



Aprisa **FE**



User Manual

July 2015

Version 1.5.0

Copyright

Copyright © 2015 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 and other countries. Java and all Java-related trademarks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All other marks are the property of their respective owners.

Disclaimer

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

RoHS and WEEE Compliance

The Aprisa FE 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 FE 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 FE radio equipment being installed at a fixed restricted access location and operated in 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 FE User Manual, is a generic term for one end station of a point-to-point Aprisa FE link and does not confer any rights to connect to any public network or to operate the equipment within any territory.

Compliance European Telecommunications Standards Institute

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

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

Frequency band	Channel size	Power input	Notified body
135-175 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	
320-400 MHz	12.5 kHz, 20 kHz, 25 kHz, 50 kHz	12 VDC	
400-470 MHz	12.5 kHz, 20 kHz, 25 kHz, 50 kHz	12 VDC	
450-520 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	

Compliance Federal Communications Commission

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

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

Frequency Band *	Channel size	Power input	Authorization	FCC ID
135-175 MHz	12.5 kHz, 25 kHz	12 VDC	Part 90	Pending
400-470 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	Part 90	UIPSQ400M131
450-520 MHz	12.5 kHz, 25 kHz	12 VDC	Part 90	UIPSQ450M140
896-902 MHz	50 kHz	12 VDC	Part 24	UIPSQ896M141
928-960 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	Part 24, Part 90 and Part 101	UIPSQ928M141

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

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

Compliance Industry Canada

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

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

Frequency Band *	Channel size	Power input	Authorization	IC ID
135-175 MHz	12.5 kHz, 25 kHz	12 VDC	RSS-119	Pending
400-470 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	RSS-119	6772A-SQ400M131
896-902 MHz	50 kHz	12 VDC	RSS-134	6772A-SQ896M141
928-960 MHz	12.5 kHz, 25 kHz, 50 kHz	12 VDC	RSS-119 and RSS-134	6772A-SQ928M141

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

RF Exposure Warning



WARNING:

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

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

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

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

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

Contents

1. Getting Started	11
2. Introduction.....	13
About This Manual.....	13
What It Covers	13
Who Should Read It	13
Contact Us.....	13
What's in the Box	13
Aprisa FE Accessory Kit.....	14
Aprisa FE CD Contents	16
Software	16
Documentation	16
3. About the Radio	17
The 4RF Aprisa FE Radio.....	17
Product Overview	17
Network Coverage and Capacity	17
Product Features	18
Functions	18
Security	19
Performance	20
Usability	20
System Gain vs FEC Coding	21
Architecture.....	22
Product Operation.....	22
Physical Layer.....	22
Adaptive Coding Modulation	22
Network Layer	23
Packet Routing.....	23
Static IP Router	24
Bridge Mode with VLAN Aware	25
VLAN Bridge Mode Description	26
Avoiding Narrow Band Radio Traffic Overloading.....	28
Interfaces.....	30
Antenna Interface	30
Ethernet Interface	30
USB Interfaces	30
Protect Interface	30
Alarms Interface.....	30
Front Panel Connections	31
LED Display Panel	32
Normal Operation	32
Single Radio Software Upgrade.....	33
Link Software Upgrade	33
Test Mode	34
Network Management	35
Hardware Alarm Inputs / Outputs	36
Alarm Input to SNMP Trap.....	36
Alarm Input to Alarm Output	36
Aprisa SR Alarm Input to Aprisa FE Alarm Output	36

4. Preparation	37
Bench Setup	37
Path Planning	38
Antenna Selection and Siting	38
Antenna Siting	39
Coaxial Feeder Cables	40
Linking System Plan	40
Site Requirements.....	41
Power Supply.....	41
Equipment Cooling	41
Earthing and Lightning Protection	42
Feeder Earthing.....	42
Radio Earthing	42
5. Installing the Radio	43
Mounting.....	43
Internal Duplexer.....	43
External Duplexer	43
Installing the Antenna and Feeder Cable	44
Connecting the Power Supply	45
External Power Supplies.....	45
Spare Fuses.....	46
Additional Spare Fuses.....	46
6. Managing the Radio	47
SuperVisor	47
PC Requirements for SuperVisor	48
Connecting to SuperVisor	49
Management PC Connection	50
PC Settings for SuperVisor	51
Login to SuperVisor.....	55
Logout of SuperVisor.....	56
SuperVisor Page Layout.....	57
SuperVisor Menu	59
SuperVisor Menu Access	60
SuperVisor Menu Items	62
Standard Radio.....	63
Terminal	63
Radio	73
Ethernet	85
IP.....	95
QoS	104
Security	126
Maintenance	144
Events	159
Software	171
Monitoring	187
Link.....	204
Protected Station	213
Terminal	214
Radio	219
Ethernet	221
IP.....	222
Security	226
Maintenance	228

Events	235
Software	238
Link	255
Command Line Interface	264
Connecting to the Management Port	264
CLI Commands	267
Viewing the CLI Terminal Summary	268
Changing the Radio IP Address with the CLI	268
In-Service Commissioning	269
Before You Start	269
What You Will Need	269
Antenna Alignment	270
Aligning the Antennas	270
7. Product Options	271
Chassis Options	271
300 mm Chassis Depth - Internal Duplexer	271
300 mm Chassis Depth - External Duplexer	272
440 mm Chassis Depth - Internal Duplexer Only	273
Protected Station	274
Protected Ports	275
Operation	275
Switch Over	275
Switching Criteria	276
Monitored Alarms	277
Configuration Management	278
Hardware Manual Lock	278
Remote Control	278
L2 / L3 Protection Operation	279
Hot-Swappable	279
Antenna and Duplexer Options	280
Installation	281
Mounting	281
Cabling	282
Power	284
Alarms	284
Maintenance	285
Changing the Protected Station IP Addresses	285
Creating a Protected Station	285
Replacing a Protected Station Faulty Radio	286
Replacing a Faulty Power Supply	287
Replacing a Faulty Protection Switch	287
Spares	287
8. Maintenance	289
No User-Serviceable Components	289
Software Upgrade	290
Non Protected Link Upgrade Process	290
Protected Link Upgrade Process	291
Single Radio Software Upgrade	293
File Transfer Method	293
USB Boot Upgrade Method	294
Software Downgrade	295
Protected Station Software Upgrade	296

9. Interface Connections.....	297
RJ45 Connector Pin Assignments.....	297
Ethernet Interface Connections.....	297
Alarm Interface Connections.....	298
Protection Switch Remote Control Connections.....	298
10. Alarm Types and Sources.....	299
Alarm Types.....	299
Alarm Events.....	300
Informational Events.....	304
11. Specifications.....	305
RF Specifications.....	305
Frequency Bands.....	305
Channel Sizes.....	306
Receiver.....	312
Transmitter.....	314
Modem.....	315
Data Payload Security.....	315
Interface Specifications.....	316
Ethernet Interface.....	316
Hardware Alarms Interface.....	317
Protection Switch Specifications.....	317
Power Specifications.....	318
Power Supply.....	318
Power Consumption.....	319
Power Dissipation.....	319
General Specifications.....	320
Environmental.....	320
Mechanical.....	320
Compliance.....	321
12. Product End Of Life.....	322
End-of-Life Recycling Programme (WEEE).....	322
The WEEE Symbol Explained.....	322
WEEE Must Be Collected Separately.....	322
YOUR ROLE in the Recovery of WEEE.....	322
EEE Waste Impacts the Environment and Health.....	322
13. Abbreviations.....	323
14. Index.....	324

1. Getting Started

This section is an overview of the steps required to commission an Aprisa FE radio link in the field:

Phase 1:	Pre-installation	
1.	Confirm path planning.	Page 38
2.	Ensure that the site preparation is complete: <ul style="list-style-type: none"> • Power requirements • Tower requirements • Environmental considerations, for example, temperature control • Mounting space 	Page 40

Phase 2:	Installing the radios	
1.	Mount the radio.	Page 43
2.	Connect earthing to the radio.	Page 42
3.	Confirm that the: <ul style="list-style-type: none"> • 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 42
5.	Connect the coaxial jumper cable between the lightning protection and the radio antenna port.	Page 44
6.	Connect the power to the radio.	Page 45

Phase 3:	Establishing the link	
1.	If radio's IP address is not the default IP address (169.254.50.10 with a subnet mask of 255.255.0.0) and you don't know the radio's IP address see 'Command Line Interface' on page 264.	Page 264
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: <ul style="list-style-type: none"> • IP address • Subnet mask • Gateway IP address 	Page 51
4.	Open a web browser and login to the radio.	Page 55
5.	Set or confirm the RF characteristics: <ul style="list-style-type: none"> • TX and RX frequencies • TX output power 	Page 75
6.	Compare the actual RSSI to the expected RSSI value (from your path planning).	
7.	Align the antennas.	Page 270
8.	Confirm that the radio is operating correctly; the OK, MODE and USB LEDs are green.	

2. Introduction

About This Manual

What It Covers

This user manual describes how to install and configure an Aprisa FE point-to-point digital radio link. It specifically documents an Aprisa FE radio running system software version 1.5.0.

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 FE after reading this manual, please contact Customer Support or your local 4RF representative.

Our area representative contact details are available from our website:

4RF Limited
26 Glover Street, Ngauranga
PO Box 13-506
Wellington 6032
New Zealand

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

What's in the Box

Inside the box you will find:

- One Aprisa FE radio fitted with a power connector.
- One Aprisa FE Accessory kit containing the following:
 - Aprisa FE Quick Start Guide
 - Aprisa FE CD
 - Mounting brackets and screws
 - Hardware kit
 - DC power cable
 - Ground cable
 - Management cable

Aprisa FE Accessory Kit

The accessory kit contains the following items:

Aprisa FE Quick Start Guide



Aprisa FE CD



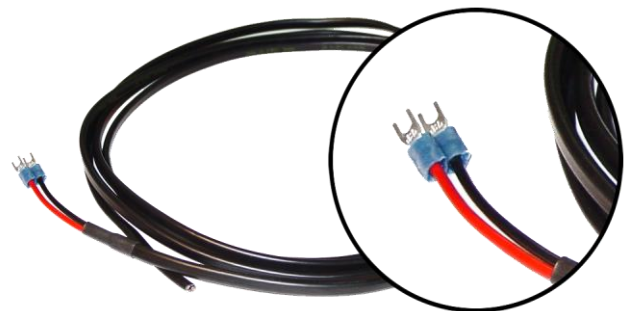
Two mounting brackets and 8 screws



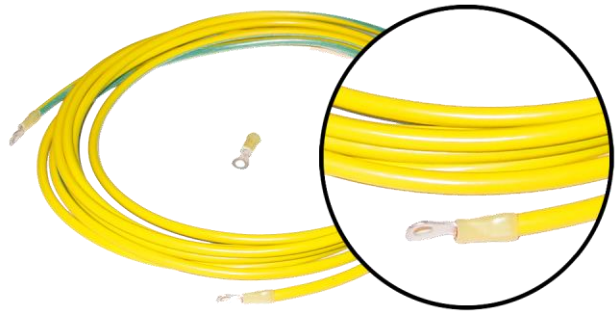
Hardware kit
(includes Allen key for lid screws)



DC power cable 3 m



Ground cable 5 m



Management Cable

USB Cable USB A to USB micro B, 1m



Aprisa FE CD Contents

The Aprisa FE CD contains the following:

Software

- The latest version of the radio software (see 'Software Upgrade' on page 290)
- USB Serial Driver
- Web browsers - Mozilla Firefox and Internet Explorer are included for your convenience
- Adobe™ Acrobat® Reader® which you need to view the PDF files on the Aprisa FE CD

Documentation

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

3. About the Radio

The 4RF Aprisa FE Radio

The 4RF Aprisa FE is a point-to-point digital radio providing secure narrowband wireless data connectivity for low capacity backhaul for SCADA, DMR infrastructure, telemetry and applications.

The radios carry Ethernet data between the local and remote radio.



Product Overview

Network Coverage and Capacity

The Aprisa FE 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 FE 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 radio link will be defined by a range of factors including the RF output power, the modulation used and its related receiver sensitivity and the geographic location.

Product Features

Functions

- Point-to-Point (PTP) operation
- Licensed frequency bands:

VHF 135	135-175 MHz
UHF 320	320-400 MHz
UHF 400	400-470 MHz
UHF 450	450-520 MHz
UHF 896	896-902 MHz
UHF 928	928-960 MHz
- Channel sizes - software selectable:
 - 12.5 kHz
 - 20 kHz
 - 25 kHz
 - 50 kHz
- Adaptive Coding Modulation (ACM): QPSK to 64 QAM
- Full duplex RF operation
- Ethernet data interface
- Data encryption and authentication using 128,192 and 256 bit AES and CCM security standards
- 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, management)
- L2/3/4 filtering for security and avoiding narrow band radio network overload
- L3 Gateway Router mode with standard static IP route for simple routing network integration
- L3 Router mode with per Ethernet interface IP address and subnet
- L2 Bridge mode with VLAN aware for standard Industrial LAN integration
- Ethernet header and IP/TCP / UDP ROCH header compression to increase the narrow band radio capacity
- Ethernet payload compression to increase the narrow band radio capacity
- SuperVisor web management support for element and sub-network (base-repeater-remotes) management
- SNMPv1/2/3 & encryption MIB supports for 4RF SNMP manager or third party SNMP agent network management
- SNMPv3 context addressing for compressed SNMP access to remote radios
- SNTP for accurate wide radio network time and date
- RADIUS authentication for remote user authorization, authentication and accounting
- Transparent to all common SCADA protocols; e.g. Modbus, IEC 60870-5-101/104, DNP3 or similar
- Complies with international standards, including ETSI, FCC, IC, EMC, safety and environmental standards

Security

The Aprisa FE 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

The security features implemented are:

- Data encryption
 - Counter Mode Encryption (CTR) using Advanced Encryption Standard (AES) 128, 192, 256 bit, based on FIPS PUB 197 AES encryption (using Rijndael version 3.0)
- Data authentication
 - NIST SP 800-38C Cipher Block Chaining Message Authentication Code (CBC-MAC) based on RFC 3610 using Advanced Encryption Standard (AES)
- Data payload security
 - CCM Counter with CBC-MAC integrity (NIST special publication 800-38C)
- Secured management interface protects configuration
- L2 / L3 / L4 Address filtering enables traffic source authorization
- Proprietary physical layer protocol and modified MAC layer protocol based on standardized IEEE 802.15.4
- Licensed radio spectrum provides recourse against interference
- SNMPv3 with Encryption for NMS secure access
- Secure USB software upgrade
- Key Encryption Key (KEK) based on RFC 3394, for secure Over The Air Re-keying (OTAR) of encryption keys
- User privilege allows the accessibility control of the different radio network users and the user permissions

Performance

- 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

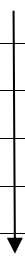
- Configuration / diagnostics via front panel Management Port USB interface, Ethernet interface
- Built-in webserver SuperVisor with full configuration, diagnostics and monitoring functionality, including remote radio configuration / diagnostics over the radio link
- LED display for on-site diagnostics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

System Gain vs FEC Coding

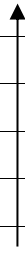
This table shows the relationship between modulation, FEC coding, system gain, capacity and coverage.

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

This table defines the modulation order based on gross capacity:

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

This table defines the modulation order based on receiver sensitivity:

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

Architecture

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

- Physical
 - Proprietary wireless
 - Ethernet interface
- Link
 - Proprietary wireless
 - VLAN aware Ethernet bridge
- Network
 - Standard IP
 - Proprietary automatic radio routing table population algorithm
- Transport
 - TCP, UDP
- Application
 - HTTPS web management access with proprietary management application software including management of remote radio over the radio link
 - SNMPv1/2/3 for network management application software

Product Operation

There are two components to the wireless interface: the Physical Layer (PHY), the Network Layer. These two layers are required to transport data across the wireless channel in the point-to-point configuration.

Physical Layer

The Aprisa FE PHY uses two frequency full duplex transmission mode with internal or external duplexer product options.

The Aprisa FE 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 FE 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.

Adaptive Coding Modulation

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

ACM automatically adjusts the modulation coding and FEC code rate in both directions of transmission over the defined modulation range based on the signal quality.

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

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

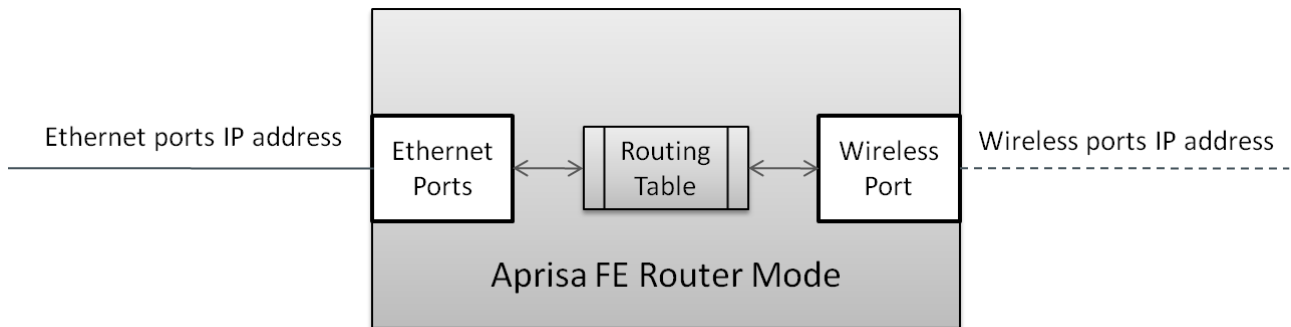
Network Layer

Packet Routing

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

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

Within the Aprisa FE 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 on a device connected to the remote FE, the packet is then forwarded to the wireless ports and transmitted in a PTP wireless packet to remote radio. 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 IP device for further packet processing.



Static IP Router

The Aprisa FE works in the point-to-point (PTP) network as a standard static IP router with the Ethernet and wireless / radio as interfaces.

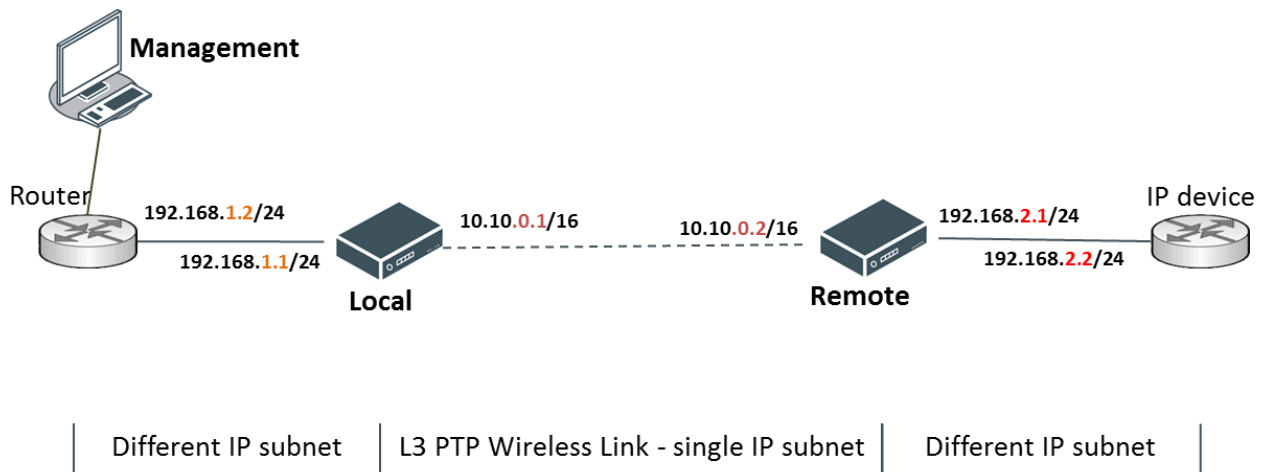
The Aprisa FE static router is semi-automated operation, where the routing table is automatically created in the local radio and populated with routes to the remote radio during the registration process and vice versa, where the routing table is automatically created in the remote radio and populated with routes to local radio during the registration process. Updates occur when the remote radio is disconnected for any reason, with the routing table updated in a controlled fashion.

Also, in decommission operation, the local radio routing tables is 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 FE works as a static IP router without using any routing protocol and therefore does not have the overhead of routing protocol for better utilization of the narrow bandwidth PTP link.

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 FE supports IP gateway connections 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 0.0.0.0. It is used by the router when an IP address does not match any other routes in the routing table.

The Aprisa FE sub-netting rules distinguish between the wireless interface and the remote Ethernet interface. The PTP link is set on a single IP subnet, while each Aprisa FE remote's Ethernet interface is set to a different subnet network.



Static IP Router - Human Error Free

To ensure correct operation, the Aprisa FE router local radio alerts when one (or more) of the devices is not configured for router mode or a duplicated IP is detected when manually inserted and etc.

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

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

Bridge Mode with VLAN Aware

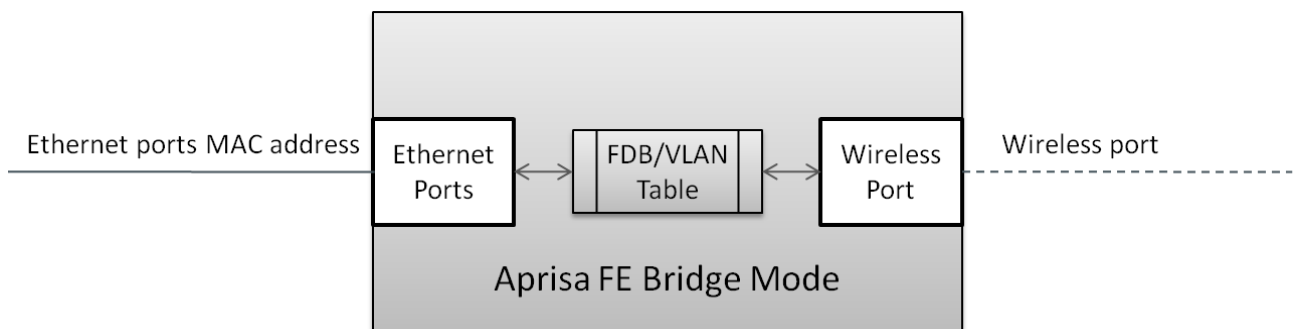
Ethernet VLAN Bridge / Switch Overview

The Aprisa FE 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 FE 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 FE PTP wireless network and in and out to the external Industrial LAN network and RTUs devices connected to the Aprisa FE wired Ethernet ports. Within the Aprisa FE 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 have any information on that 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 destination MAC address is a bridge device, the packet is then forwarded to the wireless ports and transmitted in a PTP wireless packet to the remote radio. The appropriate remote then switches the Ethernet packet and forwards it based on its FDB table (base on MAC or VLAN & MAC) to the appropriate Ethernet port to the bridge device for further packet processing.



VLAN Bridge Mode Description

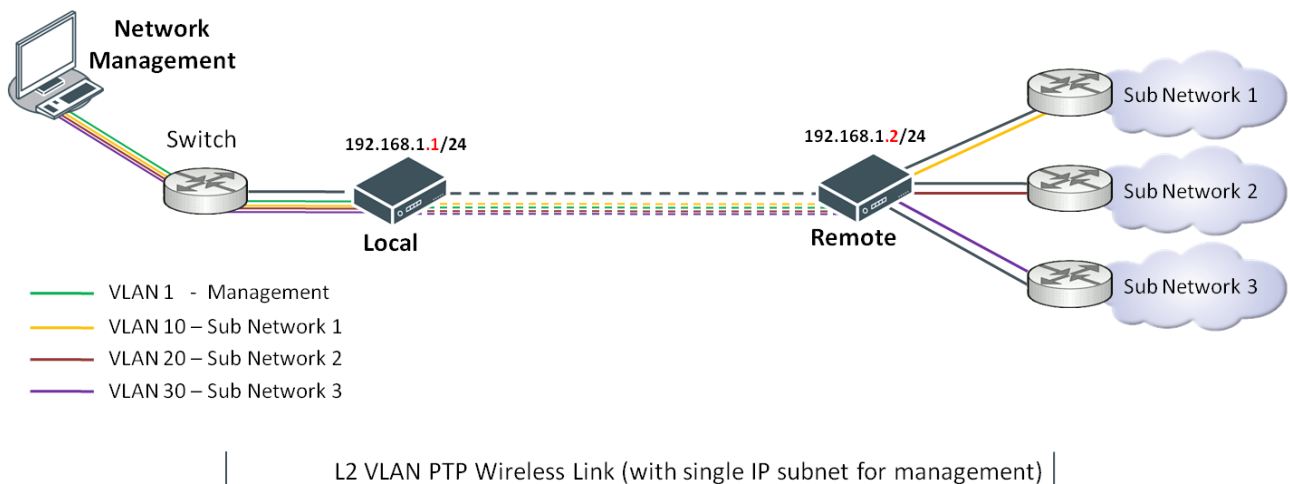
General - Aprisa FE VLAN Bridge

Aprisa FE works in the point-to-point (PTP) network as a standard VLAN bridge with the Ethernet and wireless / radio as interfaces.

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

VLANs are statically configured by the user on the ports where a Virtual LAN is required across the PTP radio link. VLAN management can be used to manage with external NMS all the Aprisa FE devices on the radio network, and is automatically created with a VLAN ID = 1 default value. The VLAN ID can be changed by the user later on.

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



VLANs - Single, Double and Trunk VLAN ports

Aprisa FE 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 different Aprisa FE PTP links, where the outer SVLAN is used to identify the link 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 FE PTP link. When packet enters the Aprisa FE PTP link, 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 PTP link.

Trunk VLAN is also supported by the Aprisa FE where the user can configure multiple VLANs on a specific Ethernet port and PTP link, creating a trunk VLAN port.

VLAN Manipulation - Add / Remove VLAN Tags

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

In an Aprisa FE VLAN tagged network, a remote Aprisa FE connected to a plain switch without VLAN support, will remove (strip-off) the VLAN tag from the packet before sending it to the switch. On the other direction, when the switch is sending an untagged packet, the Aprisa FE will add (append) an appropriate user pre-configure VLAN tag before sending it over the air to the local radio.

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 FE 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 FE radio. Packets in the queues are then scheduled out in a strict priority fashion for transmission over-the-air as per the priority level from high to low.

Avoiding Narrow Band Radio Traffic Overloading

The Aprisa FE 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 PTP radio link. 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 PTP radio links. Traffic with double VLANs which are not destined to a PTP link will be discarded on the ingress of the radio link, avoiding the overload of the radio PTP link.

Single VLAN (Bridge Mode)

Single VLAN is used to distinguish/segregate between different traffic types assigned by the user in its industrial corporate LAN. In order to avoid the overload of the radio link, traffic with single VLANs which are not destined to a specific radio network will be discarded on the Ethernet ingress port of the radio link. 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 prioritize critical mission traffic and ensure critical 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 FE (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 FE 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 management priority and rate in order to control the traffic load of the radio network, where important and high priority data will pass-through first. The user can set the use of the Ethernet Data Priority, which controls the priority of the Ethernet customer traffic relative to the management 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 link. 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 FE supports ROHC v2 (Robust Header Compression v2 RFC4995, RFC5225, RFC4996, RFC3843, RFC4815). ROHC v2 is a standard way to compress IP, UDP and TCP headers and this significantly increases IP traffic throughput especially in narrow band network.

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

Interfaces

Antenna Interface

- N type 50 ohm, female connector

Ethernet Interface

- 4 ports 10/100 base-T Ethernet layer 2 switch using RJ45
Used for Ethernet user traffic and radio sub-network management.

USB Interfaces

- 1 x Management port using USB micro type B connector
Used for product configuration with the Command Line Interface (CLI).
- 1 x Host port using USB standard type A connector
Used for software upgrade and diagnostic reporting.

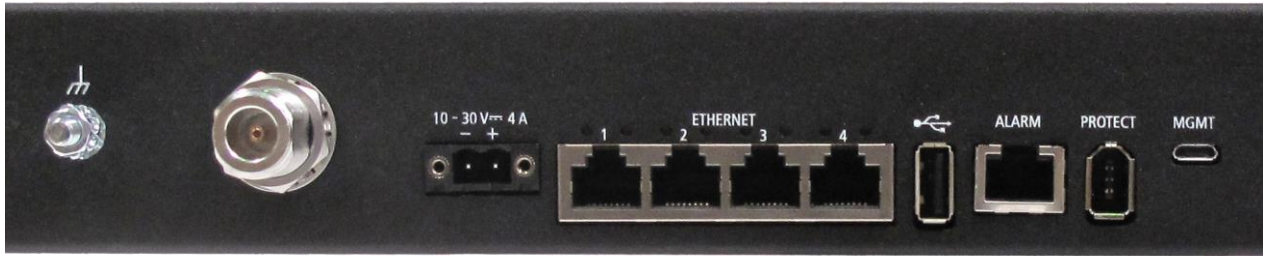
Protect Interface

- 1x Protect interface port
Used for the Protected Station operation (future option).


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



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

Designator	Description
Safety Earth Stud	An M5 stud for connection to an external protection ground. See ‘Earthing and Lightning Protection’ on page 42.
N Type Antenna	N type 50 ohm female connector for the antenna connection. See ‘Coaxial Feeder Cables’ on page 40.
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 45.
ETHERNET 1 to 4	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 86.
	Host Port using a USB standard type A connector. Used for software upgrade and diagnostic reporting. See ‘Software Upgrade’ on page 290 and ‘Maintenance > General’ on page 147.
ALARM	Alarm Port using a RJ45 connector. Used for two alarm inputs and two alarm outputs. See ‘Hardware Alarms Interface’ on page 317.
PROTECT	Protect port. Used for Protected Station operation.
MGMT	Management Port using a USB micro type B connector. Used for product configuration with the Command Line Interface. See ‘Connecting to the Management Port’ on page 264.

LED Display Panel

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

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 USB to MODE LEDs
- Software upgrade completed successfully - the OK LED solid green
- Software upgrade failed - any LED flashing red during the upgrade

Link Software Upgrade

During a link software upgrade, the MODE LED flashes orange on the local radio and the remote radio.

Test Mode

All 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 150 for Test Mode options).

To enter Test Mode, press and hold the RSSI button on the radio front 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 RSSI 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 FE contains an embedded web server application (SuperVisor) to enable element management with any major web browser (such as Mozilla Firefox or Microsoft® Internet Explorer).

SuperVisor enables operators to configure and manage the local radio and remote radio over the radio link.

The key features of SuperVisor are:

- Full element management, configuration and diagnostics
- Manage the local and remote radio (remote management)
- Managed link software distribution and upgrades
- Performance and alarm monitoring of the link, including RSSI, alarm states, time-stamped events, etc.
- View and set standard radio configuration parameters including frequencies, transmit power, channel access, Ethernet port settings
- Set and view security parameters
- User management
- Operates over a secure HTTPS session

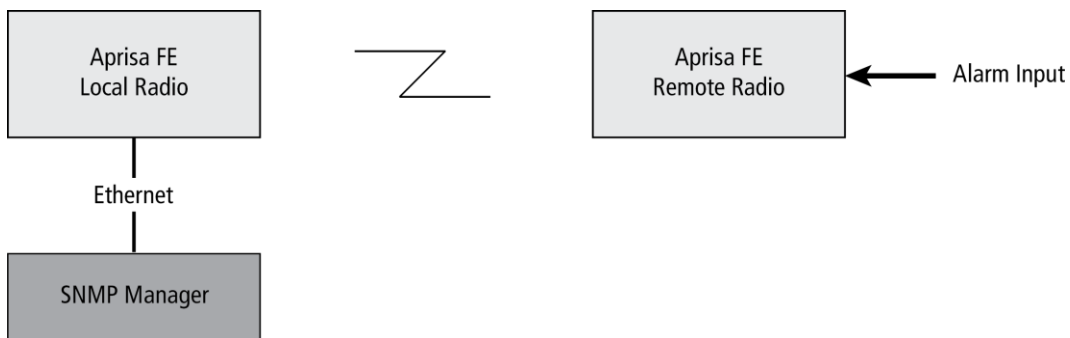
Hardware Alarm Inputs / Outputs

The Aprisa FE 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 160). These include the alarm events generated by the hardware alarm inputs.

Alarm Input to SNMP Trap

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



Alarm Input to Alarm Output

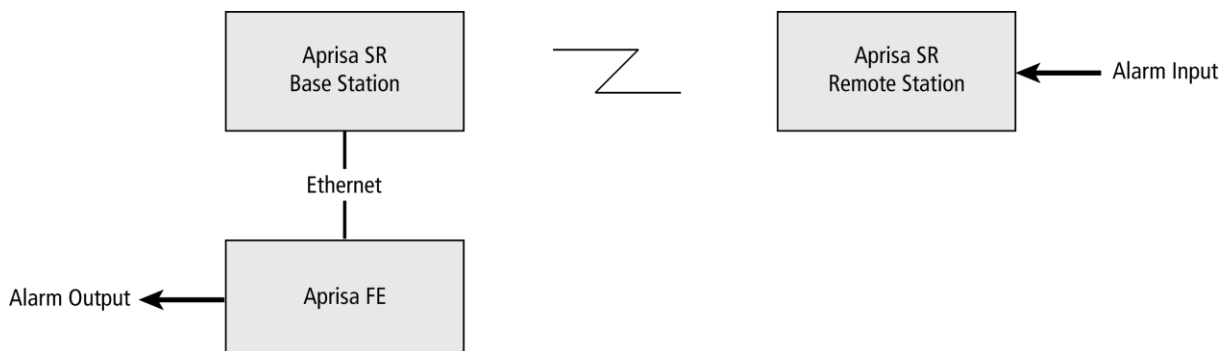
An alarm event from an Aprisa FE hardware alarm input can be mapped to an hardware alarm output of another FE using an event action setup (see ‘Events > Event Action Setup’ on page 168).



Aprisa SR Alarm Input to Aprisa FE Alarm Output

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

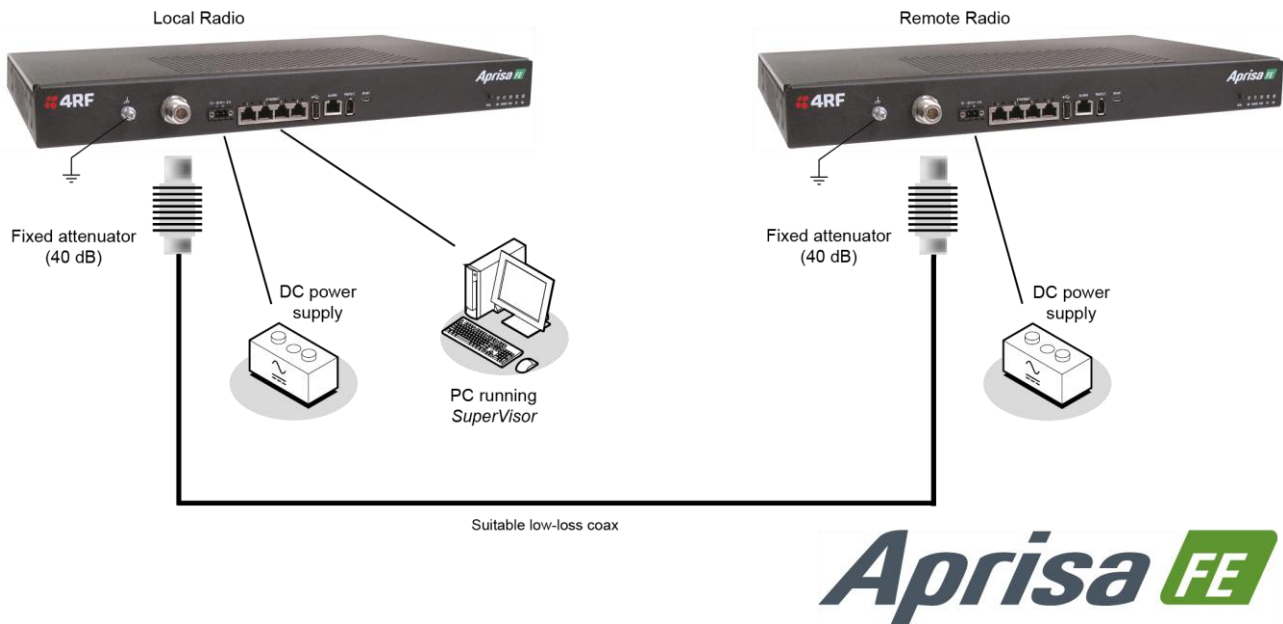
Since, the Aprisa SR only supports hardware alarm inputs, the Aprisa FE can be used as an option to provide a hardware alarm output. As shown in the figure below, an Aprisa FE connected on the same IP network of the Aprisa SR, alarm events from the SR hardware alarm input can be mapped to the hardware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



4. Preparation

Bench Setup

Before installing the links in the field, it is recommended that you bench-test the radios. 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.

Cables

Use double-screened coaxial cable that is suitable for use up to 1 GHz at \approx 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

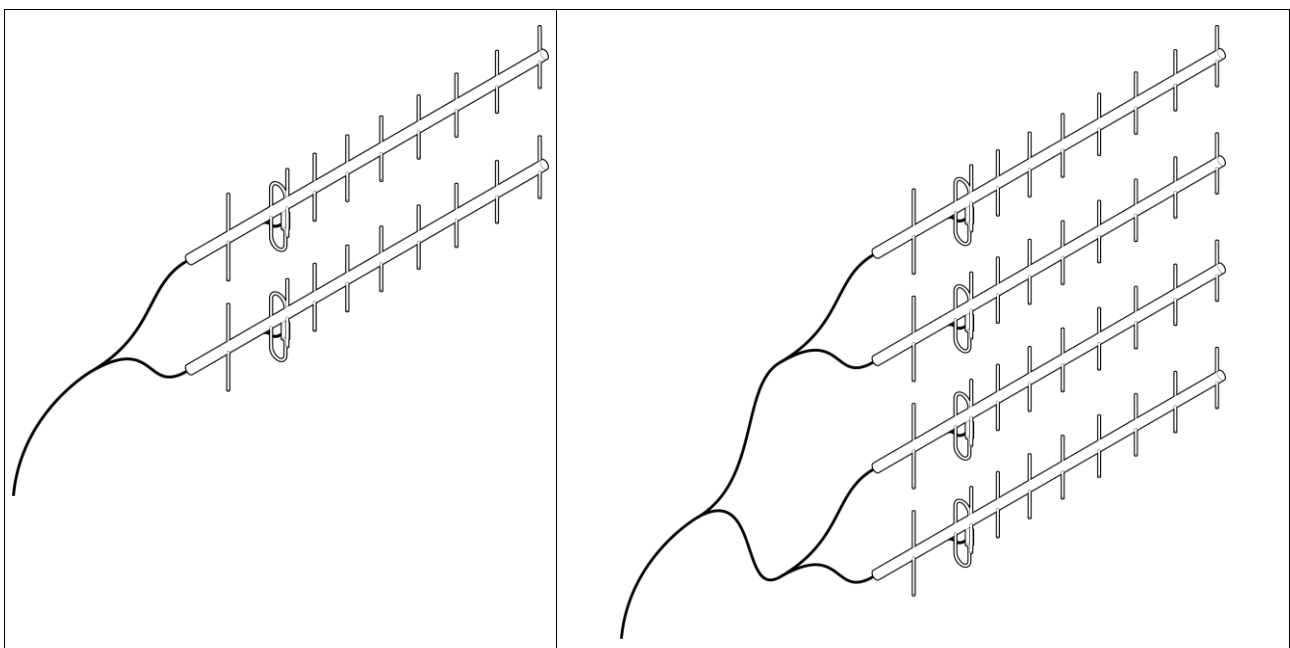
Selecting and siting antennas are important considerations in your system design. The antenna choice for the site is determined primarily by the frequency of operation and the gain required to establish reliable links.

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

Yagi Antennas

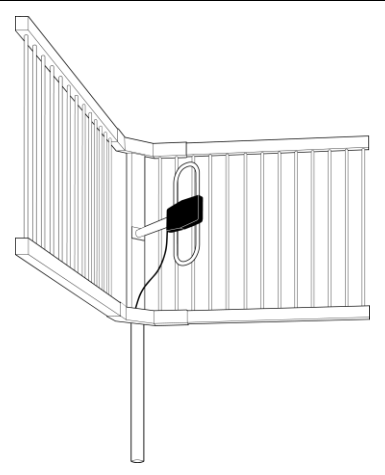
	Factor	Explanation
	Frequency	Often used in 350-600 MHz bands
	Gain	Varies with size (typically 11 dBi to 16 dBi)
	Stackable gain increase	2 Yagi antennas (+ 2.8 dB) 4 Yagi antennas (+ 5.6 dB)
	Size	Range from 0.6 m to 3 m in length
	Front to back ratio	Low (typically 18 to 20 dB)

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



Example of stacked antennas

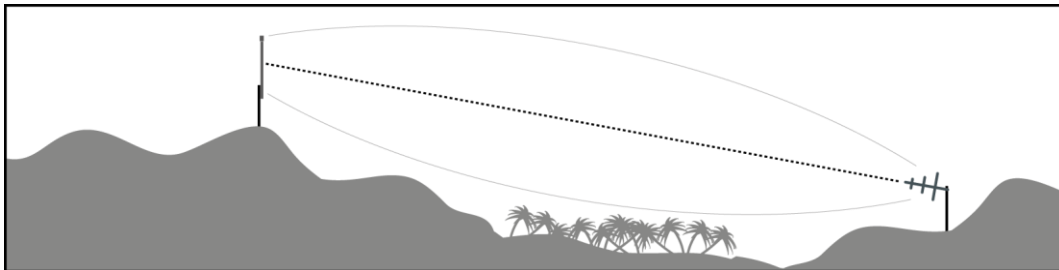
Corner Reflector Antennas

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

Antenna Siting

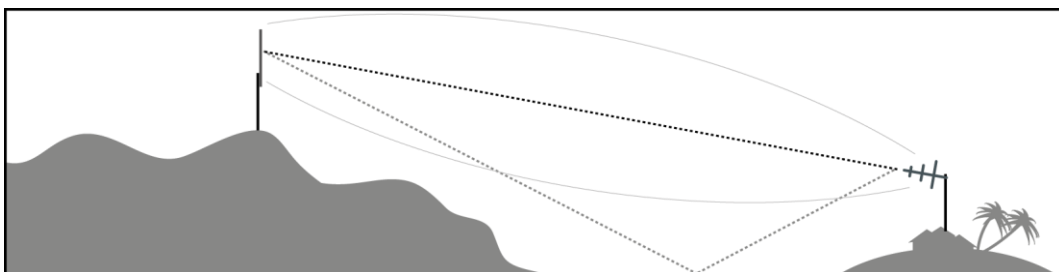
When siting antennas, consider the following points:

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



Example of a clear line-of-sight path

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



Example of a mid-path reflection path

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

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

Coaxial Feeder Cables

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

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

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

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

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

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

When running cables:

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

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

Linking System Plan

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

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

Site Requirements

Power Supply

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

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



WARNING:

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

Equipment Cooling

If the Aprisa FE is operated in an environment where the ambient temperature exceeds 40°C, the convection air flow over the enclosure must be considered.

The environmental operating conditions are as follows:

Operating temperature	-40 to +60° C
Storage temperature	-40 to +80° C
Humidity	Maximum 95% non-condensing



WARNING:

If the Aprisa FE is operated in an environment where the ambient temperature exceeds 40°C, the Aprisa FE must be installed within a restricted access location to prevent human contact with the enclosure.

Earthing and Lightning Protection



WARNING:

Lightning can easily damage electronic equipment.

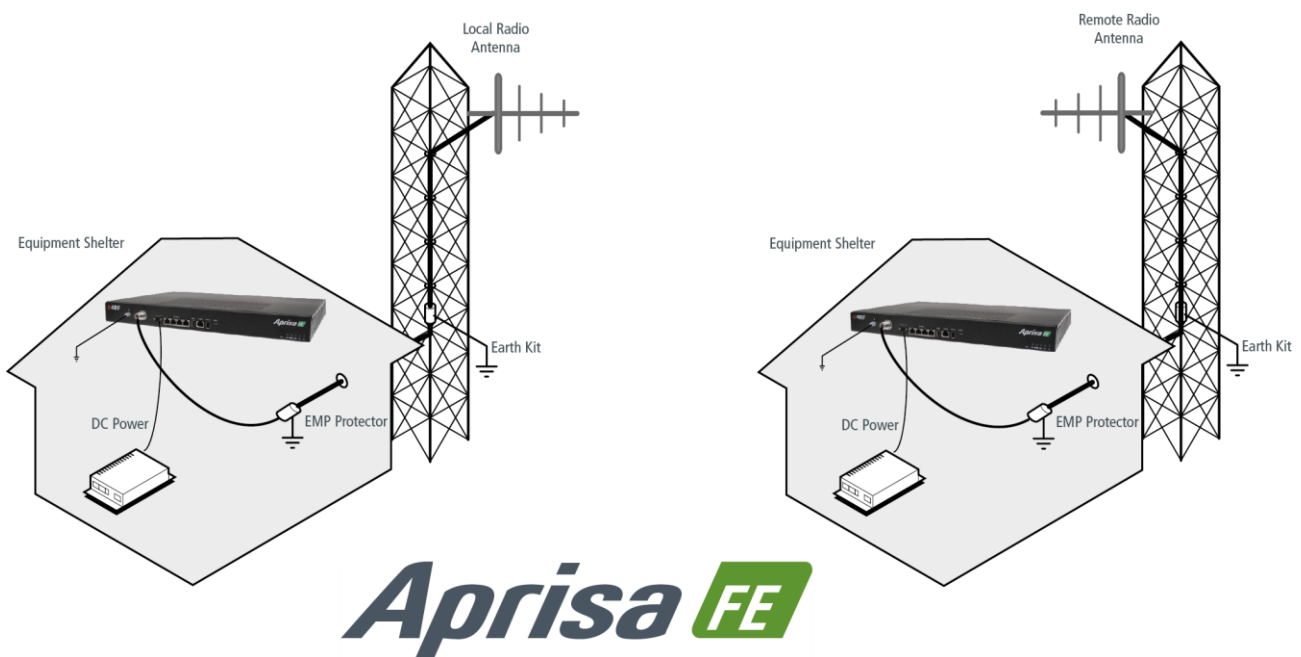
To avoid this risk, install primary lightning protection devices on any interfaces that are reticulated in the local cable network.

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

Feeder Earthing

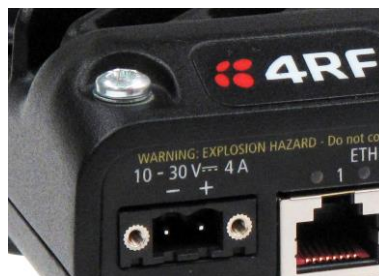
Earth the antenna tower, feeders and lightning protection devices in accordance with the appropriate local and national standards. The diagram below shows the minimum requirements.

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



Radio Earthing

The Aprisa FE has an M5 stud earth connection point on the left front of the enclosure to earth the enclosure to a protection earth.



5. Installing the Radio



CAUTION:

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

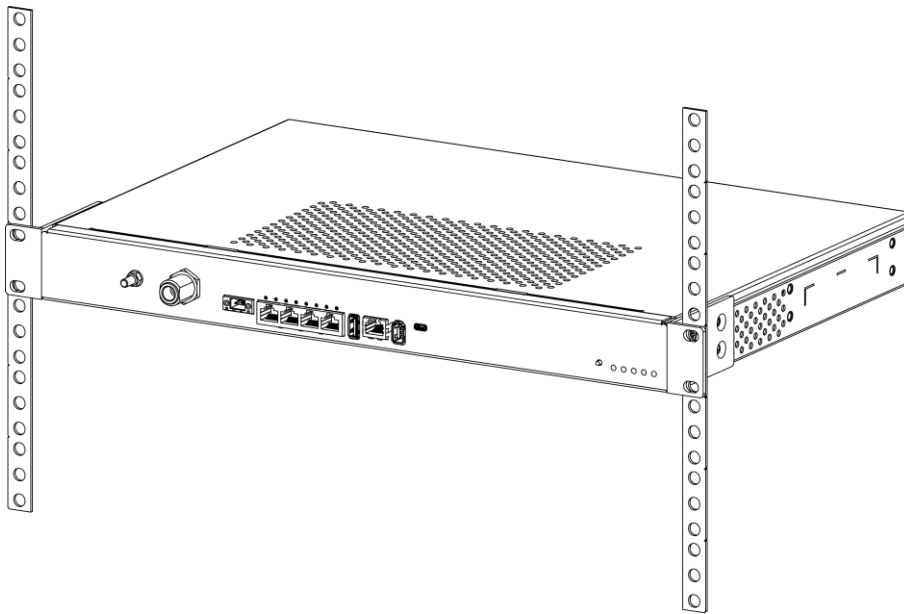
4RF does not assume any liability for failure to comply with these precautions.

Mounting

The Aprisa FE is designed to be rack mounted in a standard 19" rack.

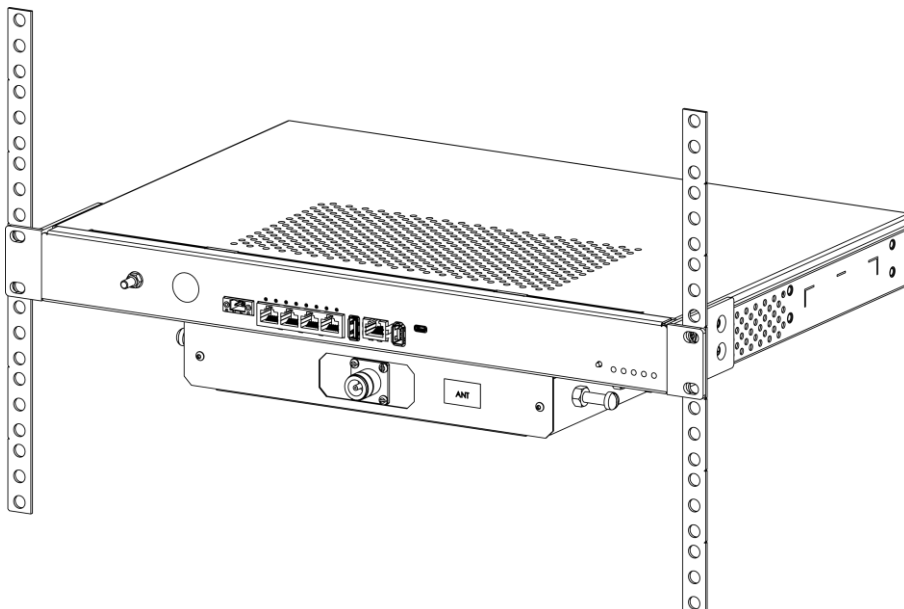
Internal Duplexer

When the duplexer mounts internally, the space required is 1U.



External Duplexer

When the duplexer mounts externally, the rack space required is 2U.



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 42).



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.

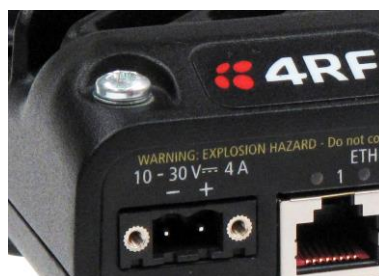
Connect the antenna and feeder cable. Weatherproof the connection with a boot, tape or other approved method.

The Aprisa FE antenna connection is an N type female connector so the feeder / jumper must be fitted with a N type 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 FE has an M5 stud earth connection point on the left front of the enclosure to earth the enclosure to a protection earth.



Connecting the Power Supply

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

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



The negative supply of the Aprisa FE power connection is internally connected to the Aprisa FE 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
APFS-CML2-FEM-01	4RF FE 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 USB LEDs will light green, the TX and RX LEDs will flash red.
- The Aprisa FE radio is ready to operate
- The TX and RX LEDs will be green (steady or flashing) when the radio is registered with the other radio.

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

Spare fuses are contained within the radio, see 'Spare Fuses' on page 46 for instructions on how to locate and replace the fuses.

External Power Supplies

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

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

Spare Fuses

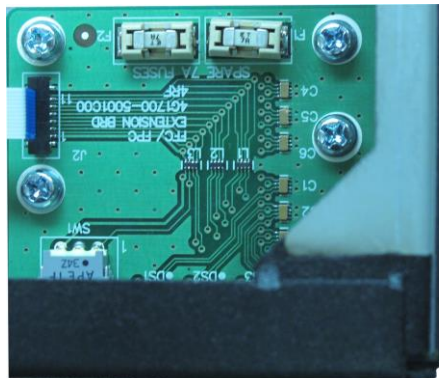
The Aprisa FE PBA contains two fuses in the power input with designators F1 and F2. Both the positive and negative power connections are fused. The fuse type is a Littelfuse 0454007 with a rating of 7 A, 125 V, very fast acting.

To replace the fuses:

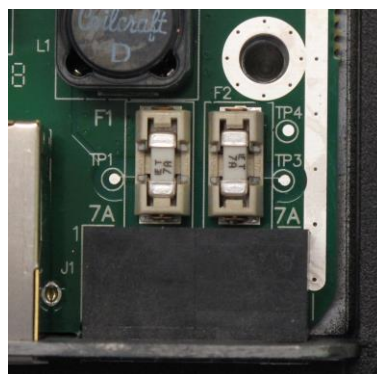
1. Remove the input power, antenna cable and all interface cables.
2. Unscrew the FE chassis lid securing screws at the rear edge of the lid.
3. Unscrew the radio from the FE chassis.

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

4. Remove the spare fuses on the small PBA at the right front of the chassis.



5. Replace the two fuses on the FE board.



6. Refit the radio to the FE chassis and tighten the screws.
7. Refit the FE chassis lid and tighten the lid securing screws at the rear edge of the lid.

Additional Spare Fuses

Additional spare fuses can be ordered from 4RF:

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

6. Managing the Radio

SuperVisor

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

SuperVisor enables operators to configure and manage the local radio and remote radio over the radio link.

The key features of SuperVisor are:

- Full element management, configuration and diagnostics
- Manage the local and remote radio (remote management)
- Managed link software distribution and upgrades
- Performance and alarm monitoring of the link, including RSSI, alarm states, time-stamped events, etc.
- View and set standard radio configuration parameters including frequencies, transmit power, and Ethernet port settings
- Set and view security parameters
- User management
- Operates over a secure HTTPS session

PC Requirements for SuperVisor

SuperVisor requires the following minimum PC requirements:

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

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

Connecting to SuperVisor

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

The Aprisa FE 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.

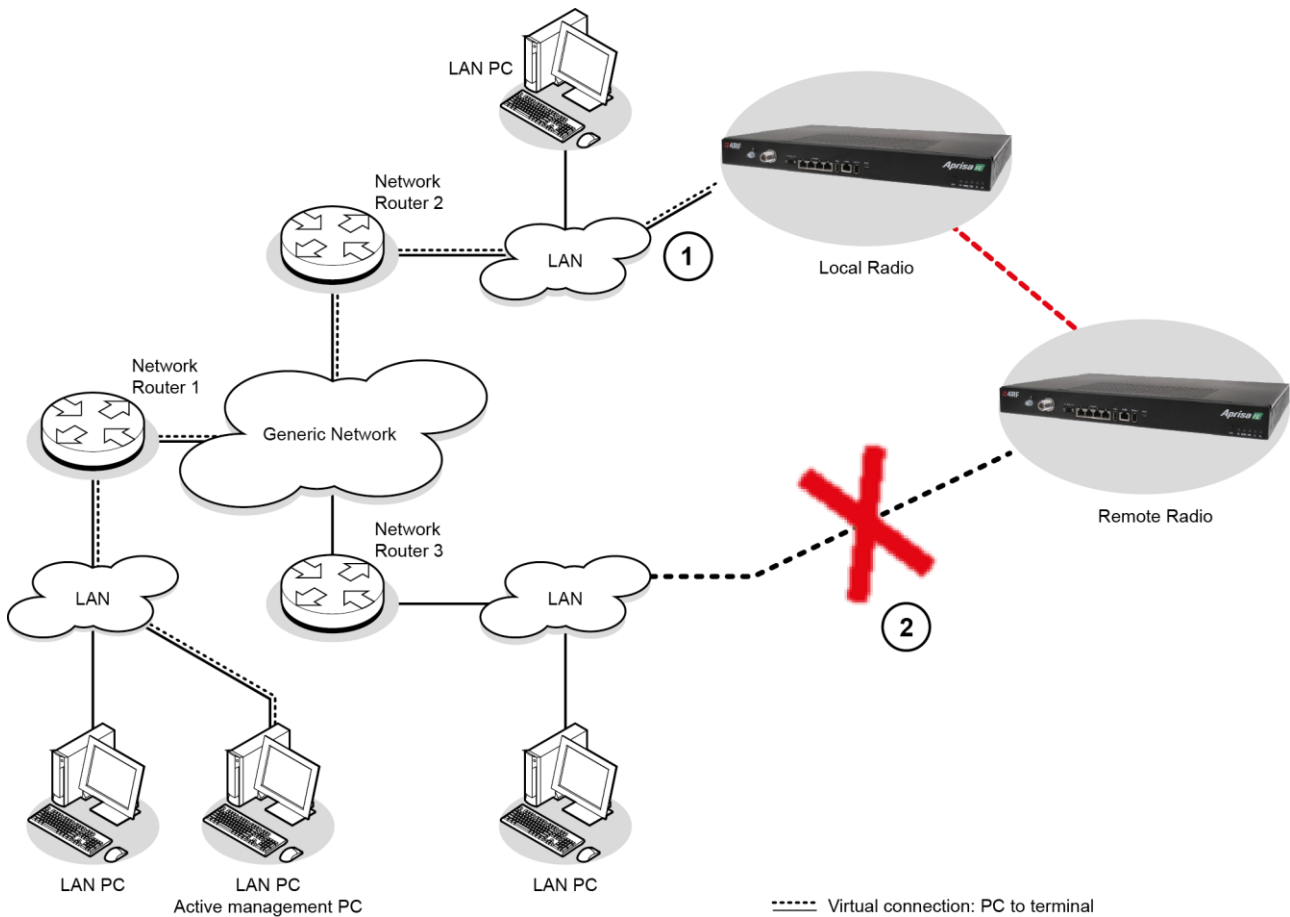
The Aprisa FE Protected Station radio A has a factory default IP address of 169.254.50.10 and radio B (right radio) has a factory default IP address of 169.254.50.20, both with a subnet mask of 255.255.0.0.

To change the Aprisa FE 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 FE Ethernet ports.
3. Open a browser and enter `http://169.254.50.10`.
4. Login to the radio with the default Username 'admin' and Password 'admin'.
5. Change the IP address to conform to the network plan in use.

Management PC Connection

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



When logging into a network, it is important to understand the relationship between the local radio and the remote radio. The local radio is the radio that your IP network is physically connected to.

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.

If ICMP is enabled on the local radio, the user will also be able to ping the local radio to confirm the connectivity.

