



Aprisa **SR+**



Software Release Notes

Version 1.4.0

April 2015

Contents

1.	Introduction	2
2.	Released Files	2
3.	Product Features	3
	3.1. New Features.....	3
	3.2. Existing Features	4
4.	Software Enhancements	10
	4.1. Major Enhancements.....	10
	4.2. Minor Enhancements.....	10
5.	Hardware Enhancements	13
	5.1. Major Enhancements.....	13
	5.2. Minor Enhancements.....	13
6.	Software Bug Fixes	14
	6.1. Major Bug Fixes.....	14
	6.2. Minor Bug Fixes	14
7.	Known Issues	15
8.	Software Upgrade	16
	Network Software Upgrade	16
	Non-Protected Network Upgrade Process	16
	Protected Network Upgrade Process.....	18
	Single Radio Software Upgrade.....	19
	File Transfer Method	19
	USB Boot Upgrade Method.....	20
	Software Downgrade	20
	Protected Station Software Upgrade	21
	USB Boot Upgrade Method.....	21

1. Introduction

The Aprisa SR+ software release 1.4.0 is a general availability release.

Aprisa SR+ software version 1.4.0 is not backwards compatible with previous Aprisa SR+ software versions. If an Aprisa SR+ network contains a radio operating on software version 1.4.0, all radios in the network must be operating on version 1.4.0 or later.

Introduction

The previous Aprisa SR+ software version release relevant to this release is:

Software Version	Release Date
1.3.0	3 rd November 2014

This release of Aprisa SR+ software is:

Software Version	Release Date
1.4.0	16 th April 2015

This document covers the major changes, product enhancements, new functionality, and bug fixes since Aprisa SR+ software version 1.3.0.

2. Released Files

Release Files

The following is a list of files released for Aprisa SR+ Software Version 1.4.0

File Name	File Type	File Function
asrapp	Upgrade App Code	Used to initiate radio software upgrade
asrboot	Bootloader	Used to initiate radio software startup
asrmain	Application Code	Main radio system software
asrrootfs	Root File System	Catalog of system files
asrver	Version File	Release build version
version.txt	Public Version File	Release information

3. Product Features

The Aprisa SR+ product release version 1.4.0 has the following new features. For more information, see the Aprisa SR+ User Manual 1.4.0.

3.1. New Features

Mirrored Bits[®] Support

In software Version 1.4.0, support has been added for the Mirrored Bits[®] protocol. Mirrored Bits[®] is a protocol devised by Schweitzer Engineering Laboratories, Inc.

The design enables point-to-point contact status bit transfer applications in protection (bus protection, blocking, unblocking, permissive, and transfer trip) and automation (sectionalizing, restoration, and interlock systems). The protocol is often described as a relay-to-relay communications technology.

Mirrored Bits[®] is a registered trademark of Schweitzer Engineering Laboratories, Inc

Gateway Router Mode / New Router Mode

In software Version 1.4.0, the existing Ethernet Operating Mode of 'Router Mode' name has been changed to 'Gateway Router Mode'. In this mode, the Ethernet interfaces have the same IP address.

A new mode 'Router Mode' has been added. In this mode, each Ethernet interface has a different IP address and subnet. See Aprisa SR+ User Manual 1.4.0 for more details.

New Monitored Parameter History Log

In software Version 1.4.0, a history log has been added for Monitored Parameter data. 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.
-

Enhanced Full Duplex Repeater MAC Scheme

In software Version 1.4.0, a new Full Duplex MAC scheme for repeater configurations has been added which allows packets to start repeater egress before the entire packet has been received into the repeater.

This scheme reduces latency on long packets through a repeater and improves performance in Overlapping Coverage mode.

To allow this new MAC scheme to operate, two new RF Network Detail parameters have been added; Base Station ID and Repeater Network Segment ID. The base station and all repeaters using this scheme must use the same settings for these two parameters.

New Enhanced Noise Rejection Mode

In software Version 1.4.0, a new Enhanced Noise Rejection Mode has been added to the Modem parameters. This feature improves co-channel interference performance at strong receiver signal levels. All radios in an Aprisa SR+ network must use the same setting i.e. enabled or disabled.

