

The information in this manual is intended to assist with equipment design and ensure proper installation.

READ THIS INSTRUCTION FIRST

To avoid serious or fatal personal injury or major property damage, read and follow all safety instruction in this manual. If you require additional assistance, please contact SOLEXY.

SAFETY INSTRUCTION TO HAZARDOUS AREA INSTALLATION

- It is the responsibility of the installer and the end-user to ensure that the Solexy WA/WS enclosures are installed and maintained according to the suitable standards for electrical application in potentially explosive atmospheres (example IEC/EN 60079-14, IEC/EN60079-17) and any other relevant electrical code.
- Suitably trained personnel shall carry out installation according with applicable code practice.
- Read this first and keep this instruction manual always available.

MARKING

SWA and SWS unit:

 I M2 Ex db I Mb (SWS only)
II 2G Ex db IIA/IIB/IIC ⁽¹⁾ T6...T4 Gb
II 2D Ex tb IIIC T110°C...T140°C Db

SWA and SWS unit complete of Solexy RX, SX or UX antenna barriers:

 I M2(M1) Ex db mb [ia Ma] I Mb (SWS only)
II 2(1)G Ex db mb [ia Ga] IIA/IIB/IIC ⁽¹⁾ T6...T5 Gb
II 2(1)D Ex tb IIIC T80°C...T100°C Db

⁽¹⁾ Refer to product marking for gas group details

This instruction refers to certified equipment covered by following certificate:

ATEX: FIDI 20 ATEX 0014
IECEx: IECEx EXA 14.0001

WARNINGS

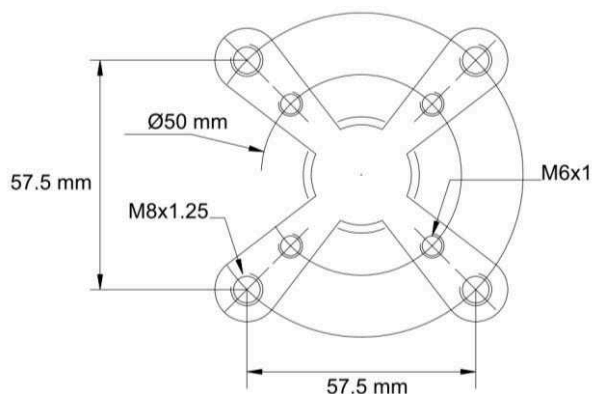
- Warns of hazard that MAY cause serious personal injury, death or major property damage.
- DISCONNECT THE EQUIPMENT FROM THE SUPPLY CIRCUIT BEFORE OPENING. KEEP ASSEMBLY TIGHTLY CLOSED WHEN IN OPERATION.
- DISCONNECT ALL POWER BEFORE SERVICING EQUIPMENT.
- HAZARDOUS VOLTAGE
- DO NOT REMOVE COVER WHEN ENERGISED.
- DO NOT OPEN WHEN AN EXPLOSIVE ATMOSPHERE IS PRESENT.

NOTES

- To avoid the thread cover blocking the thread joint can be protected with greases like Nyogel 760G, Uniflor 8512R, Uniflor 8911 or equivalent compatible with Silicone (VMQ) and Fluorosilicone (FVMQ) gasket.
- The user should not repair this equipment.
- The flameproof joints are not intended to be repaired.
- The user should not modify the unit.
- The unit should not be painted by the user.
- If the equipment is likely to come in to contact with aggressive substances, it is responsibility of the user to take suitable precautions that prevent it from being adversely affected, thus ensuring that the type of protection is not compromised. Aggressive substances: example Acids, liquids, gases with can affected metals.
- The metallic alloy used for the enclosure, in the event of a rare accident, could cause ignition sources due to impact or friction (sparks may occur). This shall be considered when the box is installed in group Ex area.
- Remove plastic plugs or plastic stickers supplied with enclosure before installation. The conduit plugs supplied are for transit purposes only, these components aren't certified.
- Weatherproof levels depend on cable gland and cabling methods used.
- For functionality of device installed inside the enclosure refer to the device's instruction.
- Use only cable glands and plugs that are suitable for the type of protection and maintain the enclosure's environmental protection rating.
- Any unused entries must be filled with appropriate equipment (i.e. plugs) that are suitable for the type of protection and maintain the enclosure's environmental protection rating.

INSTALLATION

1. The unit can be installed in all position.
2. Fix the unit using n° 4 M6x10 or M8x10 bolts



GROUNDING

1. Grounding needs to be made according to suitable standards for electrical application in potentially explosive atmospheres and/or other national standards.
2. The electrical devices must be grounded using their internal and external M4 grounding connections.

ELECTRICAL WIRING

1. Remove screw cover, remove protection plugs from cable entries and substitute them with cable glands or conduits or plugs suitable for the type of protection required.
2. Connect terminal strip and/or connector according to device's instruction manual.
3. Check that thread joint were free of foreign matters and deformations check the seal is properly fitted in the slot.
4. Reassemble screw cover and lock it by means of the screw or anti-rotation kit.
5. The cover must be screwed and securely locked to the body.

OPERATION

Refer to the device's instruction manual for set-up and functionality

PRODUCT'S STORAGE

Keep the boxes away from atmospheric agents

MAINTENANCE

- The verification and maintenance of the electrical equipment must be performed according to suitable standards for electrical application in potentially explosive atmospheres and/or other national standards.
- The user should guarantee the keeping of the safety characteristic of the device after maintenance.
- The cover must be securely locked to the body.
- After every opening must check before closing that the thread joint is free of foreign matters and deformations and if necessary lubricate the thread joint in order to

avoid cover blocking with greases like Nyogel 760G, Uniflor 8512R, Uniflor 8911 compatible with silicone or fluorosilicone gasket or equivalent according to enclosure temperature range.

- In order to guarantee the weatherproof level, it's necessary that the gasket needs to be in good conditions and it shall be verified after every opening. In case of gasket's damage replace with Solexy spare part.
- The maintenance related to the components used for wiring must be performed according to manufacturer instruction.

DISPOSAL / RECYCLING

Disposal and recycling of the product according to national regulation for waste disposal and recycling.

WARNING: Do not dispose of the product and the components in the environment.

MODEL NOMENCLATURE

X	XX	XXX	XX	-	XX	X	XX	-	XXXXX
1	2	3	4	-	5	6	7	-	8

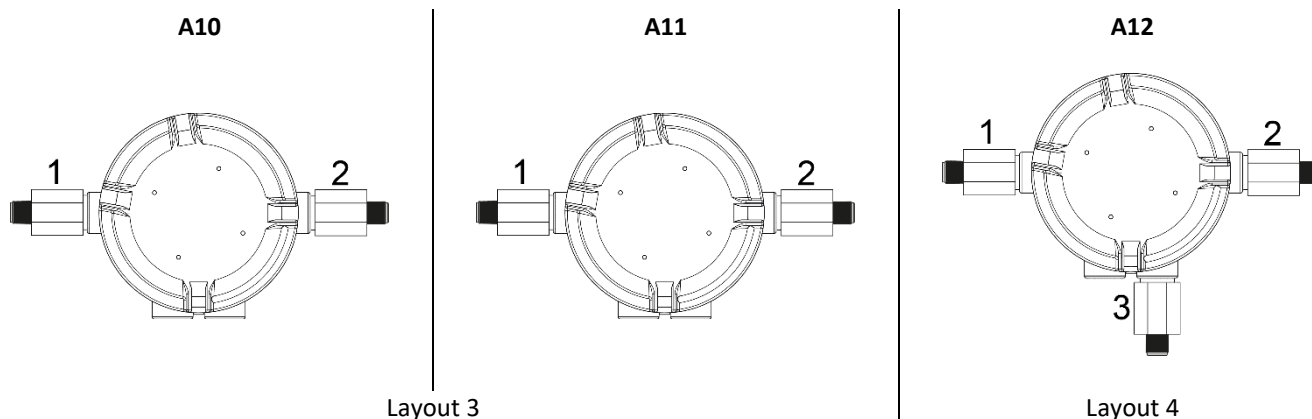
- 1 *Family*
S Enclosure supply with the electronic device
- 2 *Series*
WA aluminum enclosure
WS stainless steel enclosure
- 3 *Device*
XXX 1 digit for device type installed
2 digit for device version
- 4 *Antenna barrier*
XX 2 digit for Solexy Antenna Barrier if used (optional components)
00 for unit without Solexy Antenna Barrier
- 5 *Cable entries*
XX 2 digits for cable entries combination
- 6 *Color - Brand*
X 1 digit for housing's color and/or brand
- 7 *Certification Mark*
X0 Atex and IECEx (group II)
M0 Atex and IECEx (group I and group II)
X* Atex and IECEx (group II) + a second standard marking
M* Atex and IECEx (group I and group II) + a second standard marking
- 8 *Special execution*
XXXXX various, consult Solexy

DESCRIPTION	1
POWER SUPPLY	1
AMBIENT TEMPERATURE RANGE AND SURFACE TEMPERATURE	1
WIRING	2
DEVICE CONFIGURATION.....	3
TROUBLESHOOTING AND LED DEFINITION.....	7
ANTENNA LAYOUT	7
RF INFORMATION.....	8
MAXIMUM PERMITTED RF THRESHOLD POWER (Pth)	10
MAXIMUM JOULES CALCULATION IN CASE OF COAX CABLE INSTALLATION.....	10