PC Settings for SuperVisor

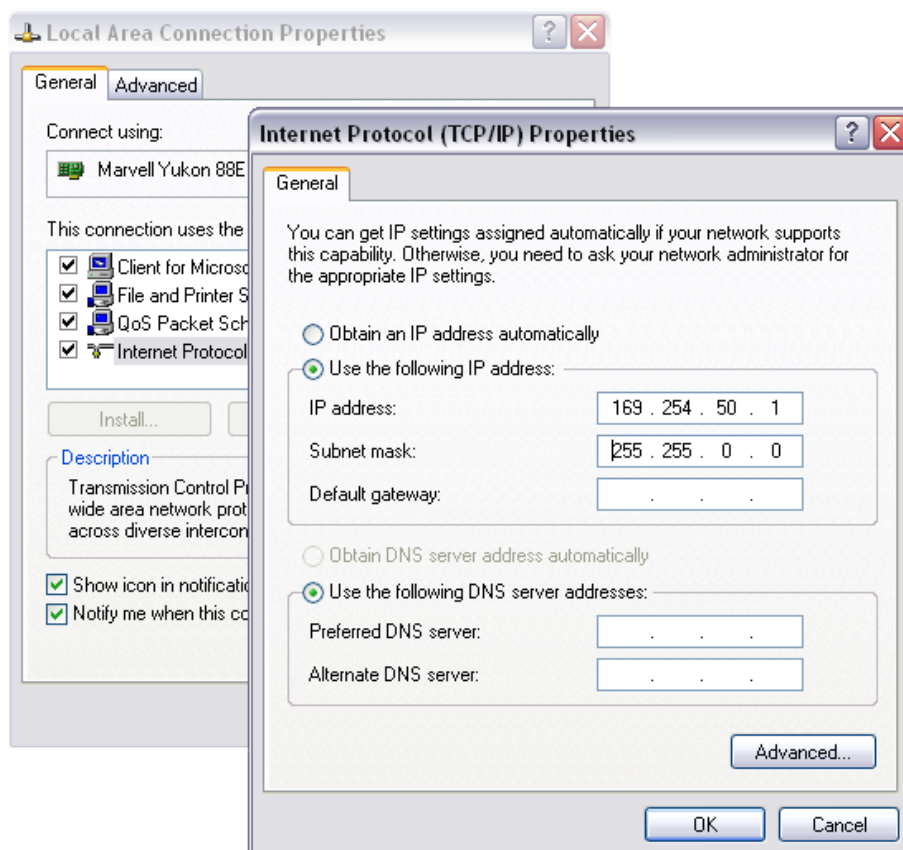
To change the PC IP address:

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

Windows XP example:

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

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

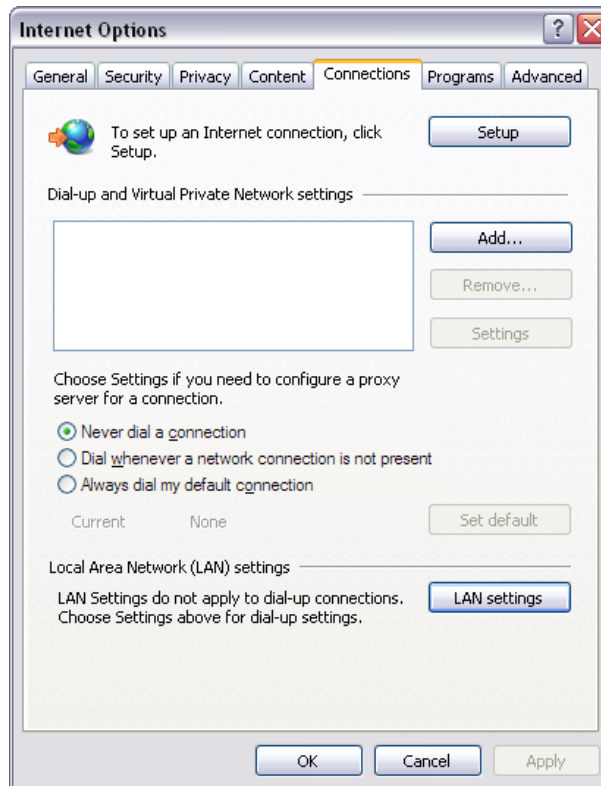


To change the PC connection type:

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

Windows Internet Explorer 8 example:

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

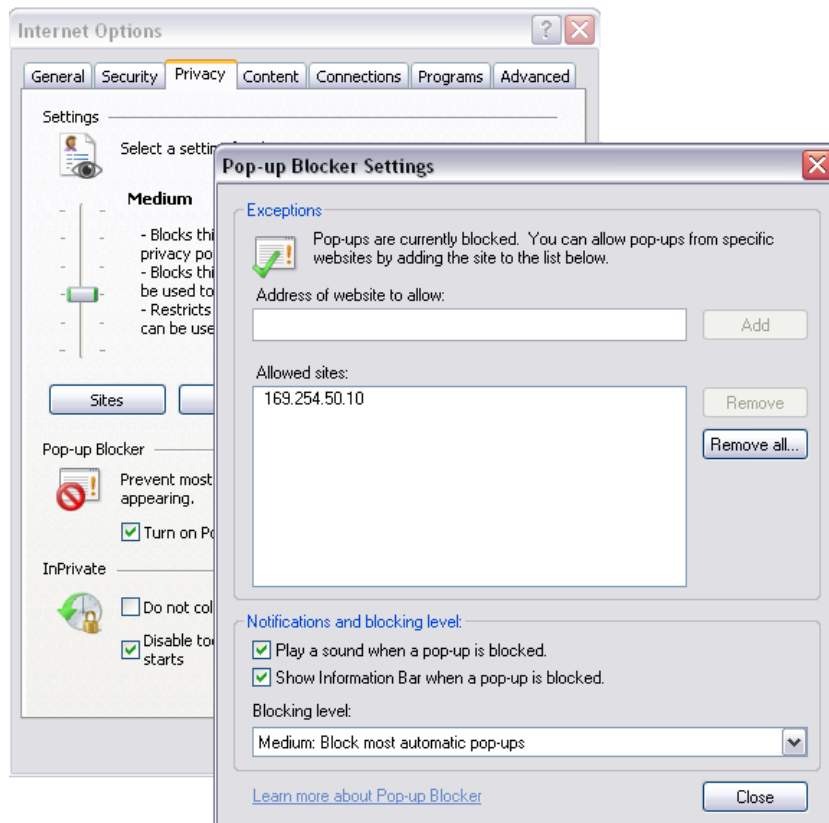


To change the PC pop-up status:

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

Windows Internet Explorer 8 example:

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

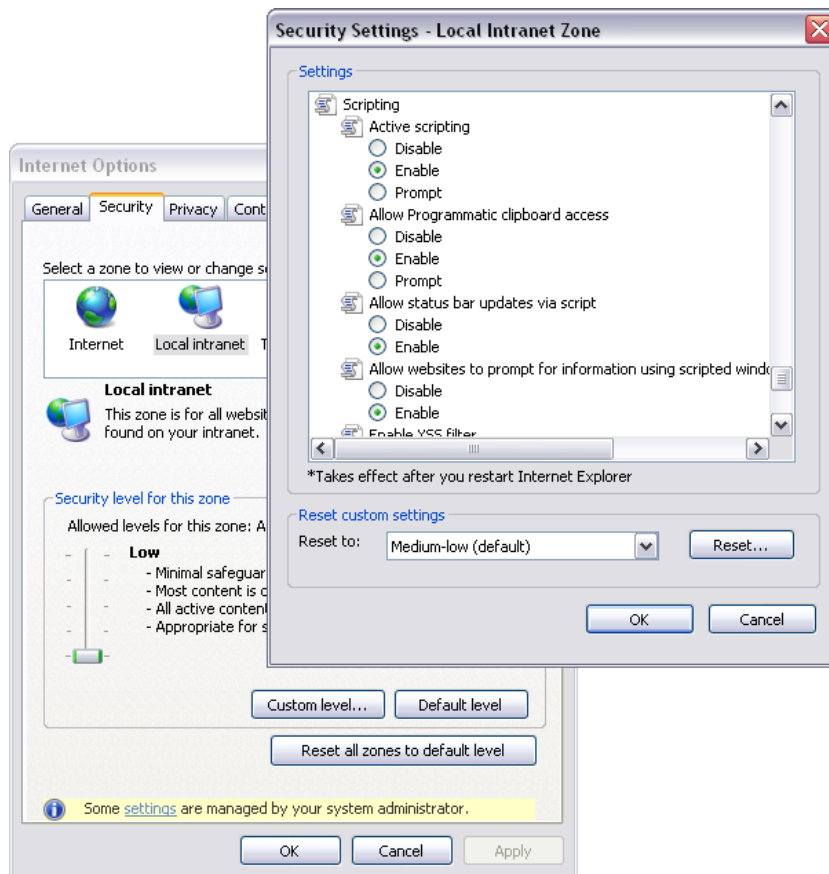


To enable JavaScript in the web browser:

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

Windows Internet Explorer 8 example:

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



Login to SuperVisor

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

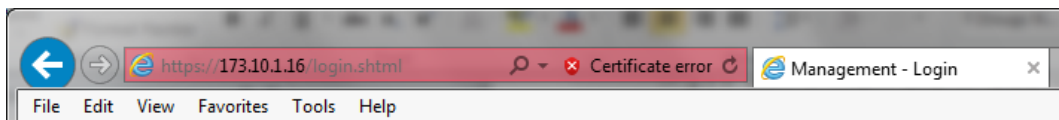
If SuperVisor is inactive for a period defined by the Inactivity Timeout option (see ‘Maintenance > General’ on page 147), the radio will automatically logout the user.

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.

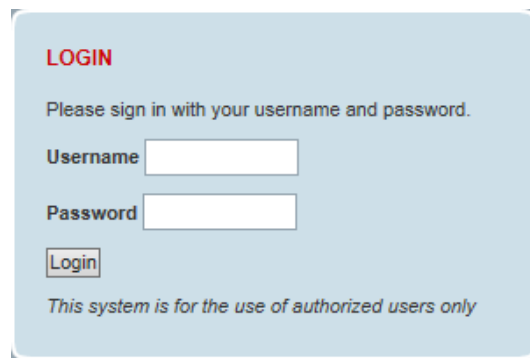
If you don’t know the IP address of the radio, you can determine it using the Command Line Interface (see ‘Command Line Interface’ on page 264).



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

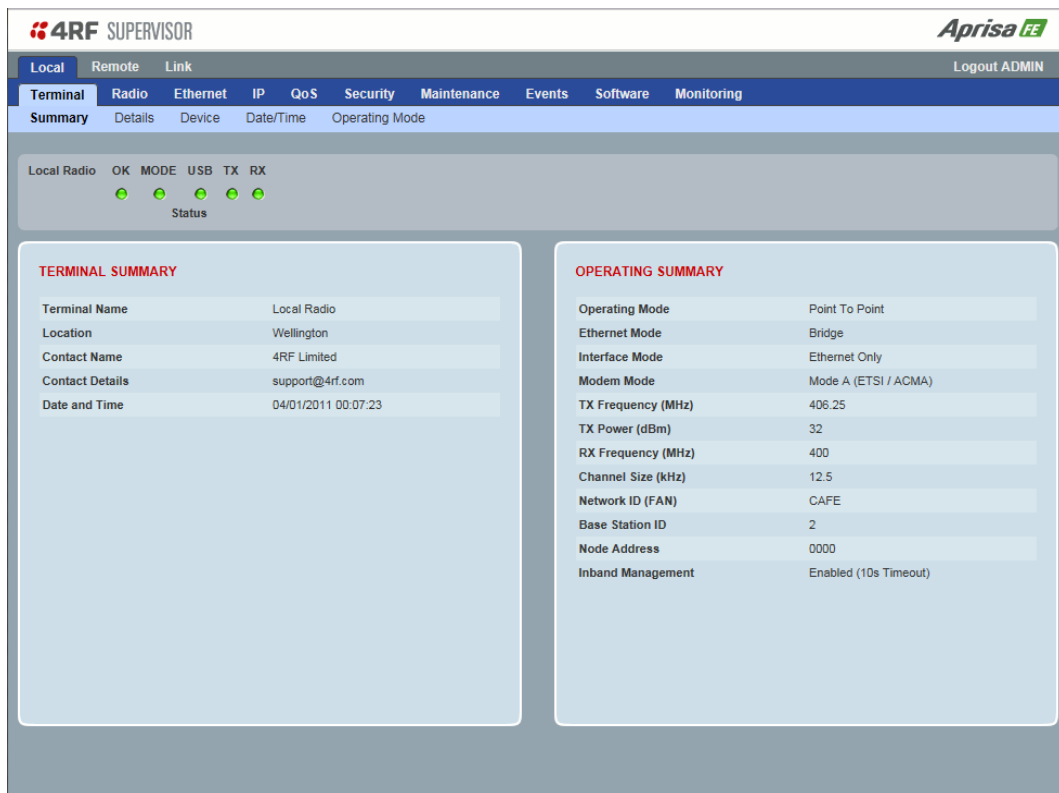
2. Login with the Username and Password assigned to you.

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

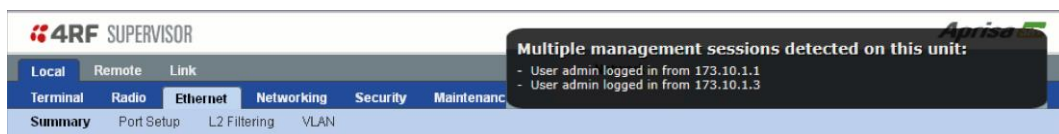


Important: After you login for the very first time, it is recommended that you change the default admin password for security reasons (see ‘Changing Passwords’ on page 133).

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



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



Logout of SuperVisor

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

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

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

To logout of SuperVisor:

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

SuperVisor Page Layout

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

The screenshot shows the SuperVisor web interface with the following components labeled:

- Branding Bar:** Located at the top, containing the 4RF SUPERVISOR logo on the left and the Aprisa FE logo on the right.
- Control Bar:** A horizontal bar below the branding bar with tabs for Local, Remote, and Link. The 'Radio' tab is selected and highlighted in red.
- Level 1 Menu:** A row of menu items including Terminal, Radio, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring.
- Level 2 Menu:** A row of sub-menu items including Summary, Details, Device, Date/Time, and Operating Mode.
- Alarm Bar:** A status bar showing 'Local Radio' with indicators for OK, MODE, USB, TX, and RX, and a 'Status' label.
- Task Window:** A window titled 'TERMINAL SUMMARY' containing a table of terminal information.
- Operating Summary:** A window titled 'OPERATING SUMMARY' containing a table of radio configuration parameters.
- Main Window Frame:** The overall container for the terminal and operating summary windows.

Field	Value
Terminal Name	Local Radio
Location	Wellington
Contact Name	4RF Limited
Contact Details	support@4rf.com
Date and Time	01/01/2011 15:02:45

Field	Value
Operating Mode	Point To Point
Ethernet Mode	Bridge
Interface Mode	Ethernet Only
Modem Mode	Mode A (ETSI / ACMA)
TX Frequency (MHz)	406.25
TX Power (dBm)	32
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

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.

SuperVisor Menu

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

Local / remote radios	Link
Terminal	Details
Radio	Configuration
Ethernet	Monitoring
IP	
QoS	
Security	
Maintenance	
Events	
Software	
Monitoring	

SuperVisor Parameter Settings

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

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

SuperVisor Menu Access

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

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

Local and remote radio Menu Items

Menu Item	View	Technician	Engineer	Admin
Terminal > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Terminal > Details	Read-Only	Read-Only	Read-Only	Read-Only
Terminal > Device	No Access	Read-Write	Read-Write	Read-Write
Terminal > Date / Time	Read-Only	Read-Only	Read-Only	Read-Only
Terminal > Operating Mode	No Access	Read-Write	Read-Write	Read-Write
Radio > Radio Summary	Read-Only	Read-Only	Read-Only	Read-Only
Radio > Channel Summary	Read-Only	Read-Only	Read-Only	Read-Only
Radio > Radio Setup	No Access	Read-Write	Read-Write	Read-Write
Radio > Channel Setup	No Access	Read-Write	Read-Write	Read-Write
Radio > Advanced Setup	No Access	Read-Write	Read-Write	Read-Write
Ethernet > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Ethernet > Port Setup	No Access	Read-Write	Read-Write	Read-Write
Ethernet > L2 Filtering	No Access	No Access	Read-Write	Read-Write
Ethernet > VLAN	No Access	No Access	Read-Write	Read-Write
IP > IP Summary	Read-Only	Read-Only	Read-Only	Read-Only
IP > IP Setup	No Access	Read-Write	Read-Write	Read-Write
IP > L3 Filtering	No Access	No Access	Read-Write	Read-Write
IP > IP Routes	No Access	No Access	Read-Write	Read-Write
QoS > Summary	Read-Only	Read-Only	Read-Only	Read-Only
QoS > Traffic Priority	No Access	No Access	Read-Write	Read-Write
QoS > Traffic Classification	No Access	No Access	Read-Write	Read-Write
Security > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Security > Setup	No Access	No Access	Read-Write	Read-Write
Security > Users	No Access	No Access	No Access	Read-Write
Security > SNMP	No Access	No Access	No Access	Read-Write
Security > RADIUS	No Access	No Access	Read-Write	Read-Write
Security > Manager	No Access	No Access	Read-Write	Read-Write
Security > Distribution	No Access	No Access	Read-Write	Read-Write
Maintenance > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Maintenance > General	No Access	Read-Write	Read-Write	Read-Write
Maintenance > Test Mode	No Access	Read-Write	Read-Write	Read-Write
Maintenance > Defaults	No Access	No Access	No Access	Read-Write
Maintenance > Protection	No Access	Read-Write	Read-Write	Read-Write
Maintenance > Licence	No Access	No Access	Read-Write	Read-Write
Maintenance > Advanced	No Access	No Access	Read-Write	Read-Write
Events > Alarm Summary	Read-Only	Read-Only	Read-Only	Read-Only
Events > Event History	Read-Only	Read-Only	Read-Only	Read-Only

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

Link Menu Items

Menu Item	View	Technician	Engineer	Admin
Details > Summary	Read-Only	Read-Only	Read-Only	Read-Only
Details > Radio	Read-Only	Read-Only	Read-Only	Read-Only
Details > Events	Read-Only	Read-Only	Read-Only	Read-Only
Configuration > Radio Setup	No Access	Read-Write	Read-Write	Read-Write
Configuration > Channel Setup	No Access	Read-Write	Read-Write	Read-Write
Monitoring > Terminal	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Ethernet	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > Radio	Read-Only	Read-Only	Read-Only	Read-Only
Monitoring > User Selected	Read-Only	Read-Only	Read-Only	Read-Only

SuperVisor Menu Items

As SuperVisor screens are dependent on the Aprisa FE 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

The screenshot shows the 4RF SUPERVISOR interface. At the top, there are tabs for 'Local', 'Remote', and 'Link', and a 'Logout ADMIN' link. Below this is a main navigation menu with categories like 'Terminal', 'Radio', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. Under the 'Terminal' category, there are sub-tabs for 'Summary', 'Details', 'Device', 'Date/Time', and 'Operating Mode'. The 'Summary' tab is active.

Below the navigation, there is a 'Local Radio' status section with indicators for 'OK', 'MODE', 'USB', 'TX', and 'RX', all of which are green. Below this are two summary tables:

TERMINAL SUMMARY	
Terminal Name	Local Radio
Location	Wellington
Contact Name	4RF Limited
Contact Details	support@4rf.com
Date and Time	04/01/2011 00:07:23

OPERATING SUMMARY	
Operating Mode	Point To Point
Ethernet Mode	Bridge
Interface Mode	Ethernet Only
Modem Mode	Mode A (ETSI / ACMA)
TX Frequency (MHz)	406.25
TX Power (dBm)	32
RX Frequency (MHz)	400
Channel Size (kHz)	12.5
Network ID (FAN)	CAFE
Base Station ID	2
Node Address	0000
Inband Management	Enabled (10s Timeout)

TERMINAL SUMMARY

This page displays the current settings for the Terminal parameters. See 'Terminal > Details' on page 65, 'Terminal > Device' on page 67 and 'Terminal > Operating Mode' on page 71 for setting details.

OPERATING SUMMARY

Operating Mode

This parameter displays the current Operating Mode i.e. if the radio is operating in Bridge Mode or Router Mode.

Interface Mode

This parameter displays the Interfaces available for traffic on the radio. The Aprisa FE traffic interface is Ethernet. For Ethernet availability on the radio see 'Maintenance > Licence' on page 154.

Modem Mode

This parameter displays the modem mode selected e.g. Mode A ETSI 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 Width (kHz)

This parameter displays the current Channel Width in kHz.

Network ID

This parameter is the network ID of this radio. Both the local and remote radio must be set to the same network ID. The entry is four hex chars (not case sensitive).

Node Address

The Node Address of a point-to-point FE is always 0000.

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 local radio waits for a response from the remote radio before aborting the Inband Management request.

Terminal > Details

The screenshot shows the 4RF SUPERVISOR web interface. At the top, there are tabs for 'Local', 'Remote', and 'Link'. Below that, a navigation menu includes 'Terminal', 'Radio', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. Under 'Terminal', there are sub-tabs for 'Summary', 'Details', 'Device', 'Date/Time', and 'Operating Mode'. The 'Details' tab is active, showing a 'Local Radio' status section with indicators for 'OK', 'MODE', 'USB', 'TX', and 'RX', all of which are green. Below this is a 'MANUFACTURING DETAILS' section with the following data:

Radio Serial Number	R1310000601
Sub-Assembly Serial Number	13092717
HW Frequency Band	400 - 470MHz
HW Type	A
Ethernet Port 1 MAC Address	00:22:b2:10:0b:76
Ethernet Port 2 MAC Address	00:22:b2:10:0b:77
Ethernet Port 3 MAC Address	00:22:b2:10:0b:78
Ethernet Port 4 MAC Address	00:22:b2:10:0b:79
Active Software Version	1.5.0
Previous Software Version	1.5.0

MANUFACTURING DETAILS

Radio Serial Number

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


Sub-Assembly Serial Number

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



HW Frequency Band

This parameter displays the hardware radio frequency operating range.

HW Type

This parameter displays the hardware board assembly type.

Radio MAC Address

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

Active Software Version

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

Previous Software Version

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

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

Terminal > Device

4RF SUPERVISOR Aprisa FE

Local Remote Link Logout ADMIN

Terminal Radio Ethernet IP QoS Security Maintenance Events Software Monitoring

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

Local Radio OK MODE USB TX RX
Status

TERMINAL DETAILS

Terminal Name

Location

Contact Name

Contact Details

REGION SETTINGS

Time Format 12 Hour (AM/PM) 24 Hour

Date Format MM/DD/YYYY DD/MM/YYYY

Measurement System US Metric

RF NETWORK DETAILS

Network ID (FAN)

Base Station ID

Inband Management

Inband Management Timeout (s)

TERMINAL DETAILS

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



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

RF NETWORK DETAILS

Network ID (network)

This parameter sets the network ID of the local and remote radio. The entry is four hexadecimal chars (not case sensitive).

The default setting is CAFE.

Inband Management

This parameter sets the Inband Management option.

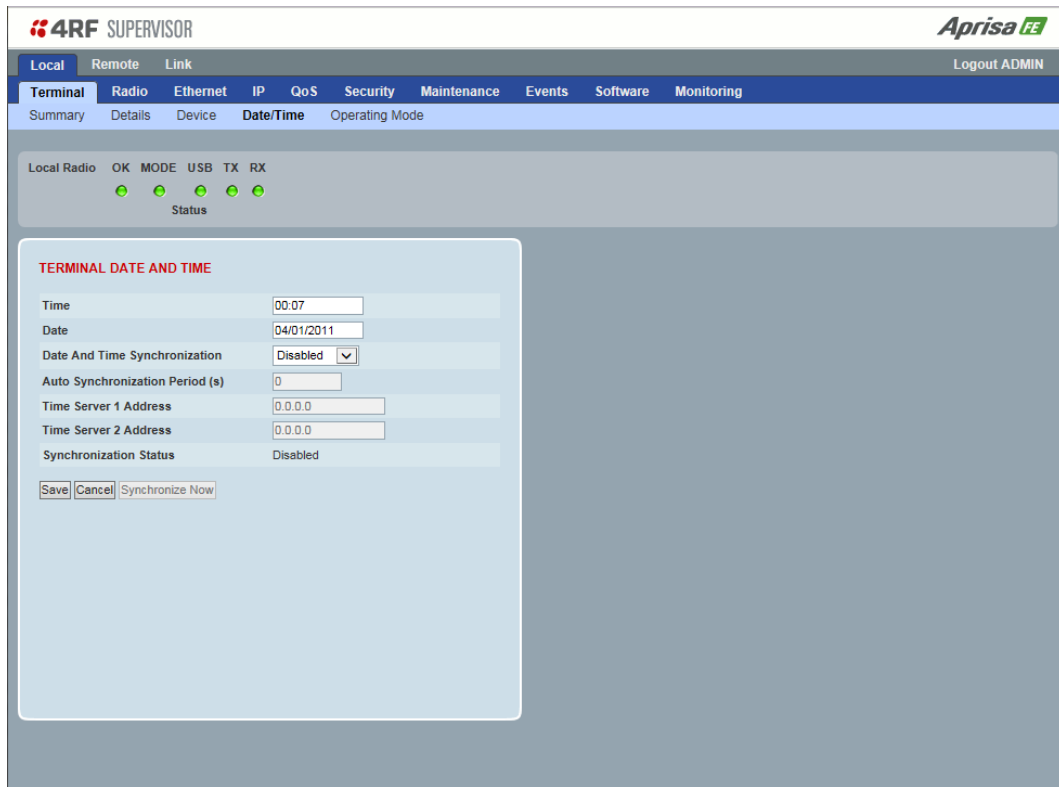
If the Inband Management option is enabled, SuperVisor operating on a local radio can also manage the remote radio.

Inband Management Timeout (sec)

This parameter sets the Inband Management timeout period. This determines the time that the local radio waits for a response from the remote radio before aborting the Inband Management request.

The default setting is 10 seconds.

Terminal > Date / Time



TERMINAL DATE AND TIME

Set the Time Format, Time, Date Format and Date. This information is controlled from a software clock.

Date and Time Synchronization

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

Using the SNTP feature will ensure that both radios have the same date and time required for accurate network diagnostics.

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

The default setting is Disabled.

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

When SNTP is enabled on a radio, it periodically sends a broadcast message to the other link radio to synchronize the radio date and time.

Auto Synchronization Period (s)

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

Time Server 1 Address

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

Time Server 2 Address

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

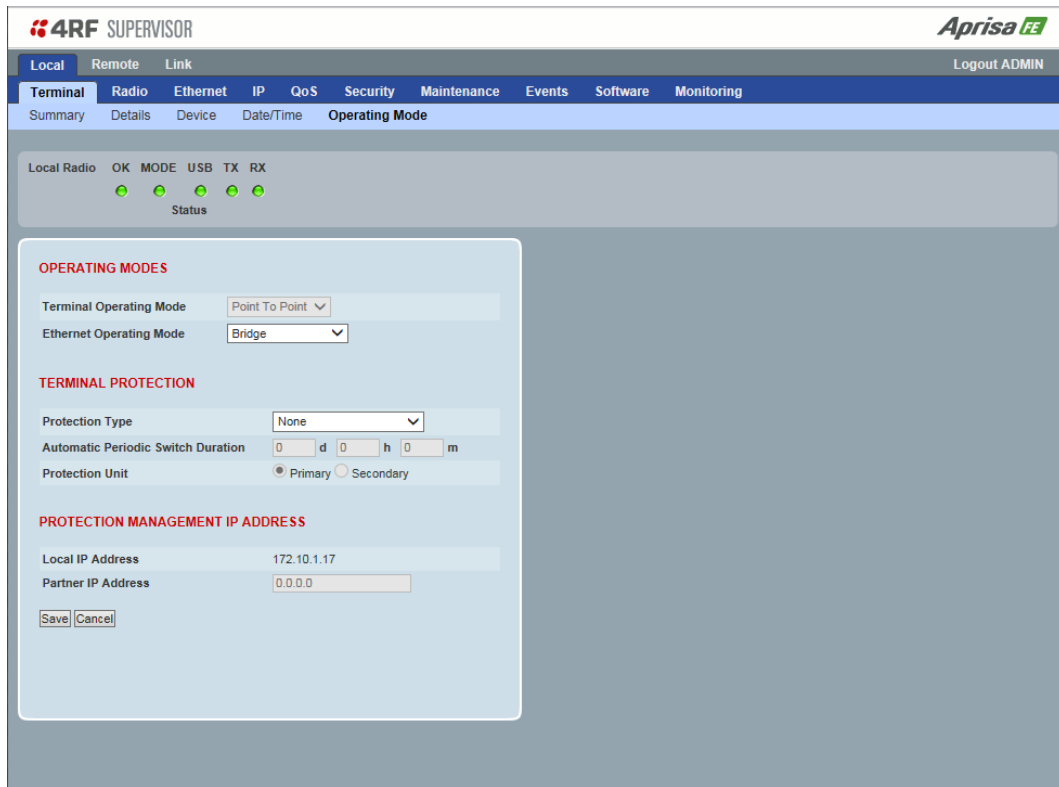
Synchronization Status

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

Synchronize Now

This Synchronize Now button provides manual Synchronization.

Terminal > Operating Mode


OPERATING MODES
Terminal Operating Mode

The Terminal Operating Mode is fixed at Point To Point.

Ethernet Operating Mode

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

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

TERMINAL PROTECTION

Protection Type

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

Option	Function
None	The FE radio is stand alone radio (not part of an Aprisa FE Protected Station).
Redundant (Protected Station)	Set to make this FE radio part of an Aprisa FE Protected Station. The RF ports and interface ports from two standard Aprisa FE 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 FE radio part of an Aprisa FE Protected Station. The RF ports and interface ports from two standard Aprisa FE 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 277 for the list of monitored alarms.

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 be configured as the Primary and that radio B 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 FE Protected Station.

PROTECTION MANAGEMENT IP ADDRESS

Local IP Address

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

Partner IP Address

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

Radio

Radio > Radio Summary

This page displays the current settings for the Radio parameters.

4RF SUPERVISOR Aprisa **FE**

Local Remote Link Logout ADMIN

Terminal **Radio** Ethernet IP QoS Security Maintenance Events Software Monitoring

Radio Summary Channel Summary Radio Setup Channel Setup Advanced Setup

Local Radio OK MODE USB TX RX
 ● ● ● ● ●
 Status

TX FREQUENCY

TX Frequency (MHz)	406.25
TX Frequency Range (MHz)	400 to 470
TX Frequency Step Size (kHz)	6.25

TX POWER

TX Power (dBm)	32
TX Power Range (dBm)	5 to 32
TX Power Step Size (dB)	1

RX FREQUENCY

RX Frequency (MHz)	400
RX Frequency Range (MHz)	400 to 470
RX Frequency Step Size (kHz)	6.25

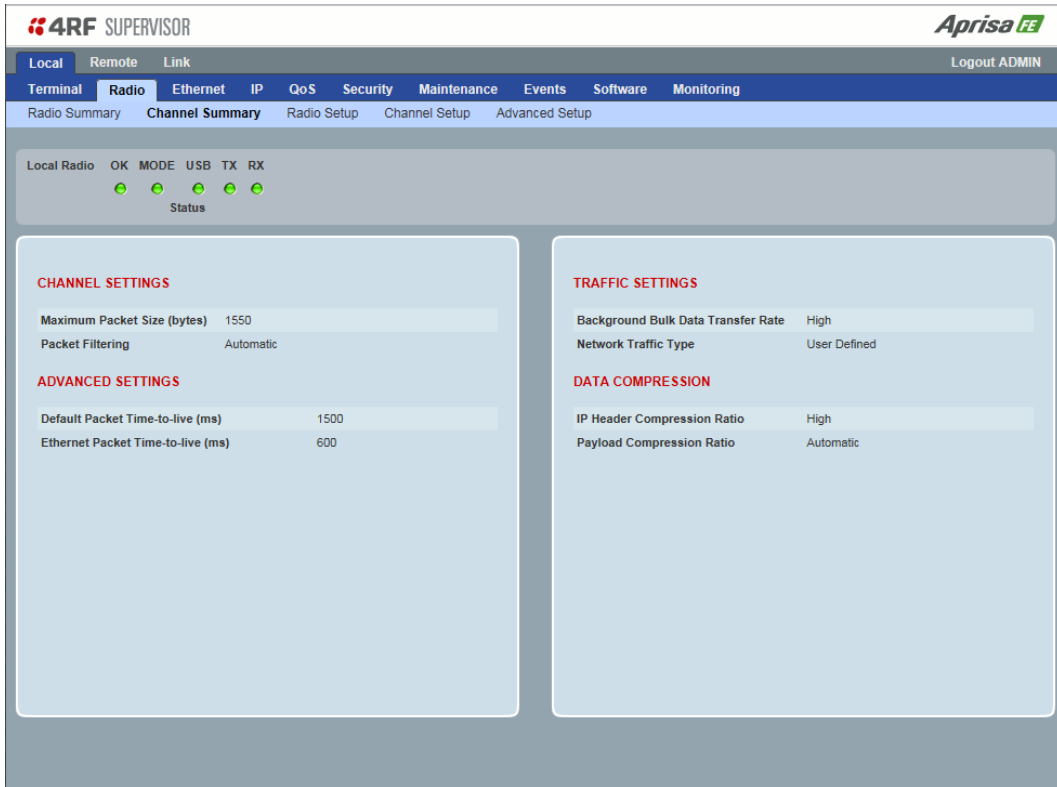
GENERAL

Modem Mode	Mode A (ETSI / ACMA)
Enhanced Noise Rejection Mode	Disabled
Channel Size (kHz)	12.5
Modulation Type	64QAM (Low Gain)
Antenna Port Configuration	Single Antenna Dual Port (Duplexer)

See 'Radio > Radio Setup' and 'Radio > Channel Setup' for setting details.

Radio > Channel Summary

This page displays the current settings for the Channel parameters.



The screenshot shows the 4RF SUPERVISOR interface with the following content:

- Header:** 4RF SUPERVISOR (left), Aprisa FE (right), Logout ADMIN (top right).
- Navigation:** Local, Remote, Link (top); Terminal, Radio, Ethernet, IP, QoS, Security, Maintenance, Events, Software, Monitoring (middle); Radio Summary, Channel Summary, Radio Setup, Channel Setup, Advanced Setup (bottom).
- Status:** Local Radio OK, MODE, USB, TX, RX (with green indicator lights); Status.
- CHANNEL SETTINGS:**
 - Maximum Packet Size (bytes): 1500
 - Packet Filtering: Automatic
- ADVANCED SETTINGS:**
 - Default Packet Time-to-live (ms): 1500
 - Ethernet Packet Time-to-live (ms): 600
- TRAFFIC SETTINGS:**
 - Background Bulk Data Transfer Rate: High
 - Network Traffic Type: User Defined
- DATA COMPRESSION:**
 - IP Header Compression Ratio: High
 - Payload Compression Ratio: Automatic

See 'Radio > Channel Setup' for setting details.

DATA COMPRESSION

IP Header Compression Ratio

See 'IP Header Compression Ratio' on page 83.

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.

The screenshot shows the 'Radio Setup' configuration page in the 4RF SUPERVISOR interface. The page is titled 'Radio Setup' and includes a navigation menu with options like 'Terminal', 'Radio', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. The 'Radio' section is active, showing 'Local Radio' status with indicators for OK, MODE, USB, TX, and RX. The configuration is split into two main panels: TRANSMITTER and RECEIVER, and a MODEM section. The TRANSMITTER panel has fields for TX Frequency (MHz) at 406.25 and TX Power (dBm) at 32. The RECEIVER panel has a field for RX Frequency (MHz) at 400. The GENERAL section includes Channel Size (kHz) at 12.5 and Antenna Port Configuration set to Single Antenna Dual Port (Duplexer). The MODEM section includes Modem Mode (Mode A (ETSI / ACMA)), Enhanced Noise Rejection Mode (Disabled), and Modulation Type (64QAM (Low Gain)). There is also an ADAPTIVE CODING MODULATION section with Default Modulation (QPSK (High Gain)) and a Modulation Range from QPSK (High Gain) to 64QAM (Low Gain). Save and Cancel buttons are present at the bottom of each section.

TRANSMITTER / RECEIVER

Important:

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 radio.

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 305).

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

The TX and RX frequencies will be dual frequency for correct full duplex RF operation. The TX and RX frequencies must not be the same.

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 +35 dBm (QPSK modulation).

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

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

GENERAL

Channel Size (kHz)

This parameter sets the Channel Size for the radio (see 'Channel Sizes' on page 306 for Radio Capacities). The default setting is 12.5 kHz.

Antenna Port Configuration

The Aprisa FE radio is always configured as Dual Antenna Port for TX and RX frequency separation and correct full duplex operation.

When the Aprisa FE uses an internal duplexer, the Aprisa FE front panel has a single N type RF female connector which provides the antenna connection.

When the Aprisa FE uses an external duplexer, the duplexer connects to the radio with dual rear SMA connectors and has a single N type RF female connector which provides the antenna connection.

MODEM

Modem Mode

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

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

Enhanced Noise Rejection Mode

This parameter enables / disables the Enhanced Noise Rejection Mode in the radio. This feature improves co-channel interference performance at strong receiver signal levels. Both the local and remote radios must use the same setting i.e. enabled or disabled.

The default setting is Disabled.

Modulation Type

This parameter sets the TX / RX Modulation Type. This parameter must be set the same in the local and remote radios for correct PTP link operation.

Option	Function
Adaptive	<p>Enables Adaptive Code Modulation for the upstream.</p> <p>The ACM will switch down one ACM level if the link quality degrades in advance of the level where errored packets would be expected and will switch to the lowest ACM level if an errored packet is received.</p> <p>The ACM will switch up when the link quality exceeds the performance threshold.</p> <p>This option preserves packet integrity but reduces network speeds</p>
Adaptive (Fast)	<p>Enables Adaptive Code Modulation.</p> <p>The ACM will switch down one ACM level if an errored packet is received.</p> <p>The ACM will switch up when the link quality exceeds the performance threshold.</p> <p>This option maintains the highest network speeds for as long as possible.</p>
QPSK (High Gain)	Sets the modulation to QPSK with Max Coded FEC.
QPSK (Low Gain)	Sets the modulation to QPSK with Min Coded FEC.
QPSK	Sets the modulation to QPSK with no FEC.
16QAM (High Gain)	Sets the modulation to 16 QAM with Max Coded FEC.
16QAM (Low Gain)	Sets the modulation to 16 QAM with Min Coded FEC.
16QAM	Sets the modulation to 16 QAM with no FEC.
64QAM (High Gain)	Sets the modulation to 64 QAM with Max Coded FEC.
64QAM (Low Gain)	Sets the modulation to 64 QAM with Min Coded FEC.

The default setting is QPSK (Low Gain).

ADAPTIVE CODING MODULATION

These settings are only used if the Modulation Type is set to Adaptive.

Default Modulation

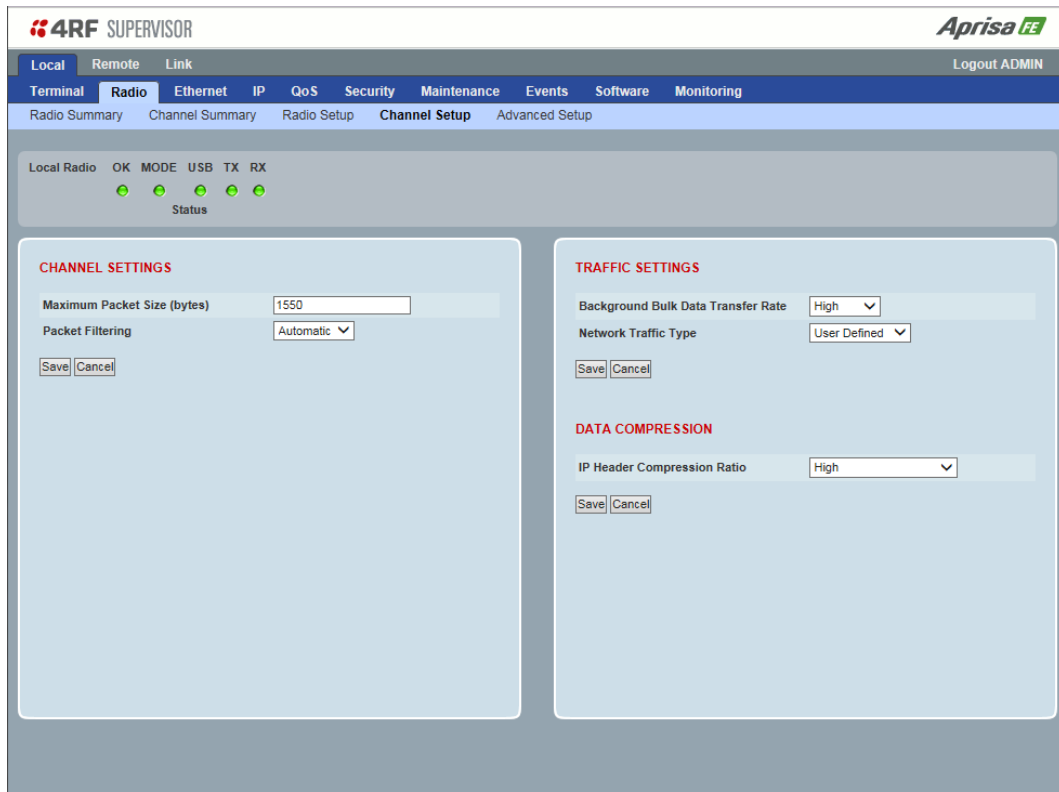
This parameter sets the default modulation and FEC code rate for the radio if the ACM mechanism fails for whatever reason. It is also used when the radio starts up, and subsequently, if there are no recommendations received from the other radio, it will remain at that setting. ACM recommendations are always expected to be received from the other radio.

Modulation Range

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

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

Radio > Channel Setup



CHANNEL SETTINGS

Maximum Packet Size (Bytes)

This parameter sets the maximum over-the-air packet size in bytes. The default setting is 1550 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 FE. This is not encrypted.

Packet Filtering

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

When set to automatic (default setting), packets received over radio link are dropped when the packet is not addressed for the Local or Remote radio.

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

Note: IP Header Compression must be disabled for this feature to operate correctly (see 'IP Header Compression Ratio' on page 83).

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 FE traffic protocols

The default setting is Automatic.

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

TRAFFIC SETTINGS

Ethernet Data Priority

The Ethernet Data Priority controls the priority of the Ethernet customer traffic relative Ethernet management traffic. If equal priority is required to management traffic, this setting must be the same as the Ethernet Management Priority.

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

A queuing system is used to prioritize customer and management Ethernet traffic 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 customer Ethernet data has a higher weighting it will be transmitted first. The Ethernet buffer is 10 Ethernet packets (1 packet can be up to Ethernet MTU, 1500 bytes).

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

Ethernet Management Priority

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

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

Background Bulk Data Transfer Rate

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

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

The default setting is high.

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 84). <div data-bbox="683 432 1174 622" style="border: 1px solid #ccc; padding: 5px; margin: 10px auto; width: fit-content;"><p>INFORMATION</p><p>For "User Defined" network traffic type, more parameters are available for configuration in the Advanced Setup menu.</p><p style="text-align: right;"><input type="button" value="OK"/></p></div>
Ethernet Only	Optimizes the channel settings for the predominantly Ethernet traffic.

The default setting is Ethernet Only.

DATA COMPRESSION

IP Header Compression Ratio

The IP Header Compression implements TCP/IP ROHC v2 (Robust Header Compression v2 RFC4995, RFC5225, RFC4996, RFC3843, RFC4815) to compress the IP header. IP Header Compression allows for faster point-to-point transactions.

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

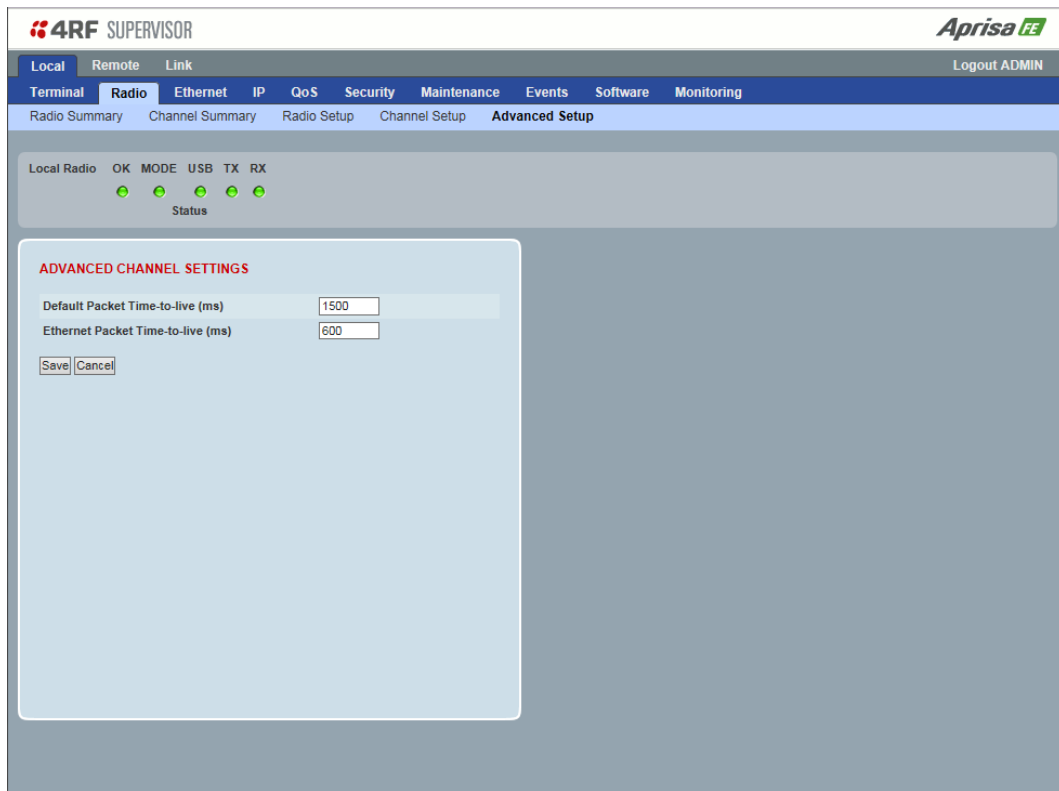
The Compression Ratio controls the rate at which compressor and decompressor synchronize state information with each other. Frequent synchronization results in reduced ratio.

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

The default setting is High.

Radio > Advanced Setup

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



ADVANCED CHANNEL SETTINGS

Default Packet Time to Live (ms)

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

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

Ethernet Packet Time to Live (ms)

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

Ethernet

Ethernet > Summary

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

The screenshot shows the 4RF SUPERVISOR web interface. At the top, there are navigation tabs for 'Local', 'Remote', and 'Link', with 'Local' selected. Below this is a menu bar with options: 'Terminal', 'Radio', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. The 'Ethernet' tab is active, and sub-tabs include 'Summary', 'Port Setup', 'L2 Filtering', and 'VLAN'. The 'Summary' sub-tab is selected. On the left, there is a 'Local Radio' status section with indicators for 'OK', 'MODE', 'USB', 'TX', and 'RX', all of which are green. Below this are two main panels: 'ETHERNET PORTS STATUS' and 'ETHERNET PORTS SETTINGS'. Each panel contains a table with columns for ID, Name, Status, Speed (Mbit/s), Duplex, and Function.

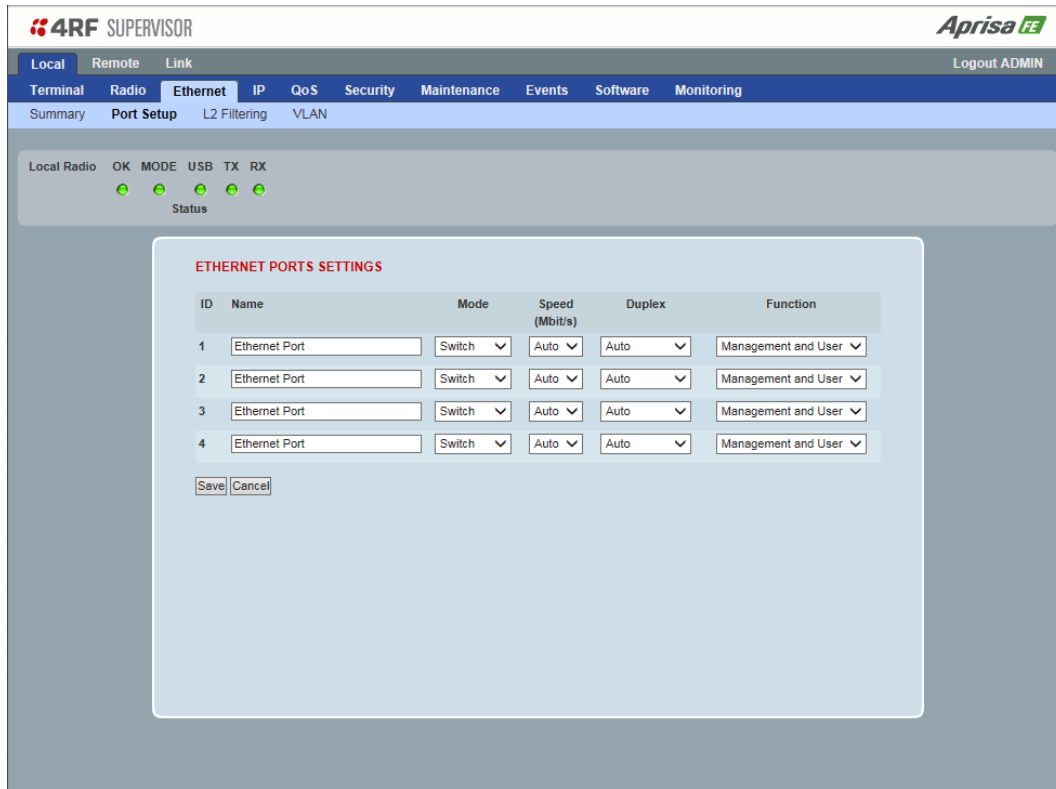
ID	Name	Status	Speed (Mbit/s)	Duplex
1	Ethernet Port	Up	100	Full
2	Ethernet Port	Down	10	Half
3	Ethernet Port	Down	10	Half
4	Ethernet Port	Down	10	Half

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

See 'Ethernet > Port Setup' for configuration options.

Ethernet > Port Setup

This page provides the setup for the Ethernet ports settings.



ETHERNET PORT SETTINGS

Mode

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

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

Speed (Mbit/s)

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

Option	Function
Auto	Provides auto selection of Ethernet Port Speed 10/100 Mbit/s
10	The Ethernet Port Speed is manually set to 10 Mbit/s
100	The Ethernet Port Speed is manually set to 100 Mbit/s

Duplex

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

Option	Function
Auto	Provides auto selection of Ethernet Port duplex setting.
Half Duplex	The Ethernet Port is manually set to Half Duplex.
Full Duplex	The Ethernet Port is manually set to Full Duplex.

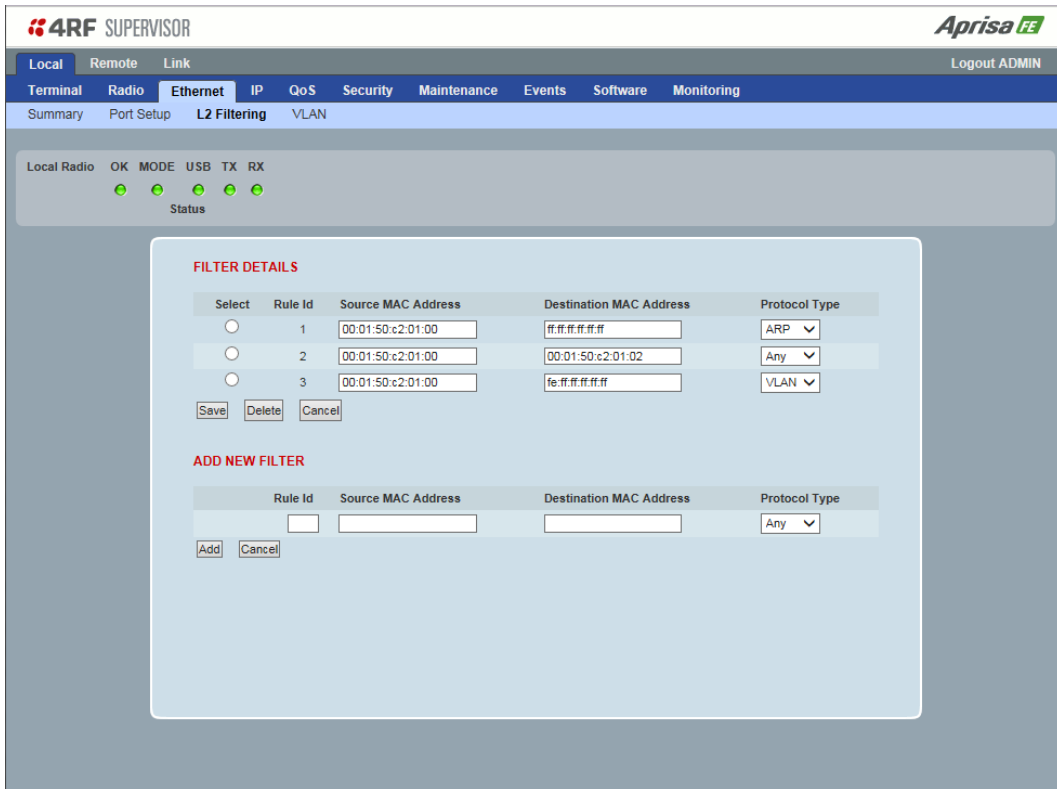
Function

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

Option	Function
Management Only	The Ethernet port is only used for management of the link.
Management and User	The Ethernet port is used for management of the link 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 154).



The screenshot shows the 4RF SUPERVISOR web interface. At the top, there is a navigation menu with options: Local, Remote, Link, Terminal, Radio, Ethernet (selected), IP, QoS, Security, Maintenance, Events, Software, and Monitoring. Below the menu, there are sub-tabs: Summary, Port Setup, L2 Filtering (selected), and VLAN. The main content area is titled 'Local Radio' and shows status indicators for OK, MODE, USB, TX, and RX. Below this, the 'FILTER DETAILS' section contains a table with three rows of filter rules. Each row has a 'Select' radio button, a 'Rule Id', 'Source MAC Address', 'Destination MAC Address', and 'Protocol Type' dropdown. The first row has Rule Id 1, Source MAC 00:01:50:c2:01:00, Destination MAC ff:ff:ff:ff:ff:ff, and Protocol Type ARP. The second row has Rule Id 2, Source MAC 00:01:50:c2:01:00, Destination MAC 00:01:50:c2:01:02, and Protocol Type Any. The third row has Rule Id 3, Source MAC 00:01:50:c2:01:00, Destination MAC fe:ff:ff:ff:ff:ff, and Protocol Type VLAN. Below the table are 'Save', 'Delete', and 'Cancel' buttons. The 'ADD NEW FILTER' section has a form with fields for Rule Id, Source MAC Address, Destination MAC Address, and Protocol Type (set to Any), with 'Add' and 'Cancel' buttons.

Select	Rule Id	Source MAC Address	Destination MAC Address	Protocol Type
<input type="radio"/>	1	00:01:50:c2:01:00	ff:ff:ff:ff:ff:ff	ARP
<input type="radio"/>	2	00:01:50:c2:01:00	00:01:50:c2:01:02	Any
<input type="radio"/>	3	00:01:50:c2:01:00	fe:ff:ff:ff:ff:ff	VLAN

Rule Id	Source MAC Address	Destination MAC Address	Protocol Type
<input type="text"/>	<input type="text"/>	<input type="text"/>	Any

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 local radio 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:

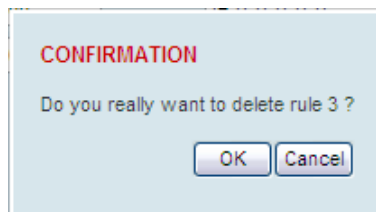
Unicast Only Traffic

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.

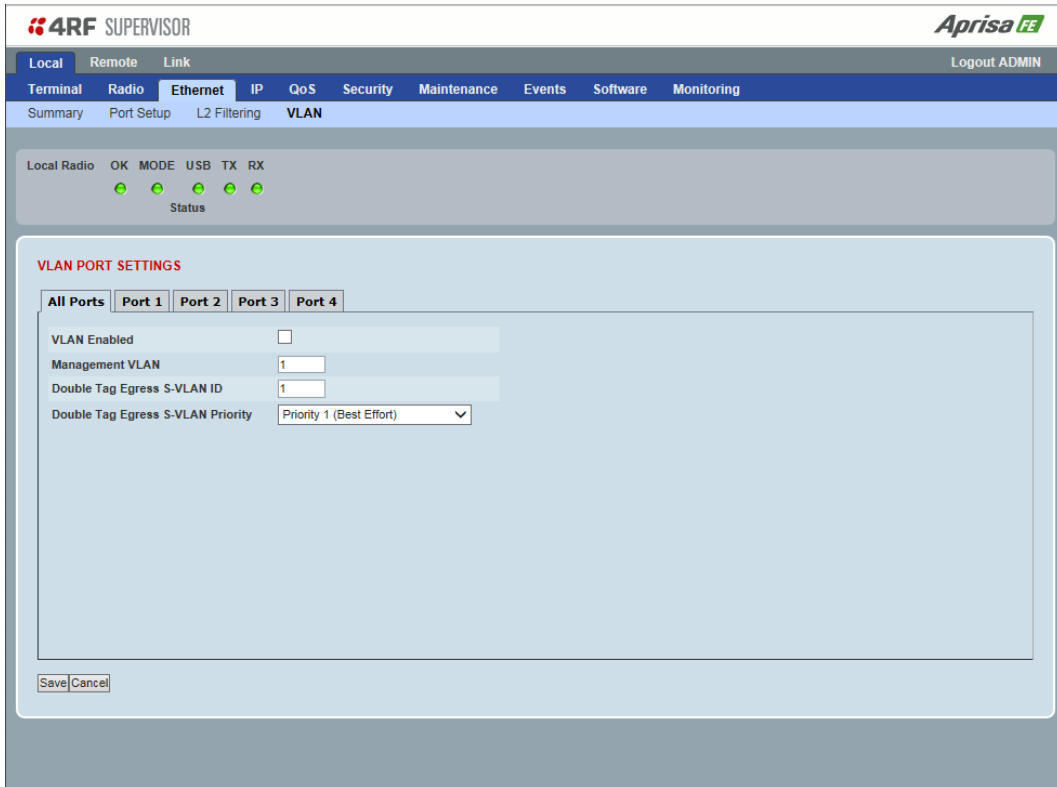
ADD NEW FILTER

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 154).



4RF SUPERVISOR Aprisa FE

Local Remote Link Logout ADMIN

Terminal Radio Ethernet IP QoS Security Maintenance Events Software Monitoring

Summary Port Setup L2 Filtering VLAN

Local Radio OK MODE USB TX RX
 Status

VLAN PORT SETTINGS

All Ports Port 1 Port 2 Port 3 Port 4

VLAN Enabled

Management VLAN

Double Tag Egress S-VLAN ID

Double Tag Egress S-VLAN Priority

Save Cancel

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 link. If it is enabled on the local radio, it must also be enabled on the remote radio. The default is disabled.

Management VLAN

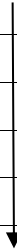
This parameter sets the VLAN ID for management traffic only. The value can be between 1 and 4094. The default is 1.

Double Tag Egress S-VLAN ID

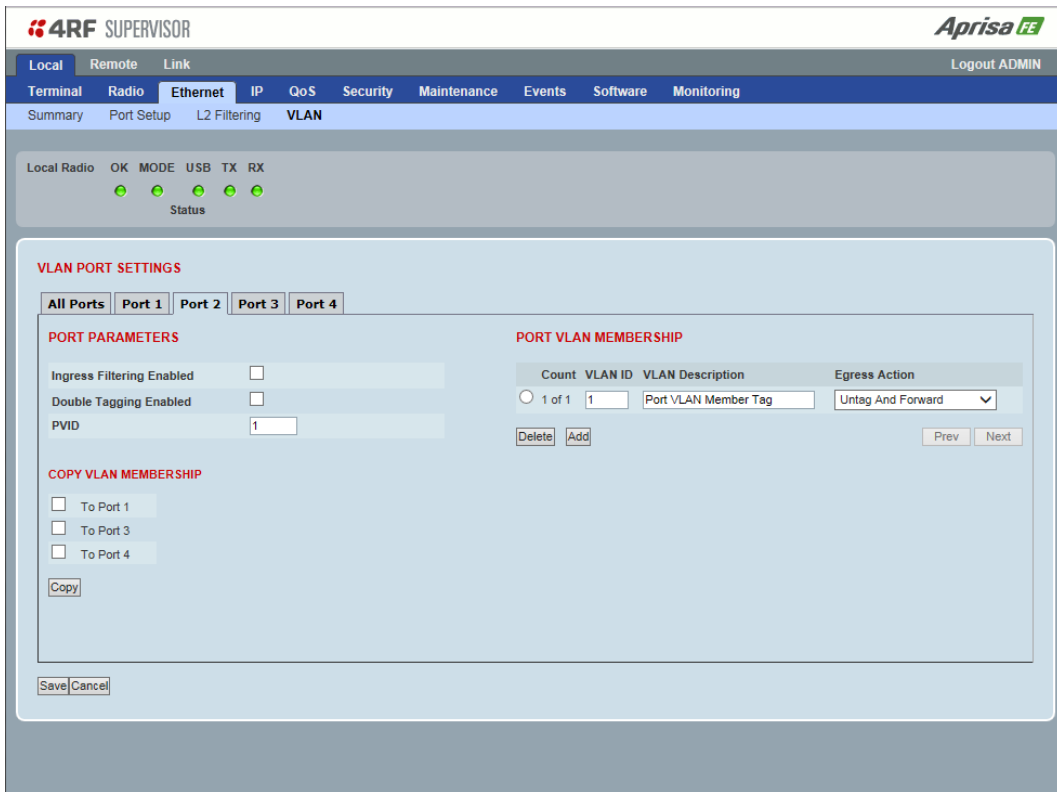
This parameter sets the S-VLAN ID (outer tag) in the egress direction. The value can be between 1 and 4094. The default is 1.

