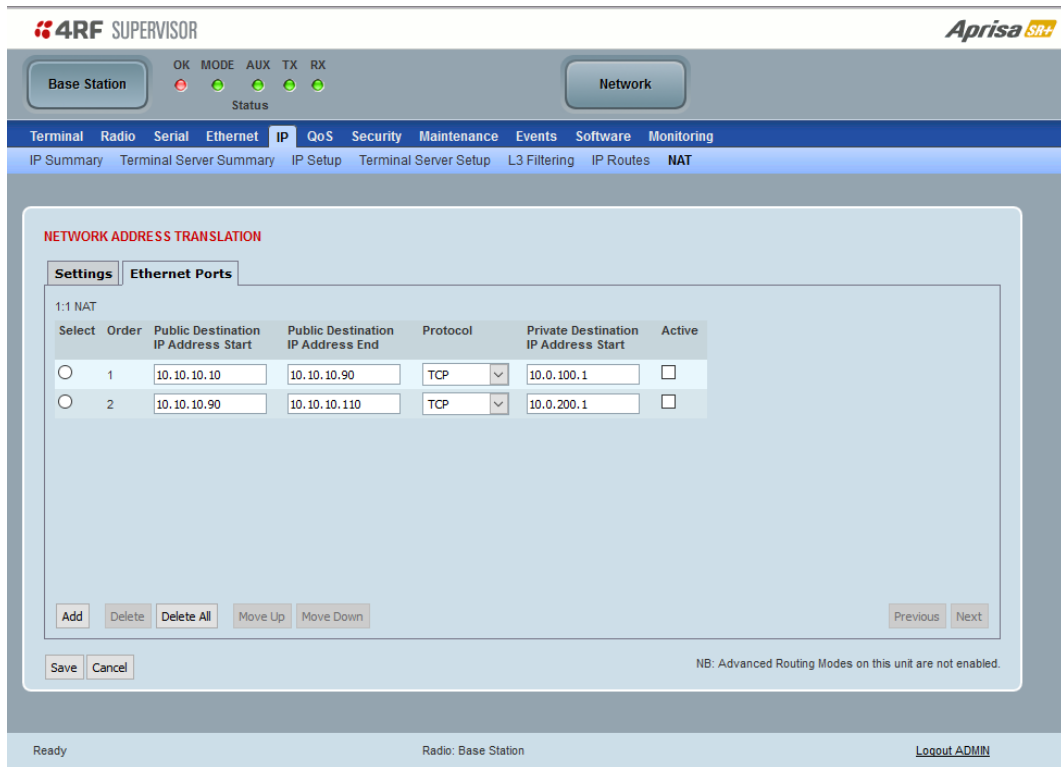
Private Destination IP Address Start

This is the start of the Private Destination IP address range. The end of the private destination IP address is automatically calculated from the start and end of public destination IP address range.

Active

If checked the rule becomes active, if unchecked the rule is inactive.

One To One > Ethernet Ports



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Status Network

Terminal Radio Serial Ethernet **IP** QoS Security Maintenance Events Software Monitoring

IP Summary Terminal Server Summary IP Setup Terminal Server Setup L3 Filtering IP Routes **NAT**

NETWORK ADDRESS TRANSLATION

Settings **Ethernet Ports**

1:1 NAT

Select	Order	Public Destination IP Address Start	Public Destination IP Address End	Protocol	Private Destination IP Address Start	Active
☐	1	10.10.10.10	10.10.10.90	TCP	10.0.100.1	☐
☐	2	10.10.10.90	10.10.10.110	TCP	10.0.200.1	☐

Add Delete Delete All Move Up Move Down Previous Next

Save Cancel

NB: Advanced Routing Modes on this unit are not enabled.

Ready Radio: Base Station Logout ADMIN

The Ethernet Ports configures the inbound NAT translation rules (public to private interface translation direction) for the selected public interface which in this case is the Ethernet port. NAT will perform the IP address translation on the inbound direction whenever there is a matching rule in the public IP address and protocol fields translating it to the private IP address. Outbound NAT translation function (private to public interface translation direction) will perform the IP address translation whenever there is a matching rule in the private IP address and protocol fields translating it to the public IP address.

Public Destination IP Address Start

The start of the public destination IP address range.

Public Destination IP Address End

The end of the public destination IP address range.

Protocol

The matching protocol where NAT should perform the IP address translation function. Supports ICMP, TCP, UDP or Any (Any means one among the list; ICMP, TCP, UDP).

Private Destination IP Address Start

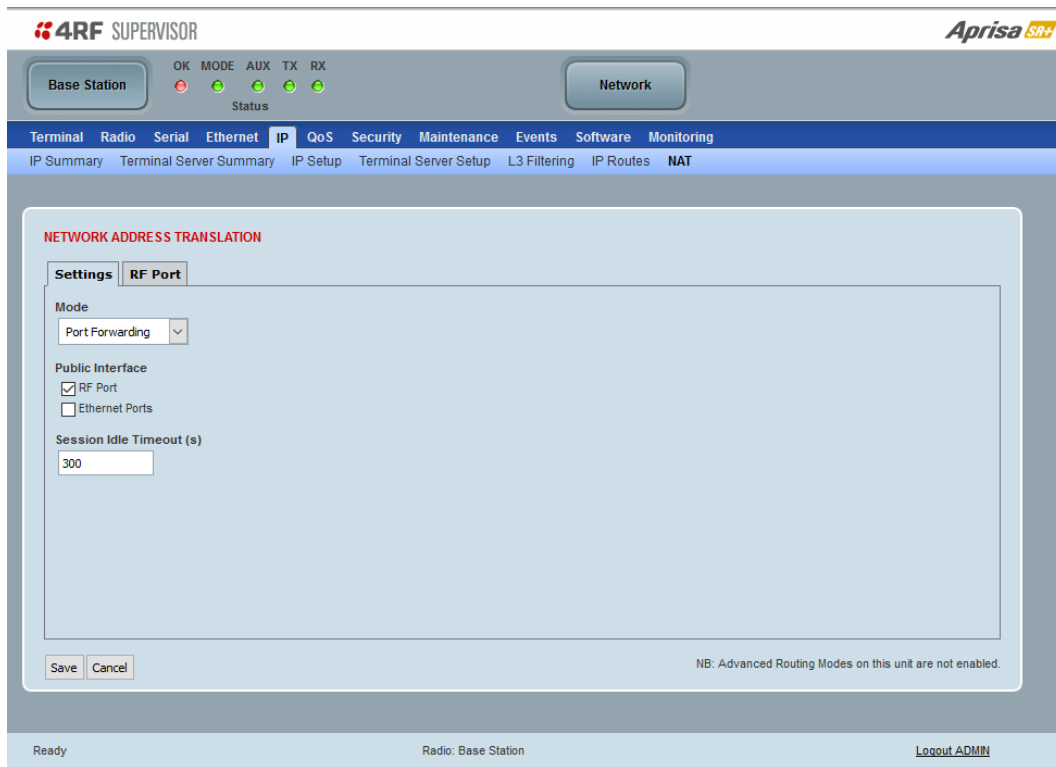
This is the start of the Private Destination IP address range. The end of the private destination IP address is automatically calculated from the start and end of public destination IP address range.

Active

If checked the rule becomes active, if unchecked the rule is inactive.

Port Forwarding

Port Forwarding NAT (NAPT) remaps the public TCP/UDP port (or ICMP query ID) of a single public IP address into multiple private IP address spaces and vice versa via AGRM/ARM router.



Public Interface

This parameter sets the Global external /public interface. The page varies depending on the router mode ARM and AGRM.

The table below shows the public interface options for ARM router (as shown in the screenshot above for 2E2S radio). In ARM, each Ethernet interface can be set with a different public IP address, thus a multiple Ethernet port can be used as a public interface. This is useful for example when radio is connected via two Ethernet ports to two different networks with different subnets for protection or for different services e.g. SCADA service and management service.

Option	Function
Radio Port	The public interface for NAT is the radio port.
Ethernet Port 1	The public interface for NAT is a Ethernet port 1.
Ethernet Port 2	The public interface for NAT is a Ethernet port 2.

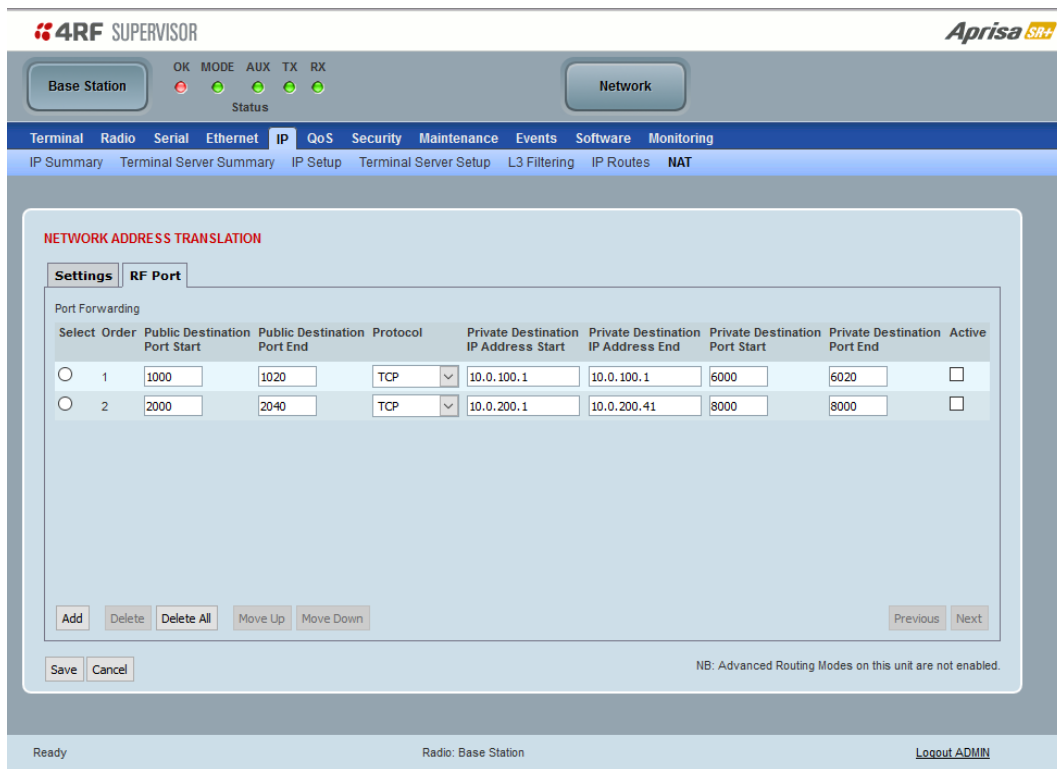
The table below shows the public interface options for a AGRM router, since in AGRM all Ethernet interfaces can be set with only a single public IP address.

Option	Function
Radio Port	The public interface for NAT is the radio port.
Ethernet Ports	The public interface for NAT is a Ethernet port.

Session Idle Timeout

This time defines the NAT session period in the NAT session table. The session will be automatically removed once the idle timer expires. The Time is common for 'ANY' protocol. This timer will be reset to 0 in session table when a matching packet hits the NAT rule.

Port Forwarding > RF Port



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Status Network

Terminal Radio Serial Ethernet **IP** QoS Security Maintenance Events Software Monitoring

IP Summary Terminal Server Summary IP Setup Terminal Server Setup L3 Filtering IP Routes **NAT**

NETWORK ADDRESS TRANSLATION

Settings **RF Port**

Port Forwarding

Select	Order	Public Destination Port Start	Public Destination Port End	Protocol	Private Destination IP Address Start	Private Destination IP Address End	Private Destination Port Start	Private Destination Port End	Active
☐	1	1000	1020	TCP	10.0.100.1	10.0.100.1	6000	6020	☐
☐	2	2000	2040	TCP	10.0.200.1	10.0.200.41	8000	8000	☐

Add Delete Delete All Move Up Move Down Previous Next

Save Cancel

NB: Advanced Routing Modes on this unit are not enabled.

Ready Radio: Base Station Logout ADMIN

When the RF Port is selected as the public interface, then the inbound NAT session is from the radio RF port to the Ethernet private network side of the network (public to private interface), commonly used in remotes. NAT will perform the translation on the inbound direction whenever there is a matching rule in the public TCP/UDP port, the single IP address of RF port and protocol fields translating it to the multiple private IP address space.

Outbound NAT translation function (private to public interface translation direction) will perform the IP address translation whenever there is a matching rule in the TCP/UDP port and private IP address and protocol fields or a dynamic rule is created translating it to the single public IP address and TCP/UDP port.

Public Destination Port Start

The start of the public destination port range between 0 to 65535.

Public Destination Port End

The end of the public destination port range between 0 to 65535.

Protocol

The matching protocol where NAT should perform the IP address translation function. Supports ICMP, TCP, UDP or Any (Any means one among the list; ICMP, TCP, UDP).

Private Destination IP Address Start

This is the start of the Private Destination IP address range.

Private Destination IP Address End

This is the end of the Private Destination IP address range.

Private Destination Port Start

The start of the private destination port range between 0 to 65535.

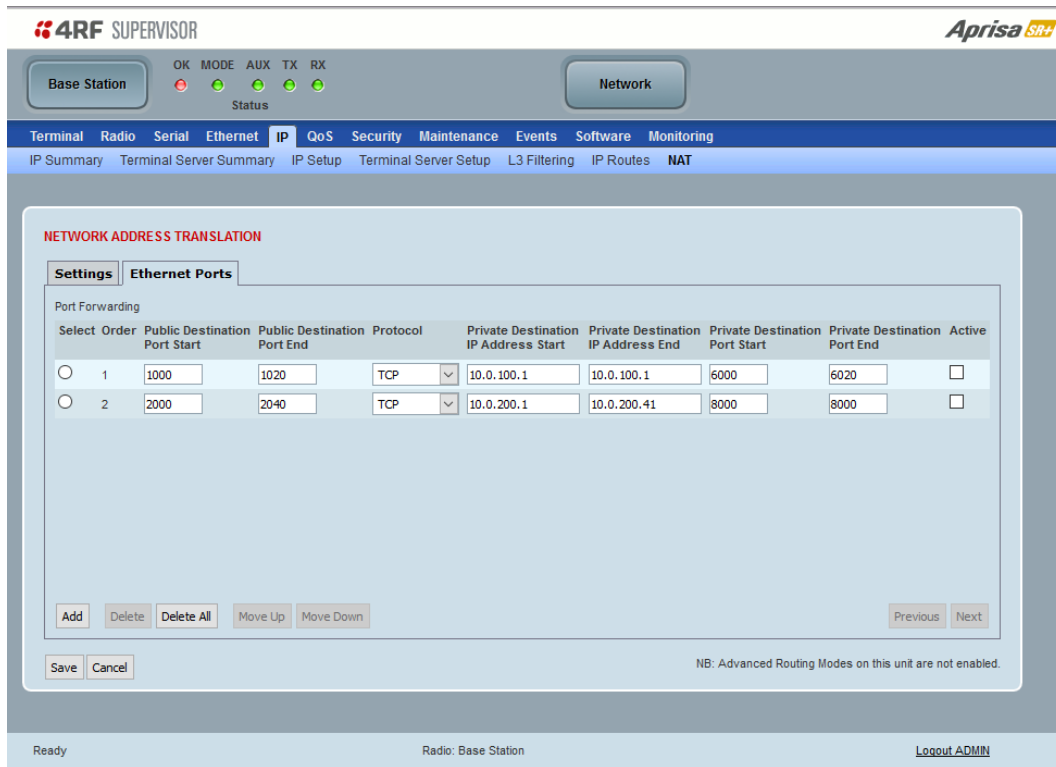
Private Destination Port End

The end of the private destination port range between 0 to 65535.

Active

If checked the rule becomes active, if unchecked the rule is inactive.

Port Forwarding > Ethernet Ports



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Status Network

Terminal Radio Serial Ethernet **IP** QoS Security Maintenance Events Software Monitoring

IP Summary Terminal Server Summary IP Setup Terminal Server Setup L3 Filtering IP Routes **NAT**

NETWORK ADDRESS TRANSLATION

Settings **Ethernet Ports**

Port Forwarding

Select	Order	Public Destination Port Start	Public Destination Port End	Protocol	Private Destination IP Address Start	Private Destination IP Address End	Private Destination Port Start	Private Destination Port End	Active
☐	1	1000	1020	TCP	10.0.100.1	10.0.100.1	6000	6020	☐
☐	2	2000	2040	TCP	10.0.200.1	10.0.200.41	8000	8000	☐

Add Delete Delete All Move Up Move Down Previous Next

Save Cancel

NB: Advanced Routing Modes on this unit are not enabled.

Ready Radio: Base Station Logout ADMIN

When the Ethernet Port is selected as the public interface, then the inbound NAT session is from the Ethernet port to the RF port private network side of the network (public to private interface), commonly used in Base station. NAT will perform the translation on the inbound direction whenever there is a matching rule in the public TCP/UDP port, the single IP address of the Ethernet port and protocol fields translating it to the multiple private IP address space.

Outbound NAT translation function (private to public interface translation direction) will perform the IP address translation whenever there is a matching rule in the TCP/UDP port and private IP address and protocol fields or a dynamic rule is created translating it to the single public IP address and TCP/UDP port.

Public Destination Port Start

The start of the public destination port range between 0 to 65535.

Public Destination Port End

The end of the public destination port range between 0 to 65535.

Protocol

The matching protocol where NAT should perform the IP address translation function. Supports ICMP, TCP, UDP or Any (Any means one among the list; ICMP, TCP, UDP).

Private Destination IP Address Start

This is the start of the Private Destination IP address range.

Private Destination IP Address End

This is the end of the Private Destination IP address range.

Private Destination Port Start

The start of the private destination port range between 0 to 65535.

Private Destination Port End

The end of the private destination port range between 0 to 65535.

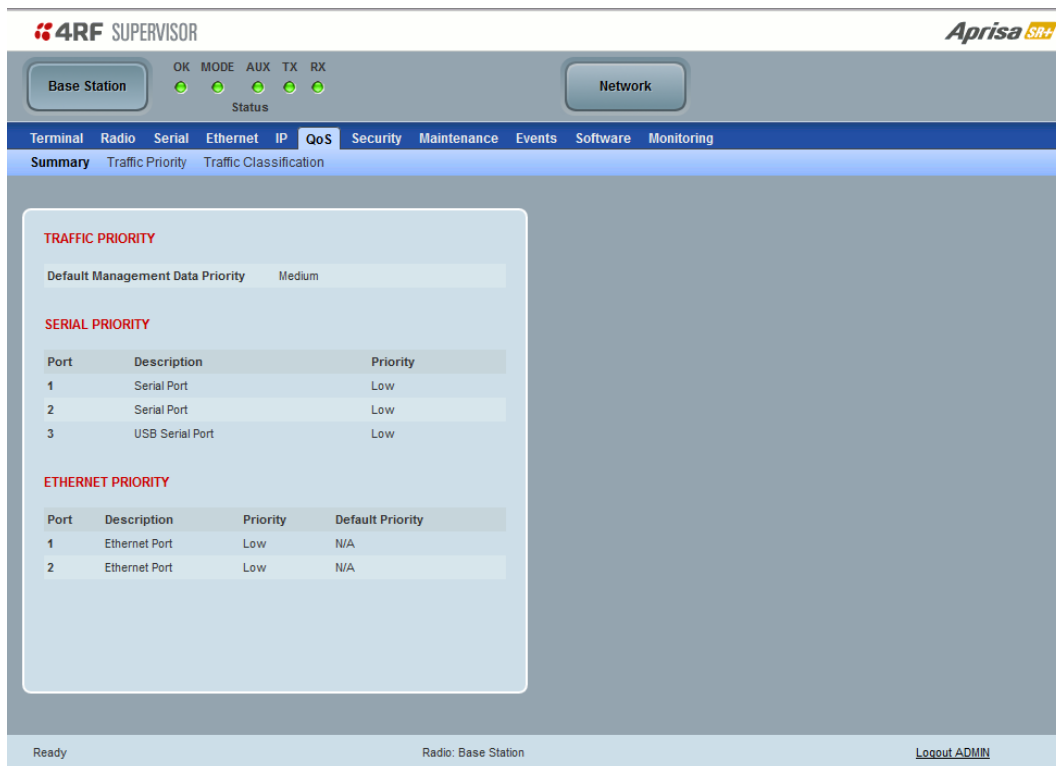
Active

If checked the rule becomes active, if unchecked the rule is inactive.

QoS

QoS > Summary

This page provides a summary of the QoS Settings.



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Network
Status

Terminal Radio Serial Ethernet IP **QoS** Security Maintenance Events Software Monitoring

Summary Traffic Priority Traffic Classification

TRAFFIC PRIORITY

Default Management Data Priority Medium

SERIAL PRIORITY

Port	Description	Priority
1	Serial Port	Low
2	Serial Port	Low
3	USB Serial Port	Low

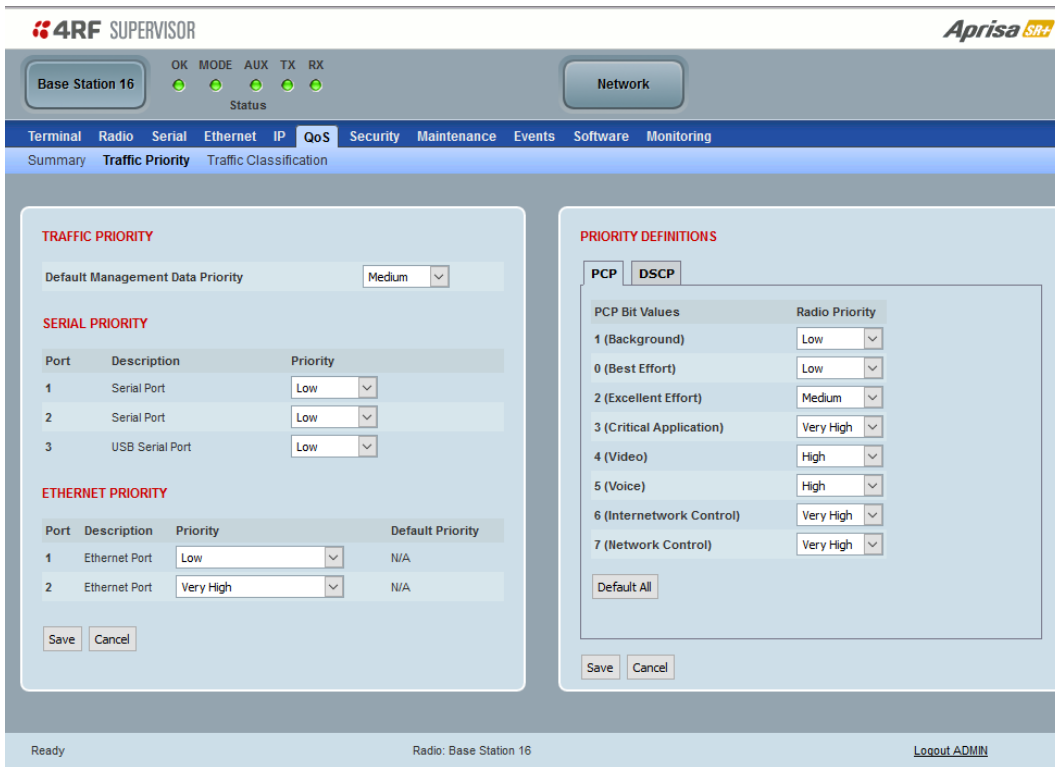
ETHERNET PRIORITY

Port	Description	Priority	Default Priority
1	Ethernet Port	Low	N/A
2	Ethernet Port	Low	N/A

Ready Radio: Base Station [Logout ADMIN](#)

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

QoS > Traffic Priority



TRAFFIC PRIORITY

Default Management Data Priority: Medium

SERIAL PRIORITY

Port	Description	Priority
1	Serial Port	Low
2	Serial Port	Low
3	USB Serial Port	Low

ETHERNET PRIORITY

Port	Description	Priority	Default Priority
1	Ethernet Port	Low	N/A
2	Ethernet Port	Very High	N/A

Save Cancel

PRIORITY DEFINITIONS

PCP DSCP

PCP Bit Values	Radio Priority
1 (Background)	Low
0 (Best Effort)	Low
2 (Excellent Effort)	Medium
3 (Critical Application)	Very High
4 (Video)	High
5 (Voice)	High
6 (Internetwork Control)	Very High
7 (Network Control)	Very High

Default All

Save Cancel

Ready Radio: Base Station 16 Logout ADMIN

TRAFFIC PRIORITY

Default Management Data Priority

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

This priority is also used for traffic if the remote serial port is not available for the radio hardware data port option e.g. if the base station is 2E2S and a remote radio is 4E0S.

SERIAL PRIORITY

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

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

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

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

Priority	Description
Low	All port frames are set to low priority
Medium	All port frames are set to medium priority
High	All port frames are set to high priority
Very High	All port frames are set to very high priority
From Tagged Frame (PCP)	All port frames are set to PCP priority bits (VLAN priority) in VLAN tagged frames or priority tag (VLAN 0) frames. To enable, see 'PCP (Priority Code Point)' on page 206.
From Packet (DSCP)	All port frames are set to DSCP priority bits in an IP packet (DSCP in IPv4 TOS field). To enable, see 'DSCP (Differentiated Services Code Point)' on page 208.

The default setting is Very High.

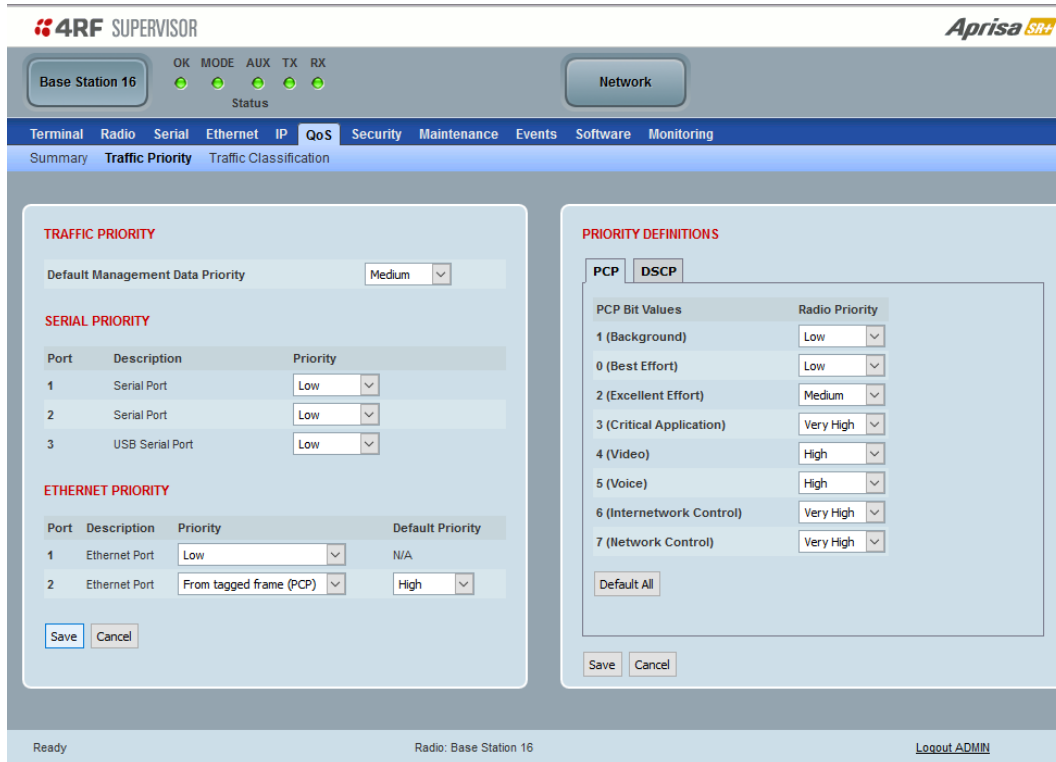
A queuing system is used to prioritize customer traffic from the serial and Ethernet interfaces for over the air transmission. A weighting may be given to each data type and this is used to schedule the next transmission over the air e.g. if there are pending data packets in multiple buffers but serial 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, 1536 bytes).

There are four priority queues in the Aprisa SR+: Very High, High, Medium and Low priority. 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.

PRIORITY DEFINITIONS

PCP (Priority Code Point)

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



4RF SUPERVISOR **Aprisa SR+**

Base Station 16 OK MODE AUX TX RX Network

Status

Terminal Radio Serial Ethernet IP **QoS** Security Maintenance Events Software Monitoring

Summary **Traffic Priority** Traffic Classification

TRAFFIC PRIORITY

Default Management Data Priority: Medium

SERIAL PRIORITY

Port	Description	Priority
1	Serial Port	Low
2	Serial Port	Low
3	USB Serial Port	Low

ETHERNET PRIORITY

Port	Description	Priority	Default Priority
1	Ethernet Port	Low	N/A
2	Ethernet Port	From tagged frame (PCP)	High

Save Cancel

PRIORITY DEFINITIONS

PCP DSCP

PCP Bit Values	Radio Priority
1 (Background)	Low
0 (Best Effort)	Low
2 (Excellent Effort)	Medium
3 (Critical Application)	Very High
4 (Video)	High
5 (Voice)	High
6 (Internetwork Control)	Very High
7 (Network Control)	Very High

Default All

Save Cancel

Ready Radio: Base Station 16 Logout ADMIN

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

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

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

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

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

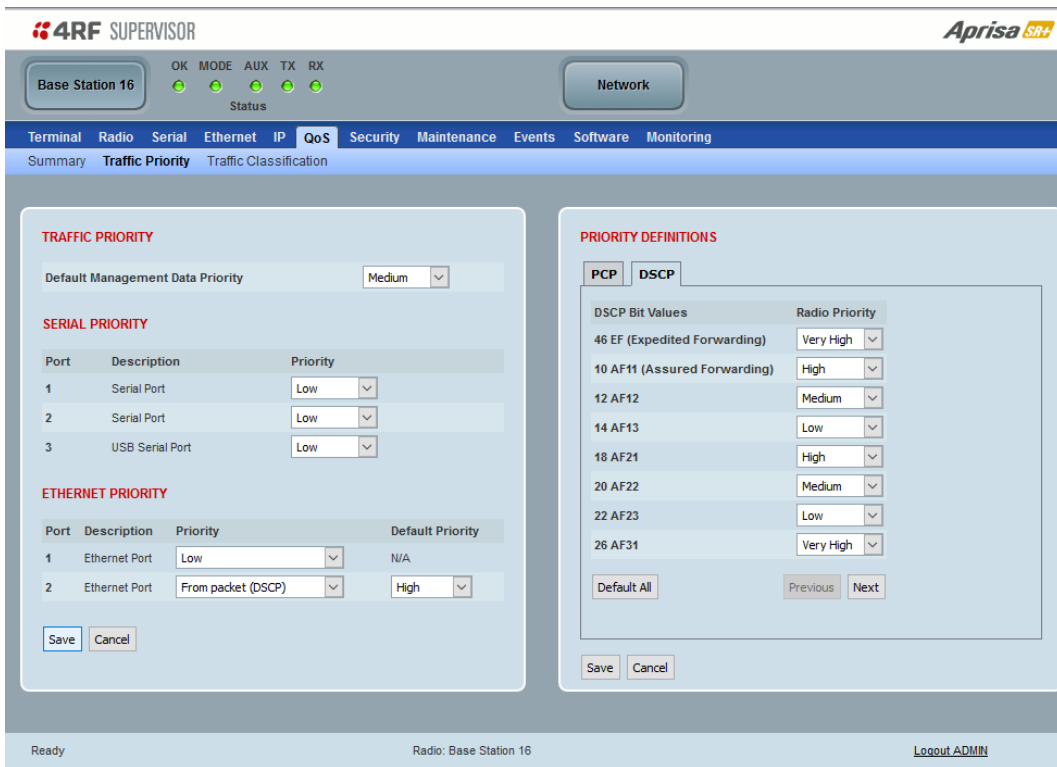
Default mapping of ingress packet VLAN priority to radio CoS / priority shown in the 'PCP priority definition' tab.

Default Priority

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

DSCP (Differentiated Services Code Point)

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



The screenshot shows the 4RF SUPERVISOR web interface for Base Station 16. The 'Network' tab is selected, and the 'QoS' sub-tab is active. The 'Traffic Priority' section is expanded, showing three sub-sections: TRAFFIC PRIORITY, SERIAL PRIORITY, and ETHERNET PRIORITY. The TRAFFIC PRIORITY section shows a 'Default Management Data Priority' set to 'Medium'. The SERIAL PRIORITY section shows a table with 3 ports, all set to 'Low' priority. The ETHERNET PRIORITY section shows a table with 2 ports, both set to 'From packet (DSCP)' priority. The 'PRIORITY DEFINITIONS' section is also expanded, showing a table for mapping DSCP Bit Values to Radio Priority. The 'DSCP' tab is selected, and the table shows mappings for various DSCP values (46 EF, 10 AF11, 12 AF12, 14 AF13, 18 AF21, 20 AF22, 22 AF23, 26 AF31) to Radio Priority levels (Very High, High, Medium, Low). The 'Default All' button is also visible.

Port	Description	Priority
1	Serial Port	Low
2	Serial Port	Low
3	USB Serial Port	Low

Port	Description	Priority	Default Priority
1	Ethernet Port	Low	N/A
2	Ethernet Port	From packet (DSCP)	High

DSCP Bit Values	Radio Priority
46 EF (Expedited Forwarding)	Very High
10 AF11 (Assured Forwarding)	High
12 AF12	Medium
14 AF13	Low
18 AF21	High
20 AF22	Medium
22 AF23	Low
26 AF31	Very High

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

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

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

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

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

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

Default Priority

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

QoS > Traffic Classification

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

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

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

These settings are different for Bridge Mode and Router Mode.

Bridge Mode Traffic Classification Settings

4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Network

Status

Terminal Radio Serial Ethernet IP **QoS** Security Maintenance Events Software Monitoring

Summary Traffic Priority **Traffic Classification**

TRAFFIC CLASSIFICATION

Select	Order	Profile Name	Assigned Priority	Assigned VLAN ID	Active
☐	1	Traff Classification L2 Rule 1	Medium	22	☒
☐	2	Traff Classification L2 Rule 2	Very High	33	☒
☐	3	Traff Classification L2 Rule 3	High	44	☒

Save Cancel Edit Add Delete Delete All Move Up Move Down Previous Next

Ready Radio: Base Station Logout ADMIN

TRAFFIC CLASSIFICATION

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

Profile name

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

Assigned Priority

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

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

Assigned VLAN ID

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

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

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

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

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

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

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

Active

Activates or deactivates the profile rule.

Controls

The Save button saves all profiles to the radio.

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

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

The Add button adds a new profile,

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

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

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

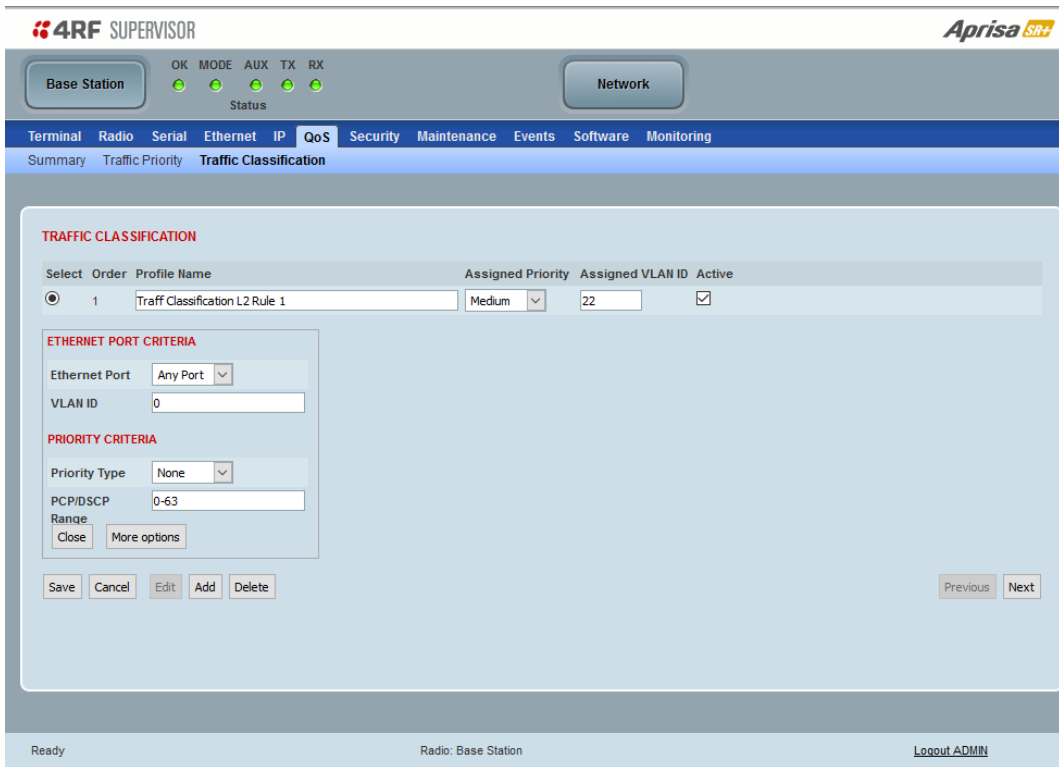
The Move up button will move the selected profile up one in the order of profiles

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

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

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

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



ETHERNET PORT CRITERIA

Ethernet Port

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

VLAN ID

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

Enable this VLAN in the network by setting the same VLAN ID value in PVID (port VLAN ID) and in the PORT VLAN MEMBERSHIP under 'VLAN PORT SETTINGS - Port 1' on page 174. If the VLAN ID is set to zero, all VLAN IDs will meet the criteria.

PRIORITY CRITERIA

Priority Type

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

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

PCP / DSCP Range

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

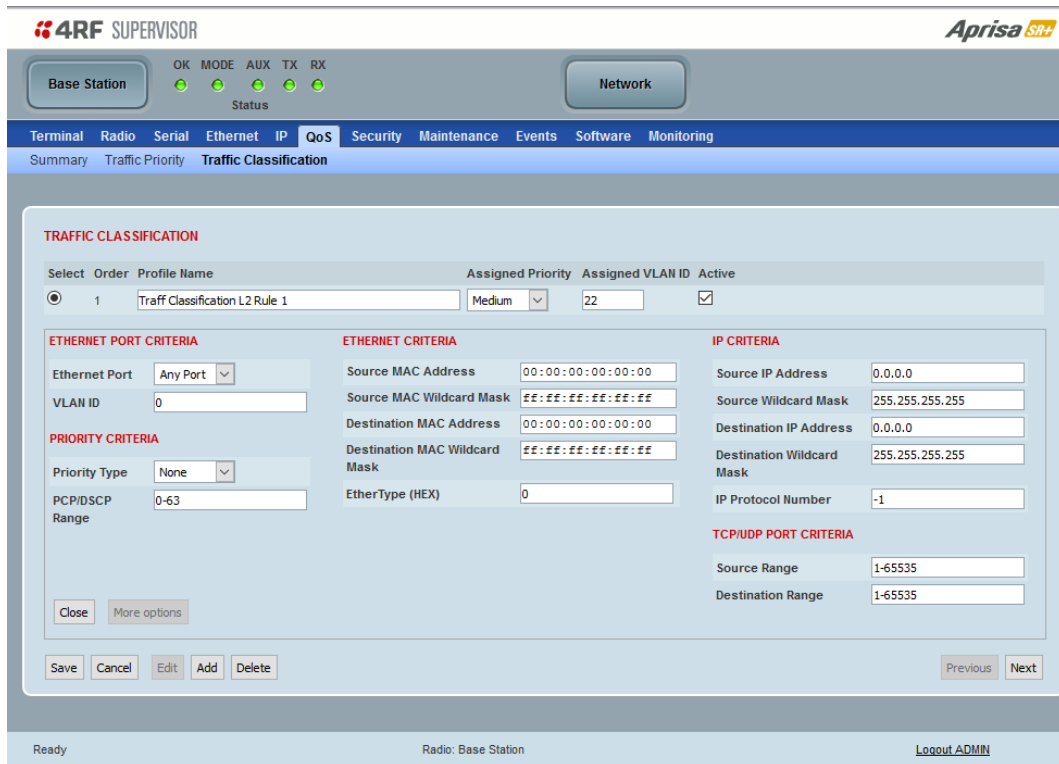
The following table shows the layer 2 packet VLAN tag header PCP priority field values

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

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

DSCP Value (Decimal)	DSCP Priority
46	EF (Expedited Forwarding)
10	AF11 (Assured Forwarding)
12	AF12
14	AF13
18	AF21
20	AF22
22	AF23
26	AF31
28	AF32
30	AF33
34	AF41
36	AF42
38	AF43
0	CS0/Best Effort (BE)
8	CS1 (Class Selector)
16	CS2
24	CS3
32	CS4
40	CS5
48	CS6
56	CS7

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



TRAFFIC CLASSIFICATION

Select	Order	Profile Name	Assigned Priority	Assigned VLAN ID	Active
☒	1	Traff Classification L2 Rule 1	Medium	22	☒

ETHERNET PORT CRITERIA

Ethernet Port: Any Port

VLAN ID: 0

PRIORITY CRITERIA

Priority Type: None

PCP/DSCP Range: 0-63

ETHERNET CRITERIA

Source MAC Address: 00:00:00:00:00:00

Source MAC Wildcard Mask: ff:ff:ff:ff:ff:ff

Destination MAC Address: 00:00:00:00:00:00

Destination MAC Wildcard Mask: ff:ff:ff:ff:ff:ff

EtherType (HEX): 0

IP CRITERIA

Source IP Address: 0.0.0.0

Source Wildcard Mask: 255.255.255.255

Destination IP Address: 0.0.0.0

Destination Wildcard Mask: 255.255.255.255

IP Protocol Number: -1

TCP/UDP PORT CRITERIA

Source Range: 1-65535

Destination Range: 1-65535

Close More options

Save Cancel Edit Add Delete Previous Next

ETHERNET CRITERIA

Source MAC Address

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

Source MAC Wildcard Mask

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

Destination MAC Address

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

Destination MAC Wildcard Mask

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

EtherType (Hex)

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

EtherType Examples:

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

IP CRITERIA

Source IP Address

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

Source IP Wildcard Mask

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

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

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

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

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

Destination IP Address

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

Destination IP Wildcard Mask

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

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

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

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

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

IP Protocol Number

This parameter sets the Layer 3 IP packet header 'Protocol' field in the selected profile classification rule. This field defines the protocol used in the data portion of the IP datagram. The default setting is '-1' which means it will pass any protocol according to the 'Assigned Priority' selection.

The options in this field are:

- A single number e.g. '6' for only TCP traffic
- More than one number e.g. '1,6'
- A range of numbers e.g. '1-17'

Protocol number Examples:

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

TCP / UDP PORT CRITERIA

Source Range

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

Destination Range

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

Examples for TCP / UDP Port Numbers:

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

Router Mode Traffic Classification Settings

TRAFFIC CLASSIFICATION

Select	Order	Profile Name	Assigned Priority	Active
☐	1	Traffic Classification L3 Rule 1	Low	☒
☐	2	Traffic Classification L3 Rule 2	Medium	☒
☒	3	Traffic Classification L3 Rule 3	High	☒

[Save](#) [Cancel](#) [Edit](#) [Add](#) [Delete](#) [Delete All](#) [Move Up](#) [Move Down](#)
[Previous](#) [Next](#)

Ready Radio: Base Station [Logout ADMIN](#)

TRAFFIC CLASSIFICATION

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

Profile name

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

Assigned Priority

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

Active

Activated or deactivate the profile rule.

Controls

The Save button saves all profiles to the radio.

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

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

The Add button adds a new profile,

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

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

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

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

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

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

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

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

ETHERNET PORT CRITERIA

Ethernet Port

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

PRIORITY CRITERIA

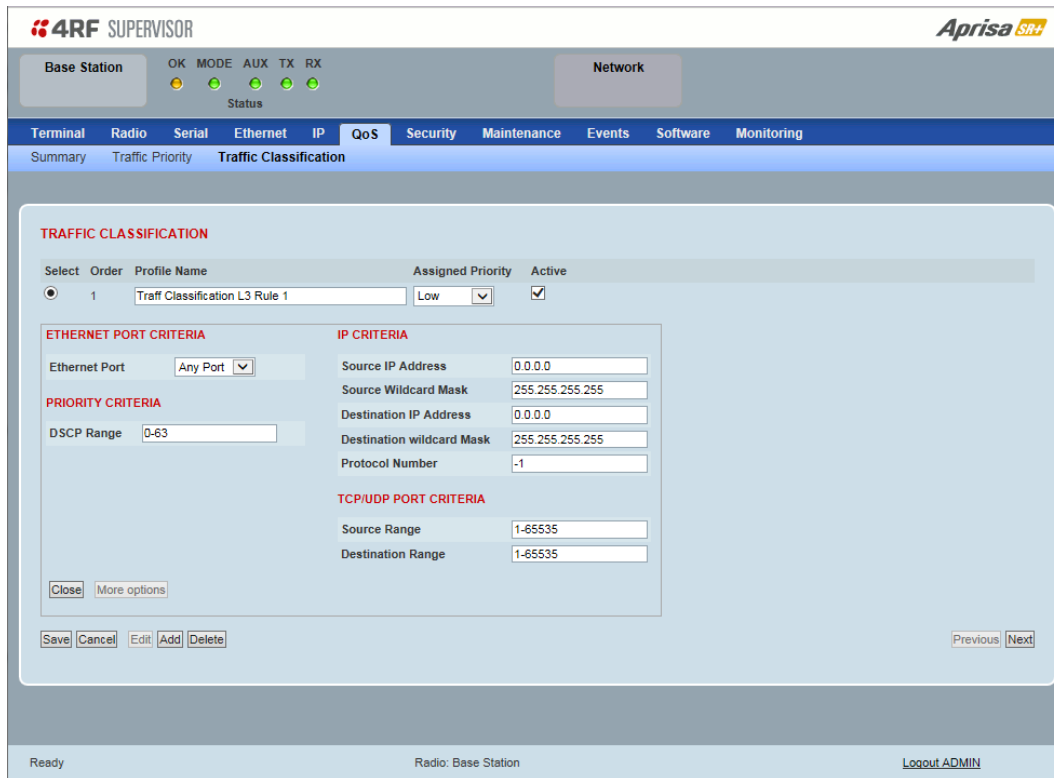
DSCP Range

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

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

DSCP Value (Decimal)	DSCP Priority
46	EF (Expedited Forwarding)
10	AF11 (Assured Forwarding)
12	AF12
14	AF13
18	AF21
20	AF22
22	AF23
26	AF31
28	AF32
30	AF33
34	AF41
36	AF42
38	AF43
0	CS0/Best Effort (BE)
8	CS1 (Class Selector)
16	CS2
24	CS3
32	CS4
40	CS5
48	CS6
56	CS7

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



IP CRITERIA

Source IP Address

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

Source IP Wildcard Mask

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

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

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

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

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

Destination IP Address

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

Destination IP Wildcard Mask

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

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

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

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

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

Protocol Number

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

Protocol number Examples:

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

TCP / UDP Port Criteria

Source Range

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

Destination Range

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

Examples for TCP / UDP Port Numbers:

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

Security

Security > Summary

This page displays the current settings for the Security parameters.

4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Network

Status

Terminal Radio Serial Ethernet IP QoS **Security** Maintenance Events Software Monitoring

Summary Setup Users SNMP RADIUS Manager Distribution

CURRENT PAYLOAD SECURITY SETTINGS

Security Profile Name	Migrated Key
Security Scheme	Disabled
Payload Encryption Key Type	Raw Hexadecimal (AES-128)

PREVIOUS PAYLOAD SECURITY SETTINGS

Security Profile Name	Inactive Payload Security
Security Scheme	Disabled
Payload Encryption Key Type	Passphrase

PREDEFINED PAYLOAD SECURITY PROFILE SETTINGS

Security Profile Name	Payload Security v22
Security Scheme	Disabled
Payload Encryption Key Type	Passphrase (AES-128)

PAYLOAD KEY ENCRYPTION KEY SETTINGS

Key Encryption Key Type	Passphrase (AES-256)

PROTOCOL SECURITY SETTINGS

Telnet	Enabled
ICMP	Enabled
HTTPS	Enabled
SNMP Protocol	All Versions
SNMP Proxy Support	Disabled
SSH	Enabled
SSH Key Status	SSH Keys Valid
SSH Public Key	View Public Key
Network Extension Mode	Disabled

SECURITY LEVEL SETTINGS

Security Level	Standard

Ready Radio: Base Station [Logout ADMIN](#)

See 'Security > Setup' and 'Security > Manager' for configuration options.

View Public Key Button

This button displays the current public SSH key which can then be copied to the SSH client.

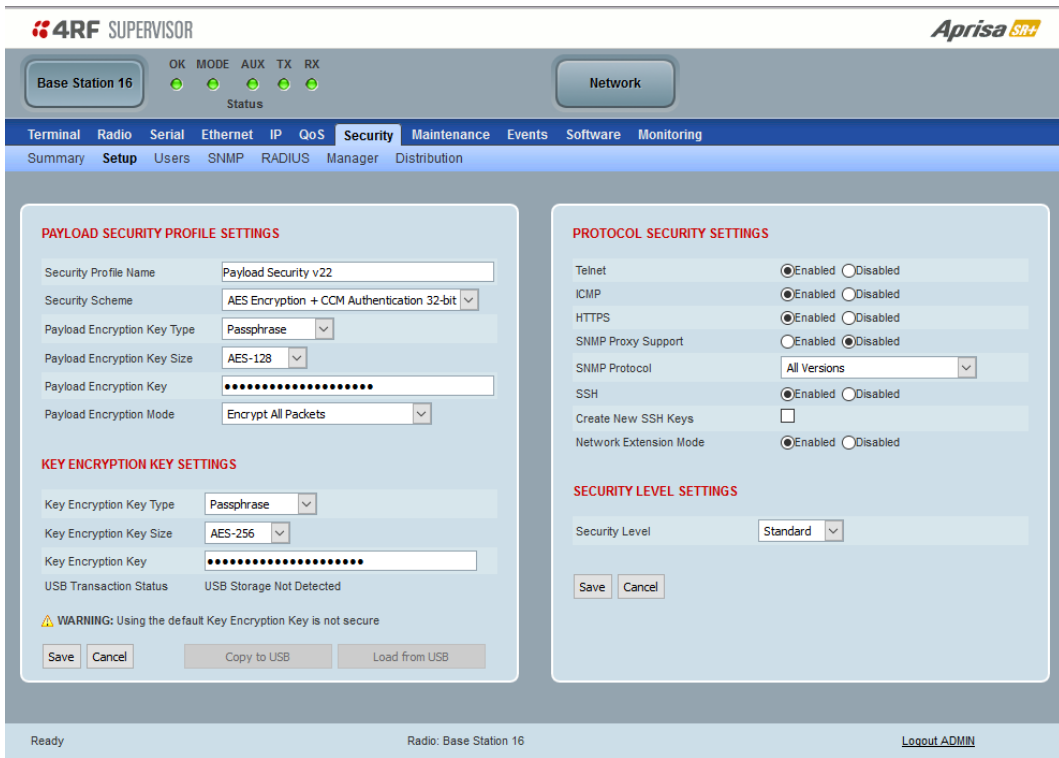
SSH Public Key

```

AAAAB3NzaC1yc2EAAAADAQABAAQCT2cF/0IU9zW+1wUjDP0QpxQLbwjNGZVLor1Y1voA
zskA3sqqSTIIJyUG0qvTn4kQwrIs4Hbhr/UEA6Kq2ed1zXQd5gpxBzkV3ZF7cTb6gFjEtcH
YR1/utEUXjczJPyatQFm4pDuVt5kpV4FUJDSF0CM7E5aH8jxP+YKQXptf+6xbmvN2EC1sm
5+OBdynYbcxWHUn1wo0ccARchZqGqATpmR3mIYgNXmx4nbS46siNFWWhY1cxfnJHgyJzatD
RVcI9EMQpMSLbvOKureqqzvQg13MQ89WG9vJ8ExyfbEh4i1pLtskIS8s8+mm+4XADyVfPd
Rbs+I7BGk6BE5Ss4B
  
```

[Copy](#) [Ok](#)

Security > Setup



PAYLOAD SECURITY PROFILE SETTINGS

Security Profile Name: Payload Security v22

Security Scheme: AES Encryption + CCM Authentication 32-bit

Payload Encryption Key Type: Passphrase

Payload Encryption Key Size: AES-128

Payload Encryption Key:

Payload Encryption Mode: Encrypt All Packets

KEY ENCRYPTION KEY SETTINGS

Key Encryption Key Type: Passphrase

Key Encryption Key Size: AES-256

Key Encryption Key:

USB Transaction Status: USB Storage Not Detected

WARNING: Using the default Key Encryption Key is not secure

Save Cancel Copy to USB Load from USB

PROTOCOL SECURITY SETTINGS

Telnet: ☒ Enabled ☐ Disabled

ICMP: ☒ Enabled ☐ Disabled

HTTPS: ☒ Enabled ☐ Disabled

SNMP Proxy Support: ☐ Enabled ☒ Disabled

SNMP Protocol: All Versions

SSH: ☒ Enabled ☐ Disabled

Create New SSH Keys: ☐

Network Extension Mode: ☒ Enabled ☐ Disabled

SECURITY LEVEL SETTINGS

Security Level: Standard

Save Cancel

Ready Radio: Base Station 16 Logout ADMIN

PAYLOAD SECURITY PROFILE SETTINGS

Security Profile Name

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

Security Scheme

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

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

The default setting is Disabled.

Payload Encryption Key Type

This parameter sets the Payload Encryption Key Type:

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

The default setting is Pass Phrase.

Payload Encryption Key Size

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

The higher the encryption size the better the security.

Payload Encryption Key

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

Pass Phrase

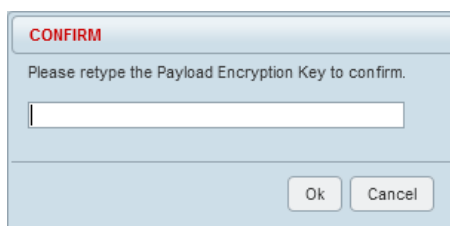
Good password policy:

- 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, 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 Hexadecimal

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

When the Payload Encryption Key is changed, you will be prompted for confirmation of the key to avoid mistypes.



Payload Encryption Mode

This parameter sets the Payload Encryption Mode:

Option	Function
Encrypt All Packets	Encrypts all payload packets
Exclude IPSEC Packet Re-encryption	Excludes radio encryption of already encrypted IPsec packets. This improves throughput for already encrypted traffic because the radio encryption overhead is not added to each packet. Radio encryption is still added for unencrypted user packets

The default setting is Encrypt All Packets.

KEY ENCRYPTION KEY SETTINGS

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

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

Key Encryption Key Type

This parameter sets the Payload Encryption Key Type:

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

The default setting is Pass Phrase.

Key Encryption Key Size

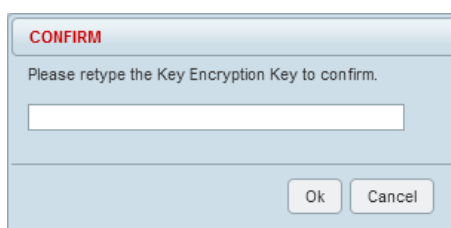
This parameter sets the Encryption Type to AES128, AES192 or AES256. The default setting is AES128.

The higher the encryption type the better the security.

Key Encryption Key

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

When the Key Encryption Key is changed, you will be prompted for confirmation of the key to avoid mistypes.



USB Transaction Status

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

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

Note: 4RF radios only support the FAT32 file system for flash drives. If the flash drive is a different format such as exFAT or NTFS, you will need to reformat it to FAT32.

Also, some brands of USB flash drives may not work with 4RF radios.

Controls

The 'Save' button saves the Key Encryption Key settings to the radio. If the Security Level is set to 'Strong' (see 'Security Level' on page 236), this button will be grayed out.

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

The 'Copy To USB' button copies the Key Encryption Key settings to a file called 'asrkek.txt' on the USB flash drive. This settings file can be used to load into other radios. If a USB flash drive is not detected or the Security Level is set to 'Strong' (see 'Security Level' on page 236), this button will not be shown.

Key Encryption Key Summary

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

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

PROTOCOL SECURITY SETTINGS

Telnet option

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

ICMP option (Internet Control Message Protocol)

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

HTTPS option

This parameter option determines if you can manage the radio via a HTTPS session (via a Browser). The default setting is disabled (see 'certificate' CLI commands for managing HTTPS certificates on page 397).

SNMP Proxy Support

This parameter option enables an SNMP proxy server in the base station. This option allows only SNMP transactions (SETs and GETs) to retrieve SNMP objects from remote radios via its base station (particularly when remote management was disabled on the base).

This option applies to the base station only but can also be used if the radio has Serial Only interfaces. The default setting is disabled.

Note: This feature does not report any OID changes and does not reduce the radio link bandwidth used for SNMP transactions.

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 (as per table below).
SNMPv3 With Encryption and Authentication	Only SNMPv3 transactions authenticated using HMAC-MD5 or HMAC-SHA with an encrypted type of DES or AES will be accepted (as per table below).

The default setting is All Versions.

The default SNMPv3 with Authentication User Details provided are:

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

SNMPv3 Authentication Passphrase

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

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

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

Generate New Keys from SNMPv3 USM User Passphrases

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

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

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

To change a user authentication passphrase:

The following are examples of:

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

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

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

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

Changing the desUserSHA user encryption key / password from desUserSHA to desUserSHANew:

```
c:\usr\bin>snmpusm -v 3 -u desUserSHA -n priv -l authPriv -a SHA -A desUserSHA -x DES -X desUserSHA  
-Cx 172.17.70.17 passwd desUserSHA desUserSHANew
```

Changing the desUserSHA user authentication key / password from desUserSHA to desUserSHANew:

```
c:\usr\bin>snmpusm -v 3 -u desUserSHA -n priv -l authPriv -a SHA -A desUserSHA -x DES -X  
desUserSHANew -Ca 172.17.70.17 passwd desUserSHA desUserSHANew
```

Changing the privUserMD5 user encryption key / password from privUserMD5 to privUserMD5New:

```
c:\usr\bin>snmpusm -v 3 -u privUserMD5 -n priv -l authPriv -a MD5 -A privUserMD5 -x AES -X privUserMD5  
-Cx 172.17.70.17 passwd privUserMD5 privUserMD5New
```

Changing the privUserMD5 user authentication key / password from privUserMD5 to privUserMD5New:

```
c:\usr\bin>snmpusm -v 3 -u privUserMD5 -n priv -l authPriv -a MD5 -A privUserMD5 -x AES -X  
privUserMD5New -Ca 172.17.70.17 passwd privUserMD5 privUserMD5New
```

Changing the desUserMD5 user encryption key / password from desUserMD5 to desUserMD5New:

```
c:\usr\bin>snmpusm -v 3 -u desUserMD5 -n priv -l authPriv -a MD5 -A desUserMD5 -x DES -X desUserMD5  
-Cx 172.17.70.17 passwd desUserMD5 desUserMD5New
```

Changing the desUserMD5 user authentication key / password from desUserMD5 to desUserMD5New:

```
c:\usr\bin>snmpusm -v 3 -u desUserMD5 -n priv -l authPriv -a MD5 -A desUserMD5 -x DES -X  
desUserMD5New -Ca 172.17.70.17 passwd desUserMD5 desUserMD5New
```

Changing the authUserSHA user authentication key / password from authUserSHA to authUserSHANew:

```
c:\usr\bin>snmpusm -v 3 -u authUserSHA -n auth -l authNoPriv -a SHA -A authUserSHA -Ca 172.17.70.17  
passwd authUserSHA authUserSHANew
```

Changing the authUserMD5 user authentication key / password from authUserMD5 to authUserMD5New:

```
c:\usr\bin>snmpusm -v 3 -u authUserMD5 -n auth -l authNoPriv -a MD5 -A authUserMD5 -Ca 172.17.70.17  
passwd authUserMD5 authUserMD5New
```

Notes

-Cx option is to change the Encryption key/password

-Ca option is to change the Authentication key/password

Other information on this utility can be obtained from the utility command help itself or online

Summary

It is necessary to record the new passphrases loaded into the Aprisa SR+ radios and then load the passphrases into the SNMP manager. There is a separate passphrase for the two supported forms of authentication (MD5 and SHA1) only as well as the two forms of authentication used in combination the two forms of encryption (DES and AES). It is vital to change all passphrases even if the depreciated mechanism is not used (MD5 and DES) otherwise an attacker could still use the default passphrases.

Reset SNMPv3 Unknown Passphrases with a CLI command

As it is not possible for users to read previously set passphrases, a CLI command is available from Aprisa SR+ software release 1.4.0 to 'reset' the SNMPv3 USM users back to defaults.

Note: USM users are not related to CLI and SuperVisor users. This command will only be accessible to the CLI 'admin' user logins.

To reset unknown passphrases:

1. Telnet into each radio in the network and via the CLI reset the passphrases
2. Login to the radio with:
 Login: admin
 Password: *****
3. Set all SNMP3 users to default values with the 'snmpusm reset' command (see 'SNMP3 users to default values' below for the list of default values).
4. Reboot the radio with the 'reboot' command.

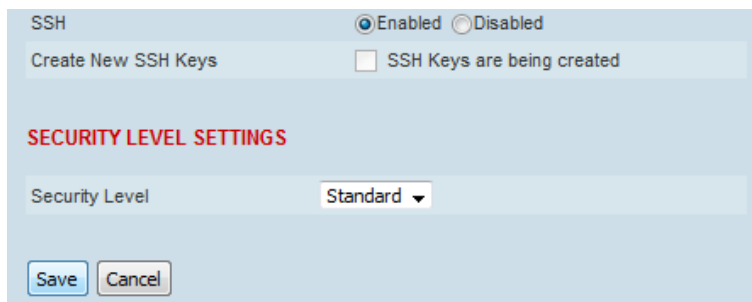
SSH

This parameter enables / disables Secure Shell (SSH). The default setting is enabled.

Create New SSH Keys

This parameter creates a replacement public and private SSH keys.

Tick the check box and click Save. This process can take a few minutes.



The image shows a web-based configuration interface for SSH. At the top, there is a section labeled 'SSH' with two radio buttons: 'Enabled' (selected) and 'Disabled'. Below this is a section labeled 'Create New SSH Keys' with a checkbox labeled 'SSH Keys are being created'. Underneath is a section titled 'SECURITY LEVEL SETTINGS' in red. It contains a label 'Security Level' and a dropdown menu currently set to 'Standard'. At the bottom of the form are two buttons: 'Save' and 'Cancel'.

Network Extension Mode

This parameter enables this radio to be part of the extended network radio list. The default setting is disabled.

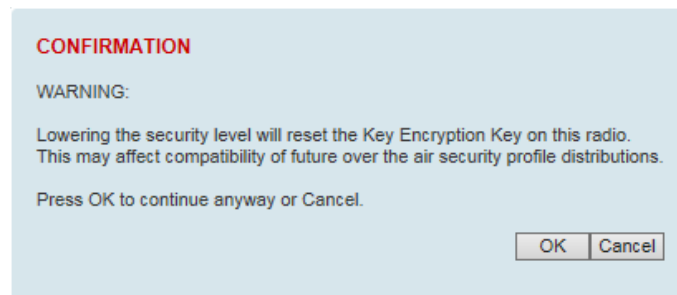
SECURITY LEVEL SETTINGS

Security Level

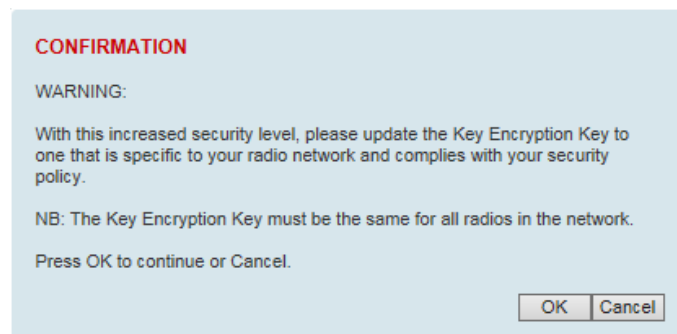
This parameter sets the Security Level active security features. The default setting is Standard.

Option	Payload Encryption	HTTPS	SNMPv3	USB KEK Only
Standard	✓	✓	✓	
Strong	✓	✓	✓	✓

If the Security Level is reduced, there will be a pop up message warning that Key Encryption Key will be reset to the default value.



If the Security Level is increased, there will be a pop up message reminding the user to enter a new Key Encryption Key.



If the Security Level is set to 'Strong', the 'Save' button on the Security > Setup page will be grayed out and the 'Copy To USB' button will not be shown. See 'Security > Setup' on page 226.

When the Security Level is set to 'Strong', the radio Key Encryption Key is used to encrypt a saved configuration file. If a saved configuration file encryption Key Encryption Key does not match the radio Key Encryption Key, the saved configuration will not be accepted / loaded. See 'File - Configuration Settings' on page 272.

SNMPv3/2c Context Addressing

This ‘SNMP Context Addressing’ technique is an implementation that compresses and utilizes a more efficient mechanism of managing communications with 4RF radios over the air within the same radio network.

SNMPv3 is not user configurable and user can use this option with any NMS. The radio SNMP management interface supports SNMPv3/2c context addressing. The SNMPv3 context addressing allows the user to use secure SNMPv3 management while improving NMS performance.

A NMS (Network Management System) can access any remote radio directly by using its IP address or via the base station SNMPv3 context addressing. The SNMPv3 context addressing can compress the SNMPv3 management traffic OTA (Over The Air) to the remote radio by up to 90% relative to direct OTA SNMPv3 access to remote radio, avoiding the radio narrow bandwidth traffic loading.

To use Context Addressing to communicate with a remote radio:

- Address the SNMP transaction to the base station i.e., use the base station’s IP address. If the base station is a protected station, target the IP address of the active radio, since targeting the standby radio will slow down the SNMP request and response as the active radio processes the context addressing messages.
- In the SNMP Context Name / Community String, use a string in the format of e.g., ‘public.runit_172.10.1.15’.
 - The ‘public’ portion is the actual community string that is required for the SNMP transaction
 - The ‘.’ is required to separate the remaining portion of the string
 - The ‘runit_’ portion is to indicate that a remote radio registered to the base station is being addressed
 - and the ‘172.10.1.15’ portion is the actual IP address of the remote radio

In this example, when the SNMP transaction is received by the base station, it is redirected to the specified remote radio using the SNMP context addressing protocol of communications. The response to the original SNMP transaction that was directed to the base station will contain the necessary information from the remote radio and will be in a standard format - appearing as a normal SNMP transaction response.

net-snmp command examples (where ‘SNMP Protocol=All Version’ at ‘Supervisor > Security > Setup’ page):

Example 1: Getting the Terminal Name (APRISASR-MIB: termName) - 1.3.6.1.4.1.14817.7.4.1.1.1.1.0 from a remote radio IP address 10.30.56.81 via Base station IP address 10.30.56.80.

```
snmpget -v2c -c public.runit_10.30.56.81 10.30.56.80 1.3.6.1.4.1.14817.7.4.1.1.1.1.0
```

Example 2: Getting the TX Power (RFCONFIG-MIB: rfConfigPowerOutputSet) - 1.3.6.1.4.1.14817.3.14.2.30.0

```
snmpget -v2c -c public.runit_10.30.56.81 10.30.56.80 1.3.6.1.4.1.14817.3.14.2.30.0
```

Example 3: Reading the IP address

```
snmpget -v2c -c "public.runit_172.17.70.32" 172.17.70.31 1.3.6.1.4.1.14817.7.4.1.1.4.1.1.0
```

Example 4 : Reading the IP address using SNMPv3

```
snmpget -v3 -u privUserSHA -n "priv.runit_172.17.70.32" -l authPriv -a SHA -A privUserSHA -x AES -X privUserSHA 172.17.70.31 1.3.6.1.4.1.14817.7.4.1.1.4.1.1.0
```

Example 5: SNMPWALK

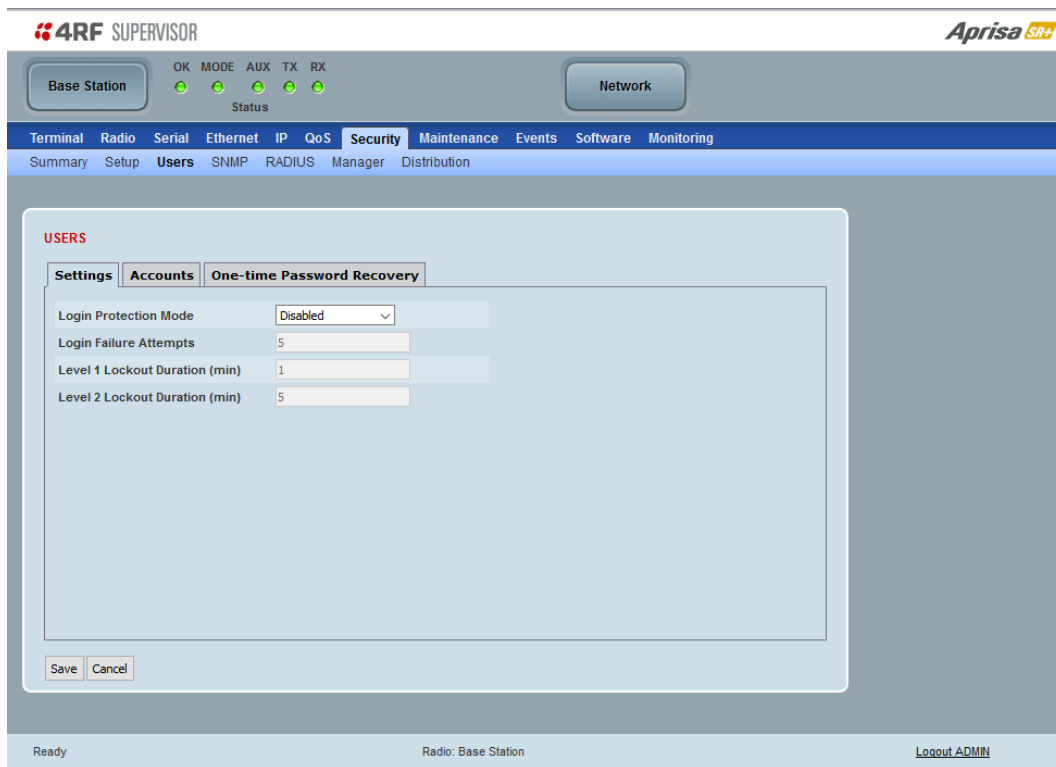
```
snmpwalk -v2c -c public.runit_10.30.56.81 10.30.56.80 1.3.6.1.4.1.14817.7
```

Example 6: SNMPWALK using retry and timeout parameters

```
snmpwalk -r1 -t5 -v2c -c public.runit_10.30.56.81 10.30.56.80 1.3.6.1.4.1.14817.7
```

Security > Users

Settings



Login Protection Mode

This parameter sets the Login Protection Mode. They provide user account lockout mechanisms to mitigate brute force password guessing attacks.