DESCRIPTION

The SWA & SWS A series is a WiFi access point equipped with 1 Ethernet port and up to 3 WiFi ports as follows:

Device version	Model	WiFi Port
A10	WiFi Access point 802.11n MIMO 2x2	n° 2
A11	WiFi Access point 802.11ac MIMO 2x2	n° 2
A12	WiFi Access point 802.11n MIMO 2x2 plus 802.11ac (1 stream)	n° 3



POWER SUPPLY

Screw terminals = Supply voltage: 18 ~ 60 VDC

RJ45 connector = PPoE @ 24 VDC or PoE @ 48 VDC *

Max Power Consumption 8W

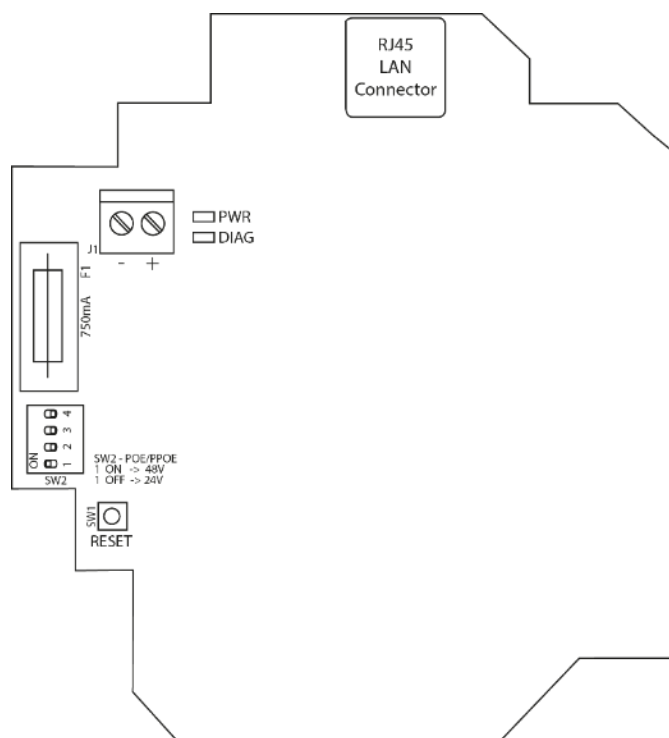
* PPoE = Passive Power over Ethernet (operating voltage 24VDC), PoE = Power over Ethernet (operating voltage 48VDC)

AMBIENT TEMPERATURE RANGE AND SURFACE TEMPERATURE

	Min. ambient temperature	Max ambient temperature	Max surface temperature	T Class
SWAA	-40°C	+60°C	+70°C	Gas = T6...T5 Dust = T80°C...T100°C
SWSA	-40°C	+50°C	+70°C	Gas = T6...T5 Dust = T80°C...T100°

The unit can reach a surface temperature of 70°C, use cable and cable glands / conduit Ex certified suitable for this temperature.

WIRING



Label **Description**
RJ45 LAN connector
(PPoE @24VDC or PoE @ 48VDC)*

J1
Label **Description**
- Power supply - (18 ~ 60 VDC)
+ Power supply + (18 ~ 60 VDC)

F1
Label **Description**
750mA 5x20 mm power line fuse
(750mA fast-blow type)

Label **Description**
PWR Power led indication
DIAG Diagnostic led indication

SW1
Label **Description**
RESET Reset button

SW2
Label **Description**
POE/PPoE DIP switch for PoE / PPoE selection *
1 ON = 48V = PoE
1 OFF = 24V = PPoE

DIP switch operate only in case of PoE/PPoE power supply

* PoE = Power over Ethernet
(operating voltage 48VDC)
PPoE = Passive Power over Ethernet
(operating voltage 24VDC)

Step 1 – ANTENNA CONNECTION

Connect the antenna before to turn on the device.

WARNING : use antenna only with 50Ω impedance and with operating frequency in according to technical data listed into the above paragraph “RF information”.

The device must be set according to limitation listed at paragraph MAXIMUM PERMITTED RF THRESHOLD POWER (Pth) for installation in Hazardous Location and the national regulation rules.

Step 2 – POWER SUPPLY CONNECTION

WARNING : DO NOT WIRED POWER SUPPLY WHEN AN EXPLOSIVE ATMOSPHERE IS PRESENT.

FOR SAFETY REASONS WIRING MUST BE MADE ACCORDING TO WA & WS INSTALLATION AND OPERATION MANUAL IM0009

The device can be powered by terminal strip (J1 18 ~ 60 VDC) or through PoE/PPoE.

In case of PoE (Power over Ethernet, 48VDC) set the DIP Switch SW2 nr. 1 to ON,

In case of PPoE (Passive Power over Ethernet, 24 VDC) set the DIP Switch SW2 nr. 1 to OFF

The DIP switch position has no influence in case of power supply through terminal strip J1

The device has no ON/OFF switch. It turns on automatically when power is applied. Check that the PWR led turn on
The DIAG led stay off for around 40 seconds, until the device is fully ready to use. Then the DIAG led turns blue.

Step 3 – ETHERNET CONNECTION

Connect the Ethernet cable (if it not connected in case of PoE or PPoE).

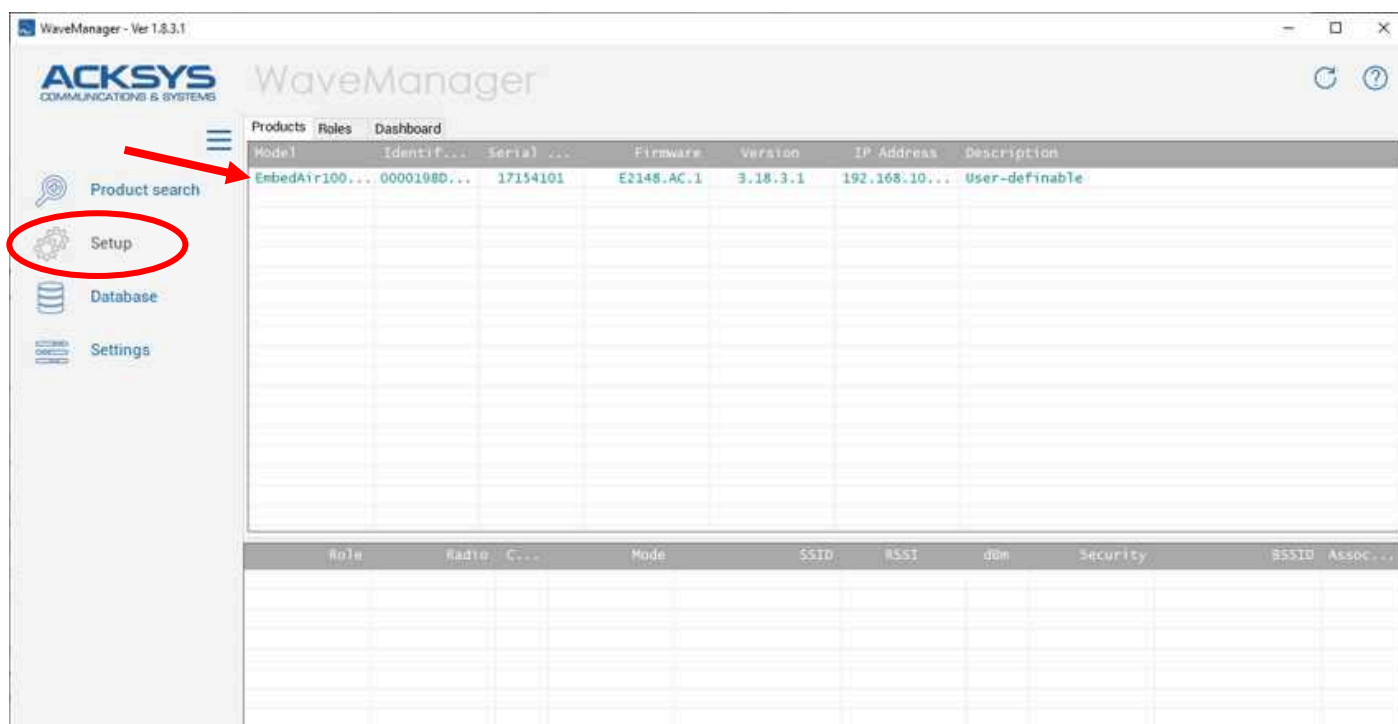
DEVICE CONFIGURATION

FACTORY SETTINGS:

- IP address: 192.168.1.253
- Radio Interface disable, preset for access point mode
- SSID: acksys (broadcast)
- No security (no WEP, no WAP, no WAP2, no MAC filter)
- 802.11n or ac mode, 5GHz band, auto-channel
- WEB interface for device configuration:
 - IP address: 192.168.1.253
 - User name: root
 - Password: no password set as factory setting