RADIUS Authentication

In software Version 1.4.0, RADIUS authentication has been added to provide centralized Authentication, Authorization, and Accounting management for users.

3.2. Existing Features

The Aprisa SR+ product release version 1.4.0 has the following existing features.

Frequency Bands Five frequency band products software selectable over the entire frequency band:

VHF 220	215-240 MHz	FCC / IC compliance
UHF 320	320-400 MHz	ETSI compliance
UHF 400	400-470 MHz	ETSI / FCC / IC compliance
UHF 450	450-520 MHz	ETSI / FCC compliance
UHF 928	896-902 MHz	FCC / IC compliance
UHF 928	928-960 MHz	FCC / IC compliance

Channel Sizes Software selectable channel sizes of 12.5, 25 kHz and 50 kHz.

Gross Radio Capacity

Maximum gross radio capacity with 12.5 kHz and 25 kHz channel sizes:

12.5 kHz	60 kbit/s (ETSI)
25 kHz	120 kbit/s (ETSI)

Software selectable channel size of 50 kHz for 220 / 928 MHz FCC / IC bands and 320 MHz ETSI band for Austria.

The maximum gross radio capacity for a 50 kHz channel size is:

ETSI	216 kbit/s (320 MHz band for Austria)
FCC / IC	216 kbit/s

Compliance

FCC / IC compliance for the 220 MHz band
 ETSI compliance for the 320 MHz band
 ETSI / FCC / IC compliance for the 400 MHz band.
 ETSI / FCC compliance for the 450 MHz band
 FCC / IC compliance for the 896 and 928 MHz bands.
 Also RoHS, WEEE and HazLoc class 1 div 2.

Operating Mode Operating modes of base, base-repeater, repeater and remote stations.

RF Operation One or two frequency half duplex RF operation which eliminates the need for external duplexers. With the dual antenna port option, an external duplexer can be used for filtering.

Channel Access Modes	<p>Channel access modes of Access Request (AR) and Listen Before Send (LBS) / CSMA for radio channel management.</p> <p>AR channel access has higher channel efficiency than LBS in a spontaneous message scheme (report by exception).</p>
MHSB 1+1 Protected Station	<p>The Aprisa SR+ 1+1 MHSB Protected Station (PS) supports:</p> <ul style="list-style-type: none"> • Operating modes of Base, Base-repeater, Repeater and Remote station • Protection types of Monitored Hot-standby and redundant • Ethernet / IP mode: Bridge or Router modes both with Virtual IP support for smooth fail switchover • Multiple Antenna and Duplexer options: single antenna with / without a duplexer and dual antenna with / without a duplexer (dual or single TNC port) • Active and standby RF ports monitored in 'monitor hot-standby' protection type
Adaptive Coding Modulation and Forward Error Correction	<p>Adaptive Coding Modulation (ACM) which maximizes the use of the RF path to provide the highest radio capacity available.</p> <p>ACM automatically adjusts the modulation coding and FEC code rate in the remote to base direction of transmission over the defined modulation range based on the signal quality and / or errored packets for each individual remote radio.</p> <p>When the RF path is healthy (no fading), modulation coding is increased and the FEC code rate is decreased to maximize the data capacity.</p> <p>If the RF path quality degrades, modulation coding is decreased and the FEC code rate is increased for maximum robustness to maintain path connectivity.</p> <p>ACM can be disabled and fixed modulations of 64 QAM, 16 QAM or QPSK used with Min / Max FEC per modulation.</p>
OTA Data Encryption	<p>OTA data encryption using Advanced Encryption Standard (AES) 128, 192 or 256.</p>
OTA Data Authentication	<p>OTA data authentication and data integrity using Cipher Block Chaining Message Authentication Code (CBC-MAC) using Advanced Encryption Standard (AES) 128, 192 or 256.</p>
OTA Data Compression	<p>Ethernet and serial payload compression to increase the narrow band radio capacity.</p>
KEK	<p>Enhanced Key Encryption Key (KEK) based on RFC 3394, for secure Over The Air Re-keying (OTAR) of encryption keys</p>
Header Compression	<p>Ethernet header and IP/TCP/UDP ROHC header compression to increase the narrow band radio capacity.</p>