Option	Function
Disabled	Disables login protection
Attack Slowdown	In this mode, the user account will be locked out for the duration specified in Level 1 Lockout Duration and Level 2 Lockout Duration, cycling between the two. This mode slows down attacks.
Attack Lockout	In this mode, the user account will be permanently locked out if the protection mechanism has reached Locked Level 1 and Locked Level 2 and the next login attempt fails. The user account must then be manually unlocked by an 'Admin' user account either from SuperVisor or via SNMP. This mode blocks persistent attacks.

Attack Slowdown

The Attack Slowdown login protection lockout mechanism will be processed as follows:

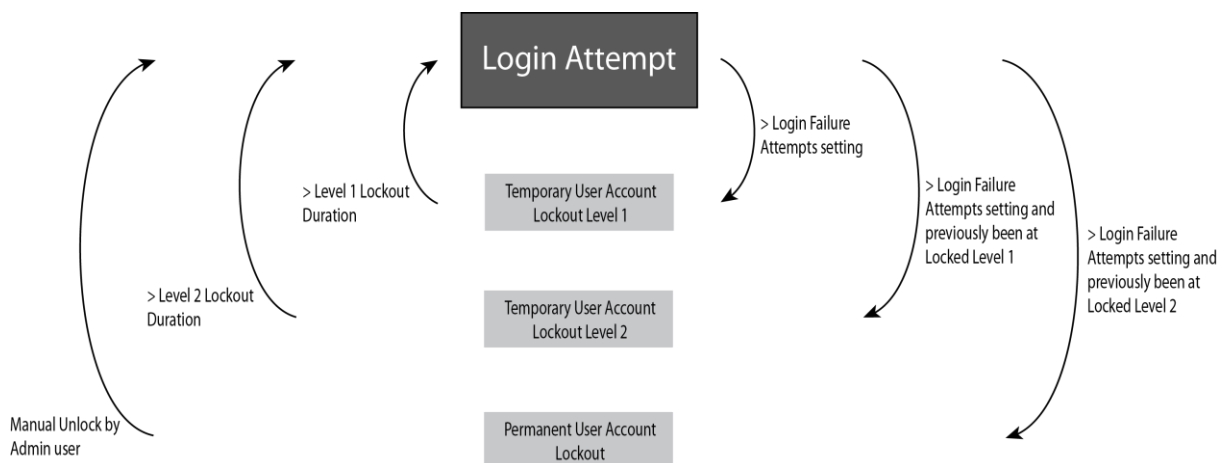
- When the number of login failure attempts is less than the setting of the 'Login Failure Attempts' field, the login attempt is processed.
- When the number of login failure attempts is greater than the setting of the 'Login Failure Attempts' field, the user account will be:
 - temporarily disabled at level 1 for the 'Level 1 Lockout Duration' period, if the user account was not previously already released from locked level 2.
 - temporarily disabled at level 2 for the 'Level 2 Lockout Duration' period, if the user account was previously already released from locked level 1.

This lockout mode will cycle the lockout of the accounts between locked level 1 and locked level 2.

Attack Lockout

The Attack Lockout login protection lockout mechanism will be processed as follows:

- When the number of login failure attempts is less than the setting of the 'Login Failure Attempts' field, the login attempt is processed.
- When the number of login failure attempts is greater than the setting of the 'Login Failure Attempts' field, the user account will be:
 - temporarily disabled at level 1 for the 'Level 1 Lockout Duration' period, if the user account was not previously already released from locked level 1.
 - temporarily disabled at level 2 for the 'Level 2 Lockout Duration' period, if the user account was previously already released from locked level 1.
 - permanently disabled if the user account was previously already released from locked level 2. The user account must then be manually unlocked by an 'Admin' user account either from SuperVisor or via SNMP.



Login Failure Attempts

When Login Protection Mode is active, this parameter sets the maximum number of consecutive failed login attempts before the relevant user account lockout process is initiated. This field can be set from 3 to 10 times and the default value is 5.

Level 1 Lockout Duration (min)

When Login Protection Mode is active and the user account is in the state of 'locked level 1', the user account will be locked out for the duration specified. This field can be set from 1 to 15 minutes and the default value is 1 minute.

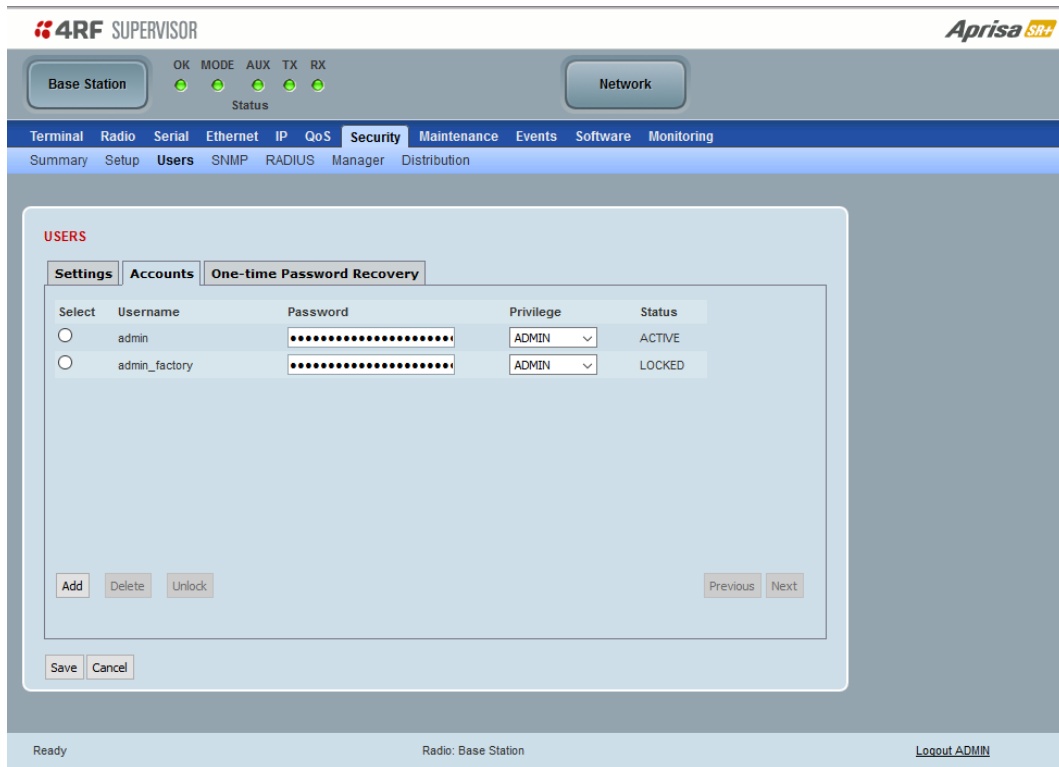
A user account in the state of 'locked level 1' shall be unlocked and put in the released from level 1 lockout state after this level 1 lockout duration has expired.

Level 2 Lockout Duration (min)

When Login Protection Mode is active and the user account is in the state of 'locked level 2', the user account will be locked out for the duration specified. This field can be set from 5 to 30 minutes and the default value is 5 minutes.

A user account in the state of 'locked level 2' shall be unlocked and put in the released from level 2 lockout state after this level 2 lockout duration has expired.

Accounts



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Network

Status

Terminal Radio Serial Ethernet IP QoS **Security** Maintenance Events Software Monitoring

Summary Setup **Users** SNMP RADIUS Manager Distribution

USERS

Settings Accounts **One-time Password Recovery**

Select	Username	Password	Privilege	Status
☐	admin		ADMIN	ACTIVE
☐	admin_factory		ADMIN	LOCKED

Add Delete Unlock Previous Next

Save Cancel

Ready Radio: Base Station Logout ADMIN

Note: You must login with 'admin' privileges to add, disable, delete a user or change a password.

Shows a list of the current user accounts setup in the radio.

To add a new user:

1. Click Add.

If the currently viewed page is full (displaying 8 user accounts), SuperVisor shall automatically display the last user account page when a new user is added. However, if there are unsaved changes on the current page, the user shall be prompted to save the changes first before adding a new user.

2. Enter the Username.

A username can be 8 to 32 characters but cannot contain tabs. Usernames are case sensitive.

3. Enter the Password.

A password can be 8 to 32 printable characters but cannot contain tabs. Passwords are case sensitive.

Good password policy:

- contains at least one upper case letter, and
- contains at least one lower case letter, and
- contains at least one digit, and
- is not a term in a familiar language or jargon, and
- is not identical to or derived from the accompanying account name, from personal characteristics or from information from one's family/social circle, and
- is easy to remember, for instance by means of a key sentence

4. Select the User Privileges

There are four pre-defined User Privilege settings to allocate access rights to users. These user privileges have associated default usernames and passwords of the same name.

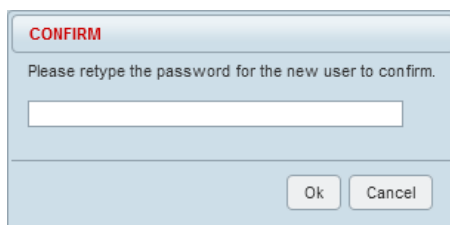
The default login is 'admin'.

This login has full access to all 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			Users in this group can only view the summary pages.
Technician			Users in this group can view and edit parameters except Security > Users and Security > Setup.
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' on page 100 for the list of SuperVisor menu items versus user privileges.

When the password is changed, you will be prompted for confirmation of the password to avoid mistypes.



The Status will show PENDING until the entry is saved.

5. Click Save.

Status

The Status indicates whether a user account is active or locked out.

Option	Function
ACTIVE	The user account is currently active.
PENDING	The user account has been entered but not saved.
LOCKED (Level 1)	Login Protection Mode is active and the user account has been locked out due to repeated unsuccessful login attempts. The account will remain locked out for a period defined in 'Level 1 Lockout Duration' at the 'Security > Users' > Settings tab.
LOCKED (Level 2)	Login Protection Mode is active and the user account has been locked out due to repeated unsuccessful login attempts. The account will remain locked out for a period defined in 'Level 2 Lockout Duration' at the 'Security > Users' > Settings tab.
LOCKED	Login Protection Mode is active and the user account has been locked out due to repeated unsuccessful login attempts. The user account is permanently locked out.

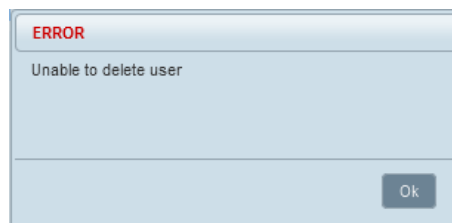
This tab shall also provide the interface for the ADMIN user to unlock any locked user accounts.

The 'Unlock' button shall be disabled unless a locked account is selected, in which case, clicking the button will unlock the selected account.

To 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'
4. Click Save.

The user can delete any user account as long as there is at least one ADMIN account left on the radio. If the user attempts to delete the last ADMIN account on the radio (and click Save), an error popup shall be displayed.

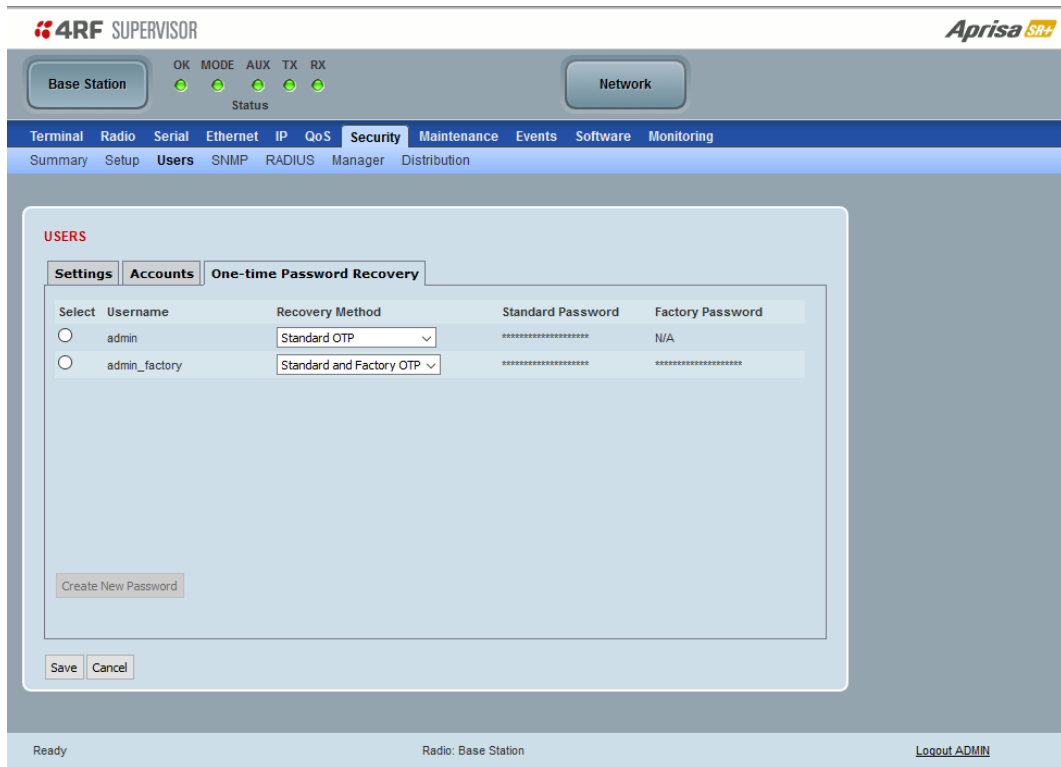


To change a Password:

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.
4. Click Save.

A password can be 8 to 32 characters but cannot contain tabs.

One-time Password Recovery



The screenshot shows the 4RF SUPERVISOR web interface. The top navigation bar includes 'Base Station' and 'Network' buttons, along with status indicators for OK, MODE, AUX, TX, and RX. The main menu includes 'Terminal', 'Radio', 'Serial', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. The 'Security' menu is expanded, showing 'Summary', 'Setup', 'Users', 'SNMP', 'RADIUS', 'Manager', and 'Distribution'. The 'Users' page is active, and the 'One-time Password Recovery' tab is selected. The table below shows the recovery methods for the 'admin' and 'admin_factory' users.

Select	Username	Recovery Method	Standard Password	Factory Password
☐	admin	Standard OTP	*****	N/A
☐	admin_factory	Standard and Factory OTP	*****	*****

Buttons at the bottom include 'Create New Password', 'Save', and 'Cancel'. The status bar at the bottom shows 'Ready', 'Radio: Base Station', and a 'Logout ADMIN' link.

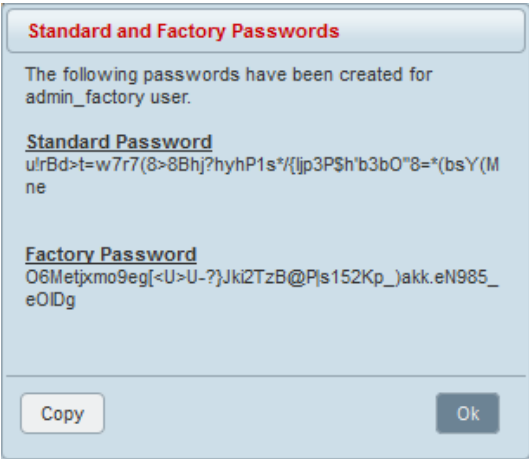
The One-time Password Recovery is a future proofing mechanism that allows an Admin user access to change the Admin password if the Admin user is permanently locked out or the Admin password is unknown. OTP passwords can be entered on this page and then saved in a text file for future use.

If these passwords are used to login to a radio, the password is immediately changed so it can't be used again.

Recovery Method

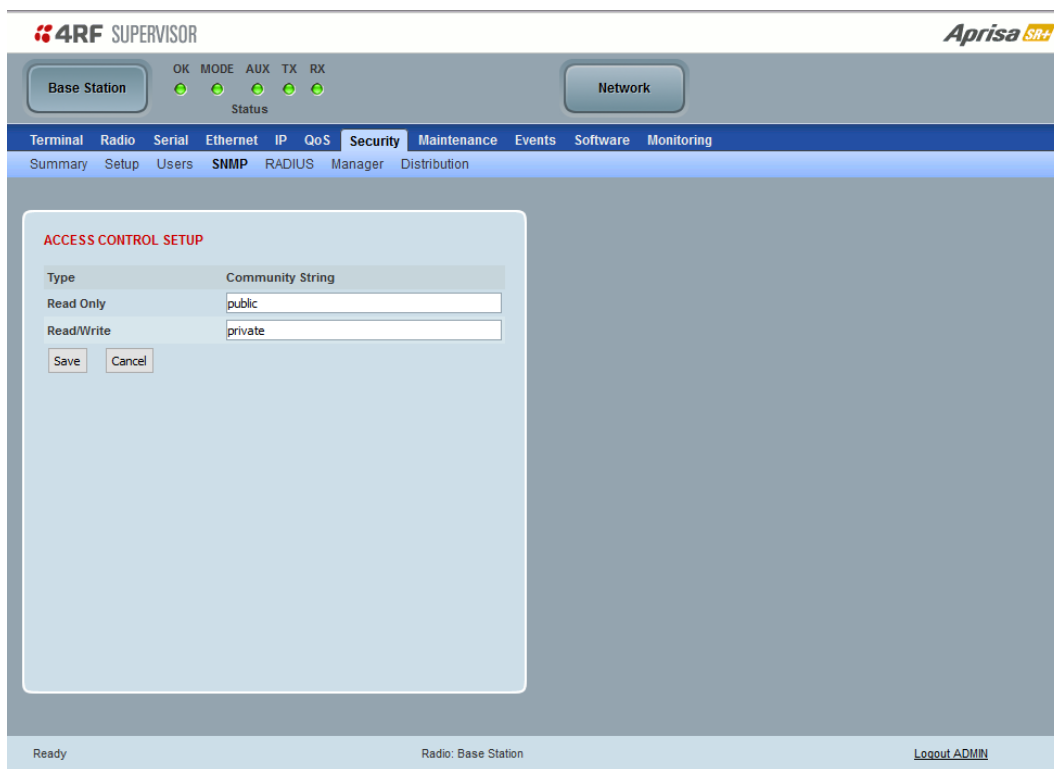
Option	Function
Standard OTP	Using the 'Standard OTP' password when logging into a radio, allows the user to change the radio Admin password so it can then be used to login and access the radio.
Standard and Factory OTP	Using the 'Standard and Factory OTP password' when logging into a radio, allows the user to change the radio Admin password BUT also restores the entire radio to Factory Defaults so be careful using this!

Whenever new passwords are generated for a user, a popup box shall be displayed with the new passwords in clear text.



The Copy button copies the generated passwords to the clipboard, for storage in a text file for future use.

Security > SNMP



ACCESS CONTROL SETUP

Type	Community String
Read Only	public
Read/Write	private

Save Cancel

In addition to web-based management (SuperVisor), the network can also be managed using the Simple Network Management Protocol (SNMP) using any version of SNMP v1/2/3. MIB files are supplied, and these can be used by a dedicated SNMP Manager, such as Castle Rock's SNMPC, to access most of the radio's configurable parameters.

For communication between the SNMP manager and the radio, Access Controls and Community strings must be set up as described in the following sections.

A **SNMP Community String** is used to protect against unauthorized access (similar to a password). The SNMP agent (radio or SNMP manager) will check the community string before performing the task requested in the SNMP message.

ACCESS CONTROL SETUP

A **SNMP Access Control** is the IP address of the radio used by an SNMP manager or any other SNMP device to access the radio. The Aprisa SR+ allows access to the radio from any IP address.

Read Only

The default Read Only community string is public.

Read Write

The default ReadWrite community string is private.

SNMP Manager Setup

The SNMP manager community strings must be setup to access the base station and remote / repeater stations.

To access the base station, a community string must be setup on the SNMP manager the same as the community string setup on the radio (see 'Security > SNMP' on page 247).

SNMP access to remote / repeater stations can be achieved by using the radio's IP address and the normal community string or by proxy in the base station.

SNMP Access via Base Station Proxy

To access the remote / repeater stations via the base station proxy, the community strings must be setup on the SNMP manager in the format:

`cccccccc:bbbbbb`

Where:

`cccccccc` is the community string of the base station

and

`bbbbbb` is the last 3 bytes of the remote radio MAC address (see 'Network Status > Network Table' on page 333).

The SNMP Proxy Support must be enabled for this method of SNMP access to operate (see 'SNMP Proxy Support' on page 231).

Security > RADIUS

This page displays the current settings for the Security RADIUS.

4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Status Network

Terminal Radio Serial Ethernet IP QoS **Security** Maintenance Events Software Monitoring

Summary Setup Users SNMP **RADIUS** Manager Distribution

RADIUS AUTHENTICATION SETTINGS

Authentication Mode: Local Authentication

Primary Server: None

Secondary Server: None

RADIUS ACCOUNTING SETTINGS

Primary Server: None

Secondary Server: None

RADIUS ADVANCED SETTINGS

Initial Transaction Timeout(s): 4

Default Transaction Timeout(s): 16

Maximum Retries: 5

Maximum Retries Duration (s): 30

Unknown Transaction Attributes: Ignore And Authenticate

Save Cancel

RADIUS SERVER SETTINGS

Server Name	IP Address	Port Number	Encryption Key
1 Radius Server 1	0.0.0.0	1812	
2 Radius Server 2	0.0.0.0	1812	
3 Radius Server 3	0.0.0.0	1813	
4 Radius Server 4	0.0.0.0	1813	

Save Cancel

Ready Radio: Base Station [Logout ADMIN](#)

RADIUS - Remote Authentication Dial In User Service

RADIUS is a client / server system that secures the radio link against unauthorized access. It is based on open standard RFCs: RFC 2865/6, 5607, 5080 and 2869. It is used for remote user Authorization, Authentication and Accounting.

When a user logs into a radio with RADIUS enabled, the user's credentials are sent to the RADIUS server for authentication of the user.

Transactions between the RADIUS client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network.

For a RADIUS server to respond to the radio, it must be configured with the following **Management-Privilege-level** attributes:

- Admin Level = 4
- Engineer Level = 3
- Technician Level = 2
- Viewer Level = 1

Alternatively, for Admin level only, for a RADIUS server to respond to the radio, it must be configured with attributes Service-Type (6) = Administrative (6) which will grant the user admin access to the radio.

A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

RADIUS AUTHENTICATION SETTINGS

Authentication Mode

This parameter sets the Authentication Mode.

Option	Function
Local Authentication	No radius Authentication - allows any local user privilege All user login attempts are authenticated against local accounts only.
Radius Authentication	Only radius Authentication - no local user privilege All user login attempts are authenticated against the Radius server accounts only.
Radius Authentication and Local admin	All user login attempts are first authenticated against the Radius server accounts. If the authentication fails, it is then authenticated against local admin accounts only.
Radius Then Local Authentication	All user login attempts are first authenticated against the Radius server accounts. If the authentication fails, it is then authenticated against local accounts.
Local Then Radius Authentication	All user login attempts are first authenticated against the local accounts. If the authentication fails, it is then authenticated against the Radius server accounts.
Radius Authentication with Local Fallback	All user login attempts are authenticated against the Radius server accounts unless the Radius server is not contactable. If unable to connect to the Radius server, only then it is authenticated against the local accounts.

Primary Server

This parameter sets which radius server is used as the primary server for authentication. Select one of the possible authentication servers setup in Radius Server Settings.

Secondary Server

This parameter sets which radius server is used as the secondary server for authentication. Select one of the possible authentication servers setup in Radius Server Settings.

RADIUS ACCOUNTING SETTINGS

Primary Server

This parameter sets which radius server is used as the primary server for accounting (log of user activity). Select one of the possible accounting servers setup in Radius Server Settings.

Secondary Server

This parameter sets which radius server is used as the secondary server for accounting. Select one of the possible accounting servers setup in Radius Server Settings.

RADIUS ADVANCED SETTINGS

Initial Transaction Timeouts (IRT) (seconds)

This parameter sets the initial time to wait before the retry mechanism starts when the server is not responding.

Default Transaction Timeouts (MRT) (seconds)

This parameter sets the maximum time between retries.

Maximum Retries (MRC)

This parameter sets the maximum number of retry attempts when the server is not responding.

Maximum Retries Duration (MRD) (seconds)

This parameter sets the maximum duration it will attempt retries when the server is not responding.

Unknown Transaction Attributes

This parameter sets the radio's response to unknown attributes received from the radius server.

Option	Function
Ignore and Authenticate	Ignore the unknown attributes and accept the authentication received from the radius server
Reject and Deny	Reject the authentication received from the radius server

RADIUS SERVER SETTINGS

Server Name

You can enter up to four radius servers 1-4.

IP Address

The IP address of the Radius server.

Port Number

The Port Number of the Radius server. RADIUS uses UDP as the transport protocol.

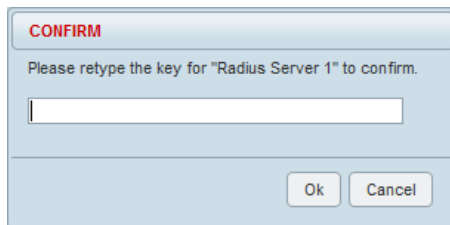
- UDP port 1812 is used for authentication / authorization
- UDP port 1813 is used for accounting.

Old RADIUS servers may use unofficial UDP ports 1645 and 1646.

Encryption Key

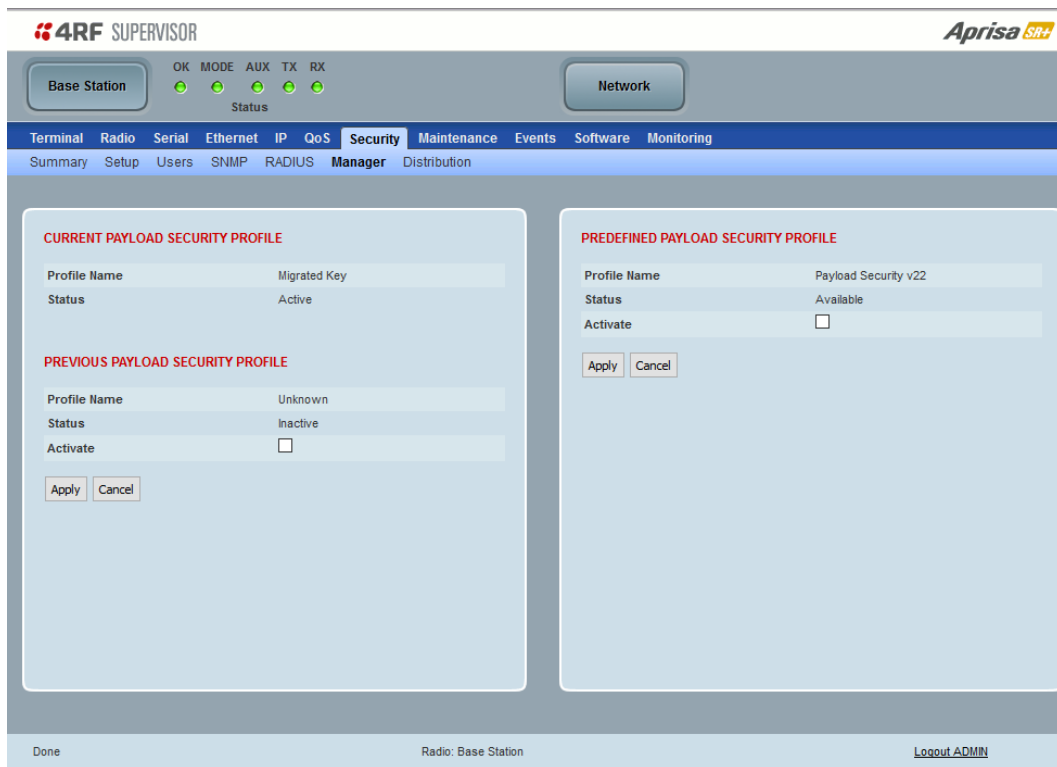
The password of the Radius server. This can include lower / upper case, numbers and special characters (~!@#\$%^&*()_+{|}) to be used in the encryption key.

When the password is changed, you will be prompted for confirmation of the password to avoid mistypes.



A confirmation dialog box with a light blue border. The title bar is red and contains the word "CONFIRM" in white. The main text area is white and contains the message "Please retype the key for 'Radius Server 1' to confirm." Below the text is a white text input field. At the bottom right, there are two buttons: "Ok" and "Cancel".

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 226.
Available	A predefined security profile is available on this radio for distribution and activation.

Security > Distribution

The screenshot shows the 4RF SUPERVISOR web interface. At the top, there's a status bar with 'Base Station' and 'Network' buttons, and a row of status indicators (OK, MODE, AUX, TX, RX) with green lights. Below this is a navigation menu with tabs: Terminal, Radio, Serial, Ethernet, IP, QoS, Security (selected), Maintenance, Events, Software, and Monitoring. Under the 'Security' tab, there's a sub-menu with 'Summary', 'Setup', 'Users', 'SNMP', 'RADIUS', 'Manager', and 'Distribution' (selected). The main content area is split into two panels. The left panel is titled 'REMOTE PAYLOAD SECURITY PROFILE DISTRIBUTION' and shows 'Predefined Profile Name' as 'Payload Security v22', 'Status' as 'Available', and a 'Start Transfer' checkbox which is unchecked. There are 'Apply' and 'Cancel' buttons at the bottom of this panel. A warning message states: 'WARNING: Using the default Key Encryption Key is not secure'. The right panel is titled 'REMOTE PAYLOAD SECURITY PROFILE ACTIVATION' and shows 'Profile Name' as 'Payload Security v22' and a 'Start Activation' button. At the bottom of the interface, there's a footer with 'Done', 'Radio: Base Station', and 'Logout ADMIN'.

REMOTE PAYLOAD SECURITY PROFILE DISTRIBUTION

Predefined Profile Name

This parameter displays the predefined security profile available for distribution to remote radios.

Status

This parameter shows if a predefined security profile is available for distribution to remote radios.

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 radios in the network.

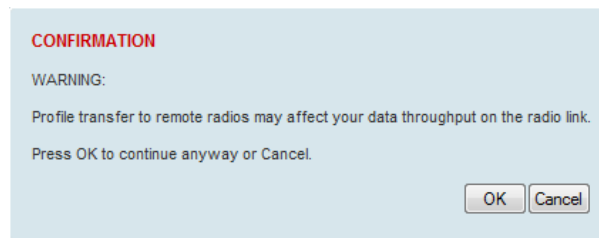
Note: The distribution of the payload security profile to remote radios does not stop customer traffic from being transferred.

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 radios:

This process assumes that a payload security profile has been setup (see 'Security > Setup' on page 226).

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 radios, the security profile is then activated in all the remote radios with this command.

The base station will always attempt to distribute the profile successfully. This broadcast distribution has its own retry mechanism. The user can find out if all the remote radios have the latest profile when the managed activation process is attempted. A pop up confirmation will be shown by SuperVisor with relevant information and the user can decide to proceed or not. The user can attempt to redistribute again if needed. If the decision is made to continue, on completion of the activation process, communication with the remote radios that did not have the new security profile will be lost.

Predefined Profile Name

This parameter displays the predefined security profile available for activation on all remote radios.

To activate the security profile in remote radios:

This process assumes that a security profile has been setup into the base station (see 'Security > Setup' on page 226) and distributed to all remote radios in the network.

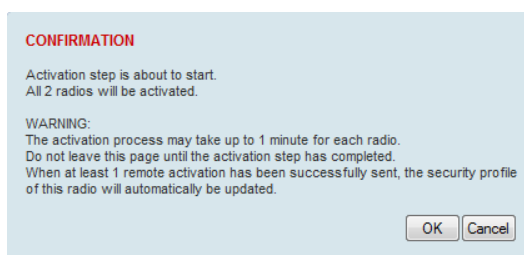
Note: Do not navigate SuperVisor away from this page during the activation process (SuperVisor can lose PC focus).

1. Click Start Activation

The remote radios 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:

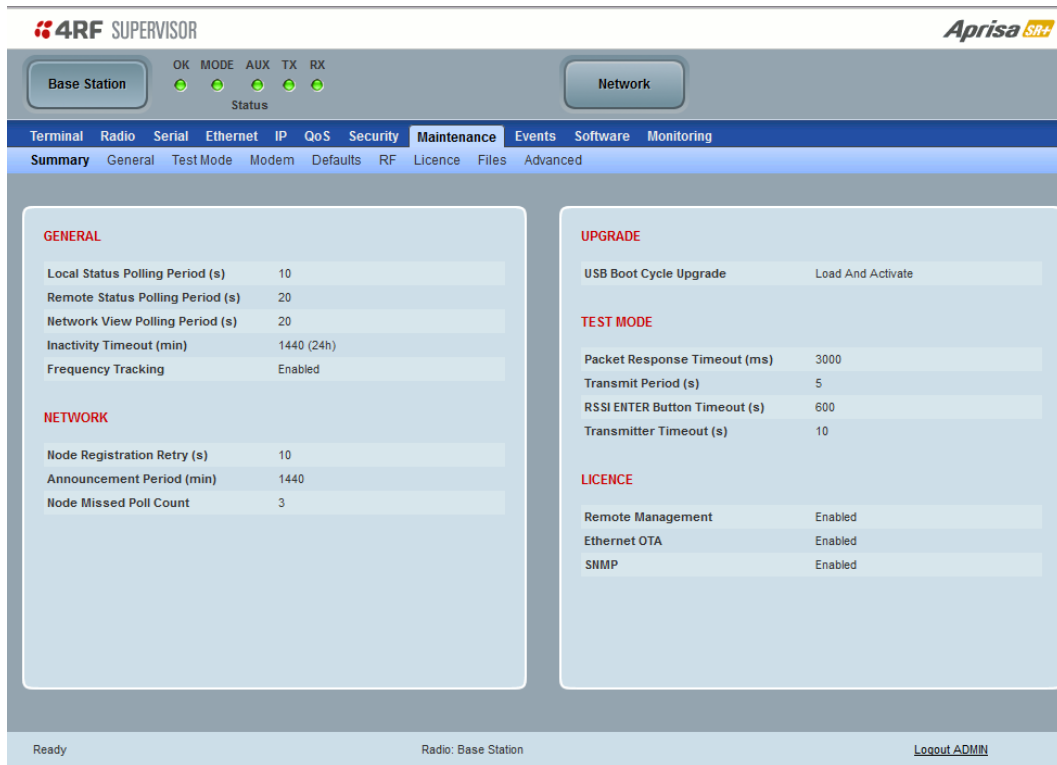


3. Click on 'OK' to start the activation process or Cancel to quit.

Maintenance

Maintenance > Summary

This page displays the current settings for the Maintenance parameters.



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Network

Status

Terminal Radio Serial Ethernet IP QoS Security **Maintenance** Events Software Monitoring

Summary General Test Mode Modem Defaults RF Licence Files Advanced

GENERAL

Local Status Polling Period (s)	10
Remote Status Polling Period (s)	20
Network View Polling Period (s)	20
Inactivity Timeout (min)	1440 (24h)
Frequency Tracking	Enabled

NETWORK

Node Registration Retry (s)	10
Announcement Period (min)	1440
Node Missed Poll Count	3

UPGRADE

USB Boot Cycle Upgrade	Load And Activate

TEST MODE

Packet Response Timeout (ms)	3000
Transmit Period (s)	5
RSSI ENTER Button Timeout (s)	600
Transmitter Timeout (s)	10

LICENCE

Remote Management	Enabled
Ethernet OTA	Enabled
SNMP	Enabled

Ready Radio: Base Station [Logout ADMIN](#)

GENERAL

Local Status Polling Period (sec)

This parameter displays the rate at which SuperVisor refreshes the Local Radio alarm LED states and RSSI value.

Remote Status Polling Period (sec)

This parameter displays the rate at which SuperVisor refreshes the Remote Radio alarm LED states and RSSI value.

Network View Polling Period (sec)

This parameter displays the rate at which SuperVisor polls all remote radios for status and alarm reporting.

Inactivity Timeout (min)

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

Frequency Tracking

This parameter displays if Frequency Tracking is enabled or disabled.

NETWORK

Node Registration Retry (sec)

This parameter displays the base station poll time at startup or the remote / repeater station time between retries until registered.

Announcement Period (min)

This parameter displays the period between base station announcement messages. The announcement messages are used to distribute the base station date and time to remote radios. The default setting is 1440 minutes (24 hours).

Node Missed Poll Count

This parameter displays the number of times the base station attempts to poll the network at startup or if a duplicate IP is detected when a remote / repeater station is replaced.

UPGRADE

USB Boot Cycle Upgrade

This parameter shows the type of USB Boot Cycle upgrade defined in 'Software Setup > USB Boot Upgrade' on page 294.

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.

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.

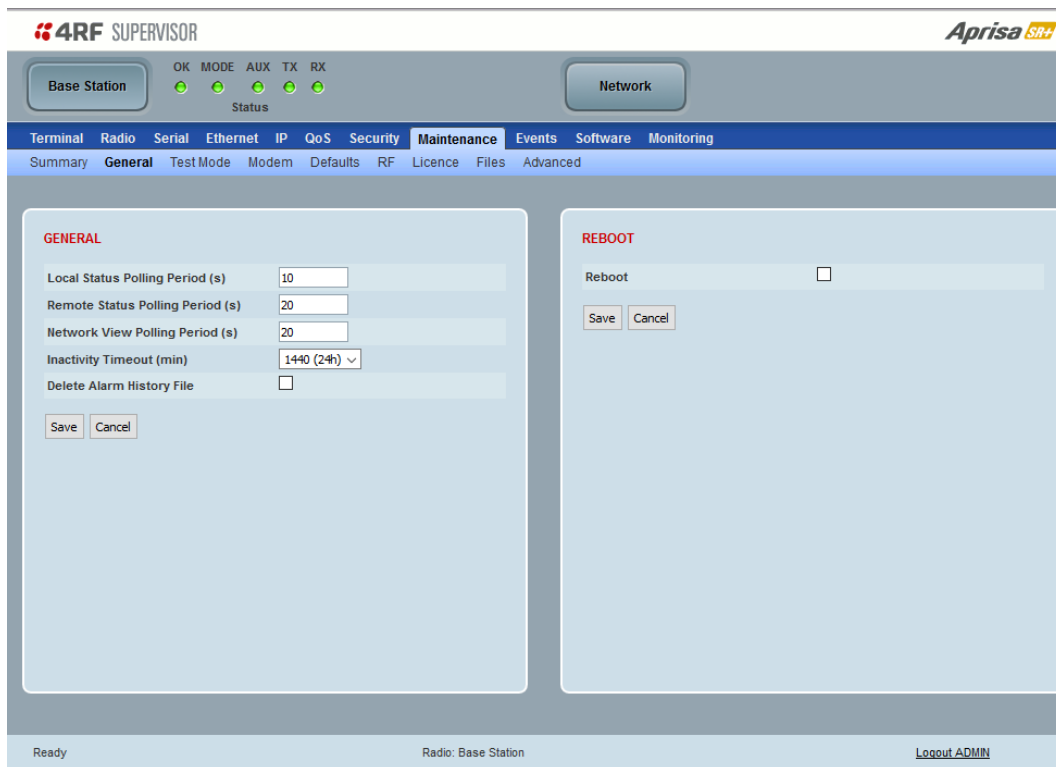
Ethernet OTA (over the air)

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 270).

SNMP Management

This parameter displays if SNMP management is enabled or disabled. The default setting is enabled.

Maintenance > General



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Network

Status

Terminal Radio Serial Ethernet IP QoS Security **Maintenance** Events Software Monitoring

Summary **General** Test Mode Modem Defaults RF Licence Files Advanced

GENERAL

Local Status Polling Period (s)

Remote Status Polling Period (s)

Network View Polling Period (s)

Inactivity Timeout (min)

Delete Alarm History File ☐

Save Cancel

REBOOT

Reboot ☐

Save Cancel

Ready Radio: Base Station [Logout ADMIN](#)

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 112). The default setting is 20 seconds.

Inactivity Timeout (min)

This parameter sets the period of user inactivity before SuperVisor automatically logs out of the radio. The default setting is 15 minutes.

Delete Alarm History file

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

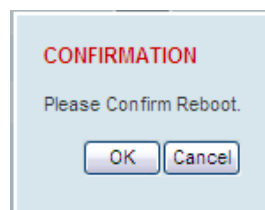
REBOOT

To reboot the radio:

1. Select Maintenance > General.
2. Tick the 'Reboot' checkbox.



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



4. Click 'OK' to reboot the radio or 'Cancel' to abort.

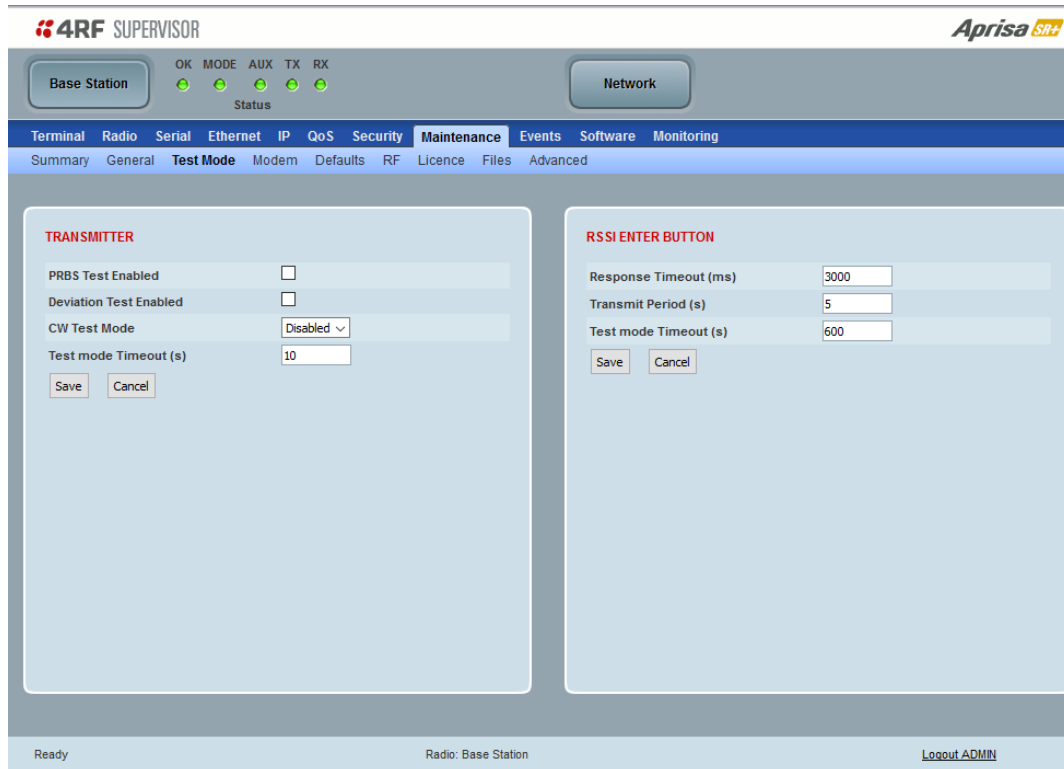
All the radio LEDs will flash repeatedly for 1 second.

The radio will be operational again in about 10 seconds.

The OK, MODE, and AUX LEDs will light green and the TX and RX LEDs will be green (steady or flashing) if the network is operating correctly.

5. Login to SuperVisor.

Maintenance > Test Mode



TRANSMITTER

PRBS Test Enabled

When active, the transmitter outputs a continuous PRBS signal. This can be used for evaluating the output spectrum of the transmitter and verifying adjacent channel power and spurious emission products.

Deviation Test Enabled

When active, the transmitter outputs a sideband tone at the deviation frequency used by the modem. This can be used to evaluate the local oscillator leakage and sideband rejection performance of the transmitter.

CW Test Mode

When active, the transmitter outputs a continuous wave signal.

Option	Function
Preamble	This mode operates the transmitter in CW mode at the preamble power level based on the set transmitter power.
PEP	This mode operates the transmitter in CW mode at the Peak Envelope Power (PEP) level based on the set transmitter power. This test mode is used to demonstrate the full power capability of the radio. To demonstrate the maximum PEP power, set the transmitter power to the maximum power level supported by the modulation selected.

The default setting is Disabled.

Test Mode Timeout (s)

This parameter sets the Transmitter Test Mode timeout period. The radio MODE LED flashes when this Test Mode is active. The radio will automatically exit Transmitter Test Mode after the Timeout period.

The default setting is 10 seconds and the maximum value is 43200 seconds (12 hours).

RSSI TEST BUTTON*Response Timeout (ms)*

This parameter sets the time RSSI Test Mode waits for a response from the base station before it times out and retries. The default setting is 3000 ms.

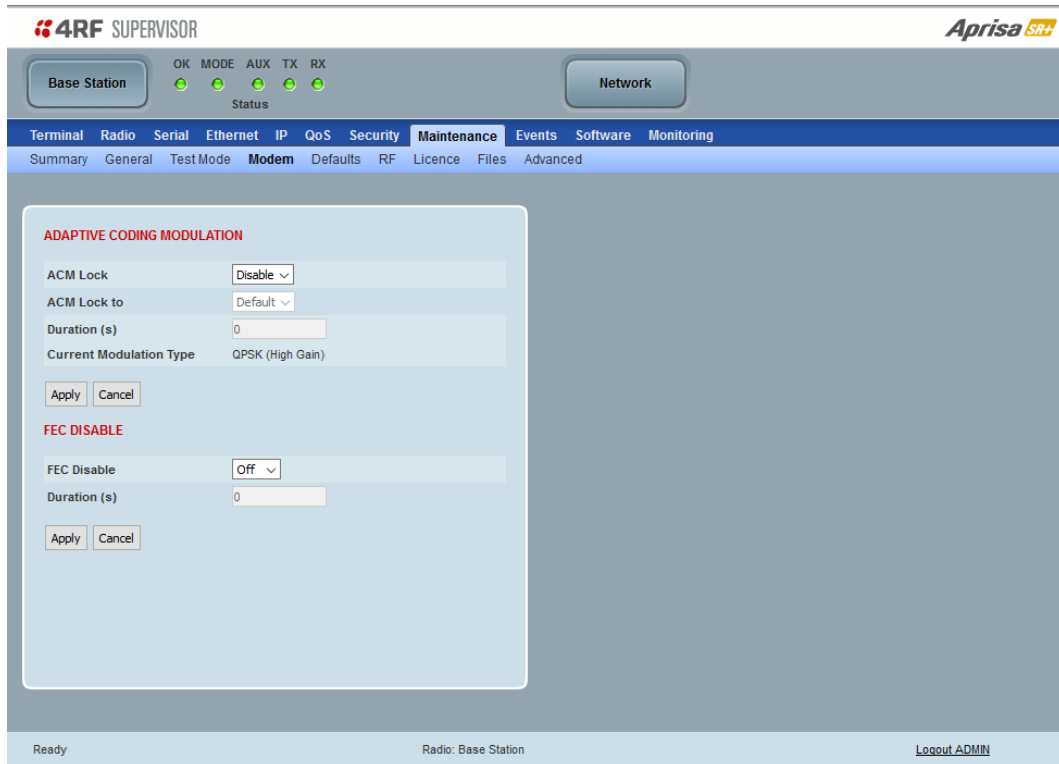
Transmit Period (sec)

This parameter sets the time between RSSI Test Mode requests to the base station. The default setting is 5 seconds.

Test Mode Timeout (s)

This parameter sets the RSSI Test Mode timeout period. The radio will automatically exit RSSI Test Mode after the Timeout period. The default setting is 600 seconds.

Maintenance > Modem



ADAPTIVE CODING AND MODULATION

ACM Lock

This parameter sets whether adaptive modulation can be locked or not.

Option	Function
Disable	Disables manual locking of the adaptive modulation i.e. allows for automatic adaptive modulation.
Enable	Allows the adaptive modulation to be manually locked
Timer	Allows the adaptive modulation to be manually locked but only for a predetermined period.

ACM Lock To

This parameter manually locks the adaptive modulation.

Option	Function
Default	Manually locks the adaptive modulation to the default modulation defined in 'Default Modulation' on page 139.
Current	Manually locks the adaptive modulation to the current modulation at that time.

Duration (s)

This parameter defines the period required for manually locking the adaptive modulation. When this period elapses, the adaptive modulation becomes automatic.

FEC DISABLE

FEC Disable

This diagnostic function allows the user to temporarily disable forward error correction on the channel when diagnosing problems on the link.

Therefore, enabling this diagnostic function would temporarily disable FEC on the channel and the associated maintenance mode alarm would activate.

Note that the opposite is not true for this diagnostic function. In other words, this diagnostic function does not provide the user with the option to temporarily enable forward error correction on the channel.

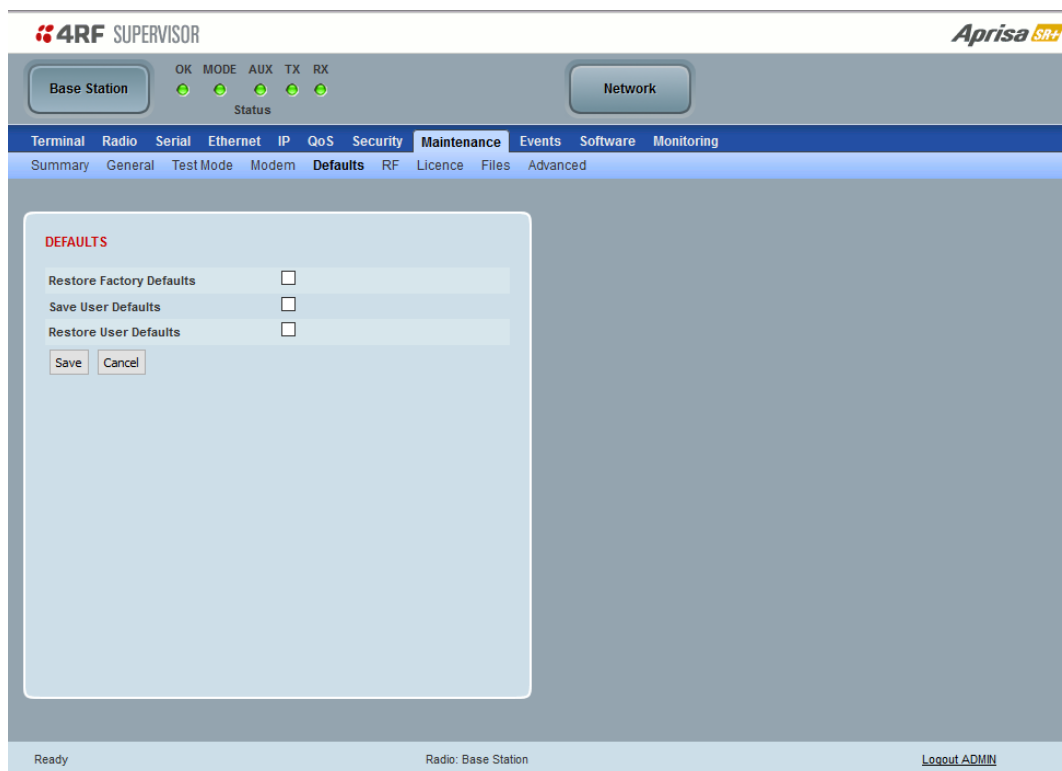
All diagnostic functions are not persistent and will be return to disabled states should the system restart.

Option	Function
Enable	Enables the FEC Disable diagnostic function
Disable	Disables the FEC Disable diagnostic function
Timer	Allows the FEC to be disabled but only for a predetermined period.

Duration (s)

This parameter defines the period required for disabling of the FEC. When this period elapses, the FEC is enabled.

Maintenance > Defaults

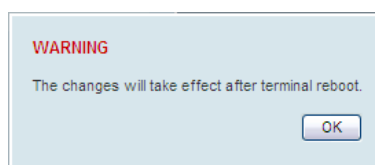


DEFAULTS

The Maintenance Defaults page is only available for the local terminal.

Restore Factory Defaults

When activated, all radio parameters will be set to the factory default values. This includes resetting the radio IP address to the default of 169.254.50.10.



Note: Take care using this command.

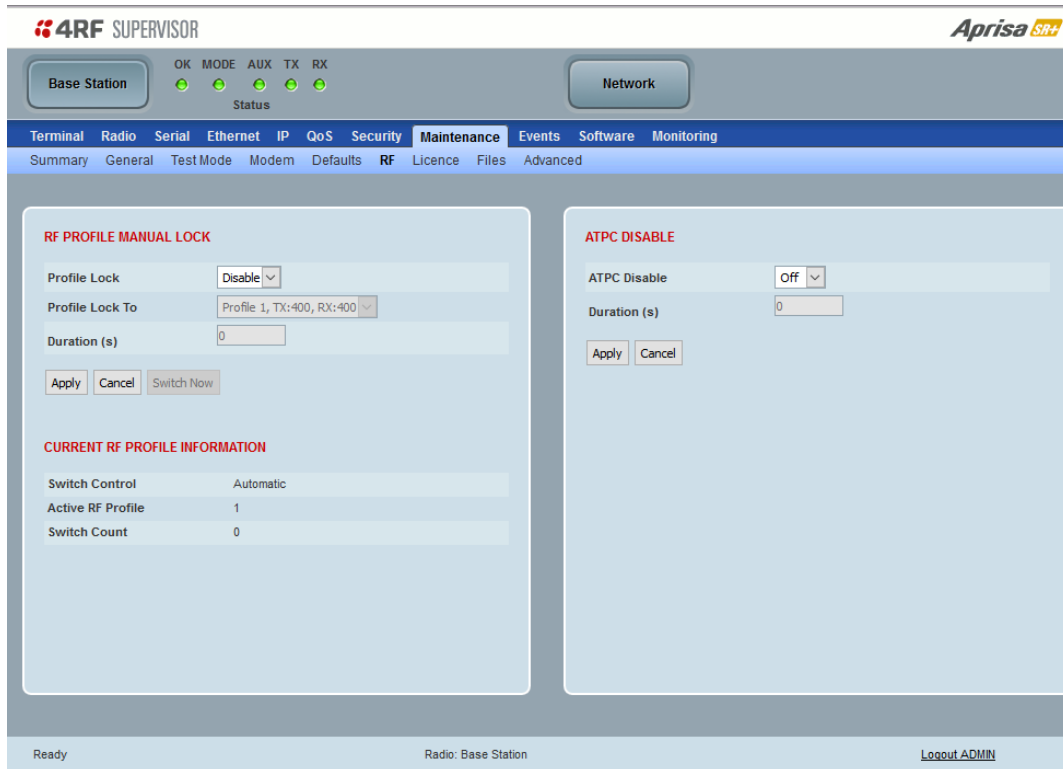
Save User Defaults

When activated, all current radio parameter settings will be saved to non-volatile memory within the radio.

Restore User Defaults

When activated, all radio parameters will be set to the settings previously saved using 'Save User Defaults'.

Maintenance > RF



RF PROFILE MANUAL LOCK

The RF Profile Manual Lock controls the manual locking of the RF Profile.

Profile Lock

This parameter enables / disables the RF Profile manual lock.

Option	Function
Disable	Disables the RF Profile manual lock so it can be changed by any predefined Event Action.
Enable	Enables the RF Profile manual lock so it cannot be changed by any predefined Event Action. The RF Profile is selected with the Profile Lock To.
Timer	Enables the RF Profile manual lock but only for a period defined in Duration.

Profile Lock To

This parameter manually locks the RF Profile to a specific profile, so it cannot be changed by any predefined Event Action see Events > Event Action Setup on page 286.

Duration (s)

This parameter defines the period to apply a manual RF Profile lock. When this period elapses, the RF Profile lock becomes Disabled.

ATPC DISABLE

ATPC Disable

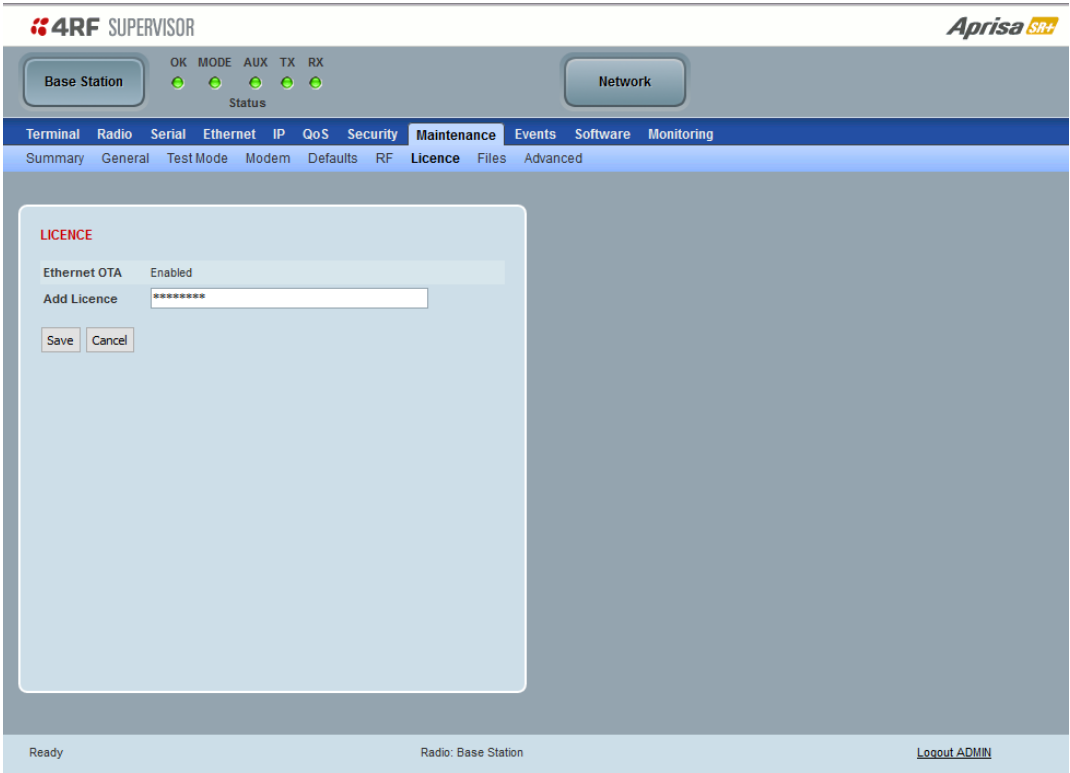
This parameter enables / disables ATPC.

Option	Function
Off	Enables ATPC for all RF Profiles that have it set.
On	Disables ATPC for all RF Profiles.
Timer	Disables ATPC for all RF Profiles but only for a period defined in Duration.

Duration (s)

This parameter defines the period to apply ATPC disable. When this period elapses, the ATPC becomes Enabled for all RF Profiles that have it set.

Maintenance > Licence



LICENCE

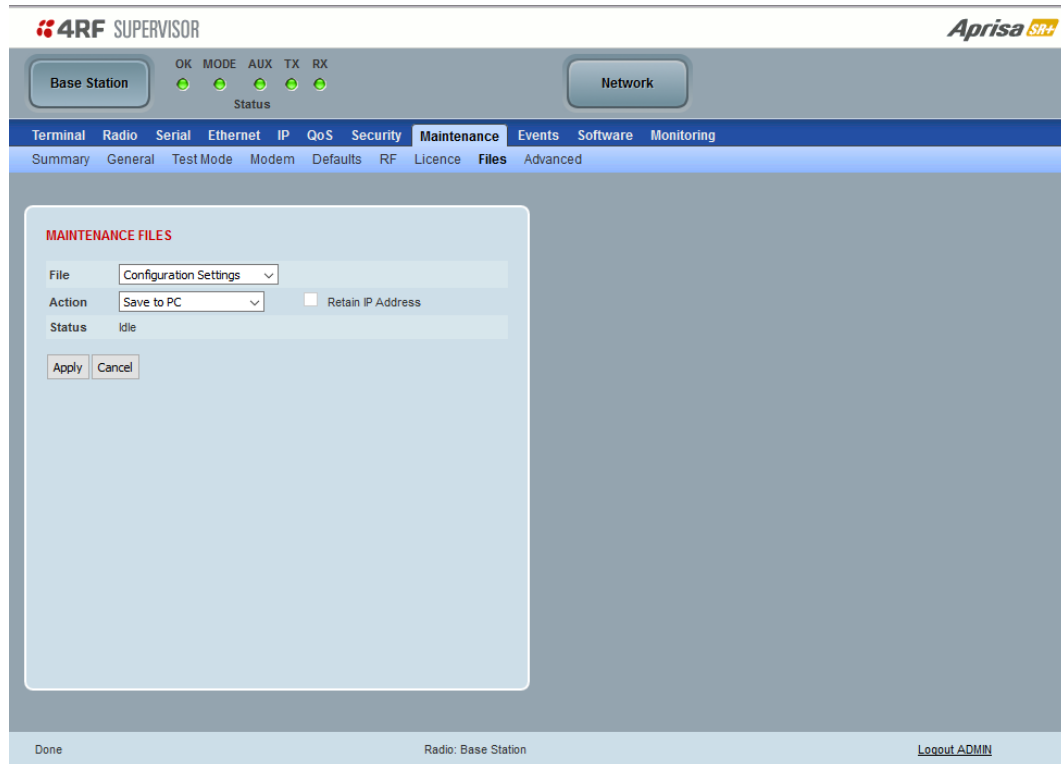
Fully Featured Radio

When a fully featured Aprisa SR+ radio is purchased (indicated by the AA), it contains the licences which activate Remote Management, Ethernet Traffic, and SNMP Management e.g.

Part Number	Part Description
APSQ-N400-SSC-HD-22-EN <u>AA</u>	4RF SR+, BR, 400-470 MHz, SSC, Half Duplex, 2E2S, EN, <u>STD</u>

In this software version, Remote Management, Ethernet Traffic and SNMP management are enabled by default.

Maintenance > Files



MAINTENANCE FILES

There are three maintenance file types which can be saved / restored to / from PC or USB flash drive:

- Configuration Settings
- Event History Log
- Performance History Log

Note: 4RF radios only support the FAT32 file system for flash drives. If the flash drive is a different format such as exFAT or NTFS, you will need to reformat it to FAT32.

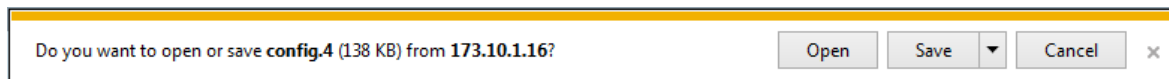
Also, some brands of USB flash drives may not work with 4RF radios.

File - Configuration Settings

This feature enables the configuration of a radio to be saved to a file for configuration backup or for copying to another radio, however the target radio being restored must be operating on the same software version as the source radio the configuration file was saved from e.g. if the configuration file was saved from a radio operating on software version 2.0.0, it can only be restored to a radio operating on software version 2.0.0.

Action

Action	Option
Save to PC	This saves the file with a filename of 'Config.4' to a binary encrypted file. This can then be saved from the Browser popup (example is Windows Internet Explorer 11). The file should be renamed to be able to identify the radio it was saved from. When the Security Level is set to 'Strong', the radio Key Encryption Key is used to encrypt the saved configuration file.



Save to Radio USB	This saves the file with a filename of 'asrcfg_2.1.5' to a binary encrypted file on the radio USB flash drive root directory.
Restore from PC	This restores all user configuration settings from a binary encrypted file on a PC directory to the radio. A reboot warning message will warn of a pending reboot after the PC file is selected. Clicking OK will open a browser file selection window to select the file. When the Security Level is set to 'Strong', the Key Encryption Key of the saved configuration file must be known as it must match the Key Encryption Key of the radio. Note: If you are using Explorer, it must be IE10 or above for this feature to work correctly.
Restore from Radio USB	This restores all user configuration settings from a binary encrypted file on the USB root directory to the radio.

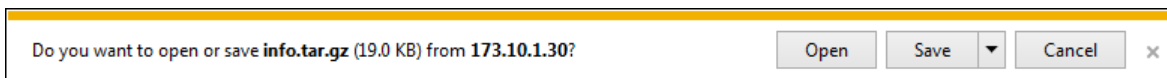
Note: 'Payload Encryption Key' and 'Key Encryption Key' parameters (see 'Security > Setup') are not saved to the configuration file. When a 'Restore from PC' or 'Restore from Radio USB' is used, these parameters will retain their existing values so are not changed by the operation of restoring the configuration file.

Note: If the remote radios are running software versions prior to 1.7.3, the configuration file cannot be downloaded over the air.

File - Event History Log

Action

Action	Option
Save to PC	This saves the Event History Log file with a filename of 'Info.tar.gz' to a binary encrypted file. This can then be saved from the Browser popup (example is Windows Internet Explorer 11). The file should be renamed to be able to identify the radio it was saved from. The 'tar.gz' file is normally for sending back to 4RF Limited for analysis but can be opened with widely available archive tools e.g. WinRar or 7-ZIP.

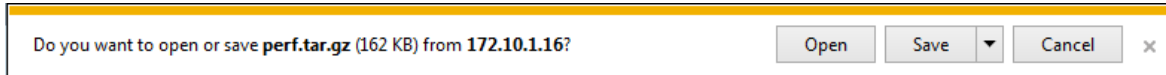


Save to Radio USB	This saves the file with a filename of e.g. 'alarm_173.10.1.30_2014-11-10,15.54.14.txt' to a text file on the radio USB flash drive root directory.

File - Performance History Log

Action

Action	Option
Save to PC	This saves the Performance History Log file with a filename of 'Perf.tar.gz'. This can then be saved from the Browser popup (example is Windows Internet Explorer 11). The file should be renamed to be able to identify the radio it was saved from. The 'tar.gz' file is normally for sending back to 4RF Limited for analysis but can be opened with widely available archive tools e.g. WinRar or 7-ZIP.



The Performance Log file contains the following files:

- perfQhour.csv
This file contains the performance data for the radio recorded on a quarter hourly basis. Up to 24 hours of data is stored in this file.
- perfDaily.csv
This file contains the performance data for the radio recorded on a daily basis. Up to 31 days of data is stored in this file.
- perfUnitQhour.csv
This file contains the performance data for the RF path of the radio to each remote radio, recorded on a quarter hourly basis. Up to 24 hours of data for each RF path is stored in this file.
- perfUnitDaily.csv
This file contains the performance data for the RF path of the radio to each remote radio, recorded on a daily basis. Up to 31 days of data for each RF path is stored in this file.

4RF has developed templates for viewing the data from the Performance Log files. These templates include the instructions for importing and graphing the log data.

The Performance History Log Templates are available in a zip file from the 4RF website <https://www.4rf.com/secure> (login required) > Aprisa SR+ > Support Tools or from 4RF.