Step 1

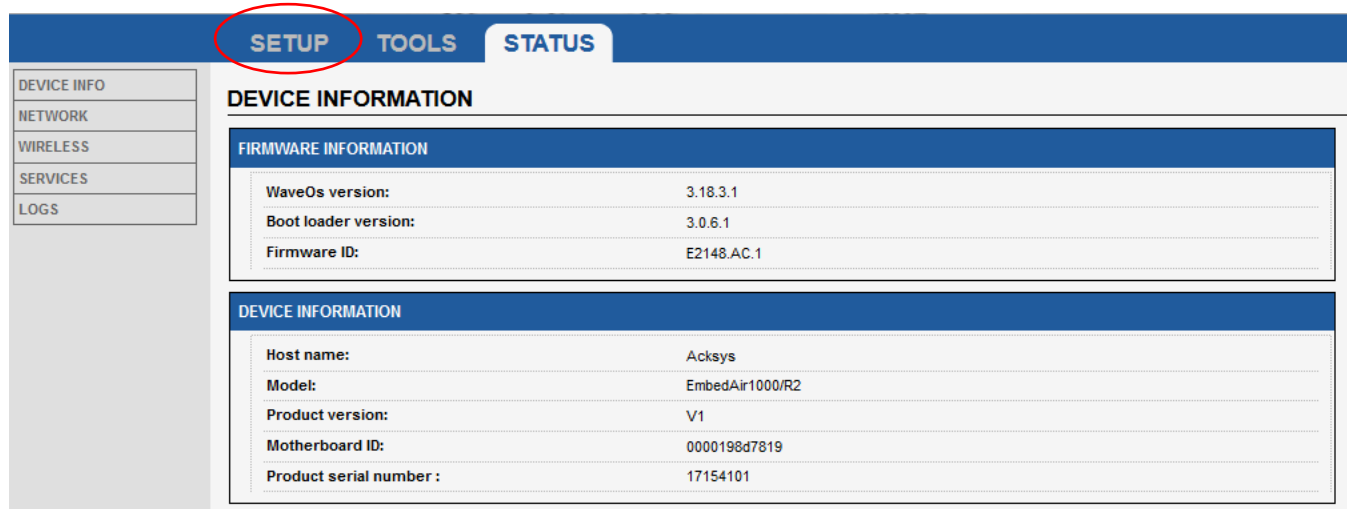
Verify that the IP address factory setting is compatible with your network, if the IP address is not suitable for your network use Windows application **WaveManager** (available on web site www.acksys.com).



After the WaveManager installation run the application, select the EmbedAir1000 device then click to “Setup”: now you can configure the IP address or you can activate the DHCP client.

Step 2

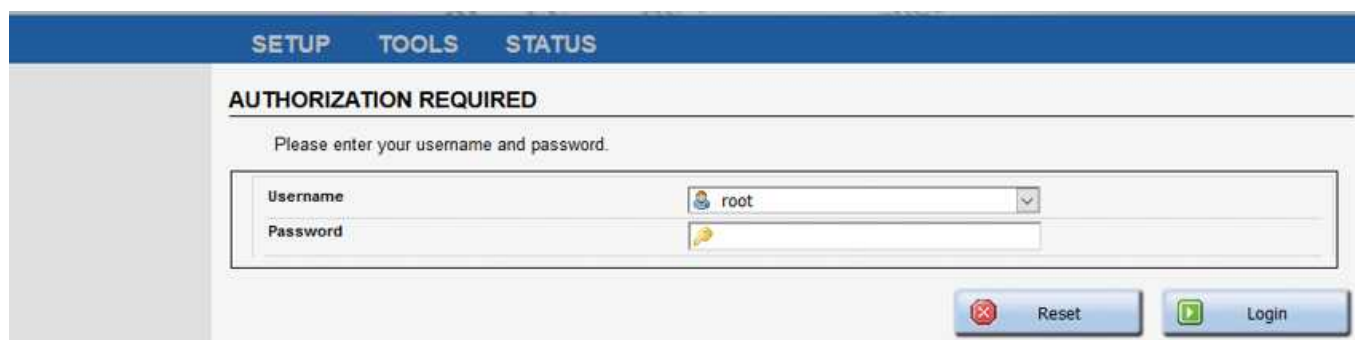
Using your web browser open the WEB interface (IP address: 192.168.1.253) and select the "SETUP" tab:



FIRMWARE INFORMATION	
WaveOs version:	3.18.3.1
Boot loader version:	3.0.6.1
Firmware ID:	E2148.AC.1

DEVICE INFORMATION	
Host name:	Acksys
Model:	EmbedAir1000/R2
Product version:	V1
Motherboard ID:	0000198d7819
Product serial number :	17154101

For setup page is required User name and password and for factory setup the user name is **root** and no password is required (these data can be changed under "TOOLS" tab, PASSWORD SETTINGS section)



Username: root

Password:

Reset Login

On the "WIRELESS INTERFACES OVERVIEW" page you should first select your **country** in order to enforce applicable **regulation rules**. The country selector is located in the global parameters, near the bottom of the page

SETUP **TOOLS** **STATUS**

PHYSICAL INTERFACES
VIRTUAL INTERFACES
NETWORK
VPN
BRIDGING
ROUTING / FIREWALL
QOS
SERVICES

WIRELESS INTERFACES OVERVIEW

You can set up to 8 simultaneous roles (wifi interface types) per radio card, among the following combinations:

Combination	Channel selection		Max number of interfaces			
	Multiplicity	Can use DFS	Access point	Infrastructure client	Mesh point	Ad-hoc
802.11ac radio cards						
Multiple access points	single, auto, multiple	yes	8			
Client / bridge	single, auto, multiple, roaming*	yes		1		
SRCC	single	yes	auto	auto		
Other / Ad-hoc	single	no			unsupported	unsupported
802.11n only radio cards						
Multiple access points	single, auto, multiple	yes	8			
Portal	single	no	8		1	
Client / bridge	single, auto, multiple, roaming	yes		1		
Other / repeater	single	no	8	1 (non-roaming)	1	1

When using several roles, they all use the same shared channel; in this case, the client role must not be set to multichannel roaming. Repeater mode is a combination of two roles: access point + client.

* The roaming feature is not yet available for IEEE802.11ac cards.

WI-FI INTERFACE



WiFi 1: Wi-Fi 4 (802.11n) Wireless interface



CHANNEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
5	802.11g+n	acksys_1_2_4_test	Access Point (infrastructure)	WPA2-PSK (Personal)	 

WI-FI INTERFACE



WiFi 2: Wi-Fi 5 (802.11ac) Wireless interface



CHANNEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
48	802.11ac+n	acksys_2_5_test	Access Point (infrastructure)	WPA2-PSK (Personal)	Interface disabled

GLOBAL PARAMETERS

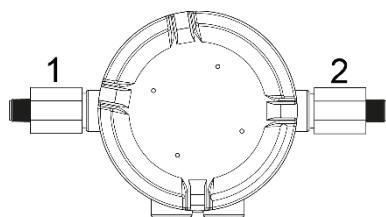
RADIO REGULATION AREA

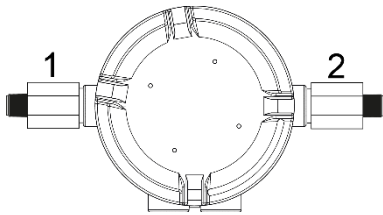
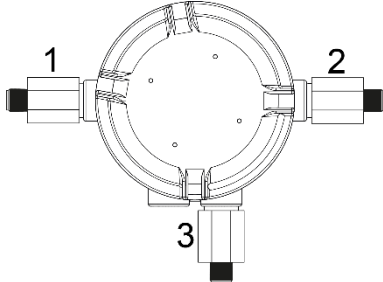
Country

United States

You can select radio interface to set up its WiFi parameters (you can also change IP configuration and services).

In function of device version the WiFi Interface available are:

Device version	Model		WiFi Interface used
A10	WiFi Access point 802.11n MIMO 2x2		WiFi Interface 1 only (antenna 1 and 2)

A11	WiFi Access point 802.11ac MIMO 2x2		WiFi Interface 2 only (antenna 1 and 2)
A12	WiFi Access point 802.11n MIMO 2x2 plus 802.11ac (1 stream)		WiFi Interface 1 (antenna 1 & 2) and WiFi Interface 2 (antenna 3)

For WiFi and LAN interface setup click on relative menu on “PHYSICAL INTERFACES” menu:

PHYSICAL INTERFACES

WIFI 1

WIFI 2

LAN

VIRTUAL INTERFACES

NETWORK

VPN

BRIDGING

ROUTING / FIREWALL

QOS

SERVICES

SETUP

TOOLS

STATUS

WIRELESS SETTINGS : WIFI 1

The *Device Configuration* section covers physical settings of the radio hardware which is shared among all defined wireless networks. Per network settings like encryption or operation mode are in the *Interface Configuration*.
If *SRCC* role is selected, most of the *Device Configuration* is irrelevant (please refer to the product user guide).