Antenna Port Options	Software selectable dual / single antenna port options (dual antenna port for external duplexers or filters using dual frequency).
Data Interface Port Options	Multiple data interface port options for combinations of Ethernet and RS-232 serial for a total of four interface ports i.e. port options of 2E2S, 3E1S or 4E0S, where E=Ethernet, S=Serial port. Optional: Additional RS-232 / RS-485 port via USB converter.
Pseudo Peer to Peer	Pseudo peer to peer communication between remote stations through base-repeater or repeater stations.
Terminal Server	Terminal server operation for transporting RS-232 / RS-485 traffic over IP or Ethernet.
L3 Router Mode	L3 Router mode with standard static IP route for simple routing network integration.
L2 Bridge Mode	L2 Bridge mode with VLAN aware for standard Industrial LAN integration.
VLAN Support	IEEE 802.1Q VLAN support with single and double VLAN tagged and add/remove VLAN manipulation to adapt to the appropriate RTU / PLCs.
QoS Support	QoS support using IEEE 802.1p VLAN priority bits to prioritize and handle the VLAN / traffic types.
L2/3/4 Filtering	L2/3/4 filtering for blocking security attacks and blocking unwanted traffic avoiding narrow band radio network overload.
Hardware Alarm Inputs / Outputs	Two hardware alarm inputs and two hardware alarm outputs mappable to any radio alarm event.
SCADA Protocol Support	Transparent to all common SCADA protocols; e.g. Modbus, IEC 60870-5-101/104, DNP3 or similar.
SuperVisor Web Management	SuperVisor web management support for element and sub-network (base-repeater-remotes) management.
Secure SuperVisor	HTTPS secure SuperVisor web access management using SSL secure protocol.

SNMP and NMS	SNMPv1/2/3 MIB supports for 4RF NMS SNMP manager or third party NMS SNMP agent network management.
SNMP Security	SNMPv1/2/3 encryption and authentication using HMAC-MD5 or HMAC-SHA for secure NMS / SNMP access and management transactions.
SNTP	Simple Network Time Protocol (SNTP) for accurate wide radio network time and date.
Multi Repeater	Multi repeater, where the Network Radius = 1 (i.e. the multi repeater is in the first hop from the base station) in AR and LBS channel access mode.
Daisy Chain	Daisy chain used for daisy chain repeaters when remote stations are very far from base station coverage. Daisy chain repeaters can only be used in LBS channel access mode.
Alarm and Event Parameter Logging	Alarm event parameters can be configured for all alarm events. All active alarms for configured alarm events will be displayed on the SuperVisor Parameters page. The last 1500 events are stored in the radio and the complete event list can be downloaded to flash drive via the radio USB host port.
Software Upgrades	Over-the-air software distribution and upgrades.
Multiple Management Session Detection	A 'Multiple Management Sessions popup' to show if there is more than one user logged into the same radio.
Frequency Tracking	A 'Frequency Tracking' setting which enables the receiver to track any frequency drift in the transmitter to maintain optimum SNR and radio link performance over the full temperature range.

QoS using Traffic Priority and Traffic Classification

Enhanced QoS (Quality of Service) mechanism to allow users to prioritize traffic per port, packet, protocol, and application etc. using most of the L2/3/4 header fields. To implement this, the radio supports the following QoS capabilities:

- VLAN and IP Traffic Priority mapping - to allow different priority schemes between corporate and radio networks with different network capacities. The radio provides:
 - Priority mapping between external / corporate VLAN priority (per IEEE 802.1p) networks and the radio internal priority network in bridge mode.
 - Priority mapping between external / corporate IP DSCP priority (DiffServ Code Point, per RFC 2474/5) networks and the radio internal priority network in router mode.
- Traffic Classification profiles are based on classification rules. A profile can be set to a particular VLAN ID and CoS / priority or only to CoS / priority to provide the appropriate QoS treatment. Each profile can be related a specific traffic type, protocol or application in the radio network.