These templates import the data from the saved csv files and generate tables and charts of the radio data.

To import the Performance Log files into excel:

- Unzip the saved perf.tar.gz file to a temporary directory using an open-source file archiver like 7-zip
- Open the performance history template zip file (.zip) and extract the templates (.xlsm) into the same temporary directory
- Open the template spreadsheet (.xlsm) appropriate to the history you want to review
- On the spreadsheet 'Instructions' sheet, click the 'Import From CSV' button. The spreadsheet will now present the raw data from the CSV file in various tables and charts.

File - Configuration Script

Action

Action	Option
Load and Execute	This loads and executes configuration script files. There are sample Master Configuration script files available from the 4RF website https://www.4rf.com/secure. The purpose of these files is to use as templates to create your own configuration scripts. Note: Be careful using this feature as incompatible configurations will change the radios settings and break radio connectivity.

Note: Activating this function will over-write all existing configuration settings in the radio (except for the non-saved settings e.g. security passwords, licence keys etc) without any verification of the command setting in the radio. Precautions should be taken to prevent radio outages with incorrect radio configurations. The following process steps are recommended:

- Save the current radio configuration to a PC or USB before uploading the new configuration script file
- Upload the new configuration script file to the radio
- If for some reason the radio doesn't work as expected, the saved configuration file can be uploaded to the radio (roll back to previous configuration).

Retain IP Address

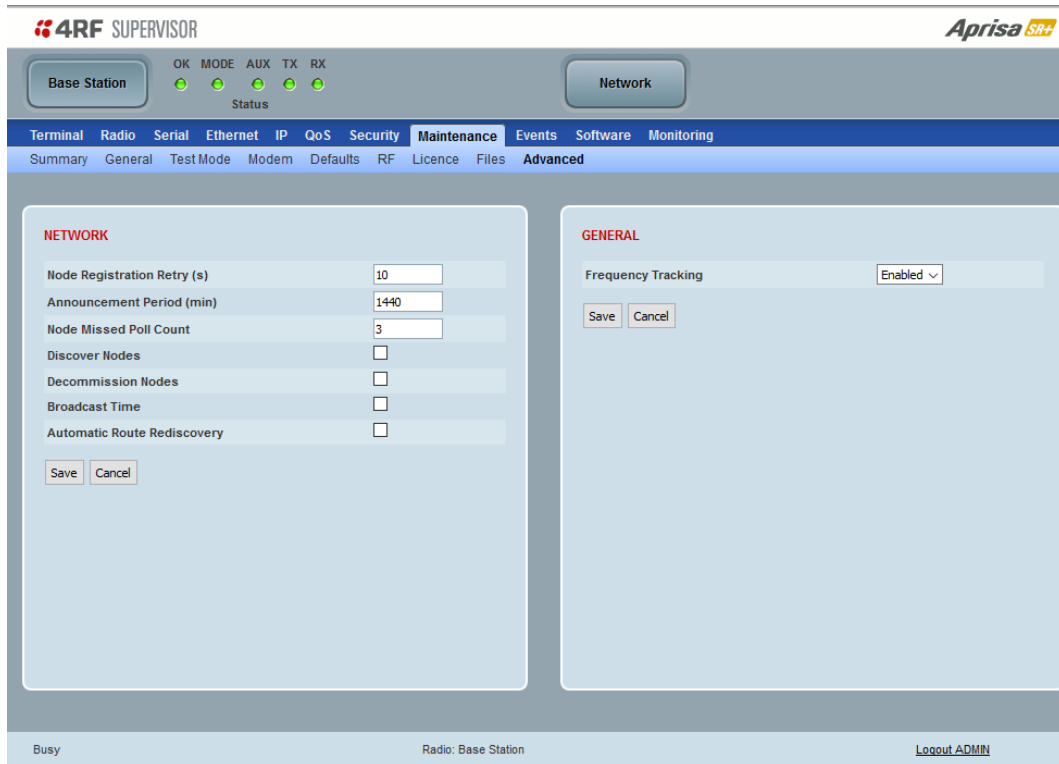
This parameter when enabled ensures that the radio IP address is not changed when the radio configuration settings are restored from a configuration file with a different IP radio address. It prevents the radio losing connectivity when the configuration settings are restored from a configuration file.

Revert Config if Connection Lost

When the Maintenance Files feature is used on remote radios from the base station, this parameter allows the configurations to be restored to the previous configuration if the connection is lost.

This must be set before executing the Configuration Settings / Configuration Script restore functions.

Maintenance > Advanced



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Status Network

Terminal Radio Serial Ethernet IP QoS Security **Maintenance** Events Software Monitoring

Summary General Test Mode Modem Defaults RF Licence Files **Advanced**

NETWORK

Node Registration Retry (s)

Announcement Period (min)

Node Missed Poll Count

Discover Nodes ☐

Decommission Nodes ☐

Broadcast Time ☐

Automatic Route Rediscovery ☐

GENERAL

Frequency Tracking

Busy Radio: Base Station [Logout ADMIN](#)

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.

Announcement Period (min)

This parameter displays the period between base station announcement messages. The announcement messages are used to distribute the base station date and time to remote radios. The default setting is 1440 minutes (24 hours).

Setting this parameter to 0 will stop periodic announcement messages being transmitted.

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.

Once a remote radio has registered with the Base Station, it will remain in the Network Table regardless of whether the remote radio is present or not until such time that you manually remove it. If you want to remove the deinstalled radios from the Network Table, you will need to use the 'Decommission Node(s)' command which will clear the entire network table and then the 'Discover Nodes' command. This will then populate the Network Table only with those remote radios that are communicating with the Base Station.

Decommission Node(s)

This parameter when activated resets the network registrations to remove the entire network from service.

Note: Take care using this option.

Individual nodes can be decommissioned using the 'registration' CLI command. See 'CLI Commands' on page 397.

Broadcast Time

This parameter when activated sends the base station Date / Time setting to all the remote and repeater stations in the network and sets their Date / Time. This option applies to the base station only.

Automatic Route Rediscovery

This parameter enables the radio to transmit route discovery messages when packets are unacknowledged.

When enabled, unacknowledged unicast packets are converted into uni-broadcast messages and sent through the network. All nodes see the message and populate their routing tables accordingly.

When the destination node is reached, it sends a route response message via the shortest path. The intermediate nodes see this message and populate their routing tables in the reverse direction, thus re-establishing the route.

The default setting is disabled.

GENERAL

Frequency Tracking

Frequency Tracking enables the receiver to track any frequency drift in the transmitter to maintain optimum SNR and radio link performance over the full temperature range.

When enabled, remote radios adjust their receive frequency to the frequency of the incoming packet rate and the base station notifies remote radios if their transmit frequency requires adjustment.

The default setting is Enabled.

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:

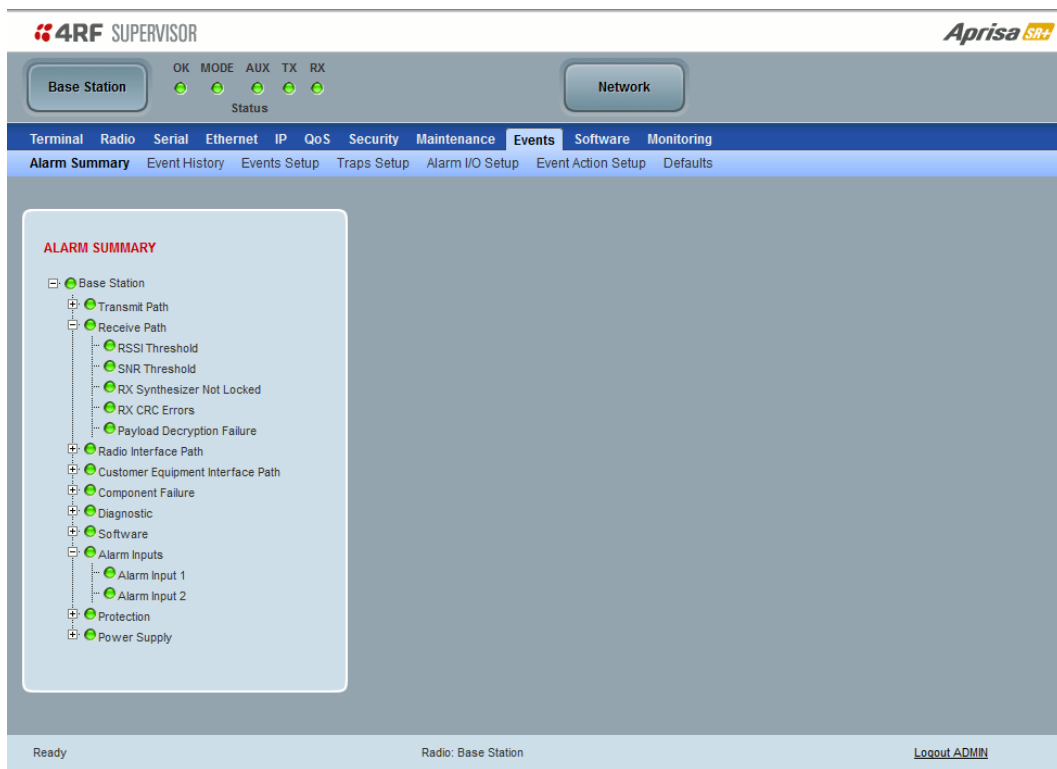
1. Alarm Events

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 458 for a complete list of events.

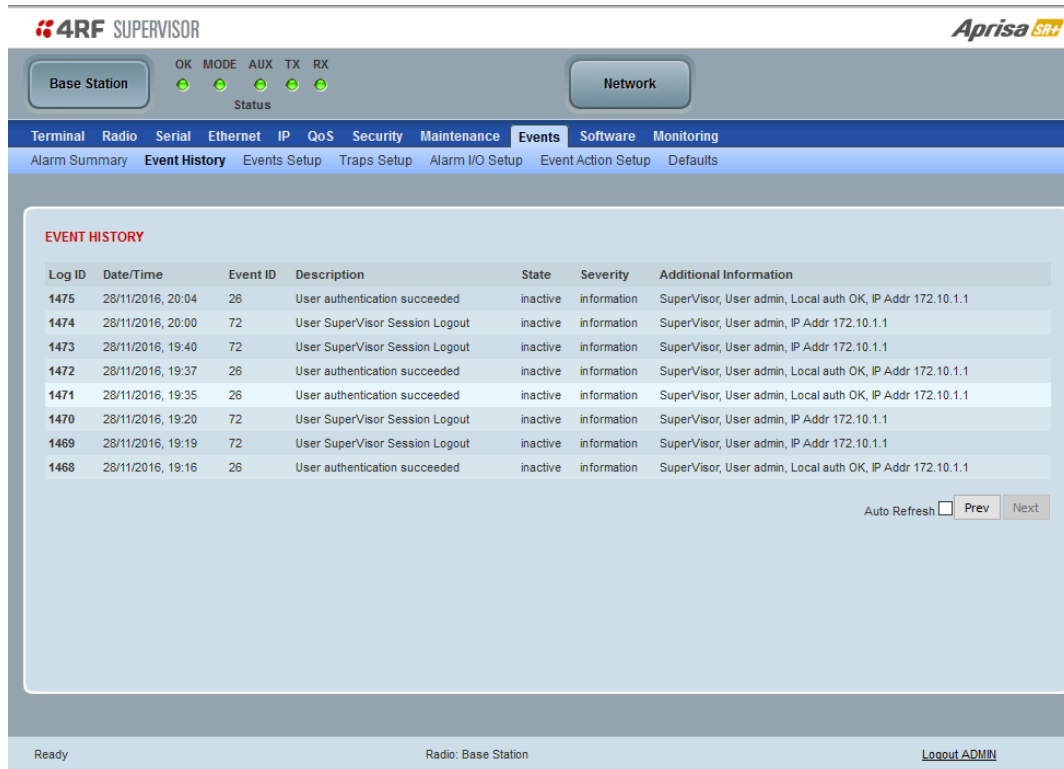


ALARM SUMMARY

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



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Network

Status

Terminal Radio Serial Ethernet IP QoS Security Maintenance **Events** Software Monitoring

Alarm Summary **Event History** Events Setup Traps Setup Alarm I/O Setup Event Action Setup Defaults

EVENT HISTORY

Log ID	Date/Time	Event ID	Description	State	Severity	Additional Information
1475	28/11/2016, 20:04	26	User authentication succeeded	inactive	information	SuperVisor, User admin, Local auth OK, IP Addr 172.10.1.1
1474	28/11/2016, 20:00	72	User SuperVisor Session Logout	inactive	information	SuperVisor, User admin, IP Addr 172.10.1.1
1473	28/11/2016, 19:40	72	User SuperVisor Session Logout	inactive	information	SuperVisor, User admin, IP Addr 172.10.1.1
1472	28/11/2016, 19:37	26	User authentication succeeded	inactive	information	SuperVisor, User admin, Local auth OK, IP Addr 172.10.1.1
1471	28/11/2016, 19:35	26	User authentication succeeded	inactive	information	SuperVisor, User admin, Local auth OK, IP Addr 172.10.1.1
1470	28/11/2016, 19:20	72	User SuperVisor Session Logout	inactive	information	SuperVisor, User admin, IP Addr 172.10.1.1
1469	28/11/2016, 19:19	72	User SuperVisor Session Logout	inactive	information	SuperVisor, User admin, IP Addr 172.10.1.1
1468	28/11/2016, 19:16	26	User authentication succeeded	inactive	information	SuperVisor, User admin, Local auth OK, IP Addr 172.10.1.1

Auto Refresh ☐ Prev Next

Ready Radio: Base Station [Logout ADMIN](#)

EVENT HISTORY

The last 1500 events are stored in the radio. The complete event history list can be downloaded to a USB flash drive (see ‘File - Event History Log’ on page 273).

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

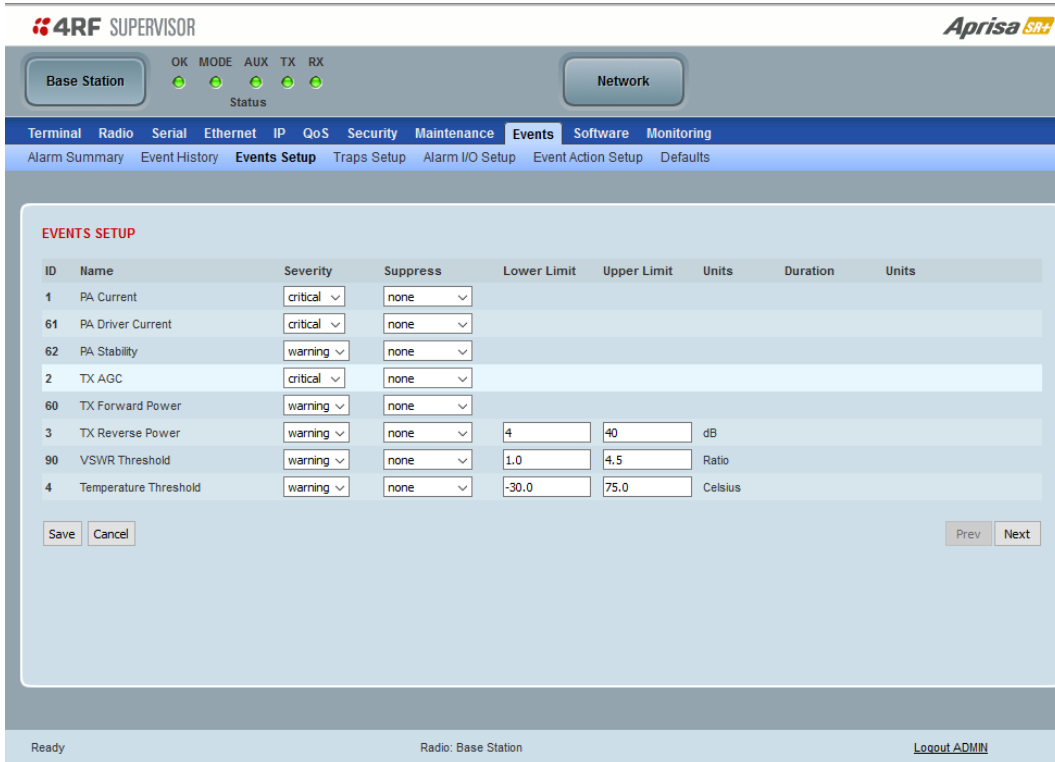
The Next button will display the next page of 8 events and the Prev button will display the previous page of 8 events. Using these buttons will disable Auto Refresh to prevent data refresh and page navigation contention.

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

ID	Name	Severity	Suppress	Lower Limit	Upper Limit	Units	Duration	Units
1	PA Current	critical	none					
61	PA Driver Current	critical	none					
62	PA Stability	warning	none					
2	TX AGC	critical	none					
60	TX Forward Power	warning	none					
3	TX Reverse Power	warning	none	4	40	dB		
90	VSWR Threshold	warning	none	1.0	4.5	Ratio		
4	Temperature Threshold	warning	none	-30.0	75.0	Celsius		

Save Cancel Prev Next

Ready Radio: Base Station Logout ADMIN

EVENTS SETUP

Alarm event parameters can be configured for all alarm events (see 'Alarm Events' on page 459).

All active alarms for configured alarm events will be displayed on the Monitoring pages (see 'Monitoring' on page 310).

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.

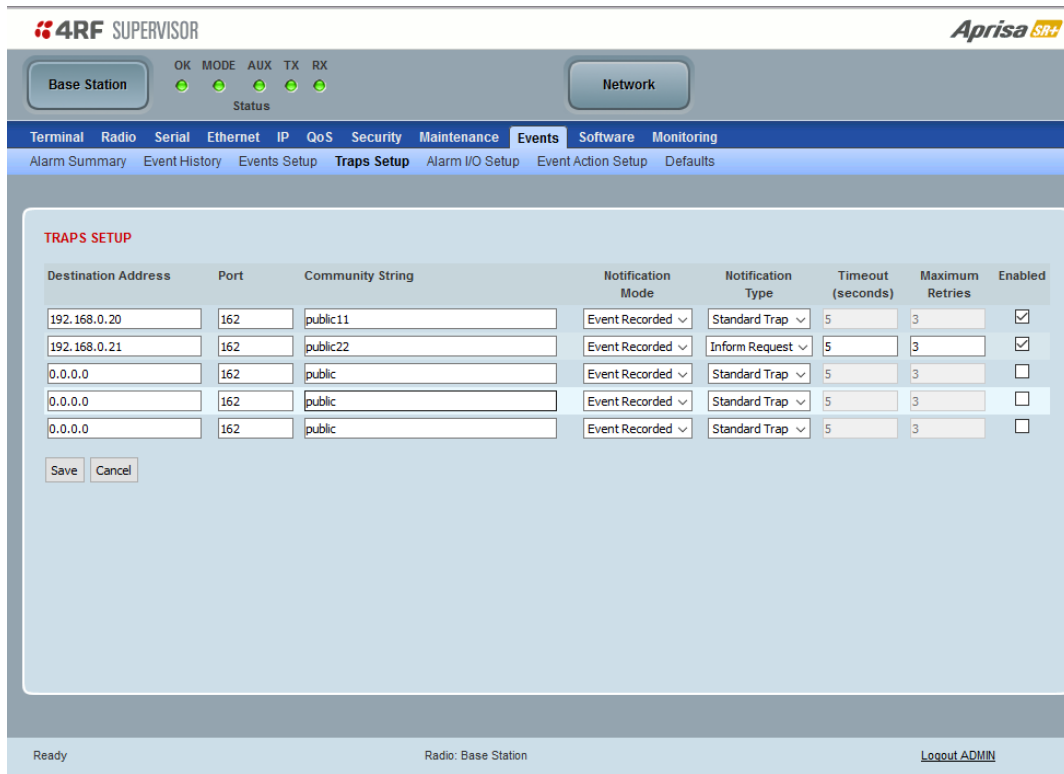
Block

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

Destination Address	Port	Community String	Notification Mode	Notification Type	Timeout (seconds)	Maximum Retries	Enabled
192.168.0.20	162	public11	Event Recorded	Standard Trap	5	3	☒
192.168.0.21	162	public22	Event Recorded	Inform Request	5	3	☒
0.0.0.0	162	public	Event Recorded	Standard Trap	5	3	☐
0.0.0.0	162	public	Event Recorded	Standard Trap	5	3	☐
0.0.0.0	162	public	Event Recorded	Standard Trap	5	3	☐

Save Cancel

TRAPS SETUP

All events can generate SNMP traps. The types of traps that are supported are defined in the 'Notification Mode'.

Destination Address

This parameter sets the IP address of the server running the SNMP manager.

Port

This parameter sets the port number the server running the SNMP manager.

Community String

This parameter sets the community string which is sent with the IP address for security. The default community string is 'public'.

Notification Mode

This parameter sets when an event related trap is sent:

Option	Function
None	No event related traps are sent.
Event Recorded	When an event is recorded in the event history log, a trap is sent.
Event Updated	When an event is updated in the event history log, a trap is sent.
All Events	When an event is recorded or updated in the event history log, a trap is sent.

Notification Type

This parameter sets the type of event notification:

Option	Function
Standard Trap	Provides a standard SNMP trap event
Inform Request	Provides a SNMP v2 Inform Request trap event including trap retry and acknowledgement

Notification Type set to Inform Request:

Timeout (second)

This parameter sets the time interval to wait for an acknowledgement before sending another retry.

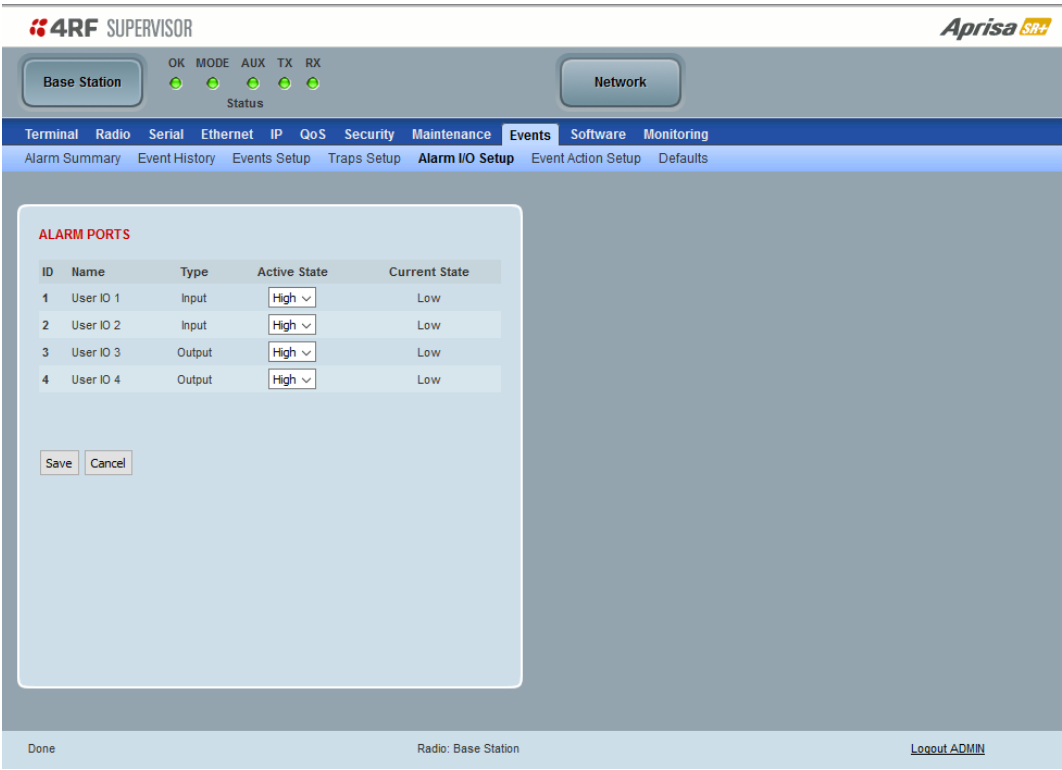
Maximum Retries

This parameter sets the maximum number of retries to send the event without acknowledgement before it gives up.

Enabled

This parameter determines if the entry is used.

Events > Alarm I/O Setup



ALARM PORTS

This page provides control of the two hardware alarm inputs and two hardware alarm outputs provided on the alarm connector.

The alarm inputs are used to transport alarms to the other radios in the network. The alarm outputs are used to receive alarms from other radios in the network.

Name

The alarm IO number.

Type

The Type shows if the alarm is an input or output.

Active State

The Active State parameter sets the alarm state when the alarm is active.

Alarm Input

Option	Function
Low	The alarm is active low i.e. a ground contact on the port will cause an active alarm state
High	The alarm is active high i.e. an open contact on the port will cause an active alarm state

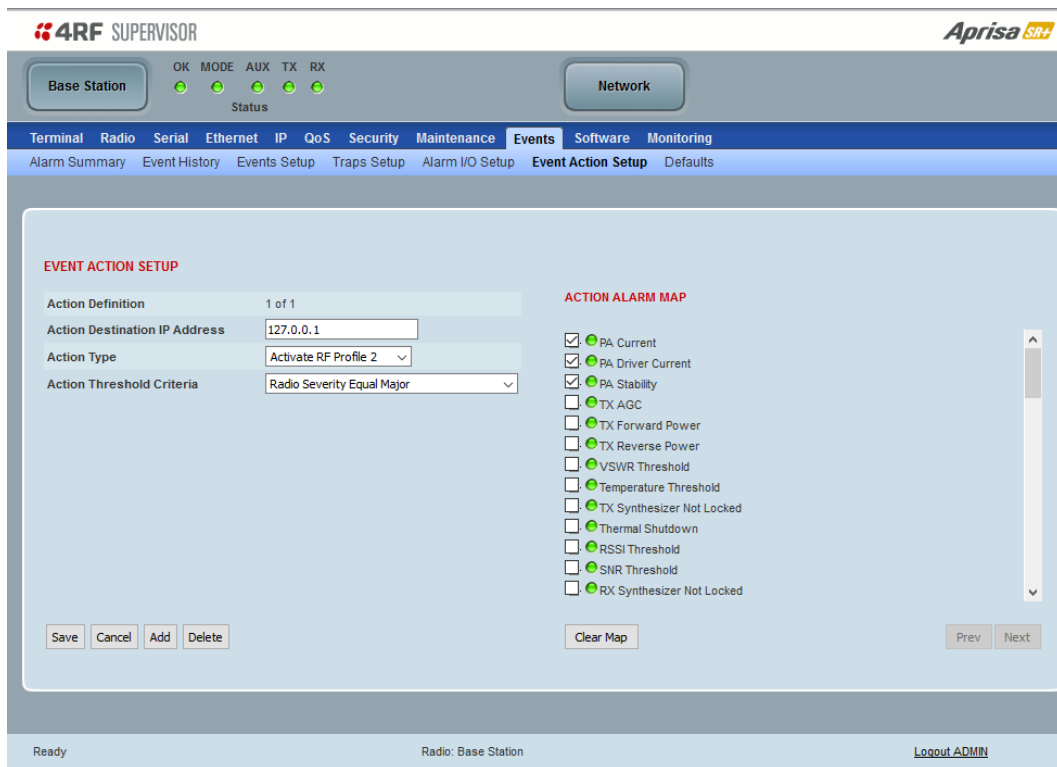
Alarm Output

Option	Function
Low	The alarm is active low i.e. the active alarm state will generate a ground contact output
High	The alarm is active high i.e. the active alarm state will generate a open contact output

Current State

The Current State shows the current state of the alarm.

Events > Event Action Setup



EVENT ACTION SETUP

This page provides control of the mapping of events to specific actions. Specific alarm events can setup to trigger outputs.

Action Definition

This parameter shows the number of the event action setup and the maximum number of setups stored.

Action Destination IP Address

This parameter sets the IP address of the radio that will output the action type.

Action Type

This parameter sets the action type that will be activated on the radio for the condition defined in Action Threshold Criteria.

Option	Function
None	This action setup does not activate any alarm output
Activate RF Profile 1 or 2	This action setup activates the RF Profile 1 or 2 (whichever is inactive)
Activate Alarm Output 1	This action setup activates alarm output 1
Activate Alarm Output 2	This action setup activates alarm output 2

Action Threshold Criteria

This parameter sets the radio event that will trigger the action output.

Option	Function
None	No action output.
Radio Severity Equal Critical	Activates the action output when a radio alarm is critical alarm
Radio Severity Equal Major	Activates the action output when a radio alarm is a major alarm
Radio Severity Equal Minor	Activates the action output when a radio alarm is minor alarm
Radio Severity Equal Warning	Activates the action output when a radio alarm is a warning alarm
Radio Severity Equal Cleared	Activates the action output when a radio alarm is cleared
Radio Severity Equal or Worse than Major	Activates the action output when a radio alarm is a major alarm or a critical alarm
Radio Severity Equal or Worse than Minor	Activates the action output when a radio alarm is a minor alarm, a major alarm or a critical alarm
Radio Severity Equal or Worse than Warning	Activates the action output when a radio alarm is a warning, a major alarm, a minor alarm or a critical alarm

Controls

The Save button saves the current event action setup.

The Cancel button cancels the new event action setup.

The Add button adds a new event action setup.

The Delete button deletes the current event action setup.

The Clear Map button clears all alarm selections on the current setup.

To add an event action setup:

1. Click on the Add button.
2. Enter the Action Destination IP Address. This is the IP address of the radio that will output the action type.
3. Select the Action Type from the list.
4. Select the Action Threshold Criteria from the list.
5. Tick the alarms required for the event action setup from the Action Alarm Map. You can clear all alarm selections with the Clear Map button.
6. Click on Save.

Events > Syslog

This menu allows configuring events that are recorded in the History Log, to also be sent to remote servers using the syslog protocol (compliant with RFC 5424 and RFC 5426). Messages from the Aprisa SR+ contain a MSG field with. Example message:

```
<13>1 2020-04-09T01:08:45+00:00 AprisaSR+ - 14 5000 - {"logId":"449","timestamp":"2020-04-09T01:08:45+00:00","eventId":"24","auth":"0","eventName":"AlarmInput1","alarmStatus":"active","severity":"Warning","message":"Input 1 is Active"}
```

The MSG field contains json formatted fields that match the fields seen in the Events->History Log screen:

logId: Integer identifier

timestamp: The time the event occurred, in RFC3339 format

eventId: Integer identifier of the type of event. Identifiers are defined in the 4RF-EVENT MIB

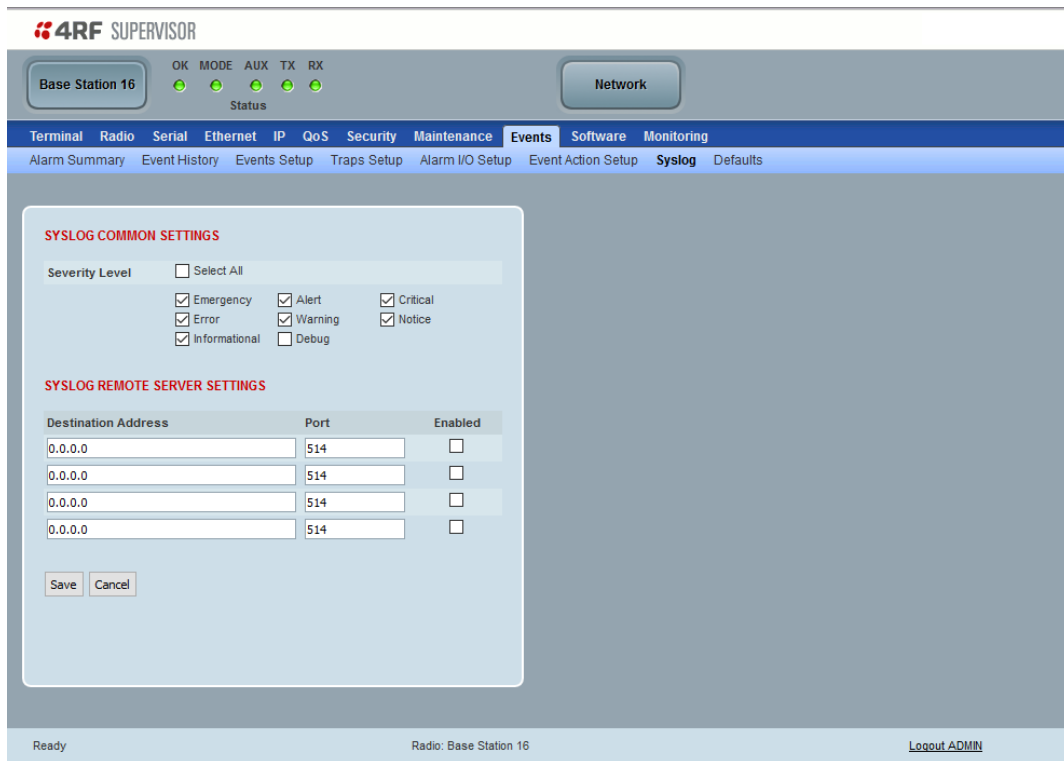
auth: 1 for authorization (login/logout) messages, 0 otherwise

eventName: String name of the event (maps to the eventId)

alarmStatus: State of the alarm (active or inactive)

severity: Can be Information, Warning, Minor, Major, or Cleared

message: Detailed description of the event and what caused it to occur



SYSLOG COMMON SETTINGS

Severity Level

The Severity Level selection options provide filtering of Syslog messages by the eight syslog severity options: Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debug.

SYSLOG REMOTE SERVER SETTINGS

Destination Address

The IP address of the remote syslog server. May be IPv4 or IPv6 address.

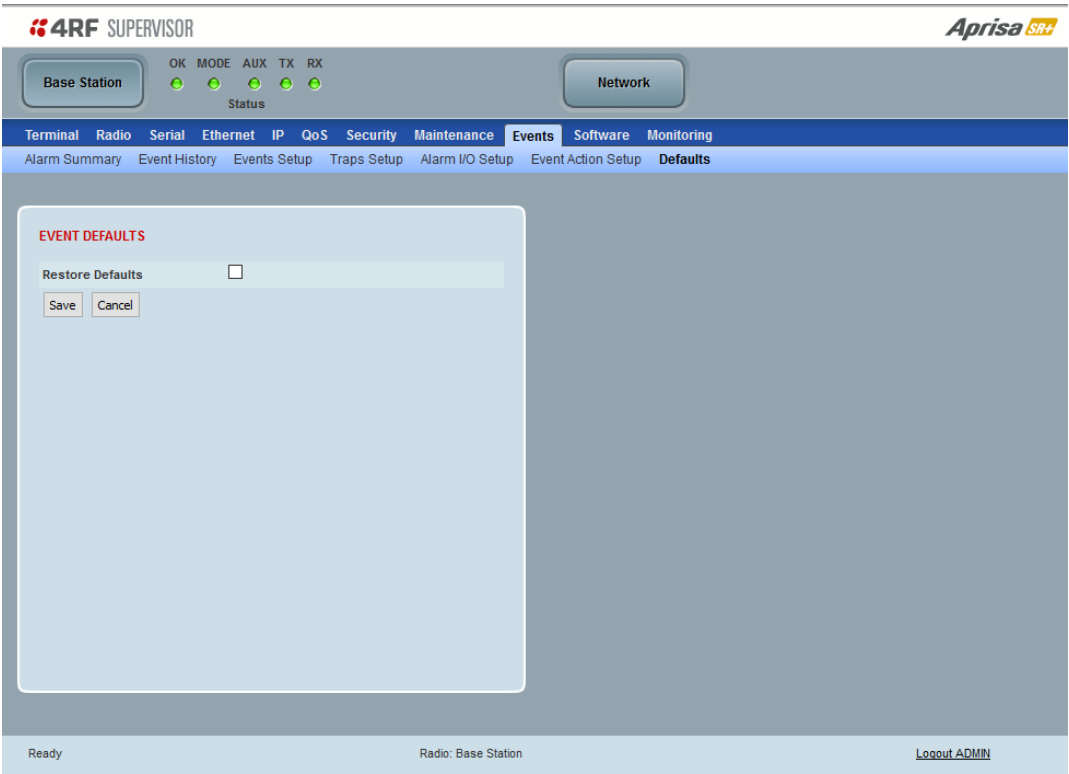
Destination Port

The TCP / UDP port of the remote syslog server. Defaults to 514.

Enabled

Syslog messages are only sent to enabled servers.

Events > Defaults



EVENT DEFAULTS

Restore Defaults

This parameter when activated restores all previously configured event parameters using ‘Events > Events Setup’ to the factory default settings.

Software

The Software menu contains the setup and management of the system software including network software distribution and activation. The distribution of the system software to the remote radios is encrypted by the AES session key over-the-air.

Single Radio Software Upgrade

The radio software can be upgraded on a single Aprisa SR+ radio (see ‘Single Radio Software Upgrade’ on page 449). This process would only be used if the radio was a replacement or a new station in an existing network.

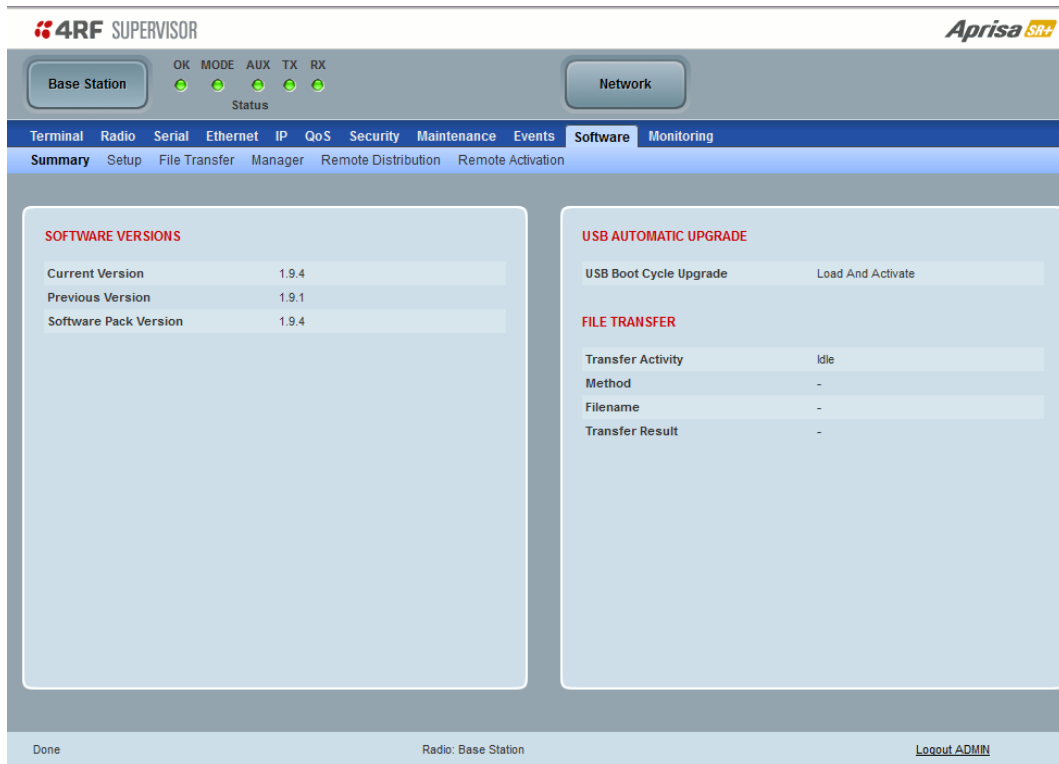
Network Software Upgrade

The radio software can be upgraded on an entire Aprisa SR+ radio network remotely over the radio link (see ‘Network Software Upgrade’ on page 445). 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 radios with ‘Software > Remote Distribution’
3. Activate of the new software on remote radios 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 294.

FILE TRANSFER

Transfer Activity

This parameter shows the status of the transfer, 'Idle', 'In Progress' or 'Completed'.

Method

This parameter shows the file transfer method. When the software distribution is in progress, this parameter will change to 'Over the Air' (from xx.xx.xx.xx) to show that the interface is busy and the transfer is in progress.

File

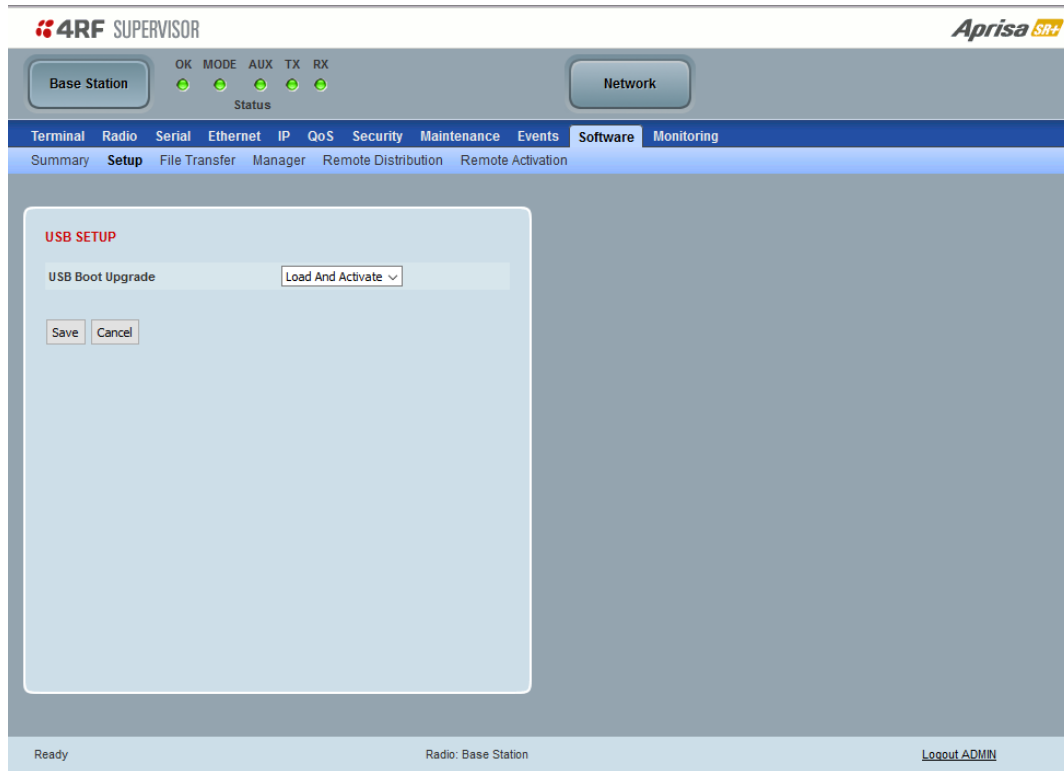
This parameter shows the software file source.

Transfer Result

This parameter shows the progress of the transfer.

Software > Setup

This page provides the setup of the USB flash drive containing a Software Pack.



USB SETUP

USB Boot Upgrade

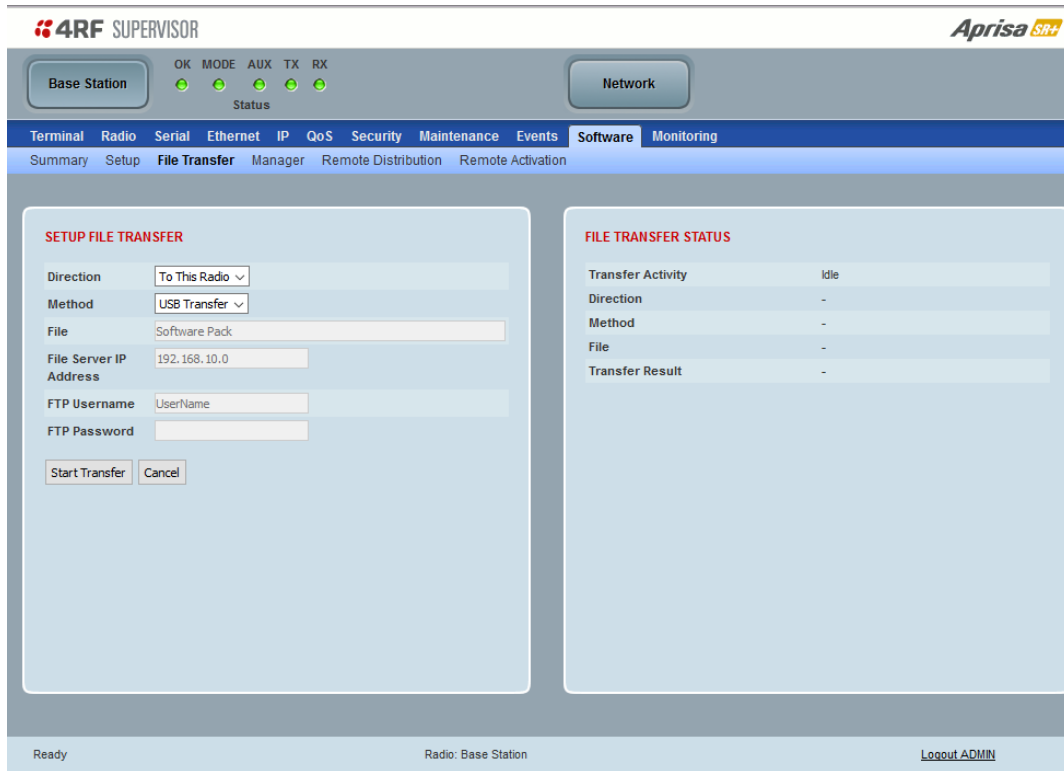
This parameter determines the action taken when the radio power cycles and finds a USB flash drive in the Host port. The default setting is 'Load Only'.

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 299).
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.
HTTP / HTTPS	Transfers the software pack file (.swpack) from a PC 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

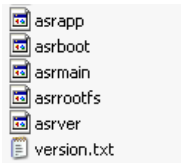
This parameter shows the file transfer method.

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;  <table><tr><td>asrapp</td><td>1,332 KB</td><td>File</td></tr><tr><td>asrboot</td><td>28 KB</td><td>File</td></tr><tr><td>asrmain</td><td>3,716 KB</td><td>File</td></tr><tr><td>asrrootfs</td><td>1,944 KB</td><td>File</td></tr><tr><td>asrver</td><td>8 KB</td><td>File</td></tr><tr><td>version.txt</td><td>1 KB</td><td>Text Document</td></tr></table>	asrapp	1,332 KB	File	asrboot	28 KB	File	asrmain	3,716 KB	File	asrrootfs	1,944 KB	File	asrver	8 KB	File	version.txt	1 KB	Text Document
asrapp	1,332 KB	File																	
asrboot	28 KB	File																	
asrmain	3,716 KB	File																	
asrrootfs	1,944 KB	File																	
asrver	8 KB	File																	
version.txt	1 KB	Text Document																	

To transfer software into the Aprisa SR+ radio:

USB Transfer Method

1. Unzip the software release files into the root directory of a USB flash drive.
2. Insert the USB flash drive into the host port .
3. Click on 'Start Transfer'.

FILE TRANSFER STATUS	
Transfer Activity	In Progress
Direction	To This Radio
Method	USB Transfer
File	Software Pack
Transfer Result	In Progress (30%)

4. When the transfer is completed, remove the USB flash drive from the host port. If the SuperVisor 'USB Boot Upgrade' setting is set to 'Disabled' (see 'USB Boot Upgrade' on page 294), 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 299). The radio will reboot automatically.

If the file transfer fails, check the Event History page (see 'Events > Event History' on page 279) for more details of the transfer.

Note: 4RF radios only support the FAT32 file system for flash drives. If the flash drive is a different format such as exFAT or NTFS, you will need to reformat it to FAT32.

Also, some brands of USB flash drives may not work with 4RF radios.

FTP Method

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

FILE TRANSFER STATUS	
Transfer Activity	In Progress
Direction	To This Radio
Method	FTP (172.17.10.11)
File	Software Pack
Transfer Result	In Progress (1%)

Go to Supervisor > Software > Manager and activate the Software Pack (see 'Software > Manager' on page 299). The radio will reboot automatically.

If the file transfer fails, check the Event History page (see 'Events > Event History' on page 279) for more details of the transfer.

HTTP / HTTPS Method

1. Unzip the software release files into a temporary directory.
2. Click on 'Start Transfer'.
3. Browse to the *.swpack file in the temporary directory and open the file.

FILE TRANSFER STATUS	
Transfer Activity	In Progress
Direction	To This Radio
Method	HTTPS
File	Software Pack
Transfer Result	In Progress (5%)

Go to Supervisor > Software > Manager and activate the Software Pack (see 'Software > Manager' on page 299). The radio will reboot automatically.

If the file transfer fails, check the Event History page (see 'Events > Event History' on page 279) for more details of the transfer.

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.
Completing Transfer	The data has fully transferred (100%) to the radio but file validation is in progress.

Note: To check that the Aprisa SR+ software upgrade file (.swpack) is valid, obtain the checksum (sha1) file for that software release contained in the Software Release zip file on the 4RF website <https://www.4rf.com/secure>.

On windows open a command prompt and type 'certutil -hashfile <updatefile>.swpack SHA1'. Next open the sha1 file in a text editor such as notepad and confirm the hashes match.

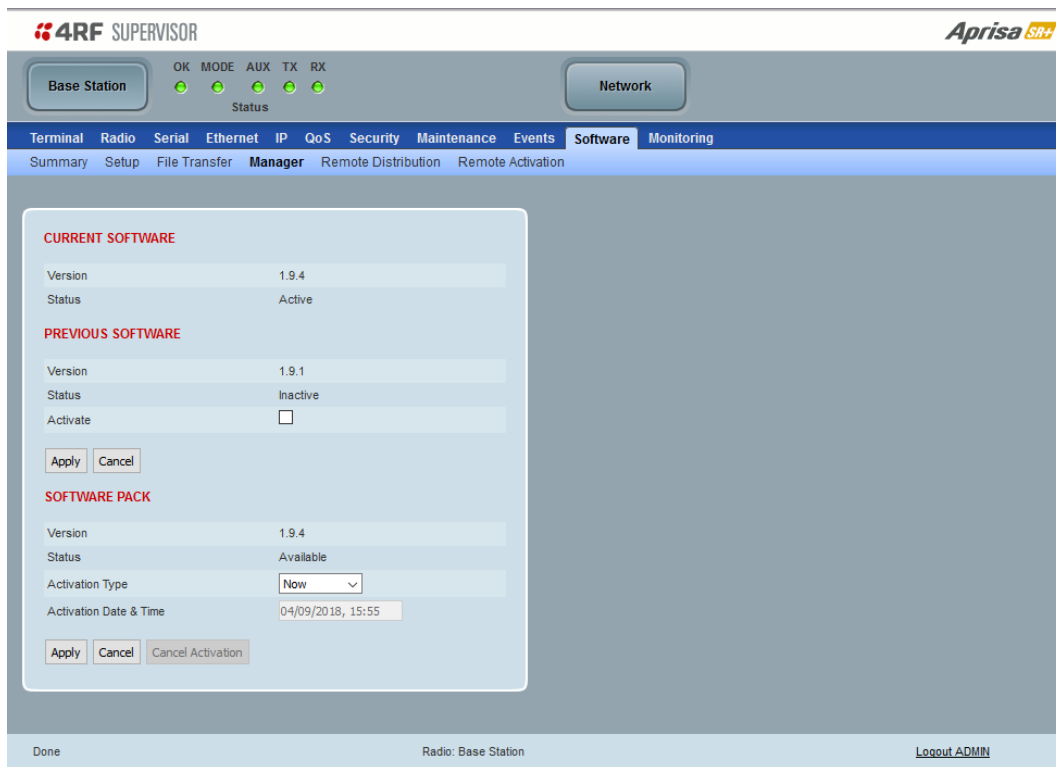
On linux type 'sha1sum -c <updatefile>.sha1' and check that the output contains 'OK'.

Software > Manager

This page summarises and manages the software versions available in the radio.

The manager is predominantly used to activate new software on single radios. Network activation is performed with 'Software > Remote Activation'.

Both the previous software (if available) and Software Pack versions can be activated on the radio from this page.



CURRENT SOFTWARE

Version

This parameter displays the software version running on the radio.

Status

This parameter displays the status of the software version running on the radio (always active).

PREVIOUS SOFTWARE

Version

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

Status

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

Option	Function
Active	The software is operating the radio.
Inactive	The software is not operating the radio but could be re-activated if required.

Activate

This parameter activates the previous software version (restores to previous version).

The Aprisa SR+ will automatically reboot after activation.

SOFTWARE PACK

Version

This parameter displays the software pack version available for distribution on base station and activate on all stations.

Status

This parameter displays the status of the software pack version.

Option	Function
Available	On the base station, the software pack is available for distribution. On all stations, the software pack is available for activation.
Activating	The software pack is activating in the radio.
Unavailable	There is no software pack loaded into the radio.

Activate

This parameter activates the software pack.

The Aprisa SR+ will automatically reboot after activation.

Activation Type

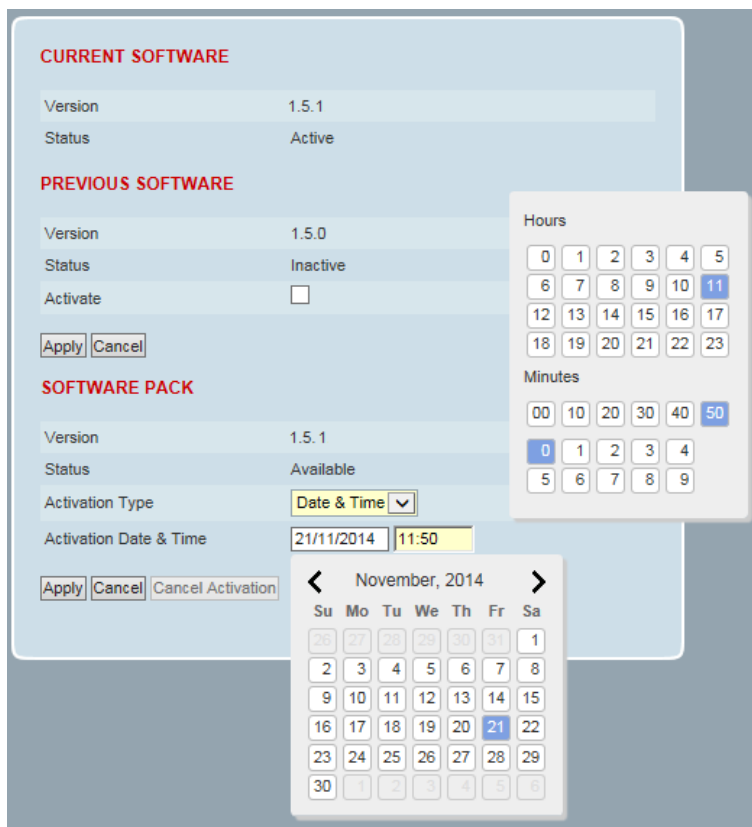
This parameter sets when the software pack activation will occur.

Option	Function
Now	Activates the software pack now.
Date & Time	Activates the software pack at the Date & Time set in the following parameter.

Activation Date & Time

This parameter sets the Date & Time when the software pack activation will occur.

This setting can be any future date and 24 hour time.



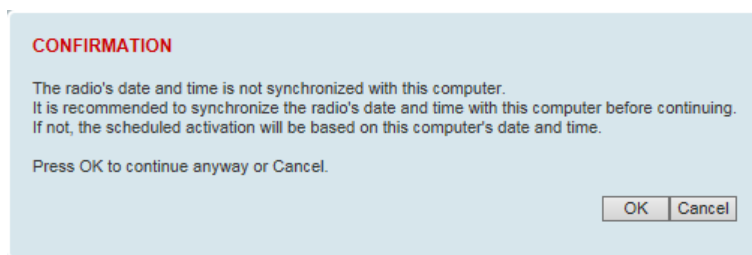
The screenshot displays the software activation configuration interface. It is divided into three main sections: **CURRENT SOFTWARE**, **PREVIOUS SOFTWARE**, and **SOFTWARE PACK**.

- CURRENT SOFTWARE:** Shows Version 1.5.1 and Status Active.
- PREVIOUS SOFTWARE:** Shows Version 1.5.0 and Status Inactive. There is an 'Activate' checkbox which is currently unchecked. Below this are 'Apply' and 'Cancel' buttons.
- SOFTWARE PACK:** Shows Version 1.5.1 and Status Available. The 'Activation Type' is set to 'Date & Time' (indicated by a dropdown arrow). The 'Activation Date & Time' is set to '21/11/2014' and '11:50'. Below this are 'Apply', 'Cancel', and 'Cancel Activation' buttons.

Two popups are overlaid on the interface for date and time selection:

- Hours Popup:** A grid showing hours from 0 to 23. The number 11 is selected.
- Minutes Popup:** A grid showing minutes from 00 to 50 in increments of 10. The number 50 is selected.
- Date Selection Popup:** A calendar view for November 2014. The date 21 is selected.

If the network base station radio date / time is not synchronized, you will get the following popup:



The screenshot shows a **CONFIRMATION** dialog box with the following text:

The radio's date and time is not synchronized with this computer.
It is recommended to synchronize the radio's date and time with this computer before continuing.
If not, the scheduled activation will be based on this computer's date and time.

Press OK to continue anyway or Cancel.

At the bottom right, there are 'OK' and 'Cancel' buttons.

You can manually enter the base station radio date / time or use the Date And Time Synchronization from a SNTP server feature (see 'Terminal > Date / Time' on page 113).

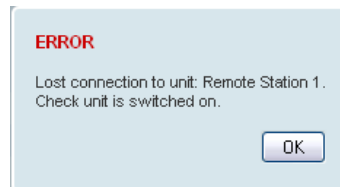
To activate a software version:

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.

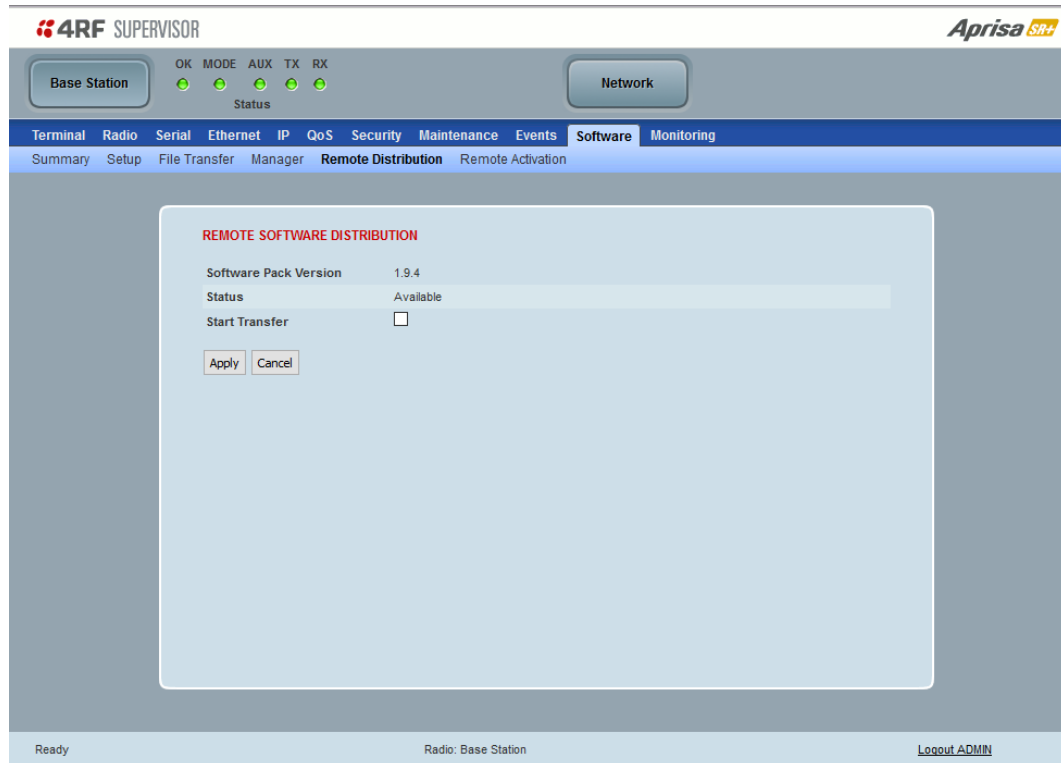
Software > Remote Distribution

This page provides the mechanism to distribute software to all remote radios 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 295) can be distributed via the radio link to all remote radios.

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 radios in the network.

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

The impact of software distribution traffic upon customer traffic is controlled by two settings. The traffic uses the 'Default Management Data Priority' QoS setting, and the rate of packets at this priority is controlled with the 'Background Bulk Data Transfer Rate' setting in Radio > Channel Setup.

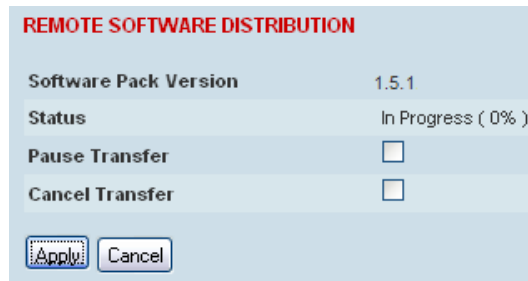
To distribute software to remote radios:

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 295).

1. Distribution is performed only to the radios listed in the Network Table and powered on. If a radio is listed in the network table, but cannot be contacted, it will slow down the distribution of software.

To ensure that the Network Table is up to date, it is recommended running the node discover function (see 'Discover Nodes' on page 276).

2. Click on 'Start Transfer'.



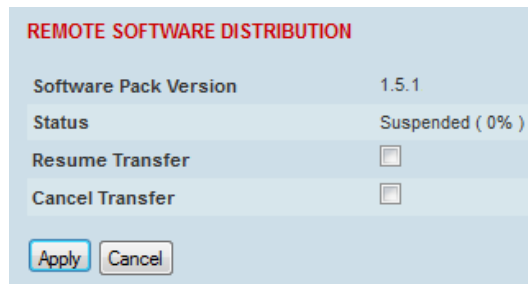
REMOTE SOFTWARE DISTRIBUTION	
Software Pack Version	1.5.1
Status	In Progress (0%)
Pause Transfer	☐
Cancel Transfer	☐
Apply Cancel	

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.



REMOTE SOFTWARE DISTRIBUTION	
Software Pack Version	1.5.1
Status	Suspended (0%)
Resume Transfer	☐
Cancel Transfer	☐
Apply Cancel	

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.

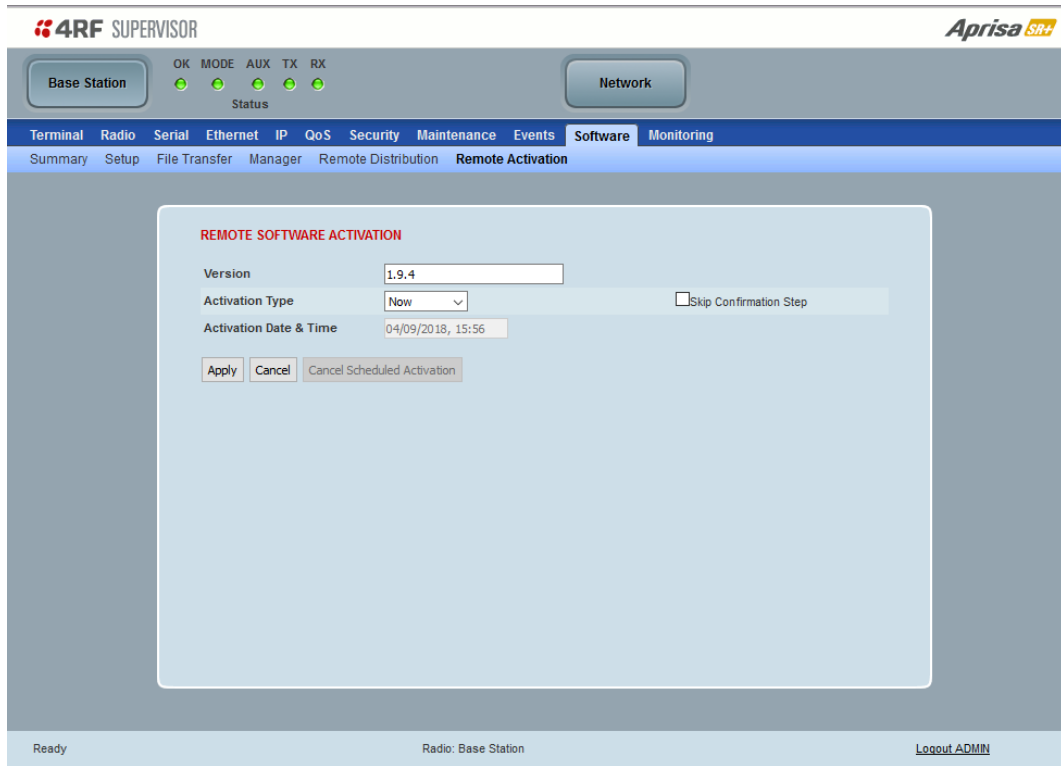
Software > Remote Activation

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

The Software Pack was loaded into the base station with the file transfer process (see ‘Software > File Transfer’ on page 295) and was distributed via the radio link to all remote radios.

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 radios, the software is then activated in all the remote radios with this command. If successful, then activate the software pack in the base station to complete the network upgrade.

Version

This parameter displays the software version for activation. The default version is the software pack version but any valid software version can be entered in the format ‘n.n.n’.

Activation Type

This parameter sets when the software pack activation will occur.

Option	Function
Now	Activates the software pack now.
Date & Time	Activates the software pack at the Date & Time set in the following parameter.

Activation Date & Time

This parameter sets the Date & Time when the software pack activation will occur.

This setting can be any future date and 24 hour time.

Skip Confirmation Step

This parameter when enabled skips the confirmation step during the activation process.

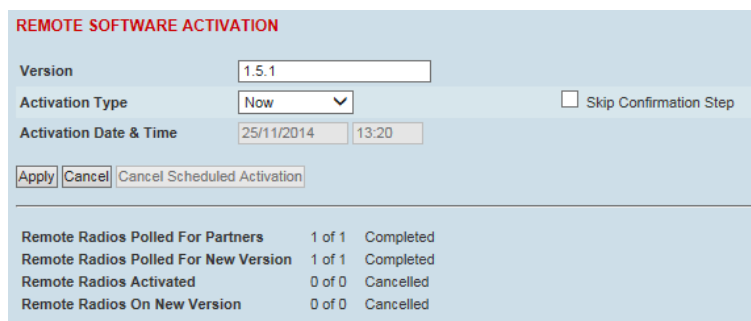
Normally, the confirmation step will require use intervention to accept the confirmation which will halt the activation process. Skipping the confirmation will enable the activation process to continue without use intervention.

To activate software in remote radios:

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 295) 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).



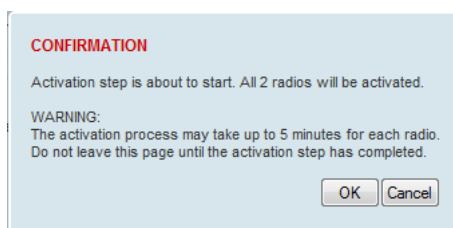
REMOTE SOFTWARE ACTIVATION		
Version	1.5.1	
Activation Type	Now	☐ Skip Confirmation Step
Activation Date & Time	25/11/2014 13:20	
Apply Cancel Cancel Scheduled Activation		
Remote Radios Polled For Partners	1 of 1	Completed
Remote Radios Polled For New Version	1 of 1	Completed
Remote Radios Activated	0 of 0	Cancelled
Remote Radios On New Version	0 of 0	Cancelled

2. Select the Activation type.
3. Click Apply.

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

Result	Function (X of Y)
Remote Radios Polled for Partners	X is the number of radios polled to determine the number of protected stations in the network. Y is the number of remote radios registered with the base station.
Remote Radios Polled for New Version	X is the number of radios polled to determine the number of radios that contain the new software version. Y is the number of remote radios registered with the base station.
Remote Radios Activated	X is the number of radios that contain the new software version and have been activated. Y is the number of radios that contain the new software version and can be activated.
Remote Radios On New Version	X is the number of radios that has been successfully activated and now running the new version of software. Y is the number of radios that the activation command was executed on. Note: When upgrading from software version 1.2.5 to 1.2.6 or later, communication to all remote radios will be lost due to a MAC protocol change. This will prevent this function from working correctly. In this case, activate the new software on the base station and run the 'Maintenance > Advanced' Discover Nodes function on page 276.

When the activation is ready to start:



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

The page will display the progress of the activation.

REMOTE SOFTWARE ACTIVATION

Version

Remote Radios Polled For Partners	4 of 4	Completed
Remote Radios Polled For New Version	0 of 4	Completed
Remote Radios Activated	0 of 0	Cancelled
Remote Radios On New Version	0 of 0	Cancelled

REMOTE ACTIVATION EXCEPTIONS

Name	IP Address	Version	Exception
Protected Remote Station	172.17.70.2	1.5.1	Software Version not on the radio (Step 2)
Remote125	172.17.70.125	1.5.1	Software Version not on the radio (Step 2)
Protected Remote Station	172.17.70.1	1.5.1	Software Version not on the radio (Step 2)

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 299).