DEVICE CONFIGURATION

General Setup

a/b/g Data Rates

802.11n Mcs

Advanced Settings

802.11 mode

802.11g+n (2.4 GHz)

Changing the mode may affect the list in the 'a/b/g data rates' tab

HT mode

40MHz 2nd channel below

Automatic 40MHz HT mode is not compatible with AP, Ad-hoc, Mesh and multi-interfaces

Automatic channel select

☐

Automatic channel select is not compatible with Ad-hoc, Mesh and multi-interfaces

Channel

5 (2.432 GHz) - Max Tx power 20 dBm

6 (2.437 GHz) - Max Tx power 20 dBm

7 (2.442 GHz) - Max Tx power 20 dBm

8 (2.447 GHz) - Max Tx power 20 dBm

9 (2.452 GHz) - Max Tx power 20 dBm

10 (2.457 GHz) - Max Tx power 20 dBm

This field is ignored in client proactive roaming mode; see 'Roaming' tab instead

INTERFACE CONFIGURATION

General Setup

Wireless Security

Advanced Settings

MAC Filter

Frame filters

Security

WPA2-PSK (Personal)

Protected management frame (802.11w)

disable

Pre-Shared Key

••••••••

This key must have a length from 8 to 63 characters. If the key length is 64 characters it will be used directly as hexadecimal format

Group rekey interval

600

Time interval for rekeying the GTK (broadcast/multicast encryption keys) in second

Pair rekey interval

600

Time interval for rekeying the PTK (unicast encryption keys) in second

Master rekey interval

86400

Time interval for rekeying the GMK (master key used internally to generate the GTK) in second

Set for each WiFi interface the following essential parameters:

- The operating mode: 802.11 mode, radio channel (take care about local legislation), SSID
- WiFi security parameters (WEP, WPA, WPA-PSK, WPA2, WPA2-PSK, SSID broadcast or not)

For more details consult Acksys WaveOS User Guide.

TROUBLESHOOTING AND LED DEFINITION

None of the LED indicators turn ON

- Verify the power supply (voltage, cabling)
- Verify the fuse F1

The WiFi link does not come up

- Make sure that the Wireless parameters of the Client (case sensitive SSID, 802.11 mode, radio channel and security) match those of the AP
- Check the radio conditions: distance between devices, placement of antennas, interferences and obstacles to radio waves propagation
- Try with all securities and encryption settings temporarily disabled
- Try another radio channel

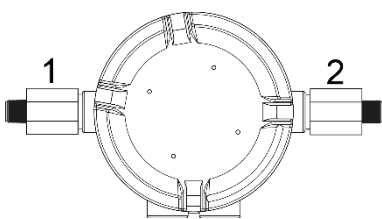
How to restore factory settings?

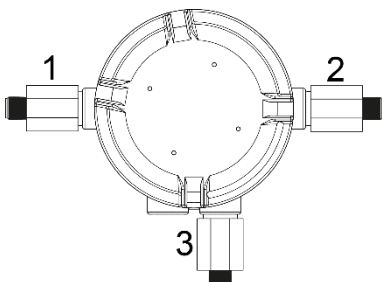
- If the built-in web-based interface is reachable, you can use a browser to restore factory settings.
- Else, power up the unit, wait for the DIAG led to turn blue, then hold down the reset button (for at least 2 seconds) until DIAG goes off. Then release it and wait for the DIAG led to turn blue again, meaning that the product rebooted with its factory settings.

LED Definition

LED	Function
PWR	Green : power on Off : power not present
DIAG	Blue : when product is OK and initialized Flashing : when firmware in flash is not valid Off : for more than 2min with PWR led green indicate a Hardware/Software failure

ANTENNA LAYOUT

A1033 A1133	WiFi Access Point		Antenna 1 - WiFi Antenna 2 - WiFi
------------------------------	-------------------	--	--------------------------------------

A1230	WiFi Access Point		Antenna 1 - WiFi Antenna 2 - WiFi Antenna 3 - WiFi
--------------	-------------------	--	--

RF INFORMATION

Device version																																							
A10	<p>ANTENNA 1 AND 2 *</p> <p>Radio modes: Support for IEEE 801.11a/h, 802.11b, 802.11g and 802.11n</p> <p>Frequency band for 802.11a/n : 5 GHz; 5.170 to 5.835 GHz</p> <p>Frequency band for 802.11b/g/n : 2.4 GHz; 2.402 to 2.494 GHz</p> <p>Tx output power (Radio card output per chain, antenna excluded)</p> <table> <tr> <td>802.11n HT20 2.4GHz band</td><td>20.5 dBm @ 7.2 Mbps (MCS 0)</td></tr> <tr> <td></td><td>18 dBm @ 72.2 Mbps (MCS 7)</td></tr> <tr> <td>802.11n HT40 2.4GHz band</td><td>20.5 dBm @ 15 Mbps (MCS 0)</td></tr> <tr> <td></td><td>18 dBm @ 150 Mbps (MCS 7)</td></tr> <tr> <td>802.11n HT20 5GHz band</td><td>18 dBm @ 7.2 Mbps (MCS 0)</td></tr> <tr> <td></td><td>15 dBm @ 72.2 Mbps (MCS 7)</td></tr> <tr> <td>802.11n HT40 5GHz band</td><td>18 dBm @ 15 Mbps (MCS 0)</td></tr> <tr> <td></td><td>15 dBm @ 150 Mbps (MCS 7)</td></tr> </table> <p><i>Value for 1 stream, add 3 dBm for 2 streams</i></p>	802.11n HT20 2.4GHz band	20.5 dBm @ 7.2 Mbps (MCS 0)		18 dBm @ 72.2 Mbps (MCS 7)	802.11n HT40 2.4GHz band	20.5 dBm @ 15 Mbps (MCS 0)		18 dBm @ 150 Mbps (MCS 7)	802.11n HT20 5GHz band	18 dBm @ 7.2 Mbps (MCS 0)		15 dBm @ 72.2 Mbps (MCS 7)	802.11n HT40 5GHz band	18 dBm @ 15 Mbps (MCS 0)		15 dBm @ 150 Mbps (MCS 7)																						
802.11n HT20 2.4GHz band	20.5 dBm @ 7.2 Mbps (MCS 0)																																						
	18 dBm @ 72.2 Mbps (MCS 7)																																						
802.11n HT40 2.4GHz band	20.5 dBm @ 15 Mbps (MCS 0)																																						
	18 dBm @ 150 Mbps (MCS 7)																																						
802.11n HT20 5GHz band	18 dBm @ 7.2 Mbps (MCS 0)																																						
	15 dBm @ 72.2 Mbps (MCS 7)																																						
802.11n HT40 5GHz band	18 dBm @ 15 Mbps (MCS 0)																																						
	15 dBm @ 150 Mbps (MCS 7)																																						
A11	<p>ANTENNA 1 AND 2 *</p> <p>Radio modes: Support for IEEE 801.11a/h, 802.11b, 802.11g, 802.11n and 802.11ac</p> <p>Frequency band for 802.11a/n : 5 GHz; 5.170 to 5.835 GHz</p> <p>Frequency band for 802.11b/g/n : 2.4 GHz; 2.402 to 2.494 GHz</p> <p>Tx output power (Radio card output per chain, antenna excluded)</p> <table> <tr> <td>802.11b 2.4GHz band</td><td>20 dBm @ 1 Mbps</td></tr> <tr> <td></td><td>20 dBm @ 11 Mbps</td></tr> <tr> <td>802.11g 2.4GHz band</td><td>21 dBm @ 6 Mbps</td></tr> <tr> <td></td><td>18 dBm @ 54 Mbps</td></tr> <tr> <td>802.11a 5GHz band</td><td>20 dBm @ 6 Mbps</td></tr> <tr> <td></td><td>15 dBm @ 54 Mbps</td></tr> <tr> <td>802.11n HT20 2.4GHz band</td><td>21 dBm @ 7.2 Mbps (MCS 0)</td></tr> <tr> <td></td><td>16 dBm @ 72.2 Mbps (MCS 7)</td></tr> <tr> <td>802.11n HT40 2.4GHz band</td><td>20 dBm @ 15 Mbps (MCS 0)</td></tr> <tr> <td></td><td>16 dBm @ 150 Mbps (MCS 7)</td></tr> <tr> <td>802.11n/ac VHT20 5GHz band</td><td>19 dBm @ 7.2 Mbps (MCS 0)</td></tr> <tr> <td></td><td>14 dBm @ 72.2 Mbps (MCS 7)</td></tr> <tr> <td></td><td>13 dBm @ 86.7 Mbps (VHT MCS 8)</td></tr> <tr> <td>802.11n/ac VHT40 5GHz band</td><td>18 dBm @ 15 Mbps (MCS 0)</td></tr> <tr> <td></td><td>14 dBm @ 150 Mbps (MCS 7)</td></tr> <tr> <td></td><td>13 dBm @ 200 Mbps (VHT MCS 9)</td></tr> <tr> <td>802.11ac VHT80 5GHz band</td><td>18 dBm @ 32.5 Mbps (MCS 0)</td></tr> <tr> <td></td><td>14 dBm @ 325 Mbps (MCS 7)</td></tr> <tr> <td></td><td>13 dBm @ 433.3 Mbps (VHT MCS 9)</td></tr> </table> <p><i>Value for 1 chain, add 3 dBm for 2 chains (Tolerance ± 2 dB)</i></p>	802.11b 2.4GHz band	20 dBm @ 1 Mbps		20 dBm @ 11 Mbps	802.11g 2.4GHz band	21 dBm @ 6 Mbps		18 dBm @ 54 Mbps	802.11a 5GHz band	20 dBm @ 6 Mbps		15 dBm @ 54 Mbps	802.11n HT20 2.4GHz band	21 dBm @ 7.2 Mbps (MCS 0)		16 dBm @ 72.2 Mbps (MCS 7)	802.11n HT40 2.4GHz band	20 dBm @ 15 Mbps (MCS 0)		16 dBm @ 150 Mbps (MCS 7)	802.11n/ac VHT20 5GHz band	19 dBm @ 7.2 Mbps (MCS 0)		14 dBm @ 72.2 Mbps (MCS 7)		13 dBm @ 86.7 Mbps (VHT MCS 8)	802.11n/ac VHT40 5GHz band	18 dBm @ 15 Mbps (MCS 0)		14 dBm @ 150 Mbps (MCS 7)		13 dBm @ 200 Mbps (VHT MCS 9)	802.11ac VHT80 5GHz band	18 dBm @ 32.5 Mbps (MCS 0)		14 dBm @ 325 Mbps (MCS 7)		13 dBm @ 433.3 Mbps (VHT MCS 9)
802.11b 2.4GHz band	20 dBm @ 1 Mbps																																						
	20 dBm @ 11 Mbps																																						
802.11g 2.4GHz band	21 dBm @ 6 Mbps																																						
	18 dBm @ 54 Mbps																																						
802.11a 5GHz band	20 dBm @ 6 Mbps																																						
	15 dBm @ 54 Mbps																																						
802.11n HT20 2.4GHz band	21 dBm @ 7.2 Mbps (MCS 0)																																						
	16 dBm @ 72.2 Mbps (MCS 7)																																						
802.11n HT40 2.4GHz band	20 dBm @ 15 Mbps (MCS 0)																																						
	16 dBm @ 150 Mbps (MCS 7)																																						
802.11n/ac VHT20 5GHz band	19 dBm @ 7.2 Mbps (MCS 0)																																						
	14 dBm @ 72.2 Mbps (MCS 7)																																						
	13 dBm @ 86.7 Mbps (VHT MCS 8)																																						
802.11n/ac VHT40 5GHz band	18 dBm @ 15 Mbps (MCS 0)																																						
	14 dBm @ 150 Mbps (MCS 7)																																						
	13 dBm @ 200 Mbps (VHT MCS 9)																																						
802.11ac VHT80 5GHz band	18 dBm @ 32.5 Mbps (MCS 0)																																						
	14 dBm @ 325 Mbps (MCS 7)																																						
	13 dBm @ 433.3 Mbps (VHT MCS 9)																																						

