

QoS

QoS > Summary

This page provides a summary of the QoS Settings.

4 R	F SUPERVISOR							Aprisa [
Base S	tation OK MOE	E AUX TX R	x)		Network			
erminal	Radio Serial	Ethernet	IP QoS Security	Maintenance	Events	Software	Monitoring	
ummary	Traffic Priority	Traffic Classifica	ation					
TRAFFI	C PRIORITY							
Default	Management Data Prior	ity Medium	1					
SERIAL	PRIORITY							
Port	Description		Priority					
1	Serial Port		Low					
2	Serial Port		Low					
3	USB Serial Port		Low					
ETHERN	NET PRIORITY							
Port	Description	Priority	Default Priority					
1	Ethernet Port	Low	N/A					
2	Ethernet Port	Low	N/A					
eady			Radio: B	ase Station				Logout ADMIN

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



4RF SUPERVISOR			Aprisa 🛲
Base Station OK MODE AUX T OK MODE AUX T OK MODE AUX T OK MODE AUX T OK MODE AUX T	X RX Ə	Network	
Terminal Radio Serial Ethernet	: IP <mark>QoS</mark> Security Maint	enance Events Software	Monitoring
Summary Traffic Priority Traffic Cla	ssification		
TRAFFIC PRIORITY Default Management Data Priority SERIAL PRIORITY Port Description 1 Serial Port 2 Serial Port 3 USB Serial Port	Medium V Priority Low V Low V Low V	PRIORITY DEFINITIONS PCP DSCP PCP Bit Values 1 (Background) 0 (Best Effort) 2 (Excellent Effort) 3 (Critical Application) 4 (Video)	Radio Priority Low V Low V Medium V Medium V High V
ETHERNET PRIORITY		5 (Voice) 6 (Internetwork Control)	High Very High V
Port Description Priority	Default Priority	7 (Network Control)	Very High 🔽
1 Ethernet Port Low 2 Ethernet Port Low	N/A N/A	Default All	
Save Cancel	_	Save Cancel	
Ready	Radio: Base Station	n	Logout ADMIN

TRAFFIC PRIORITY

Default Management Data Priority

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

This priority is also used for traffic if the remote serial port is not available for the radio hardware data port option e.g. if the base station is 2E2S and a remote radio is 4E0S.

SERIAL PRIORITY

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

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

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

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



ETHERNET PRIORITY

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

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

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

The default setting is Low.

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

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

Default Priority

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

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



PRIORITY DEFINITIONS

PCP (Priority Code Point)

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

<i>"</i>4RF SUPERVISOR				Aprisa 🛲
Base Station OK MODE AUX O O O Status	TX RX	Network		
Terminal Radio Serial Ether	net IP QoS Security	Maintenance Events	Software Monitoring	
Summary Traffic Priority Traffic	Classification			
TRAFFIC PRIORITY Default Management Data Priority	Medium		FINITIONS	
SERIAL PRIORITY		PCP Bit Valu	und)	
Port Description	Priority	0 (Best Effor	rt) Low 🗸	
1 Serial Port	Low	2 (Excellent	Effort) Medium 🔽	
2 Serial Port	Low 🗸	3 (Critical Ap	pplication) Medium 🗸	
3 USB Serial Port	Low	4 (Video)	High	
ETHERNET PRIORITY		5 (Voice)	High 🔽	
		6 (Internetwo	ork Control) Very High 🗸	
Port Description Priority	Default Priorit	y 7 (Network C	Control) Very High 🗸	
1 Ethernet Port Low		Default All		
Save Cancel		Save Cancel		
Ready	Radio: Bas	se Station		Logout ADMIN

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

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

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

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



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

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



DSCP (Differentiated Services Code Point)

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

4 R	F SUPERVI	SOR							Aprisa 🛲
Base S	Station	ok mod	E AUX TX O O Status	(RX)			Network		
Terminal	Radio	Serial	Ethernet	IP C	os Security	Maintenance	Events Softwar	re Monitoring	
Summary	Traffic Pi	riority	Traffic Clas	sification					
TRAFF							PRIORITY DEFINITIO	DNS	
Default	Management I	Data Priorit	tv		Medium 🗸		PCP DSCP		
			~				DSCP Bit Values	Padio Priority	
SERIAL	PRIORITY						46 EF (Expedited Fo	rwarding) Very High 🗸	
Port	Description	n		Priority			10 AF11 (Assured Fe	orwarding) High 🗸	
1	Serial Port			Low [~		12 AF12	Medium	
2	Serial Port			Low [~		14 AF13	Low	
3	USB Serial	Port		Low [~		18 AF21	High 🗸	•
FTHER	NET PRIORIT	Y					20 AF22	Medium 🔽	
							22 AF23	Low	
Port L	Ethernet Port	Priority			Default Priority		26 AF31	Very High 🗸	
2 6	Ethernet Port	Low			N/A		Default All	Previous Ne	xt
Save C	ancel								
							Save Cancel		
		_	_	_					
leady					Radio: Bas	e Station			Logout ADMIN

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

4 4RF	SUPERVISOR							Aprisa 🛲
Base Stat	tion OK	MODE AUX TX O O O Status	CRX ⊖		Netwo	rk		
Terminal	Radio Seri	al Ethernet	IP QoS	Security Mair	ntenance Events	Software	Monitoring	
Summary	Traffic Priority	Traffic Class	sification					
TRAFFIC	CLASSIFICATIO	N	_	_	_	_	_	
Select O	rder Profile Nam	e		Assigned Priority	Assigned VLAN ID	Active		
0 1	Traff Classif	ication L2 Rule 1		Medium 🔽	22	\checkmark		
0 2	Traff Classif	ication L2 Rule 2		Very High 🔽	33			
O 3	Traff Classif	ication L2 Rule 3		High 🔽	44	\checkmark		
Save Can	ceij Edit Add D	elete Delete All	Move Up Move Do	2007) 				Previous Next
Ready				Radio: Base Stati	on			Logout ADMIN

TRAFFIC CLASSIFICATION

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

Profile name

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

Assigned Priority

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

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



Assigned VLAN ID

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

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

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

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

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

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

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

Active

Activates or deactivates the profile rule.

Controls

The Save button saves all profiles to the radio.

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

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

The Add button adds a new profile,

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

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

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

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

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

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

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



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

4RF SUPERVISOR		Aprisa 🛲
Base Station OK MODE AUX TX RX O O O O O Status	Network	
Terminal Radio Serial Ethernet IP QoS	Security Maintenance Events Software Monitoring	
Summary Traffic Priority Traffic Classification		
Select Order Profile Name	Assigned Priority Assigned VLAN ID Active	
1 Traff Classification L2 Rule 1	Medium 🔽 22	
ETHERNET PORT CRITERIA Ethernet Port Any Port VLAN ID 0 PRIORITY CRITERIA Priority Type None PCP/DSCP Range 0-63 Close More options Save Cancel Edit Add Delete		Previous Next
Ready	Radio: Base Station	Logout ADMIN

ETHERNET PORT CRITERIA

Ethernet Port

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

VLAN ID

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

Enable this VLAN in the network by setting the same VLAN ID value in PVID (port VLAN ID) and in the PORT VLAN MEMBERSHIP under 'VLAN PORT SETTINGS - Port 1' on page 144. 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.
РСР	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	CSO/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.

4RF SUP	ERVISOR									Aprisa 🛲
Base Station		DE AUX TX O O O Status	RX O				Network			
Terminal Rad	io Serial	Ethernet	IP QoS	Security	Maint	tenance	Events	Softwa	re Monitoring	
Summary Traf	fic Priority	Traffic Classif	fication							
TRAFFIC CLAS	SIFICATION Profile Name			Assigned	Priority	Assigned	VLANID	Active	_	
 1 	Traff Classifica	ion L2 Rule 1		Medium	v	22				
ETHERNET POR			ETHERNE			00.00.00				0000
Ethernet Port	Any Port		Source N	IAC Address	Maak	00:00:00:	******		Source IP Address	255 255 255 255
VLANID	U		Destinati	on MAC Addr	ess	00:00:00:	00:00:00	-	Destination IP Address	0.0.0.0
PRIORITY CRITE	ERIA		Destinati	on MAC Wildo	ard	ff:ff:ff:	ff:ff:ff	_	Destination Wildcard Mask	255.255.255.255
Priority Type	None	~	Mask						IP Protocol Number	-1
PCP/DSCP Ran	ge 0-63		EtherTyp	e (HEX)		0			TCP/UDP PORT CRITERIA	
									Source Range	1-65535
									Destination Range	1-65535
Close More options										
Save Cancel E	Edit Add Delet	e								Previous Next
Ready				Radio: Ba	se Statio	n				Logout ADMIN

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: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: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'.

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'.

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'.

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'.

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
ТСР	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

4 4Rf	F SU	PERVISOR										Aprisa 🛲
Base St	ation	ок мо • •	DE AUX TO O O O Status	CRX O					Network			
Terminal	Ra	idio Serial	Ethernet	IP	QoS	Security	Mainte	enance	Events	Software	Monitoring	
Summary	Tr	affic Priority	Traffic Clas	sification								
V												
TRAFFIC	C CLA	SSIFICATION										
Select	Order	Profile Name				Assigned	Priority	Active				
0	1	Traff Classificat	tion L3 Rule 1			Low	~					
0 :	2	Traff Classificat	tion L3 Rule 2			Medium	~					
•	3	Traff Classificat	tion L3 Rule 3			High	~					
Save Ca	ancel	Edit Add Dele	te) Delete All	(Move Up)	Move Dow	vn						Previous Next
Brede						Dedies 2	e o Obeli					
Ready						Radio: Ba	se Station					Logout ADMIN

TRAFFIC CLASSIFICATION

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

Profile name

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

Assigned Priority

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

Active

Activated or deactivate the profile rule.





Controls

The Save button saves all profiles to the radio.

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

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

The Add button adds a new profile,

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

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

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

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

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

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

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



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

4RF SUPERVISOR		Aprisa su
Base Station OK MODE AUX TX RX Θ Θ Θ Θ Θ Status	Network	
Terminal Radio Serial Ethernet IP	QoS Security Maintenance Events Software M	onitoring
Summary Traffic Priority Traffic Classification		
TRAFFIC CLASSIFICATION Select Order Profile Name 1 Traff Classification L3 Rule 1 EthERNET PORT CRITERIA Ethernet Port Any Port V PRIORITY CRITERIA DSCP Range 0-63 Close More options Save Cancel Edit	Assigned Priority Active	Previous Next
Ready	Radio: Base Station	Logout ADMIN

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	CSO/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.

4RF SUPERVISOR				Aprisa 🛲
Base Station OK MODE AUX TX F OK MODE AUX TX F OK MODE AUX TX F OK MODE AUX TX F OK MODE AUX TX F	x 9	Network		
Terminal Radio Serial Ethernet	IP QoS Security Ma	intenance Events	Software Monitoring	
Summary Traffic Priority Traffic Classific	cation			
TRAFFIC CLASSIFICATION Select Order Profile Name 1 Traff Classification L3 Rule 1	Assigned Priori	ty Active ✓		
ETHERNET PORT CRITERIA	IP CRITERIA			
Ethernet Port Any Port 💌	Source IP Address	0.0.0.0		
PRIORITY CRITERIA	Source Wildcard Mask	255.255.255.255		
DSCP Range 0-63	Destination IP Address	255 255 255 255		
	Protocol Number	-1		
	TCP/UDP PORT CRITERIA			
	Source Range	1-65535		
	Destination Range	1-65535		
Close More options				
Save Cancel Edit Add Delete				Previous Next
Ready	Radio: Base Sta	tion		Logout ADMIN

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'.

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'.

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'.



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'.

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, 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
ТСР	6
UDP	17

TCP / UDP Port Criteria

Source Range

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

Destination Range

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

Examples for TCP / UDP Port Numbers:

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



Security

Security > Summary

This page displays the current settings for the Security parameters.



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



Security > Setup

4RF SUPERVISOR				Aprisa 🛲
Base Station OK MOI	DE AUX TX RX O O O O Status	Network		
Terminal Radio Serial	Ethernet IP QoS Security Maint	tenance Events So	oftware Monitoring	
Summary Setup Users	SNMP RADIUS Manager Distribution			
PAYLOAD SECURITY PROFIL	LE SETTINGS	PROTOCOL SEC	CURITY SETTINGS	
Security Profile Name	Payload Security v1	Telnet		Enabled Disabled
Security Scheme	Disabled	ICMP		Enabled Disabled
Payload Encryption Key Type	Passphrase V	HTTPS		Enabled Disabled
Payload Encryption Key Size	AES-128 V	SNMP Proxy Sup	pport	O Enabled O Disabled
Payload Encryption Key		SNMP Protocol		All Versions 🗸
Save Cancel		Save Cancel		
KEY ENCRYPTION KEY SET	FING S	SECURITY LEVI	EL SETTINGS	
Key Encryption Key Type	Raw Hexadecimal V	Security Level		Standard V
Key Encryption Key Size	AES-256 ¥	Save Cancel		
Key Encryption Key	•••••			
USB Transaction Status	USB Storage Detected			
Save Cancel	Load from USB Copy to USB			
Ready	Radio: Base Station	n		Logout ADMIN

PAYLOAD SECURITY PROFILE SETTINGS

Security Profile Name

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

Security Scheme

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

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

The default setting is Disabled.



Payload Encryption Key Type

This parameter sets the Payload Encryption Key Type:

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

The default setting is Pass Phrase.

Payload Encryption Key Size

This parameter sets the Encryption Type to AES128, AES192 or AES256. The default setting is AES128. The higher the encryption size the better the security.

Payload Encryption Key

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

Pass Phrase

Good password policy:

- contains at least eight characters, and
- contains at least one upper case letter, and
- contains at least one lower case letter, and
- contains at least one digit 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 key must comply with the specified encryption key size e.g. if Encryption Type to AES128, the encryption key must be 16 bytes (32 chars).



KEY ENCRYPTION KEY SETTINGS

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

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

Key Encryption Key Type

This parameter sets the Payload Encryption Key Type:

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

The default setting is Pass Phrase.

Key Encryption Key Size

This parameter sets the Encryption Type to AES128, AES192 or AES256. The default setting is AES128. The higher the encryption type the better the security.

Key Encryption Key

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

USB Transaction Status

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

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

Note: Some brands of USB flash drives may not work with 4RF radios.

Controls

The 'Save' button saves the Key Encryption Key settings to the radio. If the Security Level is set to Strong (see 'Security Level' on page 191), this button will be grayed out.

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

The 'Copy To USB' button copies the Key Encryption Key settings to a file called 'asrkek.txt' on the USB flash drive. This settings file can be used to load into other radios. If a USB flash drive is not detected or the Security Level is set to Strong (see 'Security Level' on page 191), this button will not be shown.



Key Encryption Key Summary

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

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



PROTOCOL SECURITY SETTINGS

Telnet option

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

ICMP option (Internet Control Message Protocol)

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

HTTPS option

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

SNMP Proxy Support

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

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

SNMP Protocol

This parameter sets the SNMP Protocol:

Option	Function
Disabled	All SNMP functions are disabled.
All Versions	Allows all SNMP protocol versions.
SNMPv3 Only	Only SNMPv3 transactions will be accepted.
SNMPv3 With Authentication Only	Only SNMPv3 transactions authenticated using HMAC-MD5 or HMAC-SHA will be accepted (as per table below).
SNMPv3 With Encryption Only	Only SNMPv3 transactions with an encrypted type of DES or AES will be accepted (as per table below).