INFORMATION

All remotes successfully activated.
Please install and activate software version 1.5.1 on the base station.

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

Activation Type

This parameter sets when the remote software activation will occur.

Option	Function
Now	Activates the remote software now.
Date & Time	Activates the remote software at the Date & Time set in the following parameter.

Skip Confirmation Step

This parameter when enabled skips the confirmation step during the activation process.

Normally, the confirmation step will require user intervention to accept the confirmation which will halt the activation process. Skipping the confirmation will enable the activation process to continue without user intervention.

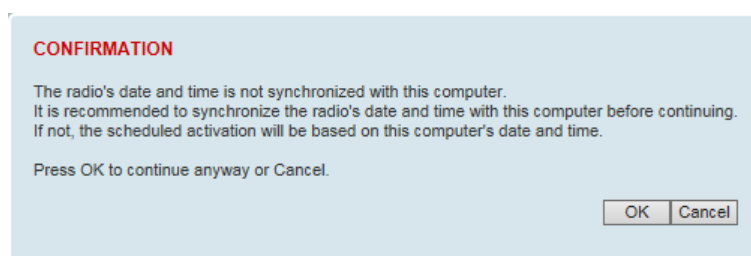
Activation Date & Time

This parameter sets the Date & Time when the remote software activation will occur.

This setting can be any future date and 24 hour time.

When the date and time is set, the remotes will be polled to setup the scheduled activation date and time.

If the network base station radio date / time is not synchronized, you will get the following popup:



You can manually enter the base station radio date / time or use the Date And Time Synchronization from a SNTP server feature (see 'Terminal > Date / Time' on page 113).

Monitoring

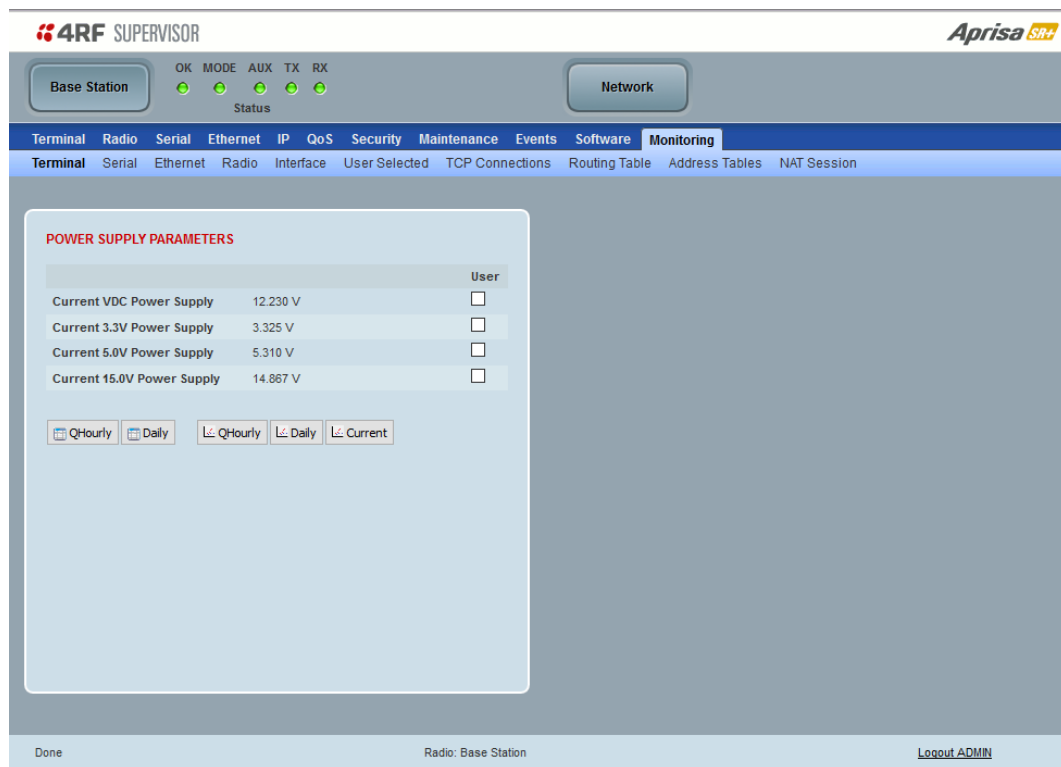
The Terminal, Serial, Ethernet, Radio and User Selected Monitored Parameter results have history log views for both Quarter Hourly and Daily.

Monitored parameter data is accumulated into 2 sets:

- 15 minutes of data, for 96 readings for the last 24 hours
- 24 hours of data, for 31 readings for the last 31 days.

Monitoring > Terminal

This page displays the current radio internal and external input source radio power supply voltage diagnostic parameters.



POWER SUPPLY PARAMETERS

Monitored Parameter	Function	Normal Operating Limits
Current VDC Power Supply	Parameter to show the current power supply input voltage.	10 to 30 VDC
Current 3.3 Volts Power Supply	Parameter to show the current 3.3 volt power rail voltage.	3.1 to 3.5 VDC
Current 5.0 Volts Power Supply	Parameter to show the current 5.0 volt power rail voltage.	4.7 to 5.5 VDC
Current 7.2 Volts Power Supply	Parameter to show the current 7.2 volt power rail voltage.	6.9 to 7.5 VDC
Current 15 Volts Power Supply	Parameter to show the current 15 volt power rail voltage. The 15 volt power supply is used to power the transmitter driver and power amplifier.	320, 400 and 450 MHz 14.5 to 15.3 VDC 135, 220, 896 and 928 MHz 12.7 to 13.5 VDC

Controls

The History Quarter Hourly button presents a log of results every quarter of an hour.

The screenshot shows the 4RF SUPERVISOR interface with the Aprisa SR+ logo. The 'Monitoring' tab is selected, and the 'Power Supply History, Quarter Hourly' window is open. The log displays power supply data for the period 01/11/2016 15:00 to 02/11/2016 22:00. The data is organized into a table with columns for time intervals and rows for various power supply metrics.

Power Supply	02/11/2016, 15:00	02/11/2016, 15:15	02/11/2016, 15:30	02/11/2016, 15:45	02/11/2016, 16:00	02/11/2016, 16:15	02/11/2016, 16:30	02/11/2016, 16:45	02/11/2016, 17:00	02/11/2016, 17:15
Maximum VDC Supply	12.269	12.269	12.278	12.269	12.269	12.269	12.269	12.278	12.269	12.269
Minimum VDC Supply	12.259	12.230	12.230	12.259	12.259	12.259	12.230	12.230	12.230	12.230
Maximum 3.3V Supply	3.325	3.325	3.325	3.325	3.325	3.325	3.325	3.325	3.325	3.325
Minimum 3.3V Supply	3.314	3.314	3.314	3.314	3.314	3.315	3.315	3.314	3.314	3.314
Maximum 5V Supply	5.310	5.310	5.310	5.308	5.310	5.308	5.308	5.310	5.310	5.308
Minimum 5V Supply	5.301	5.299	5.299	5.301	5.299	5.299	5.301	5.299	5.301	5.299
Maximum 15V Supply	14.957	14.957	14.957	14.957	14.957	14.957	14.957	14.957	14.957	14.957
Minimum 15V Supply	14.824	14.843	14.824	14.824	14.824	14.824	14.824	14.829	14.829	14.829

The interface includes a time range selector from 22:15 01/11/2016 to 22:00 02/11/2016, a 'Downloaded 7' indicator, and a 'Cancel' button. The status bar at the bottom shows 'Ready', 'Radio: Base Station', and a 'Logout ADMIN' link.

The History Daily button presents a log of results every day.

The screenshot shows the 4RF SUPERVISOR interface with the Aprisa SR+ logo. The 'Monitoring' tab is selected, and the 'Power Supply History, Daily' window is open. The log displays power supply data for the period 01/11/2016 to 01/11/2016. The data is organized into a table with columns for time intervals and rows for various power supply metrics.

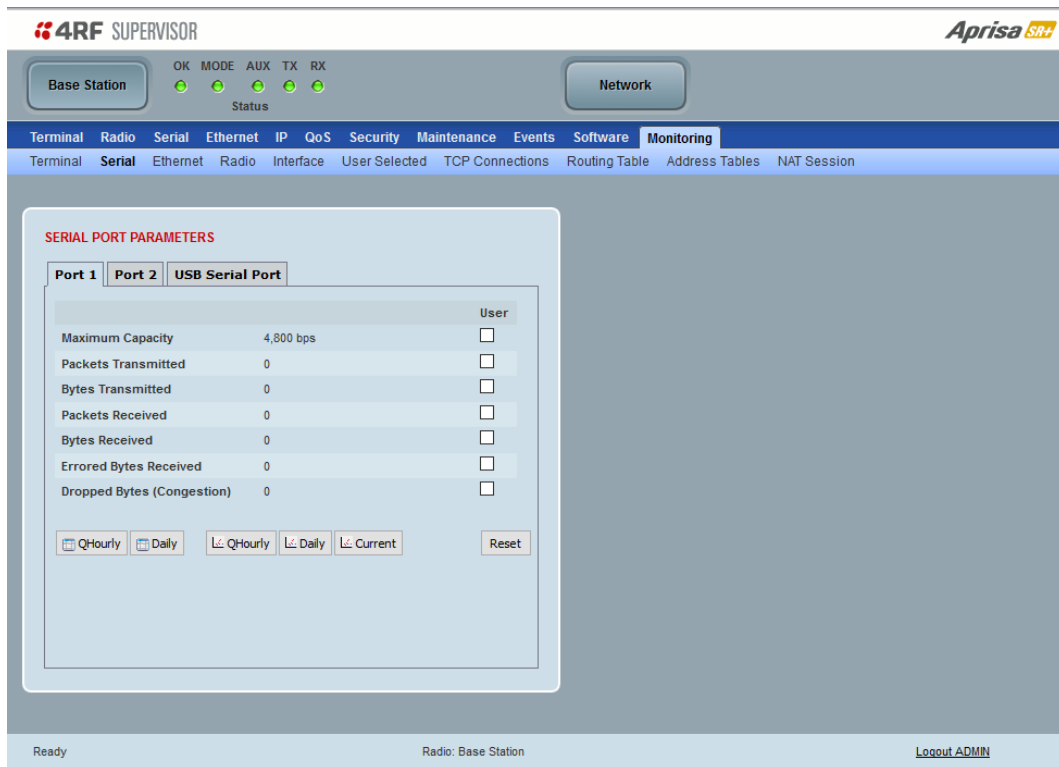
Power Supply	23/10/2016, 12:00	24/10/2016, 12:00	25/10/2016, 12:00	26/10/2016, 12:00	27/10/2016, 12:00	28/10/2016, 12:00	29/10/2016, 12:00	30/10/2016, 12:00	31/10/2016, 12:00	01/11/2016, 12:00
Maximum VDC Supply	-	12.249	12.278	12.288	12.278	12.278	12.269	12.278	12.278	12.278
Minimum VDC Supply	-	12.239	12.269	12.269	12.269	12.269	12.249	12.259	12.259	12.230
Maximum 3.3V Supply	-	3.325	3.325	3.325	3.325	3.325	3.325	3.325	3.325	3.325
Minimum 3.3V Supply	-	3.322	3.315	3.315	3.315	3.315	3.315	3.315	3.315	3.315
Maximum 5V Supply	-	5.308	5.308	5.308	5.308	5.310	5.310	5.310	5.308	5.310
Minimum 5V Supply	-	5.305	5.299	5.301	5.301	5.302	5.301	5.301	5.299	5.301
Maximum 15V Supply	-	14.890	14.952	14.952	14.952	14.952	14.957	14.957	14.957	14.957
Minimum 15V Supply	-	14.848	14.862	14.867	14.862	14.824	14.824	14.829	14.838	14.829

The interface includes a time range selector from 02/10/2016 to 01/11/2016, a 'Downloaded 1' indicator, and a 'Cancel' button. The status bar at the bottom shows 'Ready', 'Radio: Base Station', and a 'Logout ADMIN' link.

Monitoring > Serial

This page displays the current radio performance monitoring parameters per serial port in packet and byte level granularity, for serial port high level statistics and troubleshooting.

The results shown are since the page was opened and are updated automatically every 12 seconds.



SERIAL PORT PARAMETERS

All Serial Ports

Monitored Parameter	Function	Normal Operating Limits
Maximum Capacity	Parameter to show the maximum serial data rate of the serial port	Equal to the serial port baud rate setting
Packets Transmitted	Parameter to show the number of packets transmitted to the customer from the serial port	
Packets Received	Parameter to show the number of packets received from the customer into the serial port	
Bytes Received	Parameter to show the number of bytes received from the customer into the serial port	
Errored Bytes Received	Parameter to show the number of bytes received from the customer into the serial port that have errors	
Dropped Bytes (Congestion)	Parameter to show the number of bytes received from the customer into the serial port that are dropped due to over the air congestion	

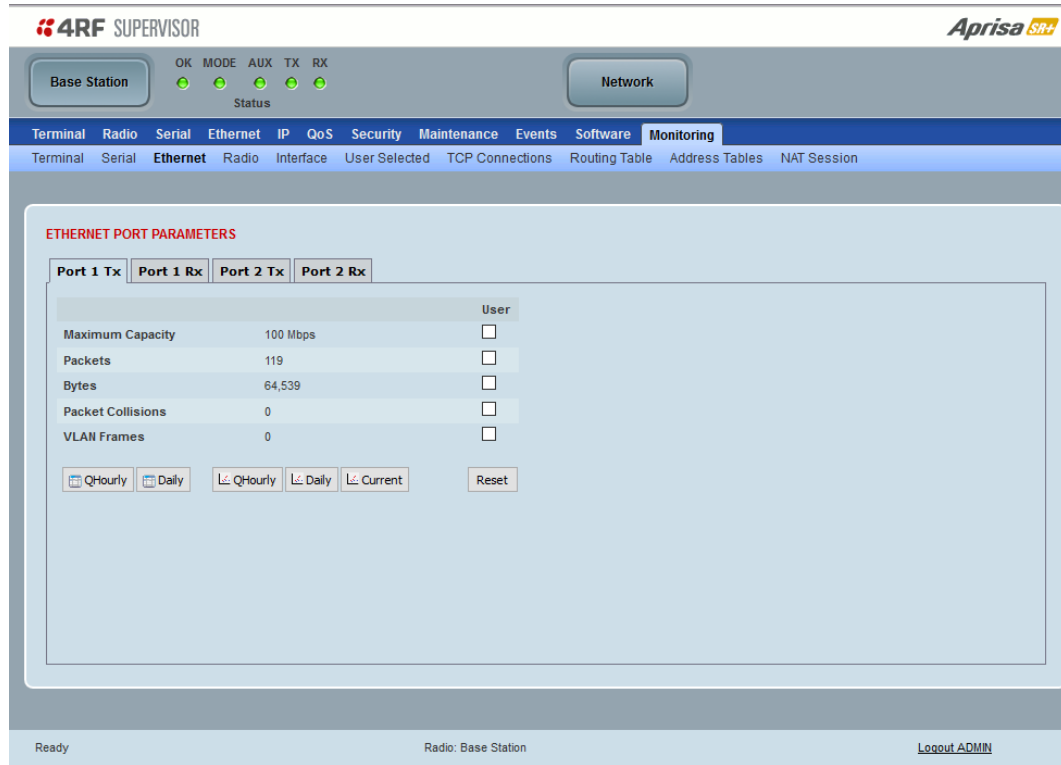
Controls

The Reset button clears the current results.

Monitoring > Ethernet

This page displays the current radio performance monitoring parameters per Ethernet port transmission (TX) out of the radio in packet and byte level granularity, for Ethernet port high level statistics and troubleshooting.

The results shown are since the page was opened and are updated automatically every 12 seconds.



ETHERNET PORT PARAMETERS

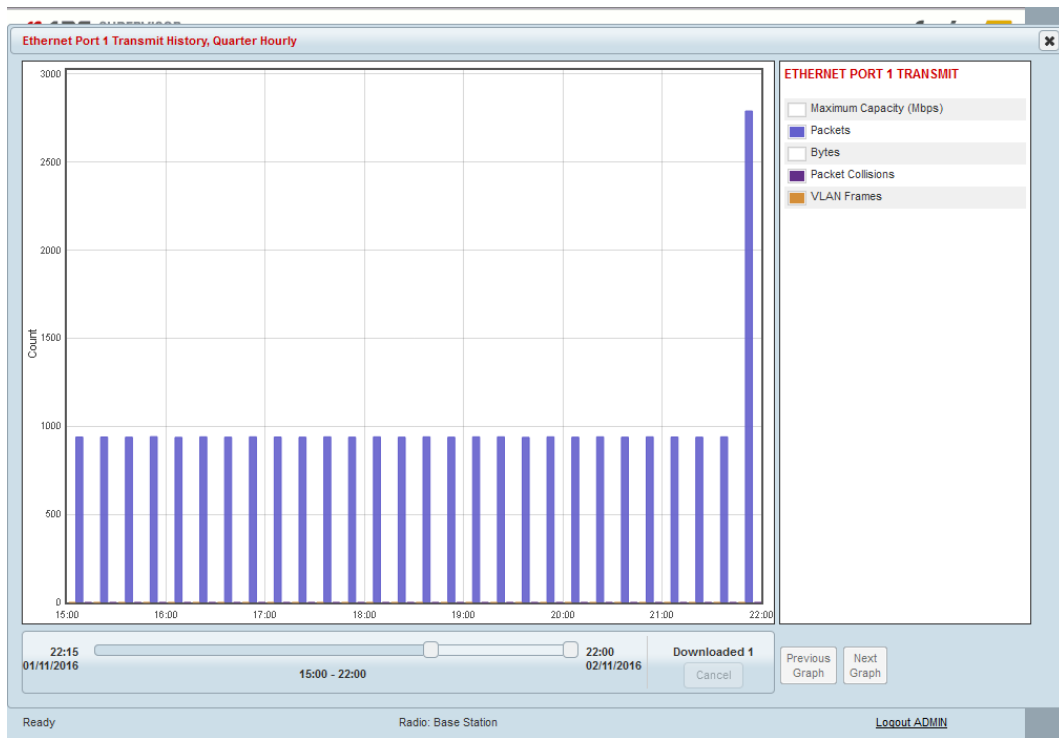
All Ethernet Ports TX (out)

Monitored Parameter	Function	Normal Operating Limits
Maximum Capacity	Parameter to show the maximum Ethernet data rate of the Ethernet port	Equal to the Ethernet port speed setting
Packets	Parameter to show the number of packets transmitted to the customer from the Ethernet port	
Bytes	Parameter to show the number of bytes transmitted to the customer from the Ethernet port	
Packet Collisions	Parameter to show the number of packet collisions on the data transmitted to the customer from the Ethernet port on a shared LAN	
VLAN Frames	Parameter to show the number of VLAN tagged frames transmitted to the customer from the Ethernet port	

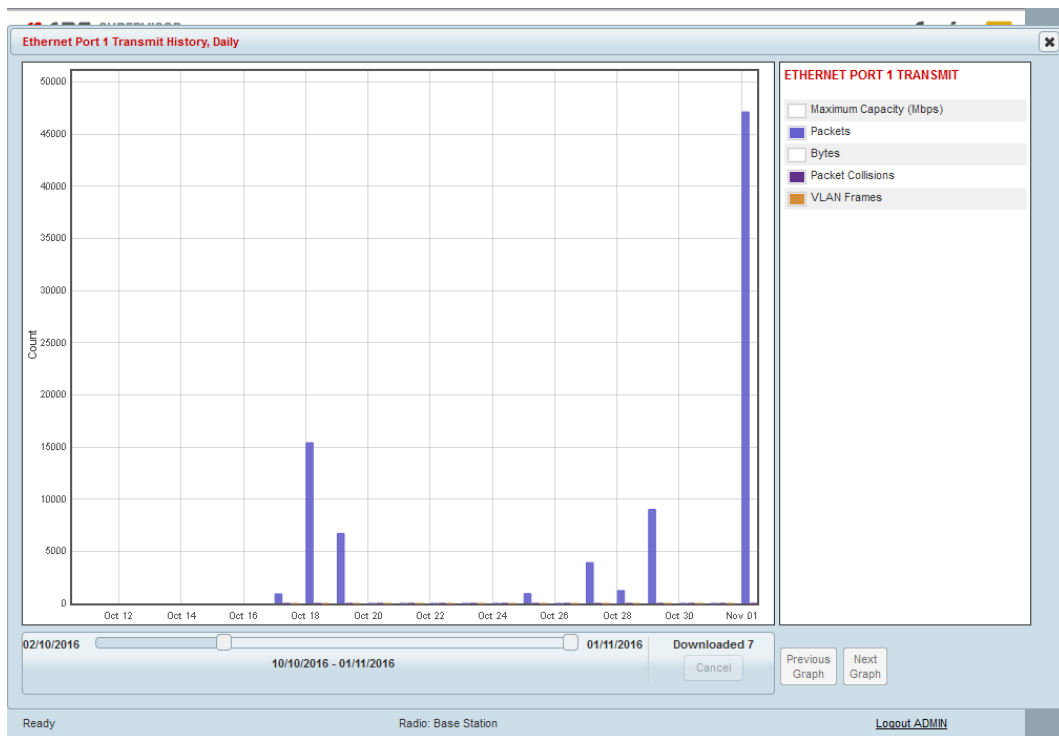
Controls

The Reset button clears the current results.

The History QHourly button presents a graph of results every quarter of an hour.



The History Daily button presents a graph of results every day.



This page displays the current radio performance monitoring parameters per Ethernet port received (RX) data in packet and byte level granularity, for Ethernet port high level statistics and troubleshooting.

The results shown are since the page was opened and are updated automatically every 12 seconds.



ETHERNET PORT PARAMETERS

All Ethernet Ports RX (in)

Monitored Parameter	Function
Packets	Parameter to show the number of packets received from the customer into the Ethernet port (including broadcasts, multicasts, unicasts, FCS/CRC error, alignment error, undersize, jabber, oversize, and fragments)
Bytes	Parameter to show the number of bytes received from the customer into the Ethernet port (including broadcasts, multicasts, unicasts, FCS/CRC error, alignment error, undersize, jabber, oversize, and fragments and excluding IFG framing bytes/bits)
Packets equal to 64 bytes	Parameter to show the number of packets received from the customer into the Ethernet port that are equal to 64 bytes (including broadcasts, multicasts, unicasts, FCS/CRC error, alignment error, undersize, jabber, oversize, and fragments)
Packets 65 to 127 bytes	Parameter to show the number of packets received from the customer into the Ethernet port that are between 65 and 127 bytes (including broadcasts, multicasts, unicasts, FCS/CRC error, alignment error, undersize, jabber, oversize, and fragments)
Packets 128 to 255 bytes	Parameter to show the number of packets received from the customer into the Ethernet port that are between 128 and 255 bytes (including broadcasts, multicasts, unicasts, FCS/CRC error, alignment error, undersize, jabber, oversize, and fragments)
Packets 256 to 511 bytes	Parameter to show the number of packets received from the customer into the Ethernet port that are between 256 and 511 bytes (including broadcasts, multicasts, unicasts, FCS/CRC error, alignment error, undersize, jabber, oversize, and fragments)
Packets 512 to 1023 bytes	Parameter to show the number of packets received from the customer into the Ethernet port that are between 512 and 1023 bytes (including broadcasts, multicasts, unicasts, FCS/CRC error, alignment error, undersize, jabber, oversize, and fragments)
Packets 1024 to 1536 bytes	Parameter to show the number of packets received from the customer into the Ethernet port that are between 1024 and 1536 bytes (including broadcasts, multicasts, unicasts, FCS/CRC error, alignment error, undersize, jabber, oversize, and fragments)

Monitored Parameter	Function
Broadcast Packets	Parameter to show the number of broadcast packets received from the customer into the Ethernet port. Broadcast packets are good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Packets	Parameter to show the number of multicast packets received from the customer into the Ethernet port. Multicast packets are packets that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
VLAN Frames	Parameter to show the number of VLAN tagged frames received from the customer into the Ethernet port, including filtering, congestion but excludes VLAN dropped packets.
VLAN Frames Dropped	Parameter to show the number of VLAN tagged frames received from the customer into the Ethernet port that were dropped due to filtered VLAN frames (filtering configuration in VLAN configuration). L3 filtered packets, bad packets or congestion dropped packets are not counted in this parameter.
Packet In Error	Parameter to show the number of errored packets received from the customer into the Ethernet port caused by CRC errors, FCS Errors, alignment errors, oversized packets, undersized packets, fragmented packets and jabber packets.
Bytes In Error	Parameter to show the number of errored bytes received from the customer into the Ethernet port.
CRC / Alignment Error	Parameter to show the number of CRC / alignment errors received from the customer into the Ethernet port. CRC / alignment errors are defined as frames that had a length excluding framing bits, but including FCS octets of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets.
Undersized Packets	Parameter to show the number of undersized packets received from the customer into the Ethernet port. Undersized packets are less than 64 octets long excluding framing bits, but including FCS octets.
Oversized Packets	Parameter to show the number of oversized packets received from the customer into the Ethernet port. Oversized packets are longer than 1518 octets excluding framing bits, but including FCS octets.
Fragmented Packets	Parameter to show the number of fragmented packets received from the customer into the Ethernet port. Fragmented packets have either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS.
Jabber Packets	Parameter to show the number of jabber packets received from the customer into the Ethernet port.
Dropped Packets (congestion)	Parameter to show the number of dropped packets received from the customer into the Ethernet port due to congestion i.e., when the Ethernet port 125 packet buffers are full, the next received packet on the ingress Ethernet port will be dropped.
Dropped Packets (filtering)	Parameter to show the number of dropped packets received from the customer into the Ethernet port caused by packet L2 / L3 filtering.
Dropped Bytes (filtering)	Parameter to show the number of dropped bytes received from the customer into the Ethernet port caused by packet L2 / L3 filtering.

Controls

The Reset button clears the current results.

The History QHourly button presents a log of results every quarter of an hour.

4RF SUPERVISOR

Aprisa SR+

Ethernet Port 1 Receive History, Quarter Hourly

Ethernet Port 1 Receive	02/11/2016, 19:45	02/11/2016, 20:00	02/11/2016, 20:15	02/11/2016, 20:30	02/11/2016, 20:45	02/11/2016, 21:00	02/11/2016, 21:15	02/11/2016, 21:30	02/11/2016, 21:45	02/11/2016, 22:00
Packets	983	987	984	986	984	986	985	984	991	2,481
Bytes	81,097	81,589	81,192	81,334	81,192	81,401	81,256	81,192	82,189	371,750
Packets equal to 64 Bytes	37	38	37	38	37	38	38	37	38	970
Packets 65 to 127 Bytes	900	902	901	902	901	902	901	901	902	1,057
Packets 128 to 255 Bytes	45	46	45	45	45	45	45	45	50	54
Packets 256 to 511 Bytes	1	1	1	1	1	1	1	1	1	115
Packets 512 to 1023 Bytes	0	0	0	0	0	0	0	0	0	285
Packets 1024 to 1536 Bytes	0	0	0	0	0	0	0	0	0	0
Broadcast Packets	31	33	32	32	32	32	32	32	32	34
Multicast Packets	15	14	14	14	14	14	14	14	19	19
VLAN Frames	0	0	0	0	0	0	0	0	0	0
VLAN Frames Dropped	0	0	0	0	0	0	0	0	0	0
Packets in Error	0	0	0	0	0	0	0	0	0	0
Bytes in Error	0	0	0	0	0	0	0	0	0	0
CRC/Alignment Errors	0	0	0	0	0	0	0	0	0	0
Undersized Packets	0	0	0	0	0	0	0	0	0	0
Oversized Packets	0	0	0	0	0	0	0	0	0	0
Fragmented Packets	0	0	0	0	0	0	0	0	0	0
Jabber Packets	0	0	0	0	0	0	0	0	0	0
Dropped Packets (Congestion)	0	0	0	0	0	0	0	0	0	0
Dropped Packets (Filtering)	46	47	46	46	46	47	45	46	51	52
Dropped Bytes (Filtering)	8,529	8,801	8,546	8,546	8,546	8,801	8,358	8,546	9,401	9,680

LeftRight

22:15 01/11/201622:00 to 22:00 02/11/2016Downloaded 1Cancel

The History Daily button presents a log of results every day.

4RF SUPERVISOR

Aprisa SR+

Ethernet Port 1 Receive History, Daily

Ethernet Port 1 Receive	23/10/2016, 12:00	24/10/2016, 12:00	25/10/2016, 12:00	26/10/2016, 12:00	27/10/2016, 12:00	28/10/2016, 12:00	29/10/2016, 12:00	30/10/2016, 12:00	31/10/2016, 12:00	01/11/2016, 12:00
Packets	66	586	1,477	1,040	3,898	1,170	9,207	0	0	48,858
Bytes	8,309	105,684	246,127	192,601	731,958	210,521	1,671,037	0	0	5,991,201
Packets equal to 64 Bytes	14	2	511	2	2,074	611	5,050	0	0	10,025
Packets 65 to 127 Bytes	29	18	122	10	577	121	1,646	0	0	32,155
Packets 128 to 255 Bytes	22	533	681	1,008	277	199	178	0	0	2,026
Packets 256 to 511 Bytes	1	33	79	20	325	81	862	0	0	1,445
Packets 512 to 1023 Bytes	0	0	84	0	645	158	1,471	0	0	3,204
Packets 1024 to 1536 Bytes	0	0	0	0	0	0	0	0	0	3
Broadcast Packets	18	95	355	647	69	92	53	0	0	1,508
Multicast Packets	48	491	457	393	256	229	178	0	0	977
VLAN Frames	0	0	0	0	0	0	0	0	0	0
VLAN Frames Dropped	0	0	0	0	0	0	0	0	0	0
Packets in Error	0	0	0	0	0	0	0	0	0	0
Bytes in Error	0	0	0	0	0	0	0	0	0	0
CRC/Alignment Errors	0	0	0	0	0	0	0	0	0	0
Undersized Packets	0	0	0	0	0	0	0	0	0	0
Oversized Packets	0	0	0	0	0	0	0	0	0	0
Fragmented Packets	0	0	0	0	0	0	0	0	0	0
Jabber Packets	0	0	0	0	0	0	0	0	0	0
Dropped Packets (Congestion)	0	0	0	0	0	0	0	0	0	0
Dropped Packets (Filtering)	67	585	805	1,040	318	295	223	0	0	2,466
Dropped Bytes (Filtering)	8,504	105,417	141,056	192,589	55,749	46,768	36,235	0	0	419,347

02/10/2016

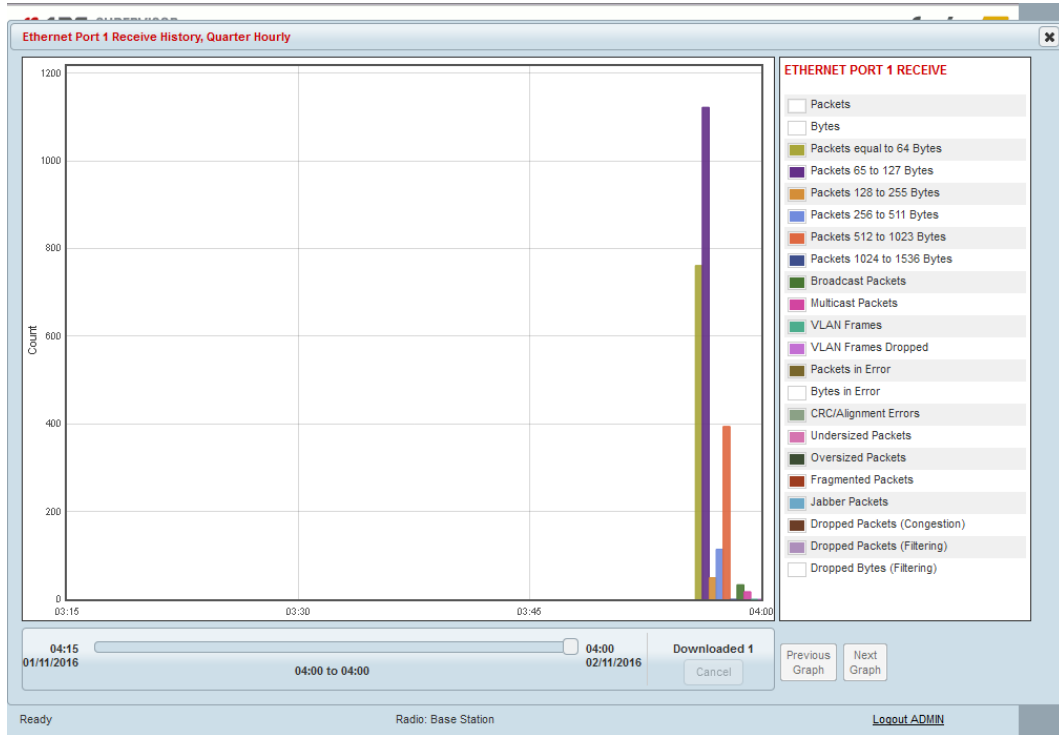
01/11/2016 to 01/11/2016

01/11/2016

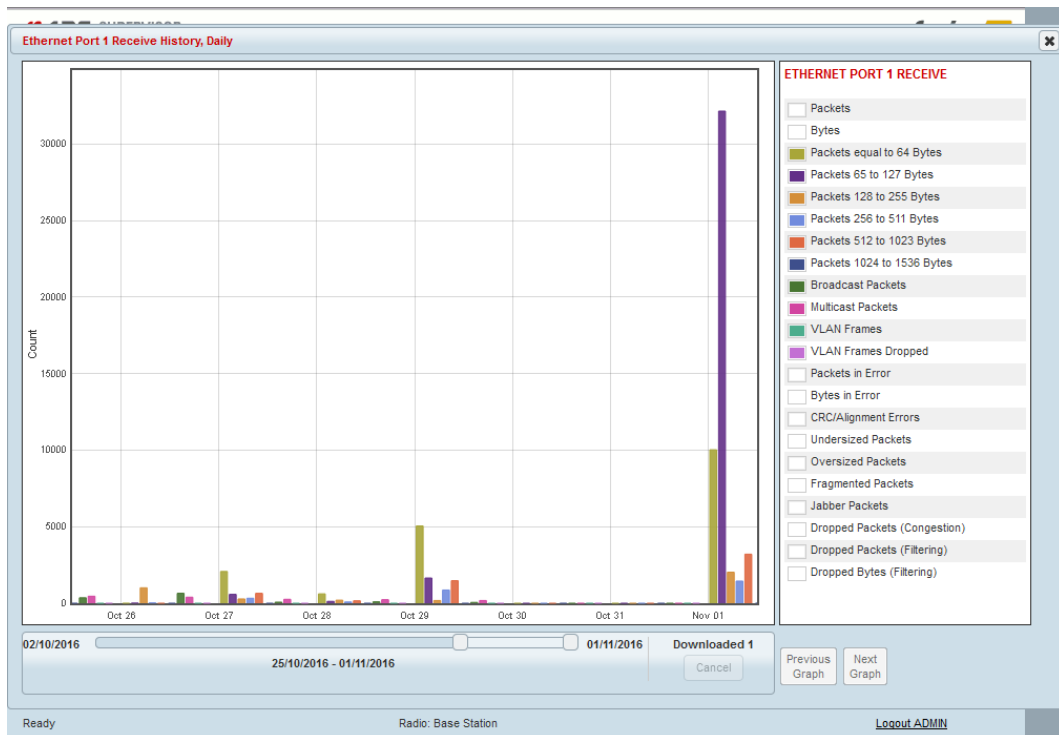
Downloaded 1

Cancel

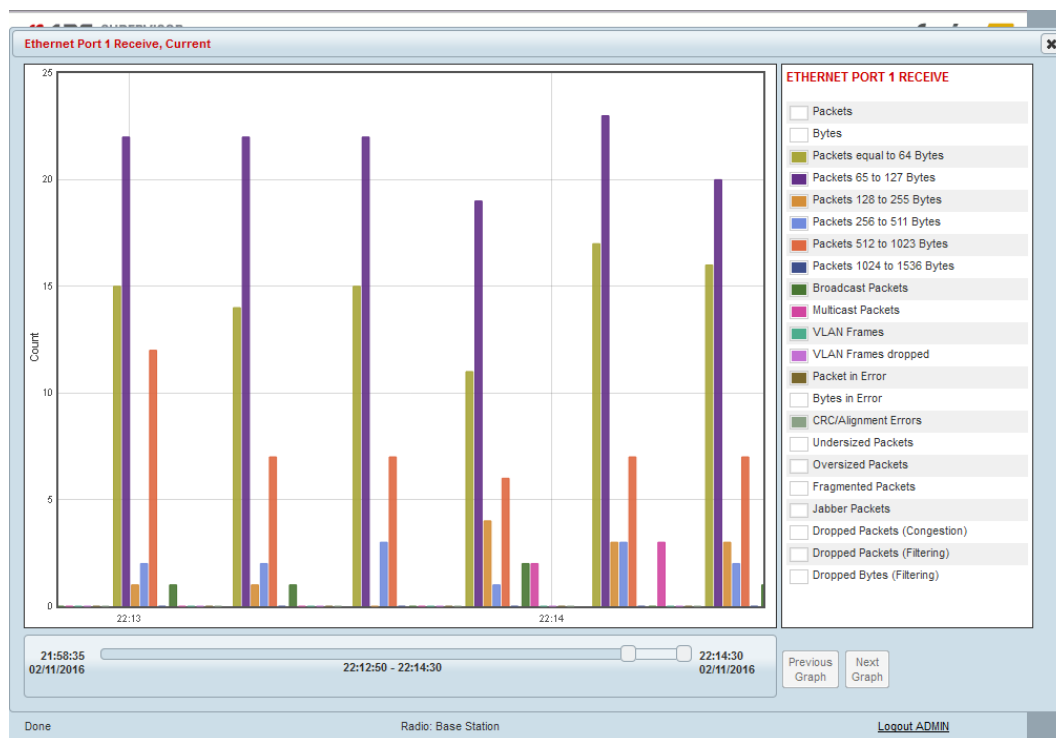
The Graph QHourly button presents a graph of results every quarter of an hour.



The Graph Daily button presents a graph of results every day.



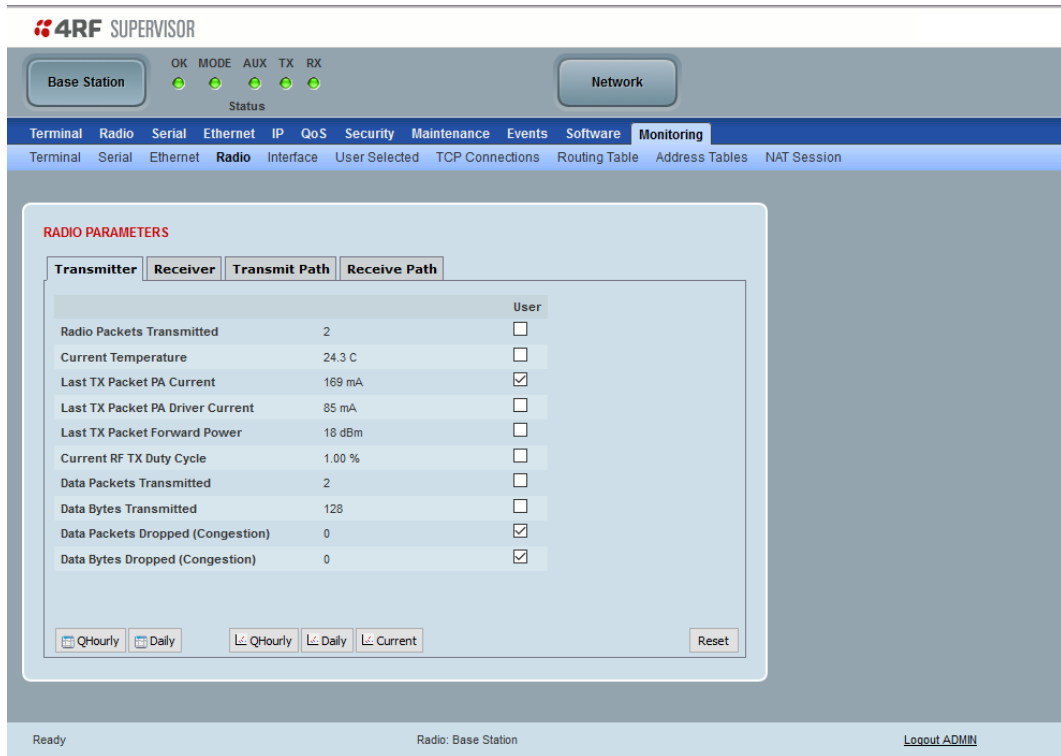
The Graph Current button presents a graph of current results.



Monitoring > Radio

This page displays the current radio diagnostic and performance monitoring parameters of the radio transmitter.

The results shown are since the page was opened and are updated automatically every 12 seconds.



The screenshot shows the 4RF SUPERVISOR interface. At the top, there are status indicators for OK, MODE, AUX, TX, and RX, all of which are green. Below these are buttons for 'Base Station' and 'Network'. A navigation bar includes links for Terminal, Radio, Serial, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring (which is highlighted). Under the Monitoring tab, there are sub-links: Terminal, Serial, Ethernet, Radio (highlighted), Interface, User Selected, TCP Connections, Routing Table, Address Tables, and NAT Session.

The main content area is titled 'RADIO PARAMETERS' and contains four tabs: Transmitter, Receiver, Transmit Path, and Receive Path. The 'Transmitter' tab is active, showing a table of parameters with their current values and checkboxes for user-defined limits.

Parameter	Value	User
Radio Packets Transmitted	2	☐
Current Temperature	24.3 C	☐
Last TX Packet PA Current	169 mA	☒
Last TX Packet PA Driver Current	85 mA	☐
Last TX Packet Forward Power	18 dBm	☐
Current RF TX Duty Cycle	1.00 %	☐
Data Packets Transmitted	2	☐
Data Bytes Transmitted	128	☐
Data Packets Dropped (Congestion)	0	☒
Data Bytes Dropped (Congestion)	0	☒

Below the table are buttons for 'QHourly', 'Daily', 'L. QHourly', 'L. Daily', 'L. Current', and a 'Reset' button.

At the bottom of the interface, it says 'Ready' on the left, 'Radio: Base Station' in the center, and 'Logout ADMIN' on the right.

RADIO PARAMETERS

Transmitter

Monitored Parameter	Function	Normal Operating Limits
Radio Packets Transmitted	Parameter to show the number of radio packets transmitted over the air. This may be lower than Data Packets Transmitted in the case of packet aggregation or may be higher than Data Packets Transmitted in cases such as radio retries, base-repeated packets, and repeater store and forward.	
Current Temperature	Parameter to show the current temperature of the transmitter.	0 to 70 °C
Last TX Packet PA Current	Parameter to show the current consumed by the transmitter power amplifier in mA. The value is stored from the last time the transmitter was active and transmitted a packet.	This value will change depending on the transmitter power setting, modulation, temperature and the VSWR of the antenna. The alarm limits for this are 50 mA to 2.5 A
Last TX Packet PA Driver Current	Parameter to show the current consumed by the transmitter power amplifier driver in mA. The value is stored from the last time the transmitter was active and transmitted a packet.	This value will change depending on the transmitter power setting, modulation and temperature. The alarm limits for the PA Driver Current are 10 mA to 500 mA.
Last TX Packet Forward Power	Parameter to show the actual transmitter power in dBm. The value is stored from the last time the transmitter was active and transmitted a packet.	This value will be dependent on the output power, the ATPC setting, the temperature and the VSWR of the antenna. The alarm limits for the Tx forward power are +/- 4 dB.

Monitored Parameter	Function	Normal Operating Limits
Last TX Packet Reverse Power (note ¹)	Parameter to show the reflected power. The value is stored from the last time the transmitter was active and transmitted a packet.	The value will be dependent on the impedance presented to that antenna port of the radio by the feeder and antenna system. A reflected power of 15 dB below the transmit power shows an acceptable performance.
Last TX Packet VSWR (note ¹)	Parameter to show numerically how well the antenna is impedance matched to the radio. The value is stored the last time the transmitter was active and transmitted a packet.	This value will be dependent on the feeder and antenna performance, a value of <1.5:1 shows acceptable performance. A value of >3.0:1 would indicate that most of the power is being reflected to the radio and that there is a fault in the feeder or antenna.
Current RF TX Duty Cycle	Parameter to show the average percentage of the RF channel utilization	Dependent on the amount of TX traffic
Data Packets Transmitted	Parameter to show the number of individual data packets transmitted over the air.	
Data Bytes Transmitted	Parameter to show the number of bytes transmitted over the air.	
Data Packets Dropped (congestion)	Parameter to show the number of dropped data packets not transmitted over the air due to the Time-To-Live (TTL) expiry of the packets in the egress buffer of the RF port. The TTL per interface is configured in 'Radio > Advanced Setup'.	
Data Bytes Dropped (congestion)	Parameter to show the number of dropped bytes not transmitted over the air due to congestion.	

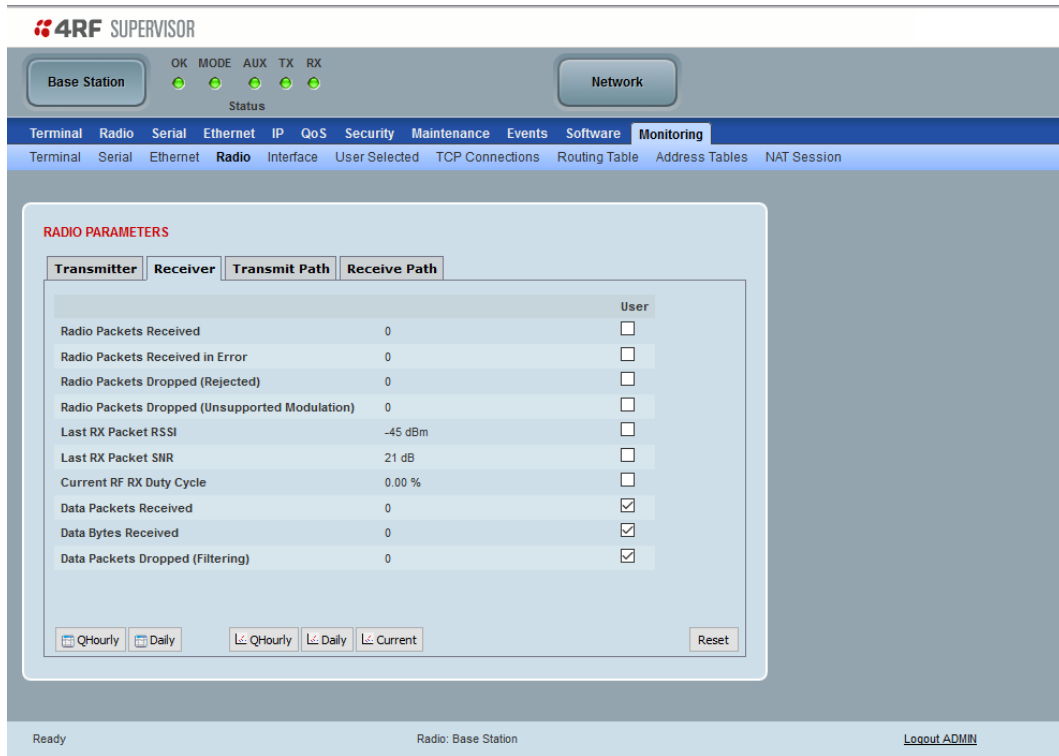
Note 1: Currently only some hardware variants are capable of providing this data. If these parameters are not shown on the Radio Parameters > Transmitter page, the hardware variant is not capable of providing this data.

Controls

The Reset button clears the current results.

This page displays the current radio performance monitoring parameters of radio receiver.

The results shown are since the page was opened and are updated automatically every 12 seconds.



The screenshot shows the 4RF SUPERVISOR interface. At the top, there are status indicators for Base Station (OK, MODE, AUX, TX, RX) and Network. Below this is a navigation bar with tabs for Terminal, Radio, Serial, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring. The Monitoring tab is active, and the Radio sub-tab is selected. The main content area displays the RADIO PARAMETERS section, which includes a table of monitored parameters for the Receiver. The table has columns for the parameter name, its value, and a checkbox for the User. The parameters are: Radio Packets Received (0), Radio Packets Received in Error (0), Radio Packets Dropped (Rejected) (0), Radio Packets Dropped (Unsupported Modulation) (0), Last RX Packet RSSI (-45 dBm), Last RX Packet SNR (21 dB), Current RF RX Duty Cycle (0.00 %), Data Packets Received (0), Data Bytes Received (0), and Data Packets Dropped (Filtering) (0). The checkboxes for Data Packets Received, Data Bytes Received, and Data Packets Dropped (Filtering) are checked. At the bottom of the table, there are buttons for Q:Hourly, D:Daily, L: Q:Hourly, L: Daily, L: Current, and a Reset button. The status bar at the bottom shows 'Ready', 'Radio: Base Station', and a 'Logout ADMIN' link.

Receiver

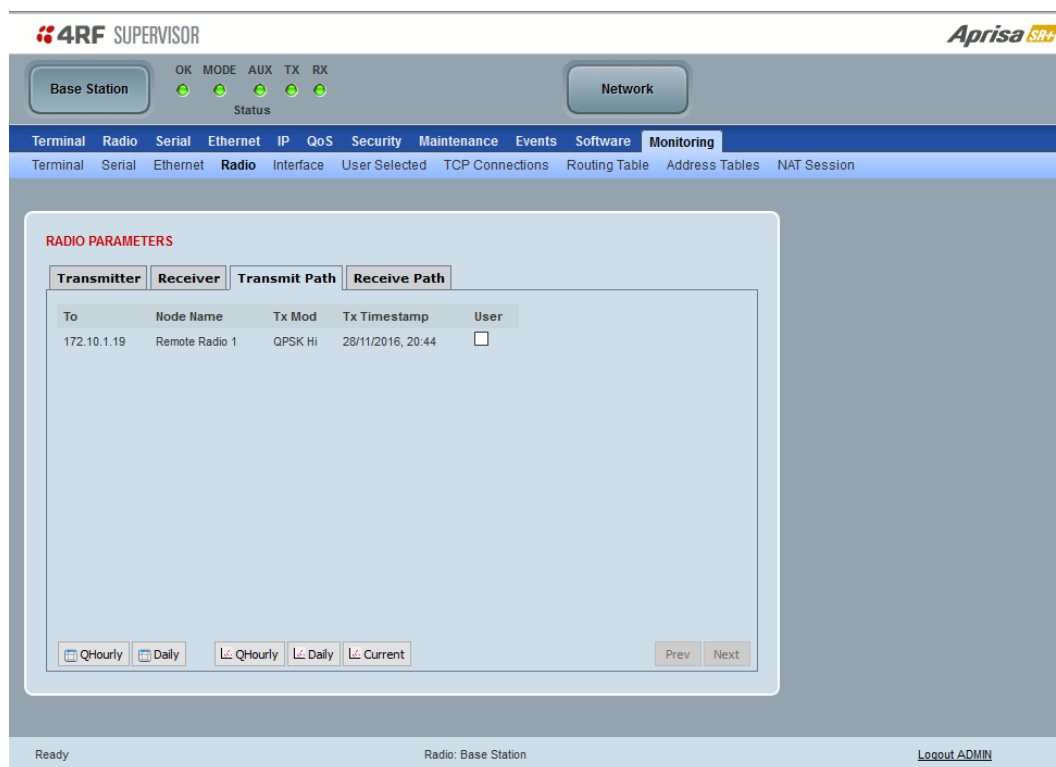
Monitored Parameter	Function	
Radio Packets Received	Parameter to show the number of radio packets received over the air without errors. This may be lower than Data Packets Received in the case of packet aggregation or may be higher than Data Packets Received in cases such as radio retries, base-repeated packets, and repeater store and forward.	
Radio Packets Received In Error	Parameter to show the number of radio packets received over the air that contained errors. It is normal to see this counter increment when ACM is enabled, and a unicast packet is sent to another radio that supports a faster modulation.	
Radio Packets Dropped (Rejected)	Parameter to show the number of radio packets rejected from overlapping SR+ radio networks. Counter is only updated when 'Enhanced Noise Rejection Mode' is configured to 'Channel Reuse and Noise Rejection'.	
Radio Packets Dropped (Unsupported Modulation)	Parameter to show the number of radio packets dropped because received packets were of higher modulation when this remote radio is only capable of lower modulations due to low SNR and when ACM is enabled.	
Last RX Packet RSSI	Parameter to show the received signal strength.	Expected values for a normally operating radio are between -115 to -10 dBm
Last RX Packet SNR	Parameter to show the received signal to noise ratio.	Typical values for SNR > 12 dB. No signal received = 0 dB
Current RF RX Duty Cycle	Parameter to show the average percentage of the RF channel utilization	Dependent on the amount of RX traffic
Data Packets Received	Parameter to show the number of packets received over the air	
Data Bytes Received	Parameter to show the number of bytes received over the air	
Data Packets Dropped (Filtering)	Parameter to show the number of packets dropped because received packets were either destined for another radio or could not be decrypted. It is normal to see this counter increment as radios filter out unicast Ethernet or management packets.	

Controls

The Reset button clears the current results.

This page displays the current radio RF transmit path modulation setting to single or multiple destination radios that the radio is transmitting to.

The results shown are since the page was opened and are updated automatically every 12 seconds.



Transmit Path

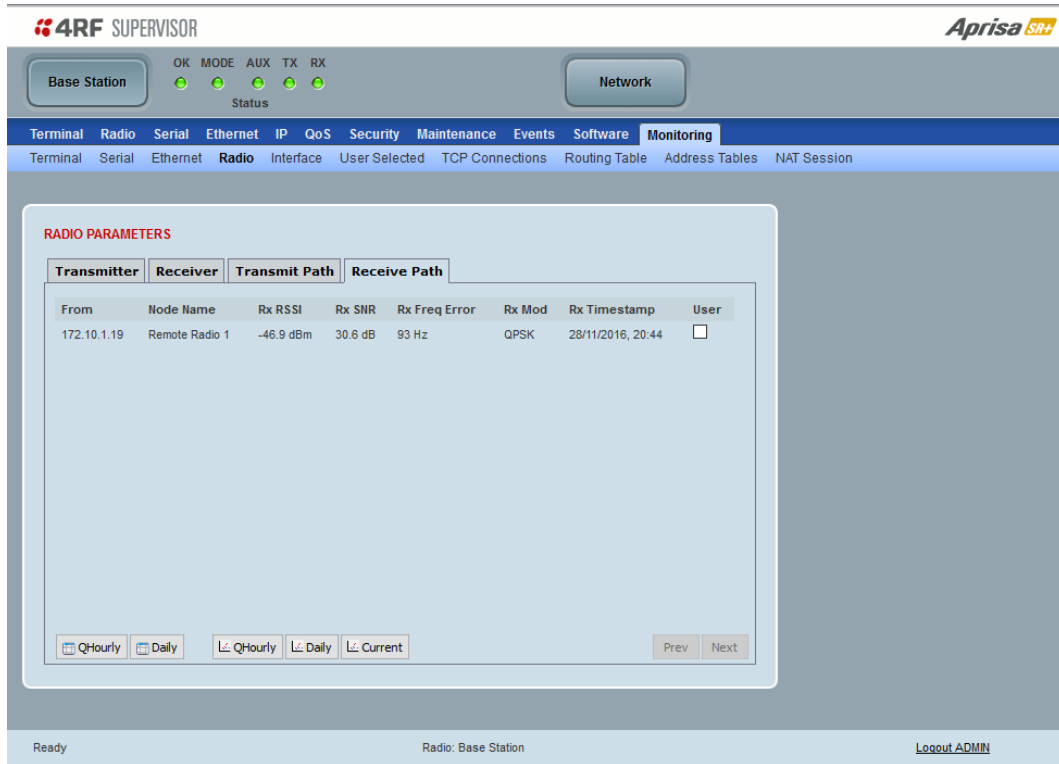
Result	Function
To	The destination IP Address and Node Name of the radio/s transmitting data to.
Tx Mod	The current radio transmitter modulation being used to communicate with the destination radio/s.
Tx Timestamp	The timestamp of the last transmitted packet to the destination radio/s.

Controls

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

This page displays the current radio RF receive path parameters from single or multiple source radios that the radio is receiving from.

The results shown are since the page was opened and are updated automatically every 12 seconds.



Receive Path

Result	Function
From	The IP Address and Node Name of the radio receiving data from.
Rx RSSI	The RSSI of the RF signal received from the source radio/s. This parameter displays the receiver RSSI reading taken from the last data packet received.
Rx SNR	The SNR of the RF signal received from the source radio/s. This parameter displays the receiver SNR reading taken from the last data packet received.
Rx Freq Error	The frequency difference between this radio's receiver and the frequency of the incoming packet rate from the source radio/s.
Rx Mod	The current radio receive modulation being used to communicate with the source radio/s.
Rx Timestamp	The timestamp of the last received packet from the source radio/s.

Controls

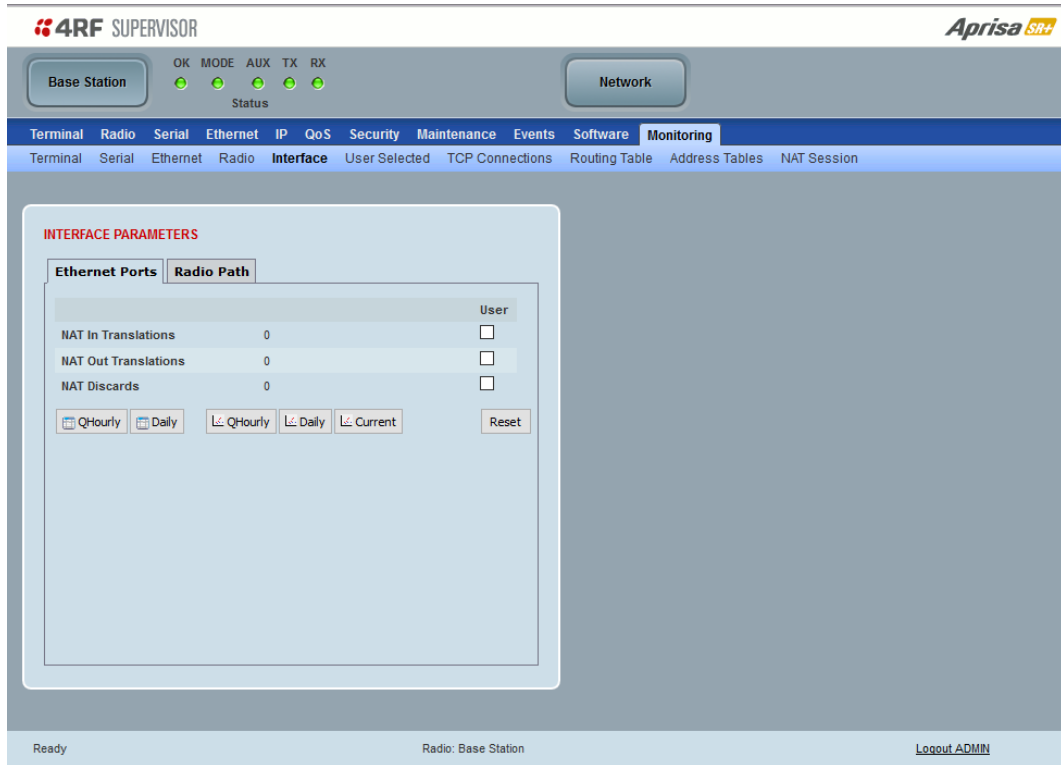
The Next button will display the next page of 8 radios and the Prev button will display the previous page of 8 radios.

Monitoring > Interface

This page displays the current radio Network Address Translation statistics.

The results shown are since the page was opened and are updated automatically every 12 seconds.

Ethernet Ports

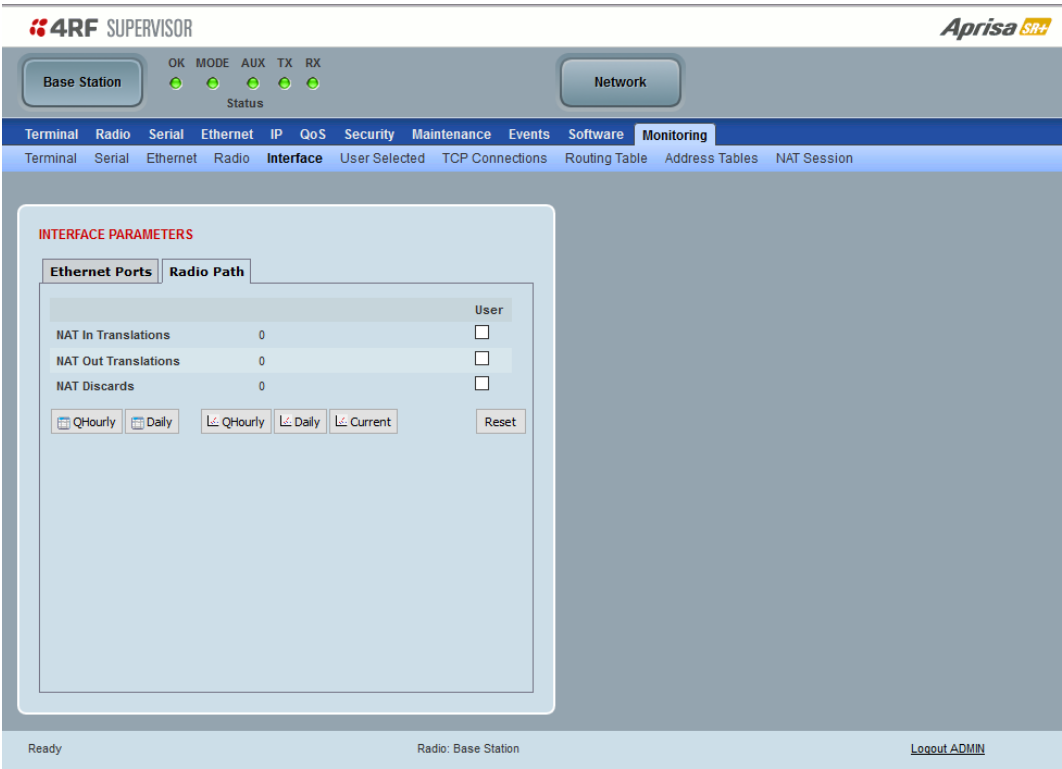


INTERFACE PARAMETERS

Ethernet Ports

Monitored Parameter	Function
NAT In Translations	The number of translated packets received on Ethernet ports
NAT Out Translations	The number of translated packets transmitted on Ethernet ports
NAT Discards	The number of translated packets rejected / discarded on Ethernet ports due to the lack of resource or other reason

Radio Path



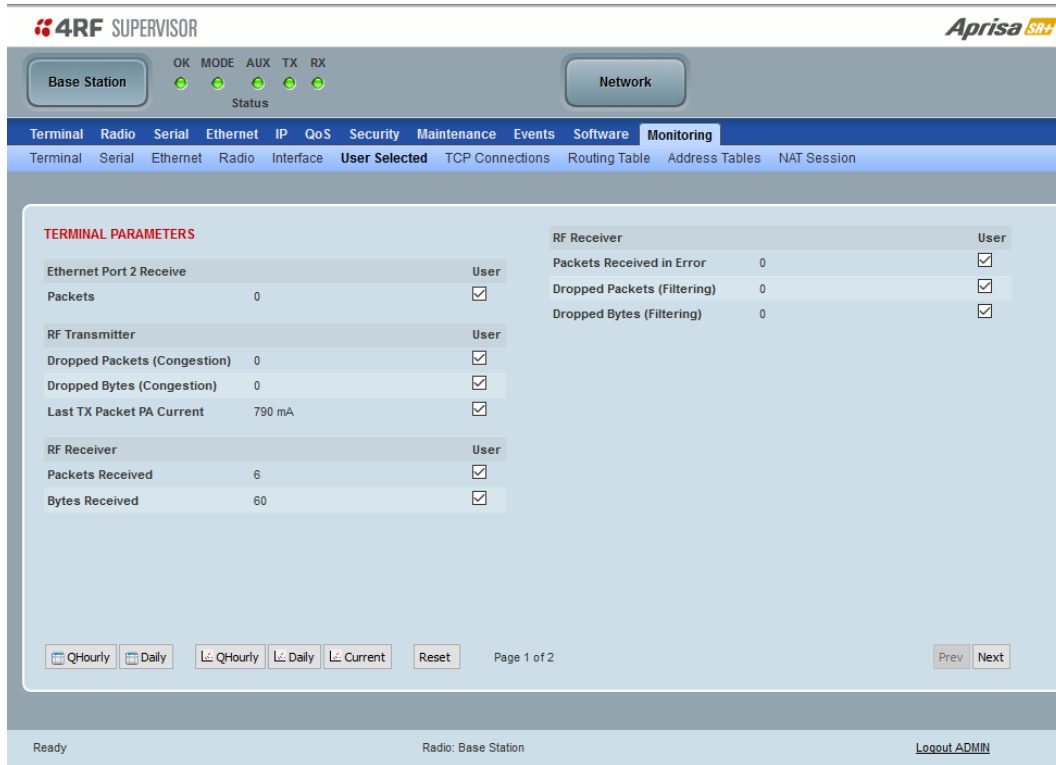
Radio Path

Monitored Parameter	Function
NAT In Translations	The number of translated packets received on the radio interface
NAT Out Translations	The number of translated packets transmitted on the radio interface
NAT Discards	The number of translated packets rejected / discarded on the radio interface due to the lack of resource or other reason

Monitoring > User Selected

This page displays the 'User' parameters setup in all the other Monitoring screens e.g. in the Monitoring > Radio > Transmitter, the User checkbox is ticked for the Dropped Packets (congestion) and Dropped Bytes (congestion).

The results shown are since the page was opened and are updated automatically every 12 seconds.



4RF SUPERVISOR **Aprisa SR+**

Base Station OK MODE AUX TX RX Status **Network**

Terminal Radio Serial Ethernet IP QoS Security Maintenance Events Software Monitoring

Terminal Serial Ethernet Radio Interface User Selected TCP Connections Routing Table Address Tables NAT Session

TERMINAL PARAMETERS

Parameter	Value	User
Ethernet Port 2 Receive		
Packets	0	☒
RF Transmitter		
Dropped Packets (Congestion)	0	☒
Dropped Bytes (Congestion)	0	☒
Last TX Packet PA Current	790 mA	☒
RF Receiver		
Packets Received	6	☒
Bytes Received	60	☒

RF Receiver

Parameter	Value	User
Packets Received in Error	0	☒
Dropped Packets (Filtering)	0	☒
Dropped Bytes (Filtering)	0	☒

QHourly Daily QHourly Daily Current Reset Page 1 of 2 Prev Next

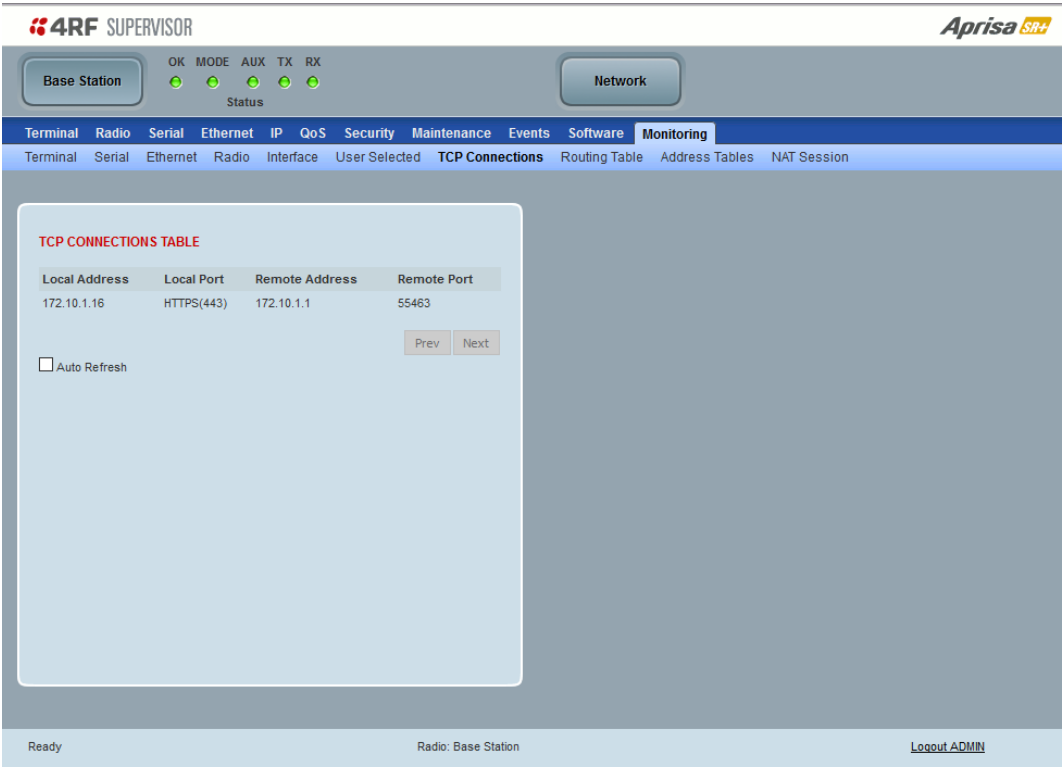
Ready Radio: Base Station [Logout ADMIN](#)

Controls

The Reset button clears the current results.