A12

ANTENNA 1 AND 2 *

Radio modes: Support for IEEE 801.11a/h, 802.11b, 802.11g and 802.11n

Frequency band for 802.11a/n : 5 GHz; 5.170 to 5.835 GHz

Frequency band for 802.11b/g/n : 2.4 GHz; 2.402 to 2.494 GHz

Tx output power (Radio card output per chain, antenna excluded)

802.11n HT20 2.4GHz band 20.5 dBm @ 7.2 Mbps (MCS 0)

18 dBm @ 72.2 Mbps (MCS 7)

802.11n HT40 2.4GHz band 20.5 dBm @ 15 Mbps (MCS 0)

18 dBm @ 150 Mbps (MCS 7)

802.11n HT20 5GHz band 18 dBm @ 7.2 Mbps (MCS 0)

15 dBm @ 72.2 Mbps (MCS 7)

802.11n HT40 5GHz band 18 dBm @ 15 Mbps (MCS 0)

15 dBm @ 150 Mbps (MCS 7)

Value for 1 stream, add 3 dBm for 2 streams

ANTENNA 3 *

Radio modes: Support for IEEE 801.11a/h, 802.11b, 802.11g, 802.11n and 802.11ac

Frequency band for 802.11a/n : 5 GHz; 5.170 to 5.835 GHz

Frequency band for 802.11b/g/n : 2.4 GHz; 2.402 to 2.494 GHz

Tx output power (Radio card output per chain, antenna excluded)

802.11b 2.4GHz band 20 dBm @ 1 Mbps

20 dBm @ 11 Mbps

802.11g 2.4GHz band 21 dBm @ 6 Mbps

18 dBm @ 54 Mbps

802.11a 5GHz band 20 dBm @ 6 Mbps

15 dBm @ 54 Mbps

802.11n HT20 2.4GHz band 21 dBm @ 7.2 Mbps (MCS 0)

16 dBm @ 72.2 Mbps (MCS 7)

802.11n HT40 2.4GHz band 20 dBm @ 15 Mbps (MCS 0)

16 dBm @ 150 Mbps (MCS 7)

802.11n/ac VHT20 5GHz band 19 dBm @ 7.2 Mbps (MCS 0)

14 dBm @ 72.2 Mbps (MCS 7)

13 dBm @ 86.7 Mbps (VHT MCS 8)

802.11n/ac VHT40 5GHz band 18 dBm @ 15 Mbps (MCS 0)

14 dBm @ 150 Mbps (MCS 7)

13 dBm @ 200 Mbps (VHT MCS 9)

802.11ac VHT80 5GHz band 18 dBm @ 32.5 Mbps (MCS 0)

14 dBm @ 325 Mbps (MCS 7)

13 dBm @ 433.3 Mbps (VHT MCS 9)

Solexy Antenna KIT	Antenna	Antenna Gain
KA-A33U	N° 2 ANH92 for WiFi port	4.7 dBi
KA-A03U	N° 3 ANH92 for WiFi port	4.7 dBi

MAXIMUM PERMITTED RF THRESHOLD POWER (P_{th})

The RF threshold power (P_{th}), sometimes called the effective isotropic radiated power (EIRP), as defined in IEC/EN 60079-0, is the product of the effective output power of the transmitter multiplied by the antenna gain. The maximum threshold powers for each equipment group as defined by Table 4 in IEC/EN 60079-0 are provided below.

Because most antennas list the gain relative to an isotropic radiator (dBi) instead of the raw power gain, it is often easier to simply add the antenna gain in dBi to the radio output power in decibel-milliwatts (dBm). Any added cable loss between the RF output and the antenna may also be factored in.

$$P_{th} \text{ (dBm)} = \text{RF output power (dBm)} + \text{Antenna gain (dBi)} - \text{Coax cable loss between RF output and Antenna (dB)}$$

The resulting threshold power calculated by the above formula MUST be below the threshold power for the operating area group rating below.

Equipment for	Threshold Power (W)	Threshold Power (dBm)
Group I	6	37.7
Group IIA	6	37.7
Group IIB	3.5	35.4
Group IIC	2	33.0
Group III	6	37.7

The above threshold level refer to installation in classified area Ex according to IEC/EN 60079-0 standard.

The use of device differs from one region and/or country to another. The user of the device must take care that the device is operated only according to local rules and standard or without the permission of the local authorities on frequencies other than those specifically reserved and intended for use without a specific permit. More detailed information is available at the local frequency management authority.

MAXIMUM JOULES CALCULATION IN CASE OF COAX CABLE INSTALLATION

In case of use of a coax cable installation for antenna installation the adding cable need to be evaluating to ensure that the maximum energy stored on cable not exceeded the value allowable per IEC/EN 60079-11:

Max energy (Joules) allowed per IEC/EN 60079-11	
Group I	1500 μJ
Group IIA	950 μJ
Group IIB	250 μJ
Group IIC	50 μJ

The calculation can be done according to following equation:

$$E = \frac{1}{2} * \{ (C_1 + C_2) * [(1.5 * (\sqrt{R * P}))^2] \}$$

Where:

E = Energy

C₁ = Antenna Barrier Capacitance (18 pF)

C₂ = Coax cable capacitance

R = Impedance (50Ω)

P = RF power output (18 dBm, 63 mW)

1.5 = Safety Factor

Example:

Antenna cable capacitance = 1195 pF

$$E = \frac{1}{2} * \{ (18pF + 1195pF) * 7.08 \} = 0,00858\mu J$$

Answer = 0,00858 μJ acceptable for any Group



SWAA / SWSA USER GUIDE



COPYRIGHT (©) SOLEXY SRL 2016-2021

This document contains information protected by Copyright.

The present document may not be wholly or partially reproduced, transcribed, stored in any computer or other system whatsoever, or translated into any language or computer language whatsoever without prior written consent from Solexy Srl – Via Enrico Fermi, 2 – 25015 Desenzano del Garda (BS) – Italy.

REGISTERED TRADEMARKS ®

- SOLEXY is a registered trademark of SOLEXY
- ACKSYS is a registered trademark of ACKSYS.
- Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.
- CISCO is a registered trademark of the CISCO company.
- Windows is a registered trademark of MICROSOFT.
- WireShark is a registered trademark of the Wireshark Foundation.
- HP OpenView® is a registered trademark of Hewlett-Packard Development Company, L.P.
- VideoLAN, VLC, VLC media player are internationally registered trademark of the French non-profit organization VideoLAN.