For example SCADA traffic, management traffic, FTP traffic, each can have its own profile built with a set of classification rules. A profile can be built using multiple classification rules such as: port, VLAN ID, DSCP, MAC/IP address, TCP/UDP port to identify and classify the specific traffic type in order to provide the appropriate QoS treatment.

The radio supports traffic classification profiles / rules for both bridge and router modes.

Diagnostics and Performance Monitoring

Diagnostic and performance monitoring parameters to support a major subset of RMON I (per RFC 2819) performance monitoring parameters on a per port basis. A subset of RMON II (RFC 4502) has been added to bridge mode using the L2 MAC address learning / aging table and the ARP table, in addition to the existing routing table in router mode.

The Monitored Parameters has menu level items of:

- Monitoring > Terminal
- Monitoring > Serial
- Monitoring > Ethernet
- Monitoring > Radio
- Monitoring > User Selected
- Monitoring > TCP Connections
- Monitoring > Routing Table
- Monitoring > Address Tables

[File Transfer For Configuration Settings And Log Files](#) File transfer save to and restore from PC or USB flash drive of configuration and log files.
SuperVisor > Maintenance > Advanced contains a Maintenance Files section which can save / restore to / from PC or USB flash drive the following file types:

Configuration Settings
Event History Log
Configuration Script

[Scheduled Software Activation](#) Scheduled software upgrade activation with two types of activation methods for base / master station activation and for all remote stations:

- Now
- Date and Time

The radio SNMP management interface supports the management of the scheduled software activation via the existing SWMANAGER-MIB interface.

[SNMPv3 Authentication Passphrase](#) SNMP management interface support for SNMPv3 Authentication Passphrase change via the SNMPv3 secure management protocol (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.

[SNMPv3 Context Addressing](#) SNMP management interface support for SNMPv3 Context Addressing.
The SNMPv3 context addressing allows the user to use a secure SNMPv3 management while boosting the NMS performance when using the SNMPv3 context addressing.
A NMS (Network Management System) can access any remote radio directly by using its IP address or via base / master station SNMPv3 context addressing. The SNMPv3 context addressing can compress the SNMPv3 management traffic OTA (Over The Air) to remote station up to 90% relative to direct OTA SNMPv3 access to remote station, avoiding the radio narrow bandwidth traffic loading.

[Aprisa SR Compatible](#) A 'SR Compatible' feature option which enables over-the-air point-to-multipoint interoperability between an Aprisa SR+ network and the New Aprisa SR radios.
When the Aprisa SR+ 'SR Compatible' option is activated, the SR+ locks its modulation to QPSK (as per the New Aprisa SR modulation) and disables functionality which is not available in New Aprisa SR for full compatibility / interoperability operation.
Note: Any mix between New Aprisa SR and Aprisa SR+ in the network will force the whole network to work in SR Compatible mode.

4. Software Enhancements

4.1. Major Enhancements

None

4.2. Minor Enhancements

Serial Port Baud Rate of 600 bit/s

In software Version 1.4.0, a baud rate of 600 bit/s has been added to the available RS-232 serial port data rates.

RS-232 Serial Port MTU Size

In software Version 1.4.0, a MTU Size parameter has been added to the RS-232 Serial Port Settings. This parameter defines the size of the size of the packet in bytes received before it is transmitted if an inter-frame gap is not detected.

USB CLI Management Support

In software Version 1.4.0, support has been added to allow the USB host port to be used to access the radio Command Line Interface (CLI). A USB converter to RS-232 convertor will be required to connect to a PC e.g.:

Part Number APSB-KFCA-USB-23-D9-MF18

Part Description: 4RF SR+ Acc, Kit, Interface, USB Conv, RS-232, DB9, Female, 1.8m

HTTPS Security Change

In software Version 1.4.0, the certificate key has been changed from RSA1024 to the more secure ECC256.

Each radio now will have its own randomly generated unique self-signed certificate instead of a common factory provisioned certificate. This change does not apply to OEM branded radios.