Monitoring > TCP Connections

This page displays the list of active TCP connections on the radio.



TCP CONNECTIONS TABLE

Result	Function
Local Address	The local radio IP address
Local Port	The local radio TCP port number
Remote Address	The remote host IP address (in most case a host PC connected to radio / network)
Remote Port	The local radio TCP port number (in most case a host PC connected to radio / network)

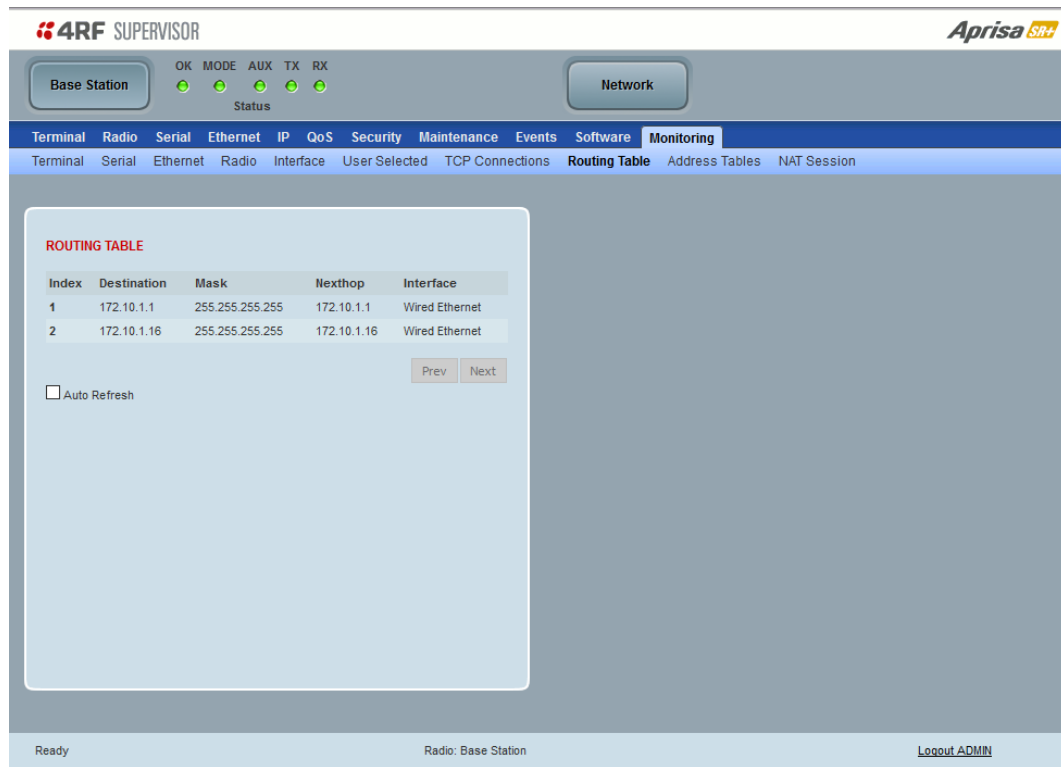
Controls

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

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

Monitoring > Routing Table

This page displays the list of active routes on the radio.



ROUTING TABLE

Result	Function
Index	The routing table index
Destination	The target destination IP address of the route
Mask	The subnet mask of the destination IP address of the route
Next Hop	The next hop IP address on the path to the destination IP address of the route
Interface	The physical interface output on the path to the destination IP address of the route

Controls

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

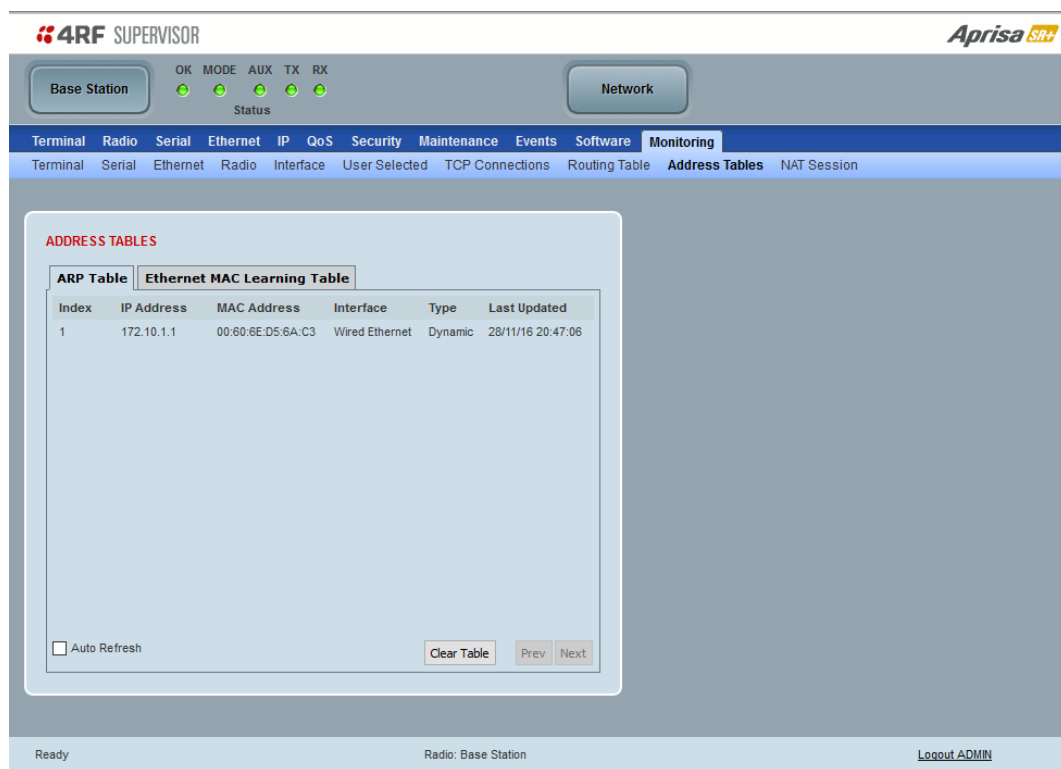
If the Auto Refresh option is ticked, the routing table will refresh every 12 seconds.

Monitoring > Address Tables

ARP Table

This page displays the current Address Resolution Protocols (ARP) on the radio. The radio implemented ARP protocol is used for resolution of network layer addresses into link layer addresses. It is used to map a IPv4 address to an Ethernet MAC address. The ARP table shows the results of the ARP protocol linkage between IPv4 address and Ethernet MAC address of the devices attached to the radio.

In a layer 2 bridge LAN, an upper layer protocol may include the IP address of the destination, but since it is an Ethernet LAN network, it also needs to know the destination MAC address. First, the radio uses a cached ARP table to look up the IPv4 destination address for the matching MAC address records. If the MAC address is found, it sends the IPv4 packet encapsulated in Ethernet frame with the found MAC address. If the ARP cache table did not produce a result for the destination IPv4 address, the radio sends a broadcast ARP message requesting an answer (of MAC address that matches) for IP address. The destination device responds with its MAC address (and IP). The response information is cached in radios' ARP table and the message can now be sent with the appropriate destination MAC address.



ADDRESS TABLES

Title	Function
IP Address	The IPv4 address of a neighboring device in the radio LAN network
MAC Address	The ARP result matching or mapping MAC address from the IPv4 address.
Interface	The Ethernet port interface the ARP results found the matching/mapping
Type	'Dynamic' indicates an ARP result and 'Static' indicates a user static mapping.

Controls

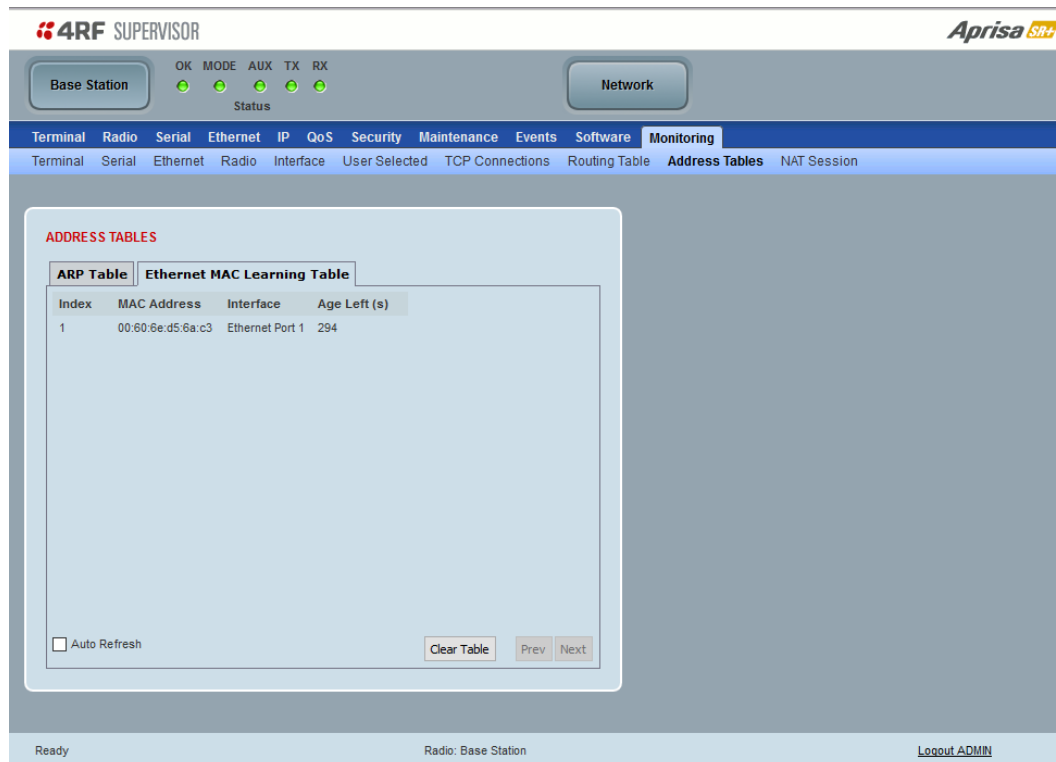
The Next button will display the next page of 8 addresses and the Prev button will display the previous page of 8 addresses.

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

Ethernet MAC Learning Table

This page displays the current Ethernet Media Access Control (MAC) Address table on the radio LAN network. In order for the radio to switch frames between Ethernet LAN ports efficiently, the radio layer 2 bridge maintains a MAC address table. When the radio bridge receives a frame, it associates the MAC address of the sending network device with the LAN port on which it was received.

The bridge dynamically learns and builds the MAC address table by using the MAC source address of the frames received. When the radio bridge receives a frame for a MAC destination address not listed in its address table, it floods the frame to all LAN ports of the same LAN (or in case of VLAN, to the specific VLAN) except the port that received the frame. When the destination bridge device replies, the radio bridge adds its relevant MAC source address and interface port number to the MAC address table. The switch then forwards subsequent frames to a single LAN port without flooding all LAN ports.



ADDRESS TABLES

Title	Function
MAC Address	The learned MAC address of a neighboring bridge device in the LAN network.
Interface	The Ethernet port interface the MAC address has learned
Age left	The aging time of this MAC entry will stay in the table, even if this MAC address is not used. Every time this MAC address is used, the aging time restarts from its maximum. Default is 300 sec.

Controls

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

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



Monitoring > NAT Session

This page displays the number of NAT sessions. The maximum number of sessions is 250.

4RF SUPERVISOR

Base Station 16

OK

MODE

AUX

TX

RX

Status

Network

Terminal

Radio

Serial

Ethernet

IP

QoS

Security

Maintenance

Events

Software

Monitoring

Terminal

Serial

Ethernet

Radio

Interface

User Selected

TCP Connections

Routing Table

Address Tables

NAT Session

NETWORK ADDRESS TRANSLATION SESSIONS

RF Port

Ethernet Ports

Filter Public Source Address

None

Filter Public Destination Address

None

Filter Private Destination Address

None

Filter Public Source Port

.

Filter Public Destination Port

.

Filter Private Destination Port

.

Public Source Address

Public Source Port

Public Destination Address

Public Destination Port

Private Destination Address

Private Destination Port

Protocol

Idle Time (s)

Session Up Time (s)

Inbound Packets

Outbound Packets

There are no session records to display

Page 0 of 0

Previous

Next

☐ Auto Refresh

Busy

Radio: Base Station 16

[Logout ADMIN](#)

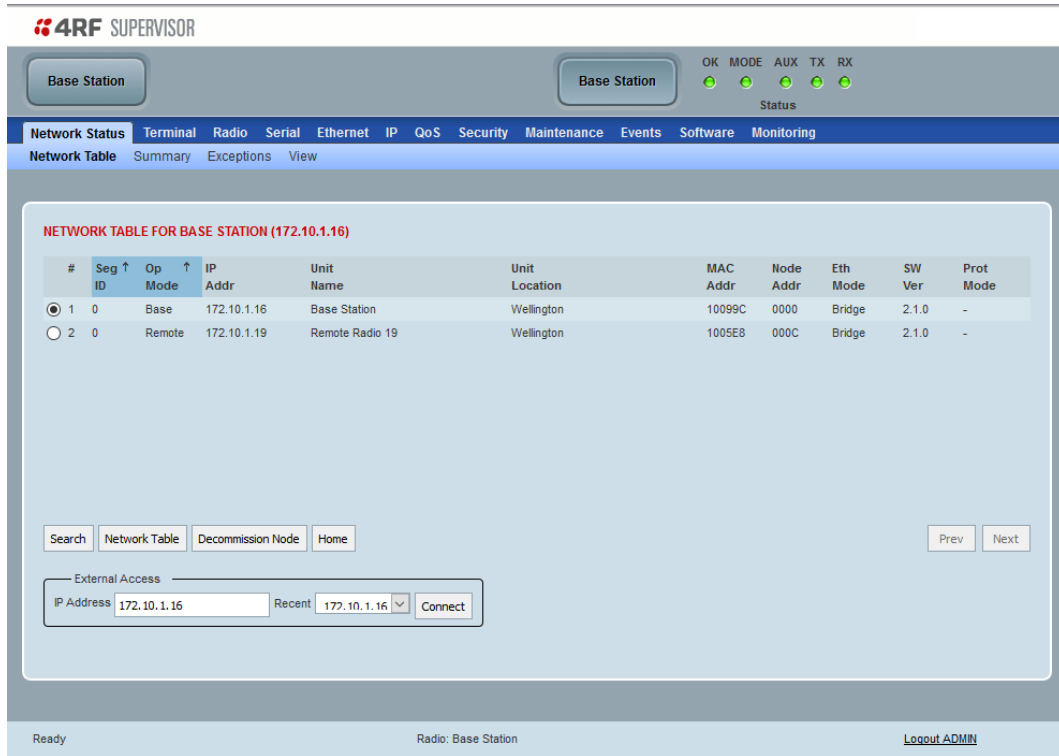
NETWORK ADDRESS TRANSLATION SESSIONS

Title	Function
Idle Time (s)	The total duration where the session has been idle. Traffic on this session will reset the Idle Time to zero.
Session Up Time (s)	The total duration that this session has been shown in the session table.
Inbound Packets	The total number of packets received on the public interface for this session.
Outbound Packets	The total number of packets transmitted from the public interface for this session.

Network Status

Network Status > Network Table

This page displays a list of all the registered nodes in the network.



4RF SUPERVISOR

Base Station Base Station OK MODE AUX TX RX Status

Network Status Terminal Radio Serial Ethernet IP QoS Security Maintenance Events Software Monitoring

Network Table Summary Exceptions View

NETWORK TABLE FOR BASE STATION (172.10.1.16)

#	Seg ID	Op Mode	IP Addr	Unit Name	Unit Location	MAC Addr	Node Addr	Eth Mode	SW Ver	Prot Mode
1	0	Base	172.10.1.16	Base Station	Wellington	10099C	0000	Bridge	2.1.0	-
2	0	Remote	172.10.1.19	Remote Radio 19	Wellington	1005E8	000C	Bridge	2.1.0	-

Search Network Table Decommission Node Home Prev Next

External Access

IP Address 172.10.1.16 Recent 172.10.1.16 Connect

Ready Radio: Base Station Logout ADMIN

NETWORK TABLE

This Network Table is available when you log into any radio with SuperVisor. On the remote radio, this will allow you to connect back to the base station.

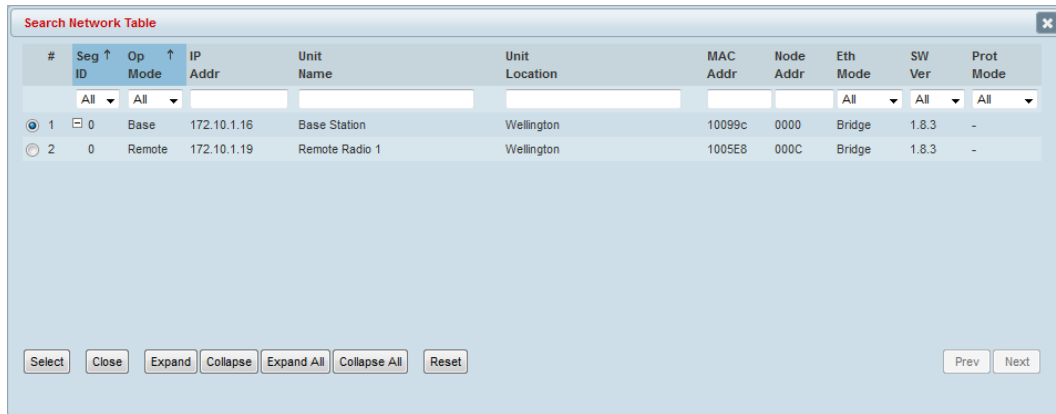
To manage a remote / repeater station with SuperVisor:

Click on the radio button of the required station. The remaining menu items then apply to the selected remote radio.

Controls

Search

The Search button brings up a search form.



#	Seg ID	Op Mode	IP Addr	Unit Name	Unit Location	MAC Addr	Node Addr	Eth Mode	SW Ver	Prot Mode
1	0	Base	172.10.1.16	Base Station	Wellington	10099c	0000	Bridge	1.8.3	-
2	0	Remote	172.10.1.19	Remote Radio 1	Wellington	1005E8	000C	Bridge	1.8.3	-

Filtering

The first row of the table in the pop up window is the search filter.

There are two types of filters:

1. Drop down lists with a finite set of options to select from
2. Text entry where any text can be entered.

When the filters are applied, the rows in the rest of the table are displayed only if they match all the filters.

Example 1 - one filter; select 'remote' in the 'Op Mode' filter with the other drop down list set to 'All' and the text entry filters blank, will show all the remote radios

Example 2 - two filters; type '98' in the MAC Addr filter and select 'Bridge' for the 'Eth Mode' filter.

Grouping

Entries in the network table can be grouped based on the Segment IDs. The user can expand the groups with the  and collapse the groups with the  button to help locate an entry.

Sorting

Clicking on a column header of the table will sort the table by that column.

The Select button closes the popup, updates the selection on the Network Table and saves the search/filter parameters which are reused the next time the search is initiated in the same SuperVisor session.

The Close button closes the Search popup.

The Expand button expands the group of the selected entry and the Expand All button expands all groups.

The Collapse button collapses the group of the selected entry and the Collapse All button collapses all groups.

The Reset button removes all filtering and expands all groups.

Network Table

Refreshes the Network table from the currently selected IP address.

Decommission Node

The selected node is removed from service.

External Access

Sets the IP address of an extended network radio for SuperVisor management.

Recent

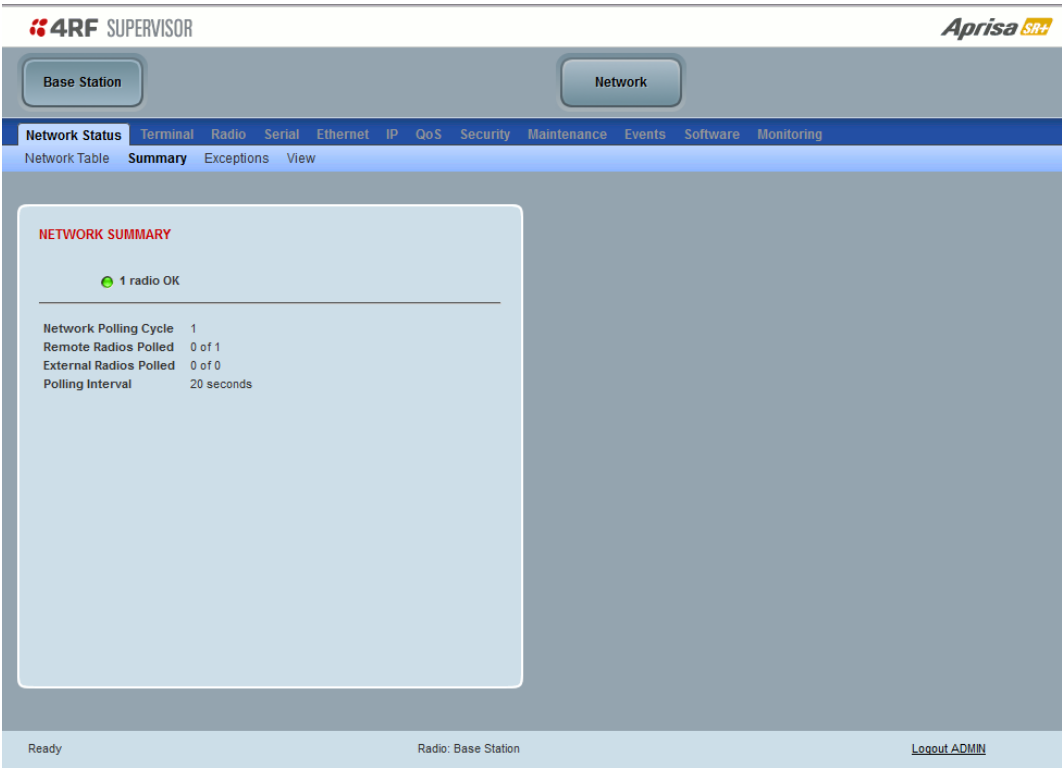
The Recent dropdown list shows the IP addresses that have been managed recently with the extended network radio.

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 radios for the base station. When open, it provides a continuous monitor of the network.

Depending on the poll period set (20 seconds minimum) and the number of remotes in the network, it will take at least three poll cycles to indicate a failure in the network. Initial results may indicate ‘All ok’ until at least three poll cycles completed. This could take ‘Number Of Remotes’ * ‘Poll Period’ * 3 seconds to complete.



NETWORK SUMMARY

A network poll will start when any of the Network Status pages are opened (Summary, Exceptions or View). The network poll will only continue to poll the remote radios 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 radios are operating correctly.

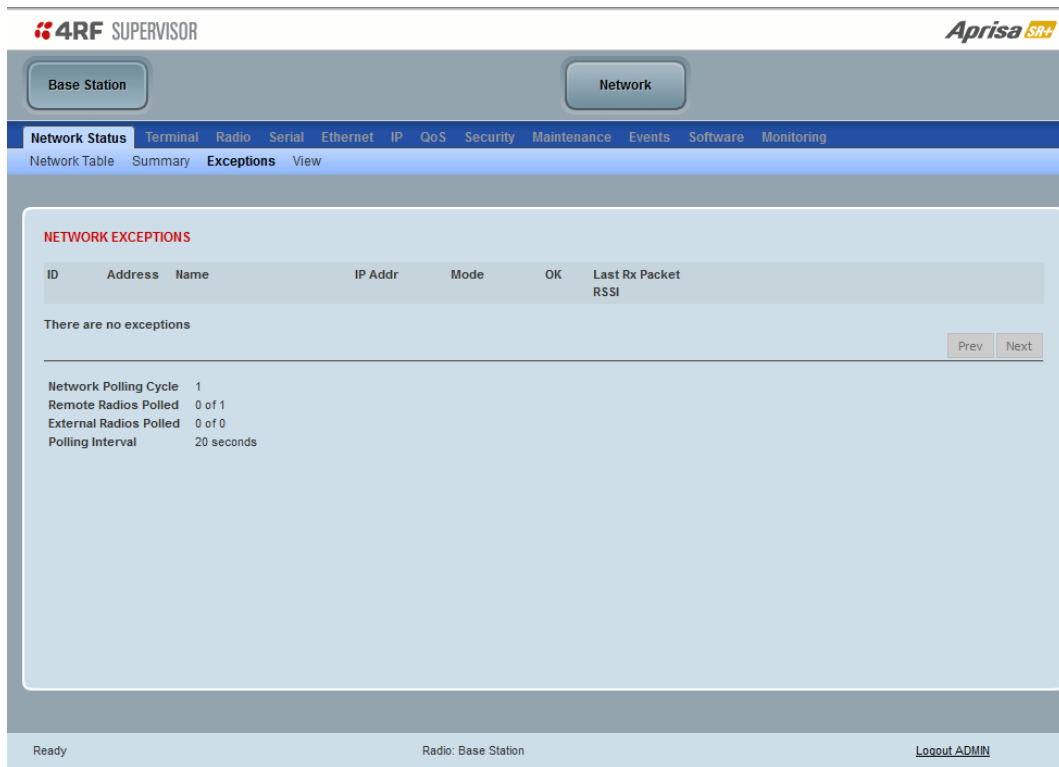
Network Summary Example:

Result	Function
Network Polling Cycle	The number of poll cycles since first opening a Network Status > Summary, Exceptions or View page.
Remote Radios Polled	This shows the number of remote radios polled for the current polling cycle out of the number of remote radios registered with the base station.
External Radios Polled	This shows the number of extended network radios polled for the current polling cycle out of the total extended network radios.
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 261.

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 radios 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.
Remote Radios Polled	This shows the number of remote radios polled for the current polling cycle out of the number of remote radios registered with the base station.
External Radios Polled	This shows the number of extended network radios polled for the current polling cycle out of the total extended network radios.
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 261.

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 shown 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

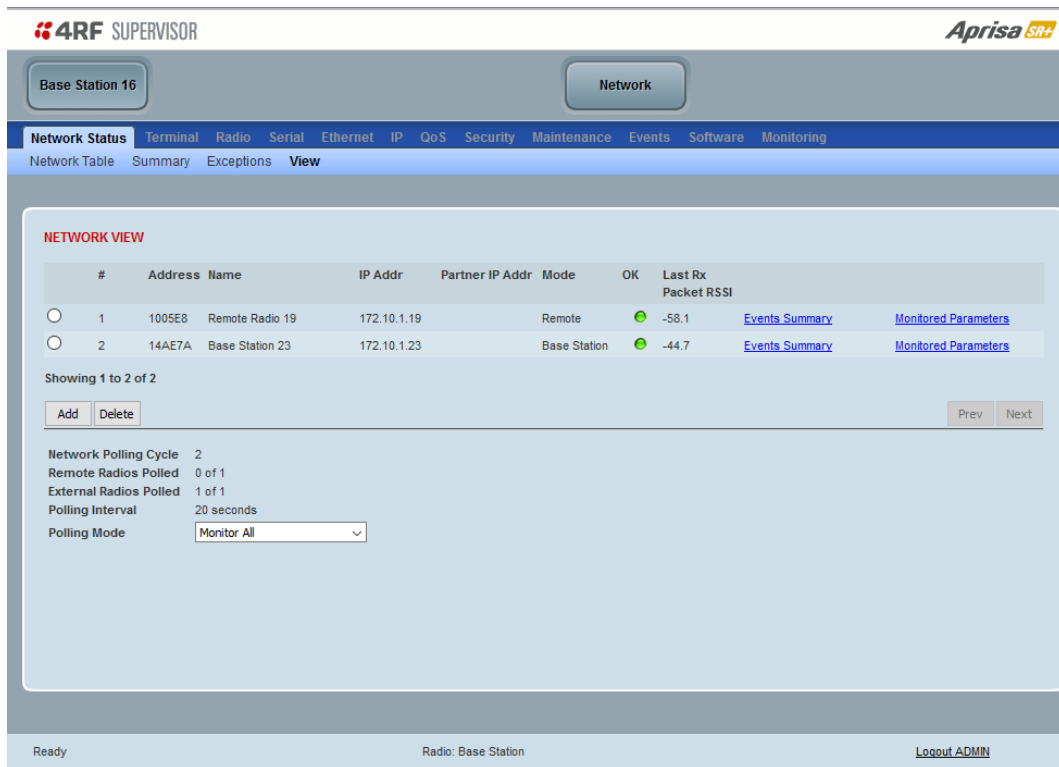
Clicking on View Events navigates to the Events page (see 'Events' on page 278) for the specific remote radio where the radio events will be displayed.

View Parameters

Clicking on View Parameters navigates to the Monitoring page (see 'Monitoring' on page 310) 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.



4RF SUPERVISOR **Aprisa SR+**

Base Station 16 Network

Network Status | Terminal | Radio | Serial | Ethernet | IP | QoS | Security | Maintenance | Events | Software | Monitoring

Network Table | Summary | Exceptions | **View**

NETWORK VIEW

#	Address	Name	IP Addr	Partner IP Addr	Mode	OK	Last Rx Packet RSSI	
☐ 1	1005E8	Remote Radio 19	172.10.1.19		Remote	●	-58.1	Events Summary Monitored Parameters
☐ 2	14AE7A	Base Station 23	172.10.1.23		Base Station	●	-44.7	Events Summary Monitored Parameters

Showing 1 to 2 of 2

Network Polling Cycle: 2
 Remote Radios Polled: 0 of 1
 External Radios Polled: 1 of 1
 Polling Interval: 20 seconds
 Polling Mode: Monitor All

Ready Radio: Base Station [Logout ADMIN](#)

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 radios 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.
Remote Radios Polled	This shows the number of remote radios polled for the current polling cycle out of the number of remote radios registered with the base station.
External Radios Polled	This shows the number of extended network radios polled for the current polling cycle out of the total extended network radios.
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 261. 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.

Events Summary

Clicking on Events Summary navigates to the Events page (see 'Events > Alarm Summary' on page 278) for the specific remote radio where the radio events will be displayed.

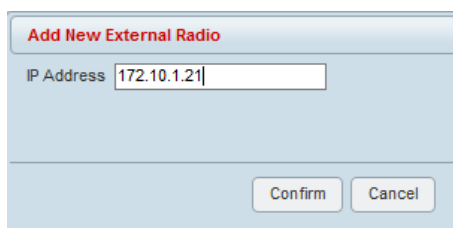
Monitored Parameters

Clicking on Monitored Parameters navigates to the Monitoring page (see 'Monitoring' on page 310) for the specific remote radio where the radio parameters will be displayed.

Controls

Add

The Add button adds a radio to the extended network radio list.

A light blue dialog box titled "Add New External Radio" in red text. It contains a label "IP Address" followed by a text input field containing "172.10.1.21". At the bottom right, there are two buttons: "Confirm" and "Cancel".

An error message will warn the user if the IP address entered is not a radio in the external network.

A maximum of 480 external radios can be added to the monitoring list but only the first 24 radios will be saved. If the user adds external radios beyond the first 24, an additional informational message will be displayed in the pop up box to inform the user that these entries will not be saved and will be lost when logging out of SuperVisor.

Delete

Deletes the selected radio from the extended network radio list.

Protected Station

The majority of SuperVisor screens are the same for the standard radio and the protected station. The following screens are specific to the protected station.

Logging into a Protected Station

When SuperVisor detects a protected station, it operates in Single Session Management operation mode.

When in Single Session Management mode, SuperVisor will automatically detect the two individual Aprisa SR+ radios configured to pair together for protection and manage the two units in a single browser session. To the user, it will appear as managing a single unit, but SuperVisor will interact with the two individual units at a lower level.

The user can login with the IP address of either the Primary or Secondary radio to manage the protected station (don't use the PVIP address as it is not a management IP address). SuperVisor will present all information appropriately where 'Common Parameters' will be presented to the user as a single parameter e.g. TX and RX Frequencies and 'Unit Specific Parameters' will be presented to the user as Primary or Secondary parameters e.g. Events and Alarms.

When saving data, SuperVisor will also validate and ensure that the correct settings are written to both units. The SuperVisor Single Session Management ensures that both units of the protected station are always configured correctly to complement each other as protected partners.

The user can still login with two different sessions to the active and standby radios. If the user opens two session management, one session logged into the active radio and a second session logged into the standby radio, the Multiple Management Sessions pop-up message will show the user names and IP addresses of the active and standby radio.

Parameter Errors

On protected station screens, parameter values displayed in red indicate discrepancies in common parameter values between the primary and secondary radios (see 'Protected Station: Terminal > Summary' on page 343 for an example of the red display). The value displayed is from the 'addressed radio'.

These value discrepancies can occur if the two protected station radios have been separately configured. The discrepancies can be corrected by re-entering the values in one of the radios. The value will be copied to the partner radio.

Terminal

Protected Station: Terminal > Summary

TERMINAL SUMMARY

This page displays the current settings for the Terminal parameters.

PROTECTION INFORMATION

Protection Type

This parameter shows the type of protection:

Option	Function
Serial Data Driven Switching	Provides radio and RS-232 serial port user interface protection for Aprisa SR+ radios.
Monitored Hot Standby (Protected Station)	The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio. The standby radio is monitored to ensure its correct operation should a switch-over be required. See 'Monitored Alarms' on page 412 for the list of monitored alarms.
Redundant (Protected Station)	The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio

Active Unit

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

Switch Count

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

Primary Address

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

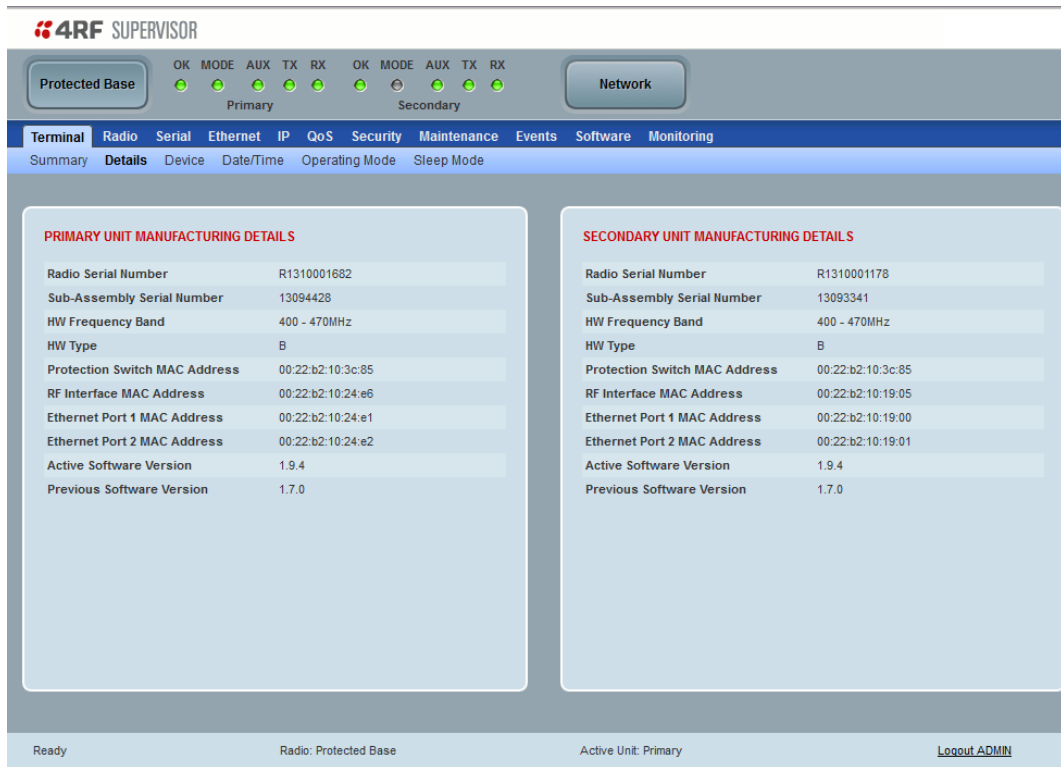
Secondary Address

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

OPERATING SUMMARY

See 'Terminal > Summary' on page 103 for parameter details.

Protected Station: Terminal > Details



4RF SUPERVISOR

Protected Base OK MODE AUX TX RX OK MODE AUX TX RX Network

Primary Secondary

Terminal Radio Serial Ethernet IP QoS Security Maintenance Events Software Monitoring

Summary **Details** Device Date/Time Operating Mode Sleep Mode

PRIMARY UNIT MANUFACTURING DETAILS

Radio Serial Number	R1310001682
Sub-Assembly Serial Number	13094428
HW Frequency Band	400 - 470MHz
HW Type	B
Protection Switch MAC Address	00:22:b2:10:3c:85
RF Interface MAC Address	00:22:b2:10:24:e6
Ethernet Port 1 MAC Address	00:22:b2:10:24:e1
Ethernet Port 2 MAC Address	00:22:b2:10:24:e2
Active Software Version	1.9.4
Previous Software Version	1.7.0

SECONDARY UNIT MANUFACTURING DETAILS

Radio Serial Number	R1310001178
Sub-Assembly Serial Number	13093341
HW Frequency Band	400 - 470MHz
HW Type	B
Protection Switch MAC Address	00:22:b2:10:3c:85
RF Interface MAC Address	00:22:b2:10:19:05
Ethernet Port 1 MAC Address	00:22:b2:10:19:00
Ethernet Port 2 MAC Address	00:22:b2:10:19:01
Active Software Version	1.9.4
Previous Software Version	1.7.0

Ready Radio: Protected Base Active Unit: Primary [Logout ADMIN](#)

PRIMARY UNIT / SECONDARY UNIT MANUFACTURING DETAILS

See 'Terminal > Details' on page 106 for parameter settings.

Terminal > Date / Time

Protected Base

OK

MODE

AUX

TX

RX

OK

MODE

AUX

TX

RX

PrimarySecondary

Network

Terminal

Radio

Serial

Ethernet

IP

QoS

Security

Maintenance

Events

Software

Monitoring

Summary

Details

Device

Date/Time

Operating Mode

Sleep Mode

TERMINAL DATE AND TIME

Time Set Method

Manual

Time Zone Offset

No Offset

Date and Time

06/05/2015, 02:02

Auto Synchronization Period (s)

0

Time Server 1 Address

0.0.0.0

Time Server 2 Address

0.0.0.0

Synchronization Status

Disabled

Save

Cancel

Synchronize Now

Ready

Radio: Protected Base

Active Unit: Primary

[Logout ADMIN](#)

TERMINAL DATE AND TIME

See ‘Terminal > Date / Time’ on page 113 for details.

Terminal > Device

Protected Base

OK

MODE

AUX

TX

RX

OK

MODE

AUX

TX

RX

Primary

Secondary

Network

Terminal

Radio

Serial

Ethernet

IP

QoS

Security

Maintenance

Events

Software

Monitoring

Summary

Details

Device

Date/Time

Operating Mode

Sleep Mode

TERMINAL DETAILS

Terminal Name

Protected Base

Location

Wellington

Contact Name

Contact

Contact Details

Support

GPS Coordinates

+50.23200, -90.65400

GPS Status

Manually Updated On 06/05/2015, 01:09:27

REGION SETTINGS

Time Format

☐ 12 Hour (AM/PM)
 ☒ 24 Hour

Date Format

☐ MM/DD/YYYY
 ☒ DD/MM/YYYY

Measurement System

☐ US
 ☒ Metric

Save

Cancel

Update GPS

RF NETWORK SETTINGS

Network ID (FAN)

CAFE

Base Station ID

2

Network Radius

1

Network Repeaters Proximity

No Repeater

Repeater Network Segment ID

0

Inband Management

☒

Inband Management Timeout (s)

10

GENERAL SETTINGS

ARP Table Maximum Age (s)

14400

Save

Cancel

Ready

Radio: Protected Base

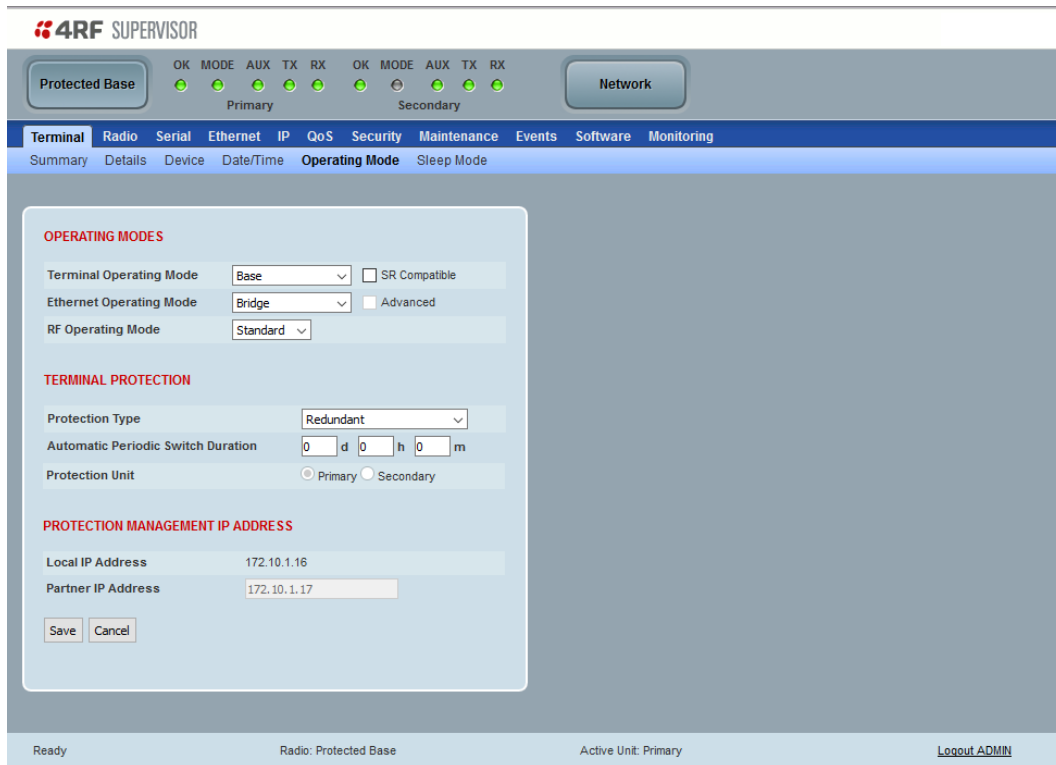
Active Unit: Primary

[Logout ADMIN](#)

TERMINAL DETAILS

See 'Terminal > Device' on page 108 for details.

Protected Station: Terminal > Operating Mode



OPERATING MODES

Terminal Operating Mode

The Terminal Operating Mode defines the radio mode of operation. The default setting is Remote.

Option	Function
Base	The Base operating mode manages all traffic activity between itself, repeaters, and remotes. It is the center-point of network where in most cases will be connected to a SCADA master.
Base Repeater	The Base Repeater operating mode has the same function as the base (and repeater station) but used when peer to peer connections between remotes is required via the base station.
Base MMS	The Base MMS operating mode has the same function as the base operating mode but used with a Migration Station (see Aprisa SR+ MMS User Manual).
Repeater	The Repeater operating mode forwards packets coming from base station and other repeaters e.g. in daisy chain LBS mode and /or remote radios.
Repeater MMS	The Repeater MMS operating mode has the same function as the repeater operating mode but used with a Migration Station (see Aprisa SR+ MMS User Manual).
Remote	The Remote operating mode in most cases is used as the end-point of the SCADA network connected to an RTU or PLC device for SCADA network control and monitoring.
Point To Point	The Point To Point operating mode configures a full duplex radio for Point-to-point (PTP) operation. Changing from PMP or PTP or vice versa requires the radio to be 'restored to factory default settings' which will clear <u>all</u> previous radio setup and configuration. See 'Point-To-Point' section on page 405.

SR Compatible

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

When the ‘SR Compatible’ option is activated on a Aprisa SR+ base station, the base station can operate with a mixture of SR+ and SRx remote radios.

In a mixed network when a Aprisa SR+ base station is working with SR+ and SRx remotes, the SR+ remote is not set to ‘SR Compatible’ mode to allow the remote SR+ work in the highest performance modulation. The SR+ base must be set to ‘SR Compatible’ mode to allow operation with SRx remotes, but it will not restrict the SR+ base to Tx packet at modulations higher than QPSK when the destination is a SR+ remote radio. Thus, the SR+ base station modulation can be set to a modulation higher than QPSK.

Ethernet Operating Mode

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

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

Advanced

Enabled for Gateway Router and Router modes only. The default setting is unticked.

To enable Advanced routing, select the operating mode; Router or Gateway Router and tick the Advanced checkbox.

Advanced Gateway Router mode (AGRM) or Advanced Router mode (ARM) act like a true router between the Ethernet ports and RF interface port where the next hop is one of these ports. This means that the RF interface is a public interface exposed to the user with IP and MAC address like the Ethernet interface.

In AGRM mode, all Ethernet interfaces have the same IP address and subnet.

In ARM mode, each Ethernet interface has a different IP address and subnet.

See ‘Advanced Gateway Router Mode (AGRM) and Advanced Router Mode (ARM)’ on page 41 for a detailed explanation of advanced router modes.

Note: The Network Address Translation feature works only in Advanced Router or Advanced Gateway Router operating mode (see ‘IP > NAT’ on page 193).

TERMINAL PROTECTION

Protection Type

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

Option	Function
None	The SR+ radio is a stand-alone radio (not part of an Aprisa SR+ Protected Station).
Redundant (Protected Station)	The SR+ radio is part of an Aprisa SR+ Protected Station. The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio
Monitored Hot Standby (Protected Station)	Set to make this SR+ radio part of an Aprisa SR+ Protected Station. The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio. The standby radio is monitored to ensure its correct operation should a switch-over be required. See 'Monitored Alarms' on page 412 for the list of monitored alarms.
Serial Data Driven Switching	The SR+ radio is part of an Aprisa SR+ Data Driven Protected Station. Provides radio and RS-232 serial port user interface protection for Aprisa SR+ radios.

Automatic Periodic Switch Duration

The Automatic Periodic Switch Duration sets the time interval for automatic switch-over from the active radio to the standby radio.

This feature will automatically switchover from the active radio to the standby radio if there are no alarms preventing the switchover to the standby radio. It can be used to provide confidence that the standby radio is still operational, maybe after many days of standby operation.

The maximum number of days that can be set is 49 days.

The default setting is 0 which disables the automatic switch-over feature.

PROTECTION MANAGEMENT IP ADDRESS

Primary Address

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

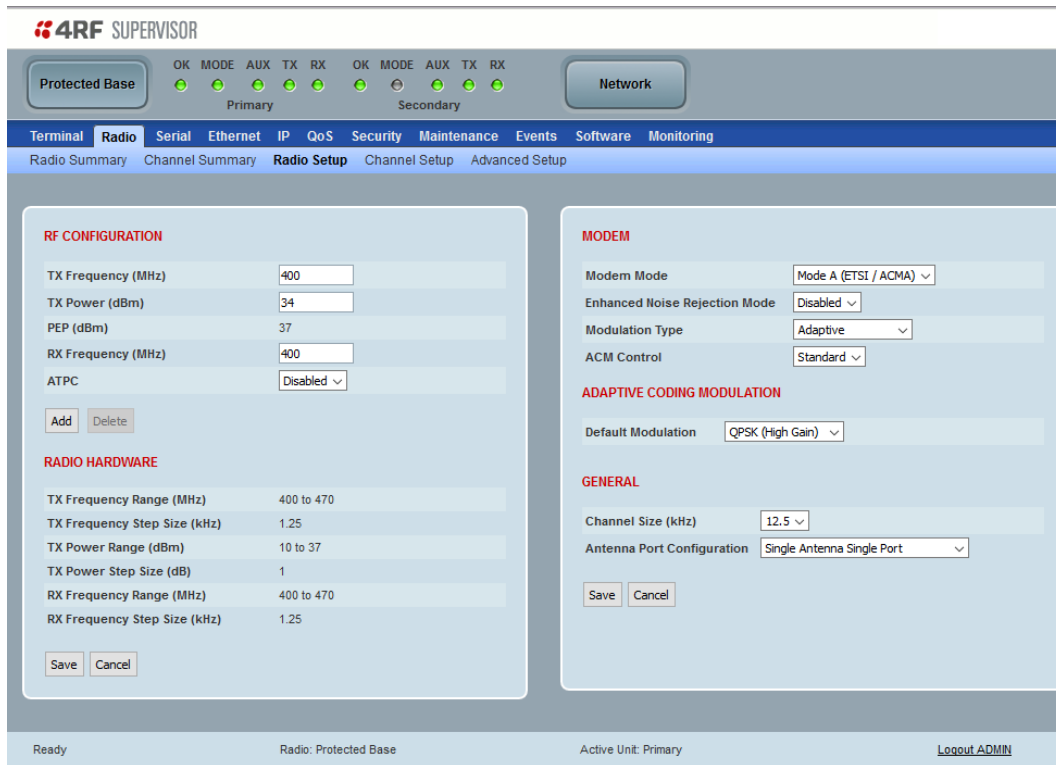
Secondary Address

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

Radio

Protected Station: Radio > Radio Setup

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



4RF SUPERVISOR

Protected Base OK MODE AUX TX RX OK MODE AUX TX RX
Primary Secondary

Network

Terminal Radio Serial Ethernet IP QoS Security Maintenance Events Software Monitoring

Radio Summary Channel Summary **Radio Setup** Channel Setup Advanced Setup

RF CONFIGURATION

TX Frequency (MHz) 400

TX Power (dBm) 34

PEP (dBm) 37

RX Frequency (MHz) 400

ATPC Disabled

Add Delete

RADIO HARDWARE

TX Frequency Range (MHz) 400 to 470

TX Frequency Step Size (kHz) 1.25

TX Power Range (dBm) 10 to 37

TX Power Step Size (dB) 1

RX Frequency Range (MHz) 400 to 470

RX Frequency Step Size (kHz) 1.25

Save Cancel

MODEM

Modem Mode Mode A (ETSI / ACMA)

Enhanced Noise Rejection Mode Disabled

Modulation Type Adaptive

ACM Control Standard

ADAPTIVE CODING MODULATION

Default Modulation QPSK (High Gain)

GENERAL

Channel Size (kHz) 12.5

Antenna Port Configuration Single Antenna Single Port

Save Cancel

Ready Radio: Protected Base Active Unit: Primary Logout ADMIN

Antenna Port Configuration

This parameter sets the Antenna Port Configuration for the radio. For more information on single and dual antenna port part numbers and cabling options, see ‘Cabling’ on page 419.

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

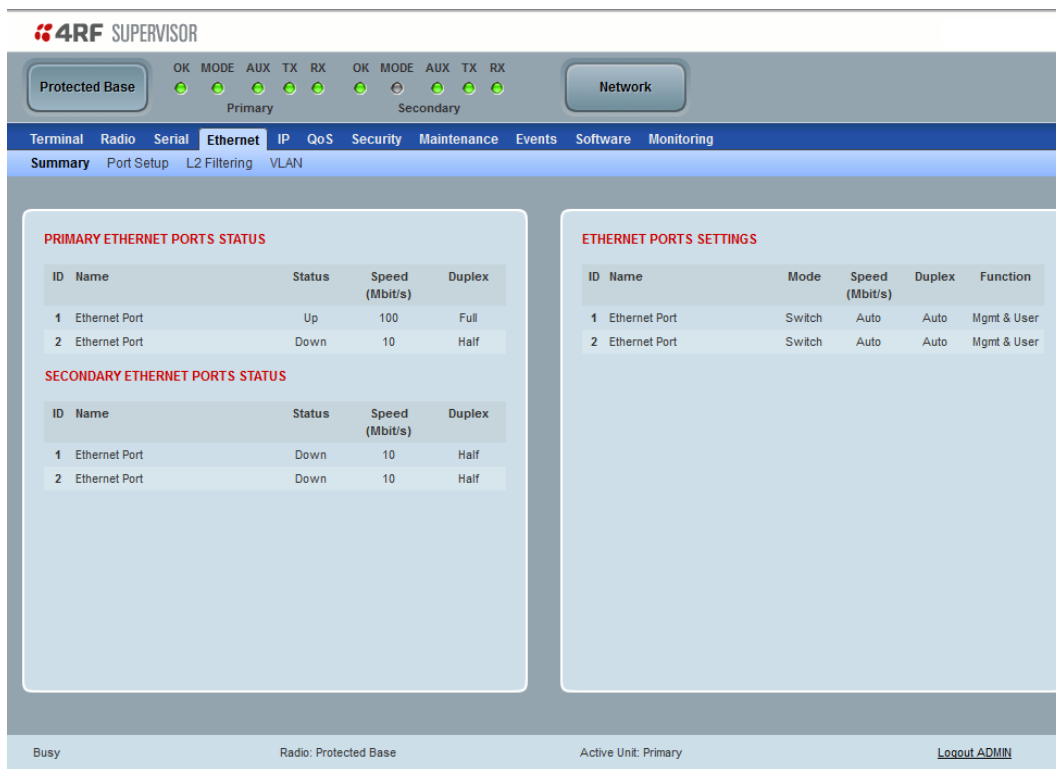
Dual Antenna Dual Port (duplexer)	Select Dual Antenna Dual Port for a dual antenna protected station using: (1) One or two frequency in half duplex transmission with two external duplexer (for filtering) connected to the A and B ANT/TX and RX antenna ports and single antenna connected to the duplexer. (2) Two frequency in full duplex transmission with an external duplexer (for full duplex operation) connected to the A and B ANT/TX and RX antenna ports and single antenna connected to the duplexer. (3) Single frequency in half duplex transmission with an external dual antennas, connected to the A and B ANT/TX and RX antenna ports. (4) Two frequency in half or full duplex transmission with external dual antennas, connected to the A and B ANT/TX and RX antenna ports.

The default setting is Single Antenna Single Port.

Ethernet

Protected Station: Ethernet > Summary

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



4RF SUPERVISOR

Protected Base Network

Terminal Radio Serial **Ethernet** IP QoS Security Maintenance Events Software Monitoring

Summary Port Setup L2 Filtering VLAN

PRIMARY ETHERNET PORTS STATUS

ID	Name	Status	Speed (Mbit/s)	Duplex
1	Ethernet Port	Up	100	Full
2	Ethernet Port	Down	10	Half

SECONDARY ETHERNET PORTS STATUS

ID	Name	Status	Speed (Mbit/s)	Duplex
1	Ethernet Port	Down	10	Half
2	Ethernet Port	Down	10	Half

ETHERNET PORTS SETTINGS

ID	Name	Mode	Speed (Mbit/s)	Duplex	Function
1	Ethernet Port	Switch	Auto	Auto	Mgmt & User
2	Ethernet Port	Switch	Auto	Auto	Mgmt & User

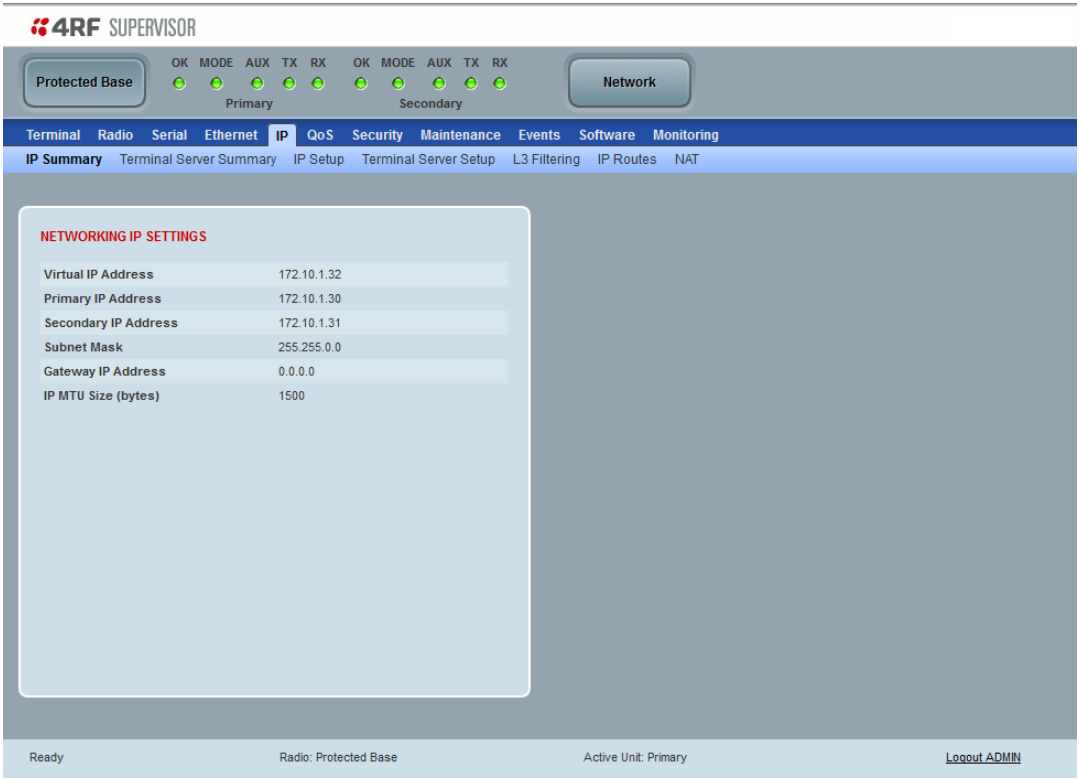
Busy Radio: Protected Base Active Unit: Primary Logout ADMIN

See 'Ethernet > Port Setup' for configuration options.

IP

Protected Station: IP > IP Summary

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



See 'IP > IP Summary > Bridge / Gateway Router Modes' on page 177 for configuration options.

Protected Station: IP > IP Setup

This page provides the setup for the Protected Station Networking IP setup.

NETWORKING IP SETTINGS

Changes in these parameters are automatically changed in the partner radio.

Virtual IP Address (PVIP)

The Protected Station Virtual IP Address (PVIP) is the IP Address of the active radio whether it is the primary radio or the secondary radio.

The PVIP is available in both bridge and router modes.

In router mode, the PVIP can be used as 'next hop' IP address by external routers to reach the protected station so the protection station switch will always be transparent to the external devices and routers.

In both bridge and router modes, the PVIP is used in terminal server mode in remote protected stations. The PVIP is used to reach the protected remote radio from the SCADA master connected to base station in terminal server mode.

Note: The radio IP address should be used for SNMP management as using the PVIP for SNMP management will result in undefined behaviour if a switch-over occurs during an SNMP transaction. Thus, using PVIP for SNMP network management is not recommended.

After a switch-over, new active radio owns the PVIP and will send out a gratuitous ARP to clear the MAC learning tables of upstream switches/routers.

Set the static IP Address of the PVIP using the standard format xxx.xxx.xxx.xxx. The default IP address is 0.0.0.0.

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 169.254.50.20.

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.xxx. The default Gateway is 0.0.0.0.

RADIO INTERFACE IP SETTINGS

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

Radio Interface IP Address

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

Radio Interface Subnet Mask

Set the Subnet Mask of the RF interface using the standard format xxx.xxx.xxx.xxx. The default subnet mask is 255.255.254.0 (/23) (see Note 2 below).

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

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

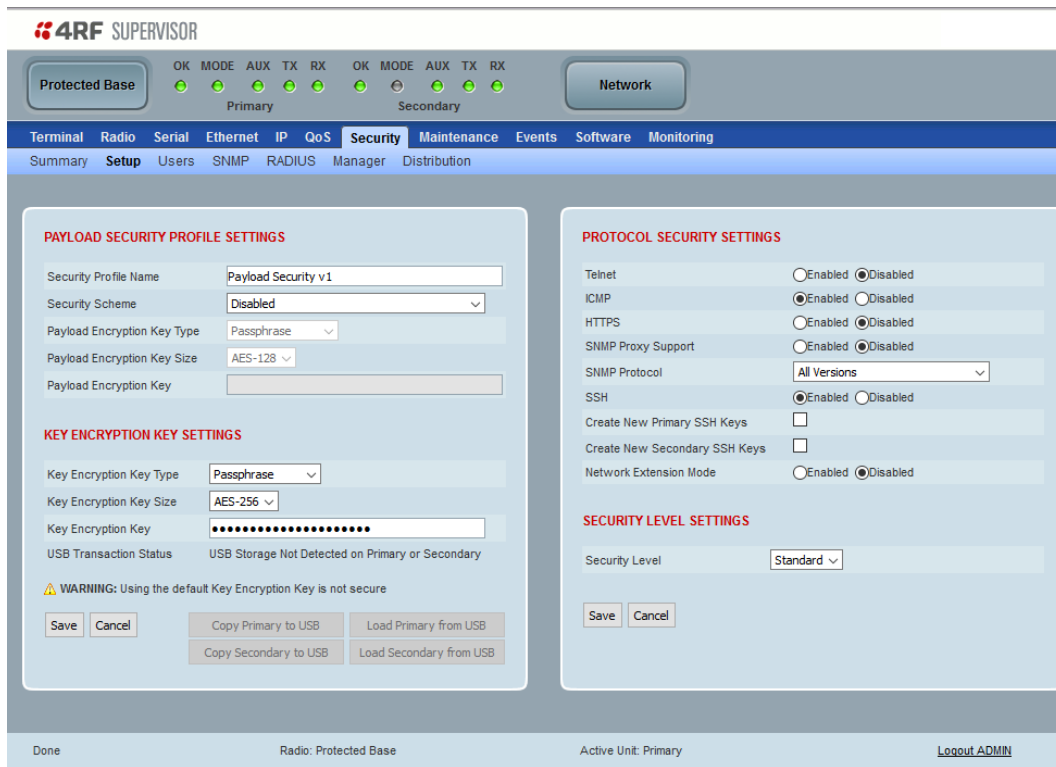
Note 2: If the user sets the RF interface IP address to a network IP address for Auto IP assignment, then the radio will ignore the Radio Interface Subnet Mask setting and use a /23 network subnet ignoring the last two octets.

Note 3: When a remote radio is configured for Router Mode and the base radio is changed from Bridge Mode to Router Mode and the RF interface IP address is set to AUTO IP configuration (at least the last octet of the RF interface IP address is zero), it is mandatory to configure the network topology by using the 'Decommission Node' and 'Discover Nodes' (see 'Maintenance > Advanced' on page 276).

Security

Protected Station: Security > Setup

This page displays the current settings for the Security parameters.



KEY ENCRYPTION KEY SETTINGS

USB Transaction Status

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

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

Controls

These buttons are grayed out if a USB flash drive is not plugged into the radio host port.

The 'Load Primary From USB' button loads the Key Encryption Key settings from the primary radio USB flash drive into the primary radio.

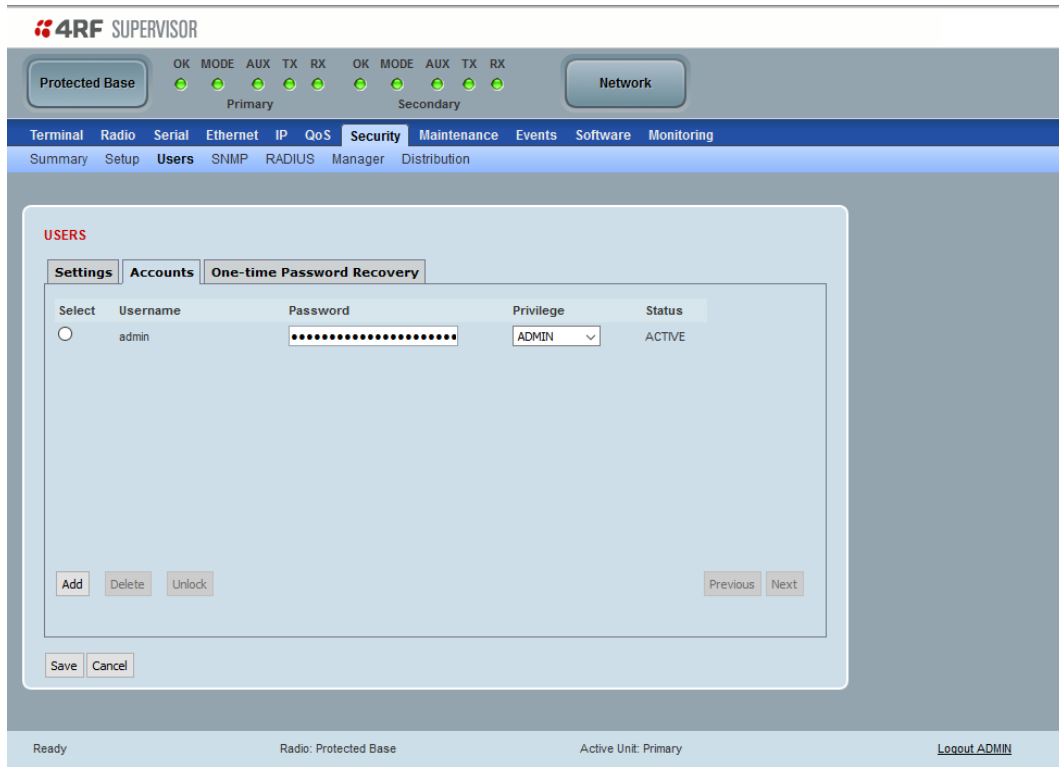
The 'Copy To Primary USB' button copies the Key Encryption Key settings from the primary radio to the primary radio USB flash drive.

The 'Load Secondary From USB' button loads the Key Encryption Key settings from the secondary radio USB flash drive into the secondary radio.

The 'Copy To Secondary USB' button copies the Key Encryption Key settings from the secondary radio to the secondary radio USB flash drive.

Protected Station: Security > Users

This page provides the management and control of the Protected Station Security Users accounts.



In a protected station, the 'Accounts' tab will indicate any differences between the user account configuration of the primary radio and the secondary radio.

- If the user account is only configured for one of the radios, the user name will appear in red text, the password field of that account will be displayed blank.
- If the user account is configured on both radios, but the privilege settings are different, then the privilege configuration dropdown list will be surrounded by two red borders.
- If the user account is configured on both radios, but the current status of user account is different, then the status field will be displayed in red text.

When there are empty password fields on the page, the user will be required to enter a new password for each of the empty fields before saving the user configuration. Validation on this is performed and a pop up will be displayed if a password has not been entered.

Protected Station: Security > Manager

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

4RF SUPERVISOR

Protected Base

OK MODE AUX TX RX OK MODE AUX TX RX

Primary Secondary

Network

Terminal Radio Serial Ethernet IP QoS Security Maintenance Events Software Monitoring

Summary Setup Users SNMP RADIUS Manager Distribution

PRIMARY CURRENT PAYLOAD SECURITY PROFILE

Profile NameMigrated Key

PRIMARY PREVIOUS PAYLOAD SECURITY PROFILE

Profile NameUnknown

StatusInactive

Activate☐

ApplyCancel

PRIMARY PREDEFINED PAYLOAD SECURITY PROFILE

Profile NameUnknown

StatusAvailable

Activate☐

ApplyCancel

SECONDARY CURRENT PAYLOAD SECURITY PROFILE

Profile NameMigrated Key

SECONDARY PREVIOUS PAYLOAD SECURITY PROFILE

Profile NameUnknown

StatusInactive

Activate☐

ApplyCancel

SECONDARY PREDEFINED PAYLOAD SECURITY PROFILE

Profile NameUnknown

StatusAvailable

Activate☐

ApplyCancel

Done

Radio: Protected Base

Active Unit: Primary

Logout ADMIN

PRIMARY / SECONDARY SECURITY PROFILE

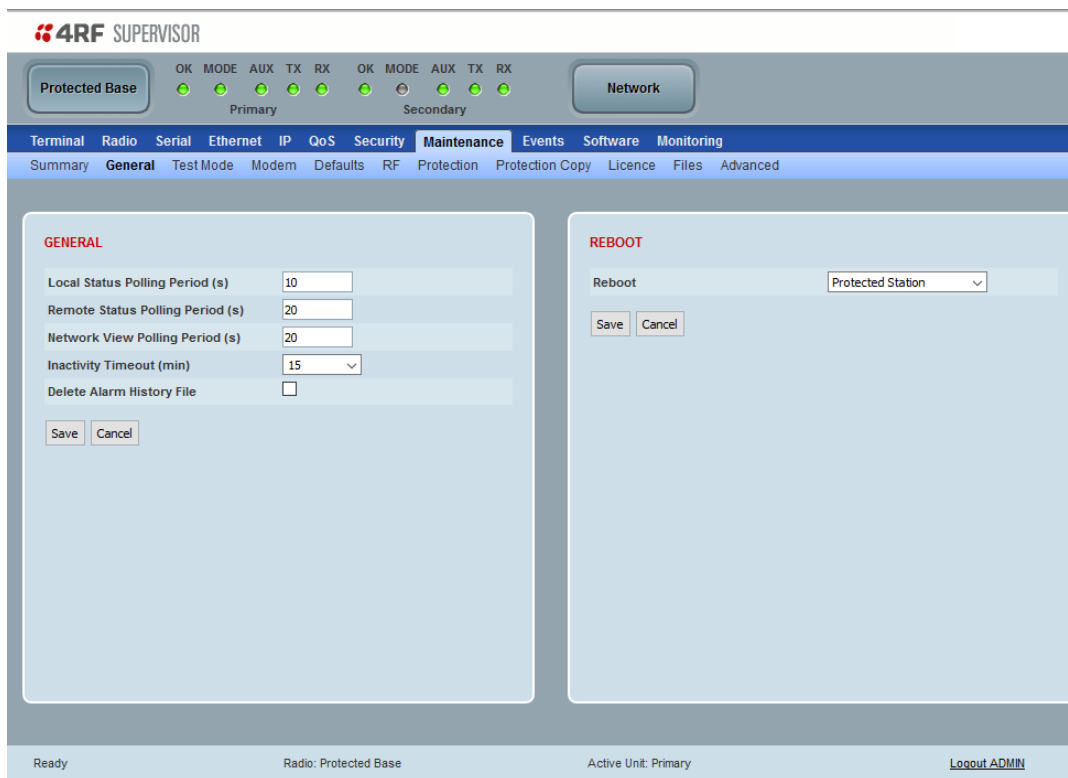
See ‘Security > Manager’ on page 253 for parameter details.