TABLE OF CONTENTS

I INTRODUCTION.....	9
II PRODUCTS LINE OVERVIEW.....	11
II.1 Products goals.....	11
II.2 Features common to all products.....	11
II.3 Extra features per product model.....	12
III Device installation.....	13
III.1 Power supply.....	13
III.2 Antenna types.....	13
III.2.1 Omnidirectional antenna.....	13
III.2.2 Patch antenna.....	14
III.2.3 Yagi antenna.....	14
III.2.4 Dish antenna.....	14
III.2.5 MIMO antenna.....	15
III.3 Antenna installation.....	15
III.3.1 Legacy 802.11a/b/g case.....	15
III.3.2 802.11n/ac.....	17
III.4 802.11 radio channel choice.....	18
III.4.1 GHz overlapping radio channels.....	18
III.5 802.11 regulatory domain rules.....	19
III.5.1 Antenna gain and RF output power.....	19
III.5.2 FCC rules for 2.4 GHz band.....	20
III.5.3 FCC rules for 5 GHz band.....	21
III.5.4 ETSI rules for 2.4 GHz band.....	23
III.5.5 ETSI rules for 5GHz band.....	23
III.5.6 Radars detection overview (DFS).....	24
III.5.7 Specific DFS features for ACKSYS products range.....	26
IV ADMINISTRATION OVERVIEW.....	27
IV.1 Web interface.....	27
IV.2 Reset button.....	27
IV.3 Acksys WaveManager.....	27
IV.4 Emergency upgrade.....	27
IV.5 SNMP agent.....	28
V TECHNICAL REFERENCE.....	28
V.1 Networking components.....	28
V.1.1 OSI model.....	28
V.1.2 TCP/IP model.....	28
V.1.3 LAN layer: network interfaces.....	29
V.1.4 Physical interface.....	30
V.1.5 Network segment.....	30
V.1.6 Virtual interface.....	30
V.1.7 VLAN.....	31
V.1.7.1 Frame tagging.....	31
V.1.7.2 Vlan interface.....	31

V.1.8 Bridge.....	32
V.1.8.1 Bridge upper layer interface.....	33
V.1.8.2 Vlan bridging.....	34
V.1.8.3 Spanning Tree Protocols (STP, RSTP).....	37
V.1.9 Tunneling.....	40
V.1.10 Unicast Routing in IP networks.....	42
V.1.11 Addressing in the Data Link Layer (OSI layer 2).....	43
V.1.11.1 Ethernet Address.....	43
V.1.11.2 Wi-Fi MAC Address.....	44
V.1.12 Addressing in the IP layer (OSI layer 3).....	44
V.1.12.1 IP addresses.....	44
V.1.12.2 Public and private addresses.....	45
V.1.12.3 Routers (a.k.a. gateways).....	45
V.1.13 Multicast routing.....	46
V.1.13.1 Multicast addresses.....	47
V.1.13.2 PIM-SM.....	47
V.1.13.3 Multicast pitfalls and solutions.....	49
V.1.14 Firewall.....	53
V.1.15 Zones and Network Address Translation (NAT).....	53
V.1.15.1 NAT/PAT (Network/Port Addresses Translation) routers.....	53
V.1.15.2 NAT 1:1.....	55
V.2 Wireless concepts in 802.11.....	56
V.2.1 Wireless architectures.....	56
V.2.1.1 Infrastructure Mode.....	56
V.2.1.2 Ad-hoc Mode.....	58
V.2.1.3 Mesh (802.11s) Mode.....	59
V.2.1.4 Wireless Network Name.....	60
V.2.1.5 Virtual AP (multi-SSID) and multifunction cards.....	60
V.2.1.6 Wireless repeater.....	61
V.2.2 Modulation and coding.....	64
V.2.2.1 802.11b.....	64
V.2.2.2 802.11g.....	64
V.2.2.3 802.11a.....	65
V.2.2.4 802.11n.....	65
V.2.2.5 802.11ac.....	67
V.2.3 Radio channels and national regulation rules.....	68
V.2.4 Wireless security.....	68
V.2.4.1 WEP encryption.....	69
V.2.4.2 WEP authentication.....	69
V.2.4.3 WPA/WPA2 encryption.....	70
V.2.4.4 Pre-shared key mode (PSK).....	70
V.2.4.5 Enterprise mode (802.1x, RADIUS).....	71
V.2.4.6 Protected management frame (802.11w).....	72
V.2.4.7 Mesh Secure Authentication of Equals (SAE).....	73
V.2.5 Wired to wireless bridging in infrastructure mode.....	73
V.2.5.1 The problem.....	73
V.2.5.2 The solutions.....	74

V.2.6 Fast roaming features.....	78
V.2.6.1 Mono-channel vs. multichannel roaming.....	78
V.2.6.2 Proactive roaming vs. reactive roaming.....	79
V.2.6.3 What happens when the current AP fails.....	80
V.2.6.4 Scanning.....	81
V.2.6.5 Advanced Roaming settings.....	83
V.2.6.6 Authentication speed up.....	87
V.2.6.7 Connect before break.....	89
V.3 High availability features.....	91
V.3.1 Router redundancy with VRRP.....	91
V.3.1.1 VRRP.....	92
V.3.1.2 Connection tracking.....	94
V.3.1.3 Failures reporting.....	94
V.3.1.4 Miscellaneous questions.....	95
V.3.2 Link layer redundancy with RSTP.....	97
V.4 SNMP agent and ACKSYS MIB.....	97
V.4.1 SNMP security.....	97
V.4.1.1 SNMP V1 and V2c.....	97
V.4.1.2 SNMP V3.....	97
V.4.2 Access methods.....	99
V.4.3 Using the Acksys MIB.....	99
V.4.4 Understanding network status tables.....	100
V.4.5 Managing network configuration tables.....	101
V.4.5.1 OIDs relevant to IP layer.....	102
V.4.5.2 OIDs relevant to Data Link layer.....	102
V.4.5.3 OIDs relevant to Physical layer.....	107
V.4.6 Managing service configuration tables.....	107
V.4.7 Using SNMP notifications (traps).....	107
V.4.8 Examples.....	108
V.5 QOS Traffic Class Management.....	110
V.5.1 Traffic Classification.....	110
V.5.1.1 802.1p traffic classes.....	110
V.5.1.2 DiffServ traffic classes.....	111
V.5.1.3 WMM Traffic Classes.....	111
V.5.2 Traffic Class to Queue Mapping.....	112
V.5.2.1 Queue definition.....	112
V.5.2.2 Queues of Ethernet Interfaces.....	112
V.5.2.3 Queues of Wireless interfaces.....	113
V.5.2.4 Queue mapping.....	113
V.5.3 Queue Management.....	113
V.5.4 GRE Tunnels.....	113
VI SECURITY MANAGEMENT.....	114
VI.1 HTTP/HTTPS server.....	114
VI.2 Bridge mode.....	114
VI.3 Router mode.....	114
VI.4 SNMP access.....	115
VII WEB INTERFACE REFERENCE.....	116



SWAA / SWSA User Guide

VII.1 Setup Menu.....	116
VII.1.1 Physical interfaces.....	116
VII.1.2 Wireless/Radio.....	119
VII.1.2.1 SETUP/PHYSICAL INTERFACES/WIRELESS SETTINGS/DEVICE CONFIGURATION	119
General Setup tab:.....	119
VII.1.2.2 SETUP/PHYSICAL INTERFACES/WIRELESS SETTINGS/INTERFACE CONFIGURATION.....	125
VII.1.3 Physical Interface: LAN.....	148
VII.1.4 Virtual interfaces.....	150
VII.1.4.1 802.1q Tagging.....	150
VII.1.4.2 BOND INTERFACES.....	152
VII.1.4.3 Wireless SSIDs.....	159
VII.1.4.4 L2 Tunnels.....	160
VII.1.5 Network.....	163
VII.1.5.1 Network configuration.....	163
VII.1.6 VPN.....	168
VII.1.7 Bridging.....	173
VII.1.7.1 STP/RSTP.....	173
VII.1.7.2 Vlan Management.....	175
VII.1.7.3 Bridge filter.....	177
VII.1.8 Routing / Firewall.....	179
VII.1.8.1 Network zones.....	179
VII.1.8.2 Static routes.....	184
VII.1.8.3 Multicast routing.....	185
VII.1.9 QOS.....	191
VII.1.9.1 Frame tagging.....	191
VII.1.9.2 Traffic Class Priorities.....	192
VII.1.9.3 WMM.....	193
VII.1.10 Services.....	195
VII.1.10.1 Alarms / events.....	195
VII.1.10.2 Connection tracking.....	197
VII.1.10.3 DHCP/DNS RELAY.....	198
VII.1.10.4 Discover Agent.....	201
VII.1.10.5 SNMP Agent.....	201
VII.1.10.6 Statistics.....	206
VII.1.10.7 VRRP.....	209
VII.1.10.8 Web Server.....	212
VII.2 Tools Menu.....	213
VII.2.1 Firmware upgrade.....	213
VII.2.2 Password Settings.....	213
VII.2.3 VII.2.3 System.....	213
VII.2.3.1 Device Local settings.....	213
VII.2.3.2 MIB-2 System Settings.....	214
VII.2.3.3 Network Timer Server.....	214
VII.2.4 Network Utilities.....	214
VII.2.5 Save Config / Reset.....	215