Also added support for TLS protocol versions 1.0, 1.1 and 1.2 and removed support for older SSL protocol (along with all cipher suites currently supported), due to insecure nature of these protocols / cipher suites.

This has the consequence of removing support for IE on Windows XP for HTTPS connections (HTTP connections still supported from all browsers).

The Aprisa SR+ will now only support the following cipher suites:

- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-ECDSA-AES256-CCM-8
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA

New CLI Reset SNMPv3 Users Command

In software version 1.4.0, a new command has been added to the Command Line Interface (CLI) to 'reset' the SNMPv3 USM users back to defaults.

This command has been added as it is not possible for users to read previously set passphrases. This command is only accessible to the CLI 'admin' user logins.

To reset all USM users back to defaults:

1. Log in to the radio CLI locally via a USB connection or use remote telnet (this will require temporarily allowing telnet to the terminal).
2. Set all SNMP3 users to default values with the 'snmpusm reset' command.
3. Reboot the radio with the 'reboot' command.

The default values are:

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

5. Hardware Enhancements

5.1. Major Enhancements

None

5.2. Minor Enhancements

None

6. Software Bug Fixes

6.1. Major Bug Fixes

None

6.2. Minor Bug Fixes

Loss Of Communications With Remote Radios

Previously, when the SuperVisor > Software Setup > USB Boot Upgrade was set to disabled, the MAC address of the radio was incorrectly set to 00:00:00:00:00:00. As an all zero MAC address is not valid for the radio, it caused a loss of communications with remote radios.

A work around is possible by setting the SuperVisor > Software Setup > USB Boot Upgrade to 'Load and Activate' or 'Load Only'.

This problem has been corrected in software version 1.4.0.

Issue #3693

Protected Station File Transfer From Partner

Previously, with an Aprisa SR+ Protected Station, the transfer of software between partner radios could fail. This problem was caused by a serial communication timeout due to the size of the file.

In software version 1.4.0, the 'Transfer From Partner' method of transfer is no longer supported.

Either the 'USB Transfer' or FTP file transfer methods are used to transfer the software pack to the primary or secondary radios.

Issue #3700

Protected Station Different Software Versions

Previously with an Aprisa SR+ Protected Station, SuperVisor pages were not loading correctly when the primary and secondary radios were running on different versions of software.

This problem has been corrected in software version 1.4.0 by adding detection of unavailable objects from the partner unit and using default values instead.

It should be noted that the intention is for both radios to always be operating on the same software version.

Issue #3697

7. Known Issues

Protected Station Partner Comms Loss

With an Aprisa SR+ Protected Station, following a software downgrade, communications to the partner radio is lost. This problem is caused by the watchdog subsystem failing to detect a data corruption.

The work around is to reboot the protected station following a software downgrade.
Issue #3696

8. Software Upgrade

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

Network Software Upgrade

This process allows customers to upgrade their Aprisa SR+ network from the central base station location without need for visiting remote sites.

The Software Pack is loaded into the base station with the file transfer process (see SuperVisor Software > File Transfer) and distributed via the radio link to all remote stations.

When all remote stations receive the Software Pack version, the software can be remotely activated on all remote stations.

Non-Protected Network Upgrade Process

This upgrade process is for upgrading the software on an entire Aprisa SR+ network from a non-protected base station. If there are protected remotes in the network, they must be locked to the current active radio.

To upgrade the entire Aprisa SR+ network software:

1. Using File Transfer, load the software pack into the base station (see SuperVisor Software > File Transfer). The software can be transferred to the radio via an FTP transfer or from a USB flash drive.

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

2. Distribute the software to the entire network of remote radios (see SuperVisor Software > Remote Distribution). Note that the distribution process over the air will take some time, depending on RF and Transfer rate settings.

The Aprisa SR+ network software distribution operation is indicated in base station and remote stations by a flashing orange MODE LED.