Aprisa SR+ User Manual 2.1.5

Maintenance

Protected Station: Maintenance > General

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



The screenshot displays the 4RF SUPERVISOR web interface. At the top, there's a status bar with 'Protected Base' and 'Network' buttons, and a row of indicator lights for Primary and Secondary units. Below this is a navigation menu with tabs: Terminal, Radio, Serial, Ethernet, IP, QoS, Security, Maintenance (selected), Events, Software, and Monitoring. Under the Maintenance tab, there are sub-tabs: Summary, General (selected), Test Mode, Modem, Defaults, RF, Protection, Protection Copy, Licence, Files, and Advanced.

The main content area is divided into two panels. The left panel, titled 'GENERAL', contains the following settings:

- Local Status Polling Period (s): 10
- Remote Status Polling Period (s): 20
- Network View Polling Period (s): 20
- Inactivity Timeout (min): 15 (dropdown menu)
- Delete Alarm History File: ☐

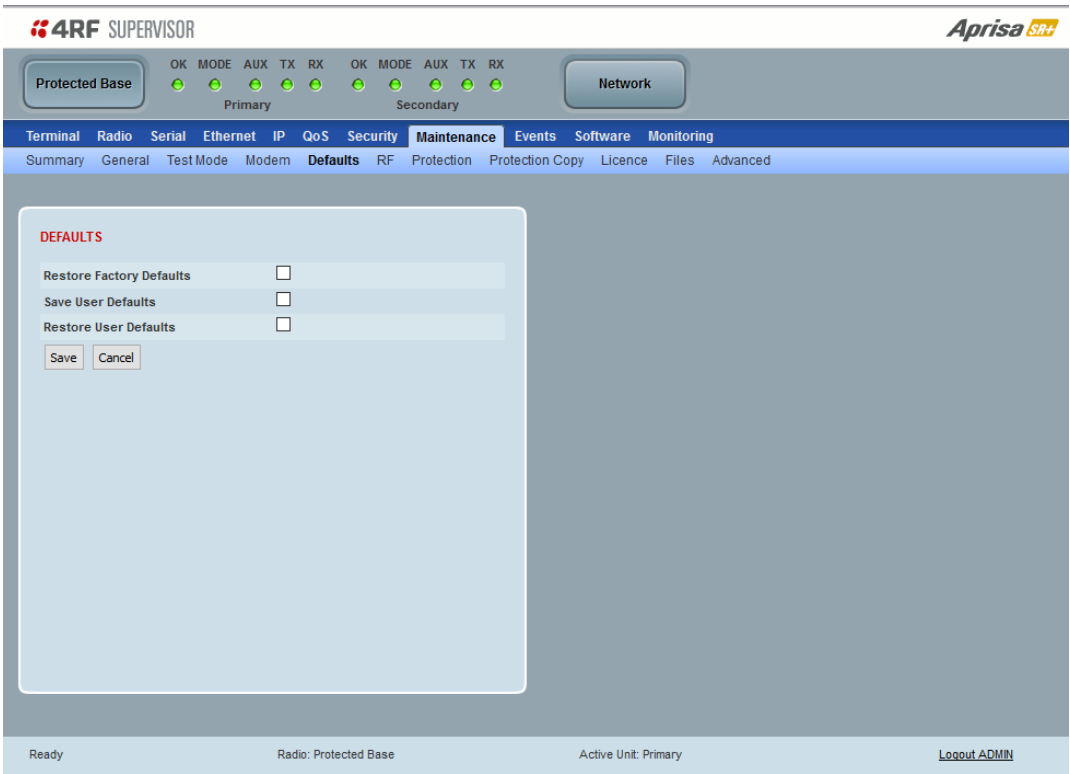
Below these settings are 'Save' and 'Cancel' buttons. The right panel, titled 'REBOOT', contains a 'Reboot' button and a dropdown menu labeled 'Protected Station'. Below these are 'Save' and 'Cancel' buttons.

The footer of the interface shows the status: 'Ready', 'Radio: Protected Base', 'Active Unit: Primary', and a 'Logout ADMIN' link.

See 'Maintenance > General' on page 261 for parameter details.

Protected Station: Maintenance > Defaults

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



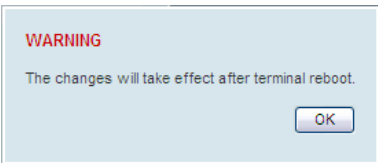
DEFAULTS

The Maintenance Defaults page is only available for the local terminal.

Restore Factory Defaults

When a radio is restored to factory defaults while installed in a protected station, the radio will default to its preconfigured protection configuration. This includes resetting the radio IP address to the default value depending on the location of the radio.

Radio Location	Protection Type	Protection Unit	Primary IP Address	Secondary IP Address	Virtual IP Address
Not in a protected station	None	Primary	169.254.50.10	0.0.0.0	0.0.0.0
Protected station radio A	Redundant	Primary	169.254.50.10	169.254.50.20	169.254.50.30
Protected station radio B	Redundant	Secondary	169.254.50.20	169.254.50.10	169.254.50.30



Note: Take care using this command.

Save User Defaults

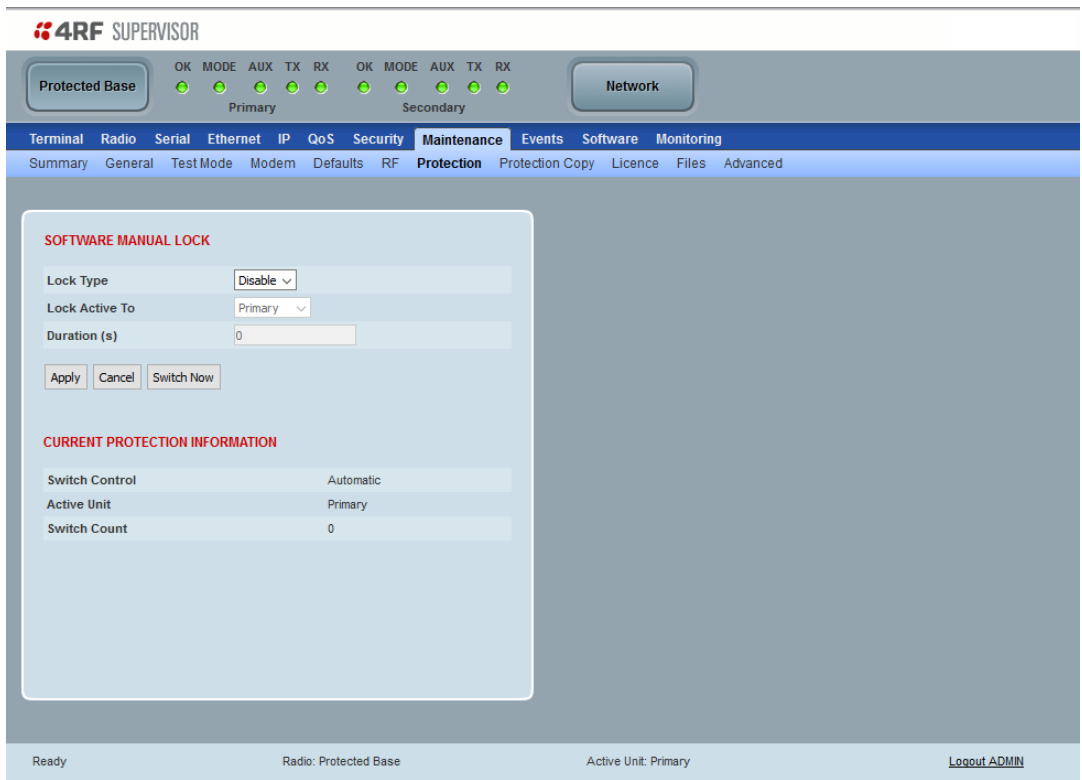
When activated, all current radio parameter settings will be saved to non-volatile memory within the radio.

Restore User Defaults

When activated, all radio parameters will be set to the settings previously saved using 'Save User Defaults'.

Protected Station: Maintenance > Protection

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



SOFTWARE MANUAL LOCK

The software Manual Lock is a software implementation of the Hardware Manual Lock switch on the Protection Switch.

Lock Active To

This parameter sets the Protection Switch Software Manual Lock. The Software Manual Lock only operates if the Hardware Manual Lock is deactivated (set to the Auto position).

Option	Function
Automatic	The protection is automatic and switching will be governed by normal switching and blocking criteria.
Primary	The primary radio will become active i.e. traffic will be switched to the primary radio.
Secondary	The secondary radio will become active i.e. traffic will be switched to the secondary radio.

Duration (s)

This parameter defines the period required for manually locking to the primary or secondary radios. When this period elapses, the Lock To becomes automatic.

Switch Now Button

This button forces a switch-over independent of the state of Lock Type.

CURRENT PROTECTION INFORMATION

Switch Control

This parameter shows the status of the switch control i.e. which mechanism is in control of the protection switch.

Option	Function
Automatic	The protection is automatic and switching will be governed by normal switching and blocking criteria.
Software Manual Lock	The Software Manual Lock has control of the protection switch.
Hardware Manual Lock	The Hardware Manual Lock has control of the protection switch.

Active Unit

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

Switch Count

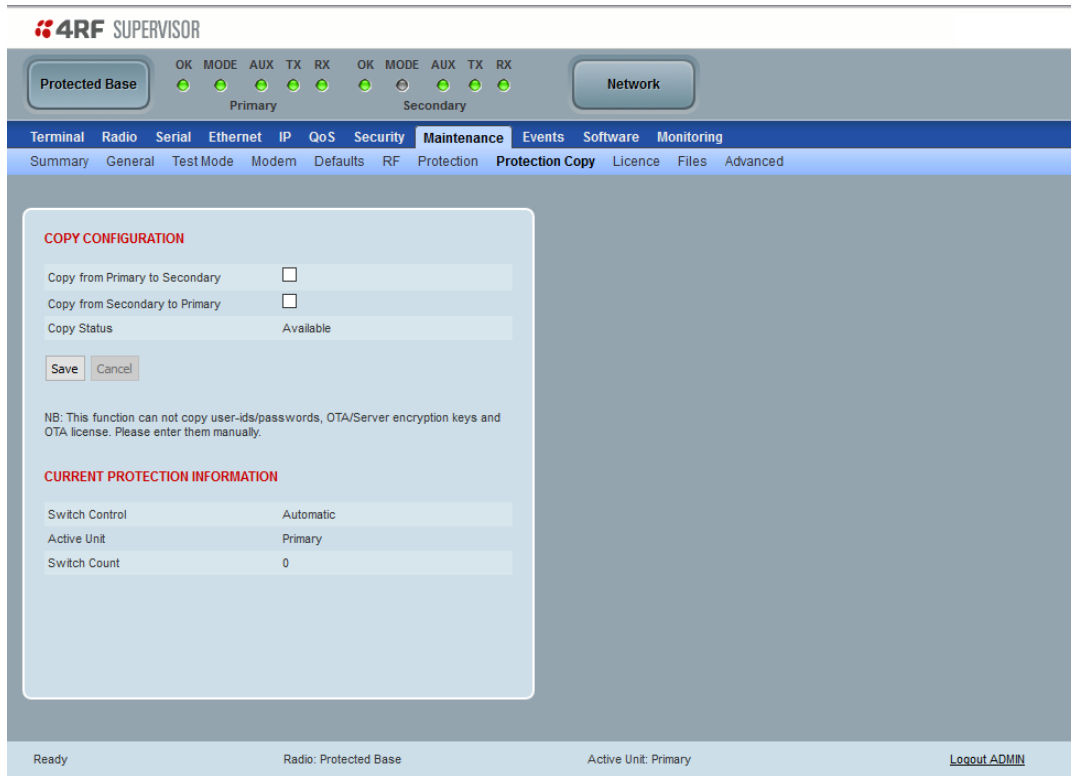
This parameter shows the number of protection switch-overs since the last radio reboot (volatile).

Automatic Periodic Switch will occur in

If this parameter is visible, the Automatic Periodic Switch feature has been enabled and will show the period before the next automatic switch-over.

Protected Station: Maintenance > Protection Copy

This page provides the management and control of the Protected Station Maintenance Protection Copy.



The screenshot shows the 4RF SUPERVISOR web interface. At the top, there are status indicators for Primary and Secondary radio units, each with OK, MODE, AUX, TX, and RX lights. Below this is a navigation bar with tabs: Terminal, Radio, Serial, Ethernet, IP, QoS, Security, Maintenance (selected), Events, Software, and Monitoring. Under the Maintenance tab, there are sub-tabs: Summary, General, Test Mode, Modem, Defaults, RF, Protection, Protection Copy (selected), Licence, Files, and Advanced.

The main content area is titled "COPY CONFIGURATION" and contains the following options:

- Copy from Primary to Secondary: ☐
- Copy from Secondary to Primary: ☐
- Copy Status: Available

Below these options are "Save" and "Cancel" buttons. A note states: "NB: This function can not copy user-ids/passwords, OTA/Server encryption keys and OTA license. Please enter them manually."

The section "CURRENT PROTECTION INFORMATION" shows the following details:

- Switch Control: Automatic
- Active Unit: Primary
- Switch Count: 0

At the bottom of the interface, a status bar shows "Ready", "Radio: Protected Base", "Active Unit: Primary", and a "Logout ADMIN" link.

COPY CONFIGURATION

When common parameters are changed in one radio, they are automatically changed in the partner radio but if one radio has been replaced in the protected station, common parameters will need to be updated in the new radio.

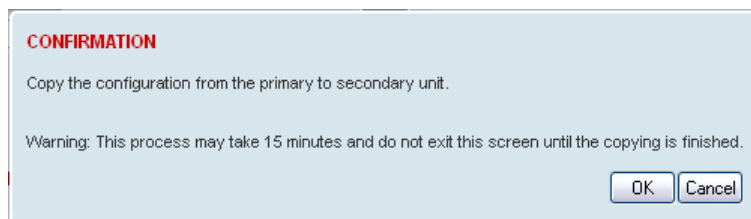
Note: This function does not copy user IDs, passwords, encryption keys or licenses. These must be entered manually.

Copy from Primary to Secondary

This parameter copies all common parameters from the primary to the secondary radio.

To activate copy configuration:

1. Tick the Copy from Primary to Secondary and click Save.



The dialog box is titled "CONFIRMATION" and contains the following text:

Copy the configuration from the primary to secondary unit.

Warning: This process may take 15 minutes and do not exit this screen until the copying is finished.

At the bottom right are "OK" and "Cancel" buttons.

2. To continue, click OK.

Copy from Secondary to Primary

This parameter copies all common parameters from the secondary to the primary radio.

Copy Status

This parameter displays the status of the Copy Configuration.

Option	Function
Available	The Copy Configuration feature can be used (but not necessarily required).
Processing	The Copy Configuration feature is running and the % completed.

CURRENT PROTECTION INFORMATION

Switch Control

This parameter shows the status of the switch control i.e. which mechanism is in control of the protection switch.

Option	Function
Automatic	The protection is automatic and switching will be governed by normal switching and blocking criteria.
Software Manual Lock	The Software Manual Lock has control of the protection switch.
Hardware Manual Lock	The Hardware Manual Lock has control of the protection switch.

Active Unit

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

Switch Count

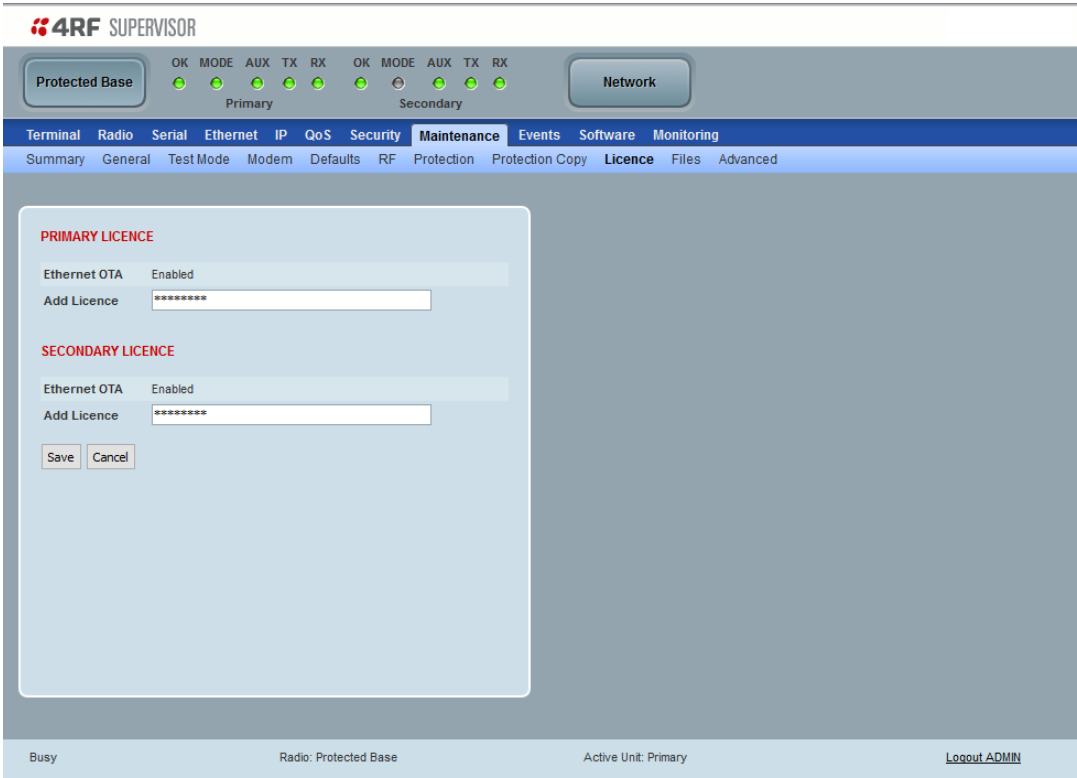
This parameter shows the number of protection switch-overs since the last radio reboot (volatile).

Automatic Periodic Switch will occur in

If this parameter is visible, the Automatic Periodic Switch feature has been enabled and will show the period before the next automatic switch-over.

Protected Station: Maintenance > Licence

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

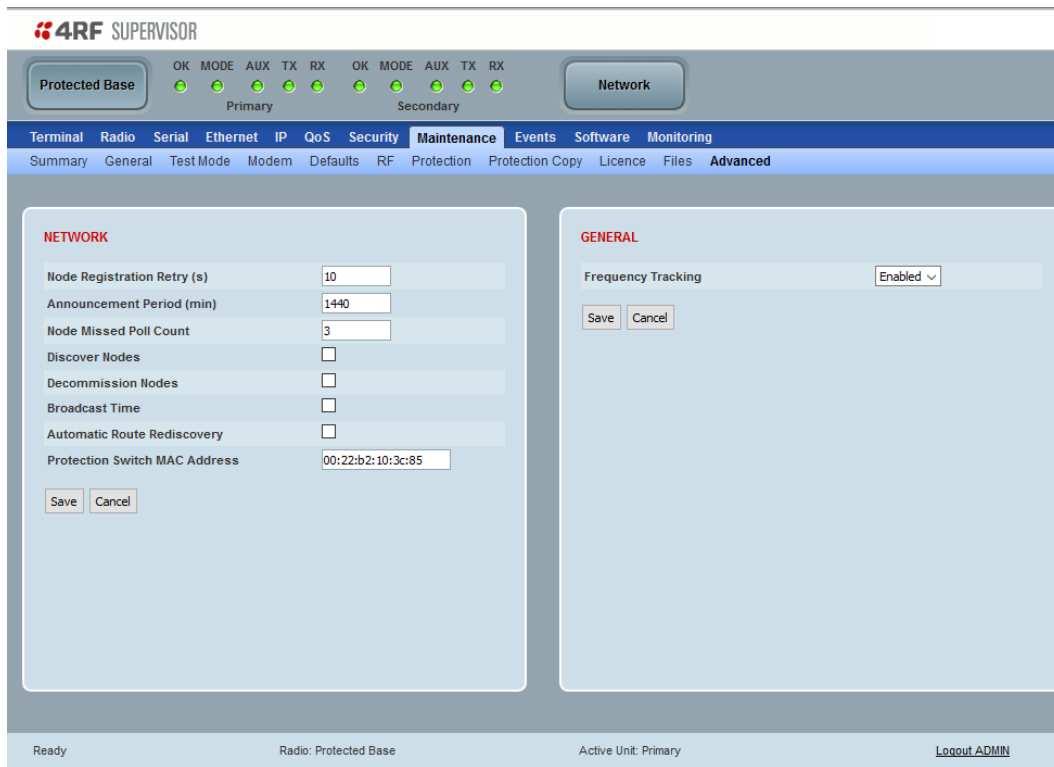


PRIMARY / SECONDARY LICENCE

See 'Maintenance > Licence' on page 270 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 276 for parameter details.

Discover Nodes

This parameter when activated triggers the base station to poll the network with Node Missed Poll Count and Node Registration Retry values.

This command only needs to be carried out on the Protected Station Active radio This will update the network table which is shared by the Standby radio.

Decommission Node(s)

This parameter when activated resets the network registrations to remove the entire network from service.

This command only needs to be carried out on the Protected Station Active radio This will update the network table which is shared by the Standby radio.

Note: Take care using this option.

Protection Switch MAC address

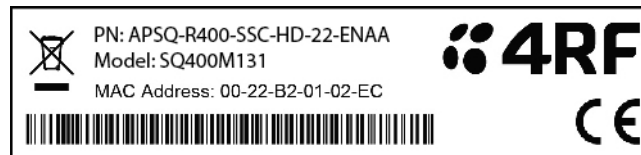
This parameter is only applicable when the radio is part of a Protected Station.

This Protection Switch MAC address is used to define the MAC address of the Protection Switch. This address is entered in the factory. Both Protected Station radios read and use this MAC address.

This MAC address entry will only be used by the software if it detects that the factory MAC address set in the internal EPROM of the protected switch is corrupted for some reason, otherwise the software will ignore the MAC address entered by the user.

The Protection Switch MAC address is used for registration process only. For example, in a remote Protected Station, both radios share the same RF MAC address and a single entry of the remote Protected Station will be presented in network table (Network Status > Network Table).

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



PRIMARY / SECONDARY CONFIGURATION

See 'Maintenance > Advanced' on page 276 for parameter details.

PRIMARY / SECONDARY MAINTENANCE FILES

See 'Maintenance > Advanced' on page 276 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:

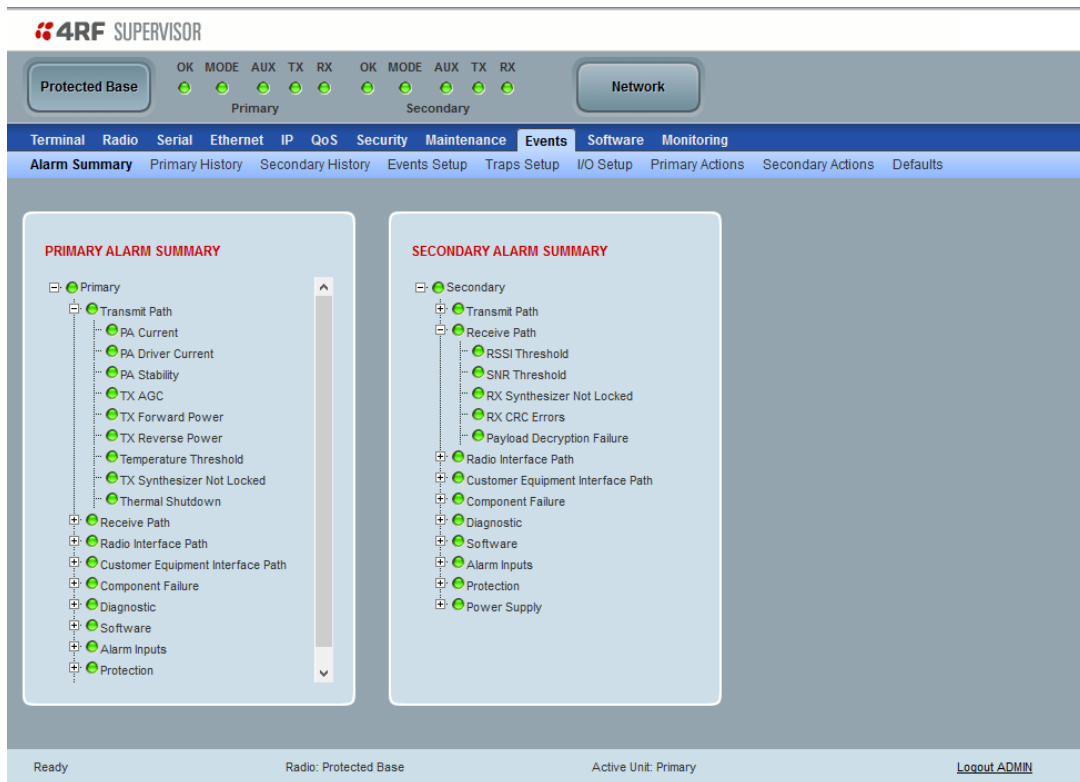
1. Alarm Events

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 458 for a complete list of events.



PRIMARY / SECONDARY ALARM SUMMARY

See ‘Events > Alarm Summary’ on page 278 for parameter details.



Protected Station: Events > Primary History

4RFSUPERVISOR

Protected Base

OKMODEAUXTXRX

Primary

OKMODEAUXTXRX

Secondary

Network

TerminalRadioSerialEthernetIPQoSSecurityMaintenanceEventsSoftwareMonitoring

Alarm SummaryPrimary HistorySecondary HistoryEvents SetupTraps SetupI/O SetupPrimary ActionsSecondary ActionsDefaults

PRIMARY EVENT HISTORY

Log ID	Date/Time	Event ID	Description	State	Severity	Additional Information
2761	06/05/2015, 02:07	55	Terminal Unit Information	inactive	information	New Registration: Remote Radio 19 (172.10.1.19) joined the network
2760	06/05/2015, 02:01	26	User Authentication Succeeded	inactive	information	SuperVisor, User admin, Local auth OK, IP Addr 172.10.1.1
2759	06/05/2015, 02:01	23	Protection Peer Comms Lost	inactive	cleared	Alarm Cleared
2758	06/05/2015, 02:01	55	Terminal Unit Information	inactive	information	Protection starting as Active
2757	06/05/2015, 02:01	23	Protection Peer Comms Lost	active	major	Comm Lost with Peer
2756	06/05/2015, 02:01	30	Software Start Up	inactive	information	User Reboot (Management)
2755	06/05/2015, 02:01	72	User Session Logout	inactive	information	SuperVisor, User admin, IP Addr 172.10.1.1
2754	06/05/2015, 02:01	39	Software Restart Required	active	warning	Channel Width Setting Changed

Auto Refresh☐PrevNext

Ready

Radio: Protected Base

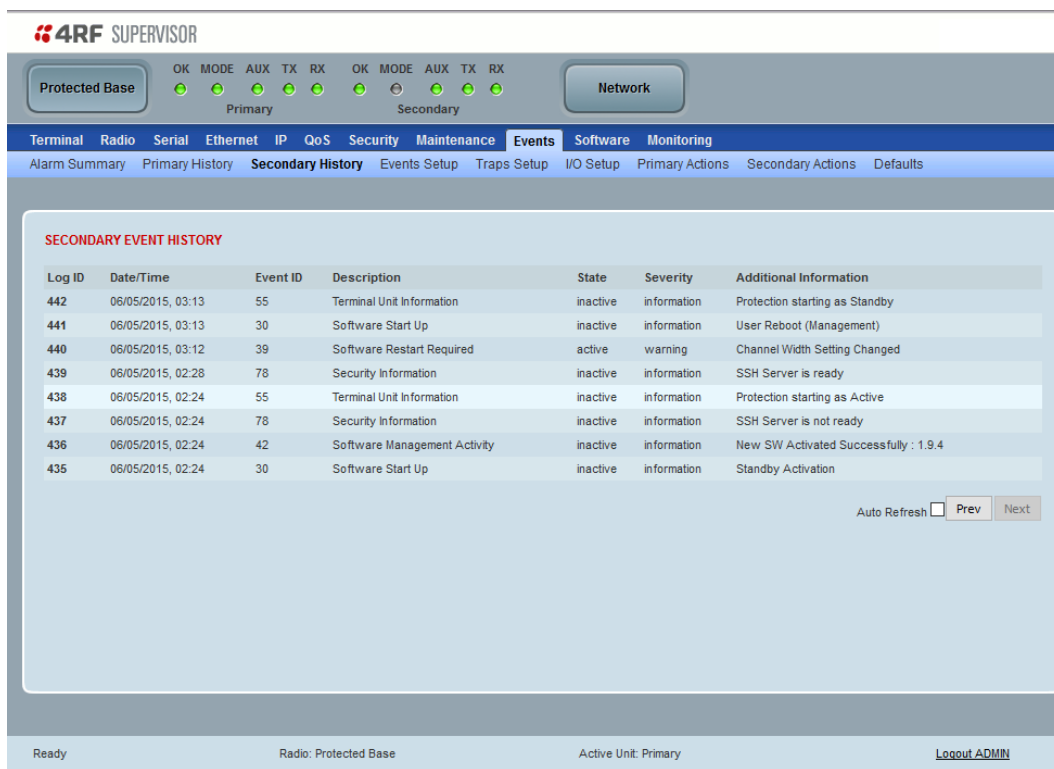
Active Unit: Primary

LogoutADMIN

PRIMARY EVENT HISTORY

See ‘Events > Event History’ on page 279 for parameter details.

Protected Station: Events > Secondary History



4RF SUPERVISOR

Protected Base OK MODE AUX TX RX OK MODE AUX TX RX Network

Primary Secondary

Terminal Radio Serial Ethernet IP QoS Security Maintenance **Events** Software Monitoring

Alarm Summary Primary History **Secondary History** Events Setup Traps Setup I/O Setup Primary Actions Secondary Actions Defaults

SECONDARY EVENT HISTORY

Log ID	Date/Time	Event ID	Description	State	Severity	Additional Information
442	06/05/2015, 03:13	55	Terminal Unit Information	inactive	information	Protection starting as Standby
441	06/05/2015, 03:13	30	Software Start Up	inactive	information	User Reboot (Management)
440	06/05/2015, 03:12	39	Software Restart Required	active	warning	Channel Width Setting Changed
439	06/05/2015, 02:28	78	Security Information	inactive	information	SSH Server is ready
438	06/05/2015, 02:24	55	Terminal Unit Information	inactive	information	Protection starting as Active
437	06/05/2015, 02:24	78	Security Information	inactive	information	SSH Server is not ready
436	06/05/2015, 02:24	42	Software Management Activity	inactive	information	New SW Activated Successfully : 1.9.4
435	06/05/2015, 02:24	30	Software Start Up	inactive	information	Standby Activation

Auto Refresh ☐ Prev Next

Ready Radio: Protected Base Active Unit: Primary [Logout ADMIN](#)

SECONDARY EVENT HISTORY

See 'Events > Event History' on page 279 for parameter details.



Protected Station: Events > I/O Setup

4RFSUPERVISOR

Protected Base

OKMODEAUXTXRX

Primary

OKMODEAUXTXRX

Secondary

Network

TerminalRadioSerialEthernetIPQoSSecurityMaintenanceEventsSoftwareMonitoring

Alarm SummaryPrimary HistorySecondary HistoryEvents SetupTraps SetupI/O SetupPrimary ActionsSecondary ActionsDefaults

PRIMARY ALARM PORTS

ID	Name	Type	Active State	Current State
1	User ID 1	Input	High	Low
2	User ID 2	Input	High	Low
3	User ID 3	Output	High	Low
4	User ID 4	Output	High	Low

SECONDARY ALARM PORTS

ID	Name	Type	Active State	Current State
1	User ID 1	Input	High	Low
2	User ID 2	Input	High	Low
3	User ID 3	Output	High	Low
4	User ID 4	Output	High	Low

SaveCancel

Done

Radio: Protected Base

Active Unit: Primary

LogoutADMIN

PRIMARY / SECONDARY ALARM PORTS

The alarm ports on a protected station are not switched. Each individual Alarm I/O goes directly to each radio. Both the Primary Alarm Ports and a Secondary Alarm Ports need to be configured.

See ‘Events > Alarm I/O Setup’ on page 284 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 449). 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 445). 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 radios 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 radios 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.

4RF SUPERVISOR

Protected Base

OK MODE AUX TX RX OK MODE AUX TX RX

PrimarySecondary

Network

TerminalRadioSerialEthernetIPQoSSecurityMaintenanceEventsSoftwareMonitoring

SummarySetupPrimary File TransferSecondary File TransferManagerRemote DistributionRemote Activation

PRIMARY SOFTWARE VERSIONS

Current Version	1.9.4
Previous Version	1.7.0
Software Pack Version	Unknown

SECONDARY SOFTWARE VERSIONS

Current Version	1.9.4
Previous Version	1.7.0
Software Pack Version	Unknown

PRIMARY USB AUTOMATIC UPGRADE

USB Boot Cycle Upgrade	Load And Activate

SECONDARY USB AUTOMATIC UPGRADE

USB Boot Cycle Upgrade	Load And Activate

PRIMARY FILE TRANSFER

Transfer Activity	Idle
Method	-
Filename	-
Transfer Result	-

SECONDARY FILE TRANSFER

Transfer Activity	Idle
Method	-
Filename	-
Transfer Result	-

DoneRadio: Protected BaseActive Unit: PrimaryLogout ADMIN

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.
HTTP	Transfers the software from a PC to the primary radio.
Transfer from Secondary Unit	Transfers the software from the secondary radio to the primary radio. This function is only available when the Protected Station is not a Base Station.

PRIMARY FILE TRANSFER STATUS

See ‘Software > File Transfer’ on page 295 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 294), 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 383 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 383 to activate the Software Pack. The radio will reboot automatically.

Transfer from Secondary Unit

1. Select Transfer from Secondary Unit.
2. Click on ‘Start Transfer’.

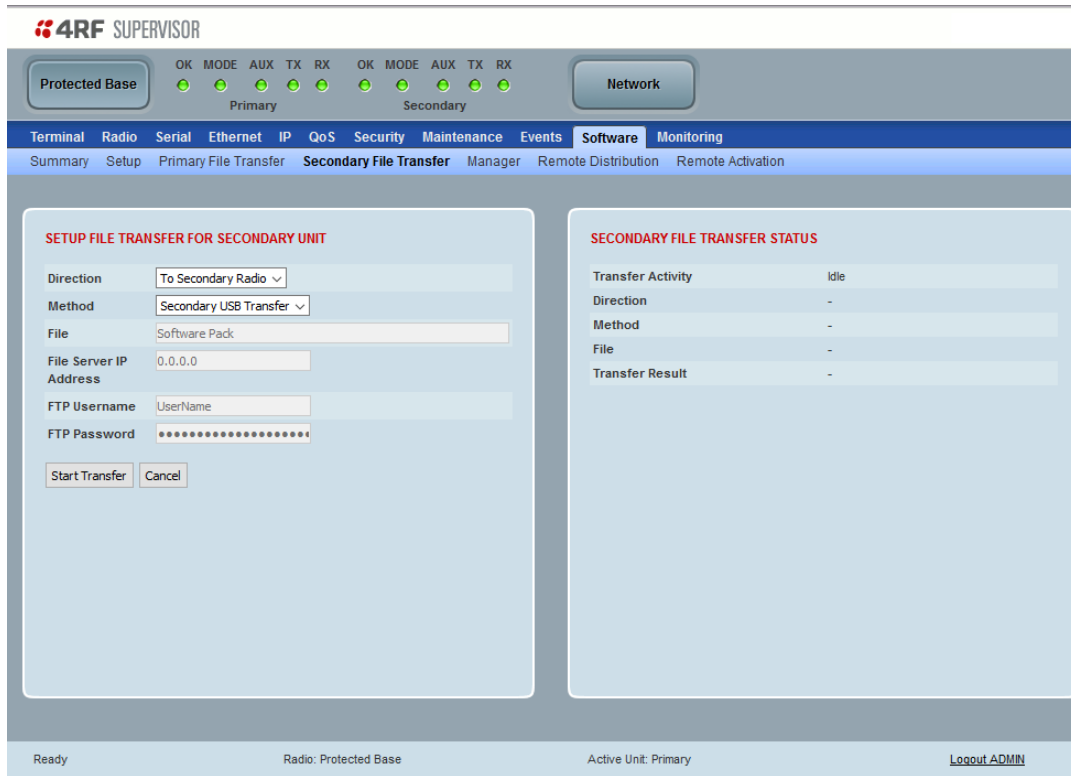
SECONDARY FILE TRANSFER STATUS	
Transfer Activity	In Progress
Direction	To This Radio
Method	Protected Partner Transfer
File	Software Pack
Transfer Result	Starting Transfer

3. Go to ‘Protected Station: Software > Manager’ on page 383 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 373) 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.
HTTP	Transfers the software from a PC to the secondary radio.
Transfer from Primary Unit	Transfers the software from the primary radio to the secondary radio. This function is only available when the Protected Station is not a Base Station.

SECONDARY FILE TRANSFER STATUS

See 'Software > File Transfer' on page 295 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 294), 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 383 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 383 to activate the Software Pack. The radio will reboot automatically.

Transfer from Primary Unit

1. Select Transfer from Primary Unit.
2. Click on 'Start Transfer'.

SECONDARY FILE TRANSFER STATUS	
Transfer Activity	In Progress
Direction	To This Radio
Method	Protected Partner Transfer
File	Software Pack
Transfer Result	Starting Transfer

3. Go to 'Protected Station: Software > Manager' on page 383 to activate the Software Pack. The radio will reboot automatically.

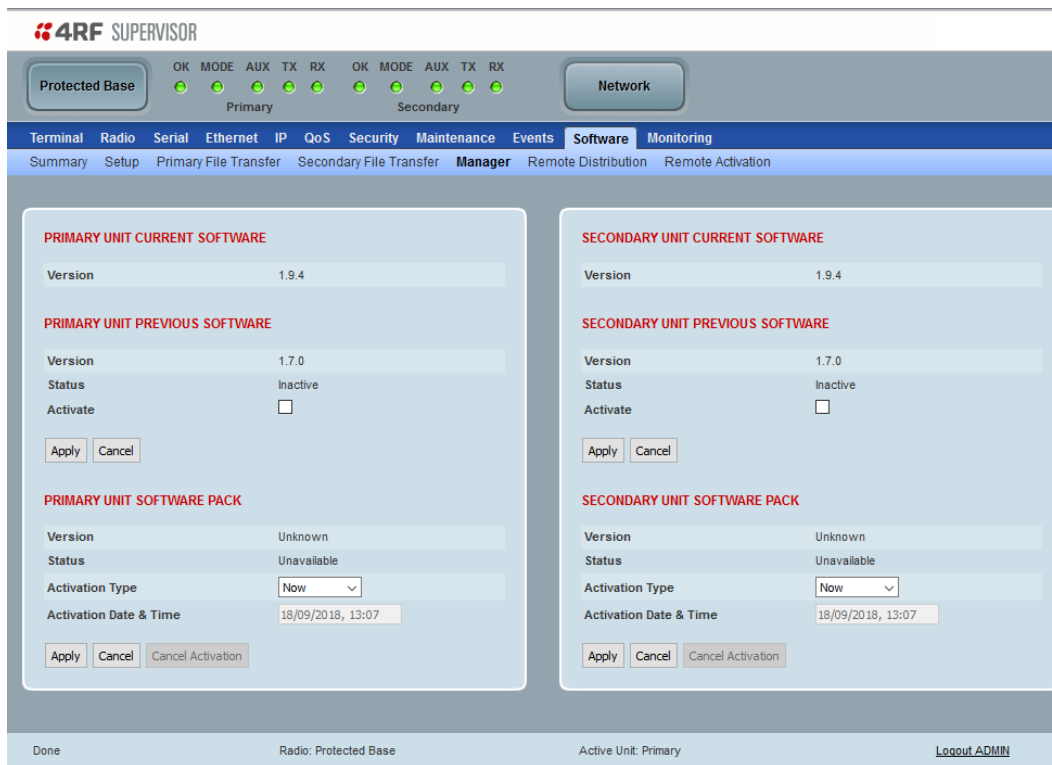
If the file transfer fails, check the Event History page (see 'Protected Station: Events > Primary History' on page 372) for more details of the transfer.

Protected Station: Software > Manager

This page summaries and manages the software versions available in the primary and secondary radios.

The manager is predominantly used to activate new software on single radios. Network activation is performed with 'Protected Station: Software > Remote Activation'.

Both the previous software (if available) and Software Pack versions can be activated on each radio from this page.



PRIMARY / SECONDARY CURRENT SOFTWARE

Version

This parameter displays the software version running on the radio.

PRIMARY / SECONDARY PREVIOUS SOFTWARE

Version

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

Status

This parameter displays the status of the software version running on the radio.

Option	Function
Active	The software is operating the radio.
Inactive	The software is not operating the radio but could be re-activated if required.

PRIMARY / SECONDARY SOFTWARE PACK*Version*

This parameter displays the software pack version available for distribution on base station and activate on all stations.

Status

This parameter displays the status of the software pack version.

Option	Function
Available	On the base station, the software pack is available for distribution. On all stations, the software pack is available for activation.
Activating	The software pack is activating in the radio.
Unavailable	There is no software pack loaded into the radio.

Activate

See 'Software > Manager' on page 299 for the activation options.

Protected Station: Software > Remote Distribution

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

The Software Pack loaded into the base station with the file transfer process (see ‘Protected Station: Software > Primary File Transfer’ on page 377) is distributed via the radio link to all remote radios from the active radio.

The distribution process is monitored from this page.

When all remote radios receive the Software Pack version, the software can be remotely activated on all remote radios.

This page is only available when the radio is configured as a Base Station.

4RF SUPERVISOR

Protected Base OK MODE AUX TX RX OK MODE AUX TX RX Network

Primary Secondary

Terminal Radio Serial Ethernet IP QoS Security Maintenance Events **Software** Monitoring

Summary Setup Primary File Transfer Secondary File Transfer Manager **Remote Distribution** Remote Activation

REMOTE SOFTWARE DISTRIBUTION

Software Pack Version Unknown

Status Available

Start Transfer ☐

Apply Cancel

Ready Radio: Protected Base Active Unit: Primary Logout ADMIN

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 radios in the network.

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

The impact of software distribution traffic upon customer traffic is controlled by two settings. The traffic uses the 'Default Management Data Priority' QoS setting, and the rate of packets at this priority is controlled with the 'Background Bulk Data Transfer Rate' setting in Radio > Channel Setup.

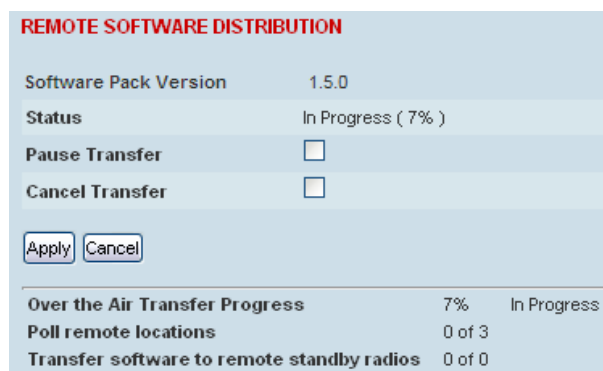
To distribute software to remote radios:

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 377).

1. Distribution is performed only to the radios listed in the Network Table and powered on. If a radio is listed in the network table, but cannot be contacted, it will slow down the distribution of software.

To ensure that the Network Table is up to date, it is recommended running the node discover function (see 'Discover Nodes' on page 276).

2. Click on 'Start Transfer'.



REMOTE SOFTWARE DISTRIBUTION		
Software Pack Version	1.5.0	
Status	In Progress (7%)	
Pause Transfer	☐	
Cancel Transfer	☐	
Apply Cancel		
Over the Air Transfer Progress	7%	In Progress
Poll remote locations	0 of 3	
Transfer software to remote standby radios	0 of 0	

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

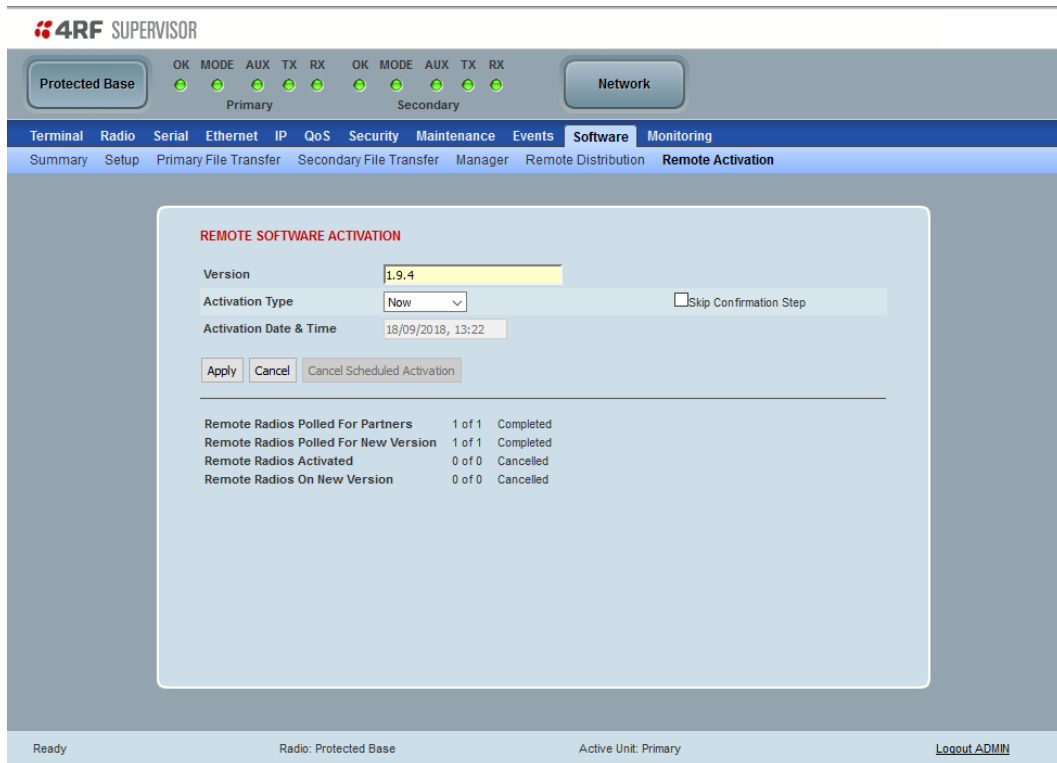
This page provides the mechanism to activate software on all remote protected stations.

The Software Pack has been loaded into the base station with the file transfer process (see ‘Protected Station: Software > Primary File Transfer’ on page 377) and distributed via the radio link to all remote radios from the active radio.

When all remote radios receive the Software Pack version, the software can be remotely activated on all remote radios.

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 radios, the software is then activated in all the remote radios with this command. If successful, then activate the software pack in the base station to complete the network upgrade.

Version

This parameter displays the software version for activation. The default version is the software pack version but any valid software version can be entered in the format ‘n.n.n’.

Activation Type

This parameter sets when the software pack activation will occur.

Option	Function
Now	Activates the software pack now.
Date & Time	Activates the software pack at the Date & Time set in the following parameter.

Activation Date & Time

This parameter sets the Date & Time when the software pack activation will occur.

This setting can be any future date and 24 hour time.

Skip Confirmation Step

This parameter when enabled skips the confirmation step during the activation process.

Normally, the confirmation step will require use intervention to accept the confirmation which will halt the activation process. Skipping the confirmation will enable the activation process to continue without use intervention.

To activate software in remote radios:

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 295) and that distributed to all remote radios in the network.

Note: Do not navigate SuperVisor away from this page during the activation process (SuperVisor can lose PC focus).

1. Enter the Software Pack version (if different from displayed version).
2. See ‘Software > Manager’ on page 299 for the activation options.

REMOTE SOFTWARE ACTIVATION

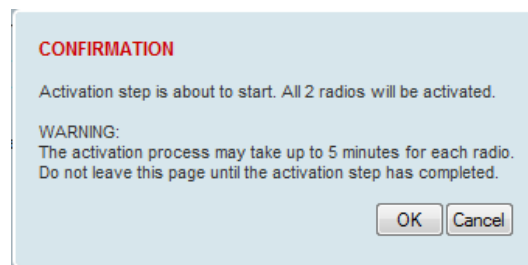
Version

Remote Radios Polled For Partners	4 of 4	Completed
Remote Radios Polled For New Version	0 of 4	In Progress
Remote Radios Activated	0 of 0	
Remote Radios On New Version	0 of 0	

The remote radios 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.

REMOTE SOFTWARE ACTIVATION

Version

Start Activation

Remote Radios Polled For Partners	4 of 4	Completed
Remote Radios Polled For New Version	0 of 4	Completed
Remote Radios Activated	0 of 0	Cancelled
Remote Radios On New Version	0 of 0	Cancelled

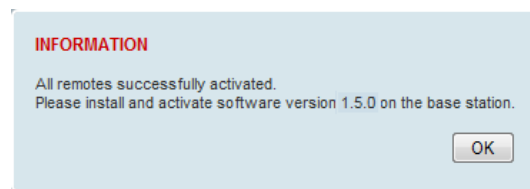
REMOTE ACTIVATION EXCEPTIONS

Name	IP Address	Version	Exception
Protected Remote Station	172.17.70.2	1.5.0	Software Version not on the radio (Step 2)
Remote125	172.17.70.125	1.5.0	Software Version not on the radio (Step 2)
Protected Remote Station	172.17.70.1	1.5.0	Software Version not on the radio (Step 2)

Prev Next

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 299).



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;

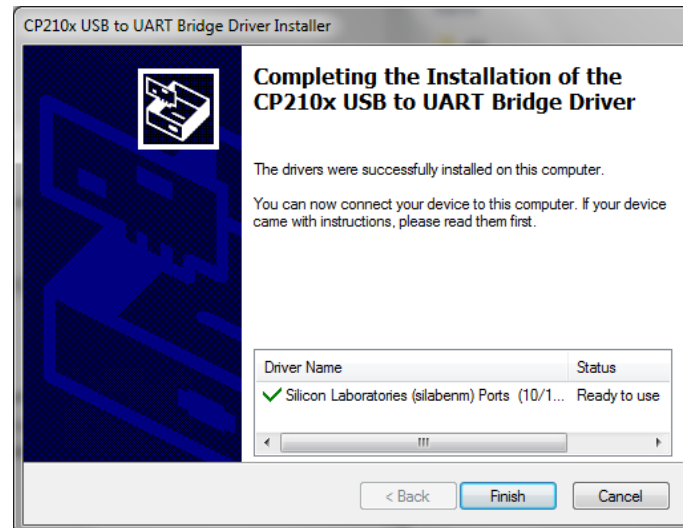
- USB via the Management Port (MGMT USB micro type B) or the USB host port  (USB type A) with a USB converter to RS-232 convertor.
- Telnet via the Ethernet Port (RJ45) using standard TCP/UDP port 23.
- Secure Shell (SSH) application via the Ethernet Port (RJ45) using standard TCP/UDP port 22.

Connecting to the CLI via the Management Port (MGMT)

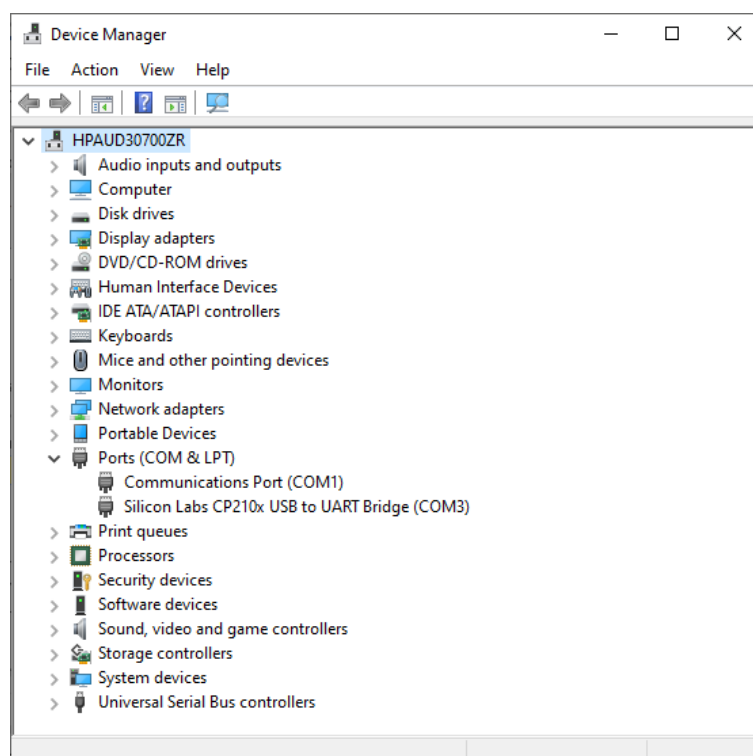
1. Connect the radio management port (MGMT) to your PC with a USB A to USB micro B cable.
2. USB to UART Bridge VCP Drivers are required to connect the radio USB port to your PC. You can download and install the relevant driver from;

<https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers>

Unzip the USB serial driver to a temporary location and install the appropriate driver on your computer.



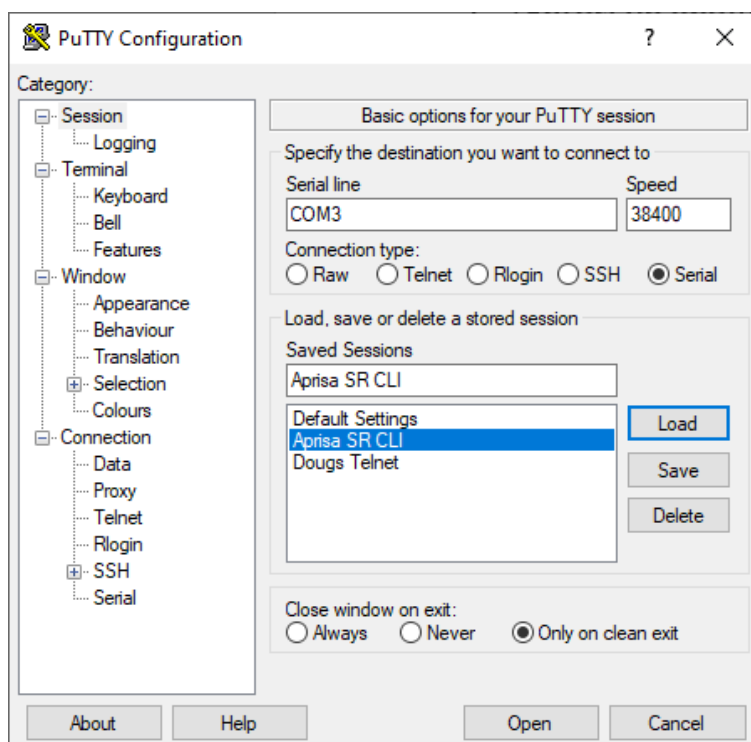
3. Go to your computer device manager (Windows > Control Panel > Device Manager)
4. Click on 'Ports (COM & LPT)'
5. Make a note of the COM port which has been allocated to the 'Silicon Labs CP210x USB to UART Bridge' (COM3 in the example below)



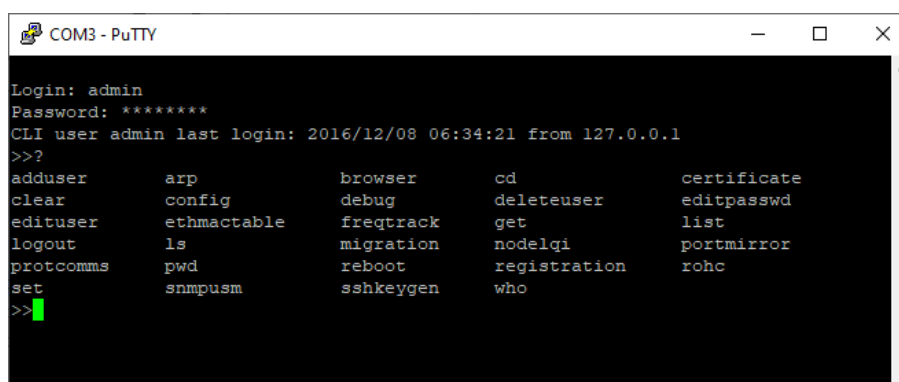
6. Open terminal emulator program e.g. Putty.

Putty Example

7. Enter a name for the connection e.g. Aprisa SR CLI and save for future use.



8. Click Open and the terminal window will open.
9. Press the enter key to initiate the session.
10. Login to the CLI with a default username 'admin' and password 'admin'.
11. Type ? enter and the Aprisa SR+ CLI top level menu is shown:



Connecting to the CLI via Telnet

1. Connect the PC Ethernet to the radio Ethernet port (assuming a compatible IP address range).
2. Open the PC Command Prompt.
3. Type Telnet and the IP address of the radio 'Telnet xx.xx.xx.xx'.
4. Login to the CLI with a default username 'admin' and password 'admin'.

Connecting to the CLI via SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. It is used in the Aprisa SR+ to provide a secure CLI remote access connection to the radio. SSH is operated in server client mode, where the radio is acting as the SSH server. The communication between the client and radio (server) is encrypted in SSHv2 (where SSHv2 vs SSHv1 uses a more enhanced security encryption algorithm).

The SSHv2 protocol consists of three major components:

- The Transport Layer Protocol provides server authentication, confidentiality and integrity with perfect forward secrecy.
- The User Authentication Protocol which authenticates the client to the server.
- The Connection Protocol which multiplexes the encrypted tunnel into several logical channels.

The SSHv2 protocol has the following advantages:

- Allows secure CLI connection over the internet.
- Provides an alternate secure CLI connection to the un-secure CLI Telnet connection.
- RADIUS, retype password change, user privilege and user account lockout are also applied over SSHv2.

The Aprisa SR+ supports the following SSH features capabilities:

- SSH is operated over Ethernet ports. It is also operated over the RF port when the radio is in Advanced Router or Gateway router modes. SSH is not operated over USB or micro USB CLI.
- The radio SSH supports 'key re-exchange' which is initiated after 1 hour or 1GB data but only if client initiates this process.
- The radio supports simultaneous sessions of CLI / USB-CLI / Telnet / SSH.
- SSH is supported OTA to repeater/remotes using the RF IP Address in advanced router mode.
- Current SSH is supported OTA to repeater/remotes using the RF IP Address in advanced router mode.
- Regenerates a new random SSH public/private key-pairs, using the CLI command 'sshkeygen'. This command will delete current key pairs and on next reboot the radio will create a new pair.
- Factory reset doesn't clear the public / private key pairs.
- Supervisor 'Inactivity timeout' in Maintenance > General is also used for SSH to expire idle sessions.
- Supervisor Maintenance > Advanced configuration save/restore does not save/restore the SSH public / private keys pairs.
- A maximum 5 simultaneous SSH sessions can be supported.

The Aprisa radio SSH server uses the following algorithms to secure the connection:

- Key exchange: diffie-hellman-group14-sha1, diffie-hellman-group1-sha1
- Data Integrity: hmac-sha2-256, hmac-sha1-96, hmac-sha1
- Encryption: aes128-cbc
- Host key: RSA

1. Connect the PC Ethernet to the radio Ethernet port (assuming a compatible IP address range).
2. Install one of the following tested SSH clients on your PC.
 - PuTTY - Windows / Ubuntu
 - TeraTerm
 - Secure CRT
 - MobaXterm
 - OpenSSH
 - Linux Terminal (Ubuntu)
 - Kitty portal
 - DameWare
 - smartTTY
 - Terminals (<https://terminals.codeplex.com/>)
 - mRemoteng - Multi-Remote Next Generation
3. Open the SSH client.
4. Login to the CLI with a default username 'admin' and password 'admin'.

CLI Commands

The `cd` and `ls` commands can be used to navigate the MIBs in the CLI however, 4RF recommends the use of the `get` and `set` commands in conjunction with the distributed MIB files.

The MIB files are provided as part of the software pack available on the 4RF website <https://www.4rf.com/secure>.

Contact support@4rf.com if you are not familiar with the use of MIB files.

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
get	Reads the value of a MIB object The MIB object name can be obtained in the MIB files. It can be a scalar object or a table object. If the MIB object is a scalar, then the CLI command needs to be 'get ObjectName' If the MIB object name is a table, then the CLI command needs to be 'get ObjectName ObjectIndex' Examples: <pre>get termName get unitConfigOperatingMode 1</pre>
set	Sets the value of a MIB object The MIB object name can be obtained in the MIB files. It can be a scalar object or a table object. If the MIB object is a scalar, then the CLI command needs to be 'set ObjectName ObjectValue' If the MIB object name is a table, then the CLI command needs to be 'set ObjectName ObjectValue ObjectIndex' Examples: <pre>set termName MyRadio set unitConfigOperatingMode 1 1</pre>
config	
cd	Changes the directory
ls	Displays the next level menu items
pwd	Displays the current working directory
clear	Clears the screen
logout	Logs out from the CLI
adduser	adduser [-i <role>] <user name> <password> <password confirmation> Notes: - The role parameter must be ALL CAPS - Neither password nor account aging are being used by the radio

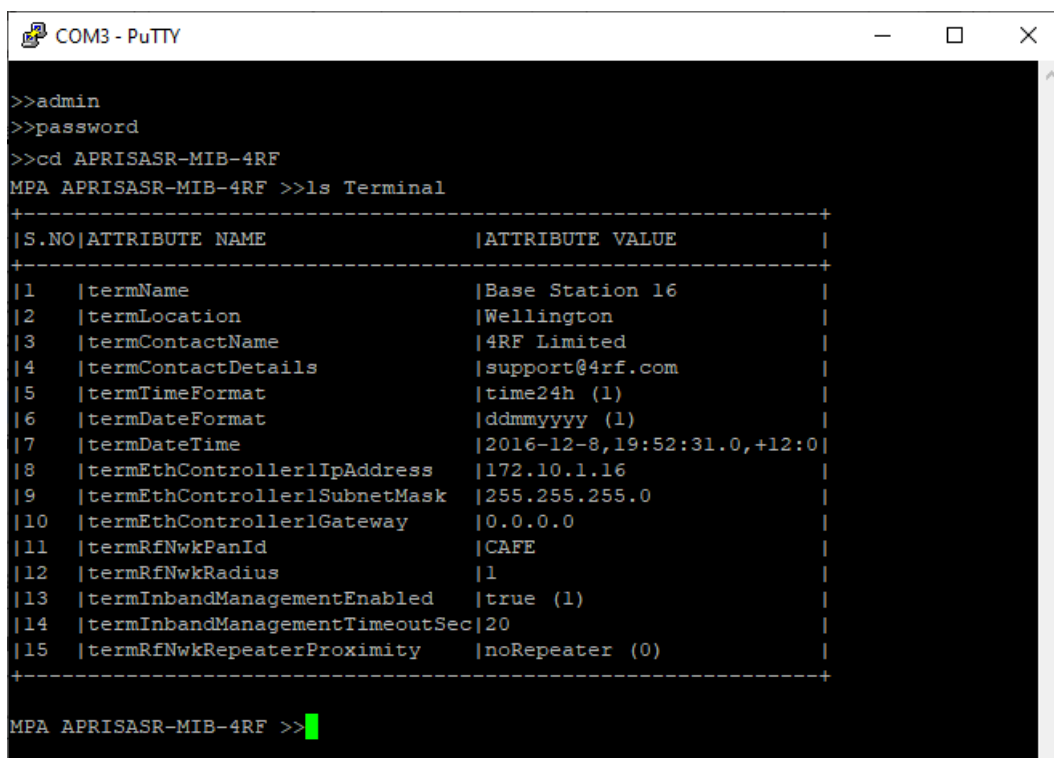
CLI Command	Usage
deleteuser	deleteuser <userName>
edituser	edituser [-p <password>] [-c <password confirmation>] [-i <role>] <userName>
editpasswd	editpasswd <old password> <new password> <password confirmation>
who	Shows the users currently logged into the radio
debug	Used by 4RF for detailed debug
list	list <tablename> e.g. list user
reboot	Reboots the radio
snmpusrm	reset Resets SNMPv3 users to Default
registration	decommissionnode nodeAddr <hex format node address> e.g. 000D Decommissions a radio from the network table using the node address
registration	decommissionnode macAddr <hex format MAC address colon separated> e.g. 00:11:22:33:44:55 Decommissions a radio from the network table using the MAC address
certificate	loaduser certfname param(STR) keyfname param(STR) Loads a user certificate into the radio. User-loaded certificates will have a higher priority in the radio's HTTPS server than automatically / manually generated certificates if they exist. 4RF has published an application note 'Aprisa SR+ Application Note - Certificate Loading Options and Instructions.pdf'. This document is available on the 4RF website https://www.4rf.com/secure .
certificate	clearuser Clears the current user-loaded certificate in the radio
certificate	create [keytype param(RSA or ECDSA)] [keylength param(INT)] Manually generates a certificate in the radio. If a valid user-loaded certificate is present in the radio, manually generating a certificate will be ignored until the current user-loaded certificate is deleted.
certificate	loadca CAcertfname param(STR) CAkeyfname param(STR) Loads a Certificate Authority (CA) certificate into the radio

Viewing the CLI Terminal Summary

At the command prompt, type:

```
cd APRISASR-MIB-4RF
```

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



```
COM3 - PuTTY
>>admin
>>password
>>cd APRISASR-MIB-4RF
MPA APRISASR-MIB-4RF >>ls Terminal
+-----+
|S.NO|ATTRIBUTE NAME          |ATTRIBUTE VALUE      |
+-----+
|1| |termName                 |Base Station 16      |
|2| |termLocation             |Wellington           |
|3| |termContactName          |4RF Limited          |
|4| |termContactDetails       |support@4rf.com      |
|5| |termTimeFormat           |time24h (1)         |
|6| |termDateFormat          |ddmmyyyy (1)        |
|7| |termDateTime             |2016-12-8,19:52:31.0,+12:0|
|8| |termEthController1IpAddress |172.10.1.16         |
|9| |termEthController1SubnetMask |255.255.255.0       |
|10| |termEthController1Gateway  |0.0.0.0              |
|11| |termRfNwkPanId           |CAFE                 |
|12| |termRfNwkRadius          |1                    |
|13| |termInbandManagementEnabled |true (1)             |
|14| |termInbandManagementTimeoutSec|20                  |
|15| |termRfNwkRepeaterProximity |noRepeater (0)      |
+-----+
MPA APRISASR-MIB-4RF >>
```

Changing the Radio IP Address

At the command prompt, type:

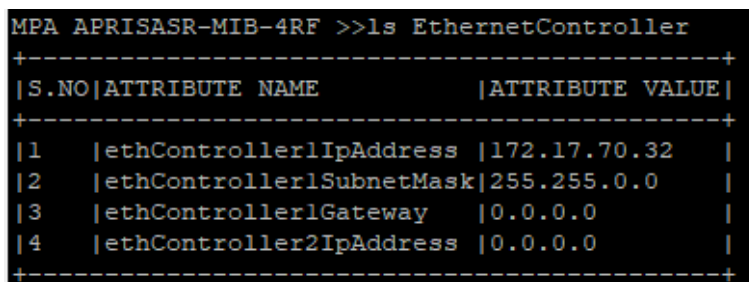
```
cd APRISASR-MIB-4RF
```

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

```
set ethController1IpAddress xxx.xxx.xxx.xxx
```

```
set ethController1SubnetMask 255.255.0.0
```

```
set ethController1Gateway 0.0.0.0
```



```
MPA APRISASR-MIB-4RF >>ls EthernetController
+-----+
|S.NO|ATTRIBUTE NAME          |ATTRIBUTE VALUE      |
+-----+
|1| |ethController1IpAddress  |172.17.70.32        |
|2| |ethController1SubnetMask |255.255.0.0         |
|3| |ethController1Gateway    |0.0.0.0              |
|4| |ethController2IpAddress  |0.0.0.0              |
+-----+
```

Wireshark Debug Access

These commands are provided for diagnosing problems using Wireshark. By enabling this function, you can connect a computer running Wireshark to the second port of a base station or remote radio to monitor the traffic of the primary port.