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	

VLAN PORT SETTINGS - Port 1



4RF SUPERVISOR Aprisa **FE**

Local Remote Link Logout ADMIN

Terminal Radio **Ethernet** IP QoS Security Maintenance Events Software Monitoring

Summary Port Setup L2 Filtering **VLAN**

Local Radio OK MODE USB TX RX
● ● ● ● ●
 Status

VLAN PORT SETTINGS

All Ports **Port 1** Port 2 Port 3 Port 4

PORT PARAMETERS

Ingress Filtering Enabled

Double Tagging Enabled

PVID

PORT VLAN MEMBERSHIP

Count	VLAN ID	VLAN Description	Egress Action
1 of 1	1	Port VLAN Member Tag	Untag And Forward

Delete Add Prev Next

COPY VLAN MEMBERSHIP

To Port 1

To Port 3

To Port 4

Copy

Save Cancel

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 FE 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 FE 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 link 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 90). 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 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

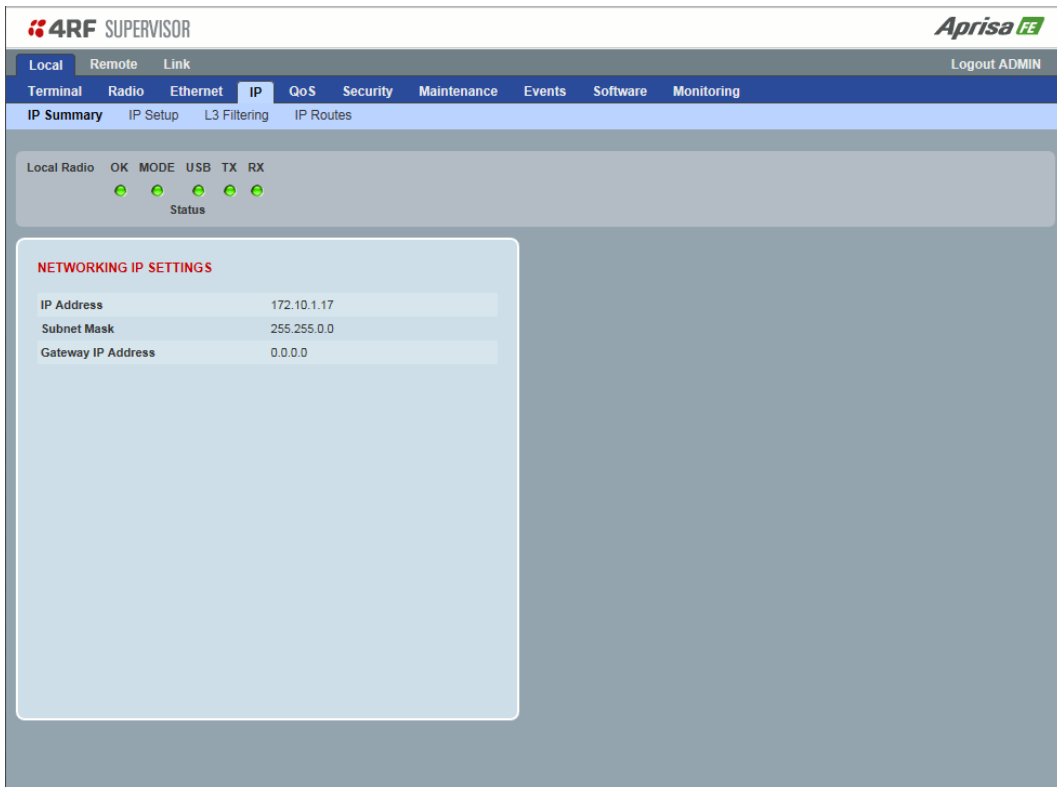
The Add button adds the selected entry.

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'.



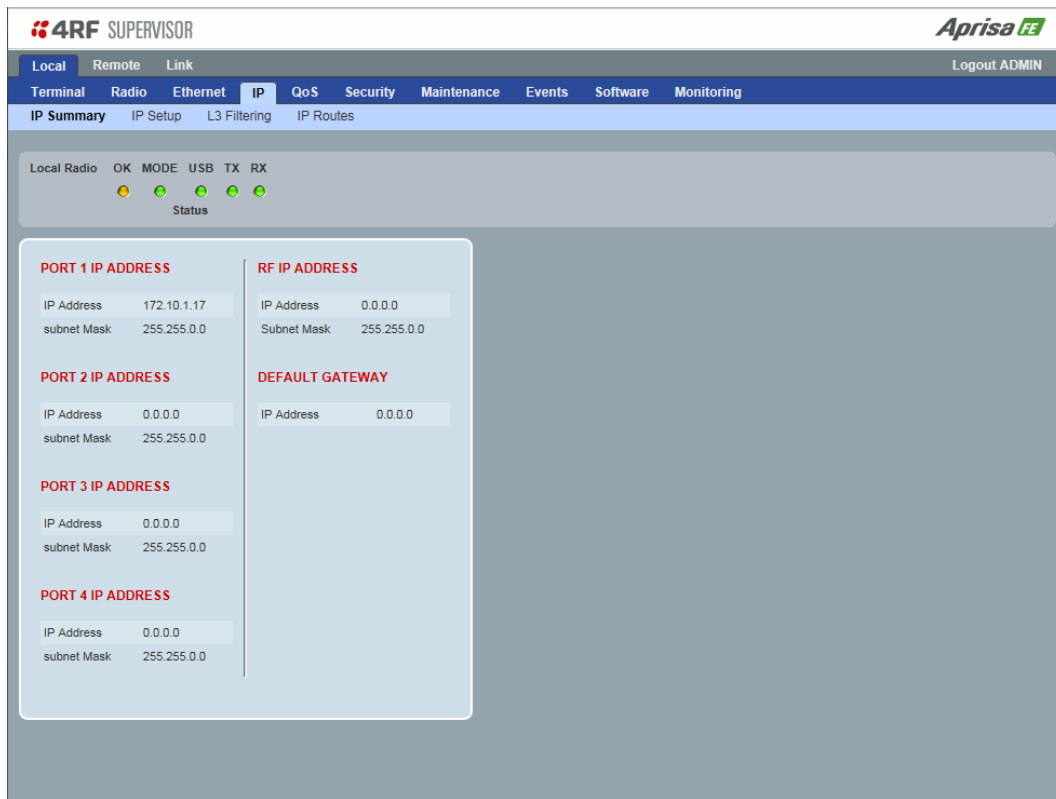
The screenshot shows the 4RF SUPERVISOR web interface. The top navigation bar includes 'Local', 'Remote', and 'Link'. Below it, a menu bar contains 'Terminal', 'Radio', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. The 'IP' menu is expanded, showing 'IP Summary', 'IP Setup', 'L3 Filtering', and 'IP Routes'. The 'IP Summary' page displays a status bar for 'Local Radio' with indicators for 'OK', 'MODE', 'USB', 'TX', and 'RX', all of which are green. Below this, a box titled 'NETWORKING IP SETTINGS' contains the following information:

NETWORKING IP SETTINGS	
IP Address	172.10.1.17
Subnet Mask	255.255.0.0
Gateway IP Address	0.0.0.0

See 'IP > IP Setup > Bridge / Gateway Router Modes' for configuration options.

IP > IP Summary > Router Mode

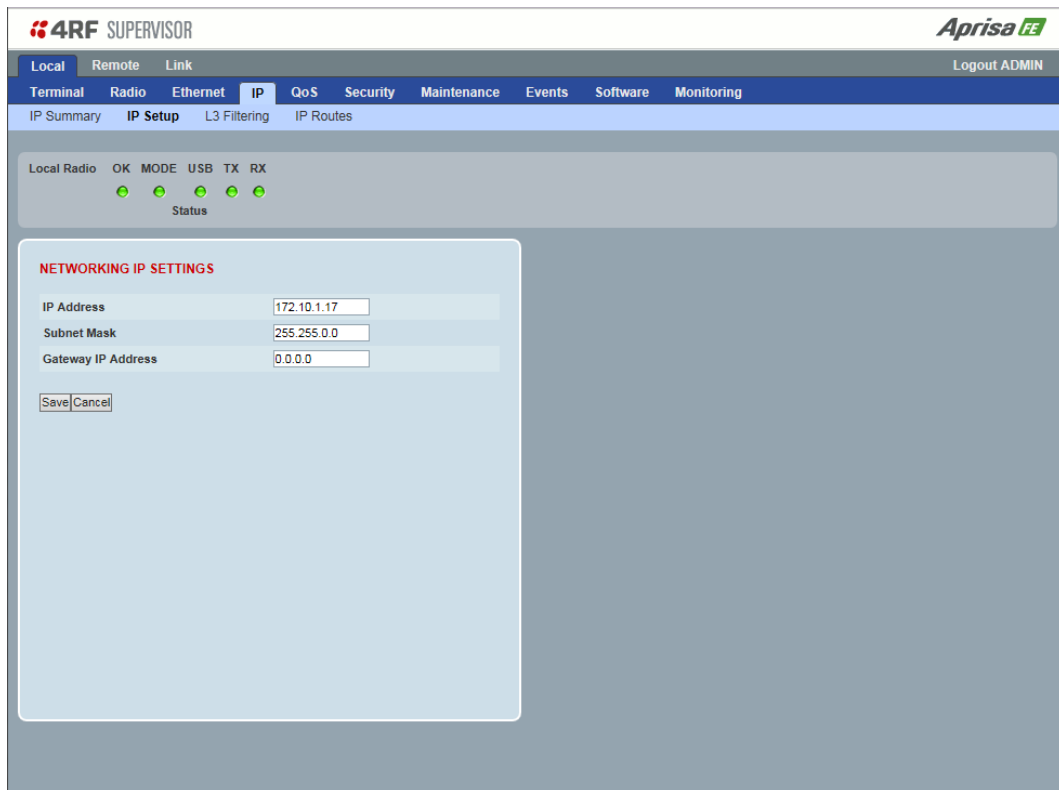
This page displays the current settings for the Networking IP Settings for an Ethernet Operating Mode of 'Router'.



See 'IP > IP Setup > Router Mode' on page 98 for configuration options.

IP > IP Setup > Bridge / Gateway Router Modes

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



NETWORKING IP SETTINGS

IP Address

Set the static IP Address of the radio (Management and Ethernet ports) assigned by your site network administrator using the standard format xxx.xxx.xxx.xxx. This IP address is used both in Bridge mode and in Router mode. The default IP address is in the range 169.254.50.10.

Subnet Mask

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

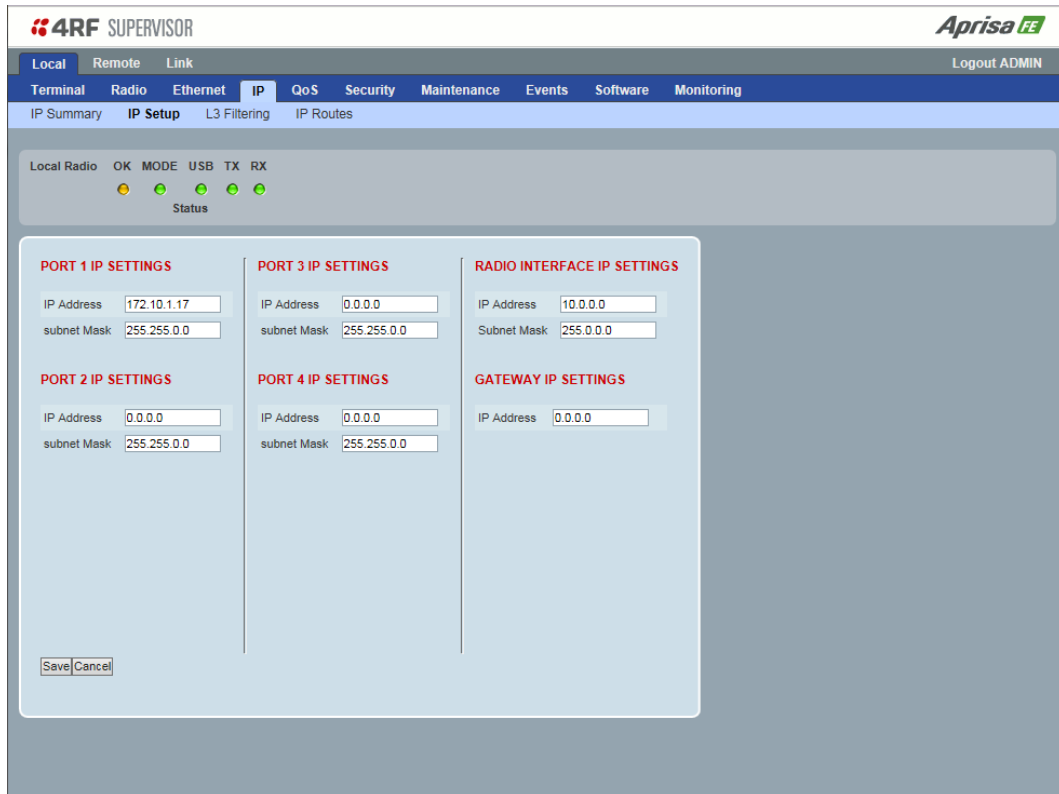
Gateway

Set the Gateway address of the radio, if required, using the standard format xxx.xxx.xxx.

A default gateway is the node on the network that traffic is directed to when an IP address does not match any other routes in the routing table. It can be the IP address of the router or PC connected to the local radio. The default gateway commonly connects the internal radio network and the outside network. The default Gateway is 0.0.0.0.

IP > IP Setup > Router Mode

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



The screenshot shows the 4RF Supervisor web interface. At the top, there's a navigation bar with 'Local', 'Remote', and 'Link' tabs. Below that, a menu includes 'Terminal', 'Radio', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. The 'IP' menu is expanded, showing 'IP Summary', 'IP Setup', 'L3 Filtering', and 'IP Routes'. The 'IP Setup' page is displayed, featuring a 'Local Radio' status bar with 'OK', 'MODE', 'USB', 'TX', and 'RX' indicators. The main content area is divided into six sections for IP settings: PORT 1, PORT 2, PORT 3, PORT 4, RADIO INTERFACE, and GATEWAY. Each section has input fields for 'IP Address' and 'Subnet Mask'. The 'PORT 1' settings are pre-filled with IP Address 172.10.1.17 and Subnet Mask 255.255.0.0. The other sections have default values of 0.0.0.0 for IP Address and 255.255.0.0 for Subnet Mask. A 'Save' button is located at the bottom left of the settings area.

PORT SETTINGS - port (n)

IP Address

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

Subnet Mask

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

Gateway

Set the Gateway address of the radio Ethernet port (n), if required, using the standard format xxx.xxx.xxx.

A default gateway is the node on the network that traffic is directed to when an IP address does not match any other routes in the routing table. It can be the IP address of the router or PC connected to the local radio. The default gateway commonly connects the internal radio network and the outside network. The default Gateway is 0.0.0.0.

RADIO INTERFACE IP SETTINGS

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

Radio Interface IP Address

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

Radio Interface Subnet Mask

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

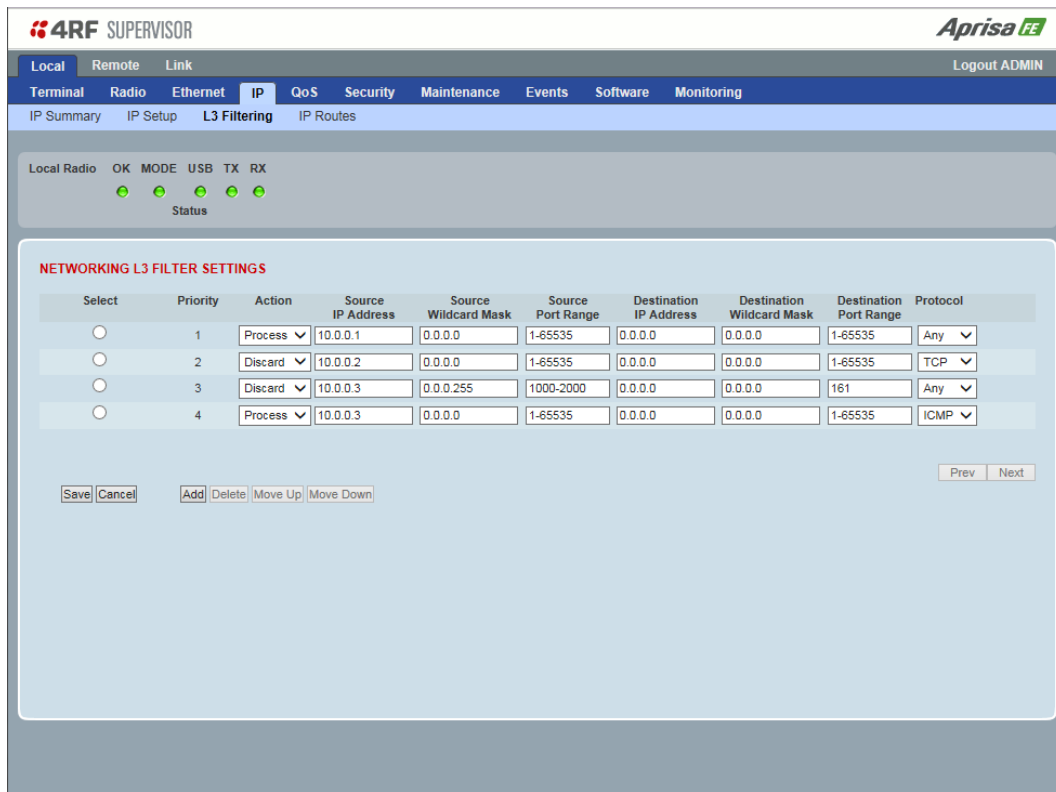
Note 1: If the local radio RF interface IP address is a network IP address, and if the remote radio is also using a network IP address within the same subnet or different subnet, then the local radio will assign an automatic RF interface IP address from its own subnet.

When the local radio has a host specific RF interface IP address, then the remote radio must have a host specific RF interface IP address from the same subnet.

Note 2: When a remote radio is configured for Router Mode and the local 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 link topology by using the 'Decommission Node' and 'Discover Nodes' (see 'Maintenance > Advanced' on page 155).

IP > L3 Filtering

This page is only available if the Ethernet traffic option has been licensed (see 'Maintenance > Licence' on page 154) and Router Mode selected. It is not active in Bridge Mode (see 'Terminal > Operating Mode' on page 71).



NETWORKING L3 FILTER SETTINGS

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

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

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

Priority

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

Action

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

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

Source IP Address

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

Source Wildcard Mask

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

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

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

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

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

Source Port Range

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

Destination IP Address

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

Destination Wildcard Mask

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

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

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

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

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

Destination Port Range

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

Protocol

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

Controls

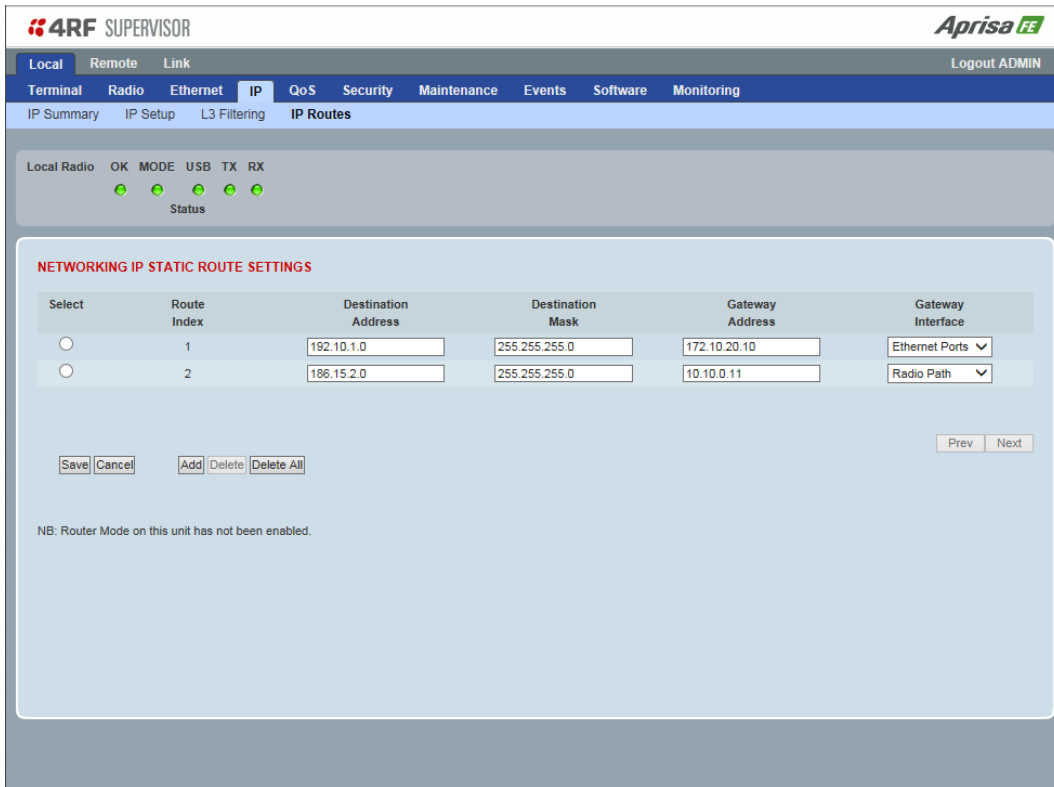
The Delete button deletes the selected entry.

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

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

IP > IP Routes

This page is only available if the Ethernet traffic option has been licensed (see 'Maintenance > Licence' on page 154) and Router Mode selected. It is not valid for Bridge Mode (see 'Terminal > Operating Mode' on page 71).



4RF SUPERVISOR Aprisa FE

Local Remote Link Logout ADMIN

Terminal Radio Ethernet **IP** QoS Security Maintenance Events Software Monitoring

IP Summary IP Setup L3 Filtering **IP Routes**

Local Radio OK MODE USB TX RX
● ● ● ● ●
 Status

NETWORKING IP STATIC ROUTE SETTINGS

Select	Route Index	Destination Address	Destination Mask	Gateway Address	Gateway Interface
<input type="radio"/>	1	192.10.1.0	255.255.255.0	172.10.20.10	Ethernet Ports
<input type="radio"/>	2	186.15.2.0	255.255.255.0	10.10.0.11	Radio Path

NB: Router Mode on this unit has not been enabled.

NETWORKING IP STATIC ROUTE SETTINGS

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

Route Index

This parameter shows the route index.

Destination Address

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

Destination Mask

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

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

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

Gateway Address

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

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

Gateway Interface

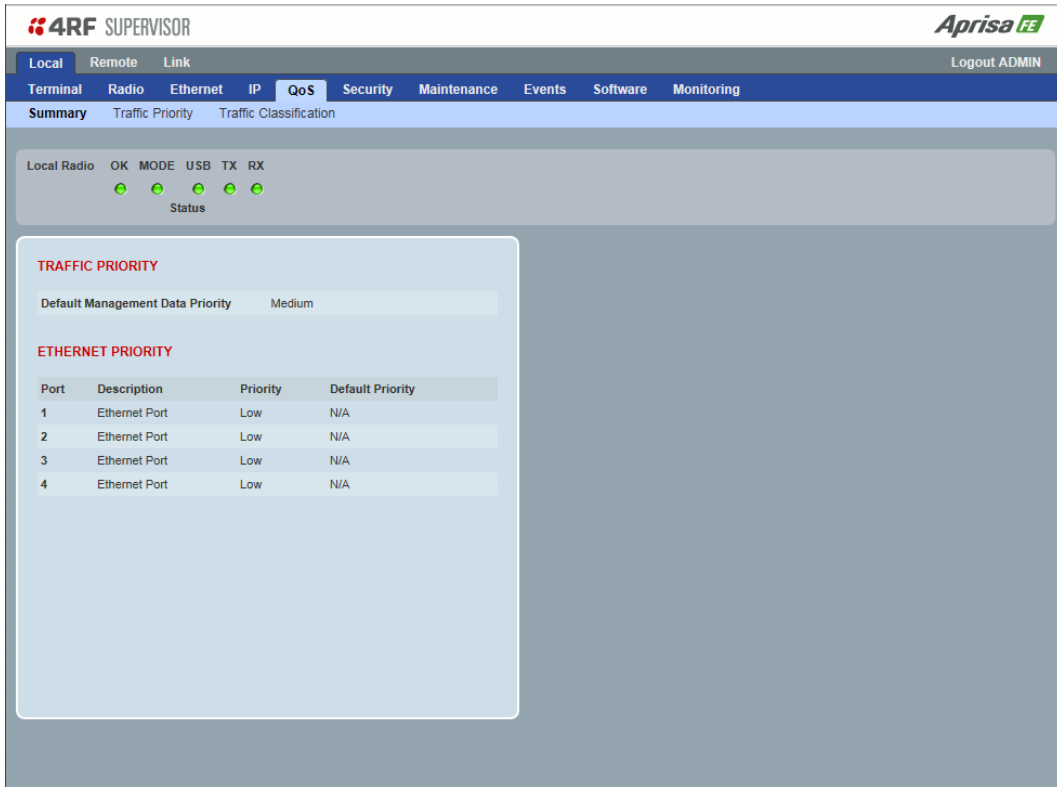
This parameter sets the destination interface.

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

QoS

QoS > Summary

This page provides a summary of the QoS Settings.



The screenshot displays the 4RF SUPERVISOR interface. At the top, there is a navigation bar with 'Local', 'Remote', and 'Link' options. Below this is a menu with 'Terminal', 'Radio', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. The 'QoS' menu is expanded, showing 'Summary', 'Traffic Priority', and 'Traffic Classification'. The 'Summary' page includes a 'Local Radio' status section with indicators for 'OK', 'MODE', 'USB', 'TX', and 'RX'. Below this, there are two sections: 'TRAFFIC PRIORITY' and 'ETHERNET PRIORITY'. The 'TRAFFIC PRIORITY' section shows 'Default Management Data Priority' set to 'Medium'. The 'ETHERNET PRIORITY' section contains a table with the following data:

Port	Description	Priority	Default Priority
1	Ethernet Port	Low	N/A
2	Ethernet Port	Low	N/A
3	Ethernet Port	Low	N/A
4	Ethernet Port	Low	N/A

See 'QoS > Traffic Priority' and 'QoS > Traffic Classification' for configuration options.

QoS > Traffic Priority

TRAFFIC PRIORITY

Default Management Data Priority

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

ETHERNET PRIORITY

This parameter controls the per port priority of the Ethernet customer traffic.

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

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

The default setting is Low.

A queuing system is used to prioritize customer traffic from the 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 other 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 FE: Very High, High, Medium and Low. Data is added to one of these queues depending on the priority setting. Data leaves the queues from highest priority to lowest: the Very High queue is emptied first, followed by High then Medium and finally Low.

Default Priority

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

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

PRIORITY DEFINITIONS

PCP (Priority Code Point)

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

The screenshot shows the 4RF SUPERVISOR web interface. At the top, there are navigation tabs: Local, Remote, Link, Terminal, Radio, Ethernet, IP, QoS (selected), Security, Maintenance, Events, Software, and Monitoring. Below these are sub-tabs: Summary, Traffic Priority (selected), and Traffic Classification. A status bar shows 'Local Radio' with indicators for OK, MODE, USB, TX, and RX, all of which are green. The main content area is split into two panels. The left panel, titled 'TRAFFIC PRIORITY', has a 'Default Management Data Priority' dropdown set to 'Medium'. Below it is the 'ETHERNET PRIORITY' section, which contains a table with 4 rows. The right panel, titled 'PRIORITY DEFINITIONS', has tabs for 'PCP' and 'DSCP'. The 'PCP' tab is active, showing a table with 7 rows mapping PCP bit values to radio priorities. A 'Default All' button is at the bottom of this table. Both panels have 'Save' and 'Cancel' buttons at the bottom.

Port	Description	Priority	Default Priority
1	Ethernet Port	Low	N/A
2	Ethernet Port	Low	N/A
3	Ethernet Port	Low	N/A
4	Ethernet Port	Low	N/A

PCP Bit Values	Radio Priority
1 (Background)	Low
0 (Best Effort)	Low
2 (Excellent Effort)	Medium
3 (Critical Application)	Medium
4 (Video)	High
5 (Voice)	High
6 (Internetwork Control)	Very High
7 (Network Control)	Very High

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.

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 an Aprisa FE device. The navigation menu includes Local, Remote, Link, Terminal, Radio, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring. The 'QoS' tab is active, showing 'Traffic Priority' and 'Traffic Classification' sub-tabs. The 'Traffic Priority' sub-tab is selected, displaying the following configuration panels:

- TRAFFIC PRIORITY:** A dropdown menu for 'Default Management Data Priority' is set to 'Medium'.
- ETHERNET PRIORITY:** A table with 4 columns: Port, Description, Priority, and Default Priority.

Port	Description	Priority	Default Priority
1	Ethernet Port	Low	N/A
2	Ethernet Port	Low	N/A
3	Ethernet Port	Low	N/A
4	Ethernet Port	Low	N/A
- PRIORITY DEFINITIONS:** A section with 'PCP' and 'DSCP' tabs. The 'DSCP' tab is active, showing a table for mapping PCP Bit Values to Radio Priority.

PCP Bit Values	Radio Priority
1 (Background)	Low
0 (Best Effort)	Low
2 (Excellent Effort)	Medium
3 (Critical Application)	Medium
4 (Video)	High
5 (Voice)	High
6 (Internetwork Control)	Very High
7 (Network Control)	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.

QoS > Traffic Classification

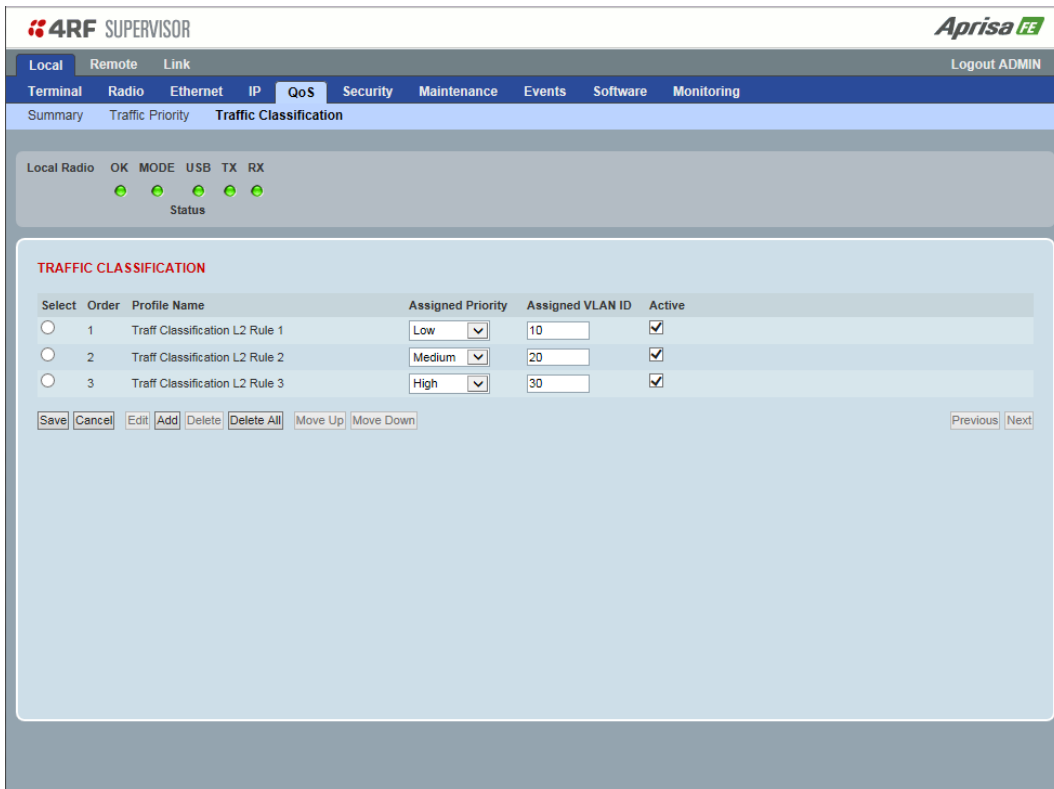
These settings provide multiple traffic classification profiles based on classification rules. Profiles for a specific traffic type, protocol or application can be assigned to a particular VLAN and CoS / priority in bridge mode or to CoS / priority in router mode to provide the appropriate QoS treatment.

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

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

These settings are different for Bridge Mode and Router Mode.

Bridge Mode Traffic Classification Settings



4RF SUPERVISOR Aprisa FE

Local Remote Link Logout ADMIN

Terminal Radio Ethernet IP **QoS** Security Maintenance Events Software Monitoring

Summary Traffic Priority **Traffic Classification**

Local Radio OK MODE USB TX RX
● ● ● ● ●
 Status

TRAFFIC CLASSIFICATION

Select	Order	Profile Name	Assigned Priority	Assigned VLAN ID	Active
<input type="radio"/>	1	Traffic Classification L2 Rule 1	Low	10	<input checked="" type="checkbox"/>
<input type="radio"/>	2	Traffic Classification L2 Rule 2	Medium	20	<input checked="" type="checkbox"/>
<input type="radio"/>	3	Traffic Classification L2 Rule 3	High	30	<input checked="" type="checkbox"/>

Save Cancel Edit Add Delete Delete All Move Up Move Down Previous Next

TRAFFIC CLASSIFICATION

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

Profile name

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

Assigned Priority

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

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

Assigned VLAN ID

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

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

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

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

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

For example, if the local radio 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 local radio 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.

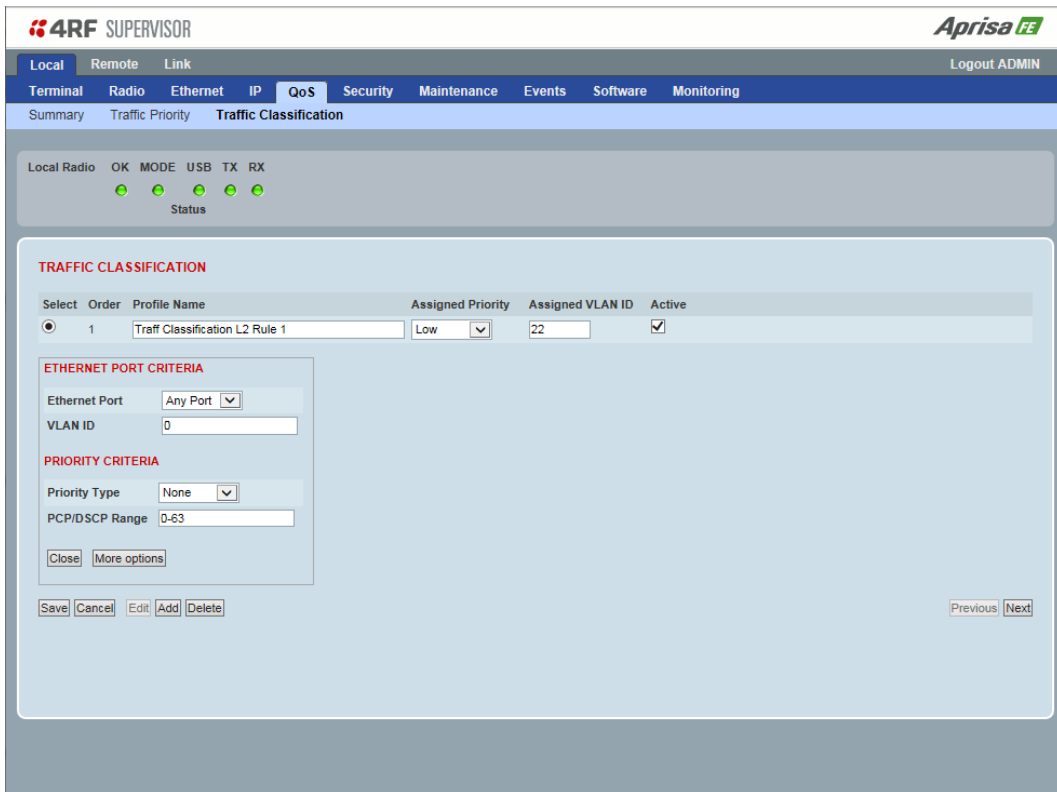
The Move up button will move the selected profile up one in the order of profiles

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



The screenshot shows the 4RF SUPERVISOR interface. At the top, there are navigation tabs: Local, Remote, Link, Terminal, Radio, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring. The 'QoS' tab is active, and the 'Traffic Classification' sub-tab is selected. Below the navigation is a status bar for 'Local Radio' with indicators for OK, MODE, USB, TX, and RX. The main content area is titled 'TRAFFIC CLASSIFICATION' and contains a table with the following data:

Select	Order	Profile Name	Assigned Priority	Assigned VLAN ID	Active
<input checked="" type="radio"/>	1	Traff Classification L2 Rule 1	Low	22	<input checked="" type="checkbox"/>

Below the table is a modal window for editing the selected rule. It has two sections: 'ETHERNET PORT CRITERIA' and 'PRIORITY CRITERIA'. The 'ETHERNET PORT CRITERIA' section has 'Ethernet Port' set to 'Any Port' and 'VLAN ID' set to '0'. The 'PRIORITY CRITERIA' section has 'Priority Type' set to 'None' and 'PCP/DSCP Range' set to '0-63'. At the bottom of the modal are buttons for 'Close', 'More options', 'Save', 'Cancel', 'Edit', 'Add', and 'Delete'. The main page also has 'Previous' and 'Next' buttons at the bottom right.

ETHERNET PORT CRITERIA

Ethernet Port

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

VLAN ID

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

Enable this VLAN in the network by setting the same VLAN ID value in PVID (port VLAN ID) and in the PORT VLAN MEMBERSHIP under 'VLAN ID' on page 94. 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.

The screenshot shows the '4RF SUPERVISOR' interface with the 'Aprisa FE' logo. The navigation menu includes 'Local', 'Radio', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. The 'QoS' section is active, showing 'Traffic Classification' settings. A table lists classification rules, with 'Traff Classification L2 Rule 1' selected. Below the table, the configuration form is divided into several sections:

- ETHERNET PORT CRITERIA:** Ethernet Port (Any Port), VLAN ID (0).
- 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).
- PRIORITY CRITERIA:** Priority Type (None), PCP/DSCP Range (0-63).
- TCP/UDP PORT CRITERIA:** Source Range (1-65535), Destination Range (1-65535).

Buttons for 'Close', 'More options', 'Save', 'Cancel', 'Edit', 'Add', 'Delete', 'Previous', and 'Next' are visible at the bottom of the form.

ETHERNET CRITERIA

Source MAC Address

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

Source MAC Wildcard Mask

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

Destination MAC Address

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

Destination MAC Wildcard Mask

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

EtherType (Hex)

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

EtherType Examples:

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

IP CRITERIA

Source IP Address

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

Source IP Wildcard Mask

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

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

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

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

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

Destination IP Address

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

Destination IP Wildcard Mask

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

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

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

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

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

IP Protocol Number

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

Protocol number Examples:

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

TCP / UDP PORT CRITERIA

Source Range

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

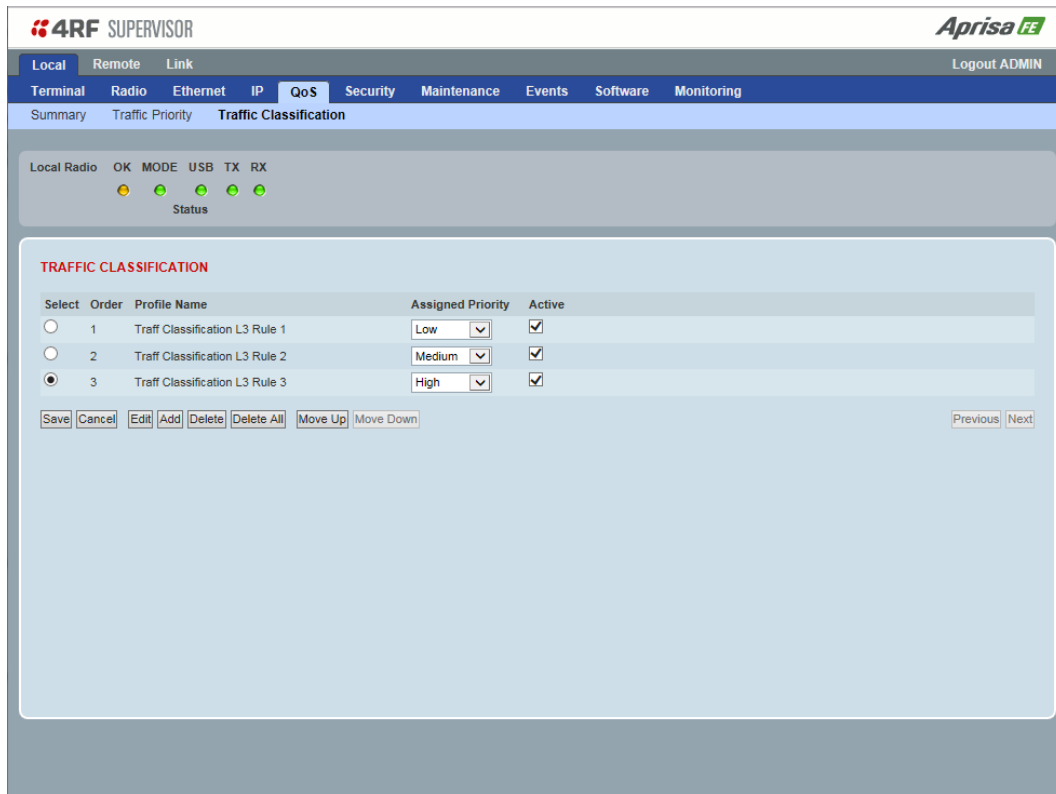
Destination Range

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

Examples for TCP / UDP Port Numbers:

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

Router Mode Traffic Classification Settings



TRAFFIC CLASSIFICATION

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

Profile name

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

Assigned Priority

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

Active

Activated or deactivate the profile rule.

Controls

The Save button saves all profiles to the radio.

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

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

The Add button adds a new profile,

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

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

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

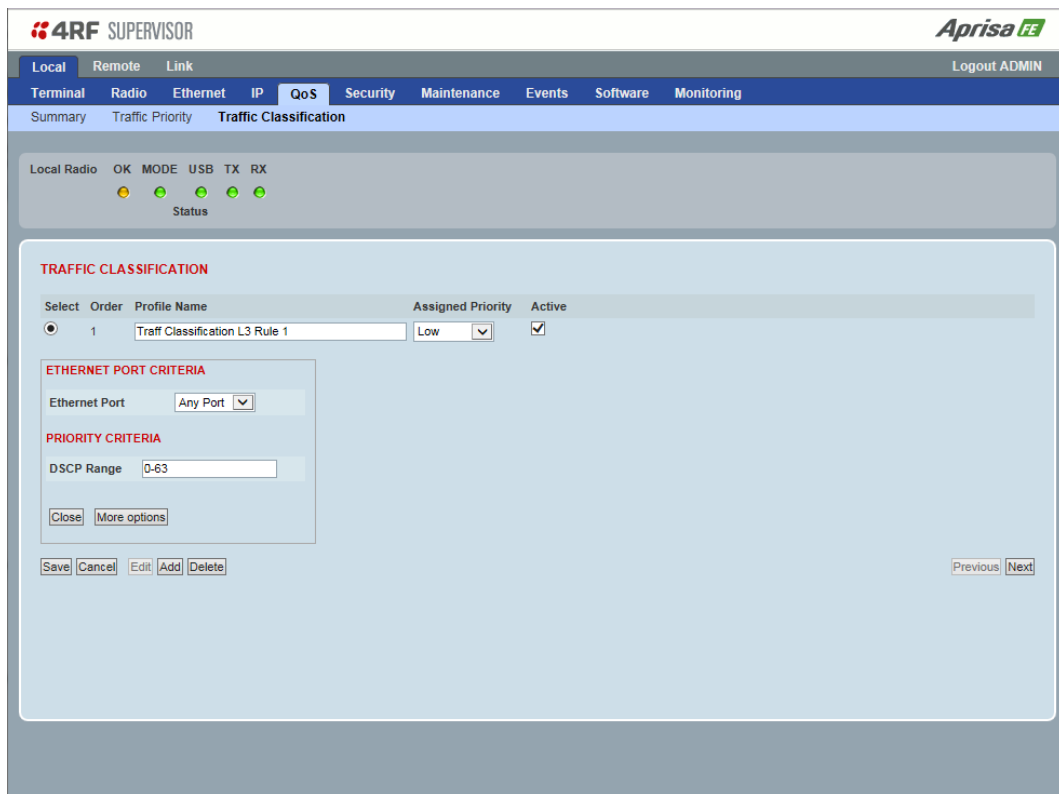
The Move up button will move the selected profile up one in the order of profiles

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

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

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

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



ETHERNET PORT CRITERIA

Ethernet Port

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

PRIORITY CRITERIA

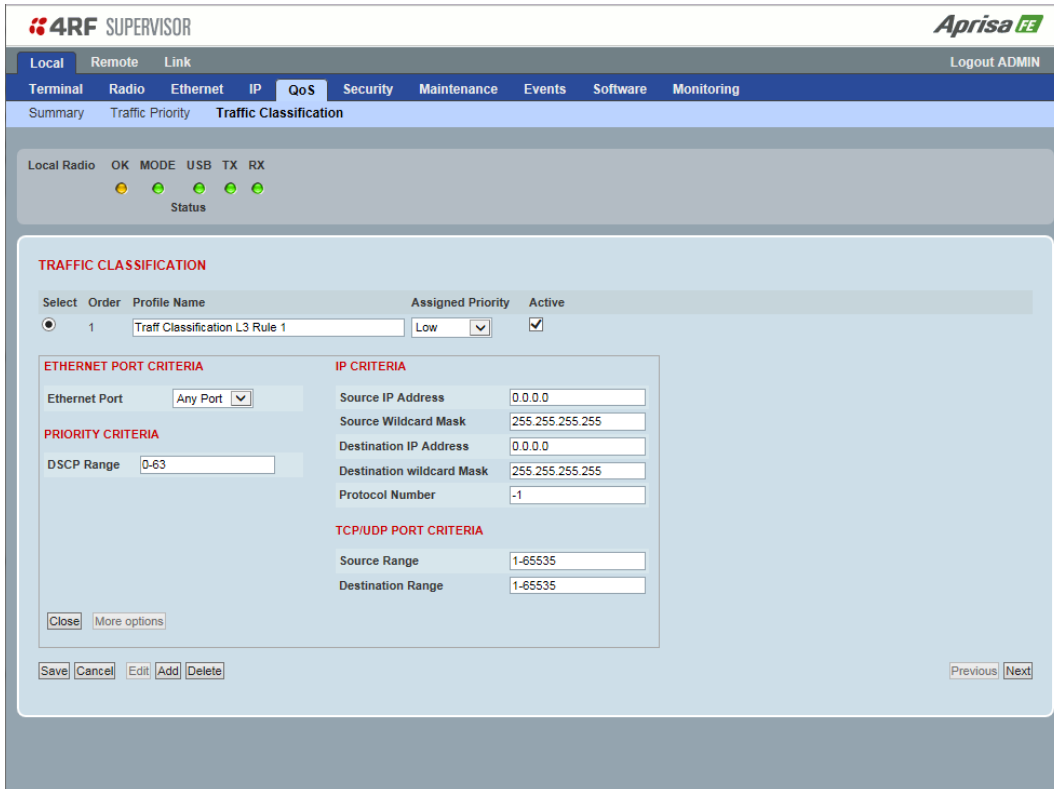
DSCP Range

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

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

DSCP Value (Decimal)	DSCP Priority
46	EF (Expedited Forwarding)
10	AF11 (Assured Forwarding)
12	AF12
14	AF13
18	AF21
20	AF22
22	AF23
26	AF31
28	AF32
30	AF33
34	AF41
36	AF42
38	AF43
0	CS0/Best Effort (BE)
8	CS1 (Class Selector)
16	CS2
24	CS3
32	CS4
40	CS5
48	CS6
56	CS7

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



The screenshot shows the 4RF SUPERVISOR interface. At the top, there are tabs for Local, Remote, and Link. Below that is a navigation menu with options: Terminal, Radio, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring. The main content area is titled 'TRAFFIC CLASSIFICATION' and includes a table with columns for Select, Order, Profile Name, Assigned Priority, and Active. Below the table is a 'More options' dialog box with the following sections:

- ETHERNET PORT CRITERIA:** Ethernet Port (Any Port)
- PRIORITY CRITERIA:** DSCP Range (0-63)
- 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), Protocol Number (-1)
- TCP/UDP PORT CRITERIA:** Source Range (1-65535), Destination Range (1-65535)

At the bottom of the dialog box are buttons for Close, More options, Save, Cancel, Edit, Add, Delete, Previous, and Next.

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 **FE**

Local Remote Link Logout ADMIN

Terminal Radio Ethernet IP QoS **Security** Maintenance Events Software Monitoring

Summary Setup Users SNMP RADIUS Manager Distribution

Local Radio OK MODE USB TX RX
● ● ● ● ●
 Status

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 v1
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

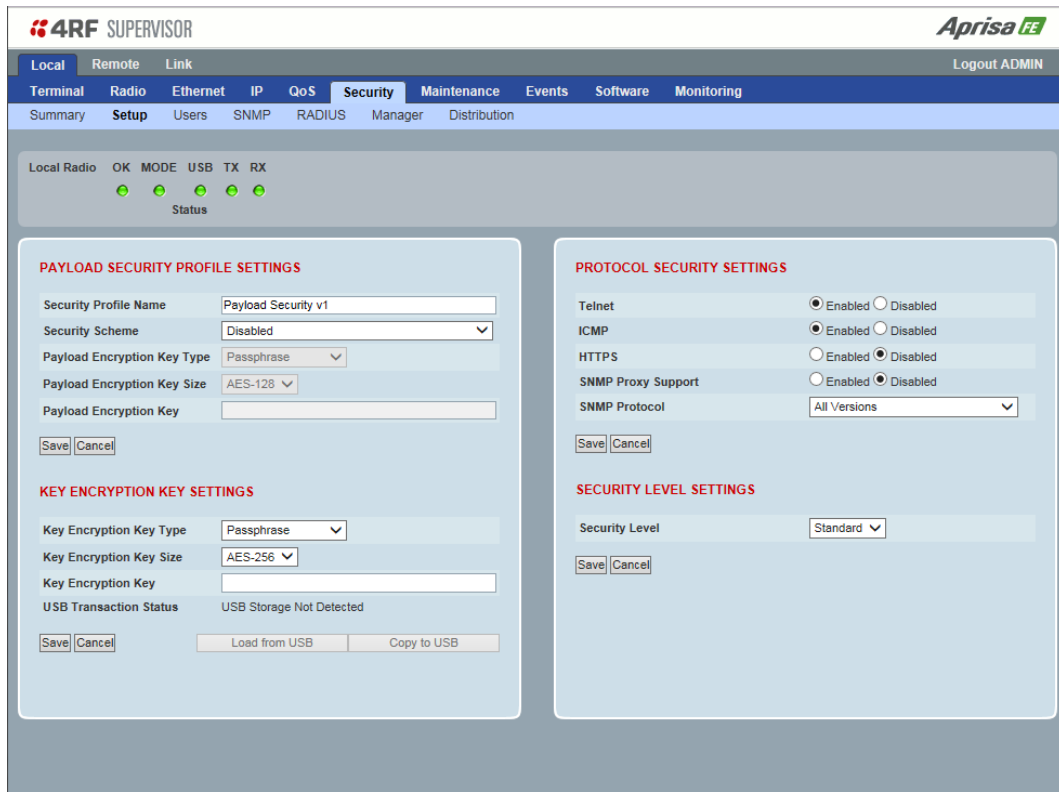
Telnet	Enabled
ICMP	Enabled
HTTPS	Disabled
SNMP Protocol	All Versions
SNMP Proxy Support	Disabled

SECURITY LEVEL SETTINGS

Security Level	Standard
----------------	----------

See 'Security > Setup' and 'Security > Manager' for configuration options.

Security > Setup


PAYLOAD SECURITY PROFILE SETTINGS
Security Profile Name

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

Security Scheme

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

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

The default setting is Disabled.

Payload Encryption Key Type

This parameter sets the Payload Encryption Key Type:

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

The default setting is Pass Phrase.

Payload Encryption Key Size

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

The higher the encryption size the better the security.

Payload Encryption Key

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

Pass Phrase

Good password policy:

- contains at least eight characters, and
- contains at least one upper case letter, and
- contains at least one lower case letter, and
- contains at least one digit or another character such as @+... , and
- is not a term in a familiar language or jargon, and
- is not identical to or derived from the accompanying account name, from personal characteristics or from information from one's family/social circle, and
- is easy to remember, for instance by means of a key sentence

Raw Hexadecimal

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

KEY ENCRYPTION KEY 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 the remote radio.

The Key Encryption Key Type, Key Encryption Key Size and Key Encryption Key must be the same on both radios in the link.

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 password format for better security. It must comply with the specified encryption key size e.g. if Encryption Type to AES128, the encryption key must be 16 bytes (32 chars)

The default setting is Pass Phrase.

Key Encryption Key Size

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

The higher the encryption type the better the security.

Key Encryption Key

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

PROTOCOL SETUP

Telnet option

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

ICMP option (Internet Control Message Protocol)

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

HTTPS option

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

SNMP Proxy Support

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

SNMP Protocol

This parameter sets the SNMP Protocol:

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

The default setting is All Versions.

The default SNMPv3 with Authentication User Details provided are:

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

SNMPv3 Authentication Passphrase

The 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.

To change a user authentication passphrase:

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

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

Utilities to generate these strings are available from NET-SNMP providers.

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

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

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

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

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

SECURITY LEVEL SETTINGS

Security Level

This parameter sets the active security features. The default setting is Standard.

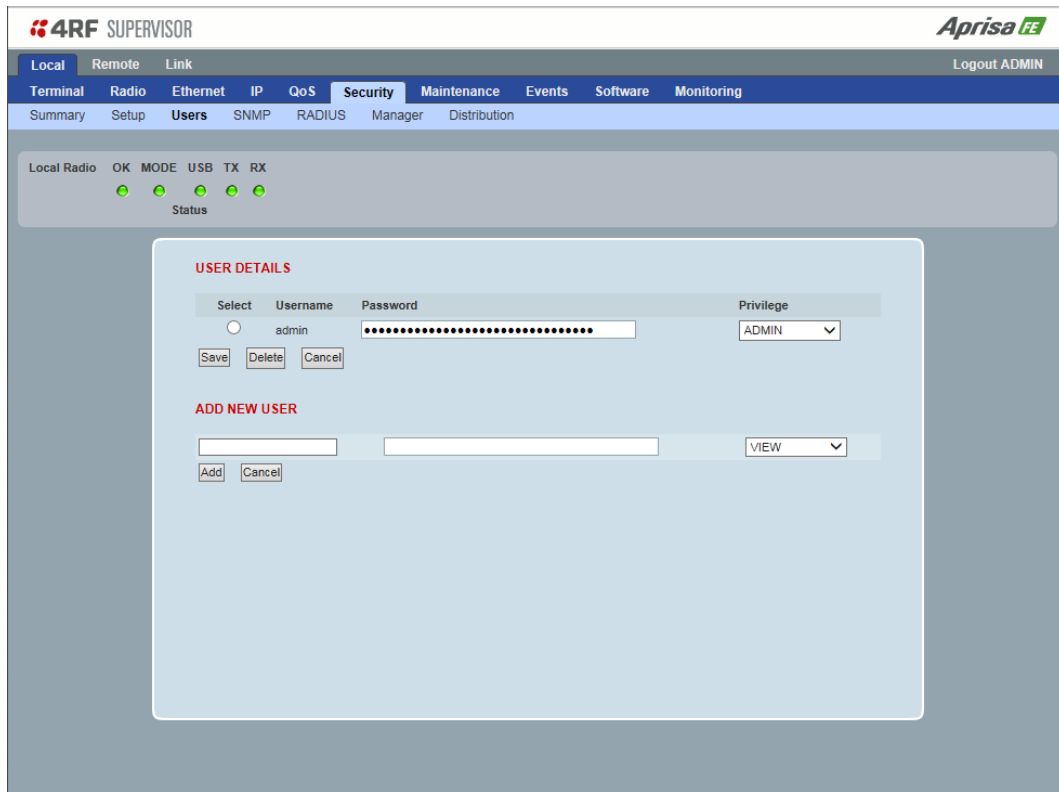
Option	Payload Encryption	HTTPS	SNMPv3	USB KEK Only
Standard	✓	✓	✓	
Strong	✓	✓	✓	✓

SNMPv3 Context Addressing

SNMPv3 is not user configurable and user can use this option with any NMS. The radio SNMP management interface supports SNMPv3/2 context addressing. The SNMPv3 context addressing allows the user to use secure SNMPv3 management while improving NMS performance.

A NMS (Network Management System) can access any radio directly by using its IP address or via the local radio 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.

Security > Users



Note: You must login with ‘admin’ privileges to add, disable, delete a user or change a password.

USER DETAILS

Shows a list of the current users setup in the radio.

ADD NEW USER

To add a new user:

1. Enter the Username.

A username can be up to 32 characters but cannot contain back slashes, forward slashes, spaces, tabs, single or double quotes. Usernames are case sensitive.

2. Enter the Password.

A password can be 8 to 32 characters but cannot contain back slashes, forward slashes, spaces, tabs, single or double quotes. Passwords are case sensitive.

Good password policy:

- contains at least eight characters, and
- contains at least one upper case letter, and
- contains at least one lower case letter, and
- contains at least one digit or another character such as !@#\$%^&(){}[]<>... , and
- is not a term in a familiar language or jargon, and
- is not identical to or derived from the accompanying account name, from personal characteristics or from information from one's family/social circle, and
- is easy to remember, for instance by means of a key sentence

3. Select the User Privileges

There are four pre-defined User Privilege settings to allocate access rights to users. These user privileges have associated default usernames and passwords of the same name.

The default login is 'admin'.

This login has full access to all radio parameters including the ability to add and change users. There can only be a maximum of two usernames with admin privileges and the last username with admin privileges cannot be deleted.

User Privilege	Default Username	Default Password	User Privileges
View	view	view	Users in this group can only view the summary pages.
Technician	technician	technician	Users in this group can view and edit parameters except Security > Users, Security > Settings and Advanced settings.
Engineer	engineer	engineer	Users in this group can view and edit parameters except Security > Users.
Admin	admin	admin	Users in this group can view and edit all parameters.

See 'SuperVisor Menu Access' on page 60 for the list of SuperVisor menu items versus user privileges.

4. Click 'Add'

To delete a user:

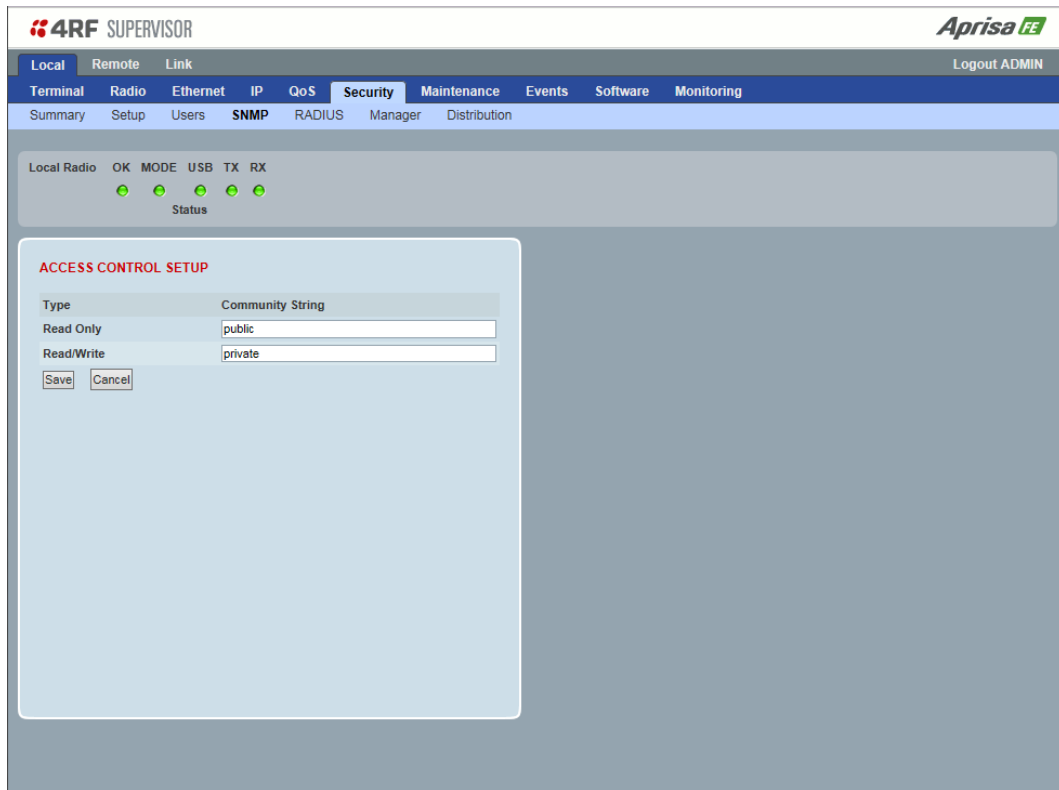
1. Select Terminal Settings > Security > Users
2. Click on the Select button for the user you wish to delete.
3. Click 'Delete'

To change a Password:

1. Select Terminal Settings > Security > Users
2. Click on the Select button for the user you wish to change the Password.
3. Enter the Password.

A password can be 8 to 32 characters but cannot contain back slashes, forward slashes, spaces, tabs, single or double quotes.

Security > SNMP



In addition to web-based management (SuperVisor), the link 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 FE 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 local radio and remote radio.

To access the local radio, 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 135).

SNMP access to the remote radio can be achieved by using the radio's IP address and the normal community string or by proxy in the local radio.

SNMP Access via Local radio Proxy

To access the remote radio via the local radio proxy, the community strings must be setup on the SNMP manager in the format:

`cccccccc:bbbbbb`

Where:

`cccccccc` is the community string of the local radio

and

`bbbbbb` is the last 3 bytes of the remote radio MAC address.

The SNMP Proxy Support must be enabled for this method of SNMP access to operate (see 'SNMP Proxy Support' on page 130).

Security > RADIUS

This page displays the current settings for the Security RADIUS.

The screenshot shows the 4RF SUPERVISOR interface for RADIUS configuration. At the top, there are navigation tabs for Local, Remote, and Link, and a sub-menu for Security. The RADIUS configuration is divided into three main sections:

- RADIUS AUTHENTICATION SETTINGS:** Includes fields for Authentication Mode (Local Authentication), Primary Server (None), and Secondary Server (None).
- RADIUS ACCOUNTING SETTINGS:** Includes fields for Primary Server (None) and Secondary Server (None).
- RADIUS ADVANCED SETTINGS:** Includes fields for Initial Transaction Timeout(s) (4), Default Transaction Timeout(s) (16), Maximum Retries (5), Maximum Retries Duration (s) (30), and Unknown Transaction Attributes (Ignore And Authenticate).