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

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

3. Activate the software on the entire network of remote radios (see SuperVisor Software > Remote Activation).

Note: When the new software activates on the remote radios, all link communication from the base station to the remote will be lost. The base station will attempt to re-establish connectivity to the remote radios for the new version verification but this will fail. However, when the new software activates on the remote radios, the remote radio will reboot automatically and link communication will restore when the base station software is activated.

When the Remote Activation process gets to the ‘Remote Radios On New Version’ step, don’t wait for this to complete but proceed to step 4.

4. Activate the software on the base station radio (see SuperVisor Software > Manager).
5. When the new software has been activated, remote stations will re-register with the base station. The remote stations software version can be verified with SuperVisor Network Status > Network Table.
6. When the base station restarts with the new software, rediscover the nodes (see SuperVisor Maintenance Advanced > Discover Nodes).
7. Check that all remote radios are now running on the new software (see SuperVisor Network Status > Network Table).

Note: The following steps will only be necessary if for some reason steps 1-7 did not operate correctly or if software activation is attempted before the distribution process ends or the remote radio was off during steps 1-7 and turns on later. Thus, the following steps will most likely not be required.

8. If step 7 shows that not all remote radios are running the latest software version, restore the base / master station to the previous software version (see SuperVisor Software > Manager).
9. Attempt to re-establish connectivity to the remote radios that have failed to upgrade by navigating to and remotely managing the remote radios individually.
10. Navigate to the remote radio history log and review the logs to determine the reason for the failure to activate the new software version.
11. Take appropriate actions to address the reported issue. If connectivity restores with the failed remotes, repeat steps 2-7 if required.

Protected Network Upgrade Process

This upgrade process is for upgrading the software on an entire Aprisa SR+ network from a protected base station. This software upgrade can be achieved without disruption to traffic.

Transferring the new software to the radios

The software can be transferred to the radio via an FTP transfer or from a USB flash drive.

1. Using the Hardware Manual Lock switch or the Software Manual Lock (see SuperVisor Protected Station: Maintenance > Protection 'Lock Active To'), force the secondary radio to active
2. Using File Transfer, load the software pack into the secondary radio (see SuperVisor Protected Station: Software > Secondary File Transfer).
3. Confirm that the transfer is successful (see SuperVisor Protected Station: Software > Manager).
4. Using the Hardware Manual Lock switch or the Software Manual Lock (see SuperVisor Protected Station: Maintenance > Protection 'Lock Active To'), force the primary radio to active.
5. Using File Transfer, load the software pack into the primary radio (see SuperVisor Protected Station: Software > Primary File Transfer).
6. Confirm that the transfer is successful (see SuperVisor Protected Station: Software > Manager).
7. Distribute the software to the entire network of remote radios (see SuperVisor Protected Station: Software > Remote Distribution). If there are protected remotes in the network, they must be locked to the current active radio.

Note that the distribution process over the air will take some time, depending on RF and Transfer rate settings.

Activating the new software on the radios

1. Activate the software on the entire network of remote radios (see SuperVisor Protected Station: Software > Remote Activation).
2. Monitor the progress of the activation process until the stage where activation of all remote radios has been confirmed.

When the new software has been activated, remote stations will re-register with the base station. The remote stations software version can be verified with Network Status > Network Table.

3. If the new software version is not over the air compatible with the version currently operating on the radio, there is no need to wait as all link communication from the base station to the remote will be lost so the verification of the new version on the remote radio will fail.
4. Activate the new version software pack of the secondary radio (see Protected Station: Software > Manager).
5. Immediately after that, activate the new version software pack of the primary radio (see Protected Station: Software > Manager). Note that the activation process will take a few minutes.

Confirm that the new software version is now running on the radios

1. Re-login into the Protection Station and navigate to SuperVisor > Software>Summary.
2. Confirm that the Primary and Secondary radio current software version is now up to date
3. Confirm that the list of remote radios are now running the latest software version with Network Status > Network Table.
4. When the upgrade process is complete, if the Hardware Manual Lock switch has been used, set it to the Auto position. The software manual lock will release automatically.

Single Radio Software Upgrade

This upgrade process is for upgrading the software on a single Aprisa SR+ radio.