The command for port mirroring (on the CLI) is as follows:

CLI Command	Usage
portmirror enable ETH1 ETH2	This will enable monitoring of ETH1 on ETH2
portmirror disable ETH1	This will disable monitoring of ETH1

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 radio yagi antennas must also have vertical polarization.

Aligning the Antennas

Align the remote radio 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 67).

Note: Low gain antennas need less adjustment in elevation as they are simply aimed at the horizon. They should always be panned horizontally to find the peak signal.

1. Press and hold the TEST button on the radio LED panel until all the LEDs flash green (about 3 - 5 seconds).

Note: The time for the LEDs to display the RSSI result is variable, depending on the network traffic, and can be up to 5 seconds. Small antenna adjustments should be made and then wait for the display to refresh.

The RSSI poll refresh rate can be set with the SuperVisor command 'Transmit Period' (see 'Maintenance > Test Mode' on page 263).

2. Move the antenna through a complete sweep horizontally (pan). Note down the RSSI reading for all the peaks in RSSI that you discover in the pan.
3. Move the antenna to the position corresponding to the maximum RSSI value obtained during the pan. Move the antenna horizontally slightly to each side of this maximum to find the two points where the RSSI drops slightly.
4. Move the antenna halfway between these two points and tighten the clamp.
5. If the antenna has an elevation adjustment, move the antenna through a complete sweep (tilt) vertically. Note down the RSSI reading for all the peaks in RSSI that you discover in the tilt.
6. Move the antenna to the position corresponding to the maximum RSSI value obtained during the tilt. Move the antenna slightly up and then down from the maximum to find the two points where the RSSI drops slightly.
7. Move the antenna halfway between these two points and tighten the clamp.
8. Recheck the pan (steps 2-4) and tighten all the clamps firmly.
9. To exit Test Mode, press and hold the TEST button until all the LEDs flash red (about 3 - 5 seconds).

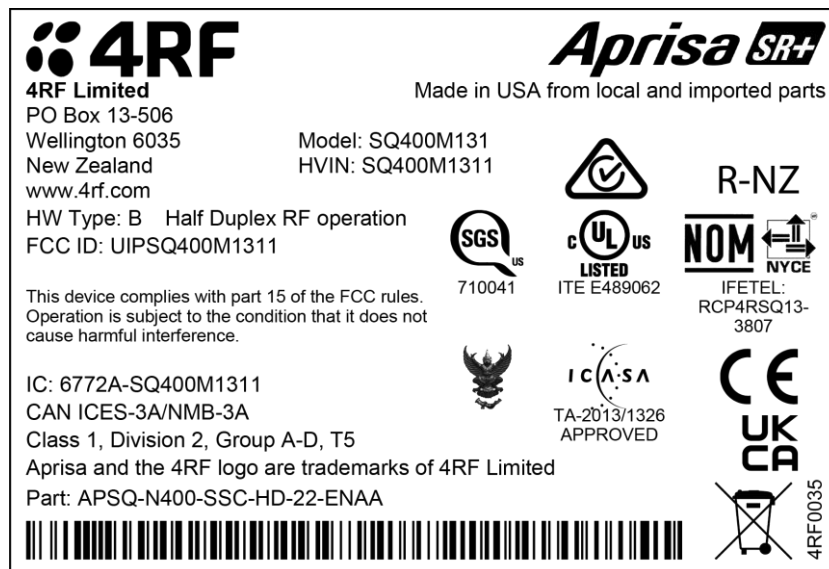
9. Product Options

Radio Hardware Types

The hardware variants of the Aprisa SR+ radio.

Option	Function
HW Type A, HW Type A1	Standard Aprisa SR+ radio
HW Type B, HW Type B1	Power optimized radio including Sleep Modes
HW Type C, HW Type C1	100 kHz channel size

The Aprisa SR+ hardware type can be identified from SuperVisor (see ‘HW Type’ on page 107) or from the Compliance label on the radio bottom.



Hardware Software Compatibility

Hardware with a 1 in the HW Type: on the product label e.g. HW Type: B1, HW Type: C1, require software version 2.1.0 or later to operate. Networks can contain a mix of hardware types.

Data Interface Ports

The standard Aprisa SR+ provides multiple interface port options for combinations of Ethernet and RS-232 serial for a total of four interface ports i.e. port options of 2E2S, 3E1S or 4E0S, where E=Ethernet, S=Serial port.

The product shown below is the two Ethernet ports plus two RS-232 serial ports.



Interface Port Option	Part Number
4 Ethernet ports and no RS-232 serial ports	APSQ-N400-SSC-HD- <u>40</u> -ENAA
3 Ethernet ports and 1 RS-232 serial port	APSQ-N400-SSC-HD- <u>31</u> -ENAA
2 Ethernet ports and 2 RS-232 serial ports	APSQ-N400-SSC-HD- <u>22</u> -ENAA

Note: The optional serial interface is always available via the USB to serial converter.

Full Duplex Base Station

The Aprisa SR+ supports Full Duplex base station hardware. This option works with half duplex repeater / remote radios. The base station can transmit while simultaneously receiving from the repeater /remote radios.

Example of a 400 MHz full duplex Aprisa SR+.

Part Number	Part Description
APSQ-N400-SSC-FD-22-ENAA	4RF SR+, BR, 400-470 MHz, SSC, Full Duplex, 2E2S, EN, STD

Point-To-Point Link

The Aprisa SR+ can be configured for Point-To-Point (PTP) operation transporting a combination of serial data and Ethernet data between the local and remote radio (see 'Terminal Operating Mode' on page 116).

SuperVisor Point-To-Point

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



Branding Bar

Control Bar

Level 1 Menu

Level 2 Menu

Selected Menu Tab

Alarm Bar

Task Window

Terminal Summary

Terminal Name	Local Radio
Location	Wellington
Contact Name	4RF Limited
Contact Details	support@4rf.com
IP Address	173.10.1.20
Subnet Mask	255.255.0.0
Gateway	0.0.0.0
Date and Time	21/04/2014 13:31

Operating Summary

Operating Mode	Point To Point (Bridge Mode)
Interface Mode	Serial and Ethernet
Modem Mode	Mode A (ETSI / ACMA)
TX Frequency (MHz)	400
TX Power (dBm)	37
RX Frequency (MHz)	400
Channel Size (kHz)	12.5
Network ID (FAN)	CAFE
Node Address	0000
Inband Management	Enabled
Inband Management Timeout (s)	10

Main Window Frame

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 Control Bar



The control bar is used for:

Position	Function
Left	Local Provides full configuration and supervision of the local radio Remote Provides full configuration and supervision of the remote radio Link Provides configuration and supervision of the common local and remote radio parameters
Right	The access level logged into SuperVisor. This label also doubles as the SuperVisor logout button.

SuperVisor Alarm Bar

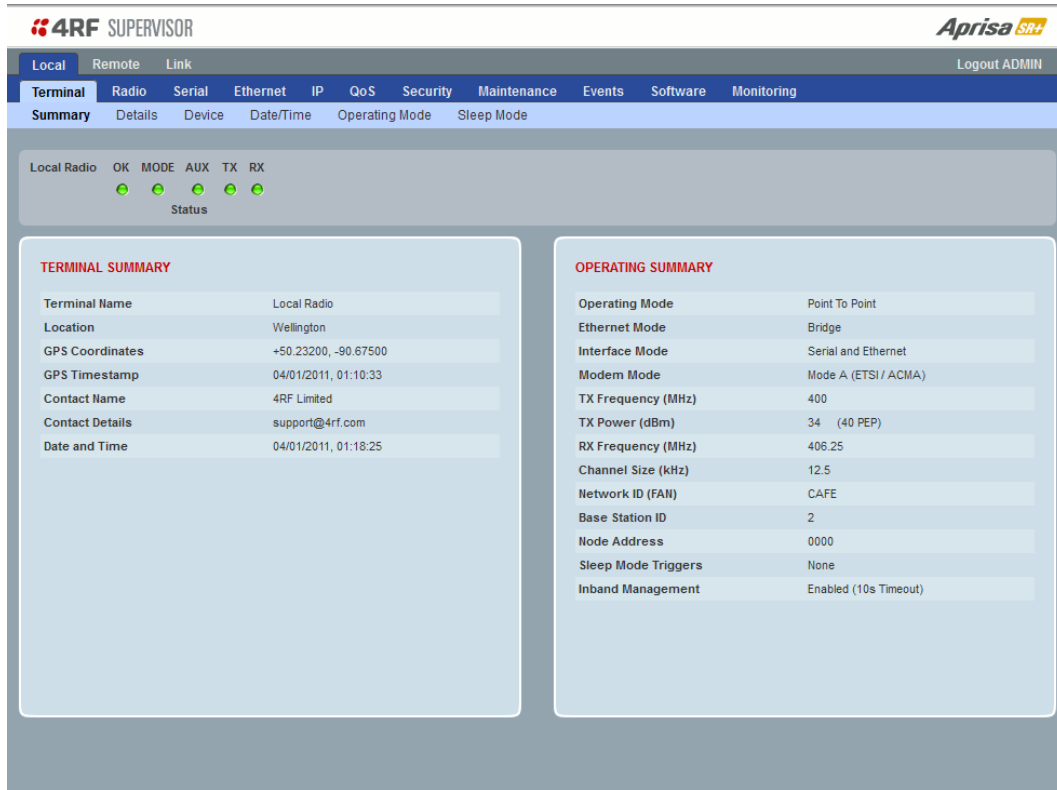


The alarm bar displays the radio name and alarms of the local radio i.e. the radio that SuperVisor is logged into on the left and the remote radio name and alarms on the right.

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

Terminal > Summary

The following is the SuperVisor Terminal Summary opening screen for a standard Point-To-Point radio:



The screenshot displays the 4RF SUPERVISOR web interface. At the top, there is a navigation bar with tabs for Local, Remote, and Link. Below this is a menu bar with options: Terminal, Radio, Serial, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring. The 'Terminal' tab is selected, and the 'Summary' sub-tab is active. The interface shows the status of a 'Local Radio' with indicators for OK, MODE, AUX, TX, and RX, all of which are green. The main content area is divided into two sections: 'TERMINAL SUMMARY' and 'OPERATING SUMMARY'.

TERMINAL SUMMARY	
Terminal Name	Local Radio
Location	Wellington
GPS Coordinates	+50.23200, -90.67500
GPS Timestamp	04/01/2011, 01:10:33
Contact Name	4RF Limited
Contact Details	support@4rf.com
Date and Time	04/01/2011, 01:18:25

OPERATING SUMMARY	
Operating Mode	Point To Point
Ethernet Mode	Bridge
Interface Mode	Serial and Ethernet
Modem Mode	Mode A (ETSI / ACMA)
TX Frequency (MHz)	400
TX Power (dBm)	34 (40 PEP)
RX Frequency (MHz)	406.25
Channel Size (kHz)	12.5
Network ID (FAN)	CAFE
Base Station ID	2
Node Address	0000
Sleep Mode Triggers	None
Inband Management	Enabled (10s Timeout)

Link > Details > Summary

The following is the SuperVisor Link Details screen for a standard Point-To-Point radio:

4RF SUPERVISOR

Aprisa SR+

Local Remote Link

Logout ADMIN

Details Configuration Monitoring

Summary Radio Events

Local Radio OK MODE AUX TX RX

Status

Remote Radio OK MODE AUX TX RX

Status

TERMINAL SUMMARY

Terminal Name	Local Radio
Location	Wellington
GPS Coordinates	+50.23200, -90.67500
GPS Timestamp	04/01/2011, 01:10:33
Contact Name	4RF Limited
Contact Details	support@4rf.com
IP Address	172.10.1.20
Subnet Mask	255.255.0.0
Gateway	0.0.0.0
Date and Time	04/01/2011, 02:41:38

OPERATING SUMMARY

Operating Mode	Point To Point
Ethernet Mode	Bridge
Interface Mode	Serial and Ethernet
Modem Mode	Mode A (ETSI / ACMA)
TX Frequency (MHz)	400
TX Power (dBm)	34 (40 PEP)
RX Frequency (MHz)	406.25
Channel Size (kHz)	12.5
Network ID (FAN)	CAFE
Base Station ID	2
Node Address	0000
Sleep Mode Triggers	None
Inband Management	Enabled
Inband Management Timeout (s)	10

TERMINAL SUMMARY

Terminal Name	Remote Radio
Location	Wellington
GPS Coordinates	+50.23200, -90.81200
GPS Timestamp	07/01/2011, 05:11:19
Contact Name	4RF Limited
Contact Details	support@4rf.com
IP Address	172.10.1.17
Subnet Mask	255.255.0.0
Gateway	0.0.0.0
Date and Time	07/01/2011, 05:11:36

OPERATING SUMMARY

Operating Mode	Point To Point
Ethernet Mode	Bridge
Interface Mode	Serial and Ethernet
Modem Mode	Mode A (ETSI / ACMA)
TX Frequency (MHz)	406.25
TX Power (dBm)	34 (40 PEP)
RX Frequency (MHz)	400
Channel Size (kHz)	12.5
Network ID (FAN)	CAFE
Base Station ID	2
Node Address	0000
Inband Management	Enabled
Inband Management Timeout (s)	10

Protected Station

The Aprisa SR+ Protected Station is fully monitored hot-standby and fully hot-swappable product providing radio and user interface protection for Aprisa SR+ radios. The RF ports and interface ports from the active radio are switched to the standby radio if there is a failure in the active radio.

Version 1 Protected Station

The version 1 Protected Station has two variants for operating input voltage; 10.5 -30 VDC negative earth (Std) and 18-60 VDC floating (48VDC).



Option Examples

Part Number	Part Description
APSQ-R400-SSC-HD-22-ENAA	4RF SR+, PS, 400-470 MHz, SSC, Half Duplex, 2E2S, EN, STD
APSQ-R400-SSC-HD-22-ENAB	4RF SR+, PS, 400-470 MHz, SSC, Half Duplex, 2E2S, EN, 48VDC

Version 2 Protected Station

As of August 2023, 4RF has a new version of the Aprisa SR+ Protected Stations. This version 2 Protected Station has an operating input voltage of 10-60 VDC floating.



Option Example

Part Number	Part Description
APSQ-R400-SSC-HD-22-ENAE	4RF SR+, PS, 400-470 MHz, SSC, Half Dup, 2E2S, EN, 10-60 VDC

The Aprisa SR+ Protected Station is comprised of an Aprisa SR+ Protection Switch and two standard Aprisa SR+ radios mounted in a 2U rack mounting chassis.

All interfaces (RF, data, etc.) are continually monitored on both the active and standby radio to ensure correct operation. The standby radio can be replaced without impacting traffic flow on the active radio.

The Aprisa SR+ radios can be any of the currently available Aprisa SR+ radio frequency bands, channel sizes or interface port options.

The Aprisa SR+ Protected Station can operate as a base station, repeater station or remote radio. The protection behaviour and switching criteria between the active and standby radios is identical for the three configurations.

By default, the Aprisa SR+ Protected Station is configured with the left-hand radio (A) designated as the primary radio and the right hand radio (B) designated as the secondary radio.

Each radio is configured with its own unique IP and MAC address and the address of the partner radio.

On power-up, the primary radio will assume the active role and the secondary radio will assume the standby role. If, for some reason, only one radio is powered on it will automatically assume the active role.

Both the Aprisa SR+ Protected Station primary radio and secondary radio must be operating on the same software version.

Protected Ports

The protected ports are located on the protected station front panel. Switching occurs between the active radio ports and the standby radio ports based on the switching criteria described below.

The protected ports include:

- Antenna ports ANT/TX and RX (if dual antenna ports used)
- Ethernet ports (depending on interface port option purchased)
- Serial ports (depending on interface port option purchased)

Operation

In hot-standby normal operation, the active radio carries all RS-232 serial and Ethernet traffic over the radio link and the standby radio transmit is on with its transmitter connected to an internal load. Both radios are continually monitored for correct operation including the transmitter and receiver and alarms are raised if an event occurs.

The active radio sends regular 'keep alive' messages to the standby radio to indicate it is operating correctly. In the event of a failure on the active radio, the RF link and user interface traffic is automatically switched to the standby radio.

The failed radio can then be replaced in the field without interrupting user traffic.

Switch Over

The switch-over to the standby radio can be initiated automatically, on fault detection, or manually via the Hardware Manual Lock switch on the Protection Switch or the Software Manual Lock from SuperVisor.

Additionally, it is possible to switch over the radios remotely without visiting the station site, via the remote control connector on the front of the Protection Switch.

On detection of an alarm fault the switchover time is less than 0.5 seconds. Some alarms may take up to 30 seconds to be detected depending on the configuration options selected.

The Protection Switch has a switch guard mechanism to prevent protection switch oscillation. If a switchover 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 switchover. It is also possible to prevent an alarm event triggering a switchover 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 280).

PA current	
Tx reverse power	Tx AGC
Temperature threshold	Thermal shutdown
RSSI Threshold	RX Synthesizer Not Locked
Rx CRC errors	RF no receive data
Port 1 Eth no receive data	Port 2 Eth no receive data
Port 1 Eth data receive errors	Port 2 Eth data receive errors
Port 1 Eth data transmit errors	Port 2 Eth data transmit errors
Port 3 Eth no receive data	Port 4 Eth no receive data
Port 3 Eth data receive errors	Port 4 Eth data receive errors
Port 3 Eth data transmit errors	Port 4 Eth data transmit errors
Port 1 Serial Data No RX Data	Port 2 Serial Data RX Data
Port 1 Serial Data RX Errors	Port 2 Serial Data RX Errors
USB Port Serial Data No RX Data	USB Port Serial Data RX Errors
Component failure	Calibration failure
Configuration not supported	Protection Hardware Failure
Alarm Input 1	Alarm Input 2

It will not attempt to switch-over to a standby radio which has power failure.

It will also not switch over to a standby radio with an active alarm event which has been configured as a 'blocking criteria'.

Switch-over will be initiated once either of these conditions is rectified, i.e. power is restored, or the alarm is cleared.

Monitored Alarms

The following alarms are monitored by default on the active / standby radio. The monitored alarms are dependent on the Protection Type selected.

Protection Type	All Protection Types	Redundant	Monitored Hot Standby	
Alarm Type	Monitored on Active Radio	Monitored on Standby Radio	Monitored on Standby Radio TX	Monitored on Standby Radio RX
PA Current	☒		☒	
PA Driver Current	☒		☒	
PA Stability	☒		☒	
TX AGC	☒			
TX Forward Power	☒		☒	
TX Reverse Power	☒		☒	
Temperature Threshold	☒	☒	☒	☒
TX Synthesizer Not Locked	☒		☒	
Thermal Shutdown	☒			
RSSI Threshold	☒			☒
RX Synthesizer Not Locked	☒			☒
RX CRC Errors	☒			☒
RF No Receive Data	☒			☒
Port1 ETH No Receive Data	☒			
Port1 ETH Data Receive Errors	☒			
Port1 ETH Data Transmit Errors	☒			
Port2 ETH No Receive Data	☒			
Port2 ETH Data Receive Errors	☒			
Port2 ETH Data Transmit Errors	☒			
Port3 ETH No Receive Data	☒			
Port3 ETH Data Receive Errors	☒			
Port3 ETH Data Transmit Errors	☒			
Port4 ETH No Receive Data	☒			
Port4 ETH Data Receive Errors	☒			
Port4 ETH Data Transmit Errors	☒			
Port1 Serial Data No RX Data	☒			
Port1 Serial Data RX Errors	☒			
Port2 Serial Data No RX Data	☒			
Port2 Serial Data RX Errors	☒			
USB Port Serial Data No RX Data	☒			
USB Port Serial Data No RX Errors	☒			
Component Failure	☒	☒	☒	☒
Protection SW Manual Lock	☒			
Protection HW Manual Lock	☒			
Modem FEC Disable	☒			

Protection Type	All Protection Types	Redundant	Monitored Hot Standby	
Alarm Type	Monitored on Active Radio	Monitored on Standby Radio	Monitored on Standby Radio TX	Monitored on Standby Radio RX
Modem ACM Lock	☒			
Alarm Input 1	☒	☒	☒	☒
Alarm Input 2	☒	☒	☒	☒
Protection Peer Comms Lost	☒			
Protection Hardware Failure	☒			
VDC Power Supply	☒	☒	☒	☒
3.3 Volts Power Supply	☒	☒	☒	☒
5.0 Volts Power Supply	☒	☒	☒	☒
7.2 Volts Power Supply	☒			
15.0 Volts Power Supply	☒	☒	☒	☒

Configuration Management

The Primary and Secondary radios are managed with the embedded web-based management tool, SuperVisor, by using either the Primary or Secondary IP address. Configuration changes in one of the radios will automatically be reflected in the partner radio.

To ensure all remote radios are registered to the correct (active) base station, changes to the Network Table are automatically synchronized from the active radio to the standby radio. The Network Table is only visible on the active radio. This synchronization does not occur if the Hardware Manual Lock is active.

Hardware Manual Lock

The Hardware Manual Lock switch on the Protection Switch provides a manual override of the active / standby radio.

When this lock is activated, the selected radio (A or B) becomes the active radio regardless of the Software Manual Lock and the current switching or block criteria.

When the lock is deactivated (set to the Auto position), the protection will become automatic and switching will be governed by normal switching and blocking criteria.



The state of the switch is indicated by the three LEDs on the Protection Switch:

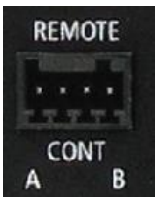
A LED	B LED	Locked LED	State
Green	Off	Off	Auto - Radio A is active
Off	Green	Off	Auto - Radio B is active
Green	Off	Orange	Manual Lock to radio A
Off	Green	Orange	Manual Lock to radio B

The Protection Switch also has a Software Manual Lock. The Hardware Manual Lock takes precedence over Software Manual Lock if both diagnostic functions are activated i.e. if the Software Manual Lock is set to ‘Primary’ and the Hardware Manual Lock set to ‘Secondary’, the system will set the Secondary radio to Active.

When a Hardware Manual Lock is deactivated (set to the Auto position), the Software Manual Lock is re-evaluated, and locks set appropriately.

Remote Control

The switch-over to the standby radio can be initiated via the Remote Control Phoenix 1963447 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 457).

L2 / L3 Protection Operation

The Aprisa SR+ Protected Station has selectable L2 Bridge or L3 Router modes, with VLAN, QoS and L2/3/4 address filtering attributes. Each Radio is configured with its own unique IP and MAC address and partner radio address. On switch-over failure, the new active radio sends out a gratuitous ARP to update the MAC learning tables / ARP tables of the upstream bridge / router for the appropriate traffic flow.

Hot-Swappable

The two Aprisa SR+ radios are mounted on a pull-out tray to making it possible to replace a failed radio without interrupting user traffic (Version 2 Protected Station shown).



Antenna and Duplexer Options

Option 1 - single antenna without a duplexer

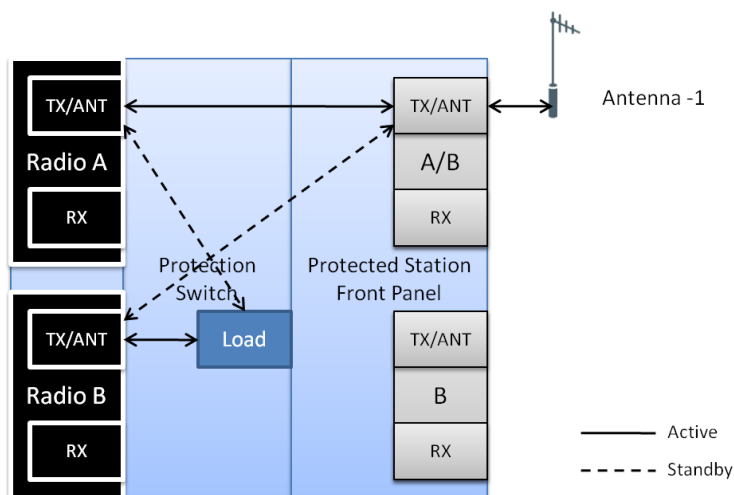
In this configuration, a single antenna is used and connected directly to the Aprisa SR+ Protected Station TX/ANT (A/B side) TNC port on the front panel. In this option Protected Station can operate in:

- Half duplex RF operation only

If single frequency used, standby radio TX is OFF/Mute (as RX/TX on same connector).

If dual frequency used, standby radio TX is ON, transmit to internal load for fault monitoring.

Only the active radio receives the signal (single RX path) from the antenna.



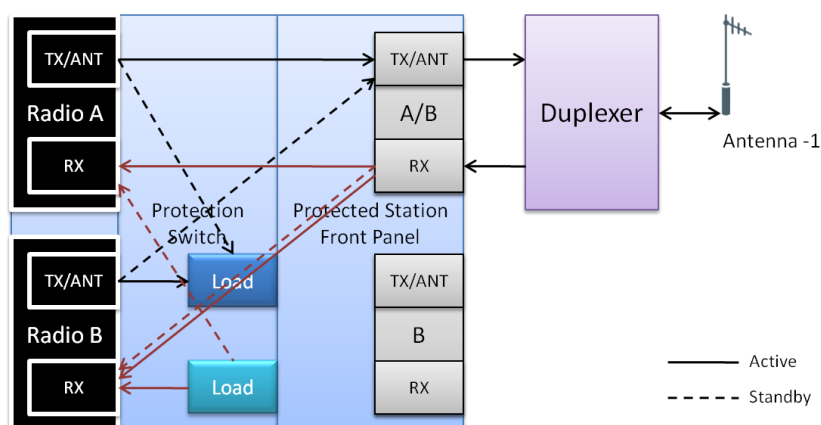
Option 2 - single antenna with a single duplexer

In this configuration, a single antenna is used with a duplexer which is connected to the Aprisa SR+ Protected Station TX/ANT and RX (A/B side) TNC ports on the front panel. In this option, the Protected Station can operate in:

- Half or full duplex RF operation
- Only dual frequency supported, where standby radio TX is ON, transmits to internal load for fault monitoring

When the 'Protection Type' is set to 'monitored hot standby' (Terminal > Operating Mode), the standby radio RX/TX can be fault monitored. This mode has a 4 dB loss in RX sensitivity.

When the 'Protection Type' is set to 'redundant', the standby radio RX/TX will not be fault monitored. This mode has 1 dB loss in RX sensitivity.



Option 3 - dual antenna without a duplexer

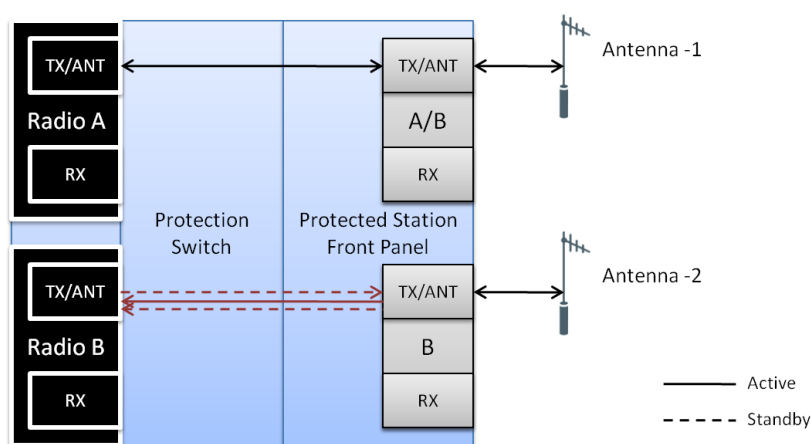
In this configuration, antenna redundancy is supported with dual antennas connected to the Aprisa SR+ Protected Station TX/ANT (A/B side) and TX/ANT (B side) TNC ports on the front panel. In this option, the Protected Station can operate in:

- Half duplex RF operation only

If single frequency used, standby radio RX (TX is off) can't be monitored as it will receive the active TX.

If dual frequency used, and the 'Protection Type' is set to 'monitored hot standby' (Terminal > Operating Mode), the standby radio RX/TX can be fault monitored. This mode has a 1 dB loss in RX sensitivity.

If dual frequency used, and the 'Protection Type' is set to 'redundant', the standby radio RX/TX will not be fault monitored.



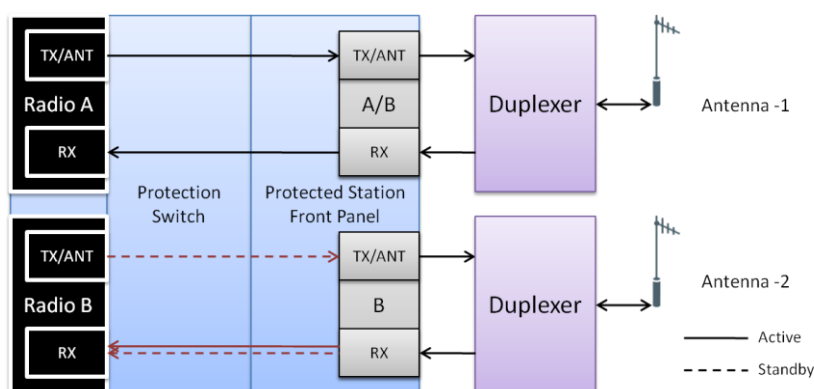
Option 4 - dual antenna with dual duplexers

In this configuration, antenna redundancy is supported with dual antennas connected via dual duplexers to the Aprisa SR+ Protected Station TX/ANT and RX (A/B side) TNC ports and TX/ANT and RX (B side) TNC ports on the front panel. In this option, the Protected Station can operate in:

- Half or full duplex RF operation
- Only dual frequency

When the 'Protection Type' is set to 'monitored hot standby' (Terminal > Operating Mode), the standby radio RX/TX can be fault monitored. This mode has a 1 dB loss in RX sensitivity.

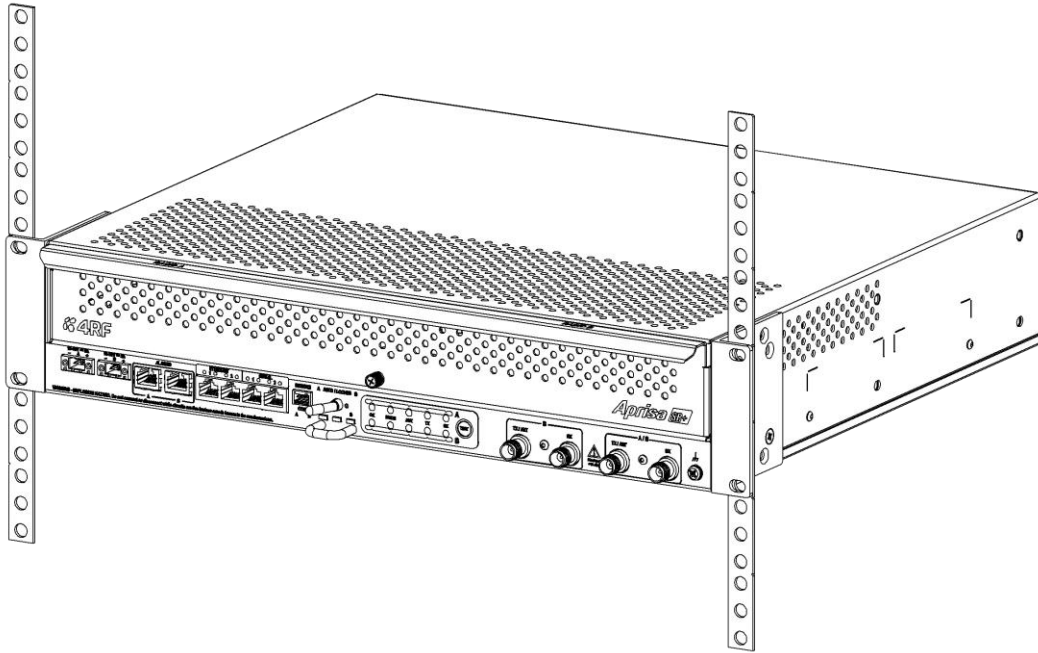
When the 'Protection Type' is set to 'redundant', the standby radio RX/TX will not be fault monitored.



Installation

Mounting

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



Cabling

The Aprisa SR+ Protected Station is delivered pre-cabled with power, interface, management and RF cables. There are two options for the pre-cabled Protected Station (see ‘Antenna and Duplexer Options’):

1. Standard Protected Station- suitable for options #1 and #2 (single antenna operation)

Part Number	Part Description
APSQ-R400-SSC-HD-22-ENAA	4RF SR+, PS, 400-470 MHz, SSC, Half Duplex, 2E2S, EN, STD

2. Dual Antenna Protected Station- suitable for options #3 and #4 (dual antenna operation)

Part Number	Part Description
APSQ-R400-SSC-HD-22-ENDA	4RF SR+, PS, 400-470 MHz, SSC, Half Duplex, 2E2S, EN, Dual Ant

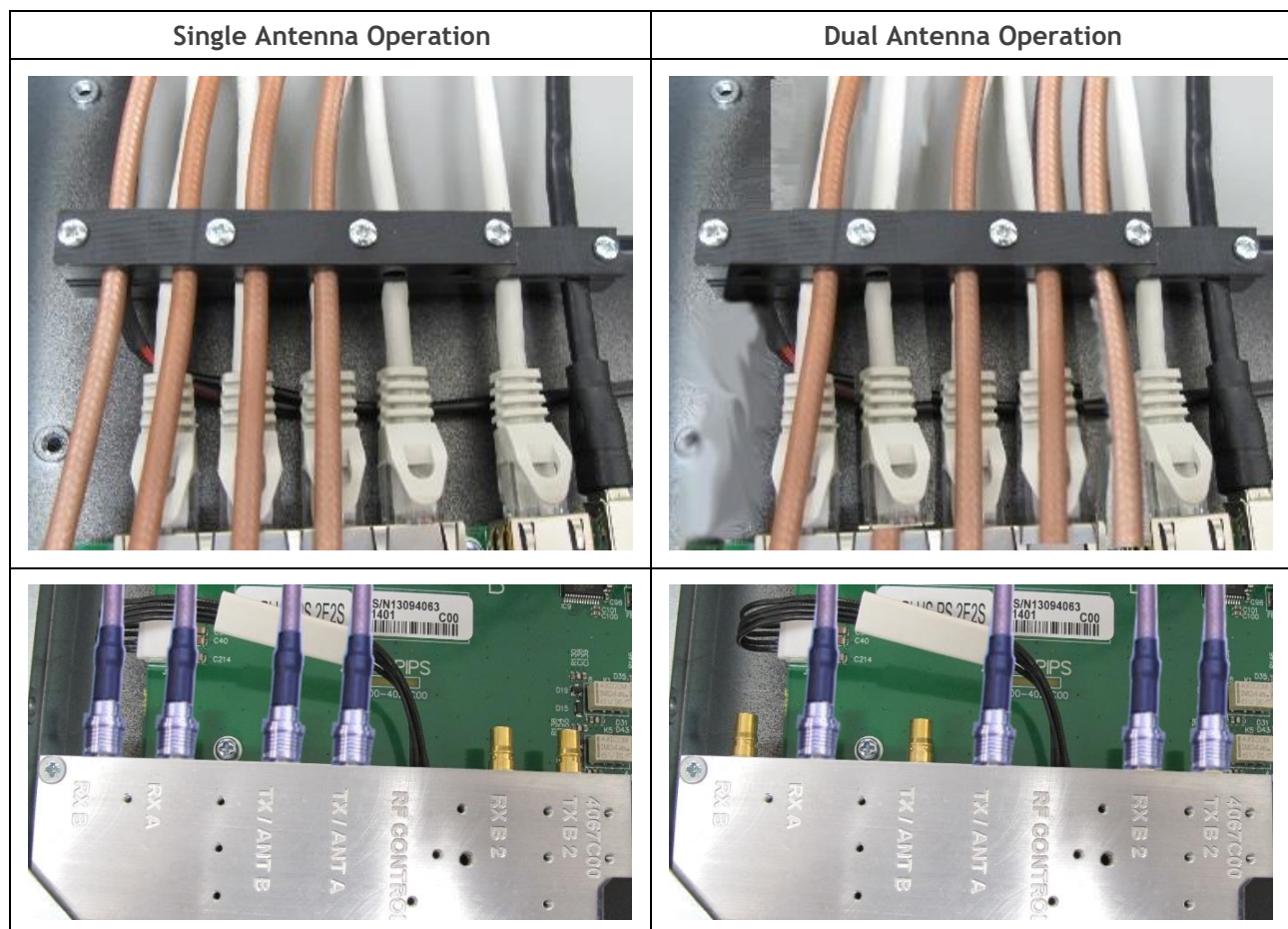
Each option (per ordered part number) is pre-cable configured as the following:

Protected Station Wiring	Internal pre-cabled Protected Station wiring setting	
	Radio / TNC Port	RF Switch Port
Standard Protected Station (single antenna operation)	Radio A TX/ANT	TX/ANTA
	Radio A RX	RXA
	Radio B TX/ANT	TX/ANTB
	Radio B RX	RXB
Dual Antenna Protected Station (dual antenna operation)	Radio A TX/ANT	TX/ANTA
	Radio A RX	RXA
	Radio B TX/ANT	TXB2
	Radio B RX	RXB2

Users can change an existing Protected Station from one option to the other option by following the procedure:

To change a pre-cabled Protected Station from one option to the other option:

1. Disconnect the power supply, antenna/s, interface cables and any other connections
2. Remove the Protected Station shelf from the rack
3. Turn the Protected Station shelf upside down
4. Remove the securing screws and remove the bottom panel
5. Unscrew the four coaxial cable clamp screws
6. Swap the two cables and position them in the appropriate connector ports
7. Refit the coaxial cable clamp and tighten the four clamp screws
8. Refit the bottom panel and tighten the two screws
9. Replace the shelf in the rack



Power

The external power source must be connected to both the A and B Molex 2 pin male power connectors located on the protected station front panel. The A power input powers the A radio and the B power input powers the B radio.

The protection switch is powered from the A power input or the B power input (whichever is available).

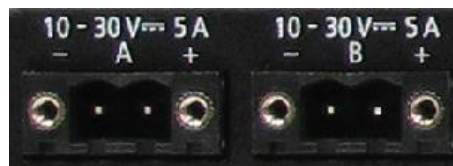
The maximum combined power consumption is 42 Watts for 10 W transmit peak power.

Version 1 Protected Stations

The version 1 Aprisa SR+ Protected station has two DC power options, nominal 12 VDC and 48 VDC.

12 VDC

The 12 VDC nominal external power source can operate over the voltage range of +10.5 to +30 V DC (negative earth).

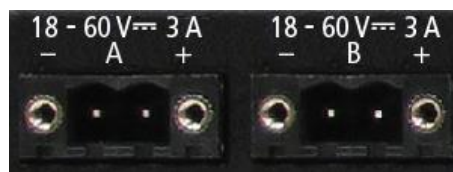


An example of the 12 VDC option part number is:

Part Number	Part Description
APSQ-R400-SSC-HD-22-ENAA	4RF SR+, PS, 400-470 MHz, SSC, Half Dup, 2E2S, EN, STD

48 VDC

The 48 VDC nominal external power source can operate over the voltage range of 18 to 60 V DC (floating).



An example of the 48 VDC option part number is:

Part Number	Part Description
APSQ-R400-SSC-HD-22-ENAB	4RF SR+, PS, 400-470 MHz, SSC, Half Dup, 2E2S, EN, 18-60 VDC

Version 2 Protected Stations

The version 2 Aprisa SR+ Protected station has one DC power option which operates over the voltage range of 10 to 60 VDC floating.



An example of the 10-60 VDC option part number is:

Part Number	Part Description
APSQ-R400-SSC-HD-22-ENAE	4RF SR+, PS, 400-470 MHz, SSC, Half Dup, 2E2S, EN, 10-60 VDC

Alarms

The protection switch provides access to both the A radio and B radio Alarm Interfaces (see ‘Alarm Interface Connections’ on page 455 for the connector pinout).



Maintenance

Changing the Protected Station IP Addresses

To change the IP address of a Protected Station radio:

1. Change the IP address of either or both the Primary Radio and Secondary radio (see 'Protected Station: IP > IP Setup' on page 355). Changes in these parameters are automatically changed in the partner radio.

Creating a Protected Station

When a Protected Station is ordered from 4RF, it will be delivered complete with radios installed, pre-cabled and pre-configured for Redundant operation. The following process will not be required.

This process is to create a protected station from two individual SR+ radios and a new spare Aprisa SR+ Protection Switch. It assumes that the SR+ radios are currently set up for non-protected operation.

1. Set the protection type and partner IP address of the SR+ radio A with SuperVisor 'Terminal > Operating Mode'. Set this radio Protection Unit to primary.
2. Set the protection type and partner IP address of the secondary SR+ radio B with SuperVisor Terminal > Operating Mode'. Set this radio Protection Unit to secondary.
3. Switch off the radios and place the two radios in the new spare Aprisa SR+ Protection Switch.
4. Ensuring that the cables are not crossed over, plug in the interface port cables, the Alarm and Protect port cables and the power connector to both the radios. Secure the power connectors with the two screws.
5. Power on the Protected Station.
6. Connect to either one of the radios via SuperVisor. This will start up SuperVisor in Single Session Management mode.
7. The user can now configure the Protected Station as required.

Replacing a Protected Station Faulty Radio

Replacing a faulty radio in a Protected Station can be achieved without disruption to traffic.

Assuming that the primary radio is active, and the secondary radio is faulty and needs replacement:

1. Ensure the replacement radio has the same version of software installed as the primary radio. If necessary, upgrade the software in the replacement radio.
2. Set the Protection Switch MAC address (see 'Protected Station: Maintenance > Advanced' on page 369). This MAC address is present on the 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 116).
5. Set the Hardware Manual Lock switch to make the primary radio active.
6. Unplug the interface port cables, the Alarm and Protect port cables and the power connector from the faulty radio being replaced. The two screws securing the power connector will need to be undone.
7. Carefully remove the faulty radio from the protection switch.
8. Install the replacement radio into the protection switch.
9. Ensuring that the cables are not crossed over, plug in the interface port cables, the Alarm and Protect port cables and the power connector to the replacement radio. Secure the power connector with the two screws.
10. Power on the replacement radio and wait for it to become standby.
11. Set the Hardware Manual Lock switch to the Auto position.

Replacing a Faulty Power Supply

Replacing one of the power supplies can be achieved without disruption to traffic.

If a power supply has failed, the associated radio will have failed which will have caused the protection switch to switch-over to the other radio. It will not have switched back unless the power was restored and another problem occurred which caused a switch-over.

1. If the A power supply is faulty, ensure that the B radio is active (whether it be the primary or secondary radio).
If the B power supply is faulty, ensure that the A radio is active (whether it be the primary or secondary radio).
2. Replace the faulty power supply.

Replacing a Faulty Protection Switch

Note: Replacing a faulty Protection Switch will disrupt traffic.

Move the radios, the interface cables and the power cables to the replacement Protection Switch.

On both Protected Station radios:

1. Power on the radio and wait for it to become ready.
2. Using SuperVisor > Maintenance > Advanced, enter the Protection Switch MAC address shown on the Protection Switch label (see 'Protected Station: Maintenance > Advanced' on page 369).
3. Using SuperVisor > Maintenance > Advanced, Decommission the node (see 'Decommission Node' on page 277) and then Discover the Nodes (see 'Discover Nodes' on page 276).

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

The Aprisa SR+ Protected Station is now ready to operate.

Spares

The Aprisa SR+ Protection Switch is available as spare parts for the three radio interface port options and single and dual antenna options:

Version 1 Protected Station

Part Number	Part Description
APST-XPSW-X22-12-SA	4RF SR+ Spare, Protection Switch, 2E2S, 10-30VDC, Single Ant
APST-XPSW-X22-12-DA	4RF SR+ Spare, Protection Switch, 2E2S, 10-30VDC, Dual Ant
APST-XPSW-X22-48-SA	4RF SR+ Spare, Protection Switch, 2E2S, 18-60VDC, Single Ant
APST-XPSW-X22-48-DA	4RF SR+ Spare, Protection Switch, 2E2S, 18-60VDC, Dual Ant
APST-XPSW-X31-12-SA	4RF SR+ Spare, Protection Switch, 3E1S, 10-30VDC, Single Ant
APST-XPSW-X31-12-DA	4RF SR+ Spare, Protection Switch, 3E1S, 10-30VDC, Dual Ant
APST-XPSW-X31-48-SA	4RF SR+ Spare, Protection Switch, 3E1S, 18-60VDC, Single Ant
APST-XPSW-X31-48-DA	4RF SR+ Spare, Protection Switch, 3E1S, 18-60VDC, Dual Ant
APST-XPSW-X40-12-SA	4RF SR+ Spare, Protection Switch, 4E0S, 10-30VDC, Single Ant
APST-XPSW-X40-12-DA	4RF SR+ Spare, Protection Switch, 4E0S, 10-30VDC, Dual Ant
APST-XPSW-X40-48-SA	4RF SR+ Spare, Protection Switch, 4E0S, 18-60VDC, Single Ant
APST-XPSW-X40-48-DA	4RF SR+ Spare, Protection Switch, 4E0S, 18-60VDC, Dual Ant

Version 2 Protected Station

Part Number	Part Description
APGS-XPSW-X22-FR-SA	4RF Spare, Protection Switch, 2E2S, 10-60VDC, Single Ant
APGS-XPSW-X22-FR-DA	4RF Spare, Protection Switch, 2E2S, 10-60VDC, Dual Ant
APGS-XPSW-X31-FR-SA	4RF Spare, Protection Switch, 3E1S, 10-60VDC, Single Ant
APGS-XPSW-X31-FR-DA	4RF Spare, Protection Switch, 3E1S, 10-60VDC, Dual Ant
APGS-XPSW-X40-FR-SA	4RF Spare, Protection Switch, 4E0S, 10-60VDC, Single Ant
APGS-XPSW-X40-FR-DA	4RF Spare, Protection Switch, 4E0S, 10-60VDC, Dual Ant

Data Driven Protected Station

The Aprisa SR+ Data Driven Protected Station provides radio and RS-232 serial port user interface protection for Aprisa SR+ radios.



Example Part:

Part Number	Part Description
APSQ-D400-SSC-HD-22-ENAA	4RF SR+, PD, 400-470 MHz, SSC, Half Dup, 2E2S, EN, STD

The Aprisa SR+ Data Driven Protected Station shown is comprised of two standard Aprisa SR+ setup as ‘dual antenna port’, ‘half duplex’ radios and two external duplexers mounted on 19" rack mounting shelves.

The Aprisa SR+ radios can be any of the currently available Aprisa SR+ radio frequency band options.

By default, the Aprisa SR+ Data Driven Protected Station is configured with the left-hand radio (A) designated as the primary radio and the right hand radio (B) designated as the secondary radio.

Each radio is configured with its own unique IP and MAC address and the address of the partner radio.

On power-up, the primary radio will assume the active role and the secondary radio will assume the standby role. If, for some reason, only one radio is powered on it will automatically assume the active role.

Operation

The active radio is determined explicitly by which radio receives data on its RS-232 serial port input from the interface.

The active radio carries all RS-232 serial traffic over its radio link and the standby radio is unused with its transmitter turned off.

If data is received on the RS-232 serial port interface input of the standby radio, it will immediately become the active radio and the radio which was active will become the standby radio.

Over The Air Compatibility

If the Aprisa SR+ Data Driven Protected Station is to be used in a network of Aprisa SRx radios, the ‘SR Compatible’ option must be enabled (see ‘SR Compatible’ on page 117).

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 87) by using either the Primary or Secondary IP address. Configuration changes in one of the radios will automatically be reflected in the partner radio.

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

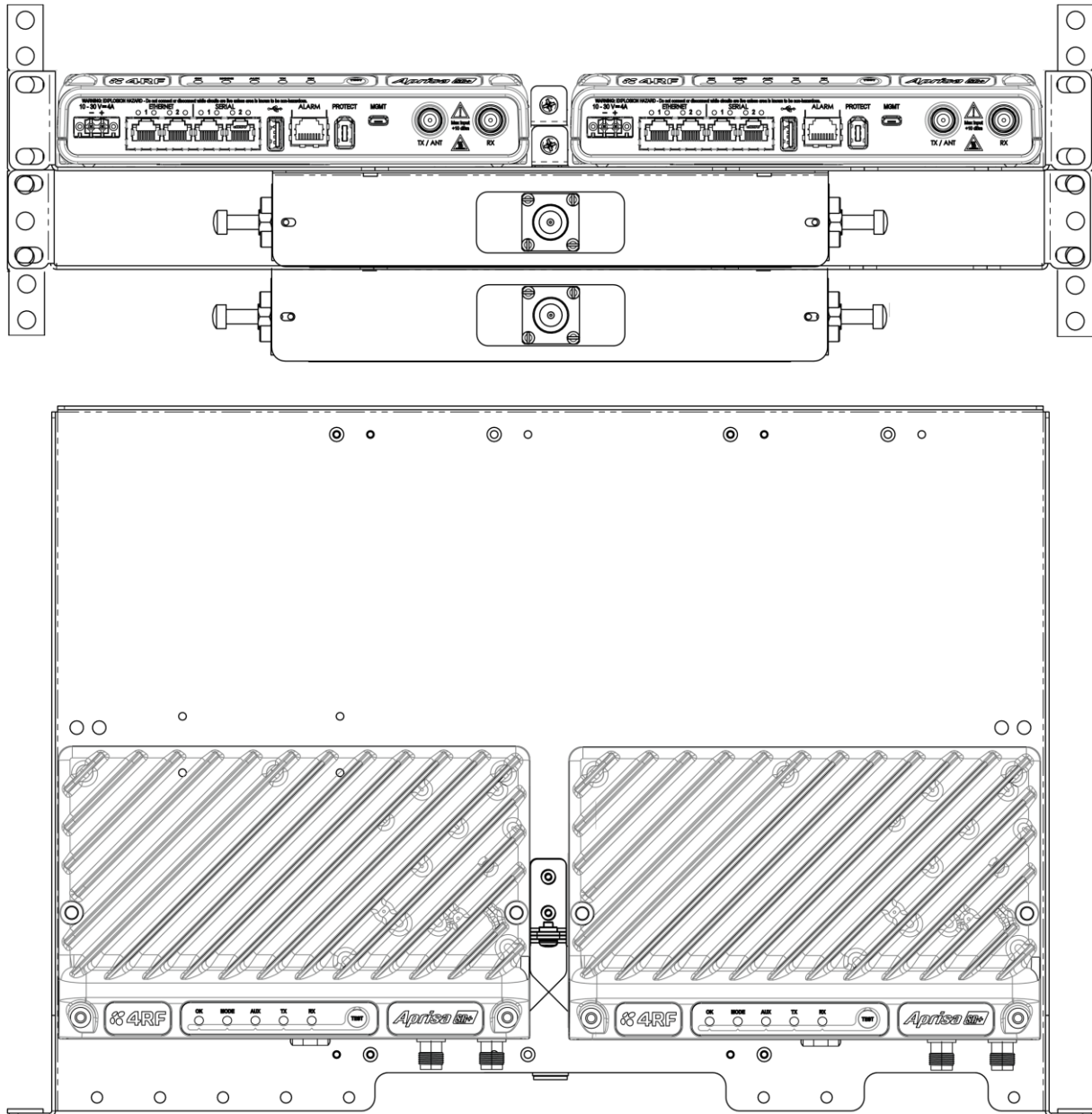
Power

A +10.5 to +30 V DC external power source must be connected to both the A and B Molex 2 pin male power connectors. The maximum combined power consumption is 42 Watts for 10 W transmit peak power.

Installation

Mounting

The Aprisa SR+ Data Driven Protected Station is designed to mount in a standard 19" rack on two 1U rack mounting shelves (total of 3RU).



Cabling

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

Duplexer Kits

The Aprisa SR+ product range contains Duplexer Kit accessories for use with Aprisa SR+ radios configured for Single Antenna Dual Port operation.

Radio Duplexer Kits



Example of part number: APSB-KDUP-400-B1-BR

Part Number	Description
APSB-KDUP-135-N0-BR	Aprisa SR+ Duplexer Kit for a Aprisa SR+ Radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x N0 Duplexer 135 MHz, s4.6 MHz, p0.5 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables
APSB-KDUP-320-A1-BR	Aprisa SR+ Duplexer Kit for a Aprisa SR+ radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x A1 Duplexer 300 MHz, s 5 MHz, p 0.5 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables
APSB-KDUP-400-B1-BR	Aprisa SR+ Duplexer Kit for a Aprisa SR+ Radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x B1 Duplexer 400 MHz, s 5 MHz, p 0.5 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables
APSB-KDUP-450-M0-BR	Aprisa SR+ Duplexer Kit for a Aprisa SR+ Radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x M0 Duplexer 450 MHz, s 5 MHz, p 0.5 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables
APSB-KDUP-450-P0-BR	Aprisa SR+ Duplexer Kit for a Aprisa SR+ Radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1 or 2 Aprisa SR+ radios and 1 duplexer 1x P0 Duplexer 450 MHz, s 3 MHz, p 0.5 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cab

Part Number	Description
APSB-KDUP-700-E0-BR	Aprisa SR+ Duplexer Kit for a Aprisa SR+ radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1 or 2 Aprisa SR+ radios and 1 duplexer 1x E0 Duplexer 700 MHz, min s 30 MHz, p 7.0 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables
APSB-KDUP-700-E0-BR-DR	Aprisa SR+ Duplexer Kit for a Aprisa SR+ radio containing: 1x DIN rail mounting bracket and duplexer plate W= 178 mm, D= 178 mm, H= 52 mm and screws to mount the duplexer 1x E0 Duplexer 700 MHz, min split 30 MHz, p 7.0 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables
APSB-KDUP-700-E1-BR-DR	Aprisa SR+ Duplexer Kit for a Aprisa SR+ radio containing: 1x DIN rail mounting bracket and duplexer plate W= 178 mm, D= 178 mm, H= 52 mm and screws to mount the duplexer 1x E1 Duplexer 700 MHz, min split 30 MHz, p 1.0 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables
APSB-KDUP-700-E1-BR-DRTF	Aprisa SR+ Duplexer Kit for a Aprisa SR+ radio containing: 1x DIN rail mounting bracket and duplexer plate W= 178 mm, D= 178 mm, H= 52 mm and screws to mount the duplexer 1x E1 Duplexer 700 MHz, min split 30 MHz, p 1.0 MHz, TNC female antenna connector 2x TNC to SMA right angle 640mm cables
APSB-KDUP-928-G0-BR	Aprisa SR+ Duplexer Kit for a Aprisa SR+ radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x G0 Duplexer 900 MHz, s 40 MHz, p 7 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables
APSB-KDUP-928-G2-BR-MM	Aprisa SR+ Duplexer Kit for a Aprisa SR+ radio containing: 1x 1U 19" rack mid mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x G2 Duplexer 900 MHz, s 9 MHz, p 1 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables
APSB-KDUP-928-G2-BR	Aprisa SR+ Duplexer Kit for a Aprisa SR+ radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x G2 Duplexer 900 MHz, s 9 MHz, p 1 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables
APSB-KDUP-928-G3-BR	Aprisa SR+ Duplexer Kit for a Aprisa SR+ radio containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x G3 Duplexer 900 MHz, s5.5 MHz, p0.5 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables

Part Number	Description
APSB-KDUP-928-G3-BR-MM	Aprisa SR+ Duplexer Kit for a Aprisa SR+ radio containing: 1x 1U 19" rack mid mount shelf with duplexer mounting brackets and screws to mount 1x SR+ radio and 1x duplexer 1x G3 Duplexer 900 MHz, s5.5 MHz, p0.5 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables

Protected Station Duplexer Kits



Example of part number: APSB-KDUP-928-G2-PS

Part Number	Description
APSB-KDUP-135-N0-PS	Aprisa SR+ Duplexer Kit for a Aprisa SR+ Protected Station containing: 1x N0 Duplexer 135 MHz, s4.6 MHz, p0.5 MHz, N type female antenna connector 2x right angle TNC to SMA right angle 640mm cables Rack front mounted
APSB-KDUP-135-N0-PS-DA	Aprisa SR+ Duplexer Kit for a dual antenna Aprisa SR+ Protected Station containing: 2x N0 Duplexer 135 MHz, s4.6 MHz, p0.5 MHz, N type female antenna connector 4x right angle TNC to SMA right angle 640mm cables Rack front mounted
APSB-KDUP-320-A1-PS	Aprisa SR+ Duplexer Kit for a Aprisa SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x A1 Duplexer 300 MHz, s 5 MHz, p 0.5 MHz, N type female antenna connector 2x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-320-A1-PS-DA	Aprisa SR+ Duplexer Kit for a dual antenna Aprisa SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 2x A1 Duplexer 300 MHz, s 5 MHz, p 0.5 MHz, N type female antenna connector 4x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-400-B1-PS-DA	Aprisa SR+ Duplexer Kit for a dual antenna Aprisa SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 2x B1 Duplexers 400 MHz, s 5 MHz, p 0.5 MHz, N type female antenna connector 4x right angle TNC to SMA right angle 640mm cables

Part Number	Description
APSB-KDUP-400-B1-PS	Aprisa SR+ Duplexer Kit for a Aprisa SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x B1 Duplexer 400 MHz, s 5 MHz, p 0.5 MHz, N type female antenna connector 2x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-450-M0-PS	Aprisa SR+ Duplexer Kit for a Aprisa SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x M0 Duplexer 450 MHz, s 5 MHz, p 0.5 MHz, N type female antenna connector 2x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-450-M0-PS-DA	Aprisa SR+ Duplexer Kit for a dual antenna Aprisa SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 2x M0 Duplexer 450 MHz, s 5 MHz, p 0.5 MHz, N type female antenna connector 4x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-450-P0-PS	Aprisa SR+ Duplexer Kit for a Aprisa SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x P0 Duplexer 450 MHz, s 3 MHz, p 0.5 MHz, N type female antenna connector 2x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-450-P0-PS-DA	Aprisa SR+ Duplexer Kit for a dual antenna Aprisa SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 2x P0 Duplexer 450 MHz, s 3 MHz, p 0.5 MHz, N type female antenna connector 4x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-700-E0-PS	Aprisa SR+ Duplexer Kit for a Aprisa SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x E0 Duplexer 700 MHz, min split 30 MHz, p 7.0 MHz, N type female antenna connector 2x right angle TNC to SMA right angle 640mm cables
APSB-KDUP-700-E1-PS-SA	Aprisa SR+ Duplexer Kit for a single antenna SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x E1 duplexer 1x E1 Duplexer 700 MHz, min split 30 MHz, p 1.0 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables

Part Number	Description
APSB-KDUP-700-E1-PS-DA	Aprisa SR+ Duplexer Kit for a dual antenna SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 2x E1 duplexers 2x E1 Duplexers 700 MHz, min split 30 MHz, p 1.0 MHz, N type female antenna connector 4x TNC to SMA right angle 640mm cables
APSB-KDUP-700-E1-PS-SATF	Aprisa SR+ Duplexer Kit for a single antenna SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 1x E1 duplexer 1x E1 Duplexer 700 MHz, min split 30 MHz, p 1.0 MHz, TNC female antenna connector 2x TNC to SMA right angle 640mm cables
APSB-KDUP-700-E1-PS-DATF	Aprisa SR+ Duplexer Kit for a dual antenna SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws to mount 2x E1 duplexers 2x E1 Duplexers 700 MHz, min split 30 MHz, p 1.0 MHz, TNC female antenna connector 4x TNC to SMA right angle 640mm cables
APSB-KDUP-928-G0-PS	Aprisa SR+ Duplexer Kit for a Aprisa SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x G0 Duplexer 900 MHz, s 40 MHz, p 7 MHz, N type female antenna connector 2x TNC to SMA right angle 590mm cables
APSB-KDUP-928-G2-PS	Aprisa SR+ Duplexer Kit for a SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x G2 Duplexer 900 MHz, s 9 MHz, p 1 MHz, N type female antenna connector 2x TNC to SMA right angle 590mm cables
APSB-KDUP-928-G2-PS-MM	Aprisa SR+ Duplexer Kit for a SR+ Protected Station containing: 1x 1U 19" rack mid mount shelf with duplexer mounting brackets and screws 1x G2 Duplexer 900 MHz, s 9 MHz, p 1 MHz, N type female antenna connector 2x TNC to SMA right angle 590mm cables
APSB-KDUP-928-G3-PS-MM	Aprisa SR+ Duplexer Kit for a SR+ Protected Station containing: 1x 2U 19" rack mid mount shelf with duplexer mounting brackets and screws 1x G3 Duplexer 900 MHz, s5.5 MHz, p0.5 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables

Part Number	Description
APSB-KDUP-928-G3-PS	Aprisa SR+ Duplexer Kit for a SR+ Protected Station containing: 1x 2U 19" rack front mount shelf with duplexer mounting brackets and screws 1x G3 Duplexer 900 MHz, s5.5 MHz, p0.5 MHz, N type female antenna connector 2x TNC to SMA right angle 640mm cables
APSB-KDUP-928-G6-PS	Aprisa SR+ Duplexer Kit for a SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x G6 Duplexer 900 MHz, min s 28 MHz, p 1.0 MHz, N type female antenna connector 2x TNC to SMA right angle 590mm cables

Protected Station with Duplexer Kit

This product option combines the Aprisa SR+ Protected Station and a Duplexer Kit in one part number (Version 2 Protected Station shown).



Option Example for 700 MHz:

Part Number	Part Description
APSQ-F700-KE0-HD-22-ENAB	4RF SR+, PS+D, 757-788 MHz, E0 Kit, Half Dup, 2E2S, EN, 48VDC

This part includes:

APSQ-R700-SSC-HD-22-ENAB	Aprisa SR+ Protected Station, half duplex RF option 2 Ethernet ports and 2 Serial ports Software Selectable Channel Sizes of 25 kHz, 50 kHz and 100 kHz FCC Part 27 Single antenna operation 18 - 60 VDC floating input power
APSB-KDUP-700-E0-PS	Aprisa SR+ Duplexer Kit for a Aprisa SR+ Protected Station containing: 1x 1U 19" rack front mount shelf with duplexer mounting brackets and screws 1x E0 Duplexer 700 MHz, min split 30 MHz, p 7.0 MHz, N type female antenna connector 2x right angle TNC to SMA right angle 640mm cables

USB RS-232 / RS-485 Serial Port

The Aprisa SR+ USB host port is predominantly used for software upgrade and diagnostic reporting. However, it can also be used to provide an additional RS-232 DCE or RS-485 serial port for customer traffic.

This is accomplished with a USB to RS-232 / RS-485 serial converter cable. This plugs into the USB host port  and can be terminated with the required customer connector.

This additional RS-232 / RS-485 serial port is enabled with the SuperVisor mode setting in Serial Port Settings (see 'Serial > Port Setup' on page 150).

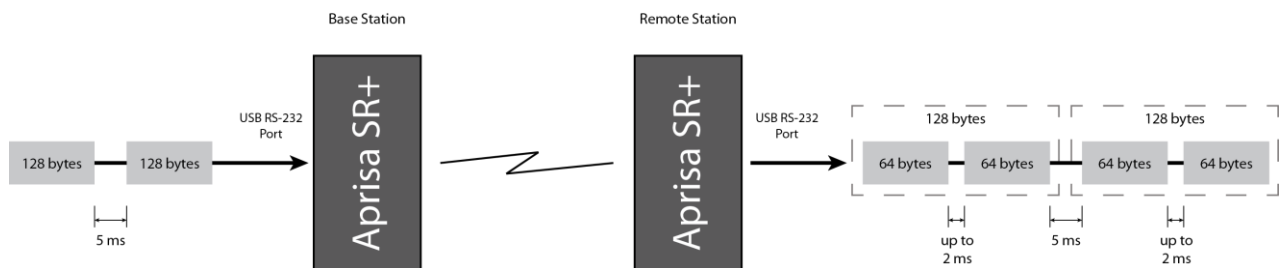
The Aprisa SR+ USB port has driver support for these USB serial converters. Other USB serial converters may not operate correctly.

USB RS-232 / RS-485 operation

The USB serial converter buffers the received data frames into 64 byte blocks separated by a small inter-frame gap.

For the majority of applications, this fragmentation of egress frames is not an issue. However, there are some applications that may be sensitive to the inter-frame gap, therefore, these applications need consideration.

A 5 ms inter-frame is recommended for the applications that are sensitive to inter-frame gap timings.



On a USB RS-232 port, Modbus RTU can operate up to 9600 bit/s with all packet sizes and up to 115200 bit/s if the packet size is less than 64 bytes. The standard RS-232 port is fully compatible with Modbus RTU at all baud rates.

USB RS-232 Cabling Options

The following converter cables are available as Aprisa SR+ accessories to provide the customer interface. The kit contains a USB connector retention clip (see 'USB Retention Clip' on page 440).

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

Part Number	Part Description
APSB-KFCA-USB-23-MS-18	4RF SR+ Acc, Kit, Interface, USB Conv, RS-232, Multi-strand, 1.8m



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

Part Number	Part Description
APSB-KFCA-USB-23-45-MF18	4RF SR+ Acc, Kit, Interface, USB Conv, RS-232, RJ45, Female, 1.8m

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

Part Number	Part Description
APSB-KFCA-USB-23-D9-MF18	4RF SR+ Acc, Kit, Interface, USB Conv, RS-232, DB9, Female, 1.8m

USB RS-485 Cabling Options

The following converter cable is available as an Aprisa SR+ accessory to provide the customer interface RS-485 2 wire. The kit contains a USB connector retention clip (see 'USB Retention Clip' on page 440).

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

Part Number	Part Description
APSB-KFCA-USB-48-MS-18	4RF SR+ Acc, Kit, Interface, USB Conv, RS-485, Multi-strand, 1.8m



USB Retention Clip

The USB Retention Clip attaches to the underside of the Aprisa SR+ enclosure adjacent to the USB connector.



To attach the USB Retention Clip:

1. Clean the enclosure surface where the retention clip will attach with an alcohol based cleaner e.g. Isopropanol.
2. Peel off the retention clip protective backing.
3. Stick the clip onto the Aprisa SR+ enclosure ensuring that it aligns to the middle of the radio USB connector.

10. Maintenance

Spare Fuses

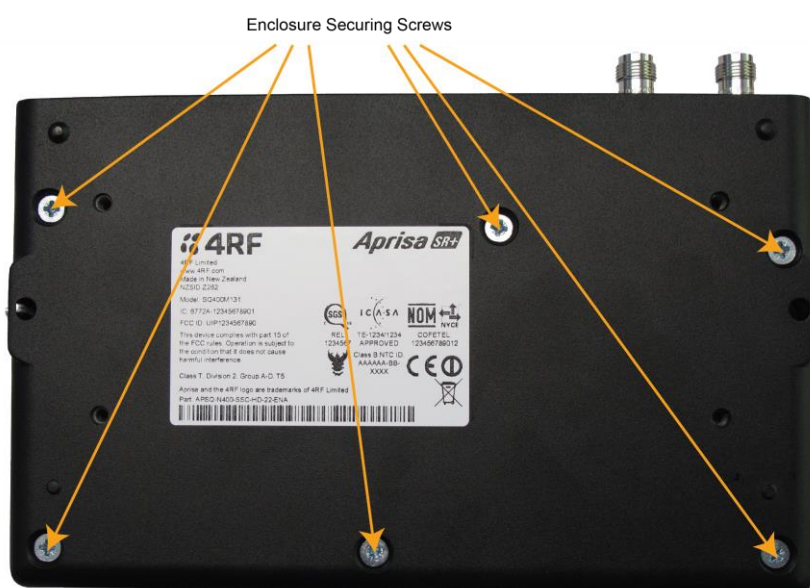
Radio Spare Fuses

The Aprisa SR+ radio PBA contains two fuses in the power input with designators F1 and F2. Both the positive and negative power connections are fused. The fuse type is a Littelfuse 0454007 NANO Slo-Blo 7 A.

Two spare fuses are located inside the enclosure.