The default setting is All Versions.

The default SNMPv3 with Authentication User Details provided are:

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

SNMPv3 Authentication Passphrase

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

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

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

Generate New Keys from SNMPv3 USM User Passphrases

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

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

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

To change a user authentication passphrase:

The following are examples of:

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

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

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

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

Changing the desUserSHA user encryption key / password from desUserSHA to desUserSHANew:

c:\usr\bin>snmpusm -v 3 -u desUserSHA -n priv -l authPriv -a SHA -A desUserSHA -x DES -X desUserSHA -cx 172.17.70.17 passwd desUserSHA desUserSHANew

Changing the desUserSHA user authentication key / password from desUserSHA to desUserSHANew:

c:\usr\bin>snmpusm -v 3 -u desUserSHA -n priv -l authPriv -a SHA -A desUserSHA -x DES -X desUserSHANew -Ca 172.17.70.17 passwd desUserSHA desUserSHANew

Changing the privUserMD5 user encryption key / password from privUserMD5 to privUserMD5New:

c:\usr\bin>snmpusm -v 3 -u privUserMD5 -n priv -l authPriv -a MD5 -A privUserMD5 -x AES -X privUserMD5 -Cx 172.17.70.17 passwd privUserMD5 privUserMD5New

Changing the privUserMD5 user authentication key / password from privUserMD5 to privUserMD5New:

c:\usr\bin>snmpusm -v 3 -u privUserMD5 -n priv -l authPriv -a MD5 -A privUserMD5 -x AES -X privUserMD5New -Ca 172.17.70.17 passwd privUserMD5 privUserMD5New



Changing the desUserMD5 user encryption key / password from desUserMD5 to desUserMD5New:

c:\usr\bin>snmpusm -v 3 -u desUserMD5 -n priv -l authPriv -a MD5 -A desUserMD5 -x DES -X desUserMD5 -Cx 172.17.70.17 passwd desUserMD5 desUserMD5New

Changing the desUserMD5 user authentication key / password from desUserMD5 to desUserMD5New:

c:\usr\bin>snmpusm -v 3 -u desUserMD5 -n priv -l authPriv -a MD5 -A desUserMD5 -x DES -X desUserMD5New -Ca 172.17.70.17 passwd desUserMD5 desUserMD5New

Changing the authUserSHA user authentication key / password from authUserSHA to authUserSHANew:

c:\usr\bin>snmpusm -v 3 -u authUserSHA -n auth -l authNoPriv -a SHA -A authUserSHA -Ca 172.17.70.17 passwd authUserSHA authUserSHANew

Changing the authUserMD5 user authentication key / password from authUserMD5 to authUserMD5New:

c:\usr\bin>snmpusm -v 3 -u authUserMD5 -n auth -l authNoPriv -a MD5 -A authUserMD5 -Ca 172.17.70.17 passwd authUserMD5 authUserMD5New

Notes

-Cx option is to change the Encryption key/password

-Ca option is to change the Authentication key/password

Other information on this utility can be obtained from the utility command help itself or online

Summary

It is necessary to record the new passphrases loaded into the Aprisa SR+ radios and then load the passphrases into the SNMP manager. There is a separate passphrase for the two supported forms of authentication (MD5 and SHA1) only as well as the two forms of authentication used in combination the two forms of encryption (DES and AES). It is vital to change all passphrases even if the depreciated mechanism are not used (MD5 and DES) otherwise an attacker could still use the default passphrases.



Reset Unknown Passphrases with the Command Line Interface

As it is not possible for users to read previously set passphrases, a CLI command is available from Aprisa SR+ software release 1.4.0 to 'reset' the SNMPv3 USM users back to defaults.

Note: USM users are not related to CLI and SuperVisor users. This command will only be accessible to the CLI 'admin' user logins.

To reset unknown passphrases:

- 1. Telnet into each radio in the network and via the CLI reset the passphrases
- 2. Login to the radio with:

Login: admin

Password: ********

- 3. Set all SNMP3 users to default values with the 'snmpusm reset' command (see 'SNMP3 users to default values' below for the list of default values).
- 4. Reboot the radio with the 'reboot' command.



SECURITY LEVEL SETTINGS

Security Level

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

Option	Payload Encryption	HTTPS	SNMPv3	USB KEK Only
Standard	~	~	~	
Strong	~	\checkmark	~	\checkmark

If the Security Level is reduced, there will be a pop up message warning that Key Encryption Key will be reset to the default value.

CONFIRMATION	
WARNING:	
Lowering the security level will reset the Key Encryption Key on this radio. This may affect compatibility of future over the air security profile distributions.	
Press OK to continue anyway or Cancel.	
OK Cancel]

If the Security Level is increased, there will be a pop up message reminding user to enter a new Key Encryption Key.



If the Security Level is set to Strong, the 'Save' button will be grayed out and the 'Copy To USB' button will not be shown.

SNMPv3 Context Addressing

SNMPv3 is not user configurable and user can use this option with any NMS. The radio SNMP management interface supports SNMPv3/2 context addressing. The SNMv3 context addressing allows the user to use secure SNMPv3 management while improving NMS performance.

A NMS (Network Management System) can access any remote radio directly by using its IP address or via the base / master station SNMPv3 context addressing. The SNMPv3 context addressing can compress the SNMPv3 management traffic OTA (Over The Air) to the remote station by up to 90% relative to direct OTA SNMPv3 access to remote station, avoiding the radio narrow bandwidth traffic loading.



Security > Users

#4RF SUPERV	ISOR	Aprisa 📶
Base Station	OK MODE AUX TX RX Network O O O O O Status	
Terminal Radio Summary Setup	Serial Ethernet IP QoS Security Maintenance Events Software Monitoring Users SNMP RADIUS Manager Distribution	
ſ	USER DETAILS	
	Select Username Password Privilege O admin ADMIN ✓ Save Delete Cancel Cancel Cancel	
	ADD NEW USER	
	Add Cancel	
Ready	Radio: Base Station	Logout ADMIN

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

USER DETAILS

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

ADD NEW USER

To add a new user:

1. Enter the Username.

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

2. Enter the Password.

A password can be 8 to 32 printable characters but cannot contain a tab. Passwords are case sensitive.

Good password policy:

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



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

The default login is 'admin'.

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

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

See 'SuperVisor Menu Access' on page 80 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

	SUK			Aprisa 🔤
Base Station	OK MODE AUX TX RX O O O O O Status	Network	t.	
erminal Radio	Serial Ethernet IP QoS Security	Maintenance Events	Software Monitoring	
antination and a second				
ACCESS CONTROL	SETUP			
Туре	Community String	_		
Read Only	public			
Read/Write	private			

In addition to web-based management (SuperVisor), the network can also be managed using the Simple Network Management Protocol (SNMP) using any version of SNMP v1/2/3. MIB files are supplied, and these can be used by a dedicated SNMP Manager, such as Castle Rock's SNMPc, to access most of the radio's configurable parameters.

For communication between the SNMP manager and the radio, Access Controls and Community strings must be set up as described in the following sections.

A SNMP **Community String** is used to protect against unauthorized access (similar to a password). The SNMP agent (radio or SNMP manager) will check the community string before performing the task requested in the SNMP message.

ACCESS CONTROL SETUP

A SNMP Access Control is the IP address of the radio used by an SNMP manager or any other SNMP device to access the radio. The Aprisa SR+ allows access to the radio from any IP address.

Read Only

The default Read Only community string is public.

Read Write

The default ReadWrite community string is private.



SNMP Manager Setup

The SNMP manager community strings must be setup to access the base station and remote / repeater stations.

To access the base station, a community string must be setup on the SNMP manager the same as the community string setup on the radio (see 'Security > SNMP' on page 194).

SNMP access to remote / repeater stations can be achieved by using the radio's IP address and the normal community string or by proxy in the base station.

SNMP Access via Base Station Proxy

To access the remote / repeater stations via the base station proxy, the community strings must be setup on the SNMP manager in the format:

ccccccc:bbbbbb

Where:

cccccccc is the community string of the base station

and

bbbbbb is the last 3 bytes of the remote station MAC address (see 'Network Status > Network Table' on page 271).

The SNMP Proxy Support must be enabled for this method of SNMP access to operate (see 'SNMP Proxy Support' on page 187).


Security > RADIUS

This page displays the current settings for the Security RADIUS.

4RF SUPERVISOR						Aprisa 🛲
Base Station OK MODE AN	JX TX RX O O O Is		Network			
Terminal Radio Serial Eth	ernet IP QoS Security	Maintenance E	vents Softwa	re Monitoring		
Summary Setup Users SNM	IP RADIUS Manager Distrit	oution				
RADIUS AUTHENTICATION SETTIN	IGS	RA	DIUS SERVER SE	ETTINGS		
Authentication Mode	Local Authentication	~	Server Name	IP Address	Port Number	Encryption Key
Primary Server	None V	1	Radius Server 1	0.0.0.0	312	•••••
Secondary Server	None V	2	Radius Server 2	0.0.0.0	312	•••••
		3	Radius Server 3	0.0.0.0	313	•••••
RADIUS ACCOUNTING SETTINGS		4	Radius Server 4	0.0.0.0	313	•••••
Drimony Server	None	Sav	Cancel			
Cocondani Conior	None					
Secondary Server	None					
RADIUS ADVANCED SETTINGS						
Initial Transaction Timeout(s)	4					
Default Transaction Timeout(s)	16					
Maximum Retries	5					
Maximum Retries Duration (s)	30					
Unknown Transaction Attributes	Ignore And Authenticate 🗸					
Save Cancel						
Ready	Radio: Base	Station				Logout ADMIN

RADIUS - Remote Authentication Dial In User Service

RADIUS is a client / server system that secures the radio link against unauthorized access. It is based on open standard RFCs: RFC 2865/6, 5607, 5080 and 2869. It is used for remote user Authorization, Authentication and Accounting.

When a user logs into a radio with RADIUS enabled, the user's credentials are sent to the RADIUS server for authentication of the user.

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

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

Admin Level = 4 Technician Level = 2 Viewer Level = 1

A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.



RADIUS AUTHENTICATION SETTINGS

Authentication Mode

This parameter sets the Authentication Mode.

Option	Function
Local Authentication	No radius Authentication - allows any local user privilege
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

4RF SUPERV	ISOR		Aprisa 🛲
Base Station	OK MODE AUX TX RX ⊖ ⊖ ⊖ ⊖ ⊖ Status	Network	
Terminal Radio	Serial Ethernet IP QoS Security	Maintenance Events	Software Monitoring
Summary Setup	Users SNMP RADIUS Manager D	istribution	
CURRENT PAYLOA	D SECURITY PROFILE	PREDEFINE	ED PAYLOAD SECURITY PROFILE
Profile Name	Migrated Key	Profile Name	e Payload Security v22
Status	Active	Status	Available
		Activate	
PREVIOUS PAYLOA	D SECURITY PROFILE	Apply Cance	el
Profile Name	Unknown		
Status	Inactive	_	
Activate			
Apply Cance			
Ready	Radio: B	lase Station	Logout ADMIN

CURRENT PAYLOAD SECURITY PROFILE

Profile Name

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

Status

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

PREVIOUS PAYLOAD SECURITY PROFILE

Profile Name

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

Status

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

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



Activate

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

PREDEFINED PAYLOAD SECURITY PROFILE

Profile Name

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

Status

This parameter displays the status of the new security profile.

Option	Function
Unavailable	A predefined security profile is not available on this radio. To create a predefined security profile, go to 'Security > Setup' on page 183.
Available	A predefined security profile is available on this radio for distribution and activation.



Security > Distribution

4RF SUPERVISOR				Aprisa 🛲
Base Station OK MODE AUX TX RX Θ Θ Θ Θ Θ Status		Network		
Terminal Radio Serial Ethernet IP QoS	Security Maintenance	Events Software	Monitoring	
Summary Setup Users SNMP RADIUS Mana	ager Distribution			
REMOTE PAYLOAD SECURITY PROFILE DISTRIBUTION		REMOTE PAYLOAD SE	CURITY PROFILE ACTIVATION	
Predefined Profile Name Payload Security v22		Profile Name	Payload Security v22	
Status Available		Start Activation		
Start Transfer				
Apply Cancel				
A WARNING: Using the default Key Encryption Key is not secure				
Ready	Radio: Base Station		Log	out ADMIN

REMOTE PAYLOAD SECURITY PROFILE DISTRIBUTION

Predefined Profile Name

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

Status

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

Option	Function
Unavailable	A predefined payload security profile is not available on this radio.
Available	A predefined payload security profile is available on this radio for distribution and activation.

Start Transfer

This parameter when activated distributes (broadcasts) the new payload security profile to all remote stations in the network.

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

Payload security profile distribution traffic is classified as 'management traffic' but does <u>not</u> use the Ethernet management priority setting. Security profile distribution traffic priority has a fixed priority setting of 'very low'.



To distribute the payload security profile to remote stations:

This process assumes that a payload security profile has been setup (see 'Security > Setup' on page 183).

1. Tick Start Transfer and click Apply.



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

2. When the distribution is completed, activate the software with the Remote Payload Security Profile Activation.



REMOTE PAYLOAD SECURITY PROFILE ACTIVATION

When the security profile has been distributed to all the remote stations, the security profile is then activated in all the remote stations with this command.

The base station will always attempt to distribute the profile successfully. This broadcast distribution has its own retry mechanism. The user can find out if all the remote radios have the latest profile when the managed activation process is attempted. A pop up confirmation will be shown by SuperVisor with relevant information and the user can decide to proceed or not. The user can attempt to redistribute again if needed. If the decision is made to continue, on completion of the activation process, communication with the remote radios that did not have the new security profile will be lost.

Predefined Profile Name

This parameter displays the predefined security profile available for activation on all remote stations.

To activate the security profile in remote stations:

This process assumes that a security profile has been setup into the base station (see 'Security > Setup' on page 183) and distributed to all remote radios in the network.

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

1. Click Start Activation

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

Result	Function (X of Y)
Remote Radios Polled for New Profile	X is the number of radios polled to determine if the radio contains the new security profile.
	Y is the number of remote radios registered with the base station.
Remote Radios Activated	X is the number of radios activated.
	Y is the number of radios with the new security profile requiring activation.
Remote Radios On New Profile	X is the number of radios activated and on the new security profile.
	Y is the number of radios with the new security profile that have been activated.

When the activation is ready to start:

CONFIRMATION
Activation step is about to start. All 2 radios will be activated.
WARNING: The activation process may take up to 1 minute for each radio. Do not leave this page until the activation step has completed. When at least 1 remote activation has been successfully sent, the security profile of this radio will automatically be updated.
OKCancel

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



Maintenance

Maintenance > Summary

This page displays the current settings for the Maintenance parameters.