On the right side, there is a **RADIUS SERVER SETTINGS** table with the following data:

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

Buttons for Save and Cancel are located below the table.

RADIUS - Remote Authentication Dial In User Service

RADIUS is a client / server system that secures the Aprisa FE radio link against unauthorized access. It is based on open standard RFCs: RFC 2865/6, 5607, 5080 and 2869.

It is a protocol for remote user Authorization, Authentication and Accounting. A standard RADIUS interface is typically used in a pulled model in which the request (authentication query) originates from the radio (RADIUS client or Network Access Server (NAS)) attached to a network and the response is sent from the queried RADIUS servers.

When a radio client is configured to use RADIUS, any user of the radio client presents authentication information to the radio client. This might be with a CLI login prompt or window login (SuperVisor/NMS), where the user is expected to enter their username and password.

RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

User accounting information is delivered from the RADIUS client/NAS to a RADIUS accounting server during RADIUS authentication and authorization operation and transaction.

Transactions between the RADIUS client/NAS and RADIUS AAA server/accounting server are authenticated through the use of a shared secret, which is never sent over the network.

For a RADIUS server to respond to the Aprisa FE radio, it must be configured with and respond to the following **Management-Privilege-level** attributes:

- Admin Level = 4
- Engineer Level = 3
- Technician Level = 2
- Viewer Level = 1

RADIUS AUTHENTICATION SETTINGS

Authentication Mode

This parameter sets the Authentication Mode.

Option	Function
Local Authentication	No radius Authentication - allows any local user privilege
Radius Authentication	Only radius Authentication - no local user privilege
Radius Authentication and Local admin	Uses radius Authentication if it is available. If radius Authentication is not available, uses local Admin login
Radius Then Local Authentication	If the user is not authenticated in the radius server, it allows any local user privilege.
Local Then Radius Authentication	If the user is not allowed in the local user privilege, radius authentication is used.

Primary Server

This parameter sets which radius server is used as the primary server for authentication. Select one of the possible authentication servers setup in Radius Server Settings.

Secondary Server

This parameter sets which radius server is used as the secondary server for authentication. Select one of the possible authentication servers setup in Radius Server Settings.

RADIUS ACCOUNTING SETTINGS

Primary Server

This parameter sets which radius server is used as the primary server for accounting (log of user activity). Select one of the possible accounting servers setup in Radius Server Settings.

Secondary Server

This parameter sets which radius server is used as the secondary server for accounting. Select one of the possible accounting servers setup in Radius Server Settings.

RADIUS ADVANCED SETTINGS

Initial Transaction Timeouts (IRT) (seconds)

This parameter sets the initial time to wait before the retry mechanism starts when the server is not responding.

Default Transaction Timeouts (MRT) (seconds)

This parameter sets the maximum time between retries.

Maximum Retries (MRC)

This parameter sets the maximum number of retry attempts when the server is not responding.

Maximum Retries Duration (MRD) (seconds)

This parameter sets the maximum duration it will attempt retries when the server is not responding.

Unknown Transaction Attributes

This parameter sets the radio's response to unknown attributes received from the radius server.

Option	Function
Ignore and Authenticate	Ignore the unknown attributes and accept the authentication received from the radius server
Reject and Deny	Reject the authentication received from the radius server

RADIUS SERVER SETTINGS

Server Name

You can enter up to four radius servers 1-4.

IP Address

The IP address of the Radius server.

Port Number

The Port Number of the Radius server. RADIUS uses UDP as the transport protocol.

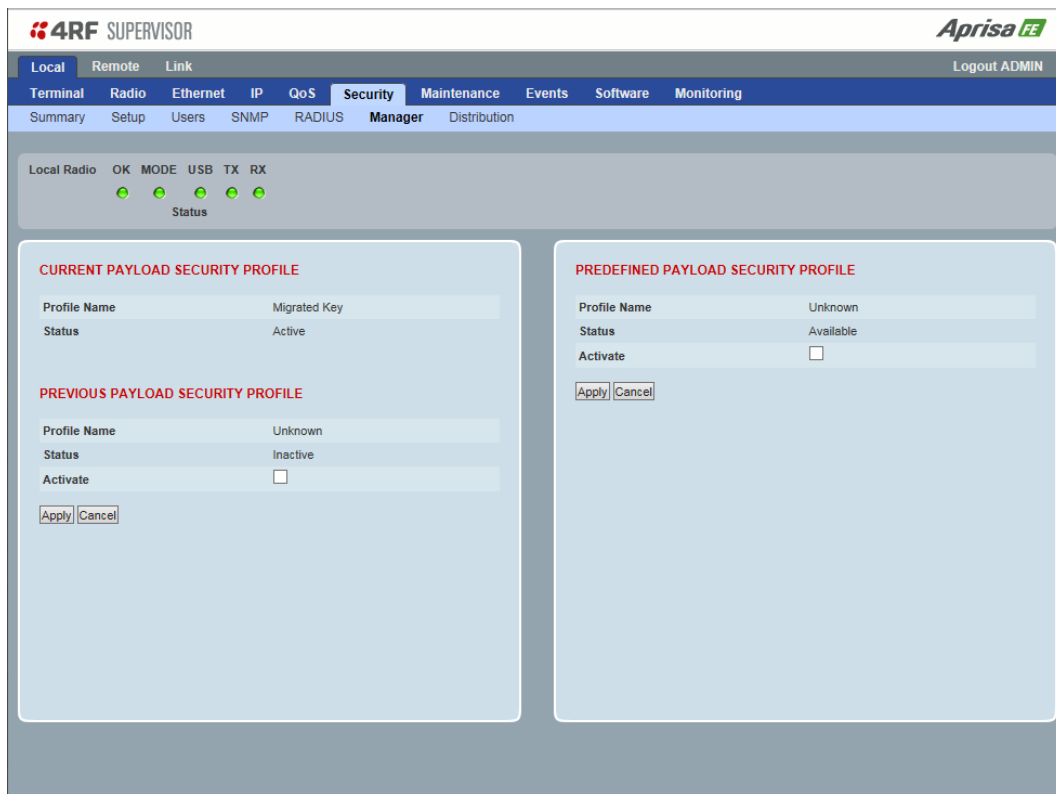
- UDP port 1812 is used for authentication / authorization
- UDP port 1813 is used for accounting.

Old RADIUS servers may use unofficial UDP ports 1645 and 1646.

Encryption Key

The password of the Radius server.

Security > Manager



CURRENT PAYLOAD SECURITY PROFILE

Profile Name

This parameter shows the predefined security profile active on the radio.

Status

This parameter displays the status of the predefined security profile on the radio (always active).

PREVIOUS PAYLOAD SECURITY PROFILE

Profile Name

This parameter displays the security profile that was active on the radio prior to the current profile being activated.

Status

This parameter displays the status of the security profile that was active on the radio prior to the current profile being activated.

Option	Function
Active	The security profile is active on the radio.
Inactive	The security profile is not active on the radio but could be activated if required.

Activate

This parameter activates the previous security profile (restores to previous version).

PREDEFINED PAYLOAD SECURITY PROFILE

Profile Name

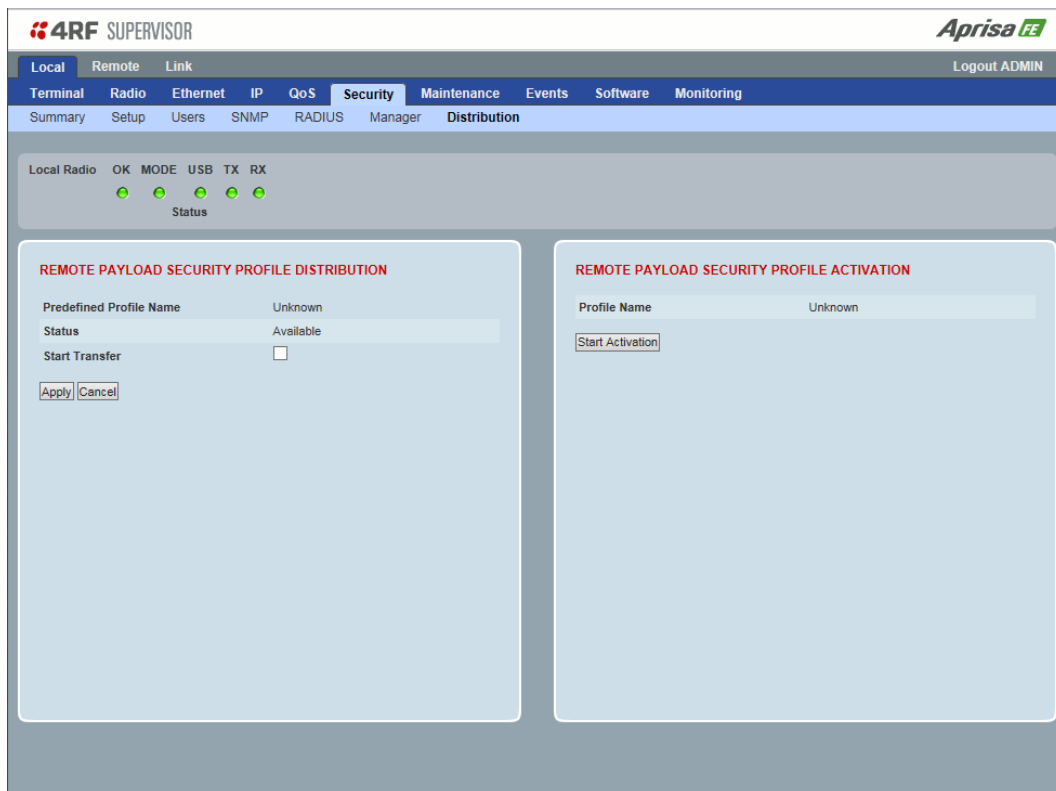
This parameter displays the new security profile that could be activated on the radio or distributed to the remote radio with Security > Distribution.

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 127.
Available	A predefined security profile is available on this radio for distribution and activation.

Security > Distribution



REMOTE PAYLOAD SECURITY PROFILE DISTRIBUTION

Predefined Profile Name

This parameter displays the predefined security profile available for distribution to the remote radio.

Status

This parameter shows if a predefined security profile is available for distribution to the remote radio.

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 the remote radio.

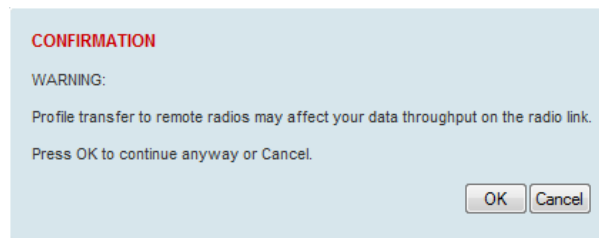
Note: The distribution of the payload security profile to the remote radio does not stop customer traffic from being transferred.

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 the remote radio:

This process assumes that a payload security profile has been setup (see 'Security > Setup' on page 127).

1. Tick Start Transfer and click Apply.



Note: This process could take up to 1 minute depending on channel size, Ethernet Management Priority setting and the amount of customer traffic on the link.

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 the remote radio, the security profile is then activated in the remote radio with this command.

The local radio will always attempt to distribute the profile successfully. This broadcast distribution has its own retry mechanism. The user can find out if the remote radio has 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 radio 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 the remote radio.

To activate the security profile in the remote radio:

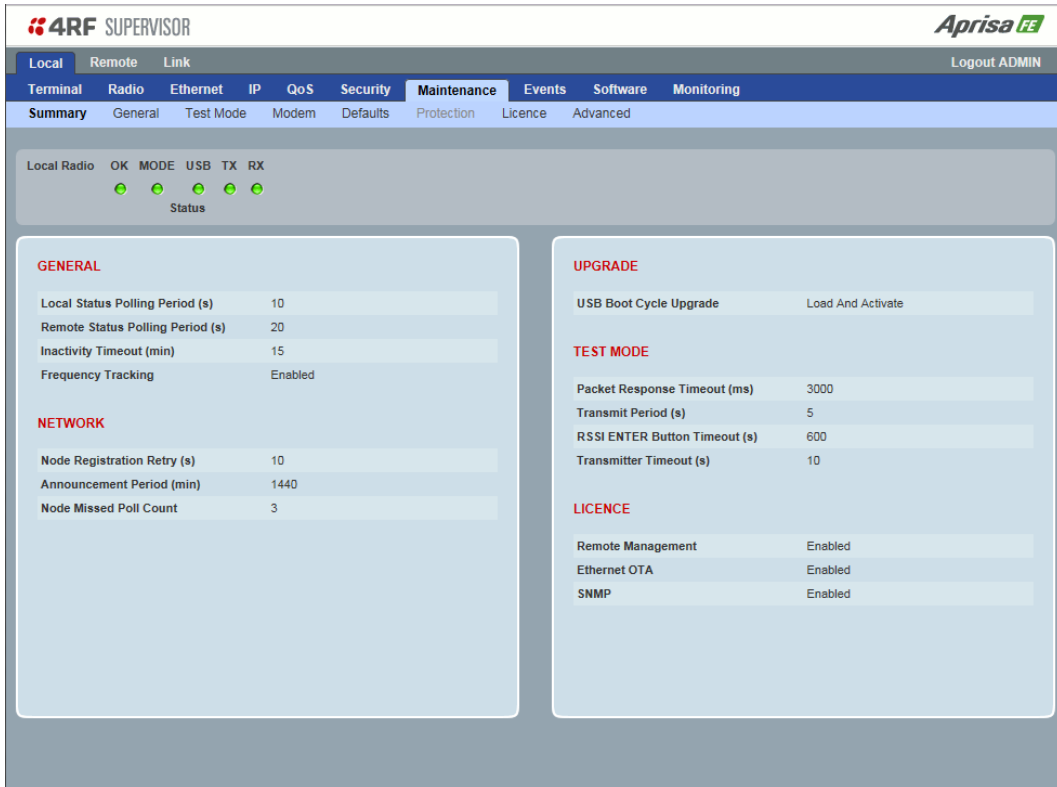
This process assumes that a security profile has been setup into the local radio (see 'Security > Setup' on page 127) and distributed to the remote radio.

Note: Do not navigate SuperVisor away from this page during the activation process (SuperVisor can lose PC focus).

Maintenance

Maintenance > Summary

This page displays the current settings for the Maintenance parameters.



DIAGNOSTICS

Last RX Packet RSSI (dBm)

This parameter displays the receiver RSSI reading taken from the last data packet received.

GENERAL

Local Status Polling Period (sec)

This parameter displays the rate at which SuperVisor refreshes the local radio alarm LED states and RSSI value.

Remote Status Polling Period (sec)

This parameter displays the rate at which SuperVisor refreshes the remote radio alarm LED states and RSSI value.

Inactivity Timeout (min)

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

Frequency Tracking

This parameter displays if Frequency Tracking is enabled or disabled.

NETWORK

Node Registration Retry (sec)

This parameter displays the local radio poll time at startup or the remote radio time between retries until registered.

Local radio Announcement Period (min)

This parameter displays the period between local radio polls post startup. The default setting is 1440 minutes (24 hours).

Node Missed Poll Count

This parameter displays the number of times the local radio attempts to poll the link at startup or if a duplicate IP is detected when a remote radio is replaced.

RF Interface MAC address

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

UPGRADE

USB Boot Cycle Upgrade

This parameter shows the type of USB Boot Cycle upgrade defined in ‘Software Setup > USB Boot Upgrade’ on page 174.

TEST MODE

Packet Response Timeout (ms)

This parameter displays the time Test Mode waits for a response from the local radio before it times out and retries.

Transmit Period (sec)

This parameter displays the time between Test Mode requests to the local radio.

Response Timeout (ms)

This parameter sets the time Test Mode waits for a response from the local radio before it times out and retries. The default setting is 3000 ms.

RSSI Enter Button Timeout (sec)

This parameter displays the Test Mode timeout period. The radio will automatically exit Test Mode after the Timeout period.

Transmitter Timeout (sec)

This parameter displays the transmitter Test Mode timeout period. The radio will automatically exit the transmitter Test Mode after the Timeout period.

LICENCE

Remote Management

This parameter displays if Remote Management is enabled or disabled. The default setting is enabled.

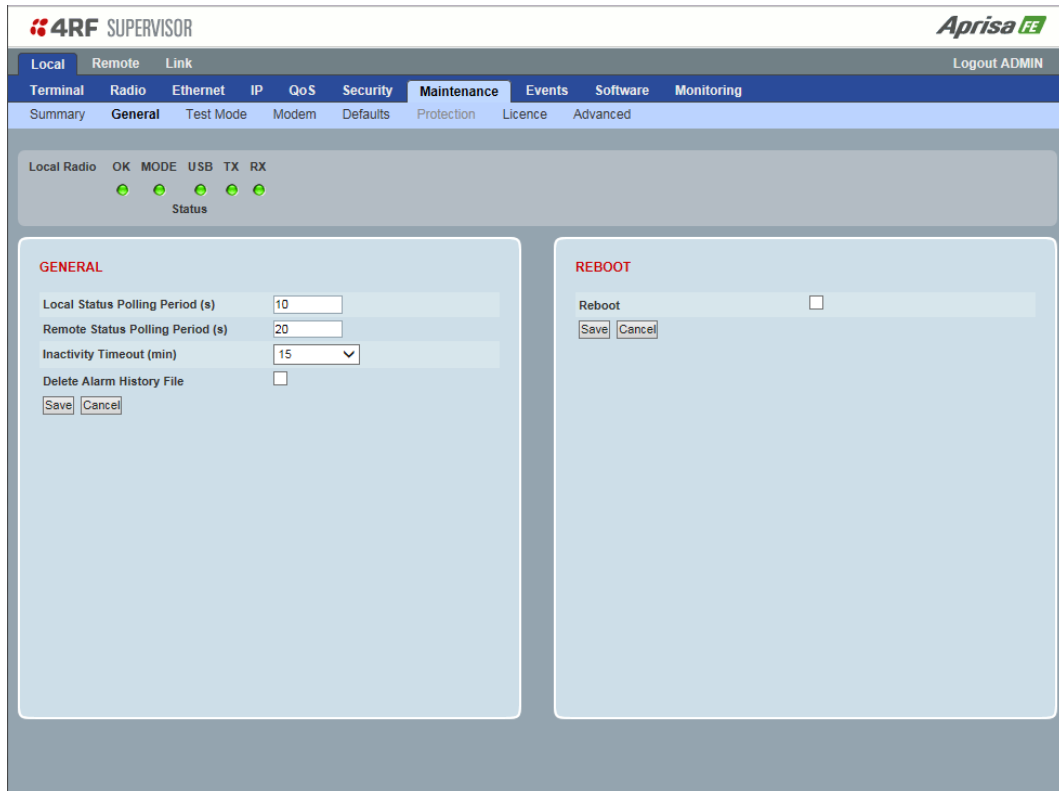
Ethernet OTA (over the air)

This parameter displays if Ethernet traffic is enabled or disabled. The Ethernet OTA will be always enabled by default and the license will be entered as a 4RF factory default (see 'Maintenance > Licence' on page 154).

SNMP Management

This parameter displays if SNMP management is enabled or disabled. The default setting is enabled.

Maintenance > General


GENERAL
Local Status Polling Period (sec)

This parameter sets the rate at which SuperVisor refreshes the local radio alarm LED states and RSSI value. The default setting is 10 seconds.

Network View Polling Period (sec)

This parameter sets the rate at which SuperVisor polls the remote radio 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 FE links, ensure that the Remote Polling Period is set to be longer than the Inband Management Timeout (set on page 67). The default setting is 20 seconds.

Inactivity Timeout (min)

This parameter sets the period of user inactivity before SuperVisor automatically logs out of the radio. The default setting is 15 minutes.

Write Alarm History to USB

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

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

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

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

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

State

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

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

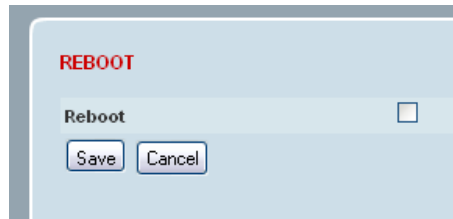
Delete Alarm History file

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

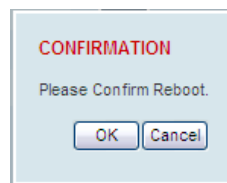
REBOOT

To reboot the radio:

1. Select Maintenance > General.
2. Tick the 'Reboot' checkbox.



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



4. Click 'OK' to reboot the radio or 'Cancel' to abort.

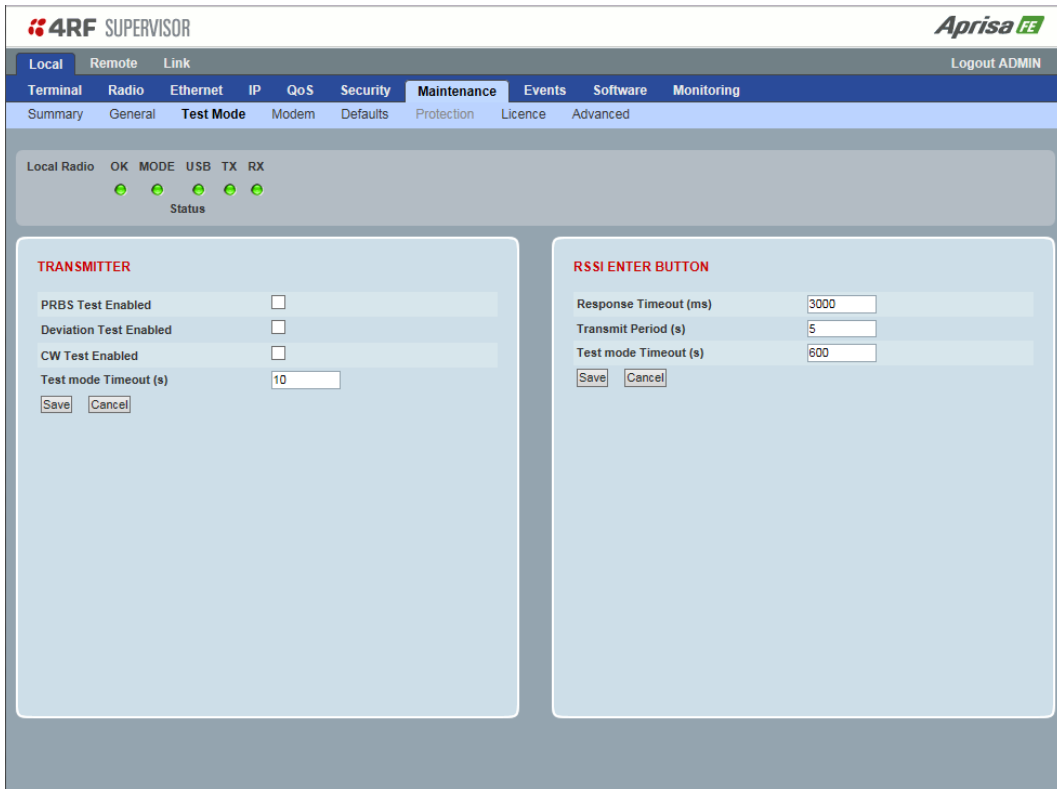
All the radio LEDs will flash repeatedly for 1 second.

The radio will be operational again in about 10 seconds.

The OK, MODE and USB LEDs will light green and the TX and RX LEDs will be green (steady or flashing) if the link is operating correctly.

5. Login to SuperVisor.

Maintenance > Test Mode



TRANSMITTER

PRBS Test Enabled

When active, the transmitter outputs a continuous PRBS signal. This can be used for evaluating the output spectrum of the transmitter and verifying adjacent channel power and spurious emission products.

Deviation Test Enabled

When active, the transmitter outputs a sideband tone at the deviation frequency used by the CPFSK modulator. This can be used to evaluate the local oscillator leakage and sideband rejection performance of the transmitter.

CW Test Enabled

When active, the transmitter outputs a continuous wave signal. This can be used to verify the frequency stability of the transmitter.

Test Mode Timeout (s)

This parameter sets the Transmitter Test Mode timeout period. The radio will automatically exit Transmitter Test Mode after the Timeout period. The default setting is 10 seconds.

RSSI TEST BUTTON

Response Timeout (ms)

This parameter sets the time RSSI Test Mode waits for a response from the local radio before it times out and retries. The default setting is 3000 ms.

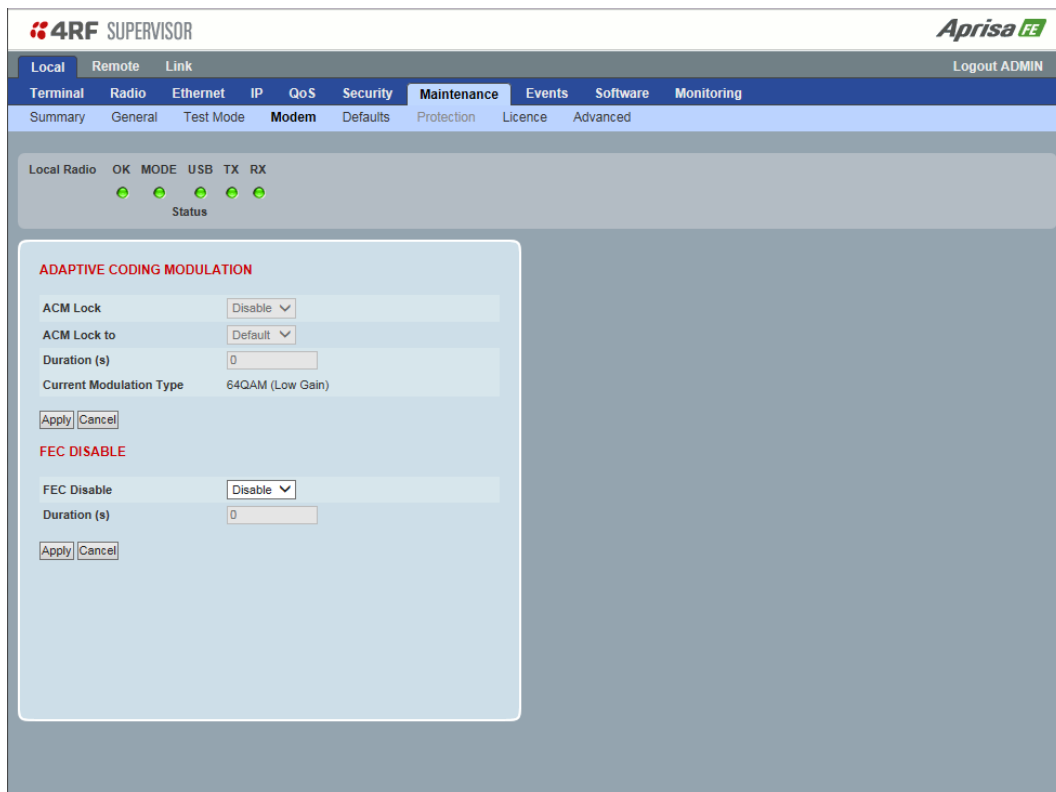
Transmit Period (sec)

This parameter sets the time between RSSI Test Mode requests to the local radio. 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



FEC DISABLE

FEC Disable

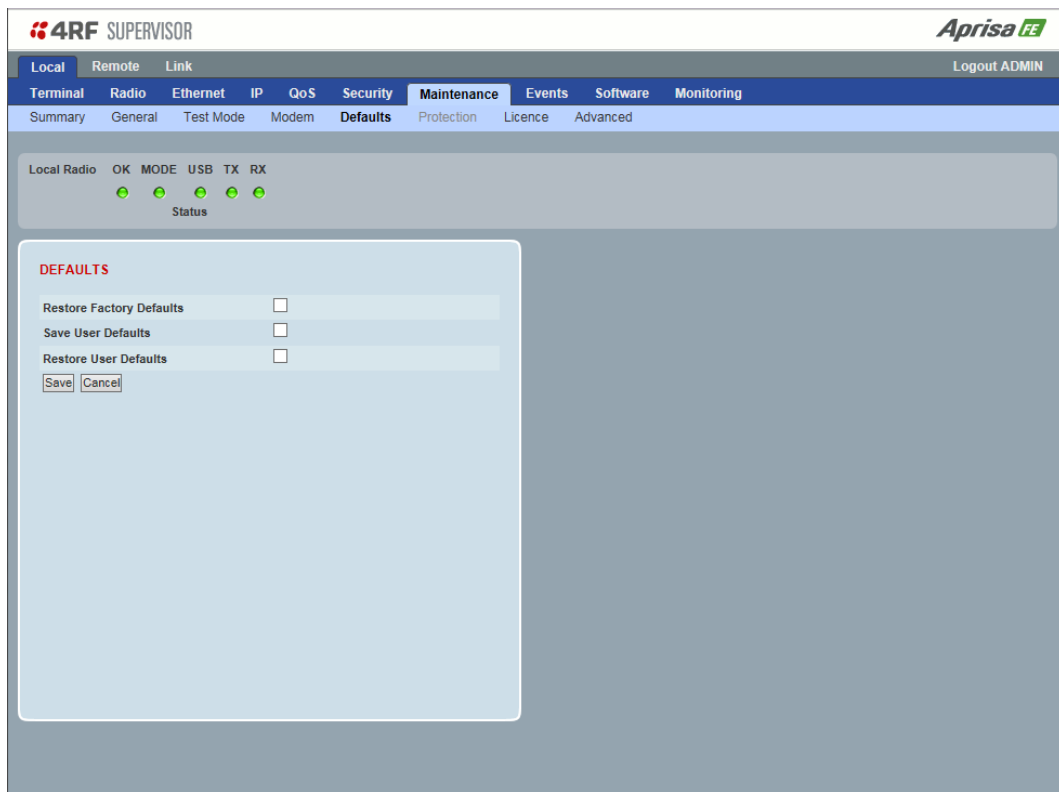
This parameter sets whether the Forward Error Correction can be disabled.

Option	Function
Enable	Enables the FEC Disable diagnostic function
Disable	Disables the FEC Disable diagnostic function
Timer	Allows the FEC to be disabled but only for a predetermined period.

Duration (s)

This parameter defines the period required for disabling of the FEC. When this period elapses, the FEC is enabled.

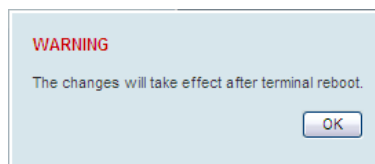
Maintenance > Defaults


DEFAULTS

The Maintenance Defaults page is only available for the local terminal.

Restore Factory Defaults

When activated, all radio parameters will be set to the factory default values. This includes resetting the radio IP address to the default of 169.254.50.10.



Note: Take care using this command.

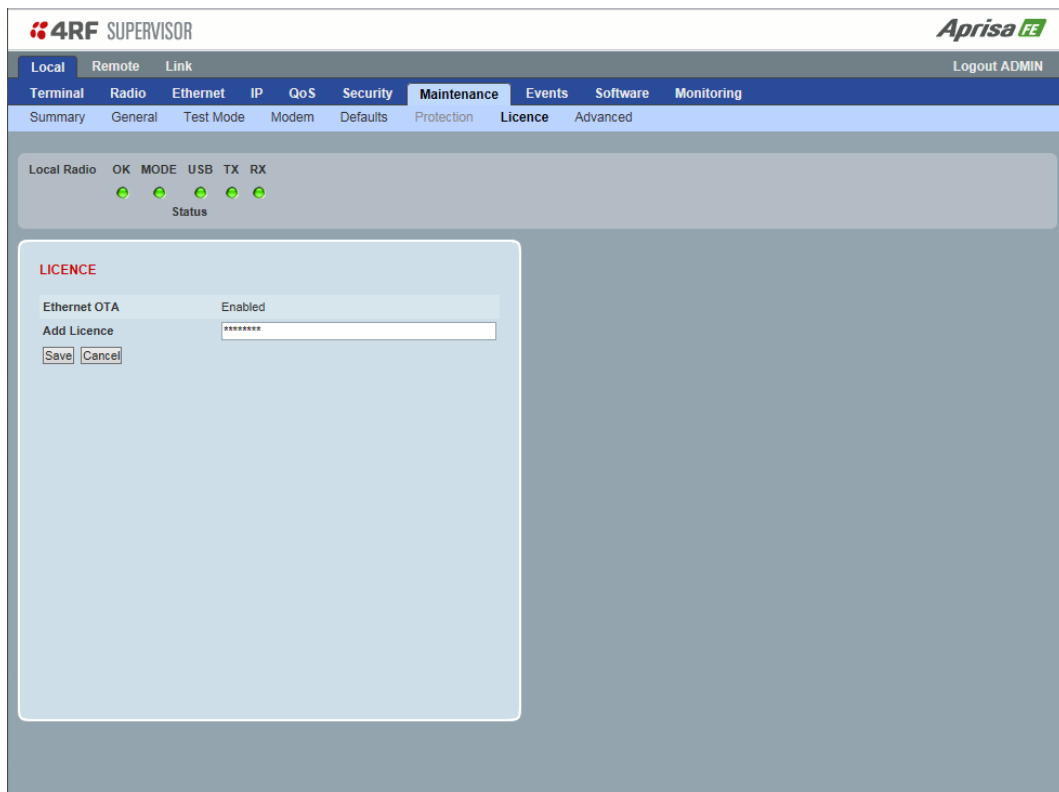
Save User Defaults

When activated, all current radio parameter settings will be saved to non-volatile memory within the radio.

Restore User Defaults

When activated, all radio parameters will be set to the settings previously saved using ‘Save User Defaults’.

Maintenance > Licence



LICENCE

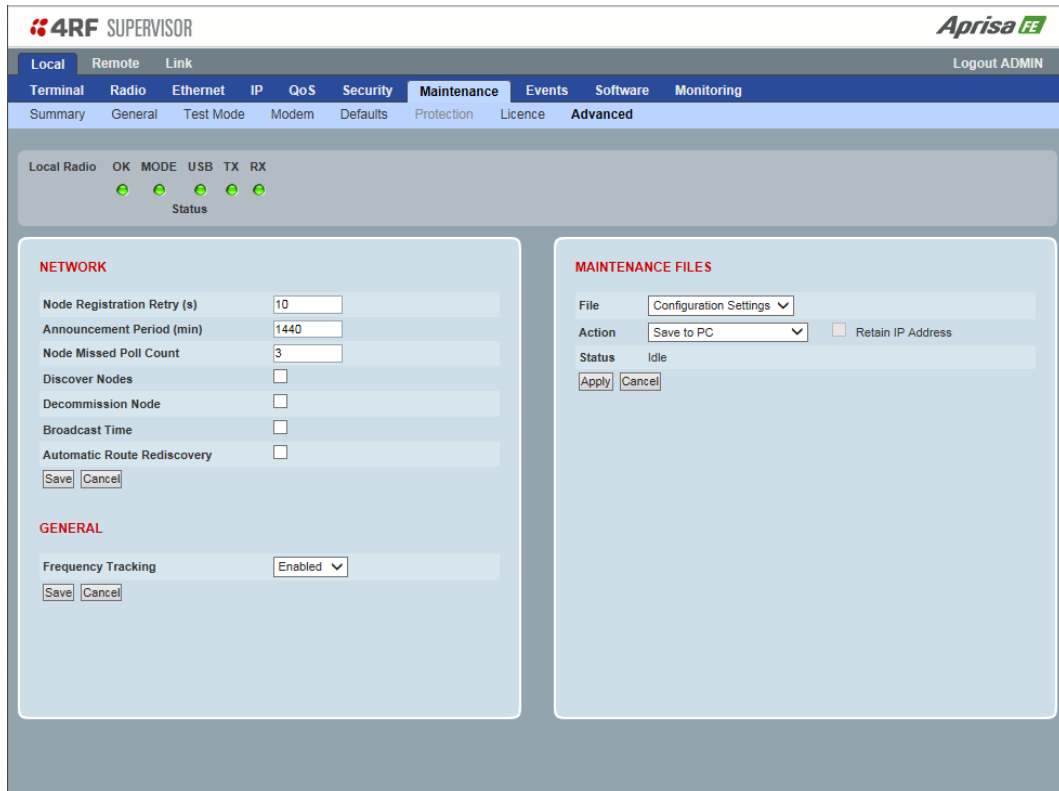
Fully Featured Radio

When a fully featured Aprisa FE 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
APFE-N400-SSC-B1-30-EN <u>AA</u>	4RF FE, 1+0, 400-470 MHz, SSC, B1, 300 mm, EN, <u>AA</u>

In this software version, Remote Management, Ethernet Traffic and SNMP management are enabled by default.

Maintenance > Advanced



NETWORK

Node Registration Retry (sec)

This parameter sets the local radio poll time at startup or the remote radio time between retries until registered. The default setting is 10 seconds.

Announcement Period (min)

This parameter sets the period between local radio polls post startup. The default setting is 1440 minutes (24 hours).

If a critical parameter is changed in the local radio, such as IP address, then the change is distributed to the remote radio using the announcement message. Note that in this case, an announcement is sent immediately independent of the Announcement Period setting.

Node Missed Poll Count

This parameter sets the number of times the local radio attempts to poll the remote radio at startup. The default setting is 3.

Discover Nodes

This parameter when activated triggers the local radio to poll the remote radio with Node Missed Poll Count and Node Registration Retry values.

Decommission Node(s)

This parameter when activated resets the registration to remove the remote radio from service.

Note: Take care using this option.

Broadcast Time

This parameter when activated sends the local radio Date / Time setting to all the remote radio and sets their Date / Time. This option applies to the local radio 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 link. 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, each radio in the link adjusts their receive frequency to the frequency of the incoming packet rate.

The default setting is Enabled.

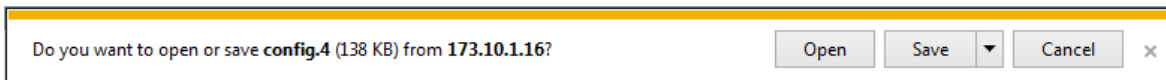
MAINTENANCE FILES

There are three maintenance file types which can saved / restored to / from PC or USB flash drive:

File - Configuration Settings

Action

Action	Option
Save to PC	This saves the file with a filename of 'Config.4' to a binary encrypted file. This can then be saved from the Browser popup (example is Windows Internet Explorer 11). The file should be renamed to be able to identify the radio it was saved from.



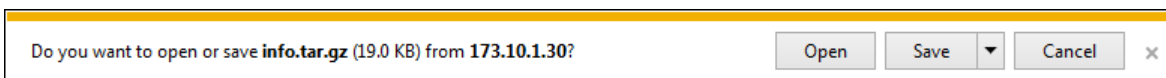
Save to Radio USB	This saves the file with a filename of 'asrcfg_1.5.0' to a binary encrypted file on the radio USB flash drive root directory.
Restore from PC	This restores all user configuration settings from a binary encrypted file on a PC directory to the radio. A reboot warning message will warn of a pending reboot after the PC file is selected. Clicking OK will open a browser file selection window to select the file. Note: If you are using Explorer, it must be IE10 or above for this feature to work correctly.
Restore from Radio USB	This restores all user configuration settings from a binary encrypted file on the USB root directory to the radio.

Note: 'Payload Encryption Key' and 'Key Encryption Key' parameters (see 'Security > Setup') are not saved to the configuration file. When a 'Restore from PC' or 'Restore from Radio USB' is used, these parameters will retain their existing values so are not changed by the operation of restoring the configuration file.

File - Event History Log

Action

Action	Option
Save to PC	This saves the file with a filename of 'Info.tar.gz' to a binary encrypted file. This can then be saved from the Browser popup (example is Windows Internet Explorer 11). The file should be renamed to be able to identify the radio it was saved from. The 'gz' file is normally for sending back to 4RF Limited for analysis but can be opened with WinRar.



Save to Radio USB	This saves the file with a filename of e.g. 'alarm_173.10.1.30_2014-11-10,15.54.14.txt' to a text file on the radio USB flash drive root directory.
-------------------	---

File - Configuration Script

Action

Action	Option
Load and Execute	<p>This loads and executes configuration script files.</p> <p>These are sample configuration script files on the product CD in a directory 'Master Configuration'.</p> <p>The purpose of these files is to use as templates to create your own configuration scripts.</p> <p>Note: Be careful using this feature as incompatible configurations will change the radios settings and break radio connectivity.</p>

Note: Activating this function will over-write all existing configuration settings in the radio (except for the non-saved settings e.g. security passwords, licence keys etc) without any verification of the command setting in the radio. Precautions should be taken to prevent radio outages with incorrect radio configurations. The following process steps are recommended:

- a. Save the current radio configuration to a PC or USB before uploading the new configuration script file
 - b. Upload the new configuration script file to the radio
 - c. If for some reason the radio doesn't work as expected, the saved configuration file can be uploaded to the radio (roll back to previous configuration).
-

Retain IP Address

This parameter when enabled ensures that the radio IP address is not changed when the radio configuration settings are restored from a configuration file with a different IP radio address. It prevents the radio losing connectivity when the configuration settings are restored from a configuration file.

Revert Config if Connection Lost

When the Maintenance Files feature is used on remote radios from the local radio, this parameter allows the configurations to be restored to the previous configuration if the connection is lost.

This must be set before executing the Configuration Settings / Configuration Script restore functions.

Events

The Events menu contains the setup and management of the alarms, alarm events and traps.

Events > Alarm Summary

There are two types of events that can be generated on the Aprisa FE radio. These are:

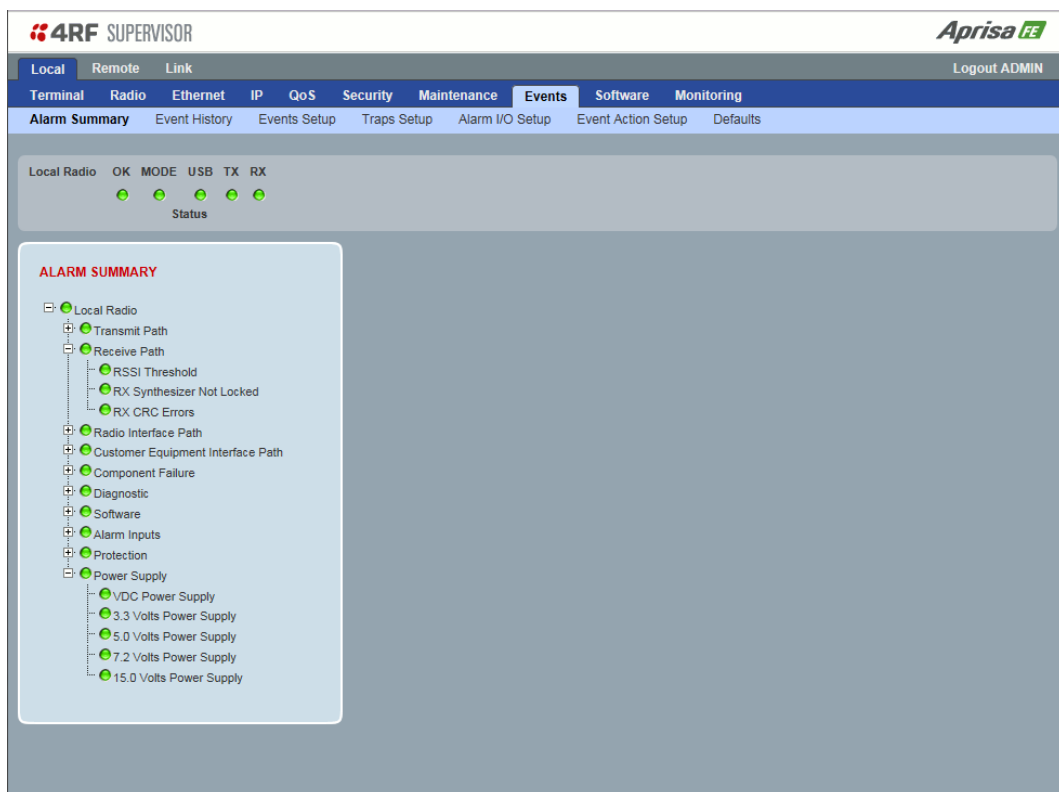
1. Alarm Events

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 299 for a complete list of events.

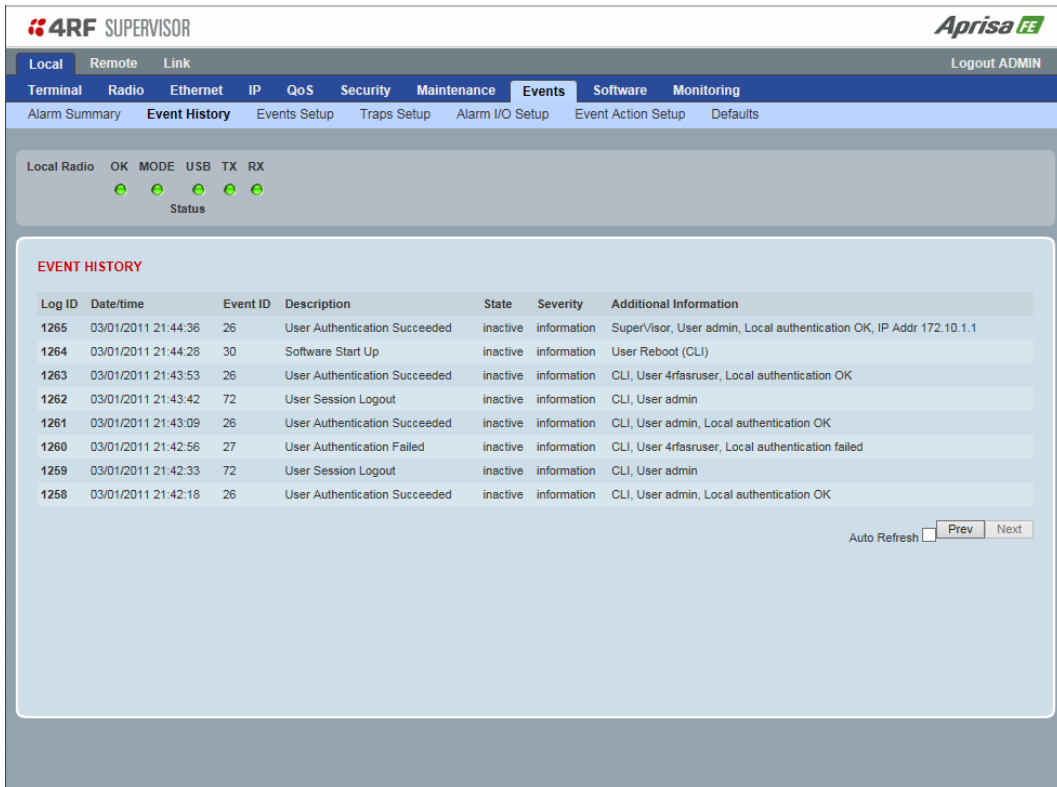


ALARM SUMMARY

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 FE

Local Remote Link Logout ADMIN

Terminal Radio Ethernet IP QoS Security Maintenance **Events** Software Monitoring

Alarm Summary **Event History** Events Setup Traps Setup Alarm I/O Setup Event Action Setup Defaults

Local Radio OK MODE USB TX RX

Status

EVENT HISTORY

Log ID	Date/time	Event ID	Description	State	Severity	Additional Information
1265	03/01/2011 21:44:36	26	User Authentication Succeeded	inactive	information	SuperVisor, User admin, Local authentication OK, IP Addr 172.10.1.1
1264	03/01/2011 21:44:28	30	Software Start Up	inactive	information	User Reboot (CLI)
1263	03/01/2011 21:43:53	26	User Authentication Succeeded	inactive	information	CLI, User 4rfasruser, Local authentication OK
1262	03/01/2011 21:43:42	72	User Session Logout	inactive	information	CLI, User admin
1261	03/01/2011 21:43:09	26	User Authentication Succeeded	inactive	information	CLI, User admin, Local authentication OK
1260	03/01/2011 21:42:56	27	User Authentication Failed	inactive	information	CLI, User 4rfasruser, Local authentication failed
1259	03/01/2011 21:42:33	72	User Session Logout	inactive	information	CLI, User admin
1258	03/01/2011 21:42:18	26	User Authentication Succeeded	inactive	information	CLI, User admin, Local authentication OK

Auto Refresh Prev Next

EVENT HISTORY

The last 1500 events are stored in the radio. The complete event list can be downloaded to a USB flash drive (see 'Write Alarm History to USB' on page 148).

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

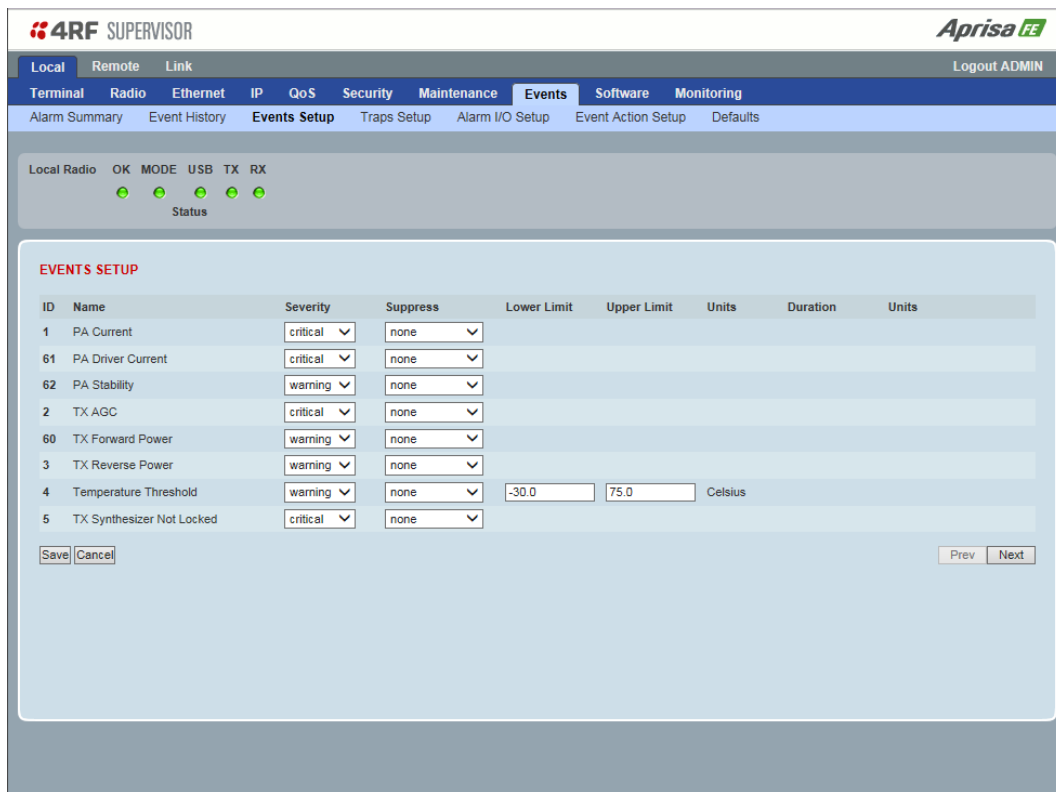
The Next button will display the next page of 8 events and the Prev button will display the previous page of 8 events. Using these buttons will disable Auto Refresh to prevent data refresh and page navigation contention.

The last 50 events stored in the radio are also accessible via an SNMP command.

Auto Refresh

The Event History page selected will refresh automatically every 12 seconds if the Auto Refresh is ticked.

Events > Events Setup


EVENTS SETUP

Alarm event parameters can be configured for all alarm events (see ‘Alarm Events’ on page 300).

All active alarms for configured alarm events will be displayed on the Monitoring pages (see ‘Monitoring’ on page 187).

The Switch and Block parameters are only visible / applicable when the radio is part of a Protected Station.

Severity

The Severity parameter sets the alarm severity.

Severity	Function
Critical	The Critical severity level indicates that a service affecting condition has occurred and an immediate corrective action is required. Such a severity can be reported, for example, when a managed object becomes totally out of service and its capability must be restored.
Major	The Major severity level indicates that a service affecting condition has developed and an urgent corrective action is required. Such a severity can be reported, for example, when there is a severe degradation in the capability of the managed object and its full capability must be restored.
Minor	The Minor severity level indicates the existence of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious (for example, service affecting) fault. Such a severity can be reported, for example, when the detected alarm condition is not currently degrading the capacity of the managed object.
Warning	The Warning severity level indicates the detection of a potential or impending service affecting fault, before any significant effects have been felt. Action should be taken to further diagnose (if necessary) and correct the problem in order to prevent it from becoming a more serious service affecting fault.

Information	No problem indicated - purely information
-------------	---

Suppress

This parameter determines if the action taken by an alarm.

Option	Function
None	Alarm triggers an event trap and is logged in the radio
Traps	Alarm is logged in the radio but does not trigger an event trap
Traps and Log	Alarm neither triggers an event trap nor is logged in the radio

Lower Limit / Upper Limit

Threshold alarm events have lower and upper limit settings. The alarm is activated if the current reading is outside the limits.

Example: 9 RX CRC Errors

The Upper Limit is set to 0.7 and the Duration is set to 5 seconds.

If in any 5 second period, the total number of errored packets divided by the total number of received packets exceeds 0.7, the alarm will activate.

Units (1)

The Units parameter shows the unit for the Lower Limit and Upper Limit parameters.

Duration

This parameter determines the period to wait before an alarm is raised if no data is received.

Units (2)

This parameter shows the unit for the Duration parameters.

Switch

This parameter determines if the alarm when active causes a switch over of the Protection Switch.

This parameter is only applicable when the radio is part of a Protected Station.

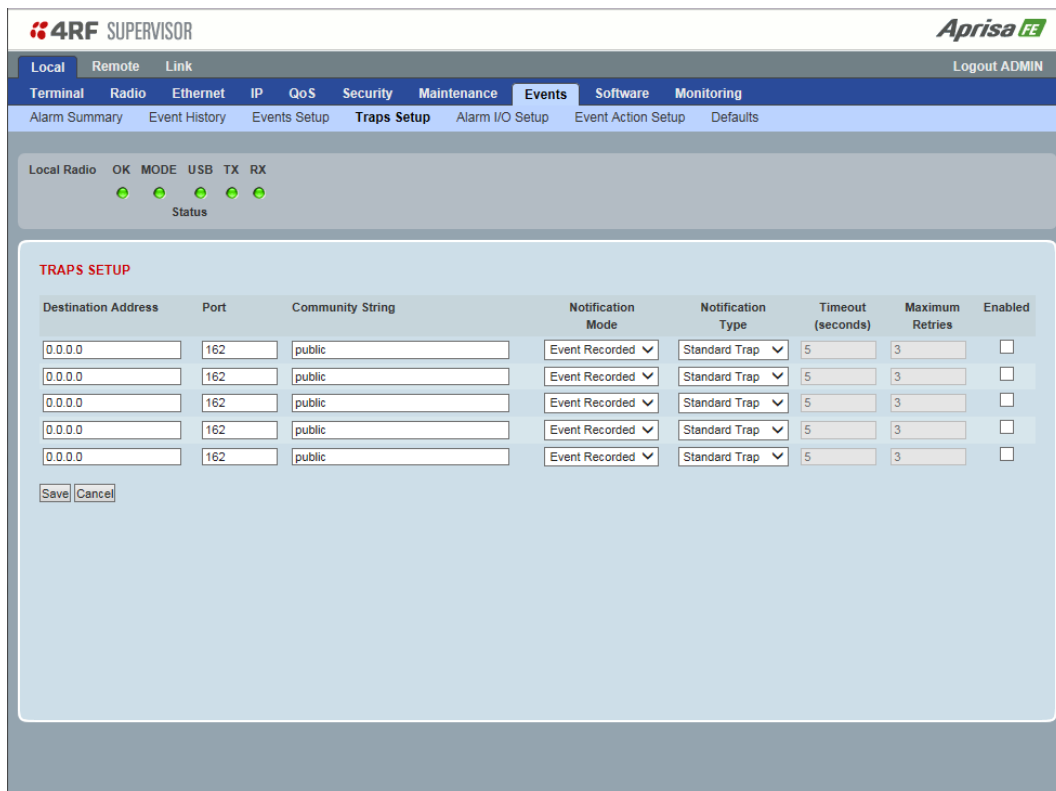
Block

This parameter determines if the alarm is prevented from causing a switch over of the Protection Switch.

This parameter is only applicable when the radio is part of a Protected Station.

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

Events > Traps Setup



TRAPS SETUP

All events can generate SNMP traps. The types of traps that are supported are defined in the ‘Notification Mode’.

Destination Address

This parameter sets the IP address of the server running the SNMP manager.

Port

This parameter sets the port number the server running the SNMP manager.

Community String

This parameter sets the community string which is sent with the IP address for security. The default community string is ‘public’.

Notification Mode

This parameter sets when an event related trap is sent:

Option	Function
None	No event related traps are sent.
Event Recorded	When an event is recorded in the event history log, a trap is sent.
Event Updated	When an event is updated in the event history log, a trap is sent.
All Events	When an event is recorded or updated in the event history log, a trap is sent.

Notification Type

This parameter sets the type of event notification:

Option	Function
Standard Trap	Provides a standard SNMP trap event
Inform Request	Provides a SNMP v2 Inform Request trap event including trap retry and acknowledgement

Notification Type set to Inform Request:

Timeout (second)

This parameter sets the time interval to wait for an acknowledgement before sending another retry.

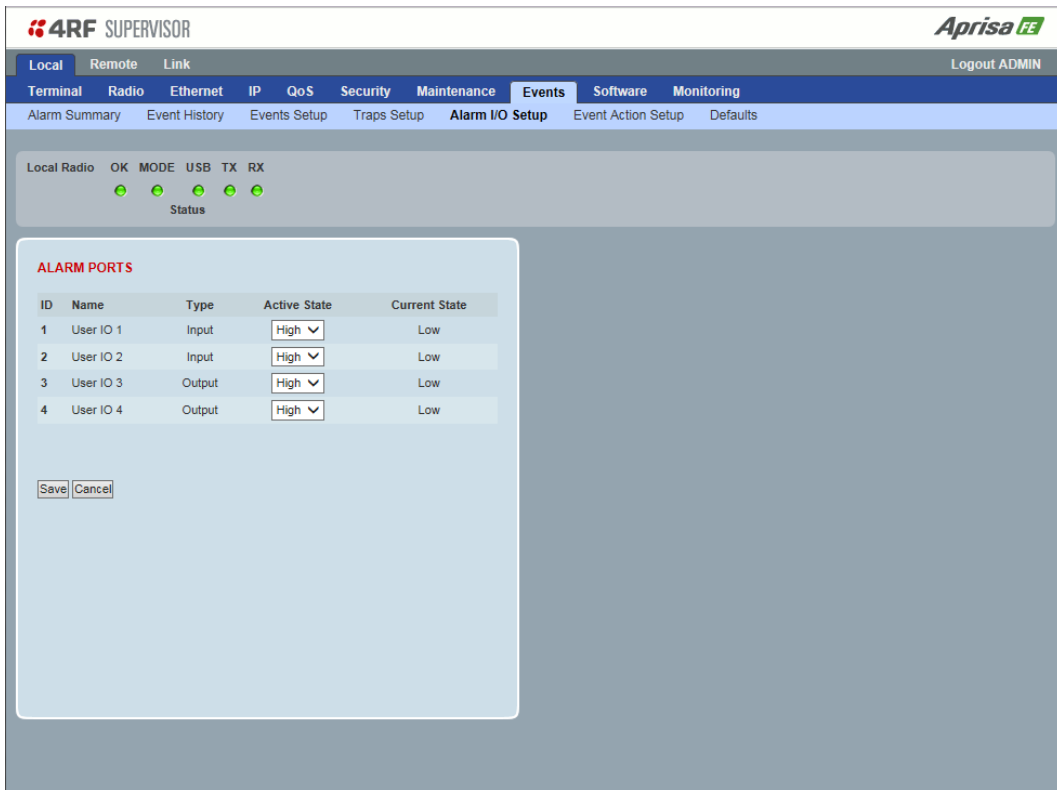
Maximum Retries

This parameter sets the maximum number of retries to send the event without acknowledgement before it gives up.

Enabled

This parameter determines if the entry is used.

Events > Alarm I/O Setup



The screenshot shows the 4RF Supervisor web interface. At the top, there is a navigation menu with options: Local, Remote, Link, Terminal, Radio, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring. Below this is a sub-menu for Alarm I/O Setup, including Alarm Summary, Event History, Events Setup, Traps Setup, Alarm I/O Setup, Event Action Setup, and Defaults. The main content area displays a status bar for Local Radio with indicators for OK, MODE, USB, TX, and RX. Below this is a section titled "ALARM PORTS" containing a table with columns for ID, Name, Type, Active State, and Current State. The table lists four entries: User IO 1 (Input), User IO 2 (Input), User IO 3 (Output), and User IO 4 (Output). Each entry has a dropdown menu for the Active State, currently set to "High". At the bottom of the table, there are "Save" and "Cancel" buttons.

ID	Name	Type	Active State	Current State
1	User IO 1	Input	High	Low
2	User IO 2	Input	High	Low
3	User IO 3	Output	High	Low
4	User IO 4	Output	High	Low

ALARM PORTS

This page provides control of the two hardware alarm inputs and two hardware alarm outputs provided on the alarm connector.

The alarm inputs are used to transport alarms to the other radios in the network. The alarm outputs are used to receive alarms from other radios in the network.

These alarms are only available when the station is non protected.

Name

The alarm IO number.

Type

The Type shows if the alarm is an input or output.

Active State

The Active State parameter sets the alarm state when the alarm is active.