Note: If a radio has been configured for a Protection Type of ‘Redundant’, and that radio is no longer part of a Protected Station, the Protection Type must be changed to ‘None’ before the radio software upgrade can be achieved.

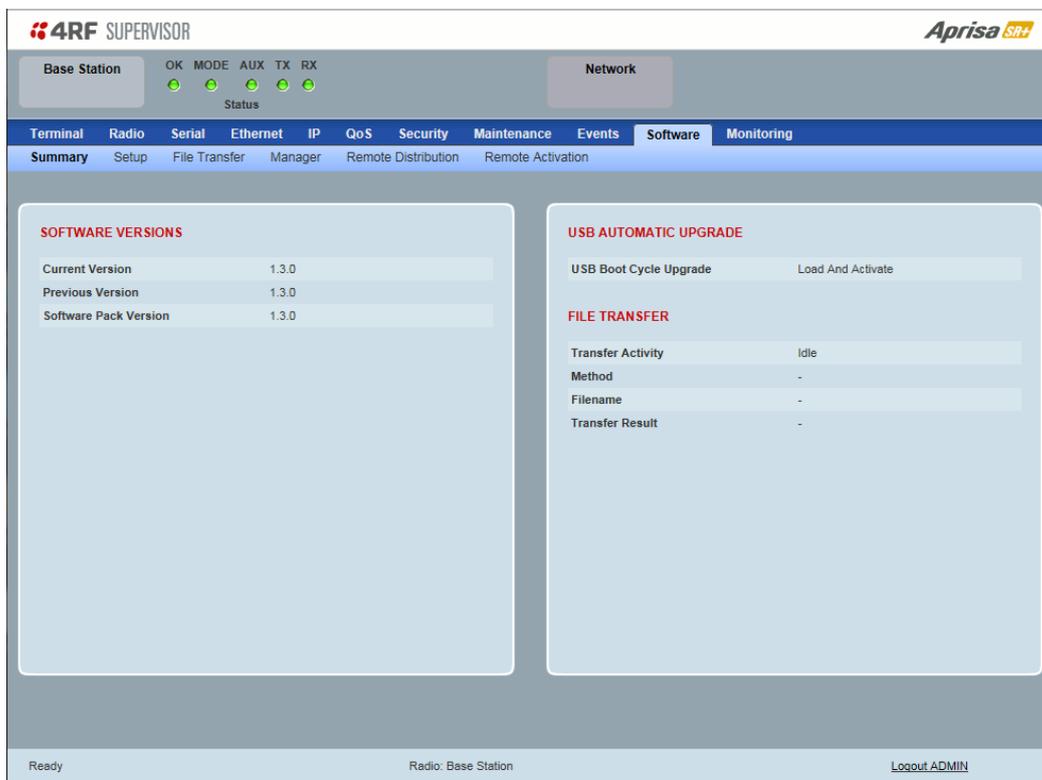
File Transfer Method

The Software Pack is loaded into the radio with the file transfer process (see SuperVisor Software > File Transfer) and activated (see SuperVisor Software > Manager).

The Aprisa SR+ upgrade operation is indicated by a flashing orange AUX LED.

To upgrade the Aprisa SR+ radio software:

1. Unzip the software release files in to the root directory of a USB flash drive.
3. Insert the USB flash drive into the host port .
4. Using File Transfer, load the software pack into the radio (see SuperVisor Software > File Transfer).
5. Remove the USB flash drive from the host port .
6. Activate the software on the radio (see SuperVisor Software > Manager).