GARF SUPERVISOR				Aprisa 🛲
Base Station OK MODE AU OK MODE AU Status	X TX RX Θ Θ Θ	Network		
Terminal Radio Serial Ethe	rnet IP QoS Security	Maintenance Events	Software Monitoring	
Summary General Test Mode	Modem Defaults Licence	Advanced		
GENERAL		UPGRADE		
Local Status Polling Period (s)	10	USB Boot C	ycle Upgrade L	oad And Activate
Remote Status Polling Period (s)	20			
Network View Polling Period (s)	20	TEST MODE	ŧ	
Inactivity Timeout (min)	1440 (24h)	Packet Resp	oonse Timeout (ms)	3000
Frequency Tracking	Enabled	Transmit Pe	riod (s) 5	5
		R\$SI ENTER	Button Timeout (s)	500
NETWORK		Transmitter	Timeout (s) 1	10
Node Registration Retry (s)	10			
Announcement Period (min)	1440	LICENCE		
Node Missed Poll Count	3	Remote Man	agement F	Enabled
		Ethernet OT	A E	Enabled
		SNMP	E	Enabled
Ready	Radio: Ba	se Station		Logout ADMIN

DIAGNOSTICS

Last RX Packet RSSI (dBm)

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



GENERAL

Local Status Polling Period (sec)

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

Remote Status Polling Period (sec)

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

Network View Polling Period (sec)

This parameter displays the rate at which SuperVisor polls all remote radios for status and alarm reporting.

Inactivity Timeout (min)

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

Frequency Tracking

This parameter displays if Frequency Tracking is enabled or disabled.



NETWORK

Node Registration Retry (sec)

This parameter displays the base station poll time at startup or the remote / repeater station time between retries until registered.

Base Station Announcement Period (min)

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

Node Missed Poll Count

This parameter displays the number of times the base station attempts to poll the network at startup or if a duplicate IP is detected when a remote / repeater station is replaced.

UPGRADE

USB Boot Cycle Upgrade

This parameter shows the type of USB Boot Cycle upgrade defined in 'Software Setup > USB Boot Upgrade' on page 237.

TEST MODE

Packet Response Timeout (ms)

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

Transmit Period (sec)

This parameter displays the time between Test Mode requests to the base station.

Response Timeout (ms)

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

RSSI Enter Button Timeout (sec)

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

Transmitter Timeout (sec)

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



LICENCE

Remote Management

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

Ethernet OTA (over the air)

This parameter displays if Ethernet traffic is enabled or disabled. The Ethernet OTA will be enabled if the Ethernet feature licence has been purchased (see 'Maintenance > Licence' on page 216).

SNMP Management

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



Maintenance > General

4RF SUPERVISOR			Aprisa 📟
Base Station OK MODE AUX O O O Status	CTX RX O O	Network	
Terminal Radio Serial Ether	rnet IP QoS Security Maintenan	ce Events Software Mo	onitoring
Summary General Test Mode	Modem Defaults Licence Advanced		
GENERAL Local Status Polling Period (s) Remote Status Polling Period (s) Network View Polling Period (s) Inactivity Timeout (min) Delete Alarm History File Save Cancel	10 20 20 1440 (24h) V	REBOOT Reboot Save [Cance]	
Ready	Radio: Base Station		Logout ADMIN

GENERAL

Local Status Polling Period (sec)

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

Network View Polling Period (sec)

This parameter sets the rate at which SuperVisor polls all remote radios for status and alarm reporting. The default setting is 20 seconds.

Remote Status Polling Period (sec)

This parameter sets the rate at which SuperVisor refreshes the Remote Radio alarm LED states and RSSI value. To avoid problems when managing Aprisa SR+ Networks, ensure that the Remote Polling Period is set to be longer than the Inband Management Timeout (set on page 88). The default setting is 20 seconds.

Inactivity Timeout (min)

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

Delete Alarm History file

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



REBOOT

To reboot the radio:

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

REBOOT	
Reboot	
Save Cancel	

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

CONFIRMATION
Please Confirm Reboot.
OK Cancel

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

All the radio LEDs will flash repeatedly for 1 second.

The radio will be operational again in about 10 seconds.

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

5. Login to SuperVisor.



Maintenance > Test Mode

4RF SUPERVISOR			Aprisa 🛲
Base Station OK MOD	DE AUX TX RX $\Theta \Theta \Theta$ Status	Network	
Terminal Radio Serial	Ethernet IP QoS Securit	Maintenance Events Software	e Monitoring
TRANSMITTER PRBS Test Enabled Deviation Test Enabled CW Test Enabled Test mode Timeout (s) Save Cancel		RSSI ENTER BUTTON Response Timeout (ms Transmit Period (s) Test mode Timeout (s) Save Cancel	a) 3000 5 600
Ready	Radio:	Base Station	Logout ADMIN

TRANSMITTER

PRBS Test Enabled

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

Deviation Test Enabled

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

CW Test Enabled

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

Test Mode Timeout (s)

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



RSSI TEST BUTTON

Response Timeout (ms)

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

Transmit Period (sec)

This parameter sets the time between RSSI Test Mode requests to the base station. The default setting is 5 seconds.

Test Mode Timeout (s)

This parameter sets the RSSI Test Mode timeout period. The radio will automatically exit RSSI Test Mode after the Timeout period. The default setting is 600 seconds.



Maintenance > Modem

Base Station

4RF SUPERV	ISOR						Aprisa
Base Station	OK MODE AUX TX RX O O O O O Status			Network			-
Terminal Radio Summary General	Serial Ethernet IP Test Mode Modem	QoS Security Defaults Licence	Maintenance Advanced	Events	Software	Monitoring	
FEC DISABLE FEC Disable Duration (s) [Apply] Cancel	Disable 🗸						
	_	_					
Ready	_	Radio: Ba	se Station			_	Logout ADMIN

FEC DISABLE

FEC Disable

This diagnostic function allows the user to temporarily disable forward error correction on the channel when diagnosing problems on the link.

Therefore, enabling this diagnostic function would temporarily disable FEC on the channel and the associated maintenance mode alarm would activate.

Note that the opposite is not true for this diagnostic function. In other words, this diagnostic function does not provide the user with the option to temporarily enable forward error correction on the channel.

All diagnostic functions are not persistent and will be return to disabled states should the system restart.

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

Duration (s)

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



Remote Station

<i>"</i>4RF SUPERVISOR			Aprisa 🛲
Remote Radio OK MODE AUX TX RX Θ Θ Θ Θ Θ Θ Status			
Terminal Radio Serial Ethernet IP	QoS Security Maintenance	Events Software Monitoring	
Summary General Test Mode Modem	Defaults Protection Licence	Advanced	
ADAPTIVE CODING MODULATION ACM Lock Default ACM Lock to Default Duration (s) 0 Current Modulation Type OPSK Apply Cancel FEC Disable FEC Disable Disable Duration (s) 0 Apply Cancel			
Ready	Radio: Remote Radio		Logout ADMIN

ADAPTIVE CODING AND MODULATION

ACM Lock

This parameter sets whether adaptive modulation can be locked or not.

Option	Function
Disable	Disables manual locking of the adaptive modulation i.e. allows for automatic adaptive modulation.
Enable	Allows the adaptive modulation to be manually locked
Timer	Allows the adaptive modulation to be manually locked but only for a predetermined period.

ACM Lock To

This parameter manually locks the adaptive modulation.

Option	Function
Default	Manually locks the adaptive modulation to the default modulation defined in 'Default Modulation' on page 113.
Current	Manually locks the adaptive modulation to the current modulation at that time.

Duration (s)

This parameter defines the period required for manually locking the adaptive modulation. When this period elapses, the adaptive modulation becomes automatic.



FEC DISABLE

FEC Disable

This diagnostic function allows the user to temporarily disable forward error correction on the channel when diagnosing problems on the link.

Therefore, enabling this diagnostic function would temporarily disable FEC on the channel and the associated maintenance mode alarm would activate.

Note that the opposite is not true for this diagnostic function. In other words, this diagnostic function does not provide the user with the option to temporarily enable forward error correction on the channel.

All diagnostic functions are not persistent and will be return to disabled states should the system restart.

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

Duration (s)

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



Maintenance > Defaults

4RF SUPERVISOR		Aprisa 🛲
Base Station OK MODE AUX TX RX O O O O O O Status	Network	
Terminal Radio Serial Ethernet IP	QoS Security Maintenance Events Software Moni	itoring
Summary General Test Mode Modem	Defaults Licence Advanced	
DEFAULTS Restore Factory Defaults Save User Defaults Restore User Defaults Save Cancel		
Ready	Radio: Base Station	Logout ADMIN

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

#4RF SUPER	VISOR						Aprisa 📶
Base Station	OK MODE AUX TX RX O O O O O Status			Network	< .		
Terminal Radio Summary Genera	Serial Ethernet IP Test Mode Modem	QoS Security Defaults Licence	Maintenance Advanced	Events	Software	Monitoring	
LICENCE Ethernet OTA Add Licence Save Cancel	Enabled						
Busy		Radio: Bas	e Station	_			Logout ADMIN

LICENCE

Fully Featured Radio

When a fully featured Aprisa SR+ radio is purchased (indicated by the \underline{AA}), it contains the licences which activate Remote Management, Ethernet Traffic, and SNMP Management e.g.

Part NumberPart DescriptionAPSQ-N400-SSC-HD-22-ENAA4RF SR+, BR, 400-470 MHz, SSC, Half Duplex, 2E2S, EN, STD

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



Maintenance > Advanced

4RF SUPERVISOR				Aprisa 🛲
Base Station OK MODE A	UX TX RX O O O us	Netwo	rk	
Terminal Radio Serial Etl	hernet IP QoS Secu	rity Maintenance Events	Software Monitoring	
Summary General Test Mode	Modem Defaults Lice	ence Advanced		
NETWORK Node Registration Retry (s)	10	MAINTEN	ANCE FILES	
Announcement Period (min)	1440	Action	Save to PC V	Retain IP Address
Node Missed Poll Count	3	Status	Idle	
Discover Nodes		Apply Ca	ancel	
Decommission Node		_		
Broadcast Time				
Save Cancel				
Frequency Tracking	Enabled V			
[Save] [Cancel]				
Ready	Rac	lio: Base Station		Logout ADMIN

NETWORK

Node Registration Retry (sec)

This parameter sets the base station poll time at startup or the remote / repeater station time between retries until registered. The default setting is 10 seconds.

Base Station Announcement Period (min)

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

When a new base station powers on, it announces its presence and each remote that receives the announcement message will be advised that a new base station is present and that they should re-register. This allows the new base station to populate its Network Table, with knowledge of the nodes in the network.

If, during this initial period, there is some temporary path disturbance to one or more remotes, they may miss the initial announcement messages and be left unaware of the base station change. For this reason, the base station must periodically send out announcement messages to pick up any stray nodes and the period of these messages is the base station Announcement Period.

Setting this parameter to 0 will stop periodic announcement messages being transmitted.

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



Node Missed Poll Count

This parameter sets the number of times the base station attempts to poll the network at startup or if a duplicate IP is detected when a remote / repeater station is replaced. The default setting is 3.

Discover Nodes

This parameter when activated triggers the base station to poll the network with Node Missed Poll Count and Node Registration Retry values.

Decommission Node(s)

This parameter when activated resets the network registrations to remove the entire network from service.

Note: Take care using this option.

Broadcast Time

This parameter when activated sends the base station Date / Time setting to all the remote and repeater stations in the network and sets their Date / Time. This option applies to the base station only.

Automatic Route Rediscovery

This parameter enables the radio to transmit route discovery messages when packets are unacknowledged.

When enabled, unacknowledged unicast packets are converted into uni-broadcast messages and sent through the network. All nodes see the message and populate their routing tables accordingly.

When the destination node is reached, it sends a route response message via the shortest path. The intermediate nodes see this message and populate their routing tables in the reverse direction, thus reestablishing the route.

The default setting is disabled.

GENERAL

Frequency Tracking

Frequency Tracking enables the receiver to track any frequency drift in the transmitter to maintain optimum SNR and radio link performance over the full temperature range.

When enabled, remote stations adjust their receive frequency to the frequency of the incoming packet rate and the base station notifies remote stations if their transmit frequency requires adjustment.

The default setting is Enabled.



×

MAINTENANCE FILES

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

Note: Some brands of USB flash drives may not work with 4RF radios.

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.

Do you want to open or save config.4 (138 KB) from 173.10.1.16? Open Save 🔻 Cancel

Save to Radio USB	This saves the file with a filename of 'asrcfg_1.6.0' 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.

Do you want to open or save info.tar.	gz (19.0 KB) from 173.10.1.30 ?	Open	Save	▼ Cancel	×
Save to Radio USB	This saves the file with a filename 'alarm_173.10.1.30_2014-11-10,15 radio USB flash drive root director	of e.g. 5.54.14.txt y.	t' to a te	ext file on	the



File - Configuration Script

Action

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

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

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

Retain IP Address

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

Revert Config if Connection Lost

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

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



Events

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

Events > Alarm Summary

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

1. Alarm Events

Alarm Events are generated to indicate a problem on the radio.

2. Informational Events

Informational Events are generated to provide information on key activities that are occurring on the radio. These events do not indicate an alarm on the radio and are used to provide information only.

See 'Alarm Types and Sources' on page 368 for a complete list of events.

Base Station OK MODE AUX TX RX Status Status Terminal Radio Radio Serial Ethernet IP QoS Security Maintenance Events Software Monitoring Alarm J/O Setup Event Action Setup Defaults Alarm Summary Event History Events Setup Events Setup Alarm I/O Setup Event Action Setup Defaults Alarm Summary Event History Events Setup Frage Station Carsonini Petition Component Failure Events Supply Network Software Radio Interface Path Component Failure Component Failure Component Failure Component Failure Component Failure Component Failure Event Supply Software Radio Interface Path Event Setup III Component Failure Radio Interface Path Event Action Setup III Component Failure Event Setup III Component	4RF SUPER	VISOR			Aprisa Sm
Terminal Radio Serial Ethernet IP QoS Security Maintenance Events Software Monitoring Alarm Summary Event History Events Setup Alarm I/O Setup Event Action Setup Defaults ALARM SUMMARY P Base Station • Reserve Path • Reserve Path • Component Failure • Oligonostic • Software • Alarm inputs • Protection • Protection • Protection 	Base Station	OK MODE AUX TX RX OOOOOO Status		Network	-
Alarm Summary Event History Events Setup Traps Setup Alarm V/O Setup Event Action Setup Defaults ALARM SUMMARY • ● Base Station • ● Transmit Peth • ● Receive Peth • ● Component Failure • ● Dilegnostic • ● Protection • ● Protection	Terminal Radio	Serial Ethernet IP	QoS Security Maintenance	Events Software Monitoring	
ALARM SUMMARY	Alarm Summary	Event History Events Setup	Traps Setup Alarm I/O Setup	Event Action Setup Defaults	
	ALARM SUMMARY	ath th face Path iquipment (nterface Path Failure \$			
	_				
	Ready		Radio: Base Station		Logout ADMIN

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

	4 R	F SUPERVISOR						Aprisa 🛲
	Base S	itation OK MC	DDE AUX	TX RX O O			Network	
Te	rminal	Radio Serial	Ethern	et IP QoS Security	Mainte	enance	Events Software Monitoring	
Ala	arm Sur	mmary Event Hist	tory Ev	ents Setup Traps Setup	Alarm I/O	Setup E	vent Action Setup Defaults	
E	EVENT	HISTORY						
	Log ID	Date/time	Event ID	Description	State	Severity	Additional Information	
	623	01/05/2015 21:08:15	55	Terminal Unit Information	inactive	information	New Registration: Remote Radio (172.10.1.19) joined the network
	622	01/05/2015 21:07:28	26	User authentication succeeded	inactive	information	SuperVisor, User admin, Local authentication	OK, IP Addr 172.10.1.1
	621	01/05/2015 21:01:50	30	Software Start Up	inactive	information	Power on Reset	
	620	01/05/2015 21:04:37	39	Software Restart Required	active	warning	Compatibility Operating Mode changed to Sta	ndard Mode
	619	01/05/2015 21:04:36	39	Software Restart Required	active	warning	Operating Mode Changed	
	618	01/05/2015 21:02:38	26	User authentication succeeded	inactive	information	SuperVisor, User admin, Local authentication	OK, IP Addr 172.10.1.1
	617	01/05/2015 21:02:17	65	Event Action Activity	inactive	information	Event action request to 127.0.0.1. Alarm output	ut #1 Activation (Confirmed).
	616	01/05/2015 21:02:17	65	Event Action Activity	inactive	information	Alarm output #1 Activated.	
								Auto Refresh Prev Next
Re	ady			Radio: B	ase Statior	n		Logout ADMIN

EVENT HISTORY

The last 1500 events are stored in the radio. The complete event history list can be downloaded to a USB flash drive (see 'File - Event History Log' on page 220).