VII.2.6 Log Settings.....	216
VII.3 STATUS Menu.....	218
VII.3.1 Device Info.....	218
VII.3.2 Network.....	218
VII.3.3 Routes.....	220
VII.3.4 Bridges.....	220
VII.3.5 Multicast routes.....	221
VII.3.6 Wireless.....	223
VII.3.6.1 Associated Stations.....	223
VII.3.6.2 Channel Status.....	225
VII.3.6.3 MESH Survey.....	226
VII.3.6.4 Service status.....	226
VII.3.6.5 Site Survey.....	227
VII.3.6.6 SRCC Status.....	230
VII.3.7 Services.....	231
VII.3.7.1 DHCP Lease.....	231
VII.3.7.2 VRRP.....	231
VII.3.8 Log.....	231
VIII WIRELESS TOPOLOGIES EXAMPLES.....	233
VIII.1 Simple “Wireless cable”.....	233
VIII.2 Multiple SSID.....	234
VIII.3 Multiple SSID with VLAN.....	235
VIII.4 Multiple separate SSID.....	237
VIII.5 Infrastructure bridge + Roaming.....	239
VIII.6 Point-to-point redundancy with dual band.....	240
VIII.7 Fixed Mesh.....	242
VIII.8 802.11s Mesh.....	245
VIII.9 High performance repeater.....	248
VIII.10 Line topology repeater (single radio card).....	250
VIII.11 Multihop tree repeater.....	252
IX FIRMWARE UPGRADE.....	256
IX.1 Standard upgrade.....	256
IX.2 Bootloader upgrade.....	257
IX.3 Fallback after an interrupted upgrade operation.....	258
X TROUBLESHOOTING.....	259
X.1 Basic checks.....	259
X.2 Network configuration checks.....	260
X.3 Multicast router checks.....	261
XI FREQUENTLY ASKED QUESTIONS.....	264
XI.1 How to reset the device to factory settings?.....	264
XI.2 I Can’t find the Transparent Client mode.....	264
XI.3 How is the Wi-Fi bit rate chosen?.....	264
XI.4 What is the difference between WMM, WME, IEEE802.11e?.....	265
XI.5 My CISCO access point rejects my client bridge?.....	265
XI.6 Fast roaming features.....	265
XI.6.1 What is the scan period when proactive roaming is enabled?.....	265
XI.6.2 What is the roaming delay when the current access point disappears suddenly?.....	266



SWAA / SWSA User Guide

XI.7 The GRE tunnel does not forward data?.....	266
XI.8 Multicast.....	266
XI.8.1 Multicast route is unstable in the Web interface?.....	266
XI.8.2 Receiver device does not send its multicast group in its IGMP reports?.....	267
XII APPENDIX – GLOSSARY AND ACRONYMS.....	268
XIII APPENDIX – 802.11 RADIO CHANNELS.....	270
XIII.1 11b/g (2.4GHz).....	270
XIII.2 802.11a/h (5 GHz).....	271



I INTRODUCTION

This reference guide applies to the Solexy Access Point SWAA and SWSA series.

Wherever this document refers to “the product” without further precision, it means one of the products of the Solexy Access Point SWAA and SWSA series.

Together with the quick start guide included in the product package, it covers product installation, configuration and usage, and general information about Wi-Fi protocols.

This reference guide describes the WaveOS version **4.18.0.1**.

If your product contains an earlier version, you can contact Solexy for firmware update

All recommendations for equipment installation, such as power supplies, antennas and connection cables are documented in the quick installation guide specific to each product.



Regulatory information / Disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution of the connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and any authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

Information in this document is subject to change without notice and does not represent a commitment on the part of SOLEXY.

SOLEXY provides this document "as is", without warranty of any kind, expressed or implied, including, but not limited to, its particular purpose and takes no responsibility for the profitability or the suitability of the equipment for the requirements of the user.

SOLEXY reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable.

However, SOLEXY assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors and these changes are incorporated in new editions of the publication.

II PRODUCTS LINE OVERVIEW

II.1 Products goals

These products provide Wi-Fi connectivity for Ethernet devices. Thanks to their configuration capabilities, they can create various topologies; see section [Wireless topologies examples](#) for details.

II.2 Features common to all products

Many features are common to all products in this product line.

Networking:

Layer 2 software bridging, VLAN, Tunneling, STP/RSTP, 802.1p and 802.11e QOS.

Layer 3 routing with DSCP retagging, NAT, firewall, Diffserv QOS, Multicast routing

DHCP server or client, DNS relay

Configuration and maintenance:

HTTP and HTTPS Web browser configuration

Acksys WaveManager compatibility

SNMP agent for status and configuration

Events handler, alarms

Browser-based firmware upgrades

Emergency upgrade mode

Performance graph trace

Wi-Fi capabilities:

Radio:

- Dual band (2.4 GHz and 5 GHz)
- Support either 802.11n, 20 or 40 MHz channel width or 802.11ac, 20, 40 or 80 MHz channel width
- Backward compatible with 802.11a, b, g, n
- Access point, bridging client, 802.11s mesh, ad-hoc
- Access point: Client isolation, 802.11x authenticator, slow bit rates lockout, clients MAC filtering
- Client modes: "4 addresses", MAC translation, cloning

Security (depending on the mode):

- WPA2, 802.1x (RADIUS)
- A/B/G compatible security: WPA, WEP

Long-distance Wi-Fi

WME/WMM configuration support

Miscellaneous: 802.11h, 802.11d, client 802.11r support.

II.3 Extra features per product model

This section focuses on the features that involve specific software configuration. Other distinctive characteristics are covered in the quick installation guide of each product.

Configuration and maintenance:

C-Key configuration backup
LED status

Ethernet capabilities:

10/100/1000 base T
Auto-crossing (MDX)
Automatic speed and duplex selection

Some features depend on Radio Card type (802.11n or 802.11ac):

Feature	Radio card type	
	802.11n	802.11ac
802.11 max modulation rate	450 Mbps	1300 Mbps
Max remote clients per access point	124	128
Fast Roaming	✓	
Scanning/roaming cluster	✓	As scanner
Mesh	✓	
Line Topology Repeater	✓	
Multiple roles per radio (repeater, portal)	✓	
Dual radio repeater	✓	✓
VLAN-tagged frames forwarding	✓	

III Device installation

The **quick start guide** shipped with your product includes specific startup instructions and recommendations. Please read it first.

III.1 Power supply

The quick start guide gives the maximum power consumption for your product. You should consider this value as the minimum that your power supply must provide. Furthermore, there is an additional point to consider: these products include Wi-Fi radio cards that can cause quick power surges during wireless communication. These surges are included into power consumption given by the quick start but, if your power supply is too slow to deliver power, it can cause product reboots or unpredictable behaviour.

III.2 Antenna types

The following sections describe the most commonly used antenna type and the way to install them.

These explanations rely on good understanding of what a radiation pattern represents. If you are not familiar with it, please read this page first: <http://www.antenna-theory.com/basics/radPattern.html>. This represents a good starting point.

The radiation patterns shown in the next sections are only provided as examples to give a better understanding of the distinctive characteristics of each antenna type.

III.2.1 Omnidirectional antenna

The radiated power is uniform in all the horizontal directions. Power drops progressively while approaching the direction of the antenna axis (vertical). The corresponding radiation pattern is given below.

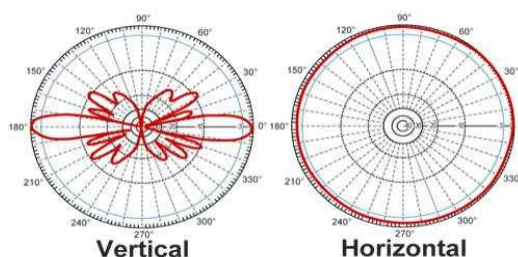
This type of antenna is used to cover a wide area all around the antenna.

When using them, make sure that they are placed in the same plane.

Antenna



Radiation pattern



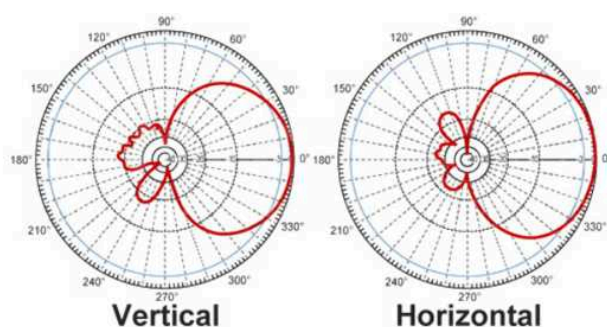
III.2.2 Patch antenna

This kind of antenna focuses radiations on one side (see radiation pattern below). This allows wall mounting without wasting radiations in the wall. The gain is generally comprised between 7dBi and 9dBi.

Antenna



Radiation pattern



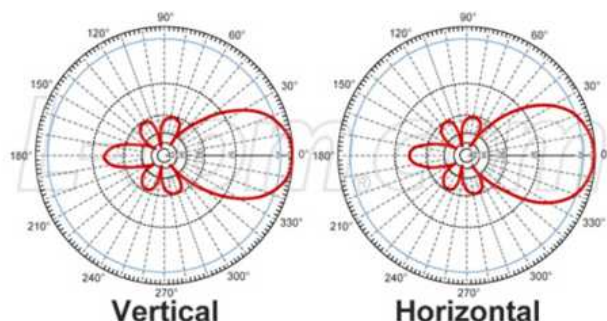
III.2.3 Yagi antenna

This kind of antenna also focuses radiations on one side (see radiation pattern below). But its gain is usually higher than patch antenna (11dBi to 15dBi).

Antenna



Radiation pattern



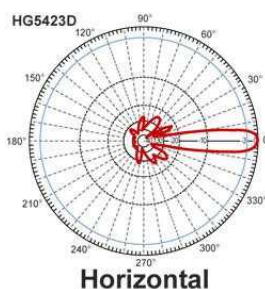
III.2.4 Dish antenna

This antenna focus the radiations in one point and then can achieve very high gain (>20dBi).

Antenna



Radiation pattern



III.2.5 MIMO antenna

Antenna manufacturers provide MIMO version of each antenna type described previously. MIMO antennas are basically a set of several (usually 2 or 3) standard antennas put together in a single enclosure.

In any case, refer to the antenna datasheet to get information about the Radiation pattern and internal layout.