To replace the fuses:

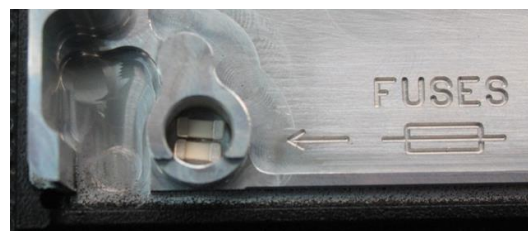
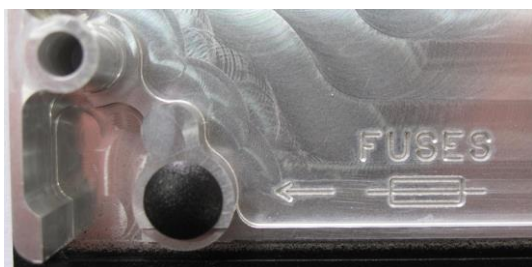
1. Remove the input power and antenna cable.
2. Unscrew the enclosure securing screws (posi 2).



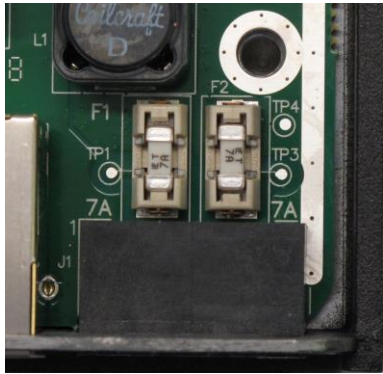
2. Separate the enclosure halves.

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 0.8 Nm. The regulatory compliance of the radio may be affected if the screws are not tightened correctly.

Additional Spare Fuses

Additional spare fuses can be ordered from 4RF:

Part Number	Part Description
APGS-FNAN-454-07-02	4RF Spare, Fuse, Nano SMF, 454 Series, 7A, 2 items
APGS-FNAN-454-07-10	4RF Spare, Fuse, Nano SMF, 454 Series, 7A, 10 items
APGS-FNAN-454-07-50	4RF Spare, Fuse, Nano SMF, 454 Series, 7A, 50 items

The Aprisa SR+ Protected Station contains two fuses in the power inputs to the Protection Switch. If the protected station power supplies are connected and operating but the radios are not operating, it may be that a power supply input fuse is blown. Spare fuses are located on the Protection Switch board.

1. Disconnect the power supply, antenna/s, interface cables and any other connections.
2. Remove the Protected Station shelf from the rack.
3. Turn the Protected Station shelf upside down.
4. Remove the rear securing screws and remove the bottom panel.
5. Locate the spare fuses.

6. Determine which fuse is blown and replace it with the spare.

7. Refit the bottom panel and tighten the two screws.
8. Replace the shelf in the rack and re-connect all the cables.

No User-Serviceable Components

Apart from changing the fuses, 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.

Do not remove the internal RF section shield as this could void the compliance and will void the product warranty.

Return all faulty radios to 4RF or an authorized service centre.

For more information on maintenance and training, please contact 4RF Customer Services at support@4rf.com.

CAUTION: Electro Static Discharge (ESD) can damage or destroy the sensitive electrical components in the radio.

Software Upgrade

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

Network Software Upgrade

This process allows customers to upgrade their Aprisa SR+ network from the central base station location without need for visiting remote sites.

The Software Pack is loaded into the base station with the file transfer process (see 'Software > File Transfer' on page 295) and distributed via the radio link to all remote radios.

When all remote radios receive the Software Pack version, the software can be remotely activated on all remote radios.

Non-Protected Network Upgrade Process

This upgrade process is for upgrading the software on an entire Aprisa SR+ network from a non-protected base station. If there are protected remotes in the network, they must be locked to the current active radio.

To upgrade the entire Aprisa SR+ network software:

1. Using File Transfer, load the software pack into the base station (see 'Software > File Transfer' on page 295). The software can be transferred to the radio via an FTP transfer or from a USB flash drive.

The Aprisa SR+ network file transfer operation is indicated in base station and remote radios by a flashing orange AUX LED.

2. Distribute the software to the entire network of remote radios (see 'Software > Remote Distribution' on page 303). Note that the distribution process over the air will take some time, depending on RF and Transfer rate settings.

The Aprisa SR+ network software distribution operation is indicated in base station and remote radios by a flashing orange MODE LED.

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

The impact of software distribution traffic upon customer traffic is controlled by two settings. The traffic uses the 'Default Management Data Priority' QoS setting, and the rate of packets at this priority is controlled with the 'Background Bulk Data Transfer Rate' setting in Radio > Channel Setup.

3. Activate the software on the entire network of remote radios (see 'Software > Remote Activation' on page 305).

Note: When the new software activates on the remote radios, all link communication from the base station to the remote will be lost. The base station will attempt to re-establish connectivity to the remote radios for the new version verification but this will fail. However, when the new software activates on the remote radios, the remote radio will reboot automatically and link communication will restore when the base station software is activated.

When the Remote Activation process gets to the 'Remote Radios On New Version' step, don't wait for this to complete but proceed to step 4.

4. Activate the software on the base station radio (see 'Software > Manager' on page 299).

5. When the new software has been activated, remote radios will re-register with the base station. The remote radios software version can be verified, with 'Network Status > Network Table' on page 333.
6. When the base station restarts with the new software, rediscover the nodes (see 'Discover Nodes' on page 276).
7. Check that all remote radios are now running on the new software (see 'Network Status > Network Table' on page 333).

Note: The following steps will only be necessary if for some reason steps 1-7 did not operate correctly or if software activation is attempted before the distribution process ends or the remote radio was off during steps 1-7 and turns on later. Thus, the following steps will most likely not be required.

8. If step 7 shows that not all remote radios are running the latest software version, restore the base station to the previous software version (see 'Software > Manager' on page 299).
9. Attempt to re-establish connectivity to the remote radios that have failed to upgrade by navigating to and remotely managing the remote radios individually.
10. Navigate to the remote radio history log and review the logs to determine the reason for the failure to activate the new software version.
11. Take appropriate actions to address the reported issue. If connectivity restores with the failed remotes, repeat steps 2-7 if required.

Protected Network Upgrade Process

This upgrade process is for upgrading the software on an entire Aprisa SR+ network from a protected base station. This software upgrade can be achieved without disruption to traffic.

Transferring the new software to the radios

The software can be transferred to the radio via an FTP transfer, HTTP transfer or from a USB flash drive.

1. Using the Hardware Manual Lock switch (see 'Hardware Manual Lock' on page 414), or the Software Manual Lock (see 'Lock Active To' on page 364), force the secondary radio to active
2. Using File Transfer, load the software pack into the secondary radio (see 'Protected Station: Software > Secondary File Transfer' on page 380).
3. Confirm that the transfer is successful (see 'Protected Station: Software > Manager' on page 383).
4. Using the Hardware Manual Lock switch (see 'Hardware Manual Lock' on page 414), or the Software Manual Lock (see 'Lock Active To' on page 364), force the primary radio to active.
5. Using File Transfer, load the software pack into the primary radio (see 'Protected Station: Software > Primary File Transfer' on page 377).
6. Confirm that the transfer is successful (see 'Protected Station: Software > Manager' on page 383).
7. Distribute the software to the entire network of remote radios (see 'Protected Station: Software > Remote Distribution' on page 385). If there are protected remotes in the network, they must be locked to the current active radio.

Note that the distribution process over the air will take some time, depending on RF and Transfer rate settings.

Activating the new software on the radios

1. Activate the software on the entire network of remote radios (see 'Protected Station: Software > Remote Activation' on page 388).
2. Monitor the progress of the activation process until the stage where activation of all remote radios has been confirmed.

When the new software has been activated, remote radios will re-register with the base station. The remote radios software version can be verified with 'Network Status > Network Table' on page 333.

3. If the new software version is not over the air compatible with the version currently operating on the radio, there is no need to wait as all link communication from the base station to the remote will be lost so the verification of the new version on the remote radio will fail.
4. Activate the new version software pack of the secondary radio (see 'Protected Station: Software > Manager' on page 383).
5. Immediately after that, activate the new version software pack of the primary radio (see 'Protected Station: Software > Manager' on page 383).

Note that the activation process will take a few minutes.

Confirm that the new software version is now running on the radios

1. Re-login into the Protection Station and navigate to SuperVisor > Software>Summary.
2. Confirm that the Primary and Secondary radio current software version is now up to date
3. Confirm that the list of remote radios are now running the latest software version with 'Network Status > Network Table' on page 333.
4. When the upgrade process is complete, if the Hardware Manual Lock switch has been used, set it to the Auto position. The software manual lock will release automatically.

Single Radio Software Upgrade

This upgrade process is for upgrading the software on a single Aprisa SR+ radio.

Note: If a radio has been configured for a Protection Type of ‘Redundant’, and that radio is no longer part of a Protected Station, the Protection Type must be changed to ‘None’ before the radio software upgrade can be achieved.

File Transfer Method

The Software Pack is loaded into the radio with the file transfer process (see ‘Software > File Transfer’ on page 295) and activated (see ‘Software > Manager’ on page 299).

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. Insert the USB flash drive into the host port .
3. Using File Transfer, load the software pack into the radio (see ‘Software > File Transfer’ on page 295).
4. Remove the USB flash drive from the host port .
5. Activate the software on the radio (see ‘Software > Manager’ on page 299).

USB Boot Upgrade Method

A single Aprisa SR+ radio can also be upgraded simply by plugging a USB flash drive containing the new software into the USB A host port  on the Aprisa SR+ front panel and power cycling the radio.

To upgrade the Aprisa SR+ radio software:

1. Unzip the software release files in to the root directory of a USB flash drive.
2. Check that the SuperVisor USB Boot Upgrade setting is set to 'Load and Activate' (see 'Software > Setup' on page 294) if you require the new software to load and automatically activate following the radio power cycle on step 7.
3. Power off the Aprisa SR+ and insert the USB flash drive into the host port .
4. Power on the Aprisa SR+.
5. The software upgrade process is complete when the OK LED flashes green. This can take about 2 minutes.

The software will have loaded in to the radio current software version.

6. Remove the USB flash drive from the host port .
7. Power cycle the Aprisa SR.

Login to the radio being upgraded and go to SuperVisor 'Software > Manager' on page 299.

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

If the upgrade process did not start, the Aprisa SR+ could already be operating on the version of software on the USB flash drive. This will be indicated by flashing OK LED and then the OK, MODE and AUX will light steady green.

If the radio is not operating on the new software (after the power cycle), it could be caused by the SuperVisor 'USB Boot Upgrade' setting set to 'Load Only' (see 'Software > Setup' on page 294).

In this case, go to SuperVisor see 'Software > Manager' on page 299 and tick the Software Pack 'Activate' checkbox and click 'Apply'.

If any Display Panel LED flashes red or is steady red during the upgrade process, it indicates that the upgrade has failed. This could be caused by incorrect files on the USB flash drive or a radio hardware failure.

Software Downgrade

Radio software can also be downgraded if required. This may be required if a new radio is purchased for an existing network which is operating on an earlier software release.

The downgrade process is the same as the upgrade process.

Protected Station Software Upgrade

This upgrade process is for upgrading the software on a single Aprisa SR+ Protected Station.

USB Boot Upgrade Method

Assuming the Primary radio is active and the Secondary radio is standby

1. Using the Hardware Manual Lock switch, force the primary radio to active.
2. Insert the USB flash drive with the new software release into the secondary radio host port .
3. Power cycle the secondary radio. The radio will be upgraded with the new software.
4. When the secondary radio upgrade is completed, remove the USB flash drive, power cycle the secondary radio and wait for it to become standby.
5. Using the Hardware Manual Lock switch, force the secondary radio to active.
6. Insert the USB flash drive with the new software release into the primary radio host port .
7. Power cycle the primary radio. The radio will be upgraded with the new software.
8. When the primary radio upgrade is completed, remove the USB flash drive, power cycle the primary radio and wait for it to become standby.
9. When the upgrade process is complete, set the Hardware Manual Lock switch to the Auto position. The secondary radio will remain active and the primary radio will remain standby. To set the primary radio to active, use the hardware lock switch to select the primary radio and wait for it to become active, then set the hardware manual lock switch to the Auto position.

Routine Maintenance

Power Supply Check

Check that power supply is within limits;

Radio	Protected Station		
12 VDC Nominal	Version 1 Protected Station (12 VDC)	Version 1 Protected Station (48 VDC)	Version 2 Protected Station
+10 to +30 VDC	+10.5 to +30 VDC	18 to 60 VDC	10 to 60 VDC

Temperature Test

Check the transmitter temperature (see Monitoring > Radio 'Transmitter Current Temperature' on page 320). The normal operating range is 0 to 70 °C.

Connections

Check that all connections including earthing, interfaces and RF connectors are secure.

Antenna and Feeder System

Check the VSWR and compare the measurement to the commissioning values (see Monitoring > Radio 'Transmitter Last TX Packet VSWR' on page 320). This value will be dependent on the feeder and antenna performance, a value of <1.5:1 shows acceptable performance.

Check the reverse power and compare the measurement to the commissioning values (see Monitoring > Radio 'Transmitter Last TX Packet Reverse Power' on page 320). The value will be dependent on the impedance presented to that antenna port of the radio by the feeder and antenna system. A reflected power of 15 dB below the transmit power shows an acceptable performance.

Transmit Power

Check the transmitter output power (see Monitoring > Radio 'Transmitter Last TX Packet Forward Power' on page 320). This value will be dependent on the output power setting, the ATPC setting, the temperature and the VSWR of the antenna.

The actual average transmit power can be measured by using a spectrum analyser with average power measurement capability. Connect the radio antenna output to the spectrum analyser input via an attenuator of at least 30 dB.

Transmit Frequency

Check the base station radio transmit frequency according to your routine maintenance schedule. It is recommended that this be done within two years of installation.

Aprisa SR+ software release 1.9.0 and later contain CLI commands to adjust the transmit frequency if necessary.

This procedure requires a frequency counter with an accuracy of 0.1 ppm or better. Do not attempt this adjustment without a counter of this stability.

Transmit Frequency CLI Adjustment Procedure:

1. Establish CLI connection to the radio see 'Command Line Interface' on page 392.
2. Turn on CW mode:

```
>> set testmodeTxCW 1
```
3. Measure the transmit frequency using a frequency counter connected to the radio antenna output via an attenuator of at least 30 dB.
4. Turn off CW mode:

```
>> set testmodeTxCW 2
```

Note: The transmission may cease if the Test mode timeout value is less than the time to measure the frequency. Increase the Test mode timeout value if necessary.
5. Calculate the frequency adjustment required in hertz.
6. Set the calibration adjustment in the format;
 'x' for a positive adjustment e.g. '105' for +105 Hz
 '-x' for a negative adjustment e.g. '-241' for -241 Hz.

```
>> freqtrack txcalibration set 'x'
```
7. Repeat process from step 2 if required to achieve an error of less than 40 Hz.

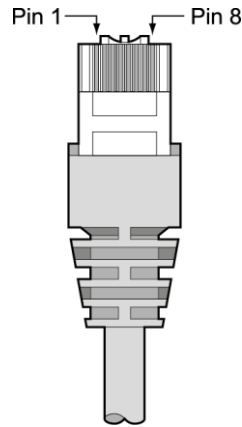
Transmit Spectrum

Check the transmit output spectrum with a spectrum analyser. Look for any visible intermodulation particularly in adjacent channels.

Note that adjacent channel power measurements require a laboratory grade spectrum analyser and cannot be performed with field instruments.

11. Interface Connections

RJ45 Connector Pin Assignments



RJ45 pin numbering

Ethernet Interface Connections

Pin Number	Pin Function	Direction	TIA-568A Wire Colour	TIA-568B Wire Colour
1	Transmit	Output	Green/white	Orange/white
2	Transmit	Output	Green	Orange
3	Receive	Input	Orange/white	Green/white
4	Not used		Blue	Blue
5	Not used		Blue/white	Blue/white
6	Receive	Input	Orange	Green
7	Not used		Brown/white	Brown/white
8	Not used		Brown	Brown

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

RJ45 connector LED indicators		
LED	Status	Explanation
Green	On	Ethernet signal received
Orange	Flashing	Data traffic present on the interface

Note: Do not connect Power over Ethernet (PoE) connections to the Aprisa SR+ Ethernet ports as this will damage the port.

RS-232 Serial Interface Connections

RS-232 Pinout

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

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

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

RS-232 Customer Cable Wiring

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

RS-232 Bit Oriented Mode Wiring

RS-232 Bit Oriented mode uses non-standard RS-232 wiring:

Aprisa BOP Interface - DCE			DTE Customer Interface		DCE Customer Interface	
RJ45 Pin Number	Pin Function	Direction	Pin Function	DB9 Male Pinout	Pin Function	DB9 Female Pinout
1 (*)	RTS	Input	TXD	3	RXD	2
2	DTR / Sleep Mode	Input	DTR / Sleep Mode	4	DSR / Sleep Mode	6
3 (*)	TXD	Input	TXD	3	RXD	2
4	Ground		Ground	5	Ground	5
5	DCD	Output	DCD	1		
6	RXD	Output	RXD	2	TXD	3
7	DSR	Output	DSR	6	DTR	4
8	CTS	Output	CTS	8	RTS	7

(*) In RS-232 Bit Oriented mode, pins 1 and 3 of the RJ45 connector must be wired together.

RS-232 RJ45 LED Indicators

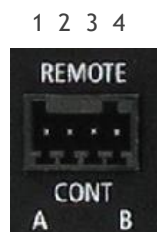
LED	Status	Explanation
Green	On	RS-232 device connected
Orange	Flashing	Data present on the interface

Alarm Interface Connections

RJ45 Pin Number	Pin Function	Direction	TIA-568A Wire Colour	TIA-568B Wire Colour
1	Alarm 1 Input / sleep control	Input	Green / white	Orange/white
2	Ground		Green	Orange
3	Alarm 2 Input	Input	Orange / white	Green/white
4	Ground		Blue	Blue
5	Alarm 1 Output	Output	Blue / white	Blue/white
6	Ground		Orange	Green
7	Alarm 2 Output	Output	Brown / white	Brown/white
8	Ground		Brown	Brown

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

Protection Switch Remote Control Connections



Pin Number	1	2	3	4
Function	Ground	A radio active	Ground	B radio active

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 280 for setup of alarm thresholds / sample durations etc.

Alarm Events

Transmit Path Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
1	PA Current	critical(1)	Threshold Type	Alarm to indicate that the current drawn by the transmitter power amplifier is outside defined limits.	Check antenna is not open or shorted, check duplexer correctly connected and tuned, if OK replace radio.
61	PA Driver Current	critical(1)	Threshold Type	Alarm to indicate that the current drawn by the transmitter power amplifier driver is outside defined limits.	Check antenna is not open or shorted, check duplexer correctly connected and tuned, if OK replace radio.
62	PA Stability	warning(4)	Threshold Type	Alarm to indicate that the power amplifier is oscillating which may cause corruption of the TX signal	Check antenna is not open or shorted, check duplexer correctly connected and tuned, if OK replace radio.
2	TX AGC	critical(1)	Threshold Type	Alarm to indicate that the variable gain control of the transmitter is outside defined limits.	Check antenna is not open or shorted, check duplexer correctly connected and tuned, if OK replace radio.
3	TX Reverse Power	warning(4)	Threshold Type	Alarm to indicate that the antenna is not connected to the radio	Check antenna is not open or shorted, check duplexer correctly connected and tuned, and confirm VSWR at TX port is less than 2:1. If OK replace radio.
60	TX Forward Power	warning(4)	Threshold Type	Alarm to indicate that the transmitter power is outside the selected TX power setting.	Check antenna is not open or shorted, check duplexer correctly connected and tuned, and confirm VSWR at TX port is less than 2:1. If OK replace radio.
4	Temperature Threshold	warning(4)	Threshold Type	Alarm to indicate that the transmitter temperature is outside defined limits.	Check ambient temperature and for airflow obstructions.
5	TX Synthesizer Not Locked	critical(1)	Threshold Type	Alarm to indicate that the transmitter synthesizer is not locked.	Power off radio and restart. If condition persists replace radio.
31	Thermal Shutdown	critical(1)	Threshold Type	Alarm to indicate that the transmitter has shutdown due to excessively high temperature.	Check ambient temperature and for airflow obstructions.
90	VSWR Threshold	warning(4)	Threshold Type	Alarm to indicate that there is a high SWR on the antenna port.	Check antenna is not open or shorted, check duplexer correctly connected and tuned.

Receive Path Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
7	RSSI Threshold	warning(4)	Threshold Type	Alarm to indicate that the receiver RSSI reading taken on the last packet received is outside defined limits.	Check antenna is not open or shorted. If the antenna is directional check for off-pointing.
88	SNR Threshold	warning(4)	Threshold Type	Alarm to indicate that the monitored SNR has exceeded its configured threshold limits	Check antenna is not open or shorted. If the antenna is directional check for off-pointing.
8	RX Synthesizer Not Locked	critical(1)	Not Configurable	Alarm to indicate that the receiver Synthesizer is not locked on the RF received signal.	Power off radio and restart. If condition persists replace radio.
9	RX CRC Errors	warning(4)	Error Ratio Type	Alarm to indicate that the data received on the RF path contains errors at a higher rate than the defined error rate threshold.	Check antenna is not open or shorted. Check duplexer is correctly tuned. If the antenna is directional check for off-pointing. Power off radio and restart. If condition persists replace radio.
87	Payload Decryption Failure	warning(4)	Sample Duration Type	Alarm to indicate that packets have been received over the air where the radio has failed to decrypt the content.	Check the event history log for more details. If the decryption failure is solely due to security setting mismatch, then the security settings of the radios involved needs to be checked and corrected. If the decryption failure is also possibly due to a security key mismatch, then this indicates that another unauthorized radio is attempting to connect to the radio network, or an authorized radio has got an invalid key that needs updating.

Radio Interface Path Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
34	RF No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that there is no data received on the RF path in the defined duration period.	Check base is operational. If new deployment check set-up, frequencies, and duplexer (if used). Check antenna is not open or shorted. If the antenna is directional check for off-pointing. Power off radio and restart. If condition persists replace radio.
86	RF Profile Manual Lock	warning(4)	Not Configurable	Alarm to indicate that the diagnostics function to lock the radio to a specific RF profile has been activated. This is only relevant when the radio has been configured with more than one RF profile.	No action required. This indicates that the diagnostic function is active.
129	Radio Self Test	minor(3)	Not Configurable	Alarm to indicate when the RF loopback self-test is not successful. This can occur due to a fault with antenna or feeder cable installation.	Check the antenna or feeder cable installation.

Modem Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
68	Modem FEC disable	warning(4)	Not Configurable	Alarm to indicate that FEC has been disabled. This could be a permanent event or a timed event.	Alarm to indicate that FEC has been disabled. This could be a permanent event or a timed event.
70	Modem ACM locked	warning(4)	Not Configurable	Alarm to indicate that the ACM has been locked to a fixed coding and modulation. This could be a permanent event or a timed event.	Alarm to indicate that the ACM has been locked to a fixed coding and modulation. This could be a permanent event or a timed event.

Customer Equipment Interface Path Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
10	Port 1 Eth No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that Ethernet port 1 has no received input signal in the defined duration period.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
11	Port 1 Eth Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 1 received input signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
12	Port 1 Eth Data Transmit Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 1 transmitted output signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
15	Port 1 Eth Port Down	critical(1)	Sample Duration Type	Alarm to indicate that Ethernet port 1 has no detected connection during the defined duration period.	Check the cable and connector. Check switch port or RTU is active. Check Ethernet Port speed/duplex configuration.
35	Port 2 Eth No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that Ethernet port 2 has no received input signal in the defined duration period.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
36	Port 2 Eth Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 2 received input signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
37	Port 2 Eth Data Transmit Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 2 transmitted output signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
38	Port 2 Eth Port Down	critical(1)	Sample Duration Type	Alarm to indicate that Ethernet port 2 has no detected connection during the defined duration period.	Check the cable and connector. Check switch port or RTU is active. Check Ethernet Port speed/duplex configuration.
44	Port 3 Eth No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that Ethernet port 3 has no received input signal in the defined duration period.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
45	Port 3 Eth Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 3 received input signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
46	Port 3 Eth Data Transmit Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 3 transmitted output signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
47	Port 3 Eth Port Down	critical(1)	Sample Duration Type	Alarm to indicate that Ethernet port 3 has no detected connection during the defined duration period.	Check the cable and connector. Check switch port or RTU is active. Check Ethernet Port speed/duplex configuration.
48	Port 4 Eth No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that Ethernet port 4 has no received input signal in the defined duration period.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
49	Port 4 Eth Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 4 received input signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
50	Port 4 Eth Data Transmit Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 4 transmitted output signal contains errors at a higher rate than the defined error rate threshold.	Check Ethernet cable and connector. Check switch port or RTU is active. Check IP and VLAN configuration.
51	Port 4 Eth Port Down	critical(1)	Sample Duration Type	Alarm to indicate that Ethernet port 4 has no detected connection during the defined duration period.	Check the cable and connector. Check switch port or RTU is active. Check Ethernet Port speed/duplex configuration.
13	Port 1 Serial Data No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that the RS-232 port 1 has no received input signal in the defined duration period.	Check serial ports settings, check serial cable and connector.
14	Port 1 Serial Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that the RS-232 port 1 received input signal contains errors at a higher rate than the defined error rate threshold.	Check serial ports settings, check serial cable and connector.
52	Port 2 Serial Data No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that the RS-232 port 2 has no received input signal in the defined duration period.	Check serial ports settings, check serial cable and connector.
53	Port 2 Serial Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that the RS-232 port 2 received input signal contains errors at a higher rate than the defined error rate threshold.	Check serial ports settings, check serial cable and connector.
63	USB Port Serial Data No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that the USB port has no received input signal in the defined duration period.	Check serial ports settings, check USB serial cable and adapter, check serial connector.
64	USB Port Serial Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that the USB port received input signal contains errors at a higher rate than the defined error rate threshold.	Check serial ports settings, check USB serial cable and adapter, check serial connector.

Component Failure Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
16	Component Failure	major(2)	Not Configurable	Alarm to indicate that a hardware component has failed.	Power off and restart radio. If fault persists replace radio.

Hardware Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
56	VDC Power Supply	warning(4)	Not Configurable	Alarm to indicate that the input power source is outside the operating limits of 10 to 30 VDC	Check DC connection to radio. Replace power supply.
57	3.3 Volts Power Supply	warning(4)	Not Configurable	Alarm to indicate that the 3.3 volt power rail is outside defined limits.	Power off and restart radio. If fault persists replace radio.
58	5.0 Volts Power Supply	warning(4)	Not Configurable	Alarm to indicate that the 5.0 volt power rail is outside defined limits.	Power off and restart radio. If fault persists replace radio.
59	7.2 Volts Power Supply	warning(4)	Not Configurable	Alarm to indicate that the 7.2 volt power rail is outside defined limits.	Power off and restart radio. If fault persists replace radio.
71	15 Volts Power Supply	warning(4)	Not Configurable	Alarm to indicate that the 15 volt power rail is outside defined limits.	Power off and restart radio. If fault persists replace radio.

Software Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
20	Calibration Failure	major(2)	Not Configurable	Alarm to indicate that the RF calibration has failed.	Power off and restart radio. If fault persists replace radio.
21	Configuration Not Supported	major(2)	Not Configurable	Alarm to indicate that a configuration has entered that is invalid.	Restore previous configuration, remove out of range or invalid parameters, updated software.
22	Remote Communications Lost	major(2)	Not Configurable	Alarm to indicate that a remote radio is not receiving packets from the base station.	Check RF configuration settings.
32	Network Configuration Warning	warning(4)	Not Configurable	Alarm to indicate a network configuration problem e.g. remote not registered.	Check for invalid parameters. Audit network settings.
73	Radio Network	warning(4)	Not Configurable	Alarm to indicate that there is an alarm in the radio network e.g. a remote radio has not registered or duplicate IP address.	Check for duplicate or invalid parameters. Audit network settings.
39	Software Restart Required	warning(4)	Not Configurable	Alarm to indicate that a configuration has changed that requires a software reboot.	Reboot radio.
74	Software Activation Pending	warning(4)	Not Configurable	Alarm to indicate that a software activation is about to occur. The activation can be on a software pack, configuration pack or security profile.	No action required. This is a warning to indicate that a type of software activation is about to happen. The information in the event history log will describe the type of activation

Hardware Alarm Input Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
24	Alarm Input 1	warning(4)	Not Configurable	Alarm to indicate that there is an active alarm on hardware alarm input 1	Action depends on nature of third-party alarm.
25	Alarm Input 2	warning(4)	Not Configurable	Alarm to indicate that there is an active alarm on hardware alarm input 2	Action depends on nature of third-party alarm.

Protected Station Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function	Recommended Actions
17	Protection Sw Manual Lock	warning(4)	Not Configurable	Alarm to indicate that the Protection Switch Software Manual Lock has been activated.	Information only.
18	Protection Hw Manual Lock	warning(4)	Not Configurable	Alarm to indicate that the Protection Switch Hardware Manual Lock has been activated.	Remember to unlock the Hardware Manual Lock for normal operation
23	Protection Peer Comms Lost	major(2)	Not Configurable	Alarm to indicate that the standby radio has lost communication with the active radio.	Check that the partner radio is powered on and the 'Protect' cable is plugged from the switch to both radios. Check that the radios have been setup for protected operation.
54	Protection Hardware Failure	major(2)	Not Configurable	Alarm to indicate that there is a failure in the protection switch hardware.	Check that the cables are connecting the switch to both radios. Check that the switch and both radios are the same Data interface port options e.g. 2E2S

Informational Events

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
26	User authentication succeeded	information(5)	Event to indicate that a user is successfully authenticated on the radio during login. The information on the user that was successfully authenticated is provided in the eventHistoryInfo object of the Event History Log.	Information No action required unless unexpected
27	User authentication failed	information(5)	Event to indicate that a user has failed to be authenticated on the radio during login. The information on the user that was unsuccessfully authenticated is provided in the eventHistoryInfo object of the Event History Log.	Check for possible intrusion attempt. If unexpected follow cyber incident report procedure.
28	Protection switch failed	information(5)	Event to indicate that a protection switch-over cannot occur for some reason. The reason for the failure to switch is described in the eventHistoryInfo object of the Event History Log.	Investigate reason for switch over and take remedial action.
29	Software System Check	information(5)	Event to indicate that the software has done a system check on the radio. Any information relevant to the cause of the event is provided in the eventHistoryInfo object of the Event History Log.	Information No action required unless unexpected
30	Software Start Up	information(5)	Event to indicate that the radio software has started. Any information relevant to the software start up is provided in the eventHistoryInfo object of the Event History Log.	Information No action required unless unexpected
33	Protection Switch Occurred	information(5)	Event to indicate that a protection switch-over occurs for some reason. The reason for the switch-over is described in the eventHistoryInfo object of the Event History Log.	Investigate reason for switch over and take remedial action.
41	File Transfer Activity	information(5)	Event to indicate that a data file is being transferred to or from the radio.	Information No action required unless unexpected
42	Software Management Activity	information(5)	Event to indicate that software is being distributed to remote radios.	Information No action required unless unexpected
43	Terminal Server TCP Activity	information(5)	Event to indicate TCP packets are being transferred from the terminal server.	Information No action required unless unexpected
55	Terminal Unit Information	information(5)	Event to indicate a miscellaneous activity occurring on the radio	Information no action required unless unexpected.
65	Event Action Activity	information(5)	Event to indicate an event action occurring on the radio	Information No action required unless unexpected
72	User SuperVisor Session Logout	information(5)	Event to indicate that a user has logged out or the user session has timed out	Information No action required unless unexpected

Event ID	Event Display Text	Default Severity	Function	Recommended Actions
75	Config Management Activity	information(5)	Event to indicate that there has been some management activity related to the configuration of the radio. As an example, the configuration of the radio has been changed via SNMP, or a new configuration script has been loaded into the radio. This event records: • When the change was made • The management interface that was used; SuperVisor, CLI or SNMP • The IP address and username of the person that made the change • The IP address of the destination radio • The category of the change as per SuperVisor menus e.g. Terminal parameters, Radio parameters	Information No action required unless unexpected
78	Security Information	information(5)	Security related events that occur on the radio. This may include events that report that a user account has been locked or recovered. Or events related to RADIUS authentication.	Refer to the event history logs for details of the events.
81	Date And Time Activity	information(5)	Events related to the date and time settings of the radio. This may include user changes to the date and time or SNTP related events.	Refer to the event history logs for details of the events.
85	GPS Activity	information(5)	Events related to GPS coordinates of the radio. This includes updates to the GPS coordinates of the radio	Refer to the event history logs for details of the events.
89	User Account Activity	information(5)	Events related to the management of User Accounts of the radio. This includes adding or deleting user accounts, or updates to existing accounts.	Refer to the event history logs for details of the events.

13. Specifications

RF Specifications

Blocking (desensitization), intermodulation, spurious response rejection, and adjacent channel selectivity values determined according to the methods introduced in V1.7.1 of ETSI standards EN 300 113.

Frequency Bands

ETSI Compliant

Broadcast Band	Frequency Band	Frequency Tuning Range	Synthesizer Step Size
VHF	135 MHz	135-175 MHz	0.625 kHz
VHF	220 MHz	215-240 MHz	0.625 kHz
UHF	320 MHz	320-400 MHz	6.250 kHz
UHF	400 MHz	400-470 MHz	1.250 kHz
UHF	450 MHz	450-520 MHz	6.250 kHz

FCC Compliant

Broadcast Band	Frequency Band	Frequency Tuning Range	Synthesizer Step Size
VHF	135 MHz	135-175 MHz	0.625 kHz
VHF	220 MHz	215-240 MHz	0.625 kHz
UHF	400 MHz	400-470 MHz	1.250 kHz
UHF	450 MHz	450-520 MHz	6.250 kHz
UHF	700 MHz	757-758 MHz and 787-788 MHz	6.250 kHz
UHF	896 MHz	896-902 MHz ^(Note 1)	6.250 kHz
UHF	928 MHz	928-960 MHz ^(Note 1)	6.250 kHz

ISED Compliant

Broadcast Band	Frequency Band	Frequency Tuning Range	Synthesizer Step Size
VHF	135 MHz	135-175 MHz	0.625 kHz
VHF	220 MHz	215-240 MHz	0.625 kHz
UHF	400 MHz	400-470 MHz	1.250 kHz
UHF	896 MHz	896-902 MHz ^(Note 1)	6.250 kHz
UHF	928 MHz	928-960 MHz ^(Note 1)	6.250 kHz

The Frequency Tuning Range is not an indication of the exact frequencies approved by FCC / ISED.

Note 1: The receive tuning range is specified. The transmit tuning range is 896 - 960 MHz.

Channel Sizes

ETSI Modem Mode

ETSI: 135 / 450 MHz Bands

No Forward Error Correction

Channel Size	Gross Radio Capacity				
	256 QAM ⁽²⁾	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	NA	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s	9.6 kbit/s
25 kHz	NA	120.0 kbit/s	80.0 kbit/s	40.0 kbit/s	19.2 kbit/s
50 kHz ⁽¹⁾	NA	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s	38.4 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	69.3 kbit/s	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s	8.4 kbit/s
25 kHz	138.6 kbit/s	103.9 kbit/s	46.2 kbit/s	23.1 kbit/s	16.7 kbit/s
50 kHz ⁽¹⁾	249.4 kbit/s	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s	33.4 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	NA	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s	4.1 kbit/s
25 kHz	NA	91.2 kbit/s	34.6 kbit/s	17.3 kbit/s	8.3 kbit/s
50 kHz ⁽¹⁾	NA	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s	16.5 kbit/s

Note 1: It is the responsibility of the user to check for country regulatory of 50 kHz availability in this frequency band.

Note 2: 256 QAM should be used with ACM

ETSI: 320 / 400 MHz Bands

No Forward Error Correction

Channel Size	Gross Radio Capacity				
	256 QAM ⁽²⁾	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	NA	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s	9.6 kbit/s
20 kHz	NA	84.0 kbit/s	56.0 kbit/s	28.0 kbit/s	9.6 kbit/s
25 kHz	NA	120.0 kbit/s	80.0 kbit/s	40.0 kbit/s	19.2 kbit/s
50 kHz ⁽¹⁾	NA	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s	38.4 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	69.3 kbit/s	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s	8.4 kbit/s
20 kHz	97.0 kbit/s	72.7 kbit/s	32.4 kbit/s	16.2 kbit/s	8.4 kbit/s
25 kHz	138.6 kbit/s	103.9 kbit/s	46.2 kbit/s	23.1 kbit/s	16.7 kbit/s
50 kHz ⁽¹⁾	249.4 kbit/s	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s	33.4 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	NA	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s	4.1 kbit/s
20 kHz	NA	63.8 kbit/s	24.2 kbit/s	12.1 kbit/s	4.1 kbit/s
25 kHz	NA	91.2 kbit/s	34.6 kbit/s	17.3 kbit/s	8.3 kbit/s
50 kHz ⁽¹⁾	NA	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s	16.5 kbit/s

Note 1: It is the responsibility of the user to check for country regulatory of 50 kHz availability in this frequency band.

Note 2: 256 QAM should be used with ACM

FCC Modem Mode

FCC: 135 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity				
FCC Part 90	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
15 kHz	NA	54.0 kbit/s	36.0 kbit/s	18.0 kbit/s	9.6 kbit/s
30 kHz	NA	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s	19.2 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
FCC Part 90	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
15 kHz	62.4 kbit/s	46.8 kbit/s	20.8 kbit/s	10.4 kbit/s	8.4 kbit/s
30 kHz	110.8 kbit/s	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s	16.7 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
FCC Part 90	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
15 kHz	NA	41.0 kbit/s	15.6 kbit/s	7.8 kbit/s	4.1 kbit/s
30 kHz	NA	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s	8.3 kbit/s

FCC: 220 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity				
FCC Part 90	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	NA	54.0 kbit/s	36.0 kbit/s	18.0 kbit/s	9.6 kbit/s
15 kHz	NA	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s	9.6 kbit/s
25 kHz	NA	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s	19.2 kbit/s
50 kHz	NA	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s	38.4 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
FCC Part 90	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	62.4 kbit/s	46.8 kbit/s	20.8 kbit/s	10.4 kbit/s	8.4 kbit/s
15 kHz	69.3 kbit/s	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s	8.4 kbit/s
25 kHz	110.8 kbit/s	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s	16.7 kbit/s
50 kHz	249.4 kbit/s	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s	33.4 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
FCC Part 90	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	NA	41.0 kbit/s	15.6 kbit/s	7.8 kbit/s	4.1 kbit/s
15 kHz	NA	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s	4.1 kbit/s
25 kHz	NA	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s	8.3 kbit/s
50 kHz	NA	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s	16.5 kbit/s

FCC: 400 / 450 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity				
FCC Part 90	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	NA	54.0 kbit/s	36.0 kbit/s	18.0 kbit/s	9.6 kbit/s
25 kHz	NA	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s	19.2 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
FCC Part 90	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	62.4 kbit/s	46.8 kbit/s	20.8 kbit/s	10.4 kbit/s	8.4 kbit/s
25 kHz	110.8 kbit/s	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s	16.7 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
FCC Part 90	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	NA	41.0 kbit/s	15.6 kbit/s	7.8 kbit/s	4.1 kbit/s
25 kHz	NA	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s	8.3 kbit/s

FCC: 700 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity				
FCC Part 27	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK ⁽¹⁾
12.5 kHz	NA	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s	9.6 kbit/s
25 kHz	NA	120.0 kbit/s	80.0 kbit/s	40.0 kbit/s	19.2 kbit/s
50 kHz	NA	240.0 kbit/s	160.0 kbit/s	80.0 kbit/s	38.4 kbit/s
100 kHz	NA	432.0 kbit/s	288.0 kbit/s	144.0 kbit/s	76.8 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
FCC Part 27	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK ⁽¹⁾
12.5 kHz	69.3 kbit/s	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s	8.4 kbit/s
25 kHz	138.6 kbit/s	103.9 kbit/s	46.2 kbit/s	23.1 kbit/s	16.7 kbit/s
50 kHz	277.1 kbit/s	207.8 kbit/s	92.5 kbit/s	46.2 kbit/s	33.4 kbit/s
100 kHz	NA	374.1 kbit/s	166.5 kbit/s	83.2 kbit/s	66.8 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
FCC Part 27	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK ⁽¹⁾
12.5 kHz	NA	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s	4.1 kbit/s
25 kHz	NA	91.2 kbit/s	34.6 kbit/s	17.3 kbit/s	8.3 kbit/s
50 kHz	NA	182.4 kbit/s	69.3 kbit/s	34.6 kbit/s	16.5 kbit/s
100 kHz	NA	328.3 kbit/s	124.7 kbit/s	62.4 kbit/s	33.0 kbit/s

Note 1: Please consult 4RF for availability.

FCC: 896 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz Part 24	NA	48.0 kbit/s	32.0 kbit/s	16.0 kbit/s	9.6 kbit/s
12.5 kHz Part 90	NA	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s	9.6 kbit/s
25 kHz Parts 24, 90	NA	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s	19.2 kbit/s
50 kHz Part 24	NA	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s	38.4 kbit/s
100 kHz Part 24	NA	432.0 kbit/s	288.0 kbit/s	144.0 kbit/s	76.8 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz Part 24	55.4 kbit/s	41.6 kbit/s	18.5 kbit/s	9.2 kbit/s	8.4 kbit/s
12.5 kHz Part 90	69.3 kbit/s	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s	8.4 kbit/s
25 kHz Parts 24, 90	110.8 kbit/s	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s	16.7 kbit/s
50 kHz Part 24	249.4 kbit/s	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s	33.4 kbit/s
100 kHz Part 24	NA	374.1 kbit/s	166.5 kbit/s	83.2 kbit/s	66.8 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz Part 24	NA	36.5 kbit/s	13.9 kbit/s	6.9 kbit/s	4.1 kbit/s
12.5 kHz Part 90	NA	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s	4.1 kbit/s
25 kHz Parts 24, 90	NA	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s	8.3 kbit/s
50 kHz Part 24	NA	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s	16.5 kbit/s
100 kHz Part 24	NA	328.3 kbit/s	124.7 kbit/s	62.4 kbit/s	33.0 kbit/s

FCC: 928 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz Part 24	NA	48.0 kbit/s	32.0 kbit/s	16.0 kbit/s	9.6 kbit/s
12.5 kHz Parts 90, 101	NA	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s	9.6 kbit/s
25 kHz Parts 24, 90, 101	NA	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s	19.2 kbit/s
50 kHz Parts 24, 101	NA	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s	38.4 kbit/s
100 kHz Part 24	NA	432.0 kbit/s	288.0 kbit/s	144.0 kbit/s	76.8 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz Part 24	55.4 kbit/s	41.6 kbit/s	18.5 kbit/s	9.2 kbit/s	8.4 kbit/s
12.5 kHz Parts 90, 101	69.3 kbit/s	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s	8.4 kbit/s
25 kHz Parts 24, 90, 101	110.8 kbit/s	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s	16.7 kbit/s
50 kHz Parts 24, 101	249.4 kbit/s	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s	33.4 kbit/s
100 kHz Part 24	NA	374.1 kbit/s	166.5 kbit/s	83.2 kbit/s	66.8 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz Part 24	NA	36.5 kbit/s	13.9 kbit/s	6.9 kbit/s	4.1 kbit/s
12.5 kHz Parts 90, 101	NA	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s	4.1 kbit/s
25 kHz Parts 24, 90, 101	NA	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s	8.3 kbit/s
50 kHz Parts 24, 101	NA	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s	16.5 kbit/s
100 kHz Part 24	NA	328.3 kbit/s	124.7 kbit/s	62.4 kbit/s	33.0 kbit/s

ISED Modem Mode

ISED: 135 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
15 kHz	NA	54.0 kbit/s	36.0 kbit/s	18.0 kbit/s	9.6 kbit/s
30 kHz	NA	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s	19.2 kbit/s
50 kHz	NA	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s	38.4 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
15 kHz	62.4 kbit/s	46.8 kbit/s	20.8 kbit/s	10.4 kbit/s	8.4 kbit/s
30 kHz	110.8 kbit/s	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s	16.7 kbit/s
50 kHz	249.4 kbit/s	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s	33.4 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
15 kHz	NA	41.0 kbit/s	15.6 kbit/s	7.8 kbit/s	4.1 kbit/s
30 kHz	NA	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s	8.3 kbit/s
50 kHz	NA	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s	16.5 kbit/s

ISED: 220 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	NA	54.0 kbit/s	36.0 kbit/s	18.0 kbit/s	9.6 kbit/s
15 kHz	NA	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s	9.6 kbit/s
25 kHz	NA	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s	19.2 kbit/s
50 kHz	NA	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s	38.4 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	62.4 kbit/s	46.8 kbit/s	20.8 kbit/s	10.4 kbit/s	8.4 kbit/s
15 kHz	69.3 kbit/s	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s	8.4 kbit/s
25 kHz	110.8 kbit/s	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s	16.7 kbit/s
50 kHz	249.4 kbit/s	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s	33.4 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	NA	41.0 kbit/s	15.6 kbit/s	7.8 kbit/s	4.1 kbit/s
15 kHz	NA	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s	4.1 kbit/s
25 kHz	NA	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s	8.3 kbit/s
50 kHz	NA	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s	16.5 kbit/s

ISED: 400 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	NA	54.0 kbit/s	36.0 kbit/s	18.0 kbit/s	9.6 kbit/s
25 kHz	NA	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s	19.2 kbit/s
50 kHz	NA	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s	38.4 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	62.4 kbit/s	46.8 kbit/s	20.8 kbit/s	10.4 kbit/s	8.4 kbit/s
25 kHz	110.8 kbit/s	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s	16.7 kbit/s
50 kHz	249.4 kbit/s	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s	33.4 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz	NA	41.0 kbit/s	15.6 kbit/s	7.8 kbit/s	4.1 kbit/s
25 kHz	NA	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s	8.3 kbit/s
50 kHz	NA	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s	16.5 kbit/s

ISED: 896 / 928 MHz Bands

No Forward Error Correction

Channel Size	Gross Radio Capacity				
	256 QAM	48.0 kbit/s	32.0 kbit/s	16.0 kbit/s	9.6 kbit/s
12.5 kHz RSS-134	NA	48.0 kbit/s	32.0 kbit/s	16.0 kbit/s	9.6 kbit/s
12.5 kHz RSS-119	NA	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s	9.6 kbit/s
25 kHz	NA	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s	19.2 kbit/s
50 kHz	NA	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s	38.4 kbit/s
100 kHz	NA	432.0 kbit/s	288.0 kbit/s	144.0 kbit/s	76.8 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz RSS-134	55.4 kbit/s	41.6 kbit/s	18.5 kbit/s	9.2 kbit/s	8.4 kbit/s
12.5 kHz RSS-119	69.3 kbit/s	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s	8.4 kbit/s
25 kHz	110.8 kbit/s	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s	16.7 kbit/s
50 kHz	249.4 kbit/s	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s	33.4 kbit/s
100 kHz	NA	374.1 kbit/s	166.5 kbit/s	83.2 kbit/s	66.8 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC				
	256 QAM	64 QAM	16 QAM	QPSK	4-CPFSK
12.5 kHz RSS-134	NA	36.5 kbit/s	13.9 kbit/s	6.9 kbit/s	4.1 kbit/s
12.5 kHz RSS-119	NA	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s	4.1 kbit/s
25 kHz	NA	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s	8.3 kbit/s
50 kHz	NA	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s	16.5 kbit/s
100 kHz	NA	328.3 kbit/s	124.7 kbit/s	62.4 kbit/s	33.0 kbit/s

Receiver

Receiver Sensitivity

			12.5 kHz	20 / 25 kHz	50 kHz	100 kHz
BER < 10 ⁻²	256 QAM	Max coded FEC	NA	NA	NA	NA
BER < 10 ⁻²	256 QAM	Min coded FEC	-97 dBm	-93 dBm	-90 dBm	NA
BER < 10 ⁻²	256 QAM	No FEC	NA	NA	NA	NA
BER < 10 ⁻²	64 QAM	Max coded FEC	-106 dBm	-102 dBm	-99 dBm	-96 dBm
BER < 10 ⁻²	64 QAM	Min coded FEC	-105 dBm	-101 dBm	-98 dBm	-95 dBm
BER < 10 ⁻²	64 QAM	No FEC	-103 dBm	-99 dBm	-96 dBm	-93 dBm
BER < 10 ⁻²	16 QAM	Max coded FEC	-113 dBm	-110 dBm	-107 dBm	-104 dBm
BER < 10 ⁻²	16 QAM	Min coded FEC	-112 dBm	-109 dBm	-106 dBm	-103 dBm
BER < 10 ⁻²	16 QAM	No FEC	-109 dBm	-106 dBm	-103 dBm	-100 dBm
BER < 10 ⁻²	QPSK	Max coded FEC	-118 dBm	-115 dBm	-112 dBm	-109 dBm
BER < 10 ⁻²	QPSK	Min coded FEC	-117 dBm	-114 dBm	-111 dBm	-108 dBm
BER < 10 ⁻²	QPSK	No FEC	-115 dBm	-112 dBm	-109 dBm	-106 dBm
BER < 10 ⁻²	4-CPFSK	Max coded FEC	NA	NA	NA	NA
BER < 10 ⁻²	4-CPFSK	Min coded FEC	-117 dBm	-114 dBm	-111 dBm	-108 dBm
BER < 10 ⁻²	4-CPFSK	No FEC	-115 dBm	-112 dBm	-109 dBm	-106 dBm

			12.5 kHz	20 / 25 kHz	50 kHz	100 kHz
BER < 10 ⁻⁶	256 QAM	Max coded FEC	NA	NA	NA	NA
BER < 10 ⁻⁶	256 QAM	Min coded FEC	-95 dBm	-91 dBm	-88 dBm	NA
BER < 10 ⁻⁶	256 QAM	No FEC	NA	NA	NA	NA
BER < 10 ⁻⁶	64 QAM	Max coded FEC	-103 dBm	-99 dBm	-96 dBm	-93 dBm
BER < 10 ⁻⁶	64 QAM	Min coded FEC	-101 dBm	-97 dBm	-94 dBm	-91 dBm
BER < 10 ⁻⁶	64 QAM	No FEC	-96 dBm	-92 dBm	-89 dBm	-86 dBm
BER < 10 ⁻⁶	16 QAM	Max coded FEC	-110 dBm	-107 dBm	-104 dBm	-101 dBm
BER < 10 ⁻⁶	16 QAM	Min coded FEC	-108 dBm	-105 dBm	-102 dBm	-99 dBm
BER < 10 ⁻⁶	16 QAM	No FEC	-102 dBm	-99 dBm	-96 dBm	-93 dBm
BER < 10 ⁻⁶	QPSK	Max coded FEC	-115 dBm	-112 dBm	-109 dBm	-106 dBm
BER < 10 ⁻⁶	QPSK	Min coded FEC	-113 dBm	-110 dBm	-107 dBm	-104 dBm
BER < 10 ⁻⁶	QPSK	No FEC	-108 dBm	-105 dBm	-102 dBm	-99 dBm
BER < 10 ⁻⁶	4-CPFSK	Max coded FEC	NA	NA	NA	NA
BER < 10 ⁻⁶	4-CPFSK	Min coded FEC	-113 dBm	-110 dBm	-107 dBm	-104 dBm
BER < 10 ⁻⁶	4-CPFSK	No FEC	-108 dBm	-105 dBm	-102 dBm	-99 dBm

Adjacent Channel Selectivity

		12.5 kHz	20 / 25 kHz	50 kHz	100 kHz
Adjacent channel selectivity		> -47 dBm	> -37 dBm	> -37 dBm	> -37 dBm
BER < 10 ⁻²	256 QAM	> 43 dB	> 53 dB	> 53 dB	NA
BER < 10 ⁻²	64 QAM	> 43 dB	> 53 dB	> 53 dB	> 53 dB
BER < 10 ⁻²	16 QAM	> 43 dB	> 53 dB	> 53 dB	> 53 dB
BER < 10 ⁻²	QPSK	> 48 dB	> 58 dB	> 58 dB	> 58 dB
BER < 10 ⁻²	4-CPFSK	> 55 dB	> 65 dB	> 65 dB	> 65 dB

Co-Channel Rejection

		12.5 kHz	20 / 25 kHz	50 kHz	100 kHz
BER < 10 ⁻²	256 QAM	> -26 dB	> -26 dB	> -26 dB	NA
BER < 10 ⁻²	64 QAM	> -23 dB	> -23 dB	> -23 dB	> -23 dB
BER < 10 ⁻²	16 QAM	> -19 dB	> -19 dB	> -19 dB	> -19 dB
BER < 10 ⁻²	QPSK	> -12 dB	> -12 dB	> -12 dB	> -12 dB
BER < 10 ⁻²	4-CPFSK	> -17 dB	> -17 dB	> -17 dB	> -17 dB

Intermodulation Response Rejection

		12.5 kHz	20 / 25 kHz	50 kHz	100 kHz
Intermodulation response rejection		> -35 dBm	> -35 dBm	> -35 dBm	> -35 dBm
BER < 10 ⁻²	256 QAM	> 55 dB	> 55 dB	> 55 dB	NA
BER < 10 ⁻²	64 QAM	> 55 dB	> 55 dB	> 55 dB	> 55 dB
BER < 10 ⁻²	16 QAM	> 55 dB	> 55 dB	> 55 dB	> 55 dB
BER < 10 ⁻²	QPSK	> 60 dB	> 60 dB	> 60 dB	> 60 dB
BER < 10 ⁻²	4-CPFSK	> 65 dB	> 65 dB	> 65 dB	> 65 dB

Blocking or Desensitization

		12.5 kHz	20 / 25 kHz	50 kHz	100 kHz
Blocking or desensitization		> -17 dBm	> -17 dBm	> -17 dBm	> -17 dBm
BER < 10 ⁻²	256 QAM	> 73 dB	> 73 dB	> 73 dB	NA
BER < 10 ⁻²	64 QAM	> 73 dB	> 73 dB	> 73 dB	> 73 dB
BER < 10 ⁻²	16 QAM	> 73 dB	> 73 dB	> 73 dB	> 73 dB
BER < 10 ⁻²	QPSK	> 78 dB	> 78 dB	> 78 dB	> 78 dB
BER < 10 ⁻²	4-CPFSK	> 85 dB	> 85 dB	> 85 dB	> 85 dB

Spurious Response Rejection

		12.5 kHz	20 / 25 kHz	50 kHz	100 kHz
Spurious response rejection		> -32 dBm	> -32 dBm	> -32 dBm	> -32 dBm
BER < 10 ⁻²	256 QAM	> 58 dB	> 58 dB	> 58 dB	NA
BER < 10 ⁻²	64 QAM	> 58 dB	> 58 dB	> 58 dB	> 58 dB
BER < 10 ⁻²	16 QAM	> 58 dB	> 58 dB	> 58 dB	> 58 dB
BER < 10 ⁻²	QPSK	> 63 dB	> 63 dB	> 63 dB	> 63 dB
BER < 10 ⁻²	4-CPFSK	> 70 dB	> 70 dB	> 70 dB	> 70 dB

Receiver Spurious Radiation

	12.5 kHz	20 / 25 kHz	50 kHz	100 kHz
Receiver spurious radiation	> -57 dBm	> -57 dBm	> -57 dBm	> -57 dBm

Transmitter

Max peak envelope power (PEP)		10.0 W (+40 dBm)
Average Power output	256 QAM	0.01 to 2.0 W (+10 to +33 dBm, in 1 dB steps)
	64 QAM	0.01 to 2.5 W (+10 to +34 dBm, in 1 dB steps)
	16 QAM	0.01 to 3.2 W (+10 to +35 dBm, in 1 dB steps)
	QPSK	0.01 to 5.0 W (+10 to +37 dBm, in 1 dB steps)
	4-CPFSK ^(Note 1)	0.01 to 10.0 W (+10 to +40 dBm, in 1 dB steps)

Note 1: Please consult 4RF for availability

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

Adjacent channel power	< - 60 dBc
Transient adjacent channel power	< - 60 dBc
Spurious emissions	< - 37 dBm
Attack time	< 1.5 ms
Release time	< 0.5 ms
Data turnaround time	< 2 ms
Frequency stability	± 0.5 ppm
Frequency aging	< 1 ppm / annum
Emission Designator Suffix	QPSK G1D, QAM D1D

Modem

Forward Error Correction	Variable length concatenated Reed Solomon plus convolutional code
Adaptive Burst Support	Adaptive FEC Adaptive Coding and Modulation

Data Payload Security

Data payload security	CCM* Counter with CBC-MAC
Data encryption	Counter Mode Encryption (CTR) using Advanced Encryption Standard (AES) 128, 192 or 256
Data authentication	Cipher Block Chaining Message Authentication Code (CBC-MAC) using Advanced Encryption Standard (AES) 128, 192 or 256

Duplexer Specifications

The specifications for the duplexers in the duplexer kits are:

Code	Frequency Band	TX / RX Split	Passband	Tuning Lo Band	Tuning Hi Band
N0	135 MHz	4.6 MHz min split	0.5 MHz	134 - 172 MHz	138 - 176 MHz
N1	135 MHz	4.0 MHz min split	1.0 MHz	135 - 175 MHz	135 - 175 MHz
A1	300 MHz	5 MHz min split	0.5 MHz	330 - 400 MHz	330 - 400 MHz
A2	300 MHz	20 MHz min split	3.5 MHz	330 - 400 MHz	330 - 400 MHz
B0	400 MHz	9.45 MHz min split	2 MHz	400 - 470 MHz	400 - 470 MHz
B1	400 MHz	5 MHz min split	0.5 MHz	400 - 470 MHz	400 - 470 MHz
M0	450 MHz	5 MHz min split	0.5 MHz	450 - 520 MHz	450 - 520 MHz
E0	700 MHz	30 MHz min split	7 MHz	757 - 788 MHz	757 - 788 MHz
E1	700 MHz	30 MHz min split	1 MHz	757 - 788 MHz	757 - 788 MHz
E2	700 MHz	30 MHz min split	1 MHz	757 - 788 MHz	757 - 788 MHz
G0	900 MHz	40 MHz min split	7 MHz	850 - 960 MHz	850 - 960 MHz
G1	900 MHz	9 MHz split	1 MHz	928 - 960 MHz	928 - 960 MHz
G2	900 MHz	9 MHz split	1 MHz	928 - 960 MHz	928 - 960 MHz
G3	900 MHz	5.5 MHz min split	0.5 MHz	928 - 960 MHz	928 - 960 MHz
G4	900 MHz	3.6 MHz split	0.5 MHz	928 - 960 MHz	928 - 960 MHz
G6	900 MHz	28 MHz min split	1 MHz	928 - 960 MHz	928 - 960 MHz

Interface Specifications

Ethernet Interface

The Aprisa SR+ radio features an integrated 10Base-T/100Base-TX layer-2 Ethernet switch.

To simplify network setup, each port supports auto-negotiation and auto-sensing MDI/MDIX. Operators can select from the following preset modes:

- Auto negotiate
- 10Base-T half or full duplex
- 100Base-TX half or full duplex

The Ethernet ports are IEEE 802.3-compatible. The L2 Bridge (Switch) is IEEE 802.1d/q/p compatible, and supports VLANs and VLAN manipulation of add/remove VLANs.

General	Interface	RJ45 x 2 (Integrated 2-port switch)
	Cabling	CAT-5/6 UTP, supports auto MDIX (Standard Ethernet)
	Maximum line length	100 metres on cat-5 or better
	Bandwidth allocation	The Ethernet capacity maximum is determined by the available radio link capacity.
	Maximum transmission unit	Option setting of 1522 or 1536 octets
	Address table size	1024 MAC addresses
	Ethernet mode	10Base-T or 100Base-TX Full duplex or half duplex (Auto-negotiating and auto-sensing)
Diagnostics	Left Green LED	Off: no Ethernet signal received On: Ethernet signal received
	Right Orange LED	Off: no data present on the interface Flashing: data present on the interface

Note: Do not connect Power over Ethernet (PoE) connections to the Aprisa SR+ Ethernet ports as this will damage the port.

RS-232 Asynchronous Interface

The Aprisa SR+ radio's ITU-T V.24 compliant RS-232 interface is configured as a Cisco® pinout DCE. The interface terminates to a DTE using a straight-through cable or to a DCE with a crossover cable (null modem).

The interface uses two handshaking control lines between the DTE and the DCE.

General	Interface	ITU-T V.24 / EIA/TIA RS-232E
	Interface direction	DCE only
	Maximum line length	10 metres (dependent on baud rate)
Async parameters	Standard mode data bits	7 or 8 bits
	Standard mode parity	Configurable for None, Even or Odd
	Standard mode stop bits	1 or 2 bits
	Interface baud rates	300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 and 115200 bit/s
Control signals	DCE to DTE	CTS, RTS, DSR, DTR
Diagnostics	Left Green LED	Off: no RS-232 device connected On: RS-232 device connected
	Right Orange LED	Off: no data present on the interface Flashing: data present on the interface

Hardware Alarms Interface

The hardware alarms interface supports two alarm inputs and two alarms outputs.

Alarm Inputs

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

Interface	RJ45 connector
Detector type	Non-isolated ground referenced voltage detector
Detection voltage - on	> +10 VDC
Detection voltage - off	< +4 VDC
Maximum applied input voltage	30 VDC
Maximum input current limit	10 mA

Alarm Outputs

The alarm connector provides two hardware alarm outputs for alarm reception from other radios in the network.

Interface	RJ45 connector
Output type	Non-isolated ground referenced open collector output
Maximum applied voltage	30 VDC
Maximum drive current	100 mA
Overload protection	Thermally resettable fuse

Protect Interface

The Protect interface is used to connect the radios to the protection switch within a Protected Station. It is not a customer interface.

Protection Switch Specifications

RF Insertion Loss	< 0.5 dB (switch and connecting cables)
Remote Control inputs	Logic 4700 ohms pullup to +3.3 VDC

Power Specifications

Power Supply

Aprisa SR+ Radio

Nominal voltage input	+12 VDC
Ground Reference	Negative earth
Absolute input voltage range	+10 to +30 VDC
Maximum power input	35 W
Connector	Molex 2 pin male screw fitting 39524-0002

Aprisa SR+ Protected Station

Protected Station Type	Version 1		Version 2
Nominal Voltage Input	12 VDC	48 VDC	
Ground Reference	Negative earth	Floating	Floating
Absolute input voltage range	+10 to +30 VDC	18 to 60 VDC	10 to 60 VDC
Maximum power input	42 W		
Connector	2x Molex 2 pin male screw fitting 39524-0002		

Aprisa SR+ Migration Master Station

Nominal Voltage Input	12 VDC	48 VDC
Ground Reference	Negative earth	Floating
Absolute input voltage range	+10 to +30 VDC	18 to 60 VDC
Maximum power input	48 W	
Connector	4x Molex 2 pin male screw fitting 39524-0002	

Power Consumption

Note: The radio power consumption is very dependent on transmitter power, the type of traffic and network activity.

Aprisa SR+ Radio

Mode	Hardware Type	Frequency Band	Power Consumption
Transmit / Receive	Standard	All	< 35 W for 10 W transmit peak power
			< 30 W for 5 W transmit power
			< 25 W for 1 W transmit power
	Power Optimized	135 and 220 MHz	< 34 W for 10 W transmit peak power
			< 25 W for 5 W transmit power
			< 15 W for 1 W transmit power
		320, 400, 450, 700, 896, 928	< 33 W for 10 W transmit peak power
			< 28 W for 5 W transmit power
			< 22 W for 1 W transmit power
Receive only	Standard	All	< 7 W
			< 3 W in active receive state
			< 2 W in idle receive state < 0.5 W in sleep mode

Aprisa SR+ Protected Station and Aprisa SR+ Data Driven Protected Station

Mode	Hardware Type	Frequency Band	Power Consumption
Transmit / Receive	Standard	All	< 42 W for 10 W transmit peak power
			< 37 W for 5 W transmit power
			< 32 W for 1 W transmit power
	Power Optimized	135 and 220 MHz	< 41 W for 10 W transmit peak power
			< 32 W for 5 W transmit power
			< 22 W for 1 W transmit power
		320, 400, 450, 700, 896, 928	< 40 W for 10 W transmit peak power
			< 35 W for 5 W transmit power
			< 29 W for 1 W transmit power
Receive only	All	All	< 15 W

Note: The product label shows a Hardware Type of 'Type A' for the 'Standard' product

The product label shows a Hardware Type of 'Type B' or greater for the 'Power Optimized' product

Power Dissipation

Aprisa SR+ Radio

Hardware Type	Transmit Power	Power Dissipation
Standard	10 W transmit power	< 25 W
	5 W transmit power	< 25 W
	1 W transmit power	< 24 W
Power Optimized	10 W transmit power	< 23 W
	5 W transmit power	< 23 W
	1 W transmit power	< 21 W

Aprisa SR+ Protected Station and Aprisa SR+ Data Driven Protected Station

Hardware Type	Transmit Power	Power Dissipation
Standard	10 W transmit power	< 32 W
	5 W transmit power	< 32 W
	1 W transmit power	< 31 W
Power Optimized	10 W transmit power	< 30 W
	5 W transmit power	< 30 W
	1 W transmit power	< 28 W

General Specifications

Environmental

Operating temperature range	-40 to +70° C (-40 to +158° F)
Storage temperature range	-40 to +85° C (-40 to +185° F)
Operating humidity	Maximum 95% non-condensing
Acoustic noise emission	No audible noise emission

Mechanical

Aprisa SR+ Radio

Dimensions	Width 210 mm (8.27") Depth 130 mm (5.12") and 146 mm (5.748") with TNC connectors Height 41.5 mm (1.63")
Weight	1.25 kg (2.81 lbs)
Colour	Matt black
Mounting	Wall (2 x M5 screws) Rack shelf (4 x M4 screws) DIN rail bracket

Aprisa SR+ Protected Station

Dimensions	Width 432.6 mm (17") Depth 372 mm (14.6") and 388 mm (15.276") with TNC connectors Height 2U plus external duplexer (if used)
Weight	10.0 kg (22 lbs) (includes the 2 radios)
Colour	Matt black
Mounting	Rack mount (4 x M6 screws)

Compliance

ETSI

Radio	12.5 kHz Channel	EN 300 113
	25 kHz / 50 kHz Channel	EN 302 561 ⁽¹⁾
EMI / EMC		EN 301 489-1 and 5
Safety		EN 60950-1:2006 Class 1 division 2 for hazardous locations
Environmental		ETS 300 019 Class 3.4 IEEE 1613 Class 2 IEC 61850-3 Ingress Protection IP51

Note 1: At 50 kHz, TX to 256 QAM, RX to 64 QAM

FCC

Radio	47CFR part 24, part 27, part 90 and part 101 Private Land Mobile Radio Services
EMC	47CFR part 15 Radio Frequency Devices, EN 301 489-1 and 5
Safety	UL / EN 60950-1:2006 Class 1 division 2 for hazardous locations
Environmental	ETS 300 019 Class 3.4 IEEE 1613 Class 2 IEC 61850-3 Ingress Protection IP51

ISED

Radio	RSS-119 / RSS-134
EMC	This Class A digital apparatus complies with Canadian standard ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.
Safety	UL / EN 60950-1:2006 Class 1 division 2 for hazardous locations
Environmental	ETS 300 019 Class 3.4 IEEE 1613 Class 2 IEC 61850-3 Ingress Protection IP51

14. Product End Of Life

End-of-Life Recycling Programme (WEEE)

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

4RF has implemented an end-of-life recycling programme to manage the reuse, recycling, and recovery of waste in an environmentally safe manner using processes that comply with the WEEE Directive (EU Waste Electrical and Electronic Equipment 2002/96/EC).

The WEEE Symbol Explained



This symbol appears on Electrical and Electronic Equipment (EEE) as part of the WEEE (Waste EEE) directive. It means that the EEE may contain hazardous substances and must not be thrown away with municipal or other waste.

WEEE Must Be Collected Separately

You must not dispose of electrical and electronic waste with municipal and other waste. You must separate it from other waste and recycling so that it can be easily collected by the proper regional WEEE collection system in your area.

YOUR ROLE in the Recovery of WEEE

By separately collecting and properly disposing of WEEE, you are helping to reduce the amount of WEEE that enters the waste stream.

One of the aims of the WEEE directive is to divert EEE away from landfill and encourage recycling. Recycling EEE means that valuable resources such as metals and other materials (which require energy to source and manufacture) are not wasted. Also, the pollution associated with accessing new materials and manufacturing new products is reduced.

EEE Waste Impacts the Environment and Health

Electrical and electronic equipment (EEE) contains hazardous substances which have potential effects on the environment and human health. If you want environmental information on the Aprisa SR+ radio, contact us (on page 19).

15. Copyrights

Mirrored Bits® is a registered trademark of Schweitzer Engineering Laboratories, Inc