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

4RF SUPERVISOR				Aprisa 🛲
Base Station OK MODE AUX OK MODE AUX OK MODE AUX OK MODE AUX OK Status	TX RX O O	Network		
Terminal Radio Serial Etherne	et IP QoS Security	Maintenance Events Softw	are Monitoring	
Alarm Summary Event History Even	nts Setup Traps Setup	Alarm I/O Setup Event Action Setup	Defaults	
EVENTS SETUP				
ID Name	Severity Suppress	Lower Limit Upper Limit	Units Duration Unit	s
1 PA Current	critical V none	✓		
61 PA Driver Current	critical V none	✓		
62 PA Stability	warning V none	<u> </u>		
2 TX AGC	critical V none	✓		
60 TX Forward Power	warning V none	<u> </u>		
3 TX Reverse Power	warning V none			
4 Temperature Threshold	warning V none	✓ -30.0 75.0	Celsius	
Save Cancel	Linucai V Inorie	_		Prev Next
Ready	Radio: B	ase Station		ogout ADMIN

EVENTS SETUP

Alarm event parameters can be configured for all alarm events (see 'Alarm Events' on page 369).

All active alarms for configured alarm events will be displayed on the Monitoring pages (see 'Monitoring' on page 253).

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

Severity

The Severity parameter sets the alarm severity.

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



Information

No problem indicated - purely information



Suppress

This parameter determines if the action taken by an alarm.

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

Lower Limit / Upper Limit

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

Example: 9 RX CRC Errors

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

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

Units (1)

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

Duration

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

Units (2)

This parameter shows the unit for the Duration parameters.

Switch

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

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

Block

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

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

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



Events > Traps Setup

4RF SUPERVISO	R						Αρ	risa <mark>&</mark>
Base Station	MODE AUX	TX RX O O		Network				
erminal Radio S	erial Etherne	et IP QoS Security	Maintenance	Events So	ftware Monitorin	g		
Jarm Summary Event	History Ever	nts Setup Traps Setup	Alarm I/O Setup	Event Action Set	up Defaults			
TRAPS SETUP	_		_	_		_	_	
Destination Address	Port	Community String		Notification Mode	Notification Type	Timeout (seconds)	Maximum Retries	Enabled
192.168.0.20	162	public11	E	vent Recorded 🗸	Standard Trap 🗸	5	3	✓
192.168.0.21	162	public22	E	vent Recorded 🗸	Inform Request 🗸	5	3	\checkmark
0.0.0.0	162	public	E	vent Recorded 🗸	Standard Trap 🗸	5	3	
0.0.0.0	162	public	E	vent Recorded 🗸	Standard Trap 🗸	5	3	
0.0.0.0	162	public	E	vent Recorded 🗸	Standard Trap 🗸	5	3	
Save Cance								
			-	_	_		-	

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

-	RF SUPE	RVISOR				Aprisa 8
Ba	e Station	OK MODE	AUX TX RX OOOO Status		Network	
erm	nal Radio) Serial	Ethernet IP	QoS Security Maintena	nce Events Software Monitoring	
Jarm	Summary	Event History	Events Setup	Traps Setup Alarm I/O Set	up Event Action Setup Defaults.	
ĂL A		-	_			
ALA						
ID	Name	Туре	Active State	Current State		
1	User IO 1	Input	High V	Low		
2	User IO 2	Input	High V	Low		
3	User IO 3	Output	High V	Low		
			(And a second s			
Sav	Cancel					

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.

Туре

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

• 4RF SUPERVISOR	con to sh		Aprisa
Base Station OK MODE	AUX TX RX O O O tatus	Network	
erminal Radio Serial Narm Summary Event History	Ethernet IP QoS Security Mainter Events Setup Traps Setup Alarm I/O Se	ance Events Software Monitoring	
EVENT ACTION SETUP			
Action Definition	1 of 1	ACTION ALARM MAP	
Action Destination IP Address	127.0.0.1	RA Current	
Action Type	Activate Alarm Output 1 🗸	OPA Driver Current	^
Action Threshold Criteria	Radio Severity Equal Major 🗸	PA Stability	
		CTX AGC	
		CTX Forward Power	
		O Temperature Threshold	
		TX Synthesizer Not Locked	
		- O Thermal Shutdown	
		ORSSI Threshold	
		KX Synthesizer Not Locked	
		RF No Receive Data	~
Save Cancel Add Delete		Clear Map	Prev Next

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

4RF SUPER	RVISOR			Aprisa 🔤
Base Station	OK MODE AUX TX RX O O O O O Status		Network	
erminal Radio	Serial Ethernet IP	QoS Security Maintenance	e Events Software Monitoring	
larm Summary	Event History Events Setup	Traps Setup Alarm I/O Setup	Event Action Setup Defaults	
EVENT DEFAULT	s			
Restore Defaults				
Save Cancel				

EVENT DEFAULTS

Restore Defaults

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



Software

The Software menu contains the setup and management of the system software including network software distribution and activation. The distribution of the system software to the remote radios is encrypted by the AES session key over-the-air.

Single Radio Software Upgrade

The radio software can be upgraded on a single Aprisa SR+ radio (see 'Single Radio Software Upgrade' on page 362). This process would only be used if the radio was a replacement or a new station in an existing network.

Network Software Upgrade

The radio software can be upgraded on an entire Aprisa SR+ radio network remotely over the radio link (see 'Network Software Upgrade' on page 358). This process involves following steps:

- 1. Transfer the new software to base station with 'Software > File Transfer'
- 2. Distribute the new software to all remote stations with 'Software > Remote Distribution'
- 3. Activate of the new software on remote stations with 'Software > Remote Activation'.
- 4. Finally, activate the new software on the base station radio with 'Software > Manager'. Note: activating the software will reboot the radio.



Software > Summary

This page provides a summary of the software versions installed on the radio, the setup options and the status of the File Transfer.

4RF SUPERVISO	OR			Aprisa 🛲
Base Station	K MODE AUX TX RX		Network	
Terminal Radio S	Serial Ethernet IP	QoS Security Maintenan	ce Events Software M	onitoring
Summary Setup	File Transfer Manager	Remote Distribution Remot	e Activation	
SOFTWARE VERSIONS Current Version Previous Version Software Pack Version	1.5.8 1.5.6 1.5.8		USB AUTOMATIC UPGRADE USB Boot Cycle Upgrade FILE TRANSFER Transfer Activity Method Filename Transfer Result	Ide - -
Ready		Radio: Base Station		Logout ADMIN

SOFTWARE VERSIONS

Current Version

This parameter displays the software version running on the radio.

Previous Version

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

Software Pack Version

On the base station, this parameter displays the software version available for distribution to all radios in the network.

On the all stations, this parameter displays the software version ready for activation.

USB AUTOMATIC UPGRADE

USB Boot Upgrade

This parameter shows the type of USB Boot upgrade defined in 'Software Setup > USB Boot Upgrade' on page 237.



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) 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.

4RF SUPERV	ISOR					Aprisa 🛲
Base Station	OK MODE AUX T O O O O Status	FX RX O O		Network		
Terminal Radio	Serial Ethernet	t IP QoS	Security Maintenan	ce Events S	oftware Monitoring	
USB SETUP USB Boot Upgrade Save Cancel	L	Load And Activate -				
Ready			Radio: Base Station			Logout ADMIN

USB SETUP

USB Boot Upgrade

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

Option	Function
Load and Activate	New software will be uploaded from a USB flash drive in to the Aprisa SR+ when the radio is power cycled and activated automatically.
Load Only	New software will be uploaded from a USB flash drive in to the Aprisa SR+ when the radio is power cycled. The software will need to be manually activated (see 'Software > Manager' on page 242).
Disabled	Software will not be uploaded from a USB flash drive into the Aprisa SR+ when the radio is power cycled.

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



Software > File Transfer

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

4RF SUPERVISOR						Aprisa 🛲
Base Station	MODE AUX TX RX O O O O Status		Networ	k		
Terminal Radio Seria	al Ethernet IP	QoS Security Maint	tenance Events	Software	Monitoring	
Summary Setup File	Transfer Manager	Remote Distribution R	emote Activation			
SETUP FILE TRANSFER			FILE TRAN	SFER STATUS		
Direction	To This Radio 👻		Transfer A	Activity	Idle	
Method	USB Transfer 👻		Direction		-	
File	Software Pack		Method		-	
File Server IP Address	192.168.10.0		File		-	
FTP Username	UserName		Transfer R	Result	-	
FTP Password						
Start Transfer Cancel						
Ready		Radio: Base Statio	on			Logout ADMIN

SETUP FILE TRANSFER

Direction

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

Method

This parameter sets the method of file transfer.

Option	Function
USB Transfer	Transfers the software from the USB flash drive to the radio.
FTP	Transfers the software from an FTP server to the radio.
HTTP / HTTPS	Transfers the software directly from a PC software pack file to the radio.

File

This parameter shows the software file source.

FTP Username

This parameter sets the Username to access the FTP server.

FTP Password

This parameter sets the Password to access the FTP server.



FILE TRANSFER STATUS

Transfer Activity

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

Direction

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

Method

This parameter shows the file transfer method.

File

This parameter shows the software file source.

Transfer Result

This parameter shows the progress of the transfer:

Transfer Result	Function					
Starting Transfer	The transfer has started but no data has transferred.					
In Progress (x %)	The transfer has started and has transferred x % of the data.					
Successful	The transfer has finished successfully.					
File Error	The transfer has failed. Possible causes of failure are: Is the source file available e.g. USB flash drive plugged in Does the file source contain the Aprisa SR+ software release files; asropp 1,332 KB File 28 KB File 3,716 KB File 3,716 KB File 3,716 KB File 3 asrver 8 KB File 1,944 KB File 1 KB Text Document					



To transfer software into the Aprisa SR+ radio:

USB Transfer Method

- 1. Unzip the software release files in to the root directory of a USB flash drive.
- 2. Insert the USB flash drive into the host port $\bullet \frown \bullet$.
- 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 237), 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 242). The radio will reboot automatically.

If the file transfer fails, check the Event History page (see 'Events > Event History' on page 223) for more details of the transfer.

Note: Some brands of USB flash drives may not work with 4RF radios.

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 242). The radio will reboot automatically.

If the file transfer fails, check the Event History page (see 'Events > Event History' on page 223) for more details of the transfer.



HTTP / HTTPS Method

- 1. Unzip the software release files in to a temporary directory.
- 2. Click on 'Start Transfer'.
- 3. Browse to the *.swpack file in the temporary directory and open the file.

FILE TRANSFER STATUS				
Transfer Activity	In Progress			
Direction	To This Radio			
Method	HTTPS			
File	Software Pack			
Transfer Result	In Progress (5%)			

Go to Supervisor > Software > Manager and activate the Software Pack (see 'Software > Manager' on page 242). The radio will reboot automatically.

If the file transfer fails, check the Event History page (see 'Events > Event History' on page 223) 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 su
Base Station OK MOD	DE AUX TX RX		Ne	work	
Terminal Radio Serial	Ethernet IP	QoS Security I	Maintenance Even	ts Software	Monitoring
Summary Setup File Tra	nsfer Manager	Remote Distribution	Remote Activation		
CURRENT SOFTWARE Version Status PREVIOUS SOFTWARE Version Status Activate Apply Cancel SOFTWARE PACK	1.5.8 Active 1.5.6 Inactive				
Version	1.5.8				
Status	Available				
Activation Type	Now 👻				
Activation Date & Time	15/03/2016 15:24				
Apply Cancel Cancel Activat	tion				
Ready		Radio: Base	Station		Logout ADMIN

CURRENT SOFTWARE

Version

This parameter displays the software version running on the radio.

Status

This parameter displays the status of the software version running on the radio (always active).



PREVIOUS SOFTWARE

Version

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

Status

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

Option	Function
Active	The software is operating the radio.
Inactive	The software is not operating the radio but could be re-activated if required.

Activate

This parameter activates the previous software version (restores to previous version).

The Aprisa SR+ will automatically reboot after activation.

SOFTWARE PACK

Version

This parameter displays the software pack version available for distribution on base station and activate on all stations.

Status

This parameter displays the status of the software pack version.

Option	Function	
Available	On the base station, the software pack is available for distribution.	
	On all stations, the software pack is available for activation.	
Activating	The software pack is activating in the radio.	
Unavailable	There is no software pack loaded into the radio.	

Activate

This parameter activates the software pack.

The Aprisa SR+ will automatically reboot after activation.

Activation Type

This parameter sets when the software pack activation will occur.

Option	Function
Now	Activates the software pack now.
Date & Time	Activates the software pack at the Date & Time set in the following parameter.



Activation Date & Time

This parameter sets the Date & Time when the software pack activation will occur. This setting can be any future date and 24 hour time.

Version	1.5.1
Status	Active
PREVIOUS SOFTWARE	
Version	1.5.0 Hours
Status	Inactive 0 1 2 3 4
Activate	
	Minutes
SOFTWARE PACK	00 10 20 30 40 5
Version	1.5.1
Status	Available 5 6 7 8 9
Activation Type	Date & Time
Activation Date & Time	21/11/2014 11:50
	ation 🖌 November, 2014 🖒
ounder contervente	Su Mo Tu We Th Fr Sa
	26 27 28 29 30 31 1
_	2 3 4 5 6 7 8
	2 3 4 5 6 7 8 9 10 11 12 13 14 15
	2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

If the network base station 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 base station radio date / time or use the Date And Time Synchronization from a SNTP server feature (see 'Terminal > Date / Time' on page 92).



To activate a software version:

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

The page will display a Status of 'Activating'.

Once started, activation cannot be cancelled.

When the activation is completed, the radio will reboot. This will cause the current SuperVisor session to expire.

ERROR	
Lost connection to unit: Remote Station 1. Check unit is switched on.	
OK	

3. Login to SuperVisor to check the result.



Software > Remote Distribution

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

The Software Pack that was loaded into the base station with the file transfer process (see 'Software > File Transfer' on page 238) can be distributed via the radio link to all remote stations.

This page is used to manage the distribution of that software pack to all remote radios on the network.

This page is only available when the radio is configured as a Base Station.