Alarm Input

Option	Function
Low	The alarm is active low i.e. a ground contact on the port will cause an active alarm state
High	The alarm is active high i.e. an open contact on the port will cause an active alarm state

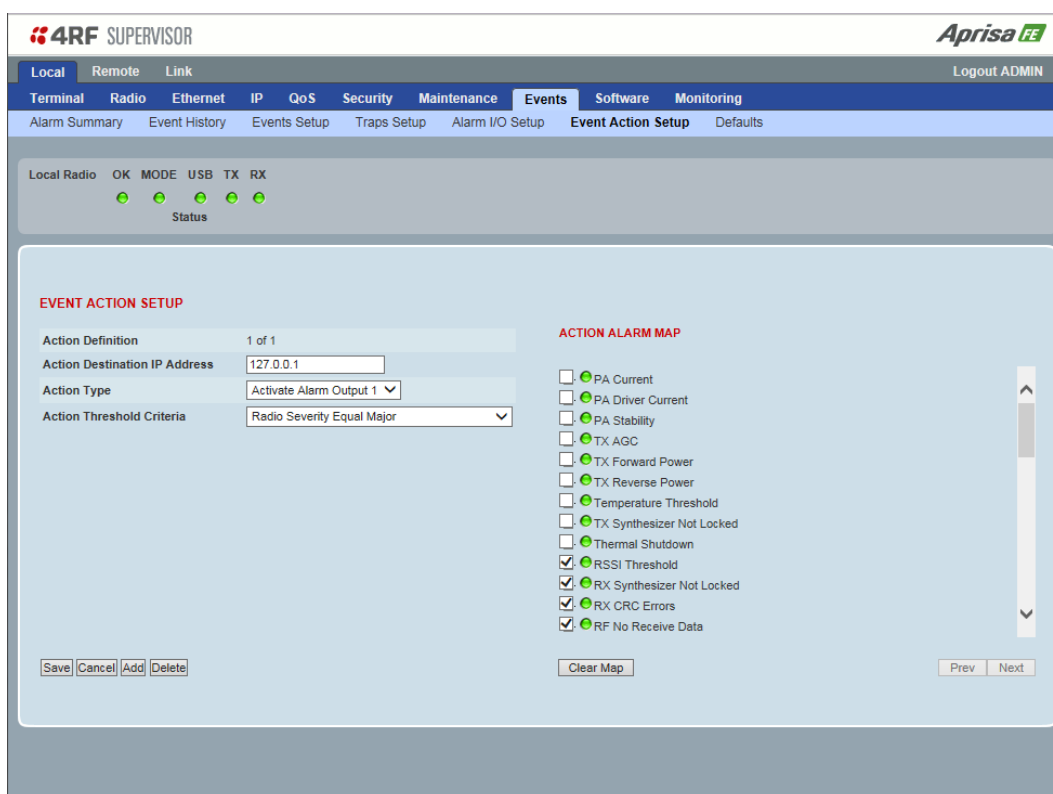
Alarm Output

Option	Function
Low	The alarm is active low i.e. the active alarm state will generate a ground contact output
High	The alarm is active high i.e. the active alarm state will generate a open contact output

Current State

The Current State shows the current state of the alarm.

Events > Event Action Setup



EVENT ACTION SETUP

This page provides control of the mapping of events to specific actions. Specific alarm events can setup to trigger outputs.

Action Definition

This parameter shows the number of the event action setup and the maximum number of setups stored.

Action Destination IP Address

This parameter sets the IP address of the radio that will output the action type.

Action Type

This parameter sets the action type that will be activated on the radio.

Option	Function
None	This action setup does not activate any alarm output
Activate Alarm Output 1	This action setup activates alarm output 1
Activate Alarm Output 2	This action setup activates alarm output 2

Action Threshold Criteria

This parameter sets the radio event that will trigger the action output.

Option	Function
None	No action output.
Radio Severity Equal Critical	Activates the action output when a radio alarm is critical alarm
Radio Severity Equal Major	Activates the action output when a radio alarm is a major alarm
Radio Severity Equal Minor	Activates the action output when a radio alarm is minor alarm
Radio Severity Equal Warning	Activates the action output when a radio alarm is a warning alarm
Radio Severity Equal Cleared	Activates the action output when a radio alarm is cleared
Radio Severity Equal or Worse than Major	Activates the action output when a radio alarm is a major alarm or a critical alarm
Radio Severity Equal or Worse than Minor	Activates the action output when a radio alarm is a minor alarm, a major alarm or a critical alarm
Radio Severity Equal or Worse than Warning	Activates the action output when a radio alarm is a warning, a major alarm, a minor alarm or a critical alarm

Controls

The Save button saves the current event action setup.

The Cancel button cancels the new event action setup.

The Add button adds a new event action setup.

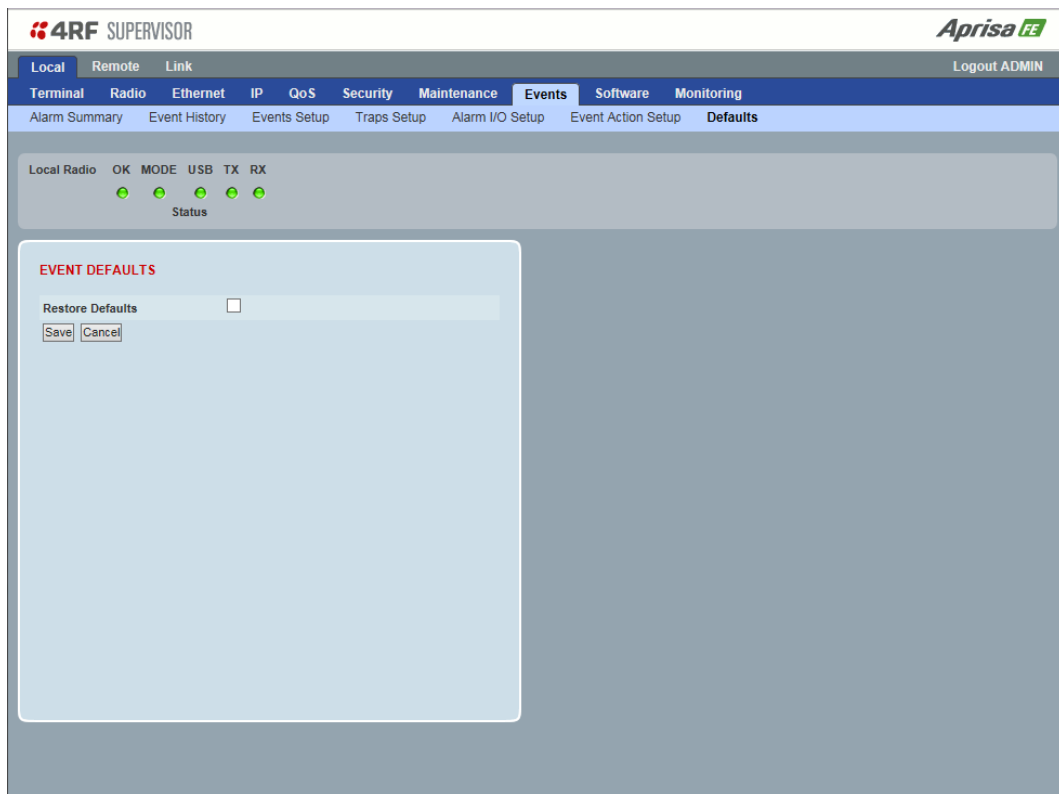
The Delete button deletes the current event action setup.

The Clear Map button clears all alarm selections on the current setup.

To add an event action setup:

1. Click on the Add button.
2. Enter the Action Destination IP Address. This is the IP address of the radio that will output the action type.
3. Select the Action Type from the list.
4. Select the Action Threshold Criteria from the list.
5. Tick the alarms required for the event action setup from the Action Alarm Map. You can clear all alarm selections with the Clear Map button.
6. Click on Save.

Events > Defaults



EVENT DEFAULTS

Restore Defaults

This parameter when activated restores all previously configured event parameters using 'Events > Events Setup' to the factory default settings.

Software

The Software menu contains the setup and management of the system software including software distribution and activation.

Single Radio Software Upgrade

The radio software can be upgraded on a single Aprisa FE radio (see ‘Single Radio Software Upgrade’ on page 293). This process would only be used if the radio was a replacement or a new radio in an existing link.

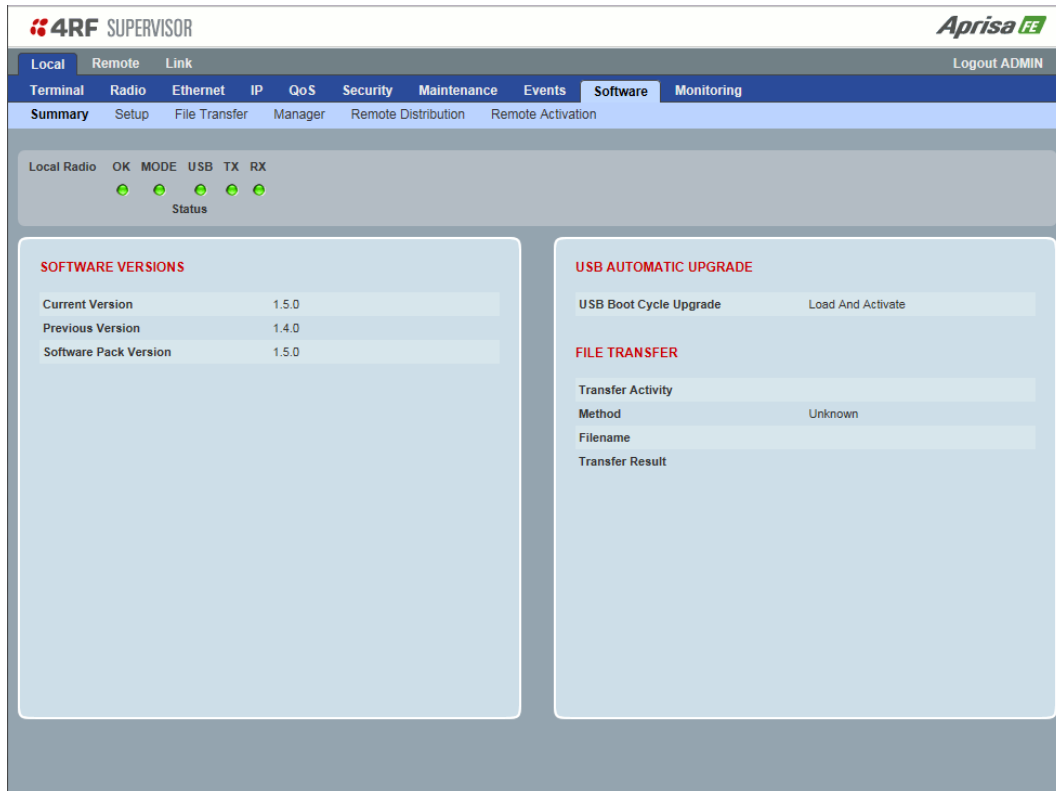
Link Software Upgrade

The radio software can be upgraded on the remote radio remotely over the radio link (see ‘Non Protected Link ’ on page 290). This process involves following steps:

1. Transfer the new software to local radio with ‘Software > File Transfer’
2. Distribute the new software to the remote radio with ‘Software > Remote Distribution’
3. Activate of the new software on the remote radio with ‘Software > Remote Activation’.
4. Finally, activate the new software on the local radio with the ‘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 local radio, this parameter displays the software version available for distribution to the remote radio.

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 174.

FILE TRANSFER

Transfer Activity

This parameter shows the status of the transfer, 'Idle', 'In Progress' or 'Completed'.

Method

This parameter shows the file transfer method. When the software distribution is in progress, this parameter will change to 'Over the Air' (from xx.xx.xx.xx) to show that the interface is busy and the transfer is in progress.

File

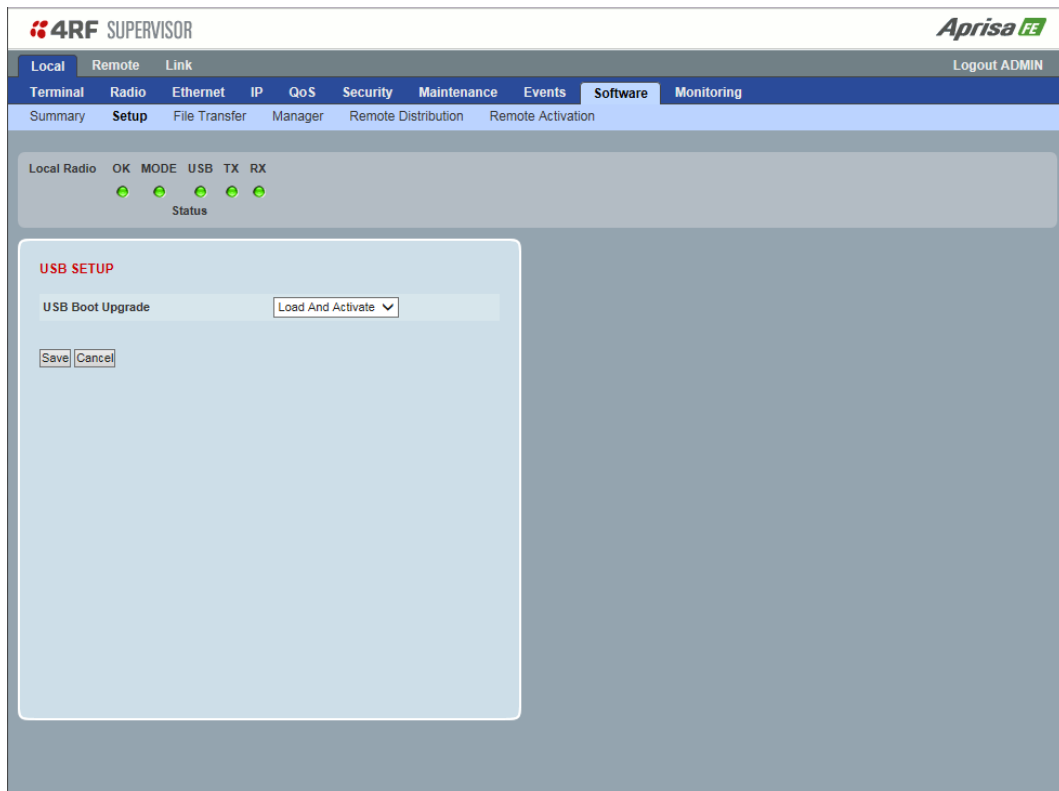
This parameter shows the software file source.

Transfer Result

This parameter shows the progress of the transfer.

Software > Setup

This page provides the setup of the USB flash drive containing a Software Pack.



USB SETUP

USB Boot Upgrade

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

Option	Function
Load and Activate	New software will be uploaded from a USB flash drive in to the Aprisa FE 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 FE when the radio is power cycled. The software will need to be manually activated (see 'Software > Manager' on page 178).
Disabled	Software will not be uploaded from a USB flash drive into the Aprisa FE when the radio is power cycled.

Note: This parameter must be set to 'Disabled' if the 'File Transfer and Activate' method of upgrade is used. This 'Disabled' setting prevents the radio from attempting another software upload when the radio boots (which it does automatically after activation).

Software > File Transfer

This page provides the mechanism to transfer new software from a file source into the radio.

SETUP FILE TRANSFER

Direction

This parameter sets the direction of file transfer. In this software version, the only choice is 'To the Radio'.

Method

This parameter sets the method of file transfer.

Option	Function
USB Transfer	Transfers the software from the USB flash drive to the radio.
FTP	Transfers the software from an FTP server to the radio.

File

This parameter shows the software file source.

FTP Username

This parameter sets the Username to access the FTP server.

FTP Password

This parameter sets the Password to access the FTP server.

FILE TRANSFER STATUS

Transfer Activity

This parameter shows the status of the transfer, 'Idle', 'In Progress' or 'Completed'.

Direction

This parameter shows the direction of file transfer. In this software version, the only choice is 'To The Radio'.

Method


This parameter shows the file transfer method. 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:

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	<p>The transfer has failed.</p> <p>Possible causes of failure are:</p> <ul style="list-style-type: none"> • Is the source file available e.g. USB flash drive plugged in • Does the file source contain the Aprisa FE software release files; 

To transfer software into the Aprisa FE radio:

USB Transfer Method

1. Unzip the software release files in to the root directory of a USB flash drive.
2. Insert the USB flash drive into the Host Port .
3. Click on 'Start Transfer'.

FILE TRANSFER STATUS	
Transfer Activity	In Progress
Direction	To This Radio
Method	USB Transfer
File	Software Pack
Transfer Result	In Progress (30%)

4. When the transfer is completed, remove the USB flash drive from the Host Port. If the SuperVisor 'USB Boot Upgrade' setting is set to 'Disabled' (see 'USB Boot Upgrade' on page 174), 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 178). The radio will reboot automatically.

If the file transfer fails, check the Event History page (see 'Events > Event History' on page 160) for more details of the transfer.

FTP Method

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

FILE TRANSFER STATUS	
Transfer Activity	In Progress
Direction	To This Radio
Method	FTP (172.17.10.11)
File	Software Pack
Transfer Result	In Progress (1%)

Go to Supervisor > Software > Manager and activate the Software Pack (see 'Software > Manager' on page 178). The radio will reboot automatically.

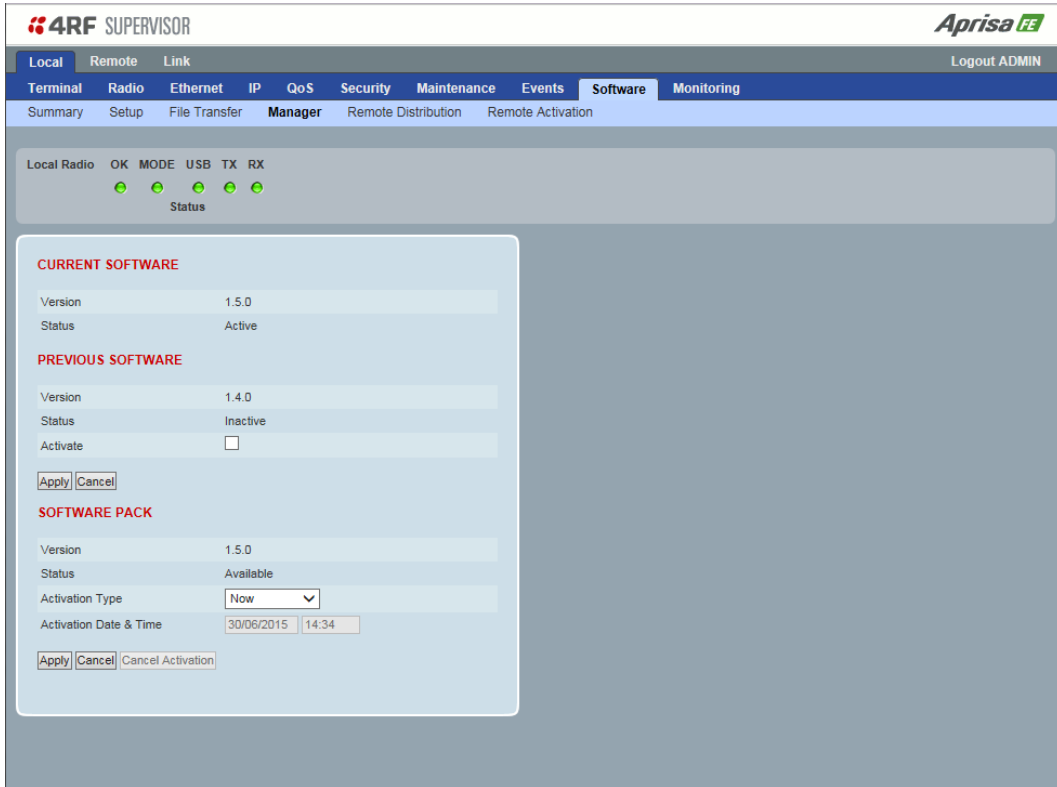
If the file transfer fails, check the Event History page (see 'Events > Event History' on page 160) for more details of the transfer.

Software > Manager

This page summarises and manages the software versions available in the radio.

The manager is predominantly used to activate new software on single radios. Network activation is performed with 'Software > Remote Activation'.

Both the previous software (if available) and Software Pack versions can be activated on the radio from this page.



4RF SUPERVISOR Aprisa FE

Local Remote Link Logout ADMIN

Terminal Radio Ethernet IP QoS Security Maintenance Events **Software** Monitoring

Summary Setup File Transfer **Manager** Remote Distribution Remote Activation

Local Radio OK MODE USB TX RX

Status

CURRENT SOFTWARE

Version 1.5.0

Status Active

PREVIOUS SOFTWARE

Version 1.4.0

Status Inactive

Activate

Apply Cancel

SOFTWARE PACK

Version 1.5.0

Status Available

Activation Type Now

Activation Date & Time 30/06/2015 14:34

Apply Cancel Cancel Activation

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 FE will automatically reboot after activation.

SOFTWARE PACK

Version

This parameter displays the software pack version available for distribution and activation.

Status

This parameter displays the status of the software pack version.

Option	Function
Available	The software pack is available for distribution and activation.
Activating	The software pack is activating in the radio.
Unavailable	There is no software pack loaded into the radio.

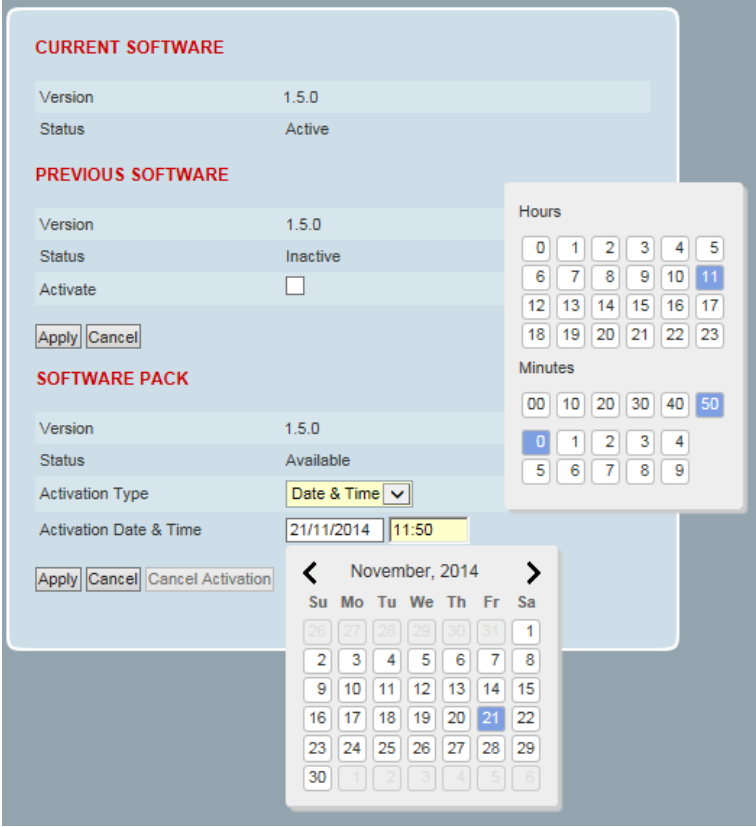
Activation Type

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.



CURRENT SOFTWARE

Version 1.5.0
Status Active

PREVIOUS SOFTWARE

Version 1.5.0
Status Inactive
Activate

Apply Cancel

SOFTWARE PACK

Version 1.5.0
Status Available
Activation Type **Date & Time**
Activation Date & Time 21/11/2014 11:50

Apply Cancel Cancel Activation

Hours: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

Minutes: 00 10 20 30 40 50

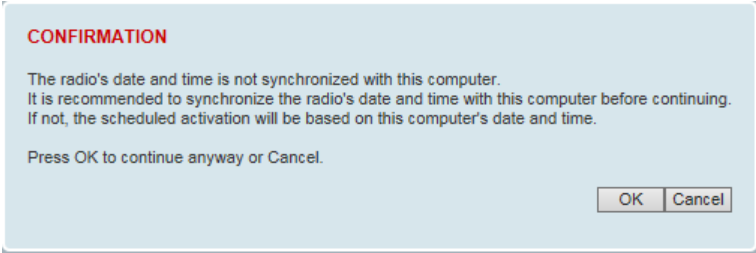
0 1 2 3 4 5 6 7 8 9

November, 2014

Su Mo Tu We Th Fr Sa

26 27 28 29 30 31 1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 1 2 3 4 5 6

If the local radio date / time is not synchronized, you will get the following popup:



CONFIRMATION

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.

OK Cancel

You can manually enter the local radio date / time or use the Date And Time Synchronization from a SNTP server feature (see 'Terminal > Date / Time' on page 69).

To activate a software version:

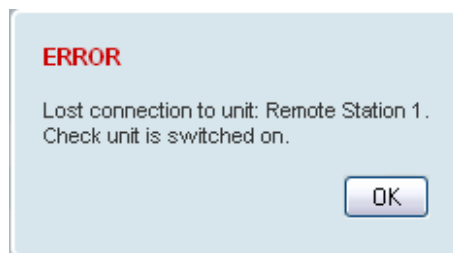
1. Tick the software version required to be activated (previous software or software pack).
2. Click 'Apply'.

SOFTWARE PACK	
Version	1.5.0
Status	Available
Activation Type	Now <input type="button" value="v"/>
Activation Date & Time	20/04/2015 14:23

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.



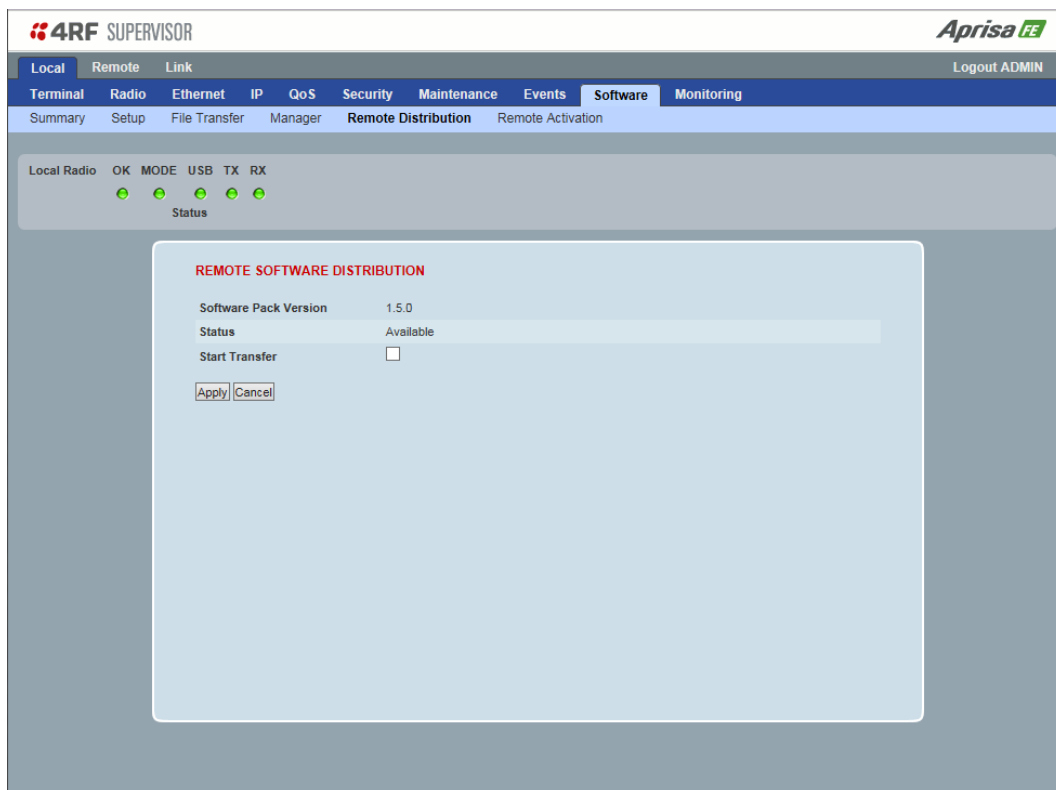
3. Login to SuperVisor to check the result.

Software > Remote Distribution

This page provides the mechanism to distribute software to the remote radio and then activate it.

The Software Pack that was loaded into the local radio with the file transfer process (see ‘Software > File Transfer’ on page 175) can be distributed via the radio link to the remote radio.

This page is used to manage the distribution of that software pack to the remote radio on the link.



REMOTE SOFTWARE DISTRIBUTION

Software Pack Version

This parameter displays the software pack version available for distribution on the local radio and activate on the remote radio.

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 the new Software Pack to the remote radio.

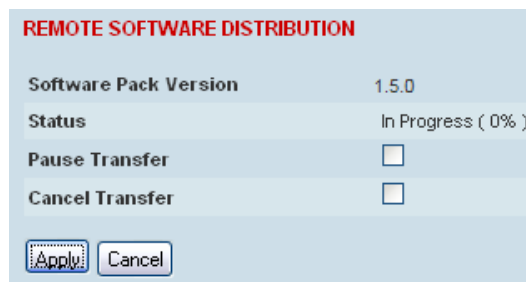
Note: The distribution of software to the remote radio does not stop customer traffic from being transferred. However, due to the volume of traffic, the software distribution process may affect customer traffic.

Software distribution traffic is classified as ‘management traffic’ but does not use the Ethernet management priority setting. Software distribution traffic priority has a fixed priority setting of ‘very low’.

To distribute software to the remote radio:

This process assumes that a Software Pack has been loaded into the local radio with the file transfer process (see ‘Software > File Transfer’ on page 175).

1. Click on ‘Start Transfer’.

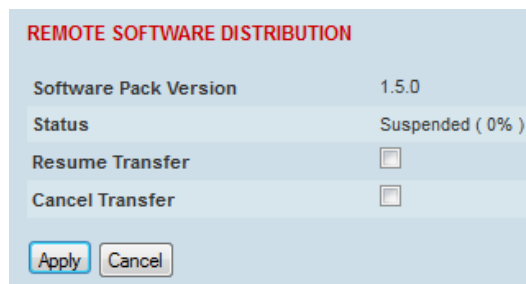


REMOTE SOFTWARE DISTRIBUTION	
Software Pack Version	1.5.0
Status	In Progress (0%)
Pause Transfer	<input type="checkbox"/>
Cancel Transfer	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. 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	1.5.0
Status	Suspended (0%)
Resume Transfer	<input type="checkbox"/>
Cancel Transfer	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Cancel Transfer

This parameter when activated, cancels the distribution process immediately.

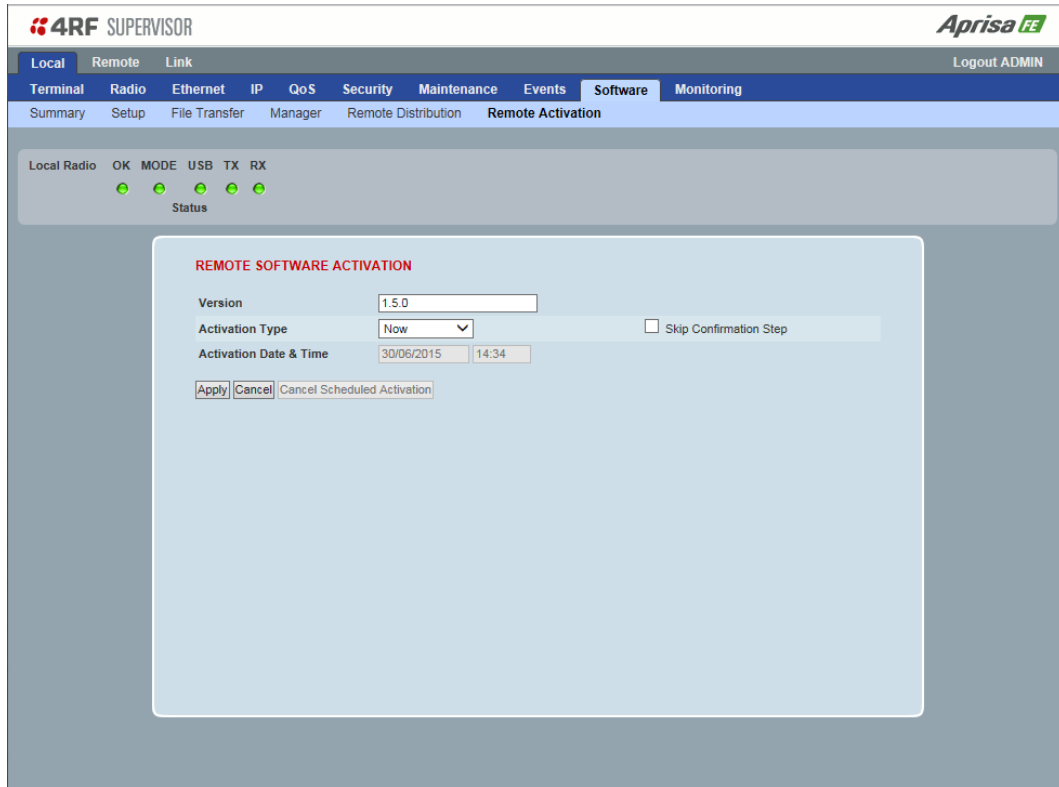
During the distribution process, it is possible to navigate away from this page and come back to it to check progress. The SuperVisor session will not timeout.

Software > Remote Activation

This page provides the mechanism to activate software on the remote radio.

The Software Pack was loaded into the local radio with the file transfer process (see ‘Software > File Transfer’ on page 175) and was distributed via the radio link to the remote radio.

This page is used to manage the activation of that software pack on the remote radio.



REMOTE SOFTWARE ACTIVATION

When the software pack version has been distributed to the remote radio, the software is then activated in the remote radio with this command. If successful, then activate the software pack in the local radio to complete the link 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.

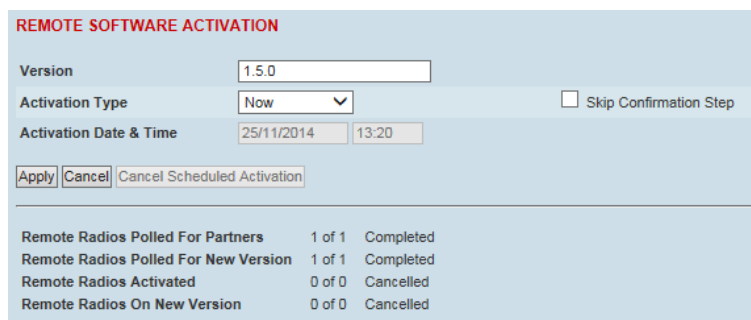
Normally, the confirmation step will require use intervention to accept the confirmation which will halt the activation process. Skipping the confirmation will enable the activation process to continue without use intervention.

To activate software in the remote radio:

This process assumes that a Software Pack has been loaded into the local radio with the file transfer process (see 'Software > File Transfer' on page 175) and distributed to the remote radio.

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).



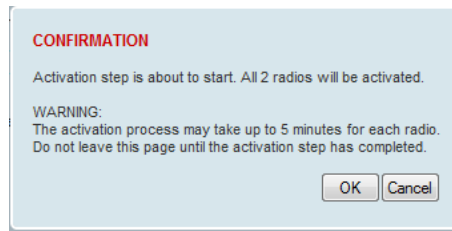
REMOTE SOFTWARE ACTIVATION		
Version	<input type="text" value="1.5.0"/>	
Activation Type	<input type="button" value="Now"/>	<input type="checkbox"/> Skip Confirmation Step
Activation Date & Time	<input type="text" value="25/11/2014"/> <input type="text" value="13:20"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="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 radio will be polled to determine if it requires 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 link. Y is always 1 for the point-to-point link.
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 always 1 for the point-to-point link.
Remote radios Activated	X is the number of radios that contain the new software version and have been activated. Y is always 1 for the point-to-point link.
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 always 1 for the point-to-point link.

When the activation is ready to start:



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

When the remote radio has been activated, the local radio must now be activated with (see 'Software > Manager' on page 178).

Monitoring

The Terminal, Ethernet, Radio and User Selected Monitored Parameter results have history log views for both Quarter Hourly and Daily.

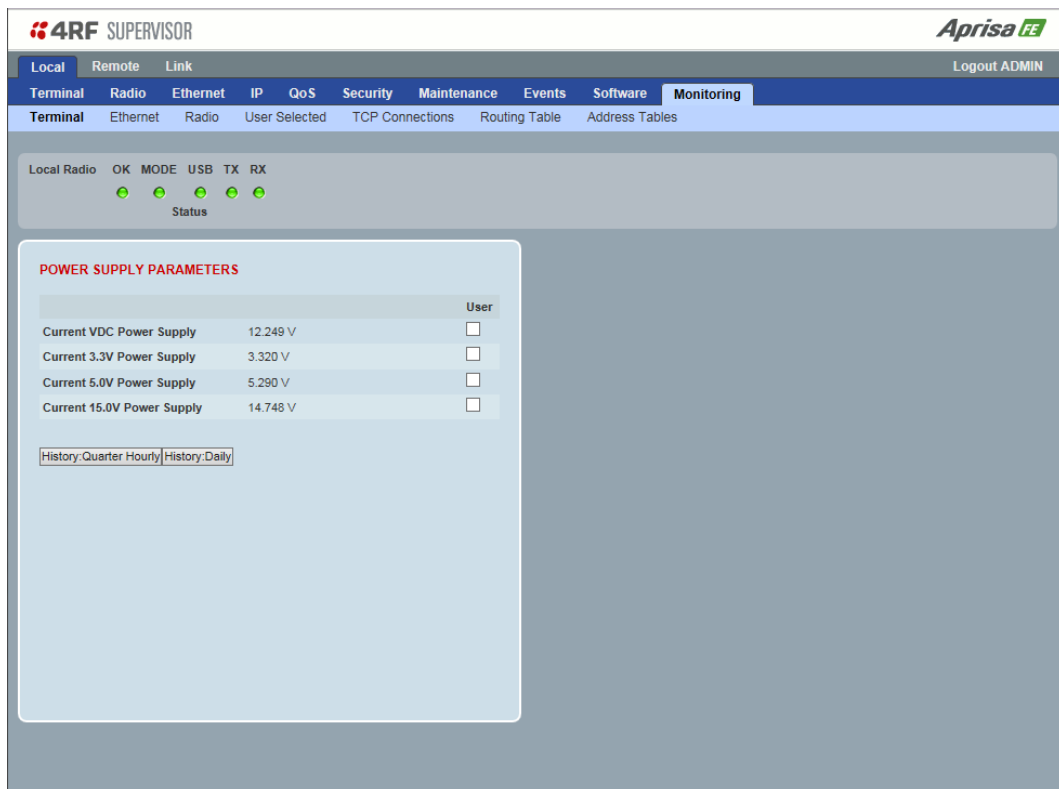
Monitored parameter data is accumulated into 2 sets:

- 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.

The results shown are since the page was opened and are updated automatically every 12 seconds.



POWER SUPPLY PARAMETERS

Monitored Parameter	Function	Normal Operating Limits
Current VDC Power Supply	Parameter to show the current power supply input voltage	10 to 30 VDC
Current 3.3 Volts Power Supply	Parameter to show the current 3.3 volt power rail voltage	3.1 to 3.5 VDC
Current 5.0 Volts Power Supply	Parameter to show the current that the current 5.0 volt power rail voltage	4.7 to 5.5 VDC
Current 7.2 Volts Power Supply	Parameter to show the current that the current 7.2 volt power rail voltage	6.9 to 7.5 VDC
Current 15 Volts Power Supply	Parameter to show the current that the current 15 volt power rail voltage. The 15 volt power supply is used to power the transmitter driver and power amplifier.	300,400 and 450 MHz transmitters 14.5 to 15.3 VDC 200 and 900 MHz transmitter 12.7 to 13.5 VDC

Controls

The History Quarter Hourly button presents a log of results every quarter of an hour.

The screenshot shows the 4RF SUPERVISOR interface with the 'Monitoring' tab selected. The 'POWER SUPPLY PARAMETERS' section is expanded, displaying a table of power supply history for a quarter-hourly period on 28/04/15. The table includes columns for time intervals and rows for various supply parameters.

Power Supply	28/04/15 6:00	28/04/15 6:15	28/04/15 6:30	28/04/15 6:45	28/04/15 7:00	28/04/15 7:15	28/04/15 7:30	28/04/15 7:45	28/04/15 8:00	28/04/15 8:15
Maximum VDC Supply	-	-	-	12.308	12.308	12.317	12.317	12.317	12.317	12.317
Minimum VDC Supply	-	-	-	12.298	12.298	12.298	12.298	12.298	12.298	12.288
Maximum 3.3V Supply	-	-	-	3.324	3.324	3.324	3.324	3.324	3.324	3.324
Minimum 3.3V Supply	-	-	-	3.322	3.322	3.322	3.322	3.322	3.322	3.322
Maximum 5V Supply	-	-	-	5.304	5.304	5.304	5.304	5.304	5.304	5.304
Minimum 5V Supply	-	-	-	5.301	5.301	5.296	5.296	5.295	5.295	5.295
Maximum 15V Supply	-	-	-	14.867	14.871	14.952	14.952	14.952	14.957	14.952
Minimum 15V Supply	-	-	-	14.862	14.829	14.852	14.862	14.852	14.862	14.862

Viewing 6:00 to 8:15 of 6:00 to 8:15

Downloaded 6

The History Daily button presents a log of results every day.

The screenshot shows the 4RF SUPERVISOR interface with the 'Monitoring' tab selected. The 'POWER SUPPLY PARAMETERS' section is expanded, displaying a table of power supply history for a daily period on 28/03/15. The table includes columns for dates and rows for various supply parameters.

Power Supply	18/04/15	19/04/15	20/04/15	21/04/15	22/04/15	23/04/15	24/04/15	25/04/15	26/04/15	27/04/15
Maximum VDC Supply	-	-	-	-	-	-	12.308	12.308	12.308	12.308
Minimum VDC Supply	-	-	-	-	-	-	12.298	12.298	12.288	12.298
Maximum 3.3V Supply	-	-	-	-	-	-	3.324	3.324	3.324	3.324
Minimum 3.3V Supply	-	-	-	-	-	-	3.322	3.322	3.322	3.322
Maximum 5V Supply	-	-	-	-	-	-	5.304	5.304	5.304	5.304
Minimum 5V Supply	-	-	-	-	-	-	5.301	5.301	5.301	5.301
Maximum 15V Supply	-	-	-	-	-	-	14.867	14.867	14.929	14.919
Minimum 15V Supply	-	-	-	-	-	-	14.862	14.862	14.824	14.862

Viewing 18/04/15 to 27/04/15 of 18/04/15 to 27/04/15

Downloaded 1

Monitoring > Ethernet

This page displays the current radio performance monitoring parameters per Ethernet port transmission (TX) out of the radio in packet and byte level granularity, for Ethernet port high level statistics and troubleshooting.

The results shown are since the page was opened and are updated automatically every 12 seconds.

ETHERNET PORT PARAMETERS

All Ethernet Ports TX

Monitored Parameter	Function	Normal Operating Limits
Maximum Capacity	Parameter to show the maximum Ethernet data rate of the Ethernet port	Equal to the Ethernet port speed setting
Packets	Parameter to show the number of packets transmitted to the customer from the Ethernet port	
Bytes	Parameter to show the number of bytes transmitted to the customer from the Ethernet port	
Packet Collisions	Parameter to show the number of packet collisions on the data transmitted to the customer from the Ethernet port on a shared LAN	
VLAN Frames	Parameter to show the number of VLAN tagged frames transmitted to the customer from the Ethernet port	

Controls

The Reset button clears the current results.

The History Quarter Hourly button presents a log of results every quarter of an hour.

ETHERNET PORT PARAMETERS

Ethernet Port 1 Transmit History, Quarter Hourly

Ethernet Port 1 Transmit	28/04/15 4:45	28/04/15 5:00	28/04/15 5:15	28/04/15 5:30	28/04/15 5:45	28/04/15 6:00	28/04/15 6:15	28/04/15 6:30	28/04/15 6:45	28/04/15 7:00
Maximum Capacity (Mb/s)	100	100	100	100	100	100	100	100	100	100
Packets	2,444	2,400	2,332	2,334	2,450	2,380	2,368	2,437	2,391	2,380
Bytes	430,710	427,959	422,584	423,669	431,094	426,678	425,354	428,735	427,318	427,460
Packet Collisions	0	0	0	0	0	0	0	0	0	0
VLAN Frames	0	0	0	0	0	0	0	0	0	0

Viewing 4:45 to 7:00 of 4:45 to 8:15

8:30 27/04/15 | 4:45 - 8:15 | 8:15 28/04/15 | Downloaded 15 | Cancel

The History Daily button presents a log of results every day.

ETHERNET PORT PARAMETERS

Ethernet Port 1 Transmit History, Daily

Ethernet Port 1 Transmit	18/04/15	19/04/15	20/04/15	21/04/15	22/04/15	23/04/15	24/04/15	25/04/15	26/04/15	27/04/15
Maximum Capacity (Mb/s)	-	-	-	-	-	-	100	100	100	100
Packets	-	-	-	-	-	-	80,995	226,794	227,299	227,306
Bytes	-	-	-	-	-	-	14,954,820	40,822,243	40,853,207	40,853,381
Packet Collisions	-	-	-	-	-	-	0	0	0	0
VLAN Frames	-	-	-	-	-	-	0	0	0	0

Viewing 18/04/15 to 27/04/15 of 18/04/15 to 27/04/15

28/03/15 | 21/04/15 - 27/04/15 | 27/04/15 | Downloaded 3 | Cancel

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

Port 1 Tx	Port 1 Rx	Port 2 Tx	Port 2 Rx	Port 3 Tx	Port 3 Rx	Port 4 Tx	Port 4 Rx
Packets	229						
Bytes	58,633						
Packets equal to 64 Bytes	134						
Packets 65 to 127 Bytes	16						
Packets 128 to 255 Bytes	7						
Packets 256 to 511 Bytes	0						
Packets 512 to 1023 Bytes	72						
Packets 1024 to 1536 Bytes	0						
Broadcast Packets	0						
Multicast Packets	7						
VLAN Frames	0						
VLAN Frames dropped	0						
Packet in Error	0						
Bytes in Error	0						
CRC/Alignment Errors	0						
Undersized Packets	0						
Oversized Packets	0						
Fragmented Packets	0						
Jabber Packets	0						
Dropped Packets (Congestion)	0						
Dropped Packets (Filtering)	7						
Dropped Bytes (Filtering)	1,197						

ETHERNET PORT PARAMETERS

All Ethernet Ports RX

Monitored Parameter	Function
Packets	Parameter to show the number of packets received by the customer from the Ethernet port (including bad packets, broadcast packets, and multicast packets)
Bytes	Parameter to show the number of bytes received (including those in bad packets) by the customer from the Ethernet port (excluding framing bits but including FCS octets)
Packets equal to 64 bytes	Parameter to show the number of packets received (including bad packets) from the customer into the Ethernet port that are equal to 64 bytes (excluding framing bits but including FCS octets)
Packets 65 to 127 bytes	Parameter to show the number of packets received (including bad packets) from the customer into the Ethernet port that are between 65 and 127 bytes (excluding framing bits but including FCS octets)
Packets 128 to 255 bytes	Parameter to show the number of packets received (including bad packets) from the customer into the Ethernet port that are between 128 and 255 bytes (excluding framing bits but including FCS octets)
Packets 256 to 511 bytes	Parameter to show the number of packets received (including bad packets) from the customer into the Ethernet port that are between 256 and 511 bytes(excluding framing bits but including FCS octets)
Packets 512 to 1023 bytes	Parameter to show the number of packets received (including bad packets) from the customer into the Ethernet port that are between 512 and 1023 bytes(excluding framing bits but including FCS octets)
Packets 1024 to 1536 bytes	Parameter to show the number of packets received (including bad packets) from the customer into the Ethernet port that are between 1024 and 1536 bytes(excluding framing bits but including FCS octets)
Broadcast Packets	Parameter to show the number of broadcast packets received from the customer into the Ethernet port. Broadcast packets are good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Monitored Parameter	Function
Multicast Packets	Parameter to show the number of multicast packets received from the customer into the Ethernet port. Multicast packets are packets that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
VLAN Frames	Parameter to show the number of VLAN tagged frames received from the customer into the Ethernet port
VLAN Frames Dropped	Parameter to show the number of VLAN tagged frames received from the customer into the Ethernet port that were dropped due to CRC errored frames, filtered VLAN frames, undersized frames or oversized frames.
Packet In Error	Parameter to show the number of errored packets received from the customer into the Ethernet port caused by CRC errors, FCS Errors, alignment errors, oversized packets, undersized packets, fragmented packets and jabber packets
Bytes In Error	Parameter to show the number of errored bytes received from the customer into the Ethernet port
CRC / Alignment Error	Parameter to show the number of CRC / alignment errors received from the customer into the Ethernet port. CRC / alignment errors are defined as frames that had a length excluding framing bits, but including FCS octets of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets.
Undersized Packets	Parameter to show the number of undersized packets received from the customer into the Ethernet port. Undersized packets are less than 64 octets long excluding framing bits, but including FCS octets.
Oversized Packets	Parameter to show the number of oversized packets received from the customer into the Ethernet port. Oversized packets are longer than 1518 octets excluding framing bits, but including FCS octets.
Fragmented Packets	Parameter to show the number of fragmented packets received from the customer into the Ethernet port. Fragmented packets have either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS.
Jabber Packets	Parameter to show the number of jabber packets received from the customer into the Ethernet port
Dropped Packets (congestion)	Parameter to show the number of dropped packets received from the customer into the Ethernet port caused by congestion
Dropped Packets (filtering)	Parameter to show the number of dropped packets received from the customer into the Ethernet port caused by packet L2 / L3 filtering
Dropped Bytes (filtering)	Parameter to show the number of dropped bytes received from the customer into the Ethernet port caused by packet L2 / L3 filtering

Controls

The Reset button clears the current results.

The History Quarter Hourly button presents a log of results every quarter of an hour.

Ethernet Port 1 Receive History, Quarter Hourly										
	28/04/15 6:00	28/04/15 6:15	28/04/15 6:30	28/04/15 6:45	28/04/15 7:00	28/04/15 7:15	28/04/15 7:30	28/04/15 7:45	28/04/15 8:00	28/04/15 8:15
Ethernet Port 1 Receive	3,114	3,089	3,103	3,108	3,108	3,088	3,106	3,117	3,106	3,091
Packets	440,980	438,486	439,559	439,954	439,954	437,660	439,826	441,385	439,826	438,280
Bytes	2,064	2,049	2,059	2,064	2,064	2,050	2,062	2,069	2,062	2,049
Packets equal to 64 Bytes	257	255	257	257	257	255	257	258	257	255
Packets 65 to 127 Bytes	535	527	529	529	529	526	529	531	529	530
Packets 128 to 255 Bytes	1	1	1	1	1	1	1	1	1	1
Packets 256 to 511 Bytes	257	257	257	257	257	256	257	258	257	256
Packets 512 to 1023 Bytes	0	0	0	0	0	0	0	0	0	0
Packets 1024 to 1536 Bytes	2	3	2	2	2	3	2	2	2	3
Broadcast Packets	20	15	14	14	14	14	14	14	14	18
Multicast Packets	0	0	0	0	0	0	0	0	0	0
VLAN Frames	0	0	0	0	0	0	0	0	0	0
VLAN Frames Dropped	0	0	0	0	0	0	0	0	0	0
Packets in Error	0	0	0	0	0	0	0	0	0	0
Bytes in Error	0	0	0	0	0	0	0	0	0	0
CRC/Alignment Errors	0	0	0	0	0	0	0	0	0	0
Undersized Packets	0	0	0	0	0	0	0	0	0	0
Oversized Packets	0	0	0	0	0	0	0	0	0	0
Fragmented Packets	0	0	0	0	0	0	0	0	0	0
Jabber Packets	0	0	0	0	0	0	0	0	0	0
Dropped Packets (Congestion)	0	0	0	0	0	0	0	0	0	0
Dropped Packets (Filtering)	22	18	16	16	16	17	16	16	16	21
Dropped Bytes (Filtering)	3,932	3,332	2,906	2,906	2,906	3,161	2,906	2,906	2,906	3,845

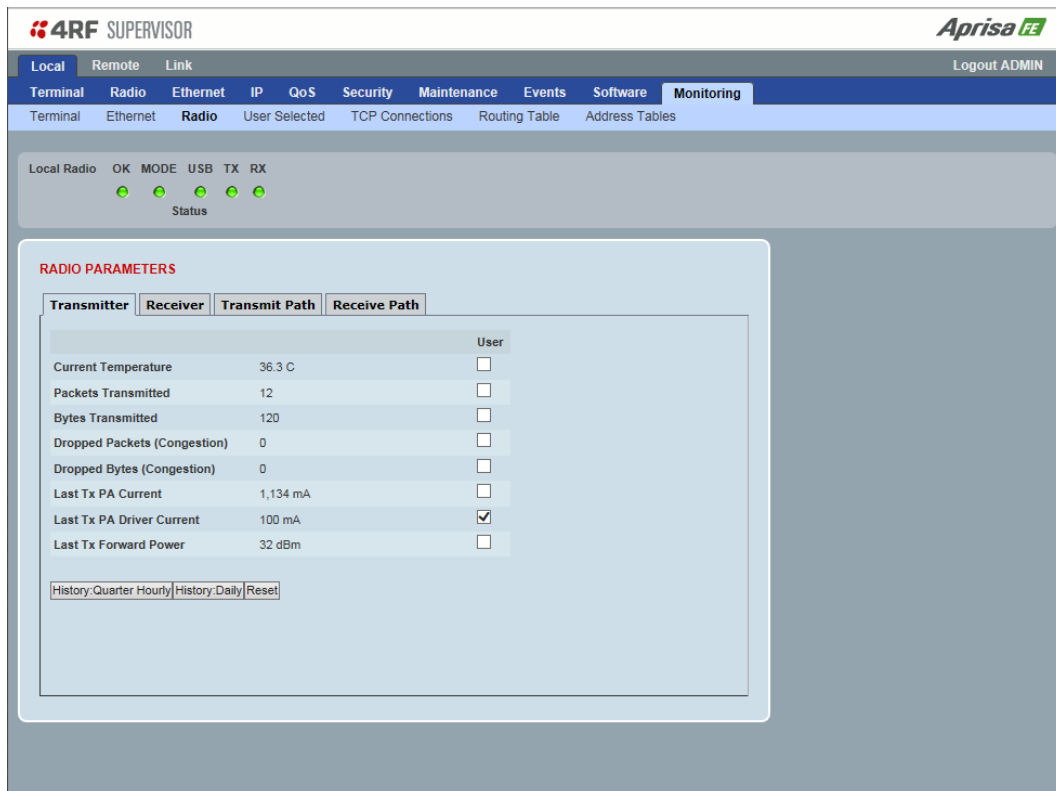
The History Daily button presents a log of results every day.

Ethernet Port 1 Receive History, Daily										
	18/04/15	19/04/15	20/04/15	21/04/15	22/04/15	23/04/15	24/04/15	25/04/15	26/04/15	27/04/15
Ethernet Port 1 Receive	-	-	-	-	-	-	105,790	298,004	297,963	297,959
Packets	-	-	-	-	-	-	14,977,084	42,212,489	42,206,282	42,205,341
Bytes	-	-	-	-	-	-	70,292	197,783	197,762	197,760
Packets equal to 64 Bytes	-	-	-	-	-	-	8,694	24,643	24,638	24,638
Packets 65 to 127 Bytes	-	-	-	-	-	-	17,954	50,811	50,801	50,799
Packets 128 to 255 Bytes	-	-	-	-	-	-	71	97	95	96
Packets 256 to 511 Bytes	-	-	-	-	-	-	8,779	24,670	24,667	24,666
Packets 512 to 1023 Bytes	-	-	-	-	-	-	0	0	0	0
Packets 1024 to 1536 Bytes	-	-	-	-	-	-	129	219	215	215
Broadcast Packets	-	-	-	-	-	-	613	1,430	1,423	1,422
Multicast Packets	-	-	-	-	-	-	0	0	0	0
VLAN Frames	-	-	-	-	-	-	0	0	0	0
VLAN Frames Dropped	-	-	-	-	-	-	0	0	0	0
Packets in Error	-	-	-	-	-	-	0	0	0	0
Bytes in Error	-	-	-	-	-	-	0	0	0	0
CRC/Alignment Errors	-	-	-	-	-	-	0	0	0	0
Undersized Packets	-	-	-	-	-	-	0	0	0	0
Oversized Packets	-	-	-	-	-	-	0	0	0	0
Fragmented Packets	-	-	-	-	-	-	0	0	0	0
Jabber Packets	-	-	-	-	-	-	0	0	0	0
Dropped Packets (Congestion)	-	-	-	-	-	-	0	0	0	0
Dropped Packets (Filtering)	-	-	-	-	-	-	734	1,649	1,638	1,637
Dropped Bytes (Filtering)	-	-	-	-	-	-	130,802	299,101	297,604	297,435

Monitoring > Radio

This page displays the current radio diagnostic and performance monitoring parameters of the radio transmitter.

The results shown are since the page was opened and are updated automatically every 12 seconds.



RADIO PARAMETERS

Transmitter

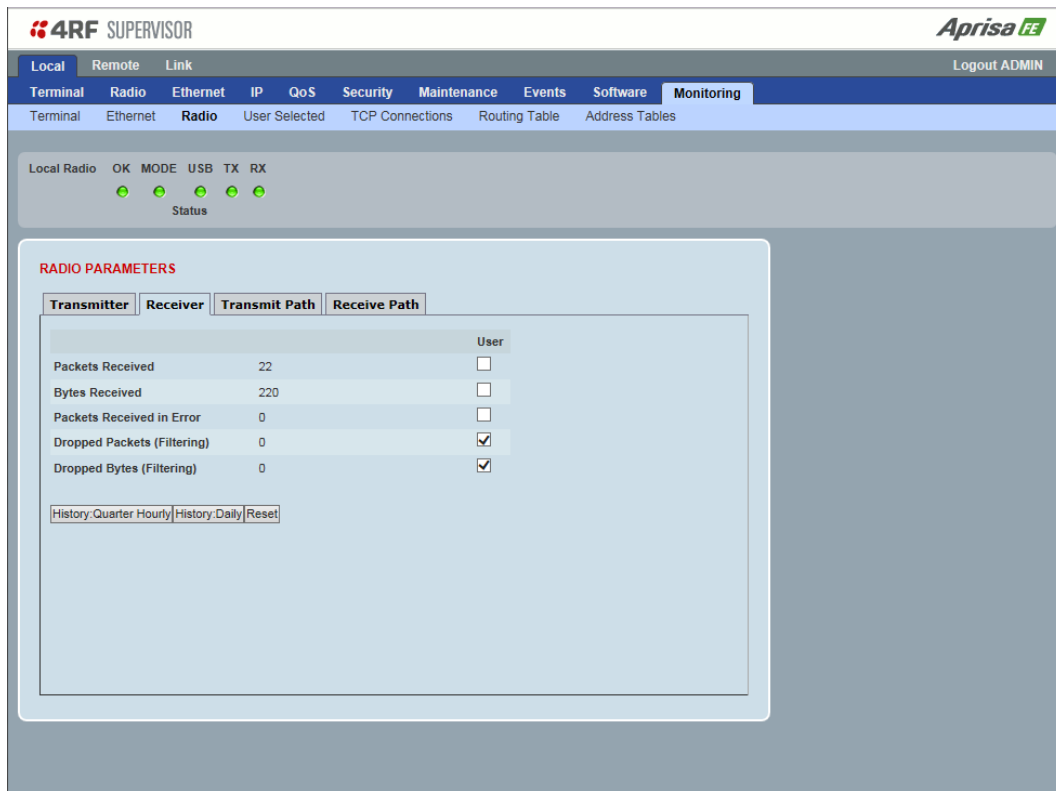
Monitored Parameter	Function	Normal Operating Limits
Current Temperature	Parameter to show the current temperature of the transmitter	0 to 70 °C
Packets Transmitted	Parameter to show the number of packets transmitted over the air	
Bytes Transmitted	Parameter to show the number of bytes transmitted over the air	
Dropped Packets (congestion)	Parameter to show the number of dropped packets transmitted over the air caused by congestion	
Dropped Bytes (congestion)	Parameter to show the number of dropped bytes transmitted over the air caused by congestion	
Last TX Packet PA Current	Parameter to show the current consumed by the transmitter power amplifier in mA. The value is stored from the last time the transmitter was active and transmitted a packet.	This value will change depending on the transmitter power setting, modulation, temperature and the VSWR of the antenna. The alarm limits for this are 50 mA to 2.5 A
Last TX Packet Driver Current	Parameter to show the current consumed by the transmitter power amplifier driver in mA. The value is stored from the last time the transmitter was active and transmitted a packet.	This value will change depending on the transmitter power setting, modulation and temperature. The alarm limits for the PA Driver Current are 10 mA to 500 mA.

Monitored Parameter	Function	Normal Operating Limits
Last TX Packet Forward Power	Parameter to show the actual transmitter power in dBm. The value is stored from the last time the transmitter was active and transmitted a packet.	This value will be dependent on the output power, the temperature and the VSWR of the antenna. The alarm limits for the Tx forward power are +/-4 dB.

Controls

The Reset button clears the current results.

This page displays the current radio performance monitoring parameters of radio receiver. The results shown are since the page was opened and are updated automatically every 12 seconds.