The screenshot displays the 4RF SUPERVISOR web interface for an Aprisa SR+ radio. The interface includes a status bar at the top with indicators for Base Station, OK, MODE, AUX, TX, and RX. The main navigation menu includes Terminal, Radio, Serial, Ethernet, IP, QoS, Security, Maintenance, Events, Software, and Monitoring. The Software page is active, showing the following sections:

- SOFTWARE VERSIONS**

Current Version	1.3.0
Previous Version	1.3.0
Software Pack Version	1.3.0
- USB AUTOMATIC UPGRADE**

USB Boot Cycle Upgrade	Load And Activate
------------------------	-------------------
- FILE TRANSFER**

Transfer Activity	Idle
Method	-
Filename	-
Transfer Result	-

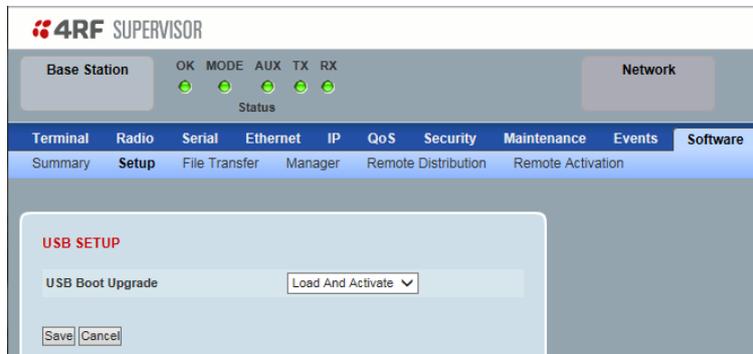
The interface also shows a status bar at the bottom with 'Ready', 'Radio: Base Station', and 'Logout ADMIN'.

USB Boot Upgrade Method

A single Aprisa SR+ radio can also be upgraded simply by plugging a USB flash drive containing the new software into the USB A host port  on the Aprisa SR+ front panel and power cycling the radio.

To upgrade the Aprisa SR+ radio software:

1. Unzip the software release files in to the root directory of a USB flash drive.
2. Check that the SuperVisor USB Boot Upgrade setting is set to 'Load and Activate' (see SuperVisor Software > Setup).



3. Power off the Aprisa SR+ and insert the USB flash drive into the host port .
4. Power on the Aprisa SR+.
5. The software upgrade process is complete when the OK LED flashes green. This can take about 2 minutes.

The software will have loaded in to the radio current software version.

6. Remove the USB flash drive from the host port .
7. Power cycle the Aprisa SR.

Login to the radio being upgraded and go to SuperVisor Software > Manager.

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

If the upgrade process did not start, the Aprisa SR+ could already be operating on the version of software on the USB flash drive. This will be indicated by flashing OK LED and then the OK, MODE and AUX will light steady green.

If the radio is not operating on the new software (after the power cycle), it could be caused by the SuperVisor 'USB Boot Upgrade' setting set to 'Load Only' (see SuperVisor Software > Setup).

In this case, go to SuperVisor see Software > Manager and tick the Software Pack 'Activate' checkbox and click 'Apply'.

If any Display Panel LED flashes red or is steady red during the upgrade process, it indicates that the upgrade has failed. This could be caused by incorrect files on the USB flash drive or a radio hardware failure.

Software Downgrade

Radio software can also be downgraded if required. This may be required if a new radio is purchased for an existing network which is operating on an earlier software release.

The downgrade process is the same as the upgrade process.

Protected Station Software Upgrade

This upgrade process is for upgrading the software on a single Aprisa SR+ Protected Station.

USB Boot Upgrade Method

Assuming the Primary radio is active and the Secondary radio is standby

1. Using the Hardware Manual Lock switch, force the primary radio to active.
2. Insert the USB flash drive with the new software release into the secondary radio host port .
3. Power cycle the secondary radio. The radio will be upgraded with the new software.
4. When the secondary radio upgrade is completed, remove the USB flash drive, power cycle the secondary radio and wait for it to become standby.
5. Using the Hardware Manual Lock switch, force the secondary radio to active.
6. Insert the USB flash drive with the new software release into the primary radio host port .
7. Power cycle the primary radio. The radio will be upgraded with the new software.
8. When the primary radio upgrade is completed, remove the USB flash drive, power cycle the primary radio and wait for it to become standby.
9. When the upgrade process is complete, set the Hardware Manual Lock switch to the Auto position. The secondary radio will remain active and the primary radio will remain standby. To set the primary radio to active, use the hardware lock switch to select the primary radio and wait for it to become active, then set the hardware manual lock switch to the Auto position.