4RF SUPERV	/ISOR	Aprisa sm
Base Station	OK MODE AUX TX RX O O O O O O Status	
Terminal Radio	Serial Ethernet IP QoS Security Maintenance Events Soft	tware Monitoring
Summary Setup	File Transfer Manager Remote Distribution Remote Activation	
	REMOTE SOFTWARE DISTRIBUTION Software Pack Version 1.5.8 Status Available Start Transfer Apply Cancel	
Ready	Radio: Base Station	Logout ADMIN

REMOTE SOFTWARE DISTRIBUTION

Software Pack Version

This parameter displays the software pack version available for distribution on base station and activate on all stations.

Status

This parameter displays the status of the software pack version.

If a Software Pack is not available, the status will display 'Unavailable' and the software distribution mechanism will not work.



Start Transfer

This parameter when activated distributes (broadcasts) the new Software Pack to all remote stations in the network.

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

Software distribution traffic is classified as 'management traffic' but does <u>not</u> use the Ethernet management priority setting. Software distribution traffic priority has a fixed priority setting of 'very low'.

To distribute software to remote stations:

This process assumes that a Software Pack has been loaded into the base station with the file transfer process (see 'Software > File Transfer' on page 238).

- 1. To ensure that the Network Table is up to date, it is recommended running the node discover function (see 'Discover Nodes' on page 218).
- 2. Click on 'Start Transfer'.

REMOTE SOFTWARE DISTRIBUTION			
Software Pack Version	1.5.1		
Status	In Progress (0%)		
Pause Transfer			
Cancel Transfer			
Apply Cancel			

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

3. When the distribution is completed, activate the software with the Remote Software Activation.

Pause Transfer

This parameter when activated, pauses the distribution process and shows the distribution status. The distribution process will continue from where it was paused with Resume Transfer.

REMOTE SOFTWARE DISTRIBUTION			
Software Pack Version	1.5.1		
Status	Suspended (0%)		
Resume Transfer			
Cancel Transfer			
Apply Cancel			

Cancel Transfer

This parameter when activated, cancels the distribution process immediately.

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



Software > Remote Activation

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

The Software Pack was loaded into the base station with the file transfer process (see 'Software > File Transfer' on page 238) and was distributed via the radio link to all remote stations.

This page is used to manage the activation of that software pack on all remote radios on the network.

This page is only available when the radio is configured as a Base Station.

	/ISOR		Aprisa 🔤
Base Station	OK MODE AUX TX RX O O O O O Status	Network	
erminal Radio Summary Setup	Serial Ethernet IP Q File Transfer Manager F	toS Security Maintenance Events Software Monitorin Remote Distribution Remote Activation	9
	REMOTE SOFTWARE ACTIV	IATION	
	Version	1.5.8	
	Activation Type	Now 👻 🗍 Skip Confirmation Step	
	Activation Date & Time	15/03/2016 15:24	
	Apply Cancel Cancel Sd	heduled Activation	
			_

REMOTE SOFTWARE ACTIVATION

When the software pack version has been distributed to all the remote stations, the software is then activated in all the remote stations with this command. If successful, then activate the software pack in the base station to complete the network upgrade.

Version

This parameter displays the software version for activation. The default version is the software pack version but any valid software version can be entered in the format 'n.n.n'.

Activation Type

This parameter sets when the software pack activation will occur.

Option	Function
Now	Activates the software pack now.
Date & Time	Activates the software pack at the Date & Time set in the following parameter.



Activation Date & Time

This parameter sets the Date & Time when the software pack activation will occur.

This setting can be any future date and 24 hour time.

Skip Confirmation Step

This parameter when enabled skips the confirmation step during the activation process.

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

To activate software in remote stations:

This process assumes that a Software Pack has been loaded into the base station with the file transfer process (see 'Software > File Transfer' on page 238) and distributed to all remote radios in the network.

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

1. Enter the Software Pack version (if different from displayed version).

REMOTE SOFTWARE ACTIVATION					
Version	1.5.1				
Activation Type	Now	~		Skip Confirmation Step	
Activation Date & Time	25/11/2014		13:20		
Apply Cancel Scheduled Activation					
Remote Radios Polled For Part	ners 1	of 1	Completed	i	
Remote Radios Polled For New	Version 1	of 1	Completed	1	
Remote Radios Activated	C) of 0	Cancelled		
Remote Radios On New Versio	n C) of 0	Cancelled		

- 2. Select the Activation type.
- 3. Click Apply.



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

Result	Function (X of Y)
Remote Radios Polled for Partners	X is the number of radios polled to determine the number of protected stations in the network.
	Y is the number of remote radios registered with the base station.
Remote Radios Polled for New Version	X is the number of radios polled to determine the number of radios that contain the new software version.
	Y is the number of remote radios registered with the base station.
Remote Radios Activated	X is the number of radios that contain the new software version and have been activated.
	Y is the number of radios that contain the new software version and can be activated.
Remote Radios On New Version	X is the number of radios that has been successfully activated and now running the new version of software.
	Y is the number of radios that the activation command was executed on.
	Note: When upgrading from software version 1.2.5 to 1.2.6 or later, communication to all remote radios will be lost due to a MAC protocol change. This will prevent this function from working correctly. In this case, activate the new software on the base station and run the 'Maintenance > Advanced' Discover Nodes function on page 217.

When the activation is ready to start:

CONFIRMATION
Activation step is about to start. All 2 radios will be activated.
WARNING: The activation process may take up to 5 minutes for each radio. Do not leave this page until the activation step has completed.
OK Cancel

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



The page will display the progress of the activation.

REMOTE SOFTW	ARE ACTIVATION			
Version	1.5.1			
Start Activation				
Remote Radios F	Polled For Partner	rs	4 of 4	Completed
Remote Radios F	Polled For New Ve	ersion	0 of 4	Completed
Remote Radios A	Activated		0 of 0	Cancelled
Remote Radios (On New Version		0 of 0	Cancelled
REMOTE ACTIVA	TION EXCEPTION	S		
Name	IP Address	Vers	sion	Exception
Protected Remote Station	172.17.70.2	1.5.1		Software Version not on the radio (Step 2)
Remote125	172.17.70.125	1.5.1		Software Version not on the radio (Step 2)
Protected Remote Station	172.17.70.1	1.5.1		Software Version not on the radio (Step 2)
				Prev

The example shows that during the activation process there were exceptions that may need to be investigated.

When all the remote radios have been activated, the base station radio must now be activated with (see 'Software > Manager' on page 242).

INFORMATION	
All remotes successfully activated. Please install and activate software version 1.5.1 on th	e base station.
	ОК

4. Click on 'OK' to start the activation on the base station.



Activation Type

This parameter sets when the remote software activation will occur.

Option	Function
Now	Activates the remote software now.
Date & Time	Activates the remote software at the Date & Time set in the following parameter.

Skip Confirmation Step

This parameter when enabled skips the confirmation step during the activation process.

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

Activation Date & Time

This parameter sets the Date & Time when the remote software activation will occur.

This setting can be any future date and 24 hour time.

When the date and time is set, the remotes will be polled to setup the scheduled activation date and time.

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

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 base station radio date / time or use the Date And Time Synchronization from a SNTP server feature (see 'Terminal > Date / Time' on page 92).



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

Monitored parameter data is accumulated into 2 sets:

- 15 minutes of data, for 96 readings for the last 24 hours
- 24 hours of data, for 31 readings for the last 31 days.

Monitoring > Terminal

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

	SUPERV	ISOR							Aprisa 🛽
Base Station OK MODE AUX TX RX									
Terminal	Radio	Serial	Ethernet	IP QoS	Security Main	ntenance	Events	Software Monitoring	
erminal	Serial	Ethernet	Radio	User Selected	TCP Connection	ns Routi	ng Table	Address Tables	
POWER	SUPPLY P.	ARAMETER	ιs	-	-				
					User				
Current V	DC Power	Supply	12.288 V						
Current 3	.3V Power	Supply	3.324 V						
Current 5	.0V Power	Supply	5.302 V						
Current 1	5.0V Power	Supply	14.867 V						

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.	320, 400 and 450 MHz 14.5 to 15.3 VDC 135, 220, 896 and 928 MHz 12.7 to 13.5 VDC



Controls

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

Base Station OK MODE AUX TX RX Neth Status Status Status Status Status Status Neth Terminal Radio Serial Ethernet IP QoS Security Maintenance Even Terminal Serial Ethernet Radio User Selected TCP Connections Routing Table POWER SUPPLY PARAMETERS Status Status Status Status Status Status Status Power Supply 28/04/15		Aprisa 🛲
Terminal Radio Serial Ethernet IP QoS Security Maintenance Even Terminal Serial Ethernet Radio User Selected TCP Connections Routing Table POWER SUPPLY PARAMETERS Security 28/04/15<	vork	
Terminal Serial Ethernet Radio User Selected TCP Connections Routing Table POWER SUPPLY PARAMETERS	ts Software Monitoring	
POWER SUPPLY PARAMETERS ower Supply History, Quarter Hourly Power Supply 28/04/15 28/04/15 28/04/15 28/04/15 7/00 Aaximum VDC Supply - - 12/208 13/22 3/322 3/322 3/322 3/321 13/31 14/31 14/31 14/31 14/31 14/31 14/31 14/31 14/329 14/329 14/329 14/329 <td< th=""><th>Address Tables</th><th></th></td<>	Address Tables	
ower Supply History, Quarter Hourly ower Supply 28/04/15 28/04/15 28/04/15 28/04/15 28/04/15 28/04/15 28/04/15 28/04/15 28/04/15 28/04/15 28/04/15 28/04/15 6:30 6:45 7:00 12:208 13:204 13:204 13:204 13:204 13:204 13:204 14:801 14:801 14:801 14:802 14:802 14:802 14:802 14:802 14:802 14:802 14:802 14:802		
Sover 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 taximum VDC Supply - - - 12.298 12.298 taximum 3.3V Supply - - - 3.324 3.324 tinimum DC Supply - - - 3.322 3.322 taximum 3.3V Supply - - - 3.322 3.322 taximum 5V Supply - - - 5.304 5.304 taximum 6V Supply - - - 5.301 5.301 taximum 16V Supply - - - 14.867 14.871 taximum 16V Supply - - - 14.862 14.829 tewing 6:00 to 8:15 of 6:00 to 8:15 - - - 8:16 8:30 - - - - - - 8:16		
taximum VDC Supply - - 12.308 12.308 tinimum VDC Supply - - 12.298 12.298 taximum 3.3V Supply - - 3.324 3.324 tinimum 3.3V Supply - - 3.322 3.322 taximum 5V Supply - - 5.304 5.304 tinimum 5V Supply - - 5.301 5.301 taximum 15V Supply - - 14.867 14.871 taximum 15V Supply - - 14.862 14.829	28/04/15 28/04/15 28/04/ 7:15 7:30 7:45	15 28/04/15 28/04/15 8:00 8:15
finimum VDC Supply - - 12 298 12 298 faximum 3.3V Supply - - 3.324 3.324 finimum 3.3V Supply - - 3.322 3.322 faximum 6V Supply - - 5.304 5.304 finimum SV Supply - - 5.301 5.301 faximum 16V Supply - - 14.867 14.871 finimum 16V Supply - - 14.862 14.829	12.317 12.317 12.317	7 12.317 12.317
taximum 3.3V Supply - - 3.324 3.324 tinimum 3.3V Supply - - 3.322 3.322 taximum 6V Supply - - 5.304 5.304 tinimum 6V Supply - - 5.301 5.301 taximum 16V Supply - - 5.301 5.301 tinimum 16V Supply - - 14.867 14.871 tinimum 16V Supply - - 14.862 14.829	12.298 12.298 12.298	3 12.298 12.288
Inimum 3.3V Supply - - 3.322 3.322 taximum 5V Supply - - 5.304 5.304 Inimum 15V Supply - - 5.301 5.301 taximum 16V Supply - - 14.867 14.871 Inimum 16V Supply - - 14.867 14.829 ewing 6:00 to 8:15 of 6:00 to 8:15 8:15 8:10 8:15	3.324 3.324 3.324	3.324 3.324
taximum 5V Supply - - 5.304 5.304 tinimum 6V Supply - - 5.301 5.301 taximum 15V Supply - - 14.867 14.871 tinimum 15V Supply - - 14.862 14.829 texing 6:00 to 8:15 of 6:00 to 8:15 8:10 8:30 8:15	3.322 3.322 3.322	3.322 3.322
Inimum 5V Supply - - 5.301 5.301 Iaximum 15V Supply - - 14.867 14.871 Inimum 15V Supply - - 14.862 14.829 ewing 6:00 to 8:15 of 6:00 to 8:15 - - 8:30 - - 8:30 - 6:45 - 8:15 28:0 - - -	5.304 5.304 5.304	5.304 5.304
taximum 15V Supply - - 14.867 14.871 tinimum 15V Supply - - 14.862 14.829 ewing 6:00 to 8:15 of 6:00 to 8:15 - - 14.862 14.829 8:30 - - - 14.862 14.829	5.296 5.296 5.295	5.295 5.295
tinimum 15V Supply 14.862 14.829 ewing 6:00 to 8:15 of 6:00 to 8:15 8:30 8:15 27/04/15 6:45 - 8:15 28:0	14.952 14.952 14.952	2 14.957 14.952
ewing 6:00 to 8:15 of 6:00 to 8:15 8:30 8:15 27/04/15 6:45 - 8:15 28:0	14.852 14.862 14.852	2 14.862 14.862
iewing 6:00 to 8:15 of 6:00 to 8:15 8:30 27/04/15 6:45 - 8:15 28:0		
8:30 8:45 - 8:15 8:48 8:	Left Right	
8:30 8:15 8:15 28/0		
	4/15 Cancel	

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

4 74	SUPERV	/ISOR									Αρ	orisa <mark>sa</mark>	7
Base Sta	tion		E AUX TX Θ Θ Status	RX O			Networ	k					
Terminal	Radio	Serial	Ethernet	IP QoS	Security	Maintenance	Events	Software	Monitoring				
Terminal	Serial	Ethernet	Radio	User Selected	TCP Con	nections Rol	uting Table	Address Tab	les				
POWER S		ARAMETER	s										
ower Supply I	History, Da	ily				_	_	_		_	_	_	
ower 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	
aximum VDC	Supply		-	-	-	-	-	-	12.308	12.308	12.308	12.308	
inimum VDC	Supply		-	-	-	-	-	-	12.298	12.298	12.288	12.298	
aximum 3.3V	Supply		-	-	-	-	-	-	3.324	3.324	3.324	3.324	
nimum 3.3V	Supply		-	-	-	-	-	-	3.322	3.322	3.322	3.322	
aximum 5V S	upply		-		-	-	-	-	5.304	5.304	5.304	5.304	
inimum 5V Si	upply		-		-	-	-	-	5.301	5.301	5.301	5.301	
aximum 15V	Supply		-	-	-	-	-	-	14.867	14.867	14.929	14.919	
inimum 15V s	Supply		-	-	-	-	-	-	14.862	14.862	14.824	14.862	
ewing 18/04/11	5 to 27/04/1	15 of 18/04/15	i to 27/04/15				27/04/11	5 Dow	Left Right				
			23	/04/15 - 27/04/15					Cancel				
													Ì



Monitoring > Serial

This page displays the current radio performance monitoring parameters per serial port in packet and byte level granularity, for serial port high level statistics and troubleshooting.