RADIO PARAMETERS

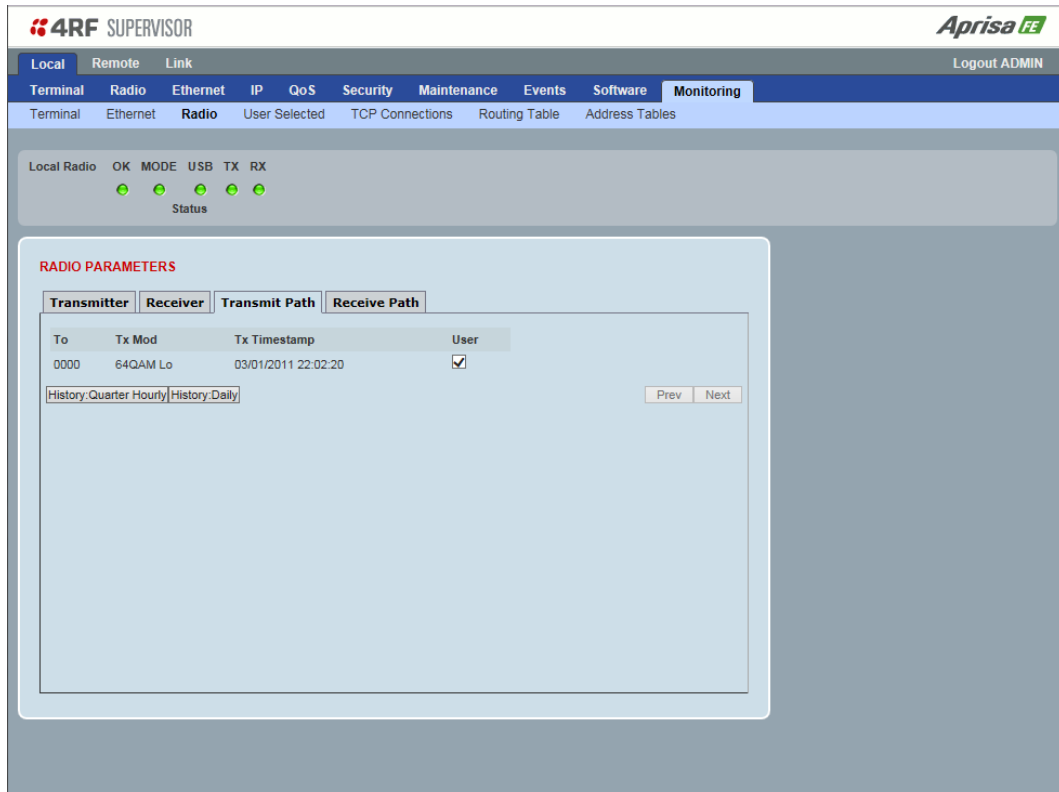
Receiver

Monitored Parameter	Function
Packets Received	Parameter to show the number of packets received over the air
Bytes Received	Parameter to show the number of bytes received over the air
Packets Received In Error	Parameter to show the number of packets received over the air
Dropped Packets (filtering)	Parameter to show the number of dropped packets received over the air caused by L2 / L3 filtering
Dropped Bytes (filtering)	Parameter to show the number of dropped bytes received over the air caused by L2 / L3 filtering

Controls

The Reset button clears the current results.

This page displays the current radio RF transmit path modulation setting of the radio it is transmitting to. The results shown are since the page was opened and are updated automatically every 12 seconds.



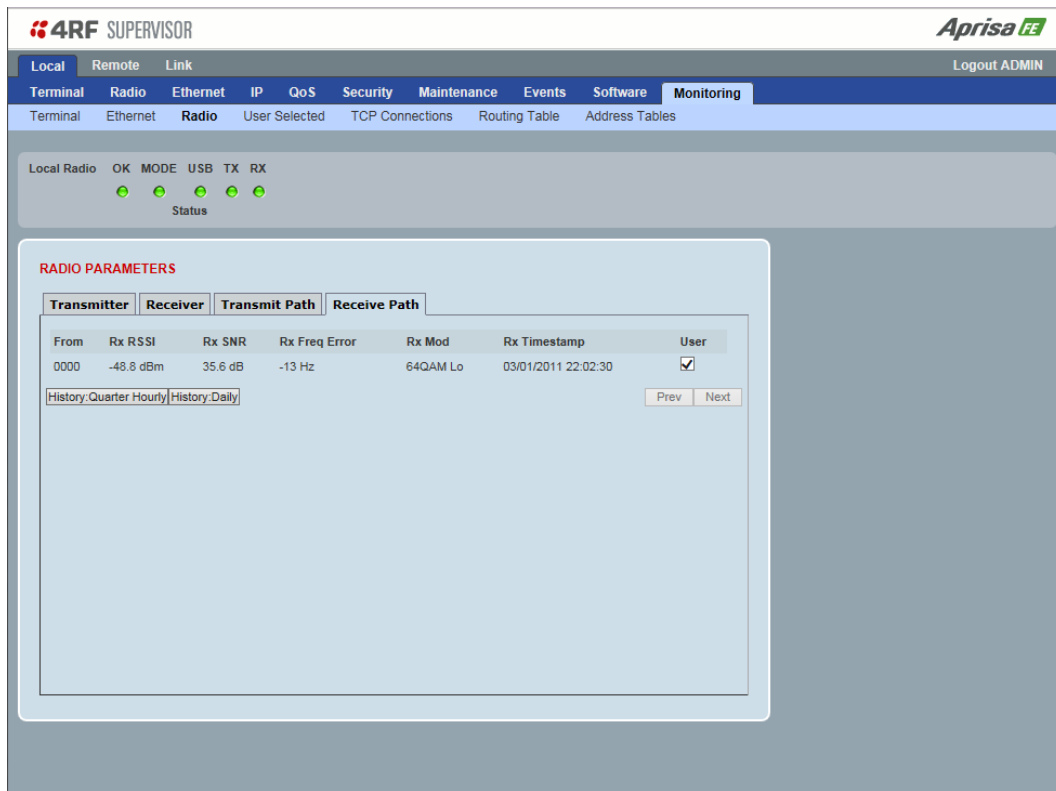
RADIO PARAMETERS

Result	Function
To	The destination Node Address of the radio/s transmitting data to.
Tx Mod	The current radio transmitter modulation being used to communicate with the destination radio/s.
Tx Timestamp	The timestamp of the last transmitted packet to the destination radio/s.

Controls

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

This page displays the current radio RF receive path parameters from the radio it is receiving from. The results shown are since the page was opened and are updated automatically every 12 seconds.



RADIO PARAMETERS

Receive Path

Result	Function
From	The source Node Address of the radio receiving data from.
Rx RSSI	The RSSI of the RF signal received from the source radio/s. This parameter displays the receiver RSSI reading taken from the last data packet received.
Rx SNR	The SNR of the RF signal received from the source radio/s. This parameter displays the receiver SNR reading taken from the last data packet received.
Rx Freq Error	The frequency difference between this radio's receiver and the frequency of the incoming packet rate from the source radio/s.
Rx Mod	The current radio receive modulation being used to communicate with the source radio/s.
Rx Timestamp	The timestamp of the last received packet from the source radio/s.

Controls

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

Monitoring > User Selected

This page displays the 'User' parameters setup in all the other Monitoring screens e.g. in the Monitoring > Radio > Transmitter, the User checkbox is ticked for the Dropped Packets (Congestion) and Dropped Bytes (Congestion).

The results shown are since the page was opened and are updated automatically every 12 seconds.

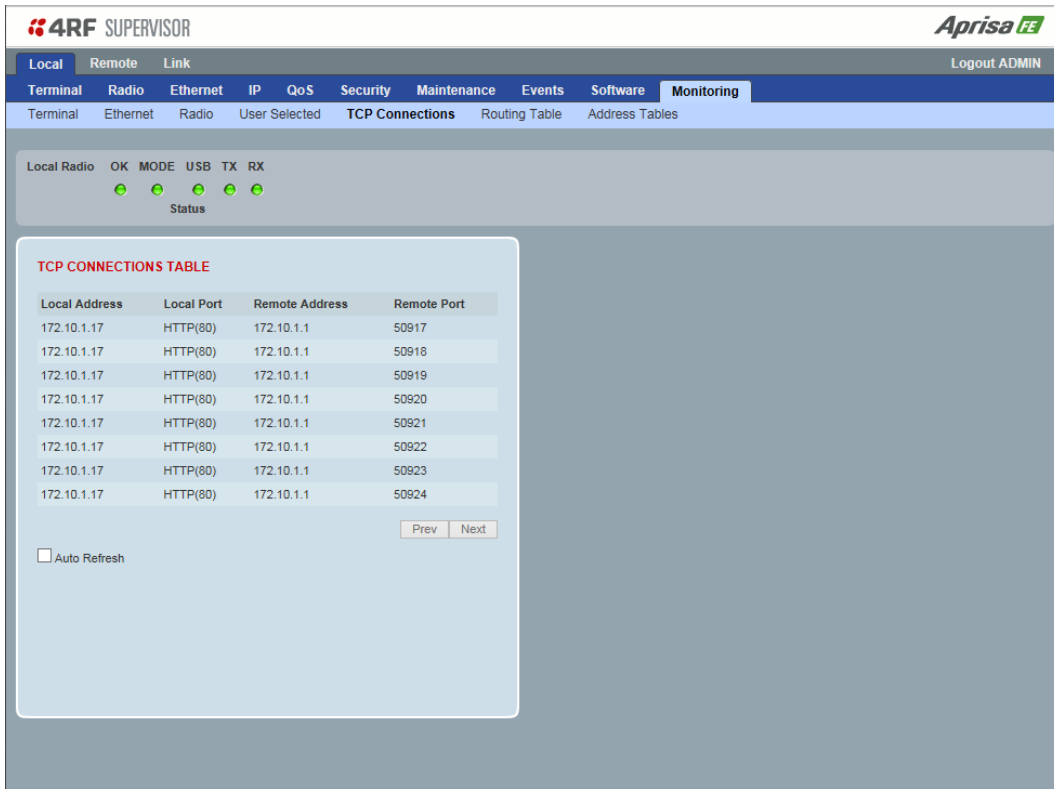
The screenshot displays the 4RF SUPERVISOR interface for the 'Monitoring > User Selected' view. At the top, there are navigation tabs for 'Local', 'Remote', and 'Link', and a 'Logout ADMIN' link. Below the navigation, there are sub-tabs for 'Terminal', 'Radio', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. The 'Monitoring' tab is active, and within it, 'User Selected' is chosen. The interface shows a 'Local Radio' status bar with 'OK', 'MODE', 'USB', 'TX', and 'RX' indicators, all of which are green. Below this, there are two main sections: 'TERMINAL PARAMETERS' and 'RF LINK PARAMETERS'. The 'TERMINAL PARAMETERS' section includes 'RF Transmitter' (Last Tx PA Driver Current: 97 mA), 'RF Receiver' (Dropped Packets (Filtering): 0, Dropped Bytes (Filtering): 0), and a 'Reset All' button. The 'RF LINK PARAMETERS' section includes 'Transmit Path' (Remote Node Address: 0000, Modulation: 64QAM Lo, Timestamp: 03/01/2011 22:03:11) and 'Receive Path' (Remote Node Address: 0000, RSSI: -48.8 dBm, SNR: 39.3 dB, Frequency Error: -12 Hz, Modulation: 64QAM Lo, Timestamp: 03/01/2011 22:03:11).

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

Local Address	Local Port	Remote Address	Remote Port
172.10.1.17	HTTP(80)	172.10.1.1	50917
172.10.1.17	HTTP(80)	172.10.1.1	50918
172.10.1.17	HTTP(80)	172.10.1.1	50919
172.10.1.17	HTTP(80)	172.10.1.1	50920
172.10.1.17	HTTP(80)	172.10.1.1	50921
172.10.1.17	HTTP(80)	172.10.1.1	50922
172.10.1.17	HTTP(80)	172.10.1.1	50923
172.10.1.17	HTTP(80)	172.10.1.1	50924

Auto Refresh
 Prev Next

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.

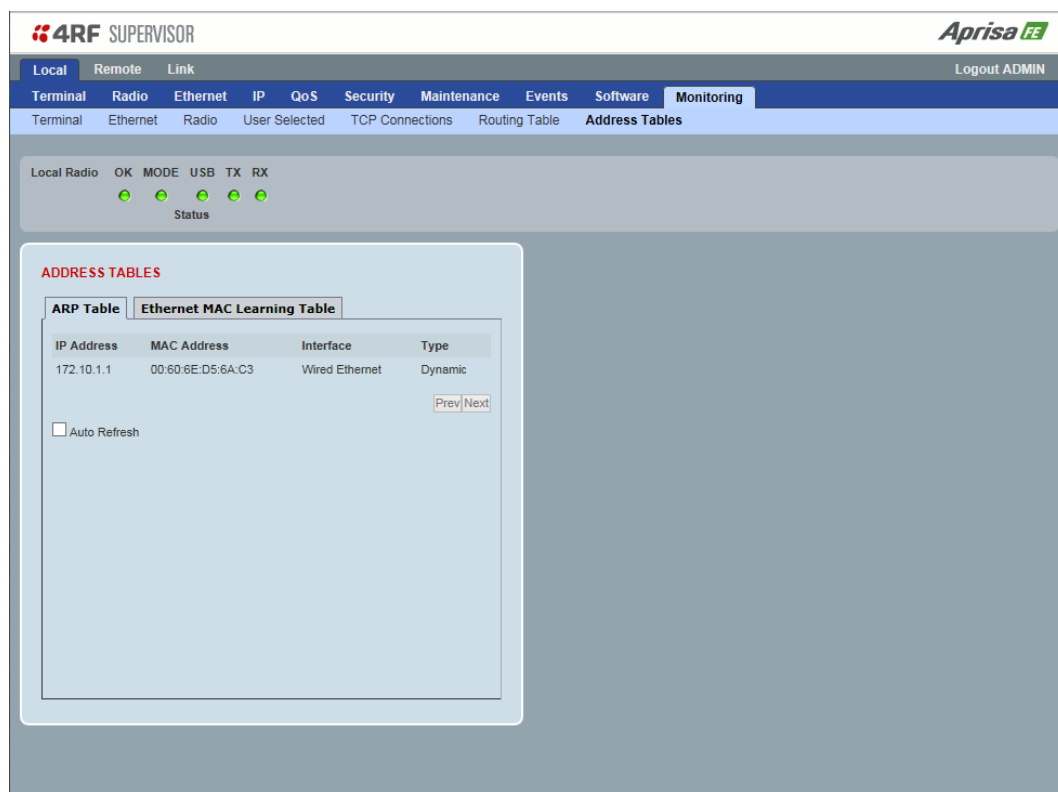
If the Auto Refresh option is ticked, the routing table will refresh every 12 seconds.

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

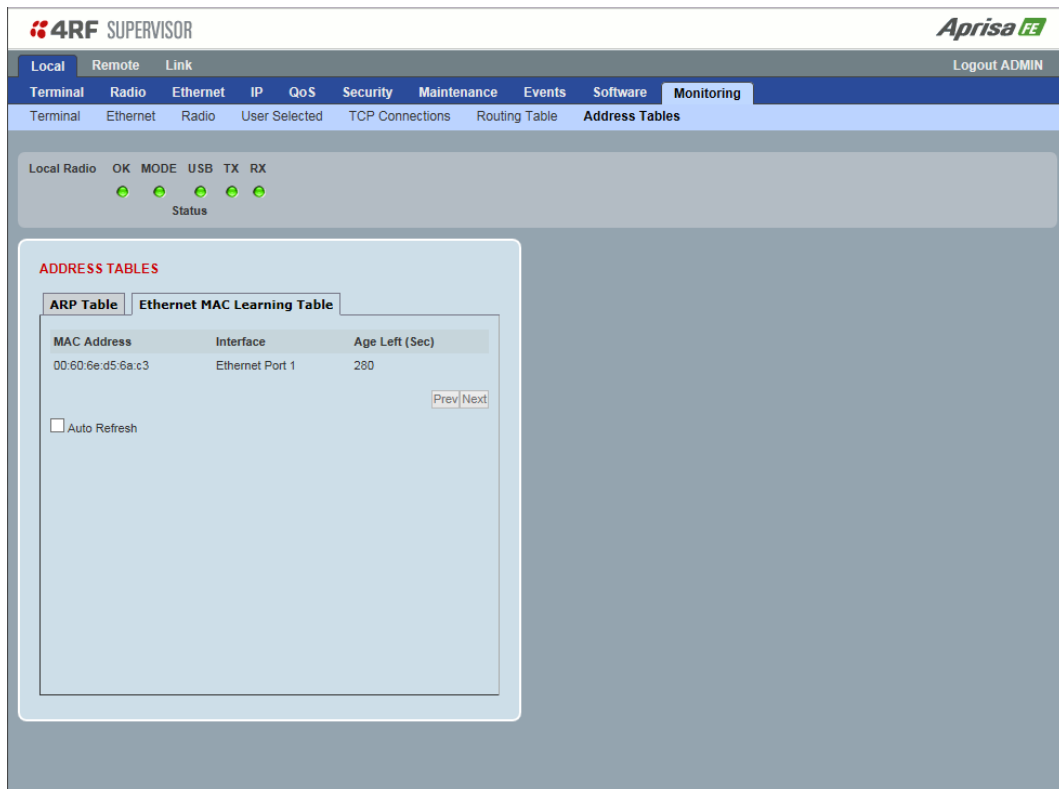
The Next button will display the next page of 8 addresses and the Prev button will display the previous page of 8 addresses.

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.

Link

The Link tab enables display of settings and configuration of common changes to be made to both the local and remote radios simultaneously.

Link > Details > Summary

This page displays a summary of both the local and remote radio Terminal Summary and Operating Summary.



The screenshot shows the 4RF Supervisor interface with the 'Link' tab selected. The 'Summary' sub-tab is active, displaying status indicators for both Local and Remote Radio. Below the status indicators are two summary tables: 'TERMINAL SUMMARY' and 'OPERATING SUMMARY' for both Local and Remote Radio.

LOCAL RADIO STATUS		REMOTE RADIO STATUS		
OK	MODE	USB	TX	RX
●	●	●	●	●

LOCAL RADIO - TERMINAL SUMMARY		REMOTE RADIO - TERMINAL SUMMARY	
Terminal Name	Local Radio	Terminal Name	Remote Radio
Location	Wellington	Location	Wellington
Contact Name	4RF Limited	Contact Name	4RF Limited
Contact Details	support@4rf.com	Contact Details	support@4rf.com
IP Address	172.10.1.17	IP Address	172.10.1.20
Subnet Mask	255.255.0.0	Subnet Mask	255.255.0.0
Gateway	0.0.0.0	Gateway	0.0.0.0
Date and Time	02/01/2011 01:42:57	Date and Time	01/01/2011 22:29:39

LOCAL RADIO - OPERATING SUMMARY		REMOTE RADIO - OPERATING SUMMARY	
Operating Mode	Point To Point	Operating Mode	Point To Point
Ethernet Mode	Bridge	Ethernet Mode	Bridge
Interface Mode	Ethernet Only	Interface Mode	Ethernet Only
Modem Mode	Mode A (ETSI / ACMA)	Modem Mode	Mode A (ETSI / ACMA)
TX Frequency (MHz)	406.25	TX Frequency (MHz)	400
TX Power (dBm)	32	TX Power (dBm)	34
RX Frequency (MHz)	400	RX Frequency (MHz)	406.25
Channel Size (kHz)	12.5	Channel Size (kHz)	12.5
Network ID (FAN)	CAFE	Network ID (FAN)	CAFE
Base Station ID	2	Base Station ID	2
Node Address	0000	Node Address	0000
Inband Management	Enabled	Inband Management	Enabled
Inband Management Timeout (s)	10	Inband Management Timeout (s)	10

TERMINAL SUMMARY

See 'Terminal > Device' for terminal settings.

OPERATING SUMMARY

See 'Terminal > Operating Mode' and 'Radio > Radio Setup' for operating mode and radio settings.

Link > Details > Radio

This page displays both the local and remote 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 displays the 4RF SUPERVISOR interface for the 'Link' radio. It features a navigation bar with 'Local', 'Remote', and 'Link' tabs, and a sub-menu with 'Details', 'Configuration', and 'Monitoring'. The 'Radio' sub-tab is active, showing 'Summary', 'Radio', and 'Events' options. The interface is divided into two columns for 'Local Radio' and 'Remote Radio', each with a status indicator (OK, MODE, USB, TX, RX) and a 'Status' label. Below these are three sections: 'TX FREQUENCY', 'TX POWER', and 'RX FREQUENCY', followed by a 'GENERAL' section. Each section contains a table of parameters and their values.

Radio Type	Parameter	Value
Local Radio	TX Frequency (MHz)	406.25
	TX Frequency Range (MHz)	400 to 470
	TX Frequency Step Size (kHz)	6.25
	TX Power (dBm)	32
	TX Power Range (dBm)	5 to 32
	TX Power Step Size (dB)	1
	RX Frequency (MHz)	400
	RX Frequency Range (MHz)	400 to 470
	RX Frequency Step Size (kHz)	6.25
	Channel Size (kHz)	12.5
	Modulation Type	64QAM (Low Gain)
	Antenna Port Configuration	Single Antenna Dual Port (Duplexer)
Remote Radio	TX Frequency (MHz)	400
	TX Frequency Range (MHz)	400 to 470
	TX Frequency Step Size (kHz)	6.25
	TX Power (dBm)	34
	TX Power Range (dBm)	7 to 34
	TX Power Step Size (dB)	1
	RX Frequency (MHz)	406.25
	RX Frequency Range (MHz)	400 to 470
	RX Frequency Step Size (kHz)	6.25
	Channel Size (kHz)	12.5
	Modulation Type	64QAM (Low Gain)
	Antenna Port Configuration	Single Antenna Dual Port (Duplexer)

See 'Radio > Radio Setup' for radio settings.

Link > Details > Events

This page displays the current alarm events of both the local and remote radios.

The screenshot shows the 4RF SUPERVISOR interface with the 'Link' tab selected. At the top, there are tabs for 'Local', 'Remote', and 'Link', and a 'Logout ADMIN' link. Below this are sub-tabs for 'Details', 'Configuration', and 'Monitoring', with 'Events' selected under 'Details'. The interface is divided into two main columns for 'Local Radio' and 'Remote Radio'. Each column has a status bar with indicators for 'OK', 'MODE', 'USB', 'TX', and 'RX'. Below the status bars are two 'ALARM SUMMARY' sections. The 'Local Radio' section lists various alarm categories such as Transmit Path, Receive Path (including RSSI Threshold, RX Synthesizer Not Locked, and RX CRC Errors), Radio Interface Path, Customer Equipment Interface Path, Component Failure, Diagnostic, Software (including Calibration Failure, Configuration Not Supported, Remote Communications Lost, Network Configuration Warning, Software Restart Required, and Software Activation Pending), Alarm Inputs, Protection, and Power Supply. The 'Remote Radio' section lists similar categories, including Transmit Path, Receive Path, Radio Interface Path, Customer Equipment Interface Path (with sub-items for Port1 and Port2 Ethernet and Serial data errors), Component Failure, Diagnostic, Software, and Alarm Inputs. A vertical scrollbar is visible on the right side of the Remote Radio alarm summary.

See 'Events > Events Setup' for alarm event setup.

Link > Configuration > Radio Setup

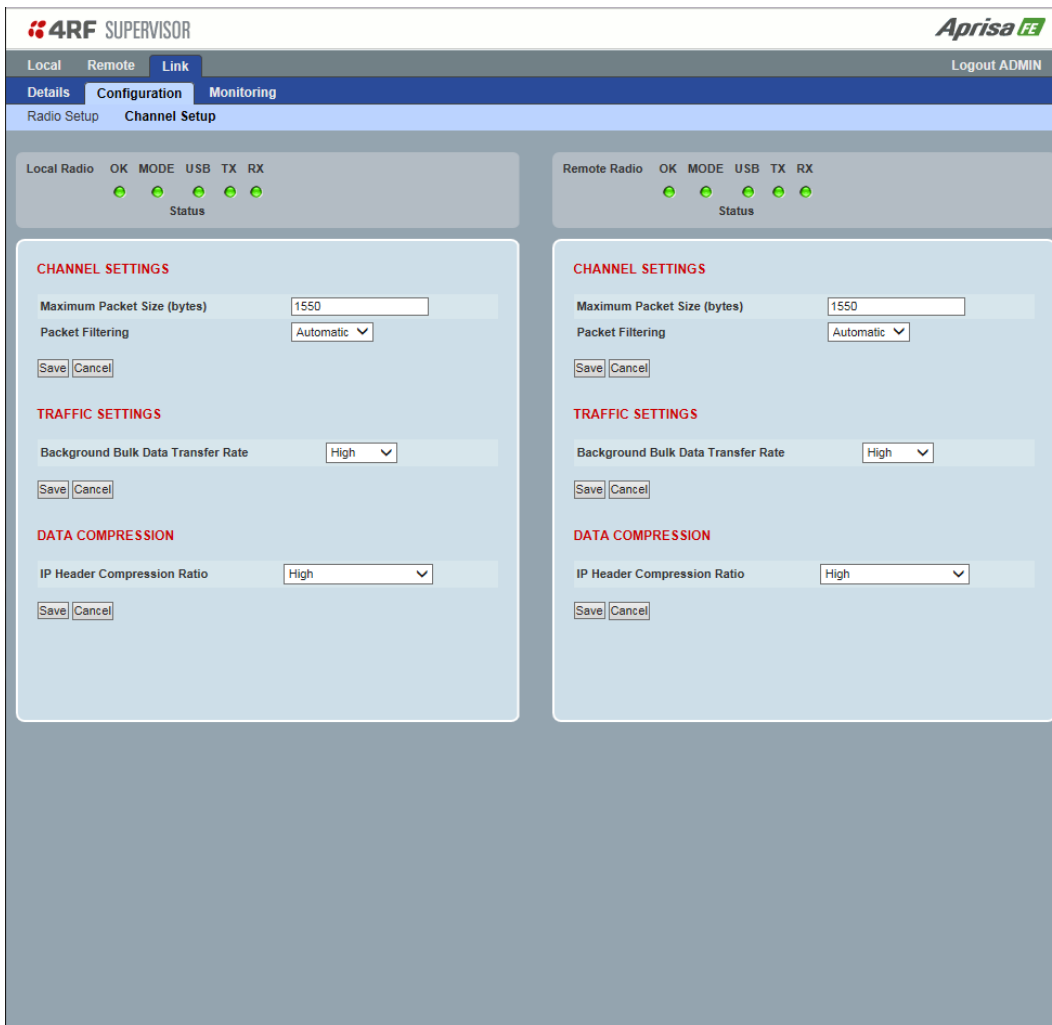
This page enables the configuration of common radio parameters to be made to both the Local and Remote radios simultaneously.

Parameters critical to the operation of the link e.g. TX and RX frequencies are automatically copied to the other radio in the link i.e. critical parameters entered on the local radio are automatically copied to the remote radio and vice versa.

See 'Radio > Radio Setup' for radio settings.

Link > Configuration > Channel Setup

This page enables the configuration of common channel and traffic parameters to be made to both the Local and Remote radios simultaneously.



The screenshot displays the '4RF SUPERVISOR' interface for 'Aprisa FE'. The navigation path is 'Local Remote Link' > 'Details Configuration Monitoring' > 'Radio Setup Channel Setup'. The 'Link' tab is active. At the top, there are status indicators for 'Local Radio' and 'Remote Radio', each with 'OK', 'MODE', 'USB', 'TX', and 'RX' indicators, all showing green lights. The main content area is split into two columns for 'Local Radio' and 'Remote Radio' settings. Each column has three sections: 'CHANNEL SETTINGS', 'TRAFFIC SETTINGS', and 'DATA COMPRESSION'. The 'CHANNEL SETTINGS' section includes 'Maximum Packet Size (bytes)' (1550) and 'Packet Filtering' (Automatic). The 'TRAFFIC SETTINGS' section includes 'Background Bulk Data Transfer Rate' (High). The 'DATA COMPRESSION' section includes 'IP Header Compression Ratio' (High). Each setting has a 'Save' and 'Cancel' button.

See 'Radio > Channel Setup' for radio channel settings.

Link > Monitoring > Terminal

This page displays both the local and remote radio current internal and external input source radio power supply voltage diagnostic parameters.

The results shown are since the page was opened and are updated automatically every 12 seconds.

The screenshot shows the 4RF SUPERVISOR interface with the 'Link' tab selected. Under 'Monitoring', the 'Terminal' sub-tab is active. The interface is split into two columns for 'Local Radio' and 'Remote Radio'. Each column has a status bar with indicators for OK, MODE, USB, TX, and RX, all of which are green. Below the status bars are two identical tables titled 'POWER SUPPLY PARAMETERS'. Each table has a 'User' column with checkboxes. The data for the Local Radio is as follows:

Parameter	Value	User
Current VDC Power Supply	24.195 V	<input type="checkbox"/>
Current 3.3V Power Supply	3.322 V	<input type="checkbox"/>
Current 5.0V Power Supply	5.287 V	<input type="checkbox"/>
Current 15.0V Power Supply	14.800 V	<input type="checkbox"/>

The data for the Remote Radio is as follows:

Parameter	Value	User
Current VDC Power Supply	24.166 V	<input type="checkbox"/>
Current 3.3V Power Supply	3.314 V	<input type="checkbox"/>
Current 5.0V Power Supply	5.308 V	<input type="checkbox"/>
Current 15.0V Power Supply	14.867 V	<input type="checkbox"/>

See 'Monitoring > Terminal' for parameters setup.

Link > Monitoring > Ethernet

This page displays both the local and remote radio current performance monitoring parameters per Ethernet port transmission (TX) 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.

The screenshot shows the 4RF SUPERVISOR interface with the 'Link' tab selected. Under 'Monitoring', the 'Ethernet' sub-tab is active. The interface is split into two columns: 'Local Radio' and 'Remote Radio'. Each column has a status bar with indicators for OK, MODE, USB, TX, and RX. Below these are two tables for 'ETHERNET PORT 1 TRANSMIT' and 'ETHERNET PORT 1 RECEIVE' statistics. Each table includes a 'Reset' button and a 'User' column with checkboxes.

ETHERNET PORT 1 TRANSMIT		User
Maximum Capacity	100 Mbps	<input type="checkbox"/>
Packets	117	<input type="checkbox"/>
Bytes	62,892	<input type="checkbox"/>
Packet Collisions	0	<input type="checkbox"/>
VLAN Frames	0	<input type="checkbox"/>
<input type="button" value="Reset"/>		

ETHERNET PORT 1 RECEIVE		User
Packets	122	<input type="checkbox"/>
Bytes	35,660	<input type="checkbox"/>
Packets equal to 64 Bytes	71	<input type="checkbox"/>
Packets 65 to 127 Bytes	4	<input type="checkbox"/>
Packets 128 to 255 Bytes	0	<input type="checkbox"/>
Packets 256 to 511 Bytes	0	<input type="checkbox"/>
Packets 512 to 1023 Bytes	47	<input type="checkbox"/>
Packets 1024 to 1536 Bytes	0	<input type="checkbox"/>
Broadcast Packets	0	<input type="checkbox"/>
Multicast Packets	0	<input type="checkbox"/>
VLAN Frames	0	<input type="checkbox"/>
VLAN Frames dropped	0	<input type="checkbox"/>
Packet in Error	0	<input type="checkbox"/>
Bytes in Error	0	<input type="checkbox"/>
CRC/Alignment Errors	0	<input type="checkbox"/>
Undersized Packets	0	<input type="checkbox"/>
Oversized Packets	0	<input type="checkbox"/>
Fraumented Packets	0	<input type="checkbox"/>

See 'Monitoring > Ethernet' on page 189 for parameters setup.

Link > Monitoring > Radio

This page displays both the local and remote radio 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 displays the 4RF SUPERVISOR interface for monitoring radio performance. It is divided into two main columns: Local Radio and Remote Radio. Each column contains status indicators (OK, MODE, USB, TX, RX) and a 'Status' section with green lights. Below these are detailed monitoring sections for TRANSMITTER, RECEIVER, TRANSMIT PATH, and RECEIVE PATH, each with a 'Reset' button and a 'User' field.

Parameter	Local Radio Value	Remote Radio Value
TRANSMITTER		
Current Temperature	35.6 C	34.3 C
Packets Transmitted	15	15
Bytes Transmitted	1,723	1,874
Dropped Packets (Congestion)	0	0
Dropped Bytes (Congestion)	0	0
Last Tx PA Current	1,135 mA	907 mA
Last Tx PA Driver Current	96 mA	35 mA
Last Tx Forward Power	32.0 dBm	34.0 dBm
RECEIVER		
Packets Received	15	15
Bytes Received	1,874	1,723
Packets Received in Error	0	0
Dropped Packets (Filtering)	0	0
Dropped Bytes (Filtering)	0	0
TRANSMIT PATH		
Remote Name	Remote Radio	Local Radio
Modulation	64QAM Lo	64QAM Lo
Timestamp	02/01/2011 01:47:07	01/01/2011 22:33:53
RECEIVE PATH		

See 'Monitoring > Radio' on page 194 for parameters setup.

Link > Monitoring > User Selected

This page displays the ‘User’ parameters setup in all the other Monitoring screens for both the local and remote radios.

The results shown are since the page was opened and are updated automatically every 12 seconds.

The screenshot shows the 4RF SUPERVISOR interface with the 'Link' tab selected. The 'Monitoring' sub-tab is active, and 'User Selected' is chosen under the 'Radio' category. The interface is split into two columns for 'Local Radio' and 'Remote Radio'. Each column has a status bar with indicators for OK, MODE, USB, TX, and RX. Below these are two panels: 'TERMINAL DETAILS' and 'RF LINK PARAMETERS'. The 'Local Radio' panel shows transmitter current (94 mA) and receiver filtering statistics (0 dropped packets/bytes). The 'Remote Radio' panel shows transmitter current (910 mA) and receiver filtering statistics (0 dropped packets/bytes). The 'RF LINK PARAMETERS' section for the local radio shows transmit path details (Remote Name: Remote Radio, Modulation: 64QAM Lo, Timestamp: 02/01/2011 01:51:57) and receive path details (Remote Name: Remote Radio, RSSI: -48.7 dBm, SNR: 37.0 dB, Frequency Error: -20 Hz, Modulation: 64QAM Lo, Timestamp: 02/01/2011 01:51:57). The 'Remote Radio' panel shows receive path details (Remote Name: Local Radio, RSSI: -47.5 dBm, SNR: 39.3 dB, Frequency Error: 82 Hz, Modulation: 64QAM Lo, Timestamp: 01/01/2011 22:38:42). A 'Logout ADMIN' link is visible in the top right corner.

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 FE 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 214 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

The screenshot shows the 4RF SUPERVISOR interface for a Protected Station. At the top, there are navigation tabs for Local, Remote, and Link, and a Logout ADMIN button. Below this is a menu with options: Terminal, Radio, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring. Under the Terminal menu, there are sub-tabs: Summary, Details, Device, Date/Time, and Operating Mode. The main content area displays the status of the Protected Station with indicators for OK, MODE, USB, TX, and RX for both Primary and Secondary stations. Below this are two summary tables:

TERMINAL SUMMARY	
Terminal Name	Protected Station
Location	Wellington
Contact Name	4RF Limited
Contact Details	support@4rf.com
Date and Time	01/05/2015 17:41:11

OPERATING SUMMARY	
Operating Mode	Point To Point
Ethernet Mode	Bridge
Interface Mode	Ethernet Only
Modem Mode	Mode A (ETSI / ACMA)
TX Frequency (MHz)	400
TX Power (dBm)	32
RX Frequency (MHz)	406.25
Channel Size (kHz)	12.5
Network ID (FAN)	CAFE
Base Station ID	2
Node Address	0000
Inband Management	Enabled
Inband Management Timeout (s)	10

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
Monitored Hot Standby (Protected Station)	The RF ports and interface ports from two standard Aprisa FE 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 277 for the list of monitored alarms.
Redundant (Protected Station)	The RF ports and interface ports from two standard Aprisa FE 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 63 for parameter details.

Protected Station: Terminal > Details

The screenshot displays the 4RF SUPERVISOR interface for a Protected Station. At the top, there are navigation tabs for 'Local', 'Remote', and 'Link', and a 'Logout ADMIN' button. Below this is a menu bar with options: 'Terminal', 'Radio', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. Under 'Terminal', there are sub-tabs for 'Summary' and 'Details'. The 'Details' tab is active, showing a status bar with 'Protected Station' and control buttons for 'OK', 'MODE', 'USB', 'TX', and 'RX' for both 'Primary' and 'Secondary' units. The 'Primary' unit has a red 'OK' button and green 'MODE', 'USB', 'TX', and 'RX' buttons. The 'Secondary' unit has a grey 'OK' button and green 'MODE', 'USB', 'TX', and 'RX' buttons.

PRIMARY UNIT MANUFACTURING DETAILS

Radio Serial Number	R1310001682
Sub-Assembly Serial Number	13094428
HW Variant Type	400 - 470MHz
Ethernet Port 1 MAC Address	00:22:b2:10:24:e1
Ethernet Port 2 MAC Address	00:22:b2:10:24:e2
Ethernet Port 3 MAC Address	00:22:b2:10:24:e3
Ethernet Port 4 MAC Address	00:22:b2:10:24:e4
Active Software Version	1.4.0
Previous Software Version	Unknown

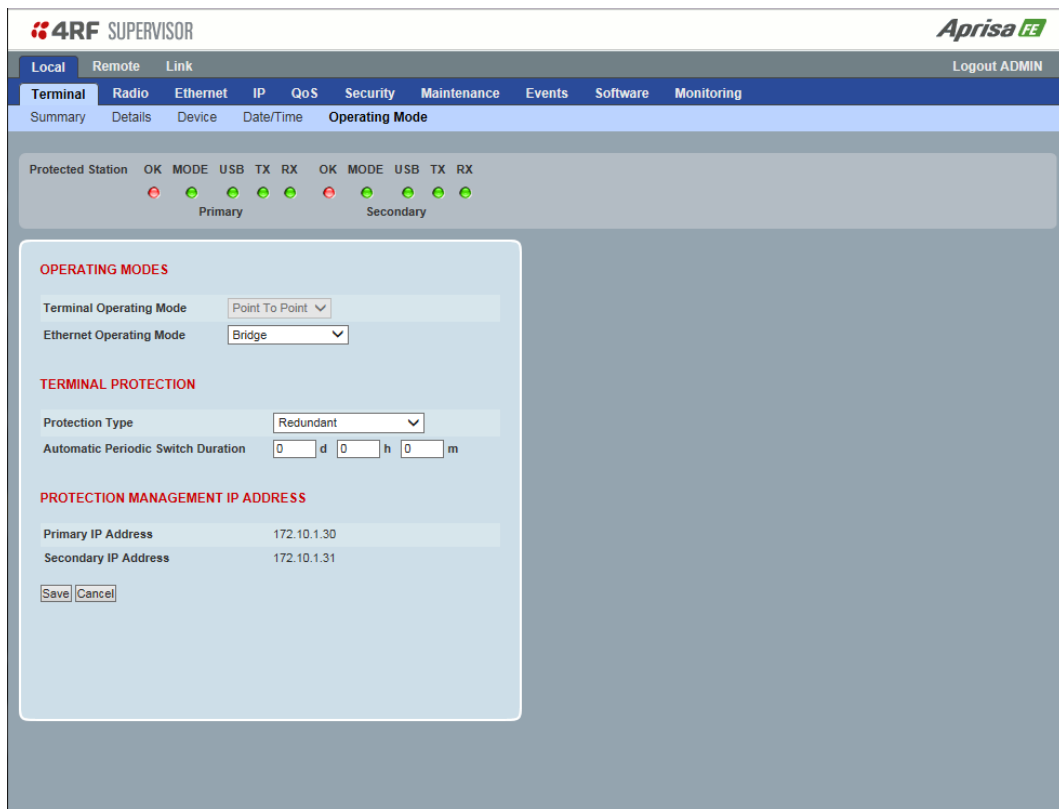
SECONDARY UNIT MANUFACTURING DETAILS

Radio Serial Number	R1310001178
Sub-Assembly Serial Number	13093341
HW Variant Type	400 - 470MHz
Ethernet Port 1 MAC Address	00:22:b2:10:19:00
Ethernet Port 2 MAC Address	00:22:b2:10:19:01
Ethernet Port 3 MAC Address	00:22:b2:10:19:02
Ethernet Port 4 MAC Address	00:22:b2:10:19:03
Active Software Version	1.4.0
Previous Software Version	Unknown

PRIMARY UNIT / SECONDARY UNIT MANUFACTURING DETAILS

See 'Terminal > Details' on page 65 for parameter settings.

Protected Station: Terminal > Operating Mode



OPERATING MODES

Terminal Operating Mode

The Terminal Operating Mode is fixed at Point To Point.

Ethernet Operating Mode

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

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

TERMINAL PROTECTION

Protection Type

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

Option	Function
None	The FE radio is a stand-alone radio (not part of an Aprisa FE Protected Station).
Redundant (Protected Station)	The FE radio is part of an Aprisa FE Protected Station. The RF ports and interface ports from two standard Aprisa FE 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 FE radio part of an Aprisa FE Protected Station. The RF ports and interface ports from two standard Aprisa FE 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 277 for the list of monitored alarms.

Automatic Periodic Switch Duration

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

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

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

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

PROTECTION MANAGEMENT IP ADDRESS

Primary Address

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

Secondary Address

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

Radio

Protected Station: Radio > Radio Setup

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

The screenshot shows the 'Radio Setup' configuration page in the 4RF SUPERVISOR interface. At the top, there are navigation tabs for 'Local', 'Remote', and 'Link', and a 'Logout ADMIN' link. Below this is a menu bar with options like 'Terminal', 'Radio', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. The 'Radio' tab is selected, and sub-tabs include 'Radio Summary', 'Channel Summary', 'Radio Setup', 'Channel Setup', and 'Advanced Setup'. The main content area is titled 'Protected Station' and shows status indicators for 'Primary' and 'Secondary' stations. The configuration is divided into several sections:

- TRANSMITTER:** TX Frequency (MHz) set to 400, TX Power (dBm) set to 32.
- RECEIVER:** RX Frequency (MHz) set to 406.25.
- GENERAL:** Channel Size (kHz) set to 12.5, Antenna Port Configuration set to 'Single Antenna Dual Port (Duplexer)'.
- MODEM:** Modem Mode set to 'Mode A (ETSI / ACMA)', Enhanced Noise Rejection Mode set to 'Disabled', Modulation Type set to '64QAM (Low Gain)'.
- ADAPTIVE CODING MODULATION:** Default Modulation set to 'QPSK (High Gain)', Modulation Range set from 'QPSK (High Gain)' to '64QAM (Low Gain)'.

 'Save' and 'Cancel' buttons are present at the bottom of each configuration section.

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 282.

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: <ol style="list-style-type: none"> (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)	<p>Select Dual Antenna Dual Port for a dual antenna protected station using:</p> <p>(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.</p> <p>(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.</p> <p>(3) Single frequency in half duplex transmission with an external dual antennas, connected to the A and B ANT/TX and RX antenna ports.</p> <p>(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.</p>

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.

The screenshot shows the 4RF SUPERVISOR interface for a Protected Station. The top navigation bar includes 'Local', 'Remote', and 'Link' tabs, with 'Local' selected. The main menu includes 'Terminal', 'Radio', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. The 'Ethernet' menu is expanded to show 'Summary', 'Port Setup', 'L2 Filtering', and 'VLAN'. The 'Summary' page displays the station's status and two tables: 'PRIMARY ETHERNET PORTS STATUS' and 'ETHERNET PORTS SETTINGS'.

Protected Station Status:

Protected Station	OK	MODE	USB	TX	RX	OK	MODE	USB	TX	RX
Primary	⊘	⊙	⊙	⊙	⊙	⊘	⊙	⊙	⊙	⊙
Secondary										

PRIMARY ETHERNET PORTS STATUS

ID	Name	Status	Speed (Mbit/s)	Duplex
1	Ethernet Port	Up	100	Full
2	Ethernet Port	Down	10	Half
3	Ethernet Port	Down	10	Half
4	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
3	Ethernet Port	Down	10	Half
4	Ethernet Port	Down	10	Half

ETHERNET PORTS SETTINGS

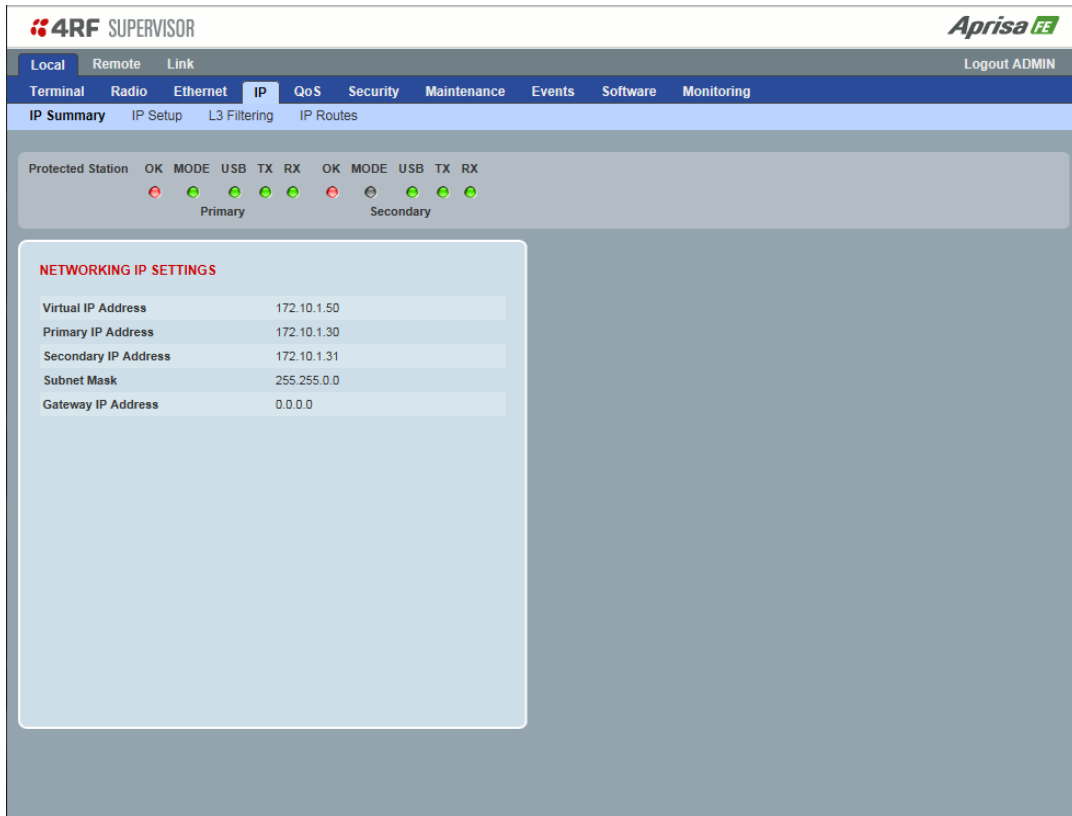
ID	Name	Mode	Speed (Mbit/s)	Duplex	Function
1	Ethernet Port	Switch	Auto	Auto	Mgmt & User
2	Ethernet Port	Switch	Auto	Auto	Mgmt & User
3	Ethernet Port	Standard	Auto	Auto	Mgmt & User
4	Ethernet Port	Standard	Auto	Auto	Mgmt & User

See 'Ethernet > Port Setup' for configuration options.

IP

Protected Station: IP > IP Summary

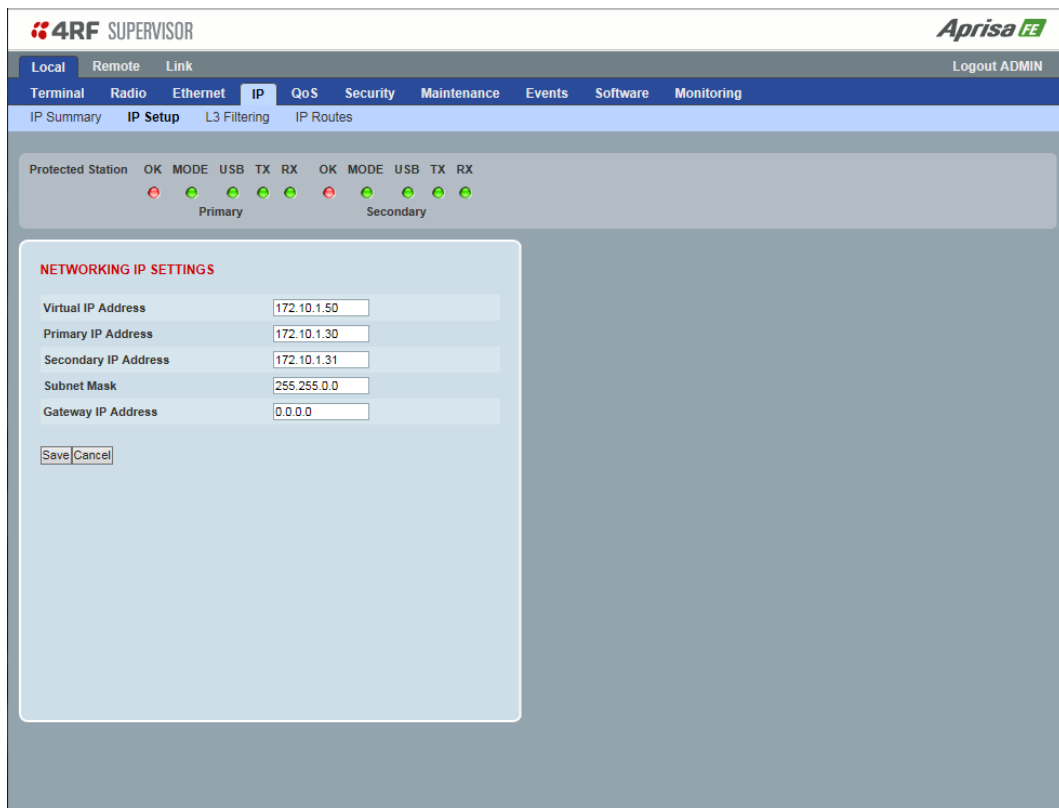
This page displays the current settings for the Protected Station Networking IP settings.



See 'IP > IP Summary > Bridge / Gateway Router Modes' on page 95 for configuration options.

Protected Station: IP > IP Setup

This page provides the setup for the Protected Station Networking IP setup.



NETWORKING IP SETTINGS

Changes in these parameters are automatically changed in the partner radio.

Primary IP Address

Set the static IP Address of the primary radio assigned by your site network administrator using the standard format xxx.xxx.xxx.xxx. The default IP address is in the range 169.254.50.10.

Secondary IP Address

Set the static IP Address of the secondary radio assigned by your site network administrator using the standard format xxx.xxx.xxx.xxx. The default IP address is in the range 169.254.50.10.

Protected Station Virtual IP Address (PVIP)

The Protected Station Virtual IP Address (PVIP) is the IP Address of the active radio whether it is the primary radio or the secondary radio.

The PVIP is available in both bridge and router modes.

In router mode, the PVIP can be used as 'next hop' IP address by external routers to reach the protected station so the protection station switch will always be transparent to the external devices and routers.

In both bridge and router modes, the PVIP is used in terminal server mode in remote protected stations. The PVIP is used to reach the protected remote radio from the SCADA master connected to local radio in terminal server mode.

Note: The radio IP address should be used for SNMP management as using the PVIP for SNMP management will result in undefined behaviour if a switch-over occurs during an SNMP transaction. Thus, using PVIP for SNMP network management is not recommended.

After a switch-over, new active radio owns the PVIP and will send out a gratuitous ARP to clear the MAC learning tables of upstream switches/routers.

Set the static IP Address of the PVIP using the standard format xxx.xxx.xxx.xxx. The default IP address is 0.0.0.0.

Subnet Mask

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

Gateway

Set the Gateway address of the radio, if required, using the standard format xxx.xxx.xxx. The default Gateway is 0.0.0.0.

RADIO INTERFACE IP SETTINGS

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

Radio Interface IP Address

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

Radio Interface Subnet Mask

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

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

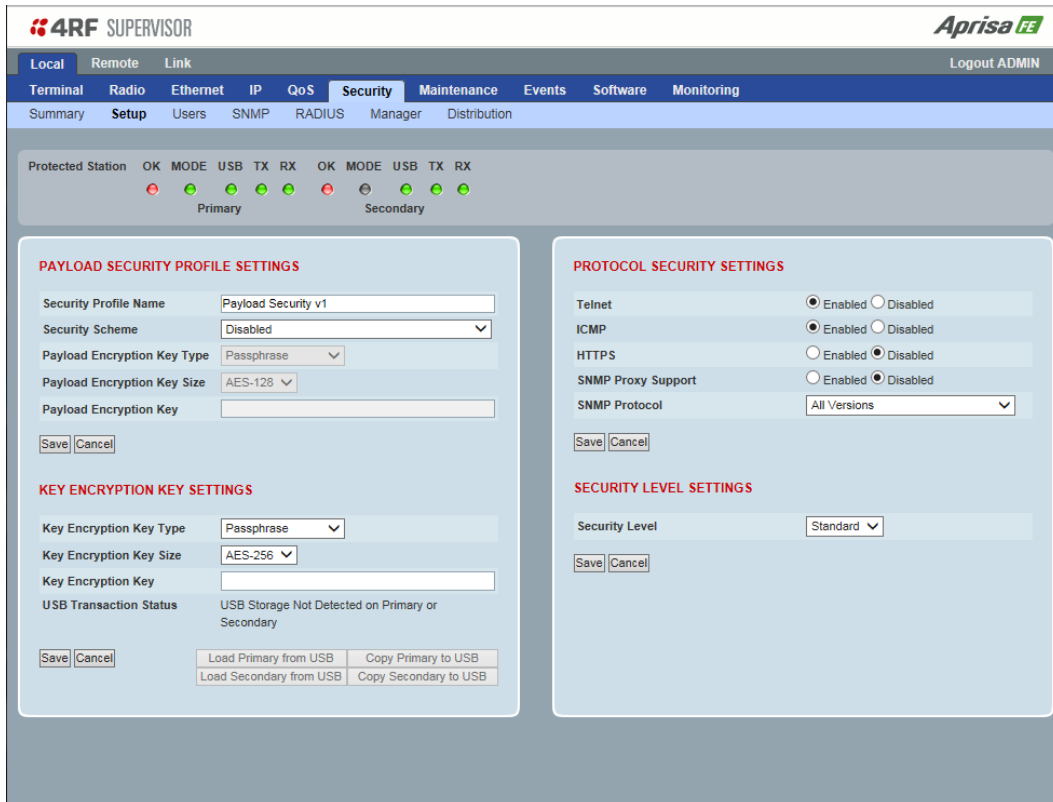
When the base radio has a host specific RF interface IP address, then all the remotes must have a host specific RF interface IP address from the same subnet.

Note 2: When a remote radio is configured for Router Mode and the base radio is changed from Bridge Mode to Router Mode and the RF interface IP address is set to AUTO IP configuration (at least the last octet of the RF interface IP address is zero), it is mandatory to configure the network topology by using the 'Decommission Node' and 'Discover Nodes' (see 'Maintenance > Advanced' on page 155).

Security

Protected Station: Security > Setup

This page displays the current settings for the Security parameters.



KEY ENCRYPTION KEY SETTINGS

USB Transaction Status

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

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

Controls

These buttons are grayed out if a USB flash drive is not plugged into the radio host port.

The ‘Load Primary From USB’ button loads the Key Encryption Key settings from the primary radio USB flash drive into the primary radio.

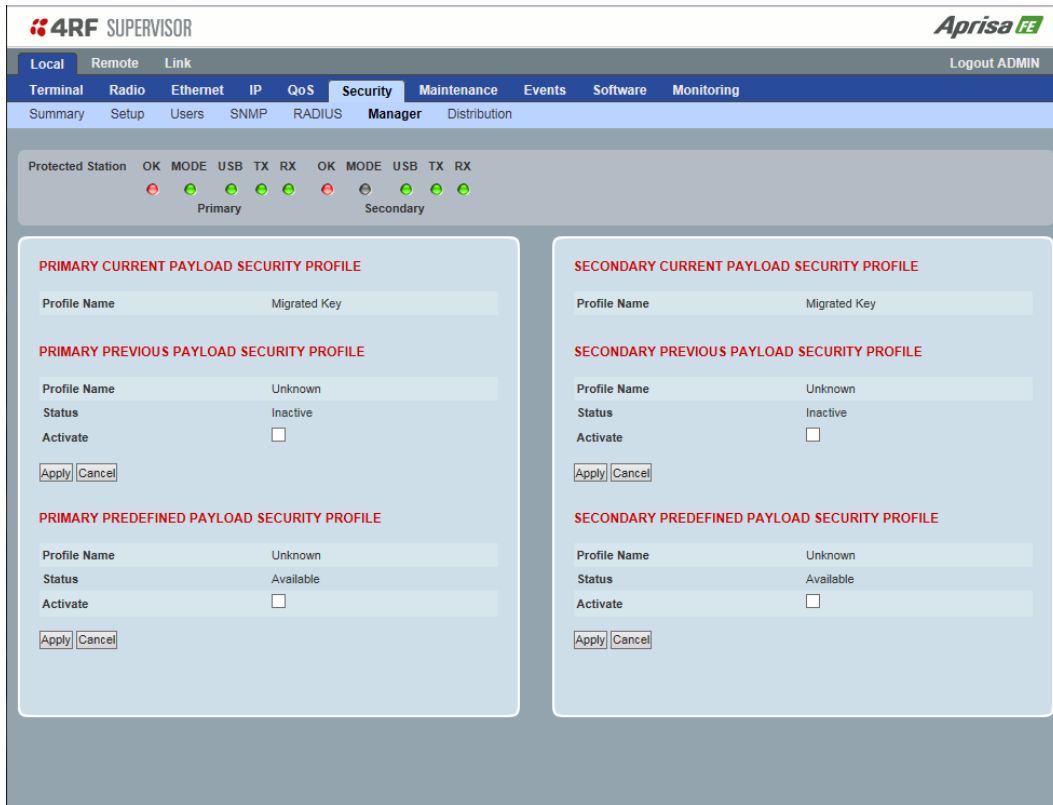
The ‘Copy To Primary USB’ button copies the Key Encryption Key settings from the primary radio to the primary radio USB flash drive.

The ‘Load Secondary From USB’ button loads the Key Encryption Key settings from the secondary radio USB flash drive into the secondary radio.

The ‘Copy To Secondary USB’ button copies the Key Encryption Key settings from the secondary radio to the secondary radio USB flash drive.

Protected Station: Security > Manager

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



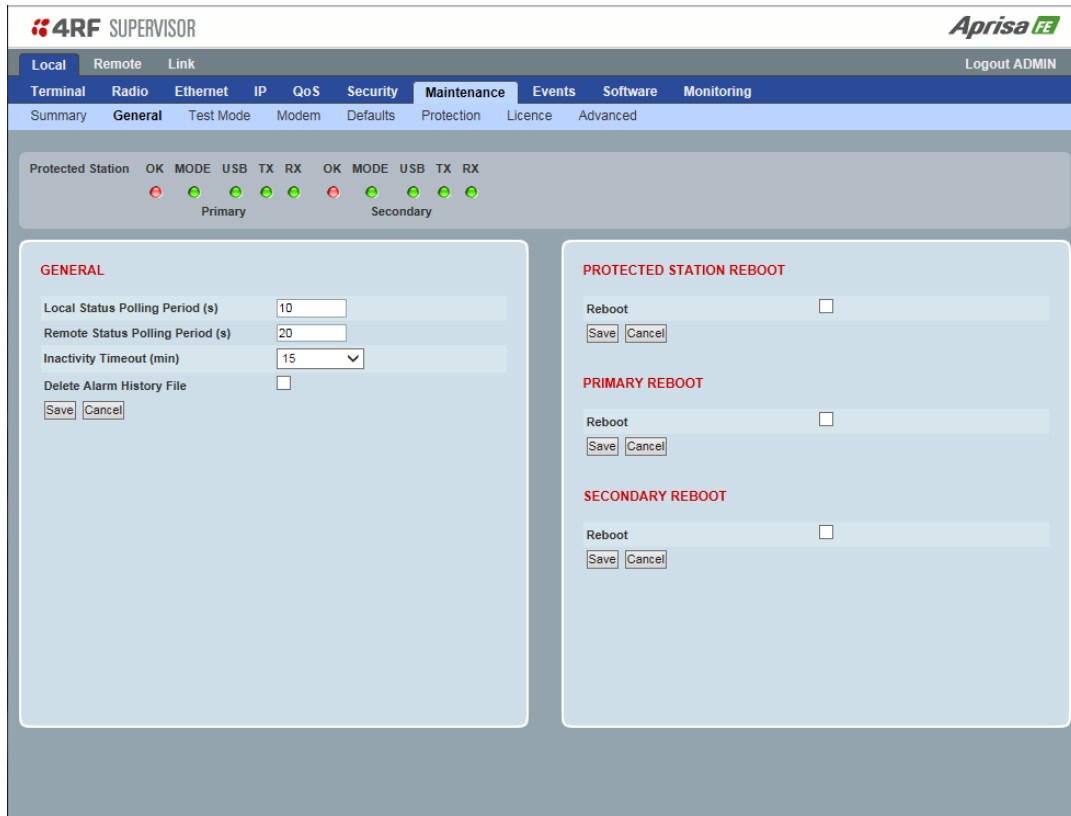
PRIMARY / SECONDARY SECURITY PROFILE

See 'Security > Manager' on page 140 for parameter details.