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

4RF SUPERVISOR			Aprisa 🛲
Base Station OK M	MODE AUX TX RX O O O O Status	Network	
erminal Radio Seria	al Ethernet IP QoS	Security Maintenance Events Software Monitoring	
erminal Serial Ether	net Radio User Selected	TCP Connections Routing Table Address Tables	
SERIAL PORT PARAMETE	ERS Serial		
		User	
Maximum Capacity	115,200 bps		
Packets Transmitted	0		
Bytes Transmitted	0		
Packets Received	0		
Bytes Received	0		
Errored Bytes Received	0		
Dropped Bytes (Congestic	on) 0 pry:Daily[Reset]		
leady		Radio: Base Station	Logout ADMIN

SERIAL PORT PARAMETERS

All Serial Ports

Monitored Parameter	Function	Normal Operating Limits
Maximum Capacity	Parameter to show the maximum serial data rate of the serial port	Equal to the serial port baud rate setting
Packets Transmitted	Parameter to show the number of packets transmitted to the customer from the serial port	
Packets Received	Parameter to show the number of packets received from the customer into the serial port	
Bytes Received	Parameter to show the number of bytes received from the customer into the serial port	
Errored Bytes Received	Parameter to show the number of bytes received from the customer into the serial port that have errors	
Dropped Bytes (Congestion)	Parameter to show the number of bytes received from the customer into the serial port that are dropped due to over the air congestion	

Controls

The Reset button clears the current results.



Monitoring > Ethernet

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

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

4RF SUPERN	VISOR								Aprisa 🛲
Base Station	ok mode O O	E AUX TX O O Status	RX O			Networ	rk		
Terminal Radio	Serial	Ethernet	IP QoS	Security	Maintena	ance Events	Software	Monitoring	
Terminal Serial	Ethernet	Radio	User Selected	TCP Con	nections	Routing Table	Address Tabl	es	
ETHERNET PORT	PARAMETE	RS rt 2 Tx P	Port 2 Rx		User				
Maximum Capacit	y	100 MI	bps						
Packets		145							
Bytes		53,765	5						
Packet Collisions		0							
History:Quarter Ho	ourly History: D	aily Reset							
Ready				Radio: Ba	se Station				Logout ADMIN

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.

4 86	SUPER	/ISOR									Αμ	orisa <mark>se</mark>	7
Base Stat	ion		AUX TX OO Status	RX O			Networ	k					
Terminal	Radio	Serial	Ethernet	IP QoS	Security	Maintenance	Events	Software	Monitoring	1			
Terminal	Serial	Ethernet	Radio	User Selected	TCP Con	nections Rou	uting Table	Address Tab	les				
ETHERNE	t port i	PARAMETE	RS										
thernet Port 1	Transmit	History, Qua	rter Hourly										
thernet 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	
laximum Capa	city (Mb/s)	100	100	100	100	100	100	100	100	100	100	
ackets			2,444	2,400	2,332	2,334	2,450	2,380	2,368	2,437	2,391	2,380	
ytes			430,710	427,959	422,584	423,669	431,094	426,678	425,354	428,735	427,318	427,460	
acket Collision	15		0	0	0	0	0	0	0	0	0	0	
										_			
iewing 4:45 to 7	:00 of 4:45	i to 8:15							Left Right				
8:30 27/04/15				4:45 - 8:15			8:15 28/04/1	5 Dowr	lloaded 15 Cancel				
													i

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

 4RF	SUPERV	/ISOR									Αρ	risa <mark>s#</mark>	
Base Sta	ation	OK MODE	E AUX TX O O Status	RX O			Networ	k					
Terminal	Radio	Serial	Ethernet	IP QoS	Security	Maintenan	ce Events	Software	Monitoring				
Terminal	Serial	Ethernet	Radio	User Selected	TCP Con	nections F	Routing Table	Address Tabl	es				
ETHERN	et port f	ARAMETEI	RS										
Ethernet Port	1 Transmit I	listory, 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 Cap	acity (Mb/s)	-	-	-	-	-	-	100	100	100	100	- 1
Packets			-	-	-	-	-	-	80,995	226,794	227,299	227,306	
Bytes			-	-	-	-	-	-	14,954,820	40,822,243	40,853,207	40,853,381	
Packet Collisi	ons		-	-	-	-		-	0	0	0	0	
VLAN Frames			-	-	-	-	-	-	0	0	0	0	
Viewing 18/04/1 28/03/15	5 to 27/04/1	5 of 18/04/15	to 27/04/15 2'	//04/15 - 27/04/15		0	27/04/1	5 Dowr	Left Right				
]			
Ready					Radio: Ba	ase Station					Logout ADM	N	



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.

4RF SUPERVISOR					Aprisa 🛲
Base Station OK MODE	AUX TX RX OOO Status		Network		
erminal Radio Serial	Ethernet IP QoS	Security Maintenance	Events Software Mo	nitoring	
erminal Serial Ethernet	Radio User Selected	TCP Connections Rout	ing Table Address Tables		
	RS				
Port 1 Tx Port 1 Rx Por	t 2 Tx Port 2 Rx				
Dackete	0	User	Packet in Error	0	User
Butes	0		Butes in Error	0	
Packets equal to 64 Bytes	0		CRC/Alignment Errors	0	
Packets 65 to 127 Bytes	0		Undersized Packets	0	
Packets 128 to 255 Bytes	0		Oversized Packets	0	
Packets 256 to 511 Bytes	0		Fragmented Packets	0	
Packets 512 to 1023 Bytes	0		Jabber Packets	0	
Packets 1024 to 1536 Bytes	0		Dropped Packets (Congestion)	0	
Broadcast Packets	0		Dropped Packets (Filtering)	0	
Multicast Packets	0		Dropped Bytes (Filtering)	0	
VLAN Frames	0		History:Quarter Hourdy History:Daily	Reset	
VLAN Frames dropped	0		Instory. deditor frouny fristory. Duly	Treaser	
one		Radio: Base Station			Logout ADMIN

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.

#4RF SUPERVISOR Aprise Stu										
Base Station OK MC	DE AUX TX	RX			Netwo	ork				
Ethernet Port 1 Receive History, Quarter Hourly										
Ethernet Port 1 Receive	28/04/15 6:00	28/04/15 6:15	28/04/15 6:30	28/04/15 6:45	28/04/15 7:00	28/04/15 7:15	28/04/15 7:30	28/04/15 7:45	28/04/15 8:00	28/04/15 8:15
Packets	3,114	3,089	3,103	3,108	3,108	3,088	3,106	3,117	3,106	3,091
Bytes	440,980	438,486	439,559	439,954	439,954	437,660	439,826	441,385	439,826	438,280
Packets equal to 64 Bytes	2,064	2,049	2,059	2,064	2,064	2,050	2,062	2,069	2,062	2,049
Packets 65 to 127 Bytes	257	255	257	257	257	255	257	258	257	255
Packets 128 to 255 Bytes	535	527	529	529	529	526	529	531	529	530
Packets 256 to 511 Bytes	1	1	1	1	1	1	1	1	1	1
Packets 512 to 1023 Bytes	257	257	257	257	257	256	257	258	257	256
Packets 1024 to 1536 Bytes	0	0	0	0	0	0	0	0	0	0
Broadcast Packets	2	3	2	2	2	3	2	2	2	3
Multicast Packets	20	15	14	14	14	14	14	14	14	18
/LAN Frames	0	0	0	0	0	0	0	0	0	0
/LAN 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.

Base Station	IODE AUX TX	RX			Netwo	rk				
hernet Port 1 Receive History, D	aily									
thernet Port 1 Receive	18/04/15	19/04/15	20/04/15	21/04/15	22/04/15	23/04/15	24/04/15	25/04/15	26/04/15	27/04/15
ackets	-	-	-	-	-	-	105,790	298,004	297,963	297,959
ytes	-	-	-	-	-	-	14,977,084	42,212,489	42,206,282	42,205,341
ackets equal to 64 Bytes	-	-	-	-	-	-	70,292	197,783	197,762	197,760
ackets 65 to 127 Bytes	-	-	-	-	-	-	8,694	24,643	24,638	24,638
ackets 128 to 255 Bytes	-	-	-	-	-	-	17,954	50,811	50,801	50,799
ackets 256 to 511 Bytes	-	-	-	-	-	-	71	97	95	96
ackets 512 to 1023 Bytes	-	-	-	-	-	-	8,779	24,670	24,667	24,666
ackets 1024 to 1536 Bytes	-	-	-	-	-	-	0	0	0	0
roadcast Packets	-	-	-	-	-	-	129	219	215	215
ulticast Packets	-	-	-	-	-	-	613	1,430	1,423	1,422
LAN Frames	-	-	-	-	-	-	0	0	0	0
LAN Frames Dropped	-	-	-	-	-	-	0	0	0	0
ackets in Error	-	-	-	-	-	-	0	0	0	0
ytes in Error			-		-	-	0	0	0	0
RC/Alignment Errors	-	-	-	-	-	-	0	0	0	0
ndersized Packets	-	-	-	-	-	-	0	0	0	0
versized Packets	-	-	-	-	-	-	0	0	0	0
ragmented Packets	-	-	-	-	-	-	0	0	0	0
abber Packets	-	-	-	-	-	-	0	0	0	0
ropped Packets (Congestion)	-	-	-	-	-	-	0	0	0	0
ropped Packets (Filtering)	-	-	-	-	-	-	734	1,649	1,638	1,637
ropped 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.

4RF SUPERVISOR				Aprisa 🛲
Base Station OK MODE A	AUX TX RX O O O tus	Netw	ork	
erminal Radio Serial Et	hernet IP QoS	Security Maintenance Events	Software Monitoring	
erminal Serial Ethernet R	adio User Selected	TCP Connections Routing Table	Address Tables	
RADIO PARAMETERS	ısmit Path Receive P	ath		
		User		
Current Temperature	30.6 C			
Packets Transmitted	0			
Bytes Transmitted	0			
Dropped Packets (Congestion)	0			
Dropped Bytes (Congestion)	0			
Last TX Packet PA Current	933 mA			
Last TX Packet PA Driver Current	90 mA			
Last TX Packet Forward Power	34 dBm			
[History:Quarter Hourly]History:Daily]	Reset			
		Radio: Base Station		Logout ADMIN

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.

GARF SUPERVISOR						Aprisa 🛲
Base Station OK MC	DDE AUX TX O O O Status	RX O		Netwo	rk	
Terminal Radio Serial	Ethernet	IP QoS	Security Mainte	enance Events	Software Monitoring	
Terminal Serial Etherne	t Radio	User Selected	TCP Connections	Routing Table	Address Tables	
RADIO PARAMETERS	Transmit P	ath Receive F	ath			
			User			
Packets Received	0					
Bytes Received	0		\checkmark			
Packets Received in Error	0					
Dropped Packets (Filtering)	0		\checkmark			
Dropped Bytes (Filtering)	0 :Daily Reset					
Done			Radio: Base Station	1		Logout ADMIN

RADIO PARAMETERS

Receiver

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

Controls

The Reset button clears the current results.



This page displays the current radio RF transmit path modulation setting to single or multiple destination radios that the radio is transmitting to.

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

4RF SUPE	RVISOR					Aprisa 🛲
Base Station	OK MODE AUX TX O O O O Status	CRX O		Networ	rk	
Terminal Radio	Serial Ethernet	IP QoS	Security Mainte	enance Events	Software Monitorin	ng
Terminal Serial	Ethernet Radio	User Selected	TCP Connections	Routing Table	Address Tables	
RADIO PARAMET Transmitter To Tx M 000C QPS	Receiver Transmit F lod Tx Timesta K Lo 01/05/2015	Path Receive F	Vath User			
History:Quarter Ho	urly History. Daily				Prev Next	
Ready			Radio: Base Station			Logout ADMIN

RADIO PARAMETERS

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

Controls

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



This page displays the current radio RF receive path parameters from single or multiple source radios that the radio is receiving from.

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

4RF SUPERVISOR			Aprisa 🛲
Base Station OK MODE AUX T OK MODE AUX T OK MODE AUX T OK Status	rx rx ⊖ ●	Network	
Terminal Radio Serial Etherne	t IP QoS Security Main	ntenance Events Software	Aonitoring
Terminal Serial Ethernet Radio	User Selected TCP Connections	s Routing Table Address Tables	
RADIO PARAMETERS	Path Receive Path		
From Rx RSSI Rx SNR	Rx Freq Error Rx Mod Rx	x Timestamp User	
000C -52.7 dBm 31.5 dB	51 Hz QPSK 01	1/05/2015 21:08:31	
Busy	Radio: Base Statio	on	Logout ADMIN

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.

4RF SUPERVISO	}					Aprisa
Base Station OK	MODE AUX TX Θ Θ Θ Status	RX O		Networ	k	
erminal Radio Se	rial Ethernet	IP QoS Security	Mainte	nance Events	Software Monitoring	
erminal Serial Eth	ernet Radio	User Selected TCP Con	inections	Routing Table	Address Tables	
TERMINAL PARAMETER	RS		_	RF LINK PARAI	METERS	
Ethernet Port 2 Receive			User	Transmit Path (M	lo Data)	User
Packets	0		✓	Remote Name	0000	
				Remote Name	0000	\checkmark
RF Transmitter			User	Remote Name	0000	\checkmark
Dropped Packets (Conges	stion) 0		⊻	Remote Name	0000	
Dropped Bytes (Congesti	on) 0			Remote Name	0000	
Last TX Packet PA Currer	nt 937 mA			Remote Name	0000	
RF Receiver			User	Remote Name	0000	\checkmark
Packets Received	0		✓	Remote Name	0000	
Bytes Received	0		✓	Remote Name	0000	
Packets Received in Error	r O		✓	Remote Name	0000	\checkmark
Dropped Packets (Filterin	g) 0		✓	Remote Name	0000	
Dropped Bytes (Filtering)	0		✓	Remote Name	0000	
Reset All History:Quarter H	ourly History:Daily	Pre	v Next	Remote Name	0000	\checkmark
				Remote Name	0000	
						PrevNext
eady		Radio: Ba	se Station			Logout ADMIN

Controls

The Reset button clears the current results.



Monitoring > TCP Connections

This page displays the list of active TCP connections on the radio.

4RF SUP	ERVISOR								Aprisa Sa
Base Station	ok modi O O	E AUX TO O C Status	RX O			Netwo	rk		
Ferminal Rad Ferminal Seria	io Serial I Ethernet	Ethernet Radio	IP QoS User Selected	Security TCP Con	Maintenance nections Rol	Events Iting Table	Software Address Tat	Monitoring	
TCP CONNECT	ONS TABLE								
Local Address	Local Port	Remo	ote Address	Remote Por	t				
172.10.1.16	HTTPS(443)) 172.1	0.1.1	50913					
				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.

 4R	F SUPERV	ISOR								Aprisa 🛲
Base S	Base Station OK MODE AUX TX RX O O O O O O Status				Network					
Terminal	Radio	Serial	Ethernet	IP QoS	Security	Maintenar	nce Events	Software	Monitoring	
Terminal	Serial	Ethernet	Radio	User Selecte	d TCP Conne	ections F	Routing Table	Address Tab	les	
ROUTII	NG TABLE									
Index	Destination	Mask		Nexthop	Interface					
1	172.10.1.1	255.255	5.255.255	172.10.1.1	Wired Ethernet					
2	127.0.0.1	255.255	5.255.255	127.0.0.1	Loopback					
Auto	Refresh									
Busy					Radio: Base	e Station				Logout ADMIN

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.

4RF SUPERN	/ISOR					Aprisa 🛲
Base Station	OK MODE AUX T O O O O Status	X RX		Netwo	rk	
Terminal Radio	Serial Ethernet	t IP QoS	Security Main	tenance Events	Software Monitoring	
Terminal Serial	Ethernet Radio	User Selected	TCP Connections	Routing Table	Address Tables	
ADDRESS TABLES) hernet MAC Learnin	g Table				
IP Address N	IAC Address	Interface	Туре			
172.10.1.1 0	0:60:6E:D5:6A:C3	Wired Ethernet	Dynamic			
			Prev Next			
Auto Refresh						
Busy			Radio: Base Statio	n		Logout ADMIN

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
Туре	'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.

4RF SUPER	VISOR					Aprisa 🔤
Base Station	OK MODE AUX TX OOOOO Status	RX O		Netwo	rk	
erminal Radio erminal Serial ADDRESS TABLE ARP Table Et MAC Address D0:60:60:45:68:c3	Serial Ethernet Ethernet Radio S thernet MAC Learning Interface Ethernet Port 1	IP QoS User Selected Table Age La 280	Security Main TCP Connections	ntenance Events s Routing Table	Software Monitoring Address Tables	
Auto Refresh			Prev Next			
	-	_				

ADDRESS TABLES

Title	Function
MAC Address	The learned MAC address of a neighboring bridge device in the LAN network.
Interface	The Ethernet port interface the MAC address has learned
Age left	The aging time of this MAC entry will stay in the table, even if this MAC address is not used. Every time this MAC address is used, the aging time restarts from its maximum. Default is 300 sec.

Controls

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

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



Network Status > Network Table

This page displays a list of all the registered remote stations for the base station and provides management access to each of the remote stations.

#4RF SUPERVISOR Aprisa set							
Base Station				Remote Statio	n 1 OK MODE A	UX TX RX O O O us	
Network Status	Terminal Radio	Serial Ethernet	Networking	Security Main	tenance Events	Software	
Network Table	Summary Exceptions	s view					
NETWORK TABI	LE						
MAC Addr	ess Name	Node Address	IP Address	SW Version	Operating Mode	Protection	OTA Ethernet
100054	Remote Station 1	000B	173.10.10.2	1.2.6	Remote Station	-	Disabled
0 100055	Remote Station 2	000C	173.10.10.3	1.2.6	Remote Station	-	Disabled

NETWORK TABLE

This Network Table is only available when the local radio is the base station i.e. SuperVisor is logged into the base station.

To manage a remote / repeater station with SuperVisor:

Click on the radio button of the required station. The remaining menu items then apply to the selected remote station.



Network Status > Summary

Network View is an overview of the health of the network providing the ability to investigate issues directly within SuperVisor.

This page provides an overall summary view of the alarm status of all registered remote stations for the base station. When open, it provides a continuous monitor of the network.

Depending on the poll period set (20 seconds minimum) and the number of remotes in the network, it will take at least three poll cycles to indicate a failure in the network. Initial results may indicate 'All ok' until at least three poll cycles completed. This could take Number Of Remotes * Poll Period * 3 seconds to complete.

GARF SUPERVISOR	Aprisa su
Base Station	Remote Station 1
Network Status	
Network Table Summary Exceptions View	
NETWORK SUMMARY 2 remote terminals OK Network Polling Cycle 1 Remote Radios Polled 0 of 2 Polling Interval 20 seconds	
Ready Radio: Base Stati	on Logout ADMN



NETWORK SUMMARY

A network poll will start when any of the Network Status pages are opened (Summary, Exceptions or View). The network poll will only continue to poll the remote stations if one of the Network Status pages is open (SuperVisor can lose PC focus). The network poll continues from where it was stopped last time it was polling.

The initial result assumes that all remote stations are operating correctly.

Network Summary Example:

Result	Function			
Network Polling Cycle	The number of poll cycles since first opening a Network Status > Summary, Exceptions or View page. The page example shows 6 polling cycles.			
Remote Radios Polled	This shows the number of radios polled for the current polling cycle out of the number remote radios registered with the base station.			
	The page example shows 1 radio polled for the current polling cycle out of 3 remote radios registered.			
Polling Interval	The time interval between the completion of one radio poll and the start of the next radio poll. To set the polling interval, see 'Maintenance > General' on page 208.			

If a remote radio does not respond to a poll request within 10 seconds, the previous readings from that radio will be presented. Connectivity to a remote radio will be show as 'lost' if the remote radio has not responded to 3 consecutive poll requests.



Network Status > Exceptions

This page provides a list of all registered remote radios that are in an alarmed state or have stopped responding to the SuperVisor polling. When open, it provides a continuous monitor of the network.

4RF SUPERVISOR					Aprisa 🛲
Base Station			Remote Station 1	OK MODE AUX TX RX O O O O O Status	
Network Status					
Network Table Summary EX	ceptions View				
NETWORK EXCEPTIONS					
ID Address Name	IP A	Addr Mode	OK Last Rx Packet RSSI		
1 011E26 Remote Station	1 173.	.10.10.2 Remote	• -	View Events	View Parameters
Showing 1 to 1 of 1 Exceptions, fro	om 2 Radios				Prev Next
Network Polling Cycle 2 Remote Radios Polled 1 of 2 Polling Interval 20 second	15				
Ready		Radio: Base Station			Logout ADMIN

NETWORK EXCEPTIONS

A network poll will start when any of the Network Status pages are opened (Summary, Exceptions or View). The network poll will only continue to poll the remote stations if one of the Network Status pages is open (SuperVisor can lose PC focus). The network poll continues from where it was stopped last time it was polling.

Network Exceptions Example:

Result	Function			
Network Polling Cycle	The number of poll cycles since first opening a Network Status > Summary, Exceptions or View page. The page example shows 4 polling cycles.			
Remote Radios Polled	This shows the number of radios polled for the current polling cycle out of the number remote radios registered with the base station.			
	The page example shows 3 radios polled for the current polling cycle out of 4 remote radios registered.			
Polling Interval	The time interval between the completion of one radio poll and the start of the next radio poll. To set the polling interval, see 'Maintenance > General' on page 208.			



If a remote radio does not respond to a poll request within 10 seconds, the previous readings from that radio will be presented. Connectivity to a remote radio will be show as 'lost' if the remote radio has not responded to 3 consecutive poll requests.

If a remote radio on the list is detected to be responding to a poll request and no longer be in an alarmed state, the entry for this remote radio will be removed from the list.

View Events

Clicking on View Events navigates to the Events page (see 'Events' on page 222) for the specific remote radio where the radio events will be displayed.

View Parameters

Clicking on View Parameters navigates to the Monitoring page (see 'Monitoring' on page 253) for the specific remote radio where the radio parameters will be displayed.



Network Status > View

This page provides a complete list of all registered remote radios. It is similar to the Exceptions page but it shows all radios, not limited to the radios with alarms. When open, it provides a continuous monitor of the network.

#4RF SUPERVISOR Aprise See									
Base Station		Remote Stat	ion 1 OK MODE	AUX TX RX O O O atus					
Network Status									
Network Table Summary Exceptions	View								
NETWORK VIEW ID Address Name	IP Addr Partner IP Addr	Mode OK	Last Rx	_					
			Packet RSSI						
1 011E26 Remote Station 1	173.10.10.2	Remote 😆	- <u>View Ev</u>	rents	View Parameters				
2 UT1E40 Remote Station 2	173.10.10.3	Remote 😈	- <u>view Ev</u>	<u>ents</u>	view Parameters				
Showing 1 to 2 of 2					Prev Next				
Network Polling Cycle 4 Remote Radios Polled 1 of 2 Polling Interval 20 seconds									
Ready	Radio: Base Station				Logout ADMIN				

NETWORK VIEW

A network poll will start when any of the Network Status pages are opened (Summary, Exceptions or View). The network poll will only continue to poll the remote stations if one of the Network Status pages is open (SuperVisor can lose PC focus). The network poll continues from where it was stopped last time it was polling.

Network View Example:

Result	Function
Network Polling Cycle	The number of poll cycles since first opening a Network Status > Summary, Exceptions or View page. The page example shows 2 polling cycles.
Remote Radios Polled	This shows the number of radios polled for the current polling cycle out of the number remote radios registered with the base station.
	The page example shows 1 radio polled for the current polling cycle out of 3 remote radios registered.
Polling Interval	The time interval between the completion of one radio poll and the start of the next radio poll. To set the polling interval, see 'Maintenance > General' on page 208.
	Note: as this polling feature utilizes air time, the polling interval should be selected to suit the network traffic.



If a remote radio does not respond to a poll request within 10 seconds, the previous readings from that radio will be presented. Connectivity to a remote radio will be show as 'lost' if the remote radio has not responded to 3 consecutive poll requests.

View Events

Clicking on View Events navigates to the Events page (see 'Events' on page 222) for the specific remote radio where the radio events will be displayed.

View Parameters

Clicking on View Parameters navigates to the Monitoring page (see 'Monitoring' on page 253) for the specific remote radio where the radio parameters will be displayed.



Protected Station

The majority of SuperVisor screens are the same for the standard radio and the protected station. The following screens are specific to the protected station.

Logging into a Protected Station

When SuperVisor detects a protected station, it operates in Single Session Management operation mode.

When in Single Session Management mode, SuperVisor will automatically detect the two individual Aprisa SR+ radios configured to pair together for protection, and manage the two units in a single browser session. To the user, it will appear as managing a single unit, but SuperVisor will interact with the two individual units at a lower level.

The user can login with the IP address of either the Primary or Secondary radio to manage the protected station (don't use the PVIP address as it is not a management IP address). SuperVisor will present all information appropriately where 'Common Parameters' will be presented to the user as a single parameter e.g. TX and RX Frequencies and 'Unit Specific Parameters' will be presented to the user as Primary or Secondary parameters e.g. Events and Alarms.

When saving data, SuperVisor will also validate and ensure that the correct settings are written to both units. The SuperVisor Single Session Management ensures that both units of the protected station are always configured correctly to complement each other as protected partners.

The user can still login with two different sessions to the active and standby radios. If the user opens two session management, one session logged into the active radio and a second session logged into the standby radio, the Multiple Management Sessions pop-up message will show the user names and IP addresses of the active and standby radio.

Parameter Errors

On protected station screens, parameter values displayed in red indicate discrepancies in common parameter values between the primary and secondary radios (see 'Protected Station: Terminal > Summary' on page 279 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

4RF SUPERVIS	SOR								Aprisa 🛲
Protected Station	OK MODE AUX TX O O O O Primary	RX OK MODI	E AUX TX O O econdary	RX O	Network				
Terminal Radio	Serial Ethernet	IP QoS	Security	Maintenance	Events	Software	Monitoring		
Summary Details	Device Date/Time	e Operating M	ode						
TERMINAL SUMMAR	Y				OPERATING	G SUMMARY			
Terminal Name	Protec	cted Station			Operating M	lode		Base	
Location	Wellin	igton			Ethernet Mo	de		Bridge	
Contact Name	4RF L	imited			Interface Mo	de		Serial and Ethernet	
Contact Details	suppo	ort@4rf.com			Modem Mod	le		Mode A (ETSI / ACMA)	
Date and Time	03/05/	/2015 00:37:12			TX Frequen	cy (MHz)		400	
					TX Power (d	Bm)		35	
PROTECTION INFOR	MATION				RX Frequen	cy (MHz)		400	
Protection Type	Redun	ndant			Channel Siz	e (kHz)		12.5	
Active Unit	Primar	irv			Network ID	FAN)		CAFE	
Switch Count	0				Base Station	n ID		2	
Primary Address	172.10	0.1.30			Node Addre	88		0000	
Secondary Address	172.10	0.1.31			Network Rad	dius		1 (No Repeater)	
					Repeater Ne	twork Segmer	nt ID	0	
					Inpand Man	agement		Enablea (10s Timeout)	
Ready	Radio:	Protected Station			Active Unit: Pr	imary		L	poout ADMIN

TERMINAL SUMMARY

This page displays the current settings for the Terminal parameters.

PROTECTION INFORMATION

Protection Type

This parameter shows the type of protection:

Option	Function
Serial Data Driven Switching	Provides radio and RS-232 serial port user interface protection for Aprisa SR+ radios.
Monitored Hot Standby (Protected Station)	The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio.
	The standby radio is monitored to ensure its correct operation should a switch-over be required. See 'Monitored Alarms' on page 333 for the list of monitored alarms.
Redundant (Protected Station)	The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio

Active Unit

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



Switch Count

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

Primary Address

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

Secondary Address

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

OPERATING SUMMARY

See 'Terminal > Summary' on page 83 for parameter details.



Protected Station: Terminal > Details

4RF SUPERVISOR				Aprisa 🔐
Protected Base Station	AUX TX RX OK MODE AUX TX O O O O O O O imary Secondary	X RX	Network	
Terminal Radio Serial	Ethernet IP QoS Security	Maintenance	Events Software Monitor	ing
Summary Details Device	Date/Time Operating Mode			
PRIMARY UNIT MANUFACTURI	NG DETAILS		SECONDARY UNIT MANUFACTUR	RING DETAILS
Radio Serial Number	R1310001682		Radio Serial Number	R1310001178
Sub-Assembly Serial Number	13094428		Sub-Assembly Serial Number	13093341
HW Variant Type	400 - 470MHz		HW Variant Type	400 - 470MHz
Ethernet Port 1 MAC Address	00:22:b2:10:24:e1		Ethernet Port 1 MAC Address	00:22:b2:10:19:00
Ethernet Port 2 MAC Address	00:22:b2:10:24:e2		Ethernet Port 2 MAC Address	00:22:b2:10:19:01
Active Software Version	1.5.0		Active Software Version	1.4.0
Previous Software Version	1.4.0		Previous Software Version	Unknown
Busy	Radio: Protected Base Station		Active Unit: Primary	Loqout ADMIN

PRIMARY UNIT / SECONDARY UNIT MANUFACTURING DETAILS

See 'Terminal > Details' on page 86 for parameter settings.



Protected Station: Terminal > Operating Mode

<i>4</i>RF SUPERVISOR				Aprisa 📶
Protected Base OK MODE Station Prin	AUX TX RX OK MODE AUX TX Θ Θ Θ Θ Θ Θ mary Secondary	RX Networ	k	
Terminal Radio Serial E	Ethernet IP QoS Security	Maintenance Events	Software Monitoring	
Summary Details Device	Date/Time Operating Mode			
OPERATING MODES Terminal Operating Mode B Ethernet Operating Mode B TERMINAL PROTECTION Protection Type Automatic Periodic Switch Duration	iase	e		
PROTECTION MANAGEMENT IP	ADDRESS			
Primary IP Address	172.10.1.30			
Secondary IP Address	172.10.1.31			
Ready	Radio: Protected Base Station	Active Unit: F	Primary	Logout ADMIN

OPERATING MODES

Terminal Operating Mode

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

Option	Function
Base	The base station manages all traffic activity between itself, repeaters and remotes. It is the center-point of network where in most cases will be connected to a SCADA master.
Base Repeater	The Base-Repeater has the same function as the base station (and repeater station), but used when peer to peer connections between remotes is required via the base station.
Base MMS	The Base-MMS has the same function as the base station, but used when Migration Master Station operation is required (see Aprisa SR+MMS User Manual).
Repeater	The repeater forwards packets coming from base station and other repeaters e.g. in daisy chain LBS mode and /or remote stations.
Remote	The remote in most cases is used as the end-point of the SCADA network connected to an RTU or PLC device for SCADA network control and monitoring.
Point To Point	Configures a full duplex radio for Point-To-Point (PTP) operation. Changing from PMP or PTP or vice versa requires the radio to be 'restored to factory default settings' which will clear all previous radio setup and configuration.
	See Aprisa SR+ User Manual 1.6.0 PTP for all Point-To-Point setup and configuration.