Maintenance

Protected Station: Maintenance > General

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



See 'Maintenance > General' on page 147 for parameter details.

Protected Station: Maintenance > Protection

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

The screenshot shows the 4RF SUPERVISOR interface for the 'Protection' settings. At the top, there are navigation tabs for 'Local', 'Remote', and 'Link'. Below that, a menu bar includes 'Terminal', 'Radio', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. The 'Maintenance' tab is active, and the 'Protection' sub-tab is selected. The interface displays status indicators for 'Protected Station' with 'OK' and 'MODE' (USB, TX, RX) for both 'Primary' and 'Secondary' units. Two main configuration panels are visible: 'SOFTWARE MANUAL LOCK' and 'COPY CONFIGURATION'. The 'SOFTWARE MANUAL LOCK' panel includes a 'Lock Type' dropdown set to 'Enabled', a 'Lock Active To' dropdown set to 'Primary', and a 'Duration (s)' input field set to '0'. There are 'Save', 'Cancel', and 'Switch Now' buttons. The 'COPY CONFIGURATION' panel has checkboxes for 'Copy from Primary to Secondary' and 'Copy from Secondary to Primary', both currently unchecked, and a 'Copy Status' field showing 'Available'. Below these panels is a 'CURRENT PROTECTION INFORMATION' table.

CURRENT PROTECTION INFORMATION	
Switch Control	Software Manual Lock
Active Unit	Primary
Switch Count	9

SOFTWARE MANUAL LOCK

The software Manual Lock is a software implementation of the Hardware Manual Lock switch on the Protection Switch.

Lock Active To

This parameter sets the Protection Switch Software Manual Lock. The Software Manual Lock only operates if the Hardware Manual Lock is deactivated (set to the Auto position).

Option	Function
Automatic	The protection is automatic and switching will be governed by normal switching and blocking criteria.
Primary	The primary radio will become active i.e. traffic will be switched to the primary radio.
Secondary	The secondary radio will become active i.e. traffic will be switched to the secondary radio.

Duration (s)

This parameter defines the period required for manually locking to the primary or secondary radios. When this period elapses, the Lock To becomes automatic.

Switch Now Button

This button forces a switch-over independent of the state of Lock Type.

CURRENT PROTECTION INFORMATION

Switch Control

This parameter shows the status of the switch control i.e. which mechanism is in control of the protection switch.

Option	Function
Automatic	The protection is automatic and switching will be governed by normal switching and blocking criteria.
Software Manual Lock	The Software Manual Lock has control of the protection switch.
Hardware Manual Lock	The Hardware Manual Lock has control of the protection switch.

Active Unit

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

Switch Count

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

Automatic Periodic Switch will occur in

If this parameter is visible, the Automatic Periodic Switch feature has been enabled and will show the period before the next automatic switch-over.

COPY CONFIGURATION

When common parameters are changed in one radio, they are automatically changed in the partner radio but if one radio has been replaced in the protected station, common parameters will need to be updated in the new radio.

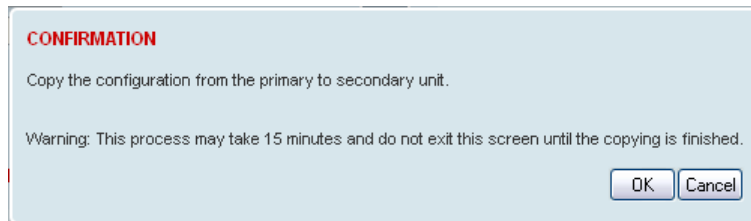
Note: This function does not copy user IDs, passwords, encryption keys or licenses. These must be entered manually.

Copy from Primary to Secondary

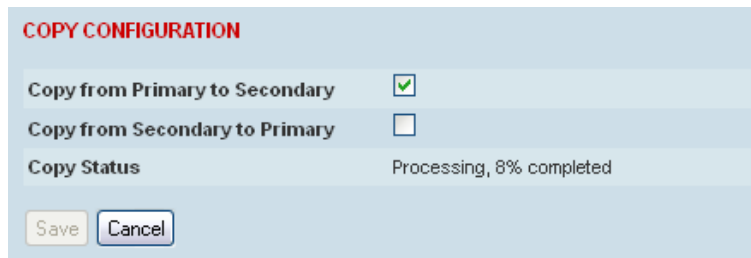
This parameter copies all common parameters from the primary to the secondary radio.

To activate copy configuration:

1. Tick the Copy from Primary to Secondary and click Save.



2. To continue, click OK.



Copy from Secondary to Primary

This parameter copies all common parameters from the secondary to the primary radio.

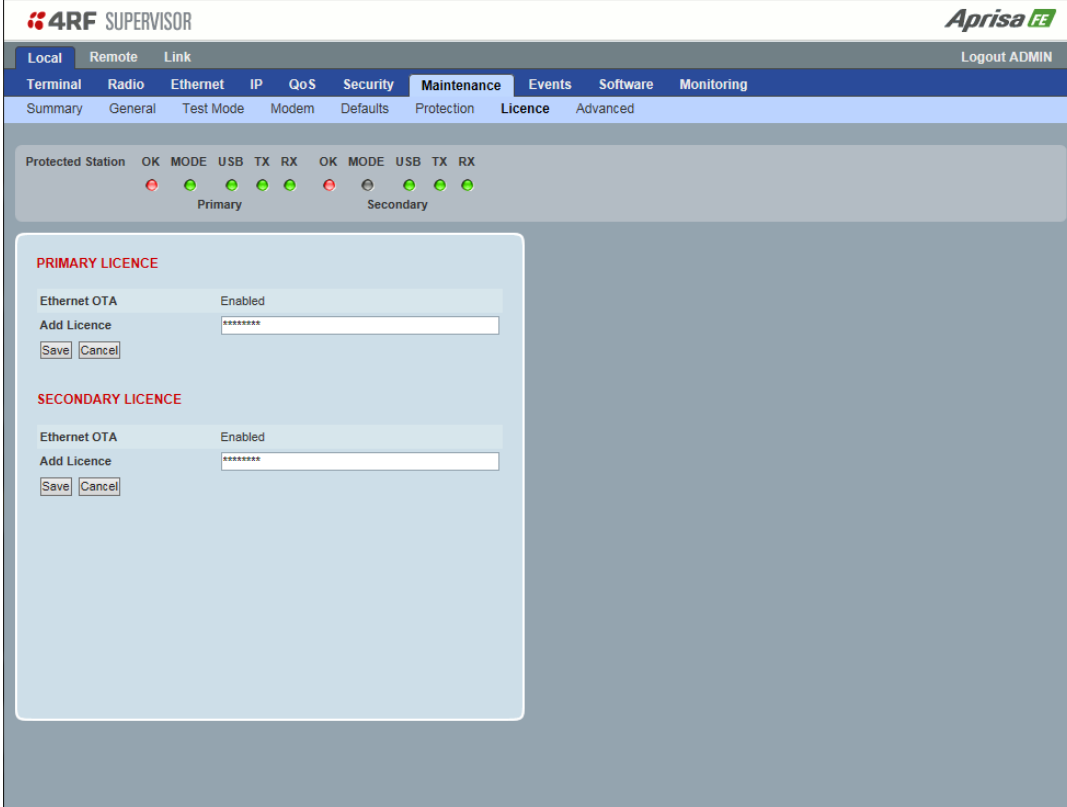
Copy Status

This parameter displays the status of the Copy Configuration.

Option	Function
Available	The Copy Configuration feature can be used (but not necessarily required).
Processing	The Copy Configuration feature is running and the % completed.

Protected Station: Maintenance > Licence

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



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 with options: Terminal, Radio, Ethernet, IP, QoS, Security, Maintenance (selected), Events, Software, and Monitoring. Under the Maintenance tab, there are sub-tabs: Summary, General, Test Mode, Modem, Defaults, Protection, Licence (selected), and Advanced. The main content area shows the status of a Protected Station with two sections: Primary and Secondary. Each section has a set of status indicators (OK, MODE, USB, TX, RX) and a configuration panel. The configuration panel for both Primary and Secondary licences includes an 'Ethernet OTA' field set to 'Enabled', an 'Add Licence' field with a masked input (*****), and 'Save' and 'Cancel' buttons.

PRIMARY / SECONDARY LICENCE

See 'Maintenance > Licence' on page 154 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 155 for parameter details.

RF Interface MAC address

This parameter is only applicable when the radio is part of a Protected Station.

This RF Interface MAC address is used to define the MAC address of the Protection Switch. This address is entered in the factory. Both Protected Station radios read and use this MAC address.

This MAC address entry will only be used by the software if it detects that the factory MAC address set in the internal EPROM of the protected switch is corrupted for some reason, otherwise the software will ignore the MAC address entered by the user.

The RF interface MAC address is used for registration process only. For example, in a remote Protected Station, both radios share the same RF MAC address and a single entry of the remote Protected Station will be presented in network table (Network Status > Network Table).

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

4RF Limited www.4RF.com Made in New Zealand MAC Address: 00-22-B2-10-19-00 Serial Number: R1310002499	

PRIMARY / SECONDARY CONFIGURATION

See 'Maintenance > Advanced' on page 155 for parameter details.

PRIMARY / SECONDARY MAINTENANCE FILES

See 'Maintenance > Advanced' on page 155 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 FE 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 299 for a complete list of events.

The screenshot shows the 4RF SUPERVISOR interface for a Protected Station. At the top, there are navigation tabs for Local, Remote, and Link, and a Logout ADMIN button. Below that is a menu bar with options like Terminal, Radio, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring. The 'Events' menu is active, showing sub-options: Alarm Summary, Primary History, Secondary History, Events Setup, Traps Setup, I/O Setup, Primary Actions, Secondary Actions, and Defaults. The main content area shows the status of the Protected Station with indicators for OK, MODE, USB, TX, and RX for both Primary and Secondary paths. Below this are two scrollable panels: 'PRIMARY ALARM SUMMARY' and 'SECONDARY ALARM SUMMARY'. The Primary panel lists various alarm events such as Transmit Path, Receive Path (including RSSI Threshold, RX Synthesizer Not Locked, and RX CRC Errors), Radio Interface Path (including RF No Receive Data and Radio Network), Customer Equipment Interface Path, Component Failure, Diagnostic, and Software (including Calibration Failure, Configuration Not Supported, Remote Communications Lost, Network Configuration Warning, Software Restart Required, and Software Activation Pending). The Secondary panel lists events like Transmit Path, PA Current, PA Driver Current, PA Stability, TX AGC, TX Forward Power, TX Reverse Power, Temperature Threshold, TX Synthesizer Not Locked, Thermal Shutdown, Receive Path, and Radio Interface Path (including Customer Equipment Interface Path, Port1 Eth No Receive Data, Port1 Eth Data Receive Errors, Port1 Eth Data Transmit Errors, Port2 Eth No Receive Data, and Port2 Eth Data Receive Errors).

PRIMARY / SECONDARY ALARM SUMMARY

See 'Events > Alarm Summary' on page 159 for parameter details.

Protected Station: Events > Primary History

4RF SUPERVISOR Aprisa FE

Local Remote Link Logout ADMIN

Terminal Radio 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

Protected Station OK MODE USB TX RX OK MODE USB TX RX

Primary Secondary

PRIMARY EVENT HISTORY

Log ID	Date/time	Event ID	Description	State	Severity	Additional Information
68	01/05/2015 17:16:34	17	Protection SW Manual Lock	active	warning	Lock Active
67	01/05/2015 17:16:22	33	Protection Switch Occurred	inactive	information	Possible Alarm condition or Auto Switch on Active
66	01/05/2015 17:16:01	33	Protection Switch Occurred	inactive	information	Alarm Condition
65	01/05/2015 17:16:00	17	Protection SW Manual Lock	inactive	cleared	Lock Cleared
64	01/05/2015 17:15:59	17	Protection SW Manual Lock	active	warning	Lock Active
63	01/05/2015 17:15:58	33	Protection Switch Occurred	inactive	information	Manual Lock
62	01/05/2015 17:11:52	33	Protection Switch Occurred	inactive	information	Alarm Condition
61	01/05/2015 17:07:52	32	Network Configuration Warning	inactive	cleared	Alarm Cleared: Forwarding type mismatch

Auto Refresh

PRIMARY EVENT HISTORY

See 'Events > Event History' on page 160 for parameter details.

Protected Station: Events > Secondary History

4RF SUPERVISOR Aprisa FE

Local Remote Link Logout ADMIN

Terminal Radio 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

Protected Station OK MODE USB TX RX OK MODE USB TX RX

Primary Secondary

SECONDARY EVENT HISTORY

Log ID	Date/time	Event ID	Description	State	Severity	Additional Information
46	01/05/2015 17:16:43	17	Protection SW Manual Lock	active	warning	Lock Active
45	01/05/2015 17:16:31	33	Protection Switch Occurred	inactive	information	Alarm Condition
44	01/05/2015 17:16:09	33	Protection Switch Occurred	inactive	information	Possible Alarm condition or Auto Switch on Active
43	01/05/2015 17:16:08	17	Protection SW Manual Lock	inactive	cleared	Lock Cleared
42	01/05/2015 17:16:07	17	Protection SW Manual Lock	active	warning	Lock Active
41	01/05/2015 17:16:06	33	Protection Switch Occurred	inactive	information	Manual Lock
40	01/05/2015 17:11:59	33	Protection Switch Occurred	inactive	information	Possible Alarm condition or Auto Switch on Active
39	01/05/2015 17:06:38	33	Protection Switch Occurred	inactive	information	Alarm Condition

Auto Refresh Prev Next

SECONDARY EVENT HISTORY

See 'Events > Event History' on page 160 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 FE radio (see ‘Single Radio Software Upgrade’ on page 293). This process would only be used if the radio was a replacement or a new station in an existing network.

Link Software Upgrade

The radio software can be upgraded on a Aprisa FE radio remotely over the radio link (see ‘Non Protected Link ’ on page 290). This process involves the following steps:

1. Transfer the new software to local primary radio with ‘Protected Station: Software > Primary File Transfer’.
2. File Transfer the new software to local secondary radio with ‘Protected Station: Software > Secondary File Transfer’.
3. Using the Software Manual Lock, manually lock the protected remote radios (if any) to the currently active radio (this is necessary to prevent automatic switching during the distribution and activation process).
4. Distribute the new software to the remote radio with ‘Protected Station: Software > Remote Distribution’. Note: The software pack in the local active radio is used for distribution.
5. Activate the new software on the remote radio with ‘Protected Station: Software > Remote Activation’.
6. Finally, activate the new software on the local 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.

The screenshot shows the 4RF Supervisor interface for a Protected Station. The top navigation bar includes 'Local', 'Remote', and 'Link' tabs, with 'Local' selected. Below this is a menu with 'Terminal', 'Radio', 'Ethernet', 'IP', 'QoS', 'Security', 'Maintenance', 'Events', 'Software', and 'Monitoring'. The 'Software' tab is active, and the sub-menu shows 'Summary', 'Setup', 'Primary File Transfer', 'Secondary File Transfer', 'Manager', 'Remote Distribution', and 'Remote Activation'. The 'Summary' sub-menu item is selected.

At the top of the main content area, there are status indicators for 'Protected Station'. For the 'Primary' station, the 'OK' indicator is red, while 'MODE', 'USB', 'TX', and 'RX' are green. For the 'Secondary' station, 'OK' is red, 'MODE' is grey, and 'USB', 'TX', and 'RX' are green.

The main content area is divided into two columns:

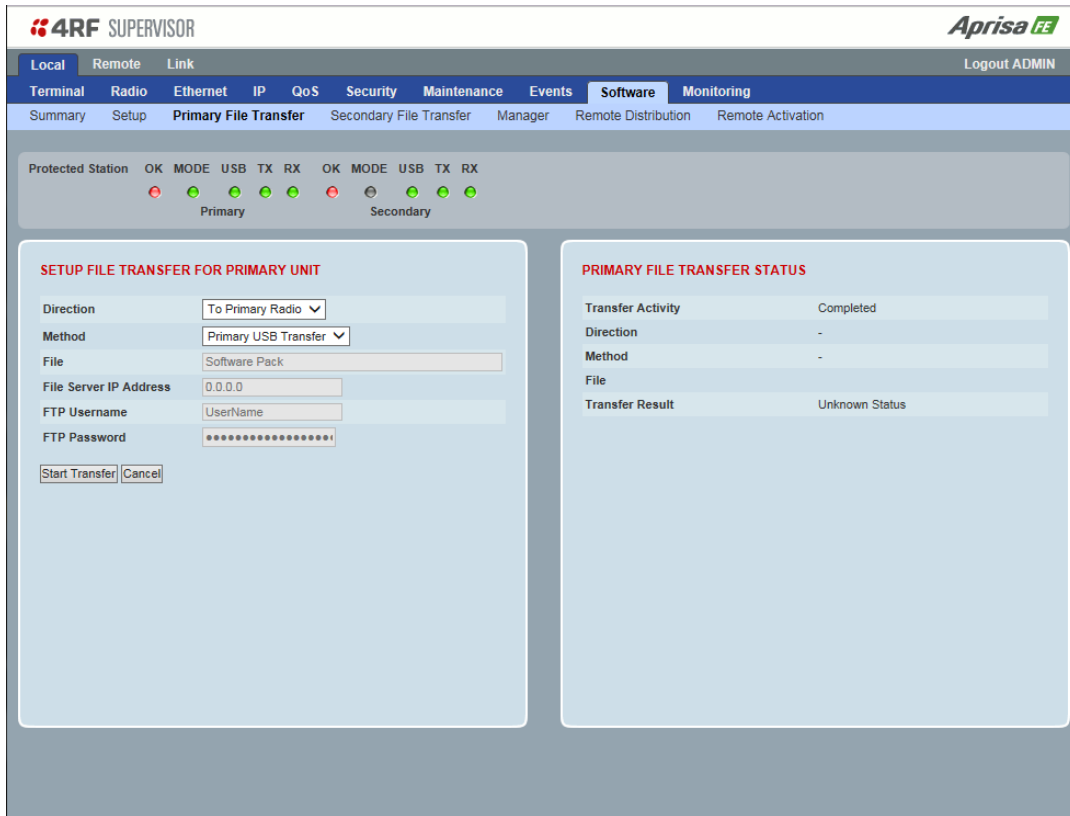
- PRIMARY SOFTWARE VERSIONS:**
 - Current Version: 1.5.0
 - Previous Version: 1.4.0
 - Software Pack Version: 1.5.0
- SECONDARY SOFTWARE VERSIONS:**
 - Current Version: 1.5.0
 - Previous Version: 1.4.0
 - Software Pack Version: 1.5.0
- PRIMARY USB AUTOMATIC UPGRADE:**
 - USB Boot Cycle Upgrade: Load And Activate
- SECONDARY USB AUTOMATIC UPGRADE:**
 - USB Boot Cycle Upgrade: Load And Activate
- PRIMARY FILE TRANSFER:**
 - Transfer Activity: [Empty]
 - Method: Unknown
 - Filename: [Empty]
 - Transfer Result: [Empty]
- SECONDARY FILE TRANSFER:**
 - Transfer Activity: [Empty]
 - Method: Unknown
 - Filename: [Empty]
 - Transfer Result: [Empty]

PRIMARY / SECONDARY SOFTWARE VERSIONS

See 'Protected Station: Software > Primary File Transfer' and 'Protected Station: Software > Secondary File Transfer' for parameter details.

Protected Station: Software > Primary File Transfer

This page provides the mechanism to transfer new software from a file source into the primary radio.



SETUP FILE TRANSFER FOR PRIMARY UNIT

Direction

This parameter sets the direction of file transfer. In this software version, the only choice is ‘To Primary Radio’.

Method

This parameter sets the method of file transfer.


Option	Function
Primary USB Transfer	Transfers the software from the USB flash drive to the primary radio.
FTP	Transfers the software from an FTP server to the primary radio.

PRIMARY FILE TRANSFER STATUS

See ‘Software > File Transfer’ on page 175 for parameter details.

To transfer software into the Aprisa FE 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 174), 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 246 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 246 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'.

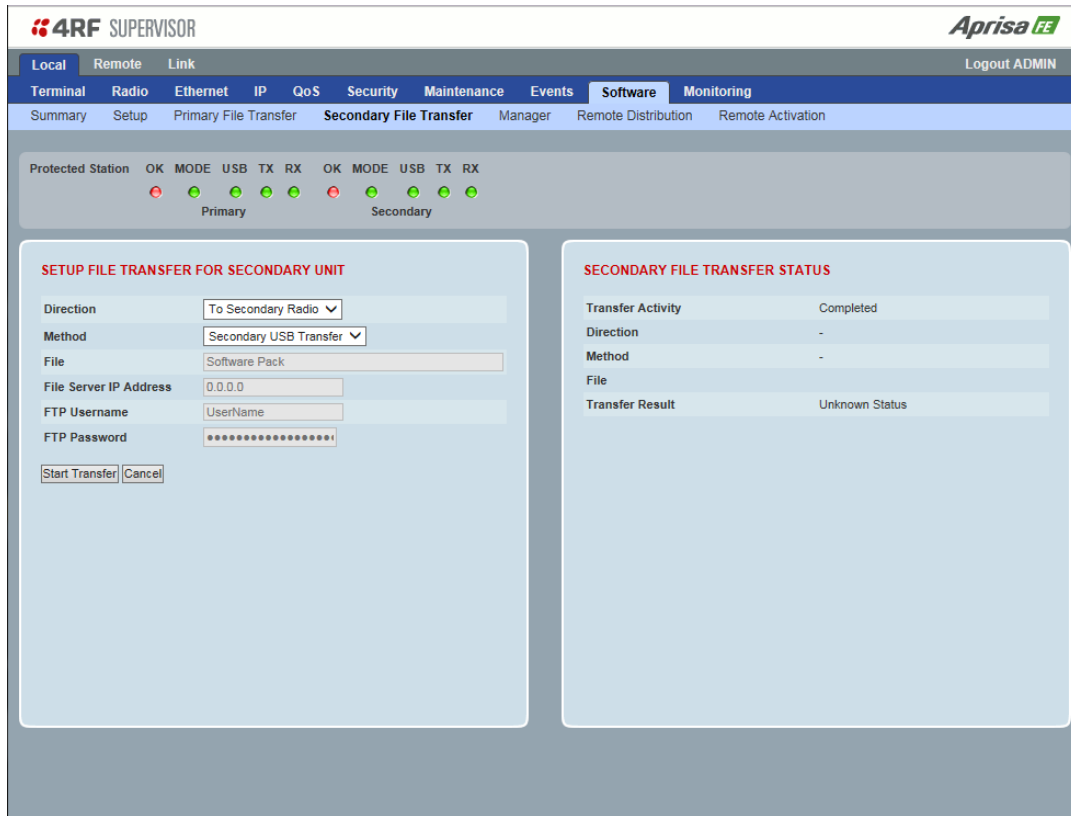
SECONDARY FILE TRANSFER STATUS	
Transfer Activity	In Progress
Direction	To This Radio
Method	Protected Partner Transfer
File	Software Pack
Transfer Result	Starting Transfer

3. Go to 'Protected Station: Software > Manager' on page 246 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 237) for more details of the transfer.

Protected Station: Software > Secondary File Transfer

This page provides the mechanism to transfer new software from a file source into the secondary radio.



SETUP FILE TRANSFER FOR SECONDARY UNIT

Direction

This parameter sets the direction of file transfer. In this software version, the only choice is 'To Secondary Radio'.

Method

This parameter sets the method of file transfer.


Option	Function
Secondary USB Transfer	Transfers the software from the USB flash drive to the secondary radio.
FTP	Transfers the software from an FTP server to the secondary radio.

SECONDARY FILE TRANSFER STATUS

See 'Software > File Transfer' on page 175 for parameter details.

To transfer software into the Aprisa FE 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 174), 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 246 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 246 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 246 to activate the Software Pack. The radio will reboot automatically.

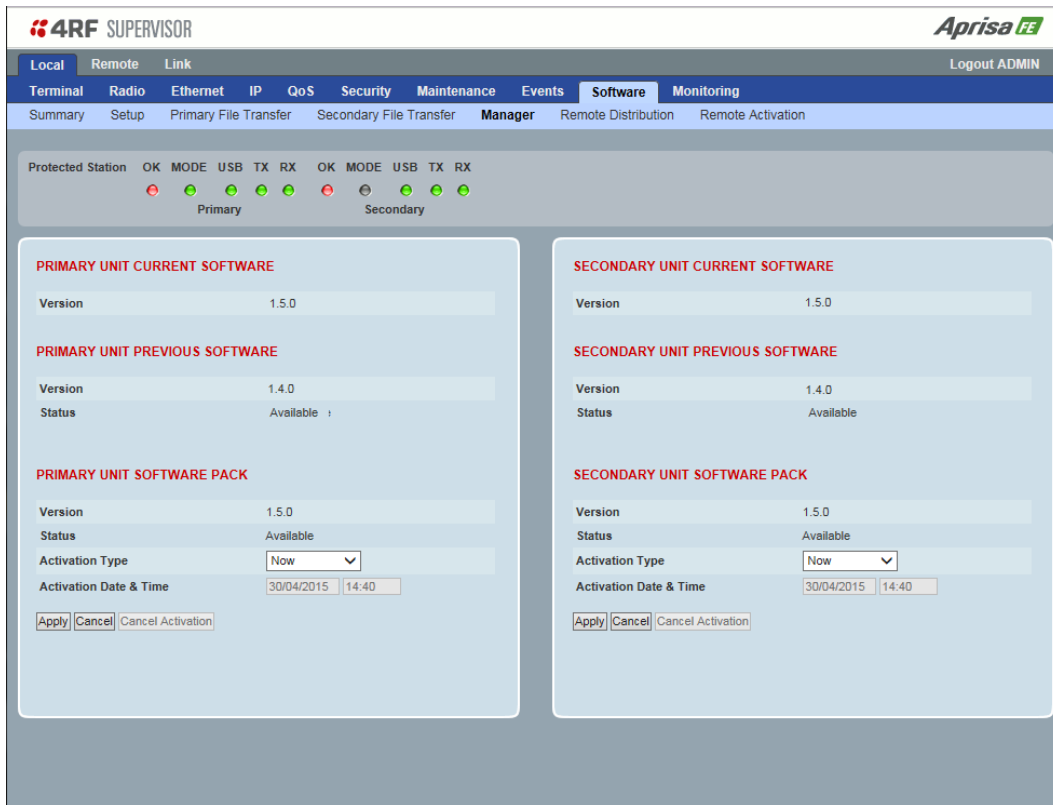
If the file transfer fails, check the Event History page (see 'Protected Station: Events > Primary History' on page 236) for more details of the transfer.

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 local radio and activate on all stations.

Status

This parameter displays the status of the software pack version.

Option	Function
Available	On the local radio, 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 178 for the activation options.

Protected Station: Software > Remote Distribution

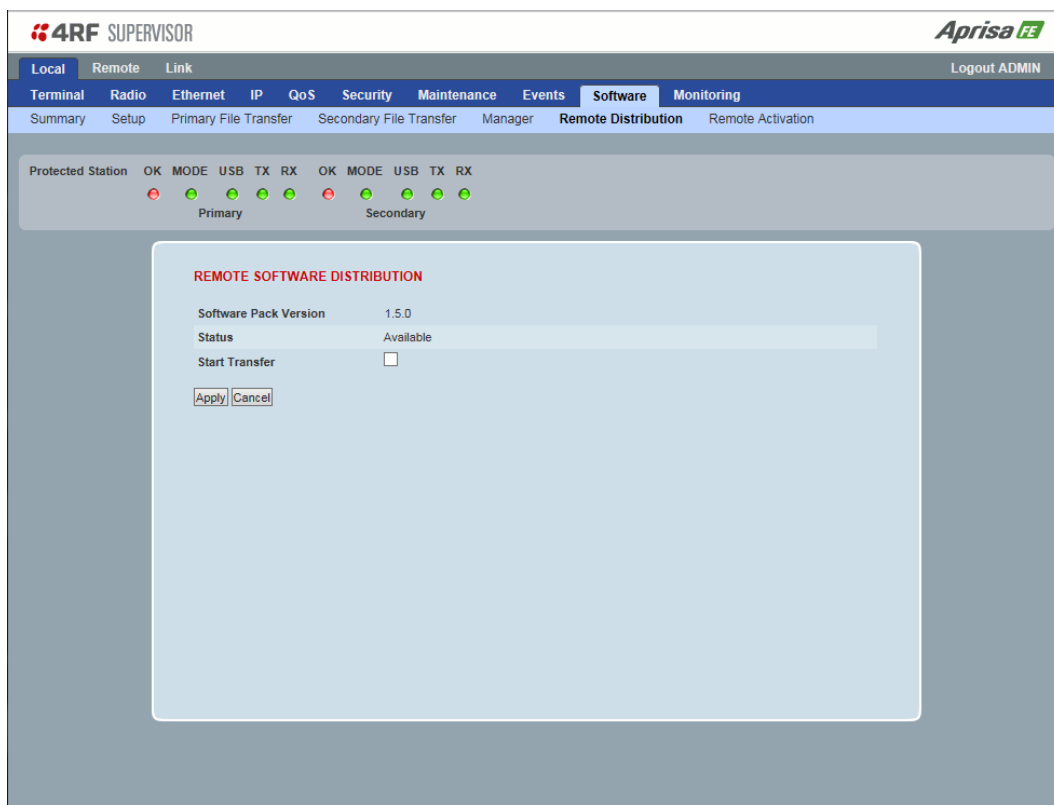
This page provides the mechanism to distribute software to all remote protected stations into the Aprisa FE network (network) and then activate it.

The Software Pack loaded into the local radio with the file transfer process (see ‘Protected Station: Software > Primary File Transfer’ on page 240) 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 Local radio.



REMOTE SOFTWARE DISTRIBUTION

Software Pack Version

This parameter displays the software pack version available for distribution on local radio 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.

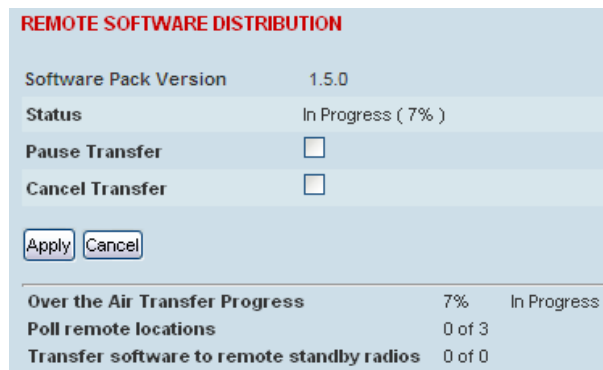
Note: The distribution of software to remote radios does not stop customer traffic from being transferred. However, due to the volume of traffic, the software distribution process may affect customer traffic.

Software distribution traffic is classified as ‘management traffic’ but does not use the Ethernet management priority setting. Software distribution traffic priority has a fixed priority setting of ‘very low’.

To distribute software to remote radios:

This process assumes that a Software Pack has been loaded into the local radio with the file transfer process (see ‘Protected Station: Software > Primary File Transfer’ on page 240).

1. To ensure that the Network Table is up to date, it is recommended running the node discover function (see ‘Discover Nodes’ on page 156).
2. Click on ‘Start Transfer’.



REMOTE SOFTWARE DISTRIBUTION	
Software Pack Version	1.5.0
Status	In Progress (7%)
Pause Transfer	<input type="checkbox"/>
Cancel Transfer	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="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 local radio.
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

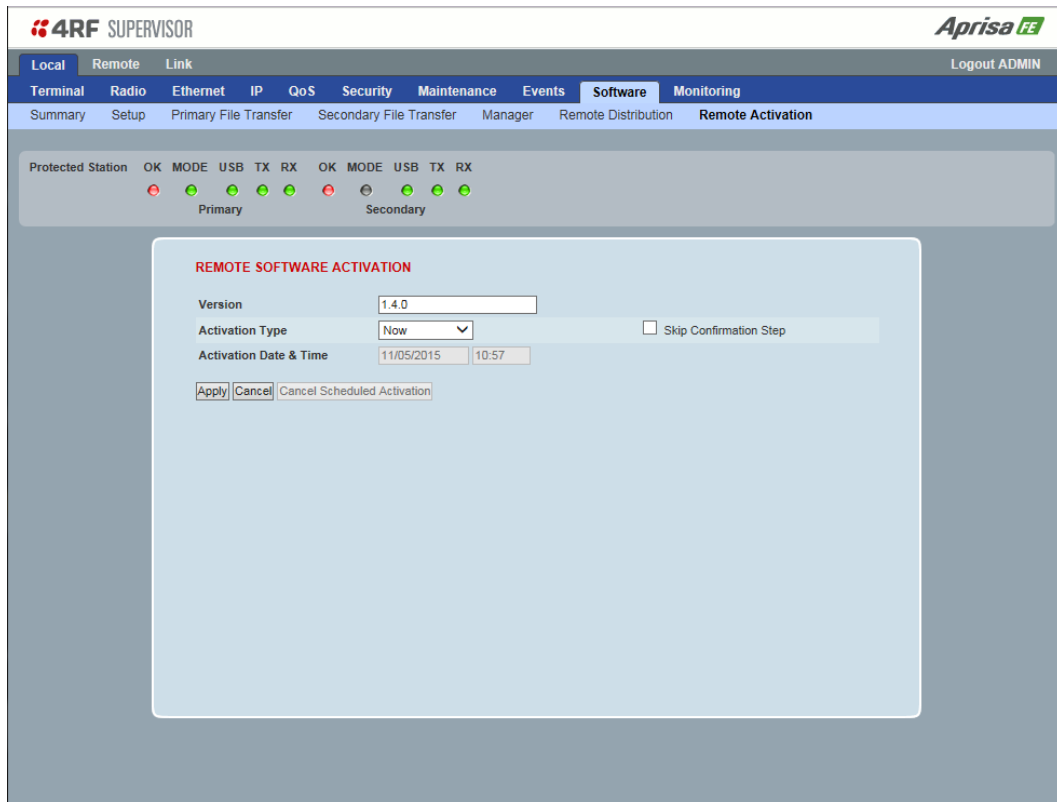
This page provides the mechanism to activate software on all remote protected stations.

The Software Pack has been loaded into the local radio with the file transfer process (see ‘Protected Station: Software > Primary File Transfer’ on page 240) 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 Local radio.



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 local radio 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 local radio with the file transfer process (see ‘Software > File Transfer’ on page 175) and that distributed to the remote radio.

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 178 for the activation options.

REMOTE SOFTWARE ACTIVATION

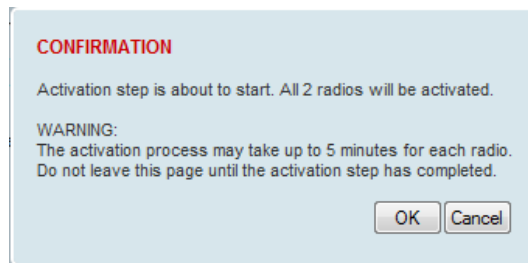
Version

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:

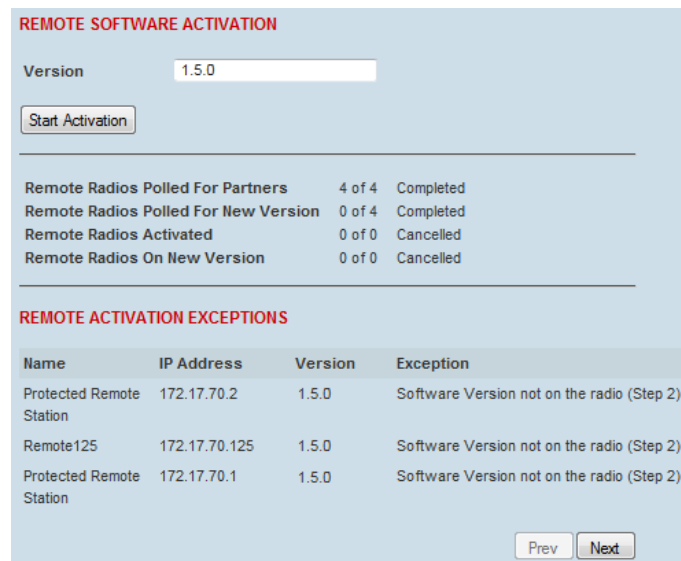
Result	Function (X of Y)
Remote Radios Polled for Partners	X is the number of radios polled to determine the number of protected stations in the network. Y is the number of remote radios registered with the local radio.
Remote Radios Polled for New Version	X is the number of radios polled to determine the number of radios that contain the new software version. Y is the number of remote radios registered with the local radio.
Remote Radios Activated	X is the number of radios that contain the new software version and have been activated. Y is the number of radios that contain the new software version and can be activated.
Remote Radios On New Version	X is the number of radios that has been successfully activated and now running the new version of software. Y is the number of radios that the activation command was executed on.

When the activation is ready to start:



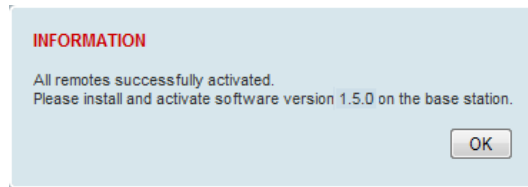
3. Click on 'OK' to start the activation process or Cancel to quit.

The page will display the progress of the activation.



The example shows that during the activation process there were exceptions that may need to be investigated.

When the remote radio has been activated, the local radio must now be activated with (see ‘Software > Manager’ on page 178).



4. Click on ‘OK’ to start the activation on the local radio.

Link

The Link tab enables display of settings and configuration of common changes to be made to both the local and remote radios simultaneously.

Protected Station: Link > Details > Summary

This page displays a summary of both the local and remote radio Terminal Summary and Operating Summary.

4RF SUPERVISOR Aprisa ^{FE}

Local Remote **Link** Logout ADMIN

Details Configuration Monitoring

Summary Radio Events

Protected Station OK MODE USB TX RX OK MODE USB TX RX
 Primary Secondary

Remote Radio OK MODE USB TX RX
 Status

TERMINAL SUMMARY

Terminal Name	Protected Station
Location	Wellington
Contact Name	4RF Limited
Contact Details	support@4rf.com
IP Address	172.10.1.30
Subnet Mask	255.255.0.0
Gateway	0.0.0.0
Date and Time	01/05/2015 18:41:47

PROTECTION INFORMATION

Protection Type	Redundant
Active Unit	Primary
Switch Count	9
Primary Address	172.10.1.30
Secondary Address	172.10.1.31

OPERATING SUMMARY

Operating Mode	Point To Point
Ethernet Mode	Bridge
Interface Mode	Ethernet Only
Modem Mode	Mode A (ETSI / ACMA)
TX Frequency (MHz)	400
TX Power (dBm)	32
RX Frequency (MHz)	406.25
Channel Size (kHz)	12.5
Network ID (FAN)	CAFE
Base Station ID	2
Node Address	0000
Inband Management	Enabled
Inband Management Timeout (s)	10

TERMINAL SUMMARY

Terminal Name	Remote Radio
Location	Wellington
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	01/01/2011 23:22:12

OPERATING SUMMARY

Operating Mode	Point To Point
Ethernet Mode	Bridge
Interface Mode	Ethernet Only
Modem Mode	Mode A (ETSI / ACMA)
TX Frequency (MHz)	406.25
TX Power (dBm)	32
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

TERMINAL SUMMARY

See 'Terminal > Device' for terminal settings.

OPERATING SUMMARY

See 'Terminal > Operating Mode' and 'Radio > Radio Setup' for operating mode and radio settings.

Protected Station: Link > Details > Radio

This page displays both the local and remote 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 with the 'Link' tab selected. The 'Radio' sub-tab is active, displaying diagnostic and performance monitoring parameters for two radio stations: a Protected Station and a Remote Radio.

Protected Station Status: OK (red), MODE (green), USB (green), TX (green), RX (green), OK (red), MODE (green), USB (green), TX (green), RX (green). Primary and Secondary status indicators are shown below.

Remote Radio Status: OK (green), MODE (green), USB (green), TX (green), RX (green). Status indicator is shown below.

Protected Station Parameters:

TX FREQUENCY	
TX Frequency (MHz)	400
TX Frequency Range (MHz)	400 to 470
TX Frequency Step Size (kHz)	6.25
TX POWER	
TX Power (dBm)	32
TX Power Range (dBm)	5 to 32
TX Power Step Size (dB)	1
RX FREQUENCY	
RX Frequency (MHz)	406.25
RX Frequency Range (MHz)	400 to 470
RX Frequency Step Size (kHz)	6.25
GENERAL	
Channel Size (kHz)	12.5
Modulation Type	64QAM (Low Gain)
Antenna Port Configuration	Single Antenna Dual Port (Duplexer)

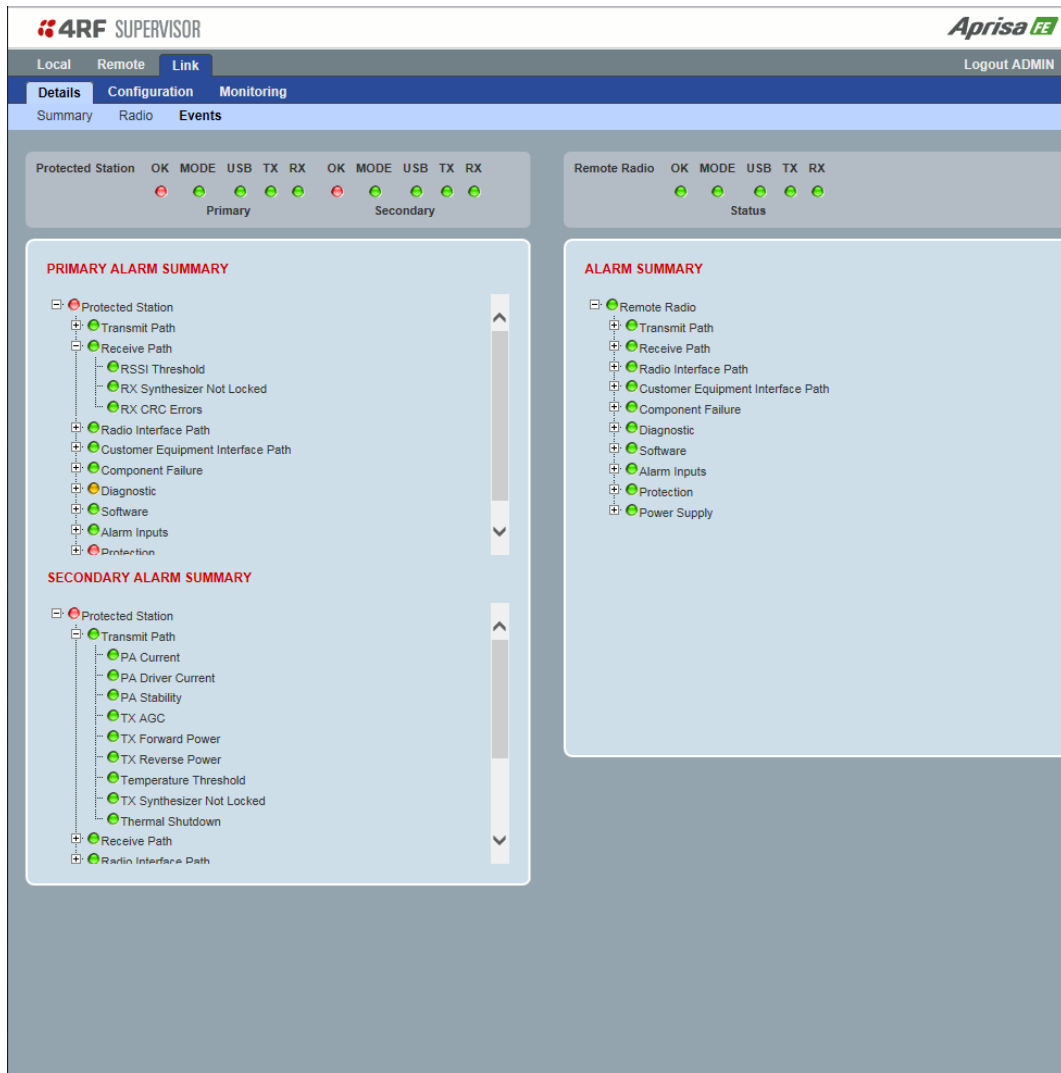
Remote Radio Parameters:

TX FREQUENCY	
TX Frequency (MHz)	406.25
TX Frequency Range (MHz)	400 to 470
TX Frequency Step Size (kHz)	6.25
TX POWER	
TX Power (dBm)	32
TX Power Range (dBm)	5 to 32
TX Power Step Size (dB)	1
RX FREQUENCY	
RX Frequency (MHz)	400
RX Frequency Range (MHz)	400 to 470
RX Frequency Step Size (kHz)	6.25
GENERAL	
Channel Size (kHz)	12.5
Modulation Type	64QAM (Low Gain)
Antenna Port Configuration	Single Antenna Dual Port (Duplexer)

See 'Radio > Radio Setup' for radio settings.

Protected Station: Link > Details > Events

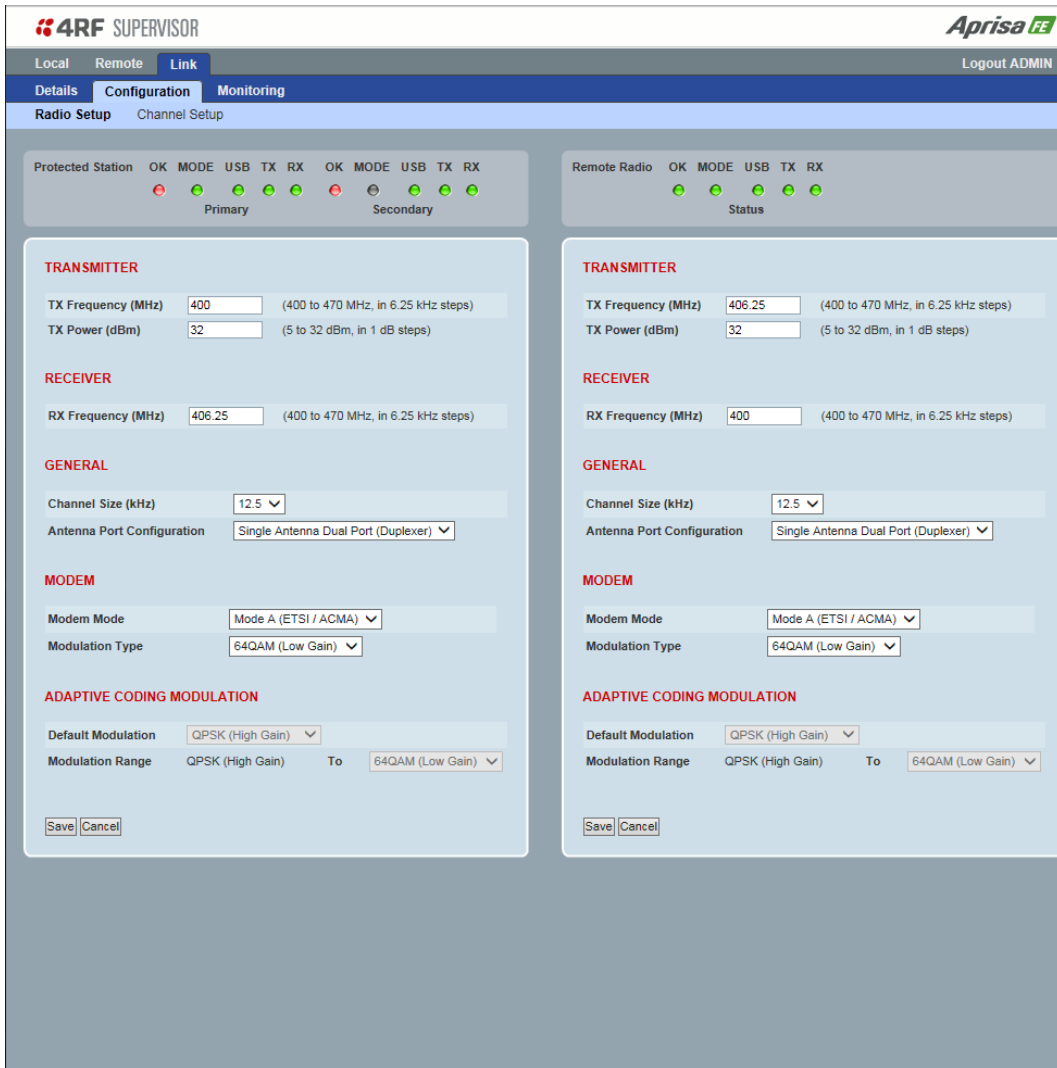
This page displays the current alarm events of both the local and remote radios.



See 'Events > Events Setup' for alarm event setup.

Protected Station: Link > Configuration > Radio Setup

This page enables the configuration of common radio parameters to be made to both the Local and Remote radios simultaneously.



4RF SUPERVISOR **Aprisa FE**

Local Remote **Link** Logout ADMIN

Details **Configuration** Monitoring

Radio Setup Channel Setup

Protected Station **OK** **MODE** **USB** **TX** **RX** **OK** **MODE** **USB** **TX** **RX**

Primary Secondary

Remote Radio **OK** **MODE** **USB** **TX** **RX**

Status

TRANSMITTER

TX Frequency (MHz) 400 (400 to 470 MHz, in 6.25 kHz steps)

TX Power (dBm) 32 (5 to 32 dBm, in 1 dB steps)

RECEIVER

RX Frequency (MHz) 406.25 (400 to 470 MHz, in 6.25 kHz steps)

GENERAL

Channel Size (kHz) 12.5

Antenna Port Configuration Single Antenna Dual Port (Duplexer)

MODEM

Modem Mode Mode A (ETSI / ACMA)

Modulation Type 64QAM (Low Gain)

ADAPTIVE CODING MODULATION

Default Modulation QPSK (High Gain)

Modulation Range QPSK (High Gain) To 64QAM (Low Gain)

Save Cancel

TRANSMITTER

TX Frequency (MHz) 406.25 (400 to 470 MHz, in 6.25 kHz steps)

TX Power (dBm) 32 (5 to 32 dBm, in 1 dB steps)

RECEIVER

RX Frequency (MHz) 400 (400 to 470 MHz, in 6.25 kHz steps)

GENERAL

Channel Size (kHz) 12.5

Antenna Port Configuration Single Antenna Dual Port (Duplexer)

MODEM

Modem Mode Mode A (ETSI / ACMA)

Modulation Type 64QAM (Low Gain)

ADAPTIVE CODING MODULATION

Default Modulation QPSK (High Gain)

Modulation Range QPSK (High Gain) To 64QAM (Low Gain)

Save Cancel

Parameters critical to the operation of the link e.g. TX and RX frequencies are automatically copied to the other radio in the link i.e. critical parameters entered on the local radio are automatically copied to the remote radio and vice versa.

See 'Radio > Radio Setup' for radio settings.

Protected Station: Link > Configuration > Channel Setup

This page enables the configuration of common channel and traffic parameters to be made to both the Local and Remote radios simultaneously.

The screenshot displays the 4RF SUPERVISOR interface for configuring channel settings. The top navigation bar includes 'Local', 'Remote', and 'Link' tabs, with 'Link' selected. Below this are 'Details', 'Configuration', and 'Monitoring' tabs, with 'Configuration' selected. The main content area is titled 'Radio Setup' and 'Channel Setup'. It features two columns of settings for 'Protected Station' and 'Remote Radio'. Each column includes status indicators (OK, MODE, USB, TX, RX) and three configuration sections: CHANNEL SETTINGS, TRAFFIC SETTINGS, and DATA COMPRESSION. The Protected Station section has sub-sections for Primary and Secondary stations. The Remote Radio section has a Status sub-section. Each setting is accompanied by a 'Save' and 'Cancel' button.

See 'Radio > Channel Setup' for radio channel settings.

Protected Station: Link > Monitoring > Terminal

This page displays both the local and remote radio current internal and external input source radio power supply voltage diagnostic parameters.

The results shown are since the page was opened and are updated automatically every 12 seconds.

The screenshot shows the 4RF SUPERVISOR interface with the 'Link' tab selected. The 'Monitoring' section is active, showing 'Terminal' selected. The interface displays status indicators for Protected Station and Remote Radio, along with two tables of power supply parameters.

Protected Station Status:

- OK: [Red X]
- MODE: [Green]
- USB: [Green]
- TX: [Green]
- RX: [Green]
- OK: [Red X]
- MODE: [Green]
- USB: [Green]
- TX: [Green]
- RX: [Green]

Remote Radio Status:

- OK: [Green]
- MODE: [Green]
- USB: [Green]
- TX: [Green]
- RX: [Green]

Protected Station POWER SUPPLY PARAMETERS:

	Primary	Secondary	User
Current VDC Power Supply	24.176 V	24.049 V	<input type="checkbox"/>
Current 3.3V Power Supply	3.341 V	3.319 V	<input type="checkbox"/>
Current 5.0V Power Supply	5.322 V	5.276 V	<input type="checkbox"/>
Current 15.0V Power Supply	15.014 V	14.910 V	<input type="checkbox"/>

Remote Radio POWER SUPPLY PARAMETERS:

		User
Current VDC Power Supply	24.186 V	<input type="checkbox"/>
Current 3.3V Power Supply	3.321 V	<input type="checkbox"/>
Current 5.0V Power Supply	5.285 V	<input type="checkbox"/>
Current 15.0V Power Supply	14.795 V	<input type="checkbox"/>

See 'Monitoring > Terminal' for parameters setup.

Protected Station: Link > Monitoring > Ethernet

This page displays both the local and remote radio current performance monitoring parameters per Ethernet port transmission (TX) 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.

The screenshot shows the 4RF SUPERVISOR interface with the 'Link' tab selected. The 'Monitoring' sub-tab is active, displaying Ethernet statistics for both Primary and Secondary ports of the Protected Station and the Remote Radio. The interface includes status indicators for OK, MODE, USB, TX, and RX for both radio types. The Protected Station shows active TX activity, while the Remote Radio shows no activity.

Protected Station		Remote Radio	
Primary	Secondary	Primary	Secondary
Maximum Capacity	100 Mbps	10 Mbps	10 Mbps
Packets	90	0	0
Bytes	54,337	0	0
Packet Collisions	0	0	0
VLAN Frames	0	0	0
ETHERNET PORT 1 RECEIVE		ETHERNET PORT 1 RECEIVE	
Packets	91	0	0
Bytes	28,485	0	0
Packets equal to 64 Bytes	53	0	0
Packets 65 to 127 Bytes	0	0	0
Packets 128 to 255 Bytes	0	0	0
Packets 256 to 511 Bytes	0	0	0
Packets 512 to 1023 Bytes	38	0	0
Packets 1024 to 1536 Bytes	0	0	0
Broadcast Packets	0	0	0
Multicast Packets	0	0	0
VLAN Frames	0	0	0
VLAN Frames dropped	0	0	0
Packet in Error	0	0	0
Bytes in Error	0	0	0
CRC/Alignment Errors	0	0	0
Undersized Packets	0	0	0
Oversized Packets	0	0	0
Fragmented Packets	0	0	0
Jabber Packets	0	0	0

See 'Monitoring > Ethernet' on page 189 for parameters setup.

Protected Station: Link > Monitoring > Radio

This page displays both the local and remote radio 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 with the 'Monitoring' tab selected. It displays two columns of data for 'Local Radio' and 'Remote Radio'. Each column includes status indicators (OK, MODE, USB, TX, RX) and detailed transmitter and receiver statistics. The 'Local Radio' data is as follows:

TRANSMITTER		User
Current Temperature	35.6 C	<input type="checkbox"/>
Packets Transmitted	15	<input type="checkbox"/>
Bytes Transmitted	1,723	<input type="checkbox"/>
Dropped Packets (Congestion)	0	<input type="checkbox"/>
Dropped Bytes (Congestion)	0	<input type="checkbox"/>
Last Tx PA Current	1,135 mA	<input type="checkbox"/>
Last Tx PA Driver Current	96 mA	<input checked="" type="checkbox"/>
Last Tx Forward Power	32.0 dBm	<input type="checkbox"/>
<input type="button" value="Reset"/>		

The 'Remote Radio' data is as follows:

TRANSMITTER		User
Current Temperature	34.3 C	<input type="checkbox"/>
Packets Transmitted	15	<input type="checkbox"/>
Bytes Transmitted	1,874	<input type="checkbox"/>
Dropped Packets (Congestion)	0	<input type="checkbox"/>
Dropped Bytes (Congestion)	0	<input type="checkbox"/>
Last Tx PA Current	907 mA	<input checked="" type="checkbox"/>
Last Tx PA Driver Current	35 mA	<input type="checkbox"/>
Last Tx Forward Power	34.0 dBm	<input type="checkbox"/>
<input type="button" value="Reset"/>		

Receiver and Transmit Path data for both radios are also visible, showing metrics like Packets Received, Bytes Received, and Remote Name.

See 'Monitoring > Radio' on page 194 for parameters setup.

Protected Station: Link > Monitoring > User Selected

This page displays the 'User' parameters setup in all the other Monitoring screens for both the local and remote radios.

The results shown are since the page was opened and are updated automatically every 12 seconds.

The screenshot displays the 4RF SUPERVISOR interface with the 'Link' tab selected. The 'Monitoring' sub-tab is active, showing 'User Selected' for the radio type. The interface is divided into two main columns for 'Local Radio' and 'Remote Radio', each with status indicators and detailed monitoring data.

Local Radio Status: OK, MODE, USB, TX, RX (all green)

Remote Radio Status: OK, MODE, USB, TX, RX (all green)

Local Radio Monitoring Data:

TERMINAL DETAILS		User
RF Transmitter		User
Last Tx PA Driver Current	94 mA	<input checked="" type="checkbox"/>
RF Receiver		User
Dropped Packets (Filtering)	0	<input checked="" type="checkbox"/>
Dropped Bytes (Filtering)	0	<input checked="" type="checkbox"/>
<input type="button" value="Reset All"/>		
RF LINK PARAMETERS		User
Transmit Path		User
Remote Name	Remote Radio	<input checked="" type="checkbox"/>
Modulation	64QAM Lo	
Timestamp	02/01/2011 01:51:57	
Receive Path		User
Remote Name	Remote Radio	<input checked="" type="checkbox"/>
RSSI	-48.7 dBm	
SNR	37.0 dB	
Frequency Error	-20 Hz	
Modulation	64QAM Lo	
Timestamp	02/01/2011 01:51:57	


Remote Radio Monitoring Data:

TERMINAL DETAILS		User
RF Transmitter		User
Last Tx PA Current	910 mA	<input checked="" type="checkbox"/>
RF Receiver		User
Dropped Packets (Filtering)	0	<input checked="" type="checkbox"/>
Dropped Bytes (Filtering)	0	<input checked="" type="checkbox"/>
<input type="button" value="Reset All"/>		
RF LINK PARAMETERS		User
Receive Path		User
Remote Name	Local Radio	<input checked="" type="checkbox"/>
RSSI	-47.5 dBm	
SNR	39.3 dB	
Frequency Error	82 Hz	
Modulation	64QAM Lo	
Timestamp	01/01/2011 22:38:42	

Command Line Interface

The Aprisa FE has a Command Line Interface (CLI) which provides basic product setup and configuration. This can be useful if you need to confirm the radio's IP address, for example.

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

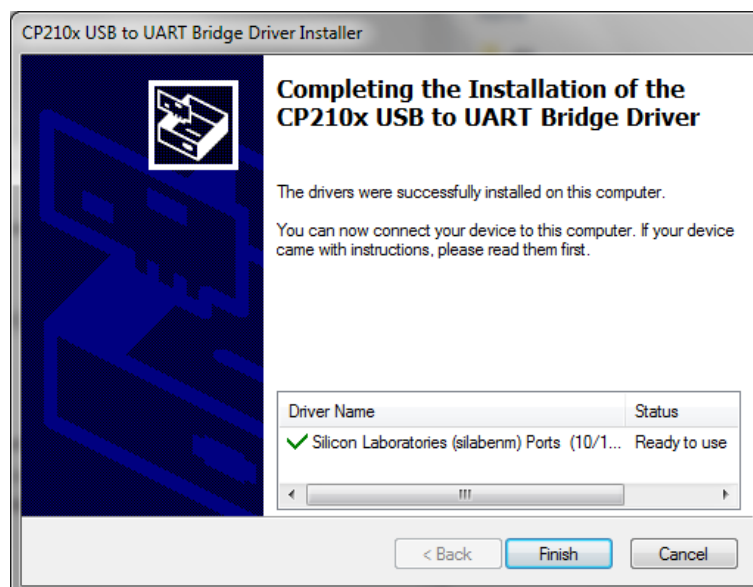
This interface can be accessed via an Ethernet Port (RJ45), the Management Port (USB micro type B) or the USB host port  with a USB converter to RS-232 convertor.