Ethernet Operating Mode

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

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

SR Compatible

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

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

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



TERMINAL PROTECTION

Protection Type

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

Option	Function					
None	The SR+ radio is a stand-alone radio (not part of an Aprisa SR+ Protected Station).					
Redundant	The SR+ radio is part of an Aprisa SR+ Protected Station.					
(Protected Station)	The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio					
Monitored Hot Standby (Protected Station)	Set to make this SR+ radio part of an Aprisa SR+ Protected Station. The RF ports and interface ports from two standard Aprisa SR+ radios are switched to the standby radio if there is a failure in the active radio.					
	The standby radio is monitored to ensure its correct operation should a switch-over be required. See 'Monitored Alarms' on page 333 for the list of monitored alarms.					
Serial Data Driven Switching	The SR+ radio is part of an Aprisa SR+ Data Driven Protected Station. Provides radio and RS-232 serial port user interface protection for Aprisa SR+ radios.					

Automatic Periodic Switch Duration

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

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

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

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

PROTECTION MANAGEMENT IP ADDRESS

Primary Address

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

Secondary Address

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



Protected Station: Radio > Radio Setup

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

4RF SUPERVISOR			Aprisa 📶
Protected Base OK MO Station	DDE AUX TX RX OK MODE AUX TX RX O O O O O O O O O O Primary Secondary	Network	
Terminal Radio Serial	Ethernet IP QoS Security Mainte	enance Events Software Monitoring	
Radio Summary Channel Su	ummary Radio Setup Channel Setup Adv	anced Setup	
TRANSMITTER TX Frequency (MHz) TX Power (dBm) RECEIVER RX Frequency (MHz)	400 (400 to 470 MHz, in 6.25 kHz steps) 34 (7 to 34 dBm, in 1 dB steps) 400 (400 to 470 MHz, in 6.25 kHz steps)	MODEM Modem Mode Mode A (Enhanced Noise Rejection Mode Disabled Modulation Type 640AM (ACM Control Disabled ADAPTIVE CODING MODULATION	ETSI / ACMA) V V Low Gain) V
GENERAL		Modulation Range QPSK (High Gain) T	o 64QAM (Low Gain) V
Channel Size (kHz) Antenna Port Configuration Save Cancel	12.5 ✓ Single Antenna Single Port ✓	Save Cancel	
Ready	Radio: Protected Base Station	Active Unit: Primary	Logout ADMIN

Antenna Port Configuration

This parameter sets the Antenna Port Configuration for the radio. For more information on single and dual antenna port part numbers and cabling options, see 'Cabling' on page 340.

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



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

The default setting is Single Antenna Single Port.



Ethernet

Protected Station: Ethernet > Summary

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

~ 4	RF SUPER	VISOR											A	prisa 🛲
Prote	ected Base Station	ок	MODE AUX	CTXRX	OK MODE	AUX TX O O ondary	RX O		Network					
Termi	nal Radio	Seri	ial Ethe	rnet IP	QoS S	ecurity	Maintenanc	e E	vents	Software	Monitoring			
Sumn	nary Port S	Setup	L2 Filtering	VLAN										
_								_						
PRI	MARY ETHER	NET PO	RTS STATU	JS				ETI	HERNET	PORTS SET	TINGS			
ID	Name			Status	Speed (Mbit/s)	Duplex		ID	Name		Mode	Speed (Mbit/s)	Duplex	Function
1	Ethernet Port			Up	100	Full		1	Etherne	t Port	Switch	Auto	Auto	Mgmt & User
2	Ethernet Port			Down	10	Half		2	Etherne	t Port	Switch	Auto	Auto	Mgmt & User
SEC	ONDARY ETH	IERNET	PORTS ST	ATUS										
ID	Name			Status	Speed (Mbit/s)	Duplex								
1	Ethernet Port			Down	10	Half								
2	Ethernet Port			Down	10	Half								
Busy			Ra	adio: Protected	Base Station			Activ	e Unit: Pi	rimary			Logo	ut ADMIN

See 'Ethernet > Port Setup' for configuration options.



IP

Protected Station: IP > IP Summary

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

4RF SUPERVISOR				Aprisa 🛲
Protected Station OK M	IODE AUX TX RX OK MODE O O O O O O Primary Sec	AUX TX RX Network		
Terminal Radio Seria	l Ethernet IP QoS S	ecurity Maintenance Events	Software Monitoring	
IP Summary Terminal Ser	rver Summary IP Setup Term	inal Server Setup L3 Filtering IP	Routes	
NETWORKING IP SETTING	iS			
Virtual IP Address	172.10.1.50			
Primary IP Address	172.10.1.30			
Secondary IP Address	172.10.1.31			
Subnet Mask	255.255.0.0			
Gateway IP Address	0.0.0.0			
Ready	Radio: Protected Station	Active Unit: F	rimary	Logout ADMIN

See 'IP > IP Summary > Bridge / Gateway Router Modes' on page 147 for configuration options.



Protected Station: IP > IP Setup

This page provides the setup for the Protected Station Networking IP setup.

GARF SUPERVISOR					Aprisa 🛲
Protected Station	AUX TX RX OK MODE A O O O O O mary Secon	AUX TX RX O O O Idary	Network		
Terminal Radio Serial E	thernet IP QoS Sec	curity Maintenance	Events Software	Monitoring	
IP Summary Terminal Server Su	mmary IP Setup Termina	al Server Setup L3 I	Filtering IP Routes		
NETWORKING IP SETTINGS Virtual IP Address Primary IP Address Secondary IP Address Subnet Mask Gateway IP Address Save Cancel	172.10.1.50 172.10.1.30 172.10.1.31 255.255.0.0 0.0.0				
_	_				
Ready	Radio: Protected Station		Active Unit: Primary		Logout ADMIN

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. 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. The default IP address is in the range 169.254.50.10.



Protected Station Virtual IP Address (PVIP)

The Protected Station Virtual IP Address (PVIP) is the IP Address of the active radio whether it is the primary radio or the secondary radio.

The PVIP is available in both bridge and router modes.

In router mode, the PVIP can be used as 'next hop' IP address by external routers to reach the protected station so the protection station switch will always be transparent to the external devices and routers.

In both bridge and router modes, the PVIP is used in terminal server mode in remote protected stations. The PVIP is used to reach the protected remote station from the SCADA master connected to base station in terminal server mode.

Note: The radio IP address should be used for SNMP management as using the PVIP for SNMP management will result in undefined behaviour if a switch-over occurs during an SNMP transaction. Thus, using PVIP for SNMP network management is not recommended.

After a switch-over, new active radio owns the PVIP and will send out a gratuitous ARP to clear the MAC learning tables of upstream switches/routers.

Set the static IP Address of the PVIP using the standard format xxx.xxx.xxx. 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. 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. 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. 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. The default subnet mask is 255.255.0.0 (/16).

Note 1: If the base station RF interface IP address is a <u>network IP address</u>, 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 217).



Security

Protected Station: Security > Setup

This page displays the current settings for the Security parameters.

4RF SUPERVISOR			Aprisa 🛲
Protected Base OK MOI Station	DE AUX TX RX OK MODE AUX TX RX O O O O O O O O O Primary Secondary	Network	
Terminal Radio Serial	Ethernet IP QoS Security Maintena	ince Events Software Monit	oring
Summary Setup Users	SNMP RADIUS Manager Distribution		
_			
PAYLOAD SECURITY PROFIL	LE SETTINGS	PROTOCOL SECURITY SETTING	38
Security Profile Name	Payload Security v1	Telnet	Enabled Disabled
Security Scheme	Disabled	ICMP	Enabled Disabled
Payload Encryption Key Type	Passphrase V	HTTPS	O Enabled Disabled
Payload Encryption Key Size	AES-128 V	SNMP Proxy Support	Enabled Disabled
Payload Encryption Key		SNMP Protocol	All Versions 🗸
Save Cancel		Save Cancel	
KEY ENCRYPTION KEY SET	TINGS	SECURITY LEVEL SETTINGS	
Key Encryption Key Type	Passphrase V	Security Level	Standard V
Key Encryption Key Size	AES-256 V	Save Cancel	
Key Encryption Key			
USB Transaction Status	USB Storage Not Detected on Primary or Secondary		
Save Cancel	oad Primary from USB Copy Primary to USB		
Los	ad Secondary from USB Copy Secondary to USB		
Ready	Radio: Protected Base Station	Active Unit: Primary	Logout ADMIN

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.

4RF SUPERV	ISOR				Aprisa 🛲
Protected Base Station	OK MODE AUX TX RX OK MODE AUX TX O O O O O O O O O Primary Secondary	K RX Net	vork		
Terminal Radio	Serial Ethernet IP QoS Security	Maintenance Eve	ts Software	Monitoring	
Summary Setup	Users SNMP RADIUS Manager Dis	tribution			
PRIMARY CURREN	T PAYLOAD SECURITY PROFILE	SECO	IDARY CURRENT	T PAYLOAD SECURITY PROFILE	
Profile Name	Migrated Key	Profile	Name	Migrated Key	
PRIMARY PREVIOU	S PAYLOAD SECURITY PROFILE	SECO	IDARY PREVIOU	S PAYLOAD SECURITY PROFILE	:
Profile Name	Unknown	Profile	Name	Unknown	
Status	Inactive	Status		Inactive	
Activate		Activa	e		
Apply Cancel		Apply	Cancel		
PRIMARY PREDEFI	NED PAYLOAD SECURITY PROFILE	SECO	IDARY PREDEFI	NED PAYLOAD SECURITY PROF	ILE
Profile Name	Unknown	Profile	Name	Unknown	
Status	Available	Status		Available	
Activate		Activa	e		
Apply Cancel		Apply	Cancel		
Busy	Radio: Protected Base Station	Active U	nit: Primary		Logout ADMIN

PRIMARY / SECONDARY SECURITY PROFILE

See 'Security > Manager' on page 199 for parameter details.



Maintenance

Protected Station: Maintenance > General

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

4RF SUPERVISOR			Aprisa 🛲
Protected Station OK MODE AUX	TX RX OK MODE AUX TX RX O O O O O O O Secondary	Network	
Terminal Radio Serial Ether	met IP QoS Security Mainten	ance Events Software Monitoring	
Guinnary General Test mode			
GENERAL		PROTECTED STATION REBOOT	
Local Status Polling Period (s)	10	Reboot	
Remote Status Polling Period (s)	20	Save Cancel	
Network View Polling Period (s)	20		
Inactivity Timeout (min)	1440 (24h) V	PRIMARY REBOOT	
Delete Alarm History File		Reboot	
Save Cancel		Save Cancel SECONDARY REBOOT	
		Rehoot	
		Save Cancel	
Ready	Radio: Protected Station	Active Unit: Primary	Logout ADMIN

See 'Maintenance > General' on page 208 for parameter details.



Protected Station: Maintenance > Protection

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

<i>4</i>RF SUPERVISOR				Aprisa 🛲
Protected Station OK MOD	E AUX TX RX OK MODE AUX TX O O O O O O Primary Secondary	RX Network		
Terminal Radio Serial	Ethernet IP QoS Security	Maintenance Events Soft	ware Monitoring	
Summary General Test Me	ode Modem Defaults Protection	Protection Copy Licence	Advanced	
SOFTWARE MANUAL LOCK Lock Type Lock Active To Duration (s) Save Cancel Switch Now	Disable V Primary V 0			
Switch Control	Automatic			
Active Unit	Primary			
Switch Count	0			
Ready	Radio: Protected Station	Active Unit: Primary		Logout ADMIN

SOFTWARE MANUAL LOCK

The software Manual Lock is a software implementation of the Hardware Manual Lock switch on the Protection Switch.

Lock Active To

This parameter sets the Protection Switch Software Manual Lock. The Software Manual Lock only operates if the Hardware Manual Lock is deactivated (set to the Auto position).

Option	Function
Automatic	The protection is automatic and switching will be governed by normal switching and blocking criteria.
Primary	The primary radio will become active i.e. traffic will be switched to the primary radio.
Secondary	The secondary radio will become active i.e. traffic will be switched to the secondary radio.

Duration (s)

This parameter defines the period required for manually locking to the primary or secondary radios. When this period elapses, the Lock To becomes automatic.

Switch Now Button

This button forces a switch-over independent of the state of Lock Type.



CURRENT PROTECTION INFORMATION

Switch Control

This parameter shows the status of the switch control i.e. which mechanism is in control of the protection switch.

Option	Function
Automatic	The protection is automatic and switching will be governed by normal switching and blocking criteria.
Software Manual Lock	The Software Manual Lock has control of the protection switch.
Hardware Manual Lock	The Hardware Manual Lock has control of the protection switch.

Active Unit

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

Switch Count

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

Automatic Periodic Switch will occur in

If this parameter is visible, the Automatic Periodic Switch feature has been enabled and will show the period before the next automatic switch-over.



Protected Station: Maintenance > Protection Copy

This page provides the management and control of the Protected Station Maintenance Protection Copy.

4RF SUPERVISOR				Aprisa 🛲
Protected Station OK MODE #	AUX TX RX OK MODE AUX TX RX $\Theta \Theta \Theta \Theta \Theta \Theta \Theta \Theta \Theta$ hary Secondary	Network		
Terminal Radio Serial Et	hernet IP QoS Security Mai	ntenance Events Soft	ware Monitoring	
Summary General Test Mode	Modem Defaults Protection P	Protection Copy Licence	Advanced	
COPY CONFIGURATION Copy from Primary to Secondary Copy from Secondary to Primary Copy Status Save Cancel NB: This function can not copy user-idas	Available			
CURRENT PROTECTION INFORM	ATION			
Switch Control	Automatic			
Active Unit	Primary			
Switch Count	0			
Ready	Radio: Protected Station	Active Unit: Primary		Logout ADMIN

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 CONFIGURATION	
Copy from Primary to Secondary	
Copy from Secondary to Primary	
Copy Status	Processing, 8% completed
Save	

Copy from Secondary to Primary

This parameter copies all common parameters from the secondary to the primary radio.

Copy Status

This parameter displays the status of the Copy Configuration.

Option	Function
Available	The Copy Configuration feature can be used (but not necessarily required).
Processing	The Copy Configuration feature is running and the % completed.

CURRENT PROTECTION INFORMATION

Switch Control

This parameter shows the status of the switch control i.e. which mechanism is in control of the protection switch.

Option	Function
Automatic	The protection is automatic and switching will be governed by normal switching and blocking criteria.
Software Manual Lock	The Software Manual Lock has control of the protection switch.
Hardware Manual Lock	The Hardware Manual Lock has control of the protection switch.

Active Unit

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

Switch Count

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

Automatic Periodic Switch will occur in

If this parameter is visible, the Automatic Periodic Switch feature has been enabled and will show the period before the next automatic switch-over.