Connecting to the Management Port

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

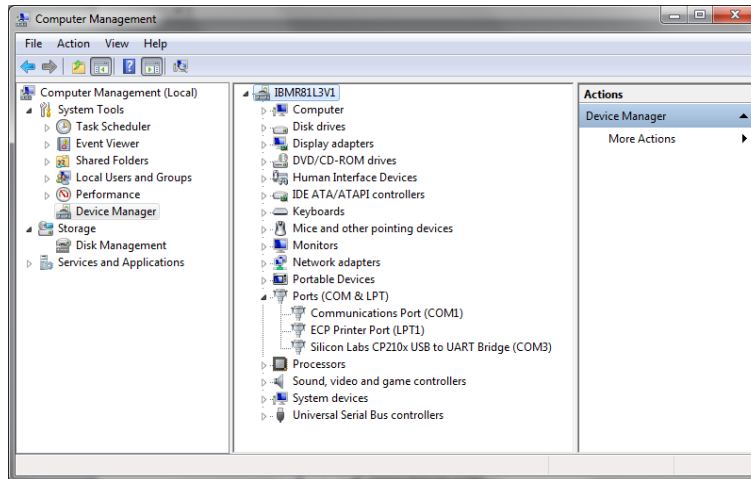


1. Connect the USB A to your computer USB port and the USB micro B to the management port of the Aprisa FE (MGMT).
2. Unzip and install the USB Serial Driver CP210x_VCP_Windows.zip on your computer. This file is on the Information and setup CD supplied with the radio.



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

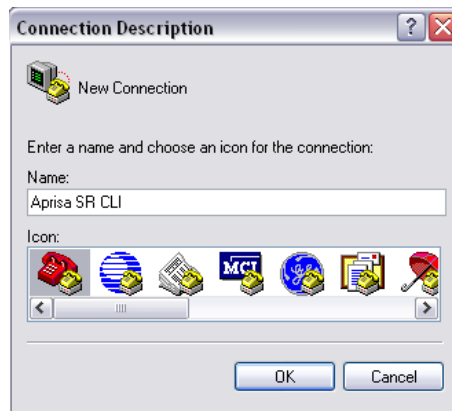
5. Make a note of the COM port which has been allocated to the 'Silicon Labs CP210x USB to UART Bridge' (COM3 in the example below)



6. Open HyperTerminal or an alternative type of terminal Emulator program e.g. TeraTerm or Putty.

HyperTerminal Example

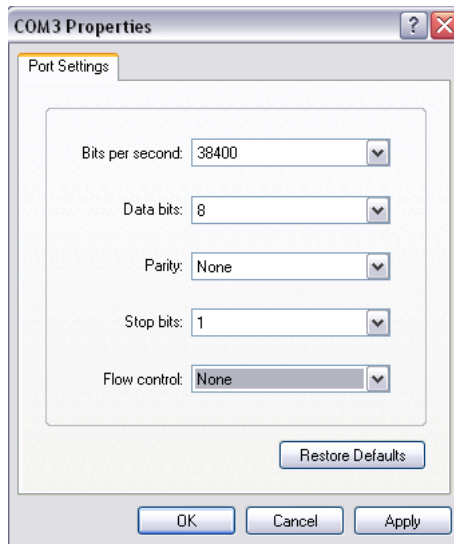
7. Enter a name for the connection (Aprisa FE CLI for example) and click OK.



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



9. Set the COM port settings as follows:



10. Click OK. The HyperTerminal window will open.

11. Press the Enter key to initiate the session.

12. Login to the Aprisa FE CLI with a default Username 'admin' and Password 'admin'.

The Aprisa MIB menu is shown:

```
Login: admin
Password: *****
CLI user admin last login: 2011/01/01 22:29:34 from 127.0.0.1
>>?
adduser      browser      cd            clear        config
debug        deleteuser  editpasswd   edituser     get
list         logout      ls            nodelqi     pwd
reboot       rohc        set           who
>>
>>
```


CLI Commands

To enter a CLI command:

1. Type the first few characters of the command and hit Tab. This auto completes the command.
2. Enter the command string and enter.

Note: All CLI commands are case sensitive.

The top level CLI command list is displayed by typing a ? at the command prompt.

The following is a list of the top level CLI commands and their usage:

CLI Command	Usage
adduser	adduser [-g <password aging>] [-a <account aging>] [-i <role>] <userName> <userPassword>
browser	browser <state(STR)>
cd	cd <changeMode(STR)>
clear	Clears the screen
config	config userdefault save restore factorydefault restore
debug	set subsystem param(INT) level param(INT) get clear subsystem param(INT) level param(INT) help log dump clear
deleteuser	deleteuser <userName>
editpasswd	editpasswd <oldpassword> <newpassword>
edituser	edituser [-p <password>] [-g <password aging>] [-a <account aging>] [-i]
get	get [-m <mib name>] [-n <module name>] <attribute name> [indexes]
list	list <tablename>
logout	Logs out from the CLI
ls	Displays the next level menu items
pwd	Displays the current working directory
reboot	Reboots the radio
rohc	stats show clear
set	set [-m <mib name>] [-n <module name>] <attribute name> <attribute set v>
who	Shows the users currently logged into the radio

Viewing the CLI Terminal Summary

At the command prompt, type:

```
cd APRISASR-MIB-4RF
```

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

```
>>cd APRISASR-MIB-4RF
MPA APRISASR-MIB-4RF >>ls Terminal
```

S.NO	ATTRIBUTE NAME	ATTRIBUTE VALUE
1	termName	Base Station
2	termLocation	Wellington
3	termContactName	4RF Limited
4	termContactDetails	support@4rf.com
5	termTimeFormat	time24h (1)
6	termDateFormat	ddmmyyyy (1)
7	termDateTime	2013-9-12,19:22:43.0
8	termEthController1IpAddress	173.10.10.1
9	termEthController1SubnetMask	255.255.0.0
10	termEthController1Gateway	0.0.0.0
11	termRfNwkPanId	CAFE
12	termRfNwkRadius	1
13	termInbandManagementEnabled	true (1)
14	termInbandManagementTimeoutSec	10
15	termRfNwkRepeaterProximity	noRepeater (0)

Changing the Radio IP Address with the CLI

At the command prompt, type 'set termEthController1IpAddress xxx.xxx.xxx.xxx'

```
1 | termName | Base Station
2 | termLocation | Wellington
3 | termContactName | 4RF Limited
4 | termContactDetails | support@4rf.com
5 | termTimeFormat | time24h (1)
6 | termDateFormat | ddmmyyyy (1)
7 | termDateTime | 2013-9-12,19:25:19.0
8 | termEthController1IpAddress | 173.10.10.1
9 | termEthController1SubnetMask | 255.255.0.0
10 | termEthController1Gateway | 0.0.0.0
11 | termRfNwkPanId | CAFE
12 | termRfNwkRadius | 1
13 | termInbandManagementEnabled | true (1)
14 | termInbandManagementTimeoutSec | 10
15 | termRfNwkRepeaterProximity | noRepeater (0)
```

```
MPA APRISASR-MIB-4RF >>set termEthController1IpAddress 173.10.10.1
termEthController1IpAddress = 173.10.10.1
MPA APRISASR-MIB-4RF >>
```

Connected 0:06:07 ANSIW 38400 8-N-1 SCROLL CAPS NUM Capture Print echo

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 link 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 local 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

Local and remote radio yagi antennas must have the same polarization.

Aligning the Antennas

Align the local and remote radio yagi antennas by making small adjustments while monitoring the RSSI. The Aprisa FE 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 34).

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 RSSI button on the radio front 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 link 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 150).

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 RSSI button until all the LEDs flash red (about 3 - 5 seconds).

7. Product Options

Chassis Options

300 mm Chassis Depth - Internal Duplexer



The standard Aprisa FE chassis has a depth of 300 mm and can accommodate some duplexer types.

The following products are supplied in a 300 mm depth chassis with the duplexer mounted internally:

Part Number	Frequency Band	Internal Duplexer
APFE-N896-SSC-G2-30-ENAA	896-902 MHz	Minimum split 9.0 MHz Passband 1.0 MHz
APFE-N928-SSC-G2-30-ENAA	928-960 MHz	Minimum split 9.0 MHz Passband 1.0 MHz

300 mm Chassis Depth - External Duplexer



The following products are supplied in a 300 mm depth chassis but with the duplexer mounted externally:

Part Number	Frequency Band	External Duplexer
APFE-N135-SSC-N0-30-ENAA	135-175 MHz	Minimum split 4.6 MHz Passband 0.5 MHz
APFE-N320-SSC-A1-30-ENAA	320-400 MHz	Minimum split 5.0 MHz Passband 0.5 MHz
APFE-N400-SSC-B1-30-ENAA	400-470 MHz	Minimum split 5.0 MHz Passband 0.5 MHz
APFE-N450-SSC-M0-30-ENAA	450-520 MHz	Minimum split 5.0 MHz Passband 0.5 MHz

440 mm Chassis Depth - Internal Duplexer Only



The full depth Aprisa FE chassis has a depth of 440 mm and can accommodate some duplexer types.

The following products are supplied in a 440 mm depth chassis with the duplexer mounted internally:

Part Number	Frequency Band	Internal Duplexer
APFE-N320-SSC-A1-44-ENAA	320-400 MHz	Minimum split 5.0 MHz Passband 0.5 MHz
APFE-N400-SSC-B1-44-ENAA	400-470 MHz	Minimum split 5.0 MHz Passband 0.5 MHz

Protected Station

The Aprisa FE Protected Station is fully monitored hot-standby and fully hot-swappable product providing radio and user interface protection for Aprisa FE radios. The RF ports and interface ports from the active radio are switched to the standby radio if there is a failure in the active radio.



Option Example

Part Number	Part Description
APFE-R400-SSC-B1-40-ENAA	4RF FE, PS, 400-470 MHz, SSC, B1, 4E0S, EN, STD

The Aprisa FE Protected Station is comprised of an Aprisa FE Protection Switch and two standard Aprisa FE point-to-point full duplex 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 FE Protected Station can operate as a local or remote radio.

The protection behaviour and switching criteria between the active and standby radios is identical for the two configurations.

Each radio is configured with its own unique IP and MAC address and the address of the partner radio.

On power-up, the primary radio will assume the active role and the secondary radio will assume the standby role. If, for some reason, only one radio is powered on it will automatically assume the active role.

Protected Ports

The protected ports are located on the protected station front panel. Switching occurs between the active radio ports and the standby radio ports based on the switching criteria described below.

The protected ports include:

- Antenna ports ANT/TX and RX
- Ethernet ports

Operation

In hot-standby normal operation, the active radio carries all Ethernet traffic over the radio link and the standby radio transmit is on with its transmitter connected to an internal load. Both radios are continually monitored for correct operation including the transmitter and receiver and alarms are raised if an event occurs.

The active radio sends regular 'keep alive' messages to the standby radio to indicate it is operating correctly. In the event of a failure on the active radio, the RF link and user interface traffic is automatically switched to the standby radio.

The failed radio can then be replaced in the field without interrupting user traffic.

Switch Over

The switch over to the standby radio can be initiated automatically, on fault detection, or manually via the Hardware Manual Lock switch on the Protection Switch or the Software Manual Lock from SuperVisor.

Additionally, it is possible to switch over the radios remotely without visiting the station site, via the remote control connector on the front of the Protection Switch.

On detection of an alarm fault the switch over time is less than 0.5 seconds. Some alarms may take up to 30 seconds to be detected depending on the configuration options selected.

The Protection Switch has a switch guard mechanism to prevent protection switch oscillation. If a switch-over has occurred, subsequent switch-over triggers will be blocked if the guard time has not elapsed.

The guard time starts at 20 seconds and doubles each switch-over to a maximum of 320 seconds and halves after a period of two times the last guard time with no protection switch-overs.

Switching Criteria

The Protected Station will switch over operation from the active to the standby radio if any of the configurable alarm events occur, or if there is a loss of the ‘keep alive’ signal from the active radio.

It is possible to configure the alarm events which will trigger the switch over. It is also possible to prevent an alarm event triggering a switch over through the configuration of blocking criteria.

Any of the following alarm events can be set to trigger or prevent switching from the active radio to the standby radio (see ‘Events > Events Setup’ on page 161).

PA current	Alarm Input 2
Tx reverse power	Tx AGC
Temperature threshold	Thermal shutdown
RSSI Threshold	RX Synthesizer Not Locked
Rx CRC errors	RF no receive data
Port1 Eth no receive data	Port2 Eth no receive data
Port1 Eth data receive errors	Port2 Eth data receive errors
Port1 Eth data transmit errors	Port2 Eth data transmit errors
Port3 Eth no receive data	Port4 Eth no receive data
Port3 Eth data receive errors	Port4 Eth data receive errors
Port3 Eth data transmit errors	Port4 Eth data transmit errors
Component failure	Calibration failure
Configuration not supported	Protection Hardware Failure
Alarm Input 1	

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	
			Monitored on Standby Radio TX	Monitored on Standby Radio RX
Alarm Type	Monitored on Active Radio	Monitored on Standby Radio	Monitored on Standby Radio TX	Monitored on Standby Radio RX
PA Current	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
PA Driver Current	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
PA Stability	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
TX AGC	<input checked="" type="checkbox"/>			
TX Forward Power	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
TX Reverse Power	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
Temperature Threshold	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TX Synthesizer Not Locked	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
Thermal Shutdown	<input checked="" type="checkbox"/>			
RSSI Threshold	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
RX Synthesizer Not Locked	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
RX CRC Errors	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
RF No Receive Data	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Port1 ETH No Receive Data	<input checked="" type="checkbox"/>			
Port1 ETH Data Receive Errors	<input checked="" type="checkbox"/>			
Port1 ETH Data Transmit Errors	<input checked="" type="checkbox"/>			
Port2 ETH No Receive Data	<input checked="" type="checkbox"/>			
Port2 ETH Data Receive Errors	<input checked="" type="checkbox"/>			
Port2 ETH Data Transmit Errors	<input checked="" type="checkbox"/>			
Port3 ETH No Receive Data	<input checked="" type="checkbox"/>			
Port3 ETH Data Receive Errors	<input checked="" type="checkbox"/>			
Port3 ETH Data Transmit Errors	<input checked="" type="checkbox"/>			
Port4 ETH No Receive Data	<input checked="" type="checkbox"/>			
Port4 ETH Data Receive Errors	<input checked="" type="checkbox"/>			
Port4 ETH Data Transmit Errors	<input checked="" type="checkbox"/>			
Component Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Protection SW Manual Lock	<input checked="" type="checkbox"/>			
Protection HW Manual Lock	<input checked="" type="checkbox"/>			
Modem FEC Disable	<input checked="" type="checkbox"/>			
Modem ACM Lock	<input checked="" type="checkbox"/>			
Alarm Input 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Alarm Input 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Protection Peer Comms Lost	<input checked="" type="checkbox"/>			
Protection Hardware Failure	<input checked="" type="checkbox"/>			
VDC Power Supply	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Protection Type	All Protection Types	Redundant	Monitored Hot Standby	
			Monitored on Standby Radio TX	Monitored on Standby Radio RX
Alarm Type	Monitored on Active Radio	Monitored on Standby Radio	Monitored on Standby Radio TX	Monitored on Standby Radio RX
3.3 Volts Power Supply	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.0 Volts Power Supply	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.2 Volts Power Supply	<input checked="" type="checkbox"/>			
15.0 Volts Power Supply	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

Hardware Manual Lock

The Hardware Manual Lock switch on the Protection Switch provides a manual override of the active / standby radio.

When this lock is activated, the selected radio (A or B) becomes the active radio regardless of the Software Manual Lock and the current switching or block criteria.

When the lock is deactivated (set to the Auto position), the protection will become automatic and switching will be governed by normal switching and blocking criteria.

The state of the switch is indicated by the three LEDs on the Protection Switch:

A LED	B LED	Locked LED	State
Green	Off	Off	Auto - Radio A is active
Off	Green	Off	Auto - Radio B is active
Green	Off	Orange	Manual Lock to radio A
Off	Green	Orange	Manual Lock to radio B

The Protection Switch also has a Software Manual Lock. The Hardware Manual Lock takes precedence over Software Manual Lock if both diagnostic functions are activated i.e. if the Software Manual Lock is set to 'Primary' and the Hardware Manual Lock set to 'Secondary', the system will set the Secondary radio to Active.

When a Hardware Manual Lock is deactivated (set to the Auto position), the Software Manual Lock is re-evaluated and locks set appropriately.

Remote Control

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

L2 / L3 Protection Operation

The Aprisa FE 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 failure switchover the new active radio sends out a gratuitous ARP to update MAC learning tables / ARP tables of upstream bridge/router for appropriate traffic flow.

Hot-Swappable

The two Aprisa FE radios are mounted on a pull-out tray to making it possible to replace a failed radio without interrupting user traffic.



Antenna and Duplexer Options

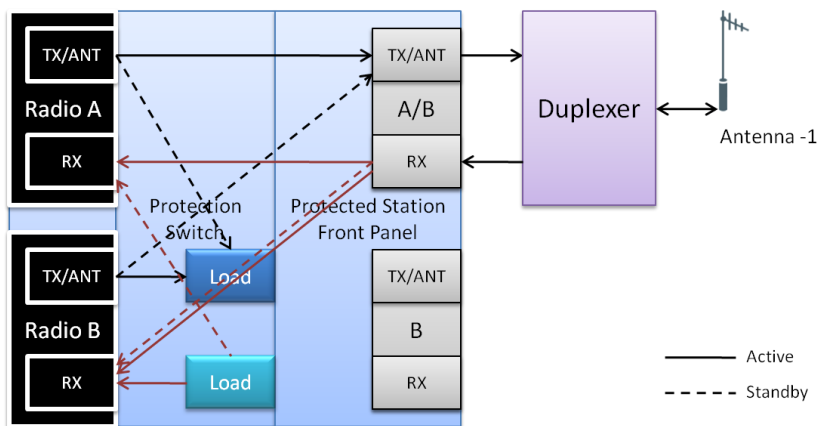
Option 2 - single antenna with a single duplexer

In this configuration, a single antenna is used with a duplexer which is connected to the Aprisa FE Protected Station TX/ANT and RX (A/B side) TNC ports on the front panel. In this option, the Protected Station can operate in:

- 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.



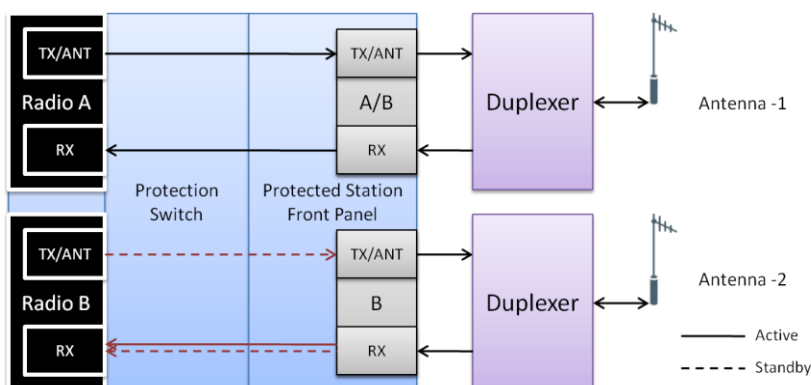
Option 2 - dual antenna with dual duplexers

In this configuration, antenna redundancy is supported with dual antennas connected via dual duplexers to the Aprisa FE 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:

- 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.



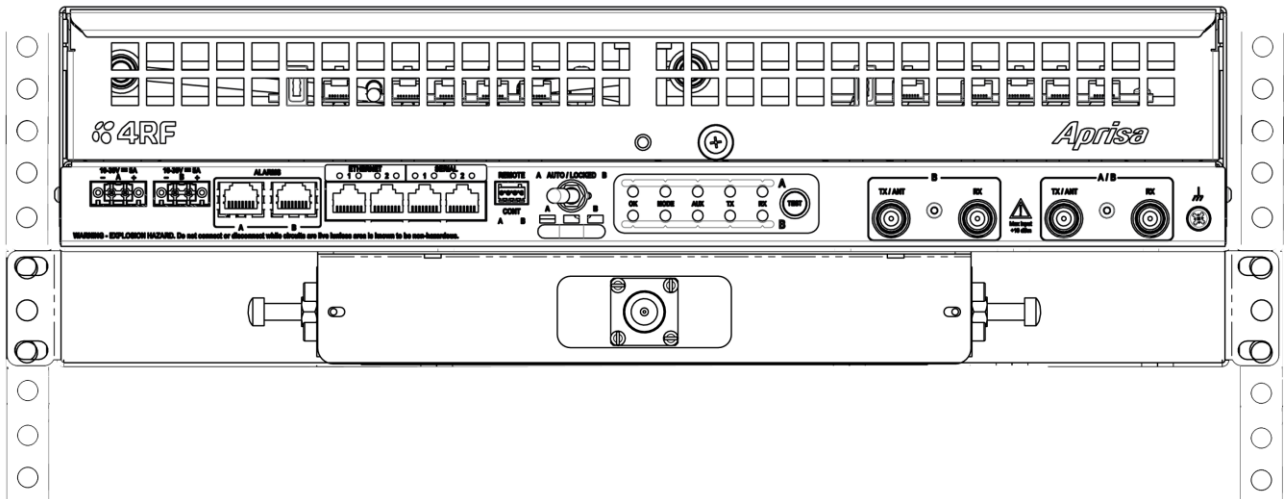
Installation

Mounting

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

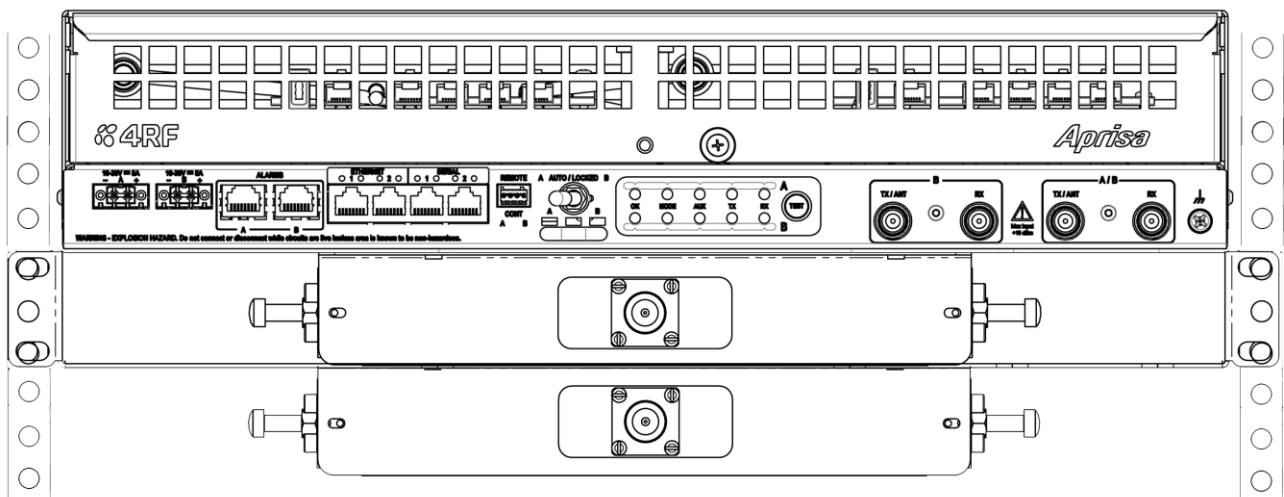
Single Antenna Operation

The single antenna option requires one duplexer;



Dual Antenna Operation

The dual antenna connection option requires two duplexers:



Cabling

The Aprisa FE 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 (single antenna operation)

Part Number	Part Description
APFE-R400-SSC-B1-40-ENAA	4RF FE, PS, 400-470 MHz, SSC, B1, 4E0S, EN, STD

2. Dual Antenna Protected Station- suitable for options #2 (dual antenna operation)

Part Number	Part Description
APFE-R400-SSC-B1-40-ENDA	4RF FE, PS, 400-470 MHz, SSC, B1, 4E0S, EN, Dual Ant

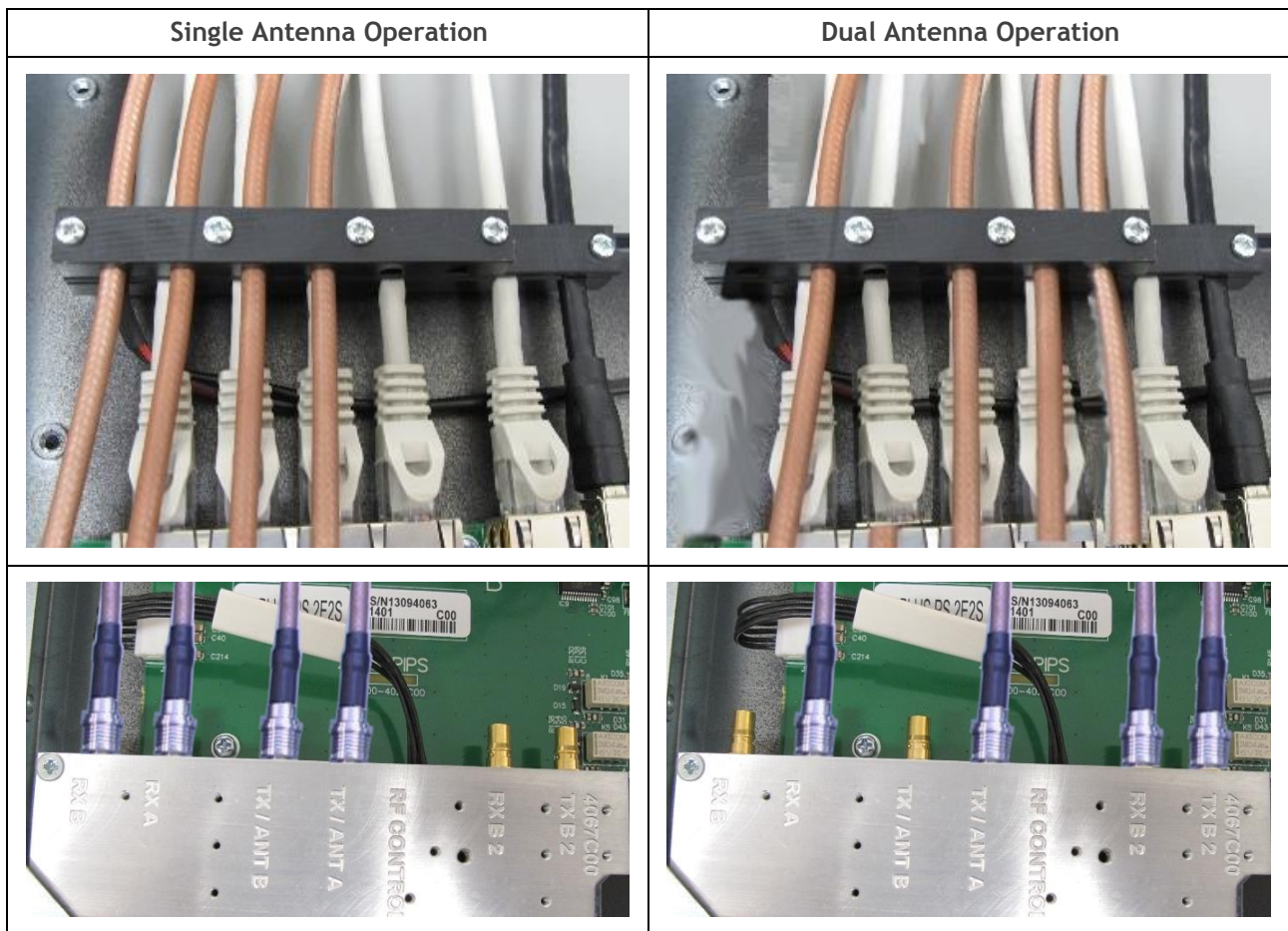
Each option (per ordered part number) is pre-cable configured as the following:

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.

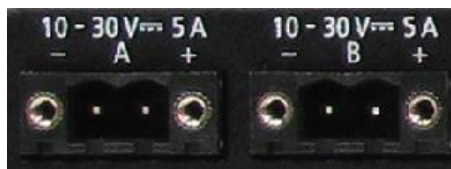
The protection switch is powered from the A power input or the B power input (whichever is available).

The maximum combined power consumption is 35 Watts.

The Aprisa FE Protected station has two DC power options, 12 VDC and 48 VDC.

12 VDC

The 13.8 VDC nominal external power source can operate over the voltage range of +10.5 to +30 V DC (negative earth).

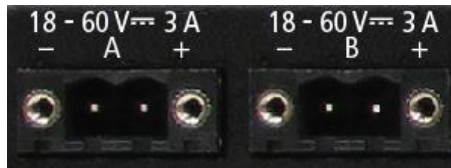


An example of the 12 VDC option part number is:

Part Number	Part Description
APFE-R400-SSC-B1-40-ENAA	4RF FE, PS, 400-470 MHz, SSC, B1, 4E0S, 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
APFE-R400-SSC-B1-40-ENAB	4RF FE, PS, 400-470 MHz, SSC, B1, 4E0S, EN, 48VDC

Alarms

The protection switch provides access to both the A radio and B radio Alarm Interfaces (see 'Alarm Interface Connections' on page 298 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 223). 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 spare FE radios and a new spare Aprisa FE Protection Switch. It assumes that the FE radios are currently setup for non-protected operation.

1. Set the protection type and partner IP address of the FE 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 FE 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 FE Protection Switch.
4. Ensuring that the cables are not crossed over, plug in the interface port cables, the Alarm and Protect port cables and the power connector to both the radios. Secure the power connectors with the two screws.
5. Power on the Protected Station.
6. Connect to either one of the radios via SuperVisor. This will start up SuperVisor in Single Session Management mode.
7. The user can now configure the Protected Station as required.

Replacing a Protected Station Faulty Radio

Replacing a faulty radio in a Protected Station can be achieved without disruption to traffic.

Assuming that the primary radio is active and the secondary radio is faulty and needs replacement:

1. Ensure the replacement radio has the same version of software installed as the primary radio. If necessary, upgrade the software in the replacement radio.
2. Set the RF Interface MAC Address (see 'Protected Station: Maintenance > Advanced' on page 233). This MAC address is present on chassis label.
3. Using SuperVisor > Maintenance > Advanced 'Save Configuration to USB' and 'Restore Configuration from USB' operation, clone the primary radio's configuration to the replacement radio.
4. Configure the replacement radio as the secondary radio and setup the IP address and other protection parameters (see 'Terminal > Operating Mode' on page 71).
5. Set the Hardware Manual Lock switch to make the primary radio active.
6. Unplug the interface port cables, the Alarm and Protect port cables and the power connector from the faulty radio being replaced. The two screws securing the power connector will need to be undone.
7. Carefully remove the faulty radio from the protection switch.
8. Install the replacement radio into the protection switch.
9. Ensuring that the cables are not crossed over, plug in the interface port cables, the Alarm and Protect port cables and the power connector to the replacement radio. Secure the power connector with the two screws.
10. Power on the replacement radio and wait for it to become standby.
11. Set the Hardware Manual Lock switch to the Auto position.

Replacing a Faulty Power Supply

Replacing one of the power supplies can be achieved without disruption to traffic.

If a power supply has failed, the associated radio will have failed which will have caused the protection switch to switch-over to the other radio. It will not have switched back unless the power was restored and another problem occurred which caused a switch-over.

1. If the A power supply is faulty, ensure that the B radio is active (whether it be the primary or secondary radio).
If the B power supply is faulty, ensure that the A radio is active (whether it be the primary or secondary radio).
2. Replace the faulty power supply.

Replacing a Faulty Protection Switch

Note: Replacing a faulty Protection Switch will disrupt traffic.

Move the radios, the interface cables and the power cables to the replacement Protection Switch.

On both Protected Station radios:

1. Power on the radio and wait for it to become ready.
2. Using SuperVisor > Maintenance > Advanced, enter the RF Interface MAC address shown on the Protection Switch label (see 'Protected Station: Maintenance > Advanced' on page 233).
3. Using SuperVisor > Maintenance > Advanced, Decommission the node (see 'Decommission Node' on page 156) and then Discover the Nodes (see 'Discover Nodes' on page 156).

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

The Aprisa FE Protected Station is now ready to operate.

Spares

The Aprisa FE Protection Switch is available as a spare part:

Part Number	Part Description
APFS-XPSW-X40	4RF FE Spare, Protection Switch, 4E0S

The Aprisa FE Protected Station radios are available as spare parts:

An example of the 400 MHz radio spare part number is:

Part Number	Part Description
APFS-R400-SSC-FD-40-ENAA	4RF FE Spare, PS, 400-470 MHz, SSC, Full Dup, 4E0S, EN, STD

8. Maintenance

No User-Serviceable Components

There are no user-serviceable components within the radio.

All hardware maintenance must be completed by 4RF or an authorized service centre.

Do not attempt to carry out repairs to any boards or parts.

Return all faulty radios to 4RF or an authorized service centre.

For more information on maintenance and training, please contact 4RF Customer Services at support@4rf.com.

CAUTION: Electro Static Discharge (ESD) can damage or destroy the sensitive electrical components in the radio.

Software Upgrade

A software upgrade can be performed on a single radio or an Aprisa FE link.

Non Protected Link Upgrade Process

This process allows customers to upgrade their Aprisa FE link from the central local radio location without need for visiting the remote site.

The Software Pack is loaded into the local radio with the file transfer process (see 'Software > File Transfer' on page 175) and distributed via the radio link to the remote radio.

When the remote radio receives the Software Pack version, the software can be remotely activated on the remote radio.

The Aprisa FE link upgrade operation is indicated in local radio and remote radio by a flashing orange MODE LED.

To upgrade the Aprisa FE link software:

1. Using File Transfer, load the software pack into the local radio (see 'Software > File Transfer' on page 175).
2. Distribute the software to the remote radio (see 'Software > Remote Distribution' on page 182).

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

Software distribution traffic is classified as 'management traffic' but does not use the Ethernet management priority setting. Software distribution traffic priority has a fixed priority setting of 'very low'.

3. Activate the software on the remote radio (see 'Software > Remote Activation' on page 184).

Where the new software has been activated, the remote radio will re-register with the local radio.

4. Activate the software on the local radio (see 'Software > Manager' on page 178).

Protected Link Upgrade Process

This upgrade process is for upgrading the software on an Aprisa FE protected link. This software upgrade can be achieved without disruption to traffic.

Transferring the new software to the radios

The software can be transferred to the radio via an FTP transfer or from a USB flash drive.

1. Using the Hardware Manual Lock switch (see 'Hardware Manual Lock' on page 278), or the Software Manual Lock (see 'Lock Active To' on page 229), 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 243).
3. Confirm that the transfer is successful (see 'Protected Station: Software > Manager' on page 246).
4. Using the Hardware Manual Lock switch (see 'Hardware Manual Lock' on page 278), or the Software Manual Lock (see 'Lock Active To' on page 229), 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 240).
6. Confirm that the transfer is successful (see 'Protected Station: Software > Manager' on page 246).
7. Distribute the software to the remote radios (see 'Protected Station: Software > Remote Distribution' on page 248). The protected remotes 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 remote radio (see 'Protected Station: Software > Remote Activation' on page 251).
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, the remote radio will re-register with the local radio. The remote radio software version can be verified with 'Link > Details > Radio' on page 205.

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 local radio 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 246).
5. Immediately after that, activate the new version software pack of the primary radio (see 'Protected Station: Software > Manager' on page 246).

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 both the local and remote radios are now running the latest software version with 'Link > Details > Radio' on page 205.
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


File Transfer Method

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


The Software Pack is loaded into the radio with the file transfer process (see 'Software > File Transfer' on page 175) and activated (see 'Software > Manager' on page 178).

The Aprisa FE upgrade operation is indicated by a flashing orange MODE LED.

To upgrade the Aprisa FE radio software:


1. Unzip the software release files in to the root directory of a USB flash drive.
2. Check that the SuperVisor USB Boot Upgrade setting is set to 'Disabled' (see 'Software > Setup' on page 174).
3. Insert the USB flash drive into the Host Port .
4. Using File Transfer, load the software pack into the radio (see 'Software > File Transfer' on page 175).
5. Activate the software on the radio (see 'Software > Manager' on page 178).

USB Boot Upgrade Method


A single Aprisa FE 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 FE front panel and power cycling the radio.

Upgrade Process

To upgrade the Aprisa FE 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 174).
3. Power off the Aprisa FE and insert the USB flash drive into the Host Port .
4. Power on the Aprisa FE.
5. The software upgrade process is complete when the OK LED lights solid green. This can take about 2 minutes.

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

6. Remove the USB flash drive from the Host Port .
7. Power cycle the Aprisa FE.

Login to the radio being upgraded and go to SuperVisor 'Software > Manager' on page 178.

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

SOFTWARE PACK	
Version	1.5.0
Status	Available
Activation Type	Now 
Activation Date & Time	20/04/2015 14:23

If the upgrade process did not start, the Aprisa FE 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 USB 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 174).

In this case, go to SuperVisor see 'Software > Manager' on page 178 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 link 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 FE Protected Station.

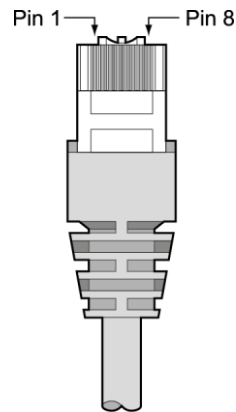
USB Boot Upgrade Method

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.

9. Interface Connections

RJ45 Connector Pin Assignments



RJ45 pin numbering

Ethernet Interface Connections

Pin Number	Pin Function	Direction	TIA-568A Wire Colour	TIA-568B Wire Colour
1	Transmit	Output	Green/white	Orange/white
2	Transmit	Output	Green	Orange
3	Receive	Input	Orange/white	Green/white
4	Not used		Blue	Blue
5	Not used		Blue/white	Blue/white
6	Receive	Input	Orange	Green
7	Not used		Brown/white	Brown/white
8	Not used		Brown	Brown

RJ45 connector LED indicators		
LED	Status	Explanation
Green	On	Ethernet signal received
Green	Flashing	Indicates data traffic present on the interface

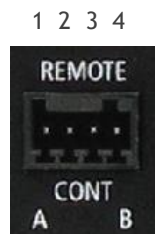
Note: Do not connect Power over Ethernet (PoE) connections to the Aprisa FE Ethernet ports as this will damage the port.

Alarm Interface Connections

RJ45 Pin Number	Pin Function	Direction	TIA-568A Wire Colour	TIA-568B Wire Colour
1	Alarm 1 Input	Input	Green / white	Orange/white
2	Ground		Green	Orange
3	Alarm 2 Input	Input	Orange / white	Green/white
4	Ground		Blue	Blue
5	Alarm 1 Output	Output	Blue / white	Blue/white
6	Ground		Orange	Green
7	Alarm 2 Output	Output	Brown / white	Brown/white
8	Ground		Brown	Brown

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

Protection Switch Remote Control Connections



Pin Number	1	2	3	4
Function	A radio active	Ground	B radio active	Ground

10. 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.

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 161 for setup of alarm thresholds / sample durations etc.

Alarm Events

Transmitter Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function
1	PA Current	critical(1)	Threshold Type	Alarm to indicate that the current drawn by the transmitter power amplifier is outside defined limits.
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.
62	PA Stability	warning(4)	Threshold Type	Alarm to indicate that the power amplifier is oscillating which may cause corruption of the TX signal
2	TX AGC	critical(1)	Threshold Type	Alarm to indicate that the variable gain control of the transmitter is outside defined limits.
3	TX Reverse Power	warning(4)	Threshold Type	Alarm to indicate that the antenna is not connected to the radio
60	TX Forward Power	warning(4)	Threshold Type	Alarm to indicate that the transmitter power is outside the selected TX power setting.
4	Temperature Threshold	warning(4)	Threshold Type	Alarm to indicate that the transmitter temperature is outside defined limits.
5	TX Synthesizer Not Locked	critical(1)	Threshold Type	Alarm to indicate that the transmitter synthesizer is not locked.
31	Thermal Shutdown	critical(1)	Threshold Type	Alarm to indicate that the transmitter has shutdown due to excessively high temperature.

Receiver Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function
7	RSSI Threshold	warning(4)	Threshold Type	Alarm to indicate that the receiver RSSI reading taken on the last packet received is outside defined limits.
8	RX Synthesizer Not Locked	critical(1)	Not Configurable	Alarm to indicate that the receiver Synthesizer is not locked on the RF received signal.
9	RX CRC Errors	warning(4)	Error Ratio Type	Alarm to indicate that the data received on the RF path contains errors at a higher rate than the defined error rate threshold.

Radio Interface Path Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function
34	RF No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that there is no data received on the RF path in the defined duration period.

Modem Alarm Events

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

Customer Equipment Interface Path Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function
10	Port 1 Eth No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that Ethernet port 1 has no received input signal in the defined duration period.
11	Port 1 Eth Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 1 received input signal contains errors at a higher rate than the defined error rate threshold.
12	Port 1 Eth Data Transmit Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 1 transmitted output signal contains errors at a higher rate than the defined error rate threshold.
35	Port 2 Eth No Receive Data	warning(4)	Sample Duration Type	Alarm to indicate that Ethernet port 2 has no received input signal in the defined duration period.
36	Port 2 Eth Data Receive Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 2 received input signal contains errors at a higher rate than the defined error rate threshold.
37	Port 2 Eth Data Transmit Errors	warning(4)	Error Ratio Type	Alarm to indicate that Ethernet port 2 transmitted output signal contains errors at a higher rate than the defined error rate threshold.
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.
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.
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.
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.
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.

Event ID	Event Display Text	Default Severity	Configuration Type	Function
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.

Component Failure Alarm Events

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

Hardware Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function
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
57	3.3 Volts Power Supply	warning(4)	Not Configurable	Alarm to indicate that the 3.3 volt power rail is outside defined limits.
58	5.0 Volts Power Supply	warning(4)	Not Configurable	Alarm to indicate that the 5.0 volt power rail is outside defined limits.
59	7.2 Volts Power Supply	warning(4)	Not Configurable	Alarm to indicate that the 7.2 volt power rail is outside defined limits.
71	15 Volts Power Supply	warning(4)	Not Configurable	Alarm to indicate that the 15 volt power rail is outside defined limits.

Software Alarm Events

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

Hardware Alarm Input Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function
24	Alarm Input 1	warning(4)	Not Configurable	Alarm to indicate that there is an active alarm on hardware alarm input 1
25	Alarm Input 2	warning(4)	Not Configurable	Alarm to indicate that there is an active alarm on hardware alarm input 2

Protected Station Alarm Events

Event ID	Event Display Text	Default Severity	Configuration Type	Function
17	Protection Sw Manual Lock	warning(4)	Not Configurable	Alarm to indicate that the Protection Switch Software Manual Lock has been activated.
18	Protection Hw Manual Lock	warning(4)	Not Configurable	Alarm to indicate that the Protection Switch Hardware Manual Lock has been activated.
23	Protection Peer Comms Lost	major(2)	Not Configurable	Alarm to indicate that the standby radio has lost communication with the active radio.
54	Protection Hardware Failure	major(2)	Not Configurable	Alarm to indicate that there is a failure in the protection switch hardware.

Informational Events

Event ID	Event Display Text	Default Severity	Function
26	User authentication succeeded	information(5)	Event to indicate that a user is successfully authenticated on the radio during login. The information on the user that was successfully authenticated is provided in the eventHistoryInfo object of the Event History Log.
27	User authentication failed	information(5)	Event to indicate that a user has failed to be authenticated on the radio during login. The information on the user that was unsuccessfully authenticated is provided in the eventHistoryInfo object of the Event History Log.
28	Protection switch failed	information(5)	Event to indicate that a protection switch over cannot occur for some reason. The reason for the failure to switch is described in the eventHistoryInfo object of the Event History Log.
29	Software System Check	information(5)	Event to indicate that the software has done a system check on the radio. Any information relevant to the cause of the event is provided in the eventHistoryInfo object of the Event History Log.
30	Software Start Up	information(5)	Event to indicate that the radio software has started. Any information relevant to the software start up is provided in the eventHistoryInfo object of the Event History Log.
33	Protection Switch Occurred	information(5)	Event to indicate that a protection switch over occurs for some reason. The reason for the switch over is described in the eventHistoryInfo object of the Event History Log.
41	File Transfer Activity	information(5)	Event to indicate that a data file is being transferred to or from the radio.
42	Software Management Activity	information(5)	Event to indicate that software is being distributed to the remote radio.
43	Terminal Server TCP Activity	information(5)	Event to indicate TCP packets are being transferred from the terminal server.
55	Terminal Unit Information	information(5)	Event to indicate a miscellaneous activity occurring on the radio
65	Event Action Activity	information(5)	Event to indicate an event action occurring on the radio
72	User SuperVisor Session Logout	information(5)	Event to indicate that a user has logged out or the user session has timed out

11. Specifications

RF Specifications

Blocking (desensitization), intermodulation, spurious response rejection, and adjacent channel selectivity values determined according to the methods introduced in V1.7.1 of ETSI standards EN 300 113-1.

Frequency Bands

ETSI Compliant

Broadcast Band	Frequency Band	Frequency Tuning Range	Synthesizer Step Size
UHF	320 MHz	320-400 MHz	6.250 kHz

ETSI / FCC / IC Compliant

Broadcast Band	Frequency Band	Frequency Tuning Range	Synthesizer Step Size
VHF	135 MHz ⁽¹⁾	135-175 MHz	2.5 kHz
UHF	400 MHz	400-470 MHz	6.250 kHz

ETSI / FCC Compliant

Broadcast Band	Frequency Band	Frequency Tuning Range	Synthesizer Step Size
UHF	450 MHz	450-520 MHz	6.250 kHz

FCC / IC Compliant

Broadcast Band	Frequency Band	Frequency Tuning Range	Synthesizer Step Size
UHF	896 MHz	896-902 MHz	6.250 kHz
UHF	928 MHz	928-960 MHz	6.250 kHz

Note 1: Please consult 4RF for availability.

The Frequency Tuning Range is not an indication of the exact frequencies approved by FCC / IC.

Channel Sizes

ETSI Compliant

320 / 400 MHz Bands

No Forward Error Correction

Channel Size	Gross Radio Capacity		
	64 QAM	16 QAM	QPSK
12.5 kHz	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s
20 kHz	84.0 kbit/s	56.0 kbit/s	28.0 kbit/s
25 kHz	120.0 kbit/s	80.0 kbit/s	40.0 kbit/s
50 kHz	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
12.5 kHz	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s
20 kHz	72.7 kbit/s	32.4 kbit/s	16.2 kbit/s
25 kHz	103.9 kbit/s	46.2 kbit/s	23.1 kbit/s
50 kHz	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
12.5 kHz	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s
20 kHz	63.8 kbit/s	24.2 kbit/s	12.1 kbit/s
25 kHz	91.2 kbit/s	34.6 kbit/s	17.3 kbit/s
50 kHz	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s

450 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity		
	64 QAM	16 QAM	QPSK
12.5 kHz	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s
25 kHz	120.0 kbit/s	80.0 kbit/s	40.0 kbit/s
50 kHz	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
12.5 kHz	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s
25 kHz	103.9 kbit/s	46.2 kbit/s	23.1 kbit/s
50 kHz	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
12.5 kHz	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s
25 kHz	91.2 kbit/s	34.6 kbit/s	17.3 kbit/s
50 kHz	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s

FCC Compliant

400 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity		
	64 QAM	16 QAM	QPSK
12.5 kHz	54.0 kbit/s	36.0 kbit/s	18.0 kbit/s
25 kHz	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s
50 kHz	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
12.5 kHz	46.8 kbit/s	20.8 kbit/s	10.4 kbit/s
25 kHz	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s
50 kHz	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
12.5 kHz	41.0 kbit/s	15.6 kbit/s	7.8 kbit/s
25 kHz	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s
50 kHz	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s

450 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity		
	64 QAM	16 QAM	QPSK
12.5 kHz	54.0 kbit/s	36.0 kbit/s	18.0 kbit/s
25 kHz	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
12.5 kHz	46.8 kbit/s	20.8 kbit/s	10.4 kbit/s
25 kHz	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
12.5 kHz	41.0 kbit/s	15.6 kbit/s	7.8 kbit/s
25 kHz	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s

896 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity		
	64 QAM	16 QAM	QPSK
50 kHz	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
50 kHz	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
50 kHz	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s

928 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity		
	64 QAM	16 QAM	QPSK
12.5 kHz	60.0 kbit/s	40.0 kbit/s	20.0 kbit/s
25 kHz	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s
50 kHz	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
12.5 kHz	52.0 kbit/s	23.1 kbit/s	11.6 kbit/s
25 kHz	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s
50 kHz	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
12.5 kHz	45.6 kbit/s	17.3 kbit/s	8.7 kbit/s
25 kHz	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s
50 kHz	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s

IC Compliant

400 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity		
	64 QAM	16 QAM	QPSK
12.5 kHz	54.0 kbit/s	36.0 kbit/s	18.0 kbit/s
25 kHz	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s
50 kHz	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
12.5 kHz	46.8 kbit/s	20.8 kbit/s	10.4 kbit/s
25 kHz	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s
50 kHz	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
12.5 kHz	41.0 kbit/s	15.6 kbit/s	7.8 kbit/s
25 kHz	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s
50 kHz	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s

896 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity		
	64 QAM	16 QAM	QPSK
50 kHz	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
50 kHz	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
50 kHz	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s

928 MHz Band

No Forward Error Correction

Channel Size	Gross Radio Capacity		
	64 QAM	16 QAM	QPSK
12.5 kHz	54.0 kbit/s	36.0 kbit/s	18.0 kbit/s
25 kHz	96.0 kbit/s	64.0 kbit/s	32.0 kbit/s
50 kHz	216.0 kbit/s	144.0 kbit/s	72.0 kbit/s

Minimum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
12.5 kHz	46.8 kbit/s	20.8 kbit/s	10.4 kbit/s
25 kHz	83.1 kbit/s	37.0 kbit/s	18.5 kbit/s
50 kHz	187.1 kbit/s	83.2 kbit/s	41.6 kbit/s

Maximum Coded Forward Error Correction

Channel Size	Gross Radio Capacity less FEC		
	64 QAM	16 QAM	QPSK
12.5 kHz	41.0 kbit/s	15.6 kbit/s	7.8 kbit/s
25 kHz	73.0 kbit/s	27.7 kbit/s	13.9 kbit/s
50 kHz	164.2 kbit/s	62.4 kbit/s	31.2 kbit/s

Receiver

Receiver Sensitivity

			12.5 kHz	25 kHz	50 kHz
BER < 10 ⁻²	64 QAM	Max coded FEC	-104 dBm	-100 dBm	-97 dBm
BER < 10 ⁻²	64 QAM	Min coded FEC	-103 dBm	-99 dBm	-96 dBm
BER < 10 ⁻²	64 QAM	No FEC	-101 dBm	-97 dBm	-94 dBm
BER < 10 ⁻²	16 QAM	Max coded FEC	-111 dBm	-108 dBm	-105 dBm
BER < 10 ⁻²	16 QAM	Min coded FEC	-110 dBm	-107 dBm	-104 dBm
BER < 10 ⁻²	16 QAM	No FEC	-107 dBm	-104 dBm	-101 dBm
BER < 10 ⁻²	QPSK	Max coded FEC	-116 dBm	-113 dBm	-110 dBm
BER < 10 ⁻²	QPSK	Min coded FEC	-115 dBm	-112 dBm	-109 dBm
BER < 10 ⁻²	QPSK	No FEC	-113 dBm	-110 dBm	-107 dBm
BER < 10 ⁻⁶	64 QAM	Max coded FEC	-101 dBm	-97 dBm	-94 dBm
BER < 10 ⁻⁶	64 QAM	Min coded FEC	-99 dBm	-95 dBm	-92 dBm
BER < 10 ⁻⁶	64 QAM	No FEC	-94 dBm	-90 dBm	-87 dBm
BER < 10 ⁻⁶	16 QAM	Max coded FEC	-108 dBm	-105 dBm	-102 dBm
BER < 10 ⁻⁶	16 QAM	Min coded FEC	-106 dBm	-103 dBm	-100 dBm
BER < 10 ⁻⁶	16 QAM	No FEC	-100 dBm	-97 dBm	-94 dBm
BER < 10 ⁻⁶	QPSK	Max coded FEC	-113 dBm	-110 dBm	-107 dBm
BER < 10 ⁻⁶	QPSK	Min coded FEC	-111 dBm	-108 dBm	-105 dBm
BER < 10 ⁻⁶	QPSK	No FEC	-106 dBm	-103 dBm	-100 dBm

Adjacent Channel Selectivity

		12.5 kHz	25 kHz	50 kHz
Adjacent channel selectivity		> -45 dBm	> -35 dBm	> -35 dBm
BER < 10 ⁻²	64 QAM	> 43 dB	> 53 dB	> 53 dB
BER < 10 ⁻²	16 QAM	> 43 dB	> 53 dB	> 53 dB
BER < 10 ⁻²	QPSK	> 48 dB	> 58 dB	> 58 dB

Co-Channel Rejection

		12.5 kHz	25 kHz	50 kHz
BER < 10 ⁻²	64 QAM	> -23 dB	> -23 dB	> -23 dB
BER < 10 ⁻²	16 QAM	> -19 dB	> -19 dB	> -19 dB
BER < 10 ⁻²	QPSK	> -12 dB	> -12 dB	> -12 dB

Intermodulation Response Rejection

		12.5 kHz	25 kHz	50 kHz
Intermodulation response rejection		> -33 dBm	> -33 dBm	> -33 dBm
BER < 10 ⁻²	64 QAM	> 55 dB	> 55 dB	> 55 dB
BER < 10 ⁻²	16 QAM	> 55 dB	> 55 dB	> 55 dB
BER < 10 ⁻²	QPSK	> 60 dB	> 60 dB	> 60 dB

Blocking or Desensitization

		12.5 kHz	25 kHz	50 kHz
Blocking or desensitization		> -15 dBm	> -15 dBm	> -15 dBm
BER < 10 ⁻²	64 QAM	> 73 dB	> 73 dB	> 73 dB
BER < 10 ⁻²	16 QAM	> 73 dB	> 73 dB	> 73 dB
BER < 10 ⁻²	QPSK	> 78 dB	> 78 dB	> 78 dB

Spurious Response Rejection

		12.5 kHz	25 kHz	50 kHz
Spurious response rejection		> -30 dBm	> -30 dBm	> -30 dBm
BER < 10 ⁻²	64 QAM	> 58 dB	> 58 dB	> 58 dB
BER < 10 ⁻²	16 QAM	> 58 dB	> 58 dB	> 58 dB
BER < 10 ⁻²	QPSK	> 63 dB	> 63 dB	> 63 dB

Receiver Spurious Radiation

		12.5 kHz	25 kHz	50 kHz
Receiver spurious radiation		> -57 dBm	> -57 dBm	> -57 dBm

Transmitter

Average Power output Note: The Peak Envelope Power (PEP) at maximum set power level is +41 dBm.	64 QAM	0.01 to 1.6 W (+10 to +32 dBm, in 1 dB steps)
	16 QAM	0.01 to 2.0 W (+10 to +33 dBm, in 1 dB steps)
	QPSK	0.01 to 3.2 W (+10 to +35 dBm, in 1 dB steps)

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

Adjacent channel power	< - 60 dBc
Transient adjacent channel power	< - 60 dBc
Spurious emissions	< - 37 dBm
Attack time	< 1.5 ms
Release time	< 0.5 ms
Data turnaround time	< 2 ms
Frequency stability	± 1.0 ppm
Frequency aging	< 1 ppm / annum

Modem

Forward Error Correction	Variable length concatenated Reed Solomon plus convolutional code
Adaptive Burst Support	Adaptive FEC Adaptive Coding Modulation

Data Payload Security

Data payload security	CCM* Counter with CBC-MAC
Data encryption	Counter Mode Encryption (CTR) using Advanced Encryption Standard (AES) 128, 192 or 256
Data authentication	Cipher Block Chaining Message Authentication Code (CBC-MAC) using Advanced Encryption Standard (AES) 128, 192 or 256

Interface Specifications

Ethernet Interface

The Aprisa FE 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 Green LED	Off: Indicates no data traffic present on the interface Flashing: Indicates data traffic present on the interface

Note: Do not connect Power over Ethernet (PoE) connections to the Aprisa FE Ethernet ports as this will damage the port.

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

The Aprisa FE Protected Station is a future development.

Power Specifications

Power Supply

Aprisa FE Radio

Nominal voltage	+13.8 VDC (negative earth)
Absolute input voltage range	+10 to +30 VDC
Maximum power input	35 W
Connector	Molex 2 pin male screw fitting 39526-4002

Aprisa FE Protected Station

The Aprisa FE Protected Station is a future development.

Power Consumption

Note: The radio power consumption is very dependent on transmitter power, the type of traffic and network activity.

Aprisa FE Radio

Mode	Power Consumption
Transmit / Receive	< 35 W for 10 W transmit power
	< 25.0 W for 1 W transmit power
Receive only	< 7 W

Aprisa FE Protected Station

Mode	Power Consumption (10 W radios with 4-CPFSK modulation)
Transmit / Receive	< 42 W for 10 W transmit power
	< 32.0 W for 1 W transmit power
Receive only	< 15 W

Power Dissipation

Aprisa FE Radio

Transmit Power	Power Dissipation
10 W transmit power	< 25 W
1 W transmit power	< 24 W

Aprisa FE Protected Station

Transmit Power	Power Dissipation (10 W radios with 4-CPFSK modulation)
10 W transmit power	< 32 W
1 W transmit power	< 31 W

General Specifications

Environmental

Operating temperature range	-40 to +60° C (-40 to +140° F)
Storage temperature range	-40 to +80° C (-40 to +176° F)
Operating humidity	Maximum 95% non-condensing
Acoustic noise emission	No audible noise emission

Mechanical

Aprisa FE Radio

Dimensions	Width 434 mm (17.1") Depth 300 mm (11.8") and 440 mm (17.3") Height 44.45 mm (1.75")
Weight	5.0 kg (11.3 lbs) (dependent on duplexer type)
Colour	Matt black
Mounting	Rack mount 19" 1U high (internal duplexer)

Aprisa FE 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 (s)
Weight	12 kg (27 lbs) (includes the 2 radios)
Colour	Matt black
Mounting	Rack mount (2 x M6 screws)

Compliance

ETSI

Radio	EN 300 113-2
EMI / EMC	EN 301 489 Parts 1 & 5
Safety	EN 60950-1:2006
Environmental	ETS 300 019 Class 3.4 Ingress Protection code IP51

FCC

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

IC

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

12. 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 FE radio, contact us (on page 13).

13. Abbreviations

AES	Advanced Encryption Standard	TCP/IP	Transmission Control Protocol/Internet Protocol
AGC	Automatic Gain Control	TCXO	Temperature Compensated Crystal Oscillator
BER	Bit Error Rate	TFTP	Trivial File Transfer Protocol
CBC	Cipher Block Chaining	TMR	Trunk Mobile Radio
CCM	Counter with CBC-MAC integrity	TX	Transmitter
DCE	Data Communications Equipment	UTP	Unshielded Twisted Pair
DTE	Data Radio Equipment	VAC	Volts AC
EMC	Electro-Magnetic Compatibility	VCO	Voltage Controlled Oscillator
EMI	Electro-Magnetic Interference	VDC	Volts DC
ESD	Electro-Static Discharge	WEEE	Waste Electrical and Electronic Equipment
ETSI	European Telecommunications Standards Institute		
FW	Firmware		
HW	Hardware		
IF	Intermediate Frequency		
IP	Internet Protocol		
I/O	Input/Output		
ISP	Internet Service Provider		
kbit/s	Kilobits per second		
kHz	Kilohertz		
LAN	Local Area Network		
LED	Light Emitting Diode		
mA	Milliamps		
MAC	Media Access Control		
MAC	Message Authentication Code		
Mbit/s	Megabits per second		
MHz	Megahertz		
MIB	Management Information Base		
MTBF	Mean Time Between Failures		
MTTR	Mean Time To Repair		
ms	milliseconds		
NMS	Network Management System		
PC	Personal Computer		
PCA	Printed Circuit Assembly		
PLL	Phase Locked Loop		
ppm	Parts Per Million		
PMR	Public Mobile Radio		
RF	Radio Frequency		
RoHS	Restriction of Hazardous Substances		
RSSI	Received Signal Strength Indication		
RX	Receiver		
SNMP	Simple Network Management Protocol		
SNR	Signal to Noise Ratio		
SWR	Standing Wave Ratio		

14. Index

		requirement for	16, 48
A			
access rights	133		
accessory kit	14		
antennas			
aligning	270		
installing	44		
selection and siting	38		
siting	39		
attenuators	37		
B			
bench setup	37		
C			
cabling			
accessory kit	14		
coaxial feeder	37, 40		
CD contents	16		
E			
earthing	37, 40, 42		
environmental requirements	41		
F			
feeder cables	40		
front panel			
connections	31		
H			
hardware			
accessory kit	14		
installing	44		
humidity	41		
I			
in-service commissioning	269		
interface connections	297		
Ethernet	297		
J			
Java			
L			
lightning protection	42		
linking system plan	40		
logging in			
SuperVisor	55		
logging out			
SuperVisor	56		
M			
maintenance summary	144		
mounting kit	14		
O			
operating temperature	41		
P			
passwords			
changing	134		
path planning	38		
path propagation calculator	38		
pinouts			
Ethernet	297		
RS-232	298		
power supply	41		
R			
radio			
earthing	37, 42		
logging into	55		
logging out	56		
operating temperature	41		
rebooting	149		
storage temperature	41		
rebooting the radio	149		
S			
security			
settings	127, 135, 140, 142, 159, 164, 166, 168, 170		
summary	126, 137, 226		
security users			

user privileges	133
SuperVisor	
logging into	55
logging out	56
PC requirements for	48
PC settings for	51

T

temperature	41
-------------	----

U

users	
adding	133
changing passwords	134
deleting	134
user details	133
user privilege	134

W

WEEE	322
------	-----