III.3 Antenna installation

Radio connectors come in several flavors: SMA, RPSMA, QMA, N-Type and so on. Please do not mistake SMA for RPSMA. They look alike, but the central pin or hole is inverted. RPSMA is reserved for Wi-Fi only operation. Other uses, like GPS or Cellular radio, use SMA connectors.

There are two major cases when considering Wi-Fi antenna installation.

III.3.1 Legacy 802.11a/b/g case

You can establish Wi-Fi links from a few feet to several miles but it requires some cautions:

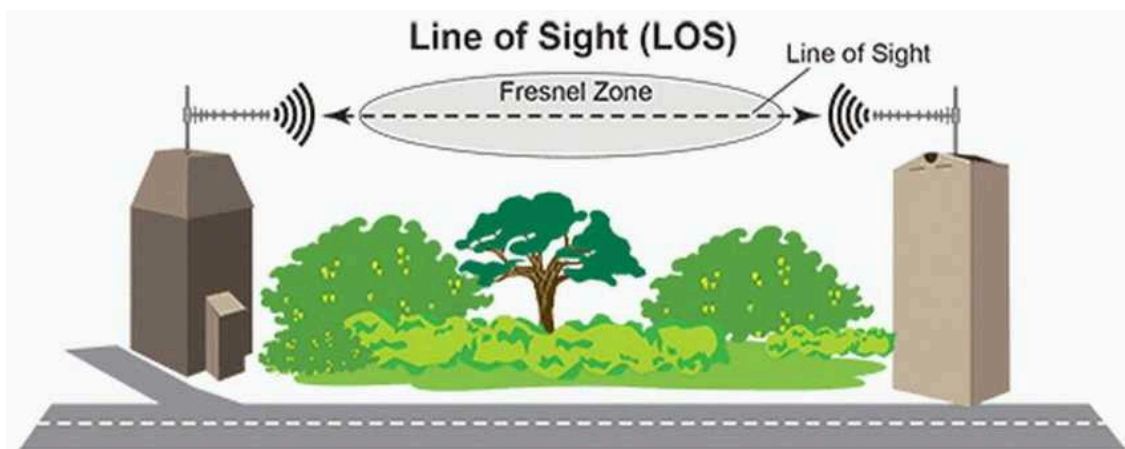
You must adapt the EIRP of the products (but you must keep it in the local regulations range) according to the distance and obstacles between devices.

The link RSSI must be high enough, else when environment changes (climatic conditions change or space reorganization) the link might break.

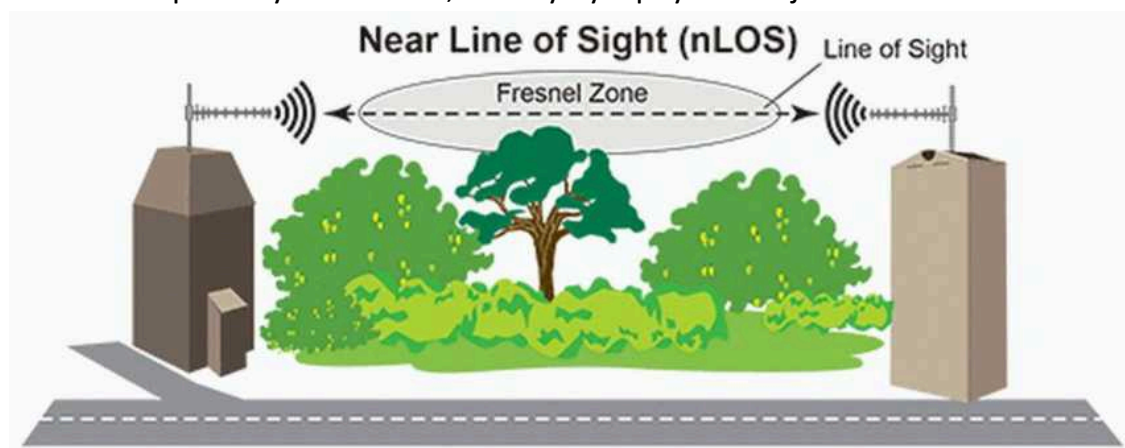
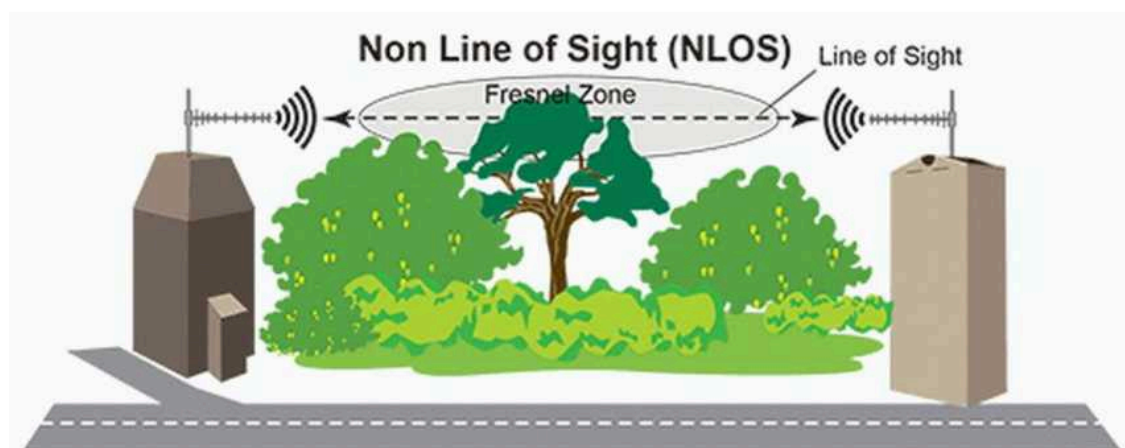
To increase the EIRP you can either:

- use an antenna with a larger gain,
- use a product with a larger radio output power
- marginally, use better quality connectors and radio cables.

For outdoor link, products must be “line of sight” from the other one. This is a **mandatory condition** and should be considered with attention. The schematic below explains what we mean by “line of sight”.



Non-line-of-sight (NLOS) and near-line-of-sight are radio transmissions across a path that is partially obstructed, usually by a physical object in the innermost Fresnel zone.

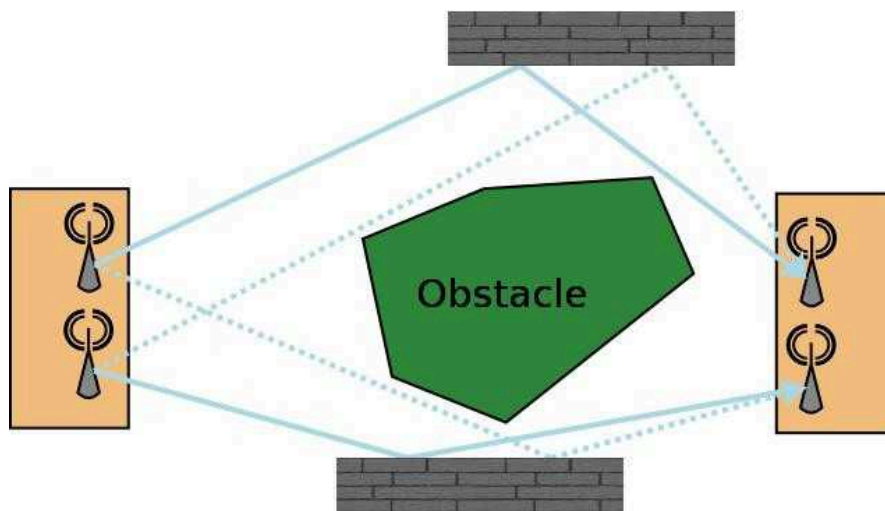


Near Line Of Sight can usually be dealt with using better antennas, but Non Line Of Sight usually requires alternative paths or multipath propagation methods. Obstacles that commonly cause NLOS conditions include buildings, trees, hills, mountains ...

III.3.2 802.11n/ac

With these norms, considerations about EIRP and RSSI are still relevant. But the 802.11n/ac takes advantage of MIMO (Multiple Input Multiple Output) technology and introduces new ways to use multiple antennas.

802.11a/b/g products already use more than one antenna but they were limited to the diversity mode (only one antenna transmits at a time). Moreover, bounces on walls or other obstacles cause multiple paths that confuse the receiver (see figure below).



802.11n/ac uses these bounces to allow several independent streams (2 to 4) to be sent and identified simultaneously. At the beginning of the transmission, a well-known pattern is sent. The receiver uses that pattern to calibrate itself and characterize the transmission channel for each antenna.

Using that information, the receiver is able to calculate which stream belongs to what antenna.

In this case there must be at least one antenna per stream to be sent. Supernumerary antennas are used to transmit additional spatial information.

Since 802.11n/ac use bounces to increase bandwidth, a line of sight outdoor application will have less performance compared to an indoor one, because there are potentially no bounces at all. This problem can be solved by sending polarized radio waves orthogonal to each other. Such so-called "Slant Antennas" are actually made of 2 specifically polarized antennas put together in a single case.

III.4 802.11 radio channel choice

Wi-Fi standard compliant products can use two RF bands:

- The 2.4 GHz band covers the channels compatible with 802.11b/g/n standards,
- The 5 GHz band covers the channels compatible with 802.11a/n/ac standards.

Several points must be considered when selecting a radio channel for optimal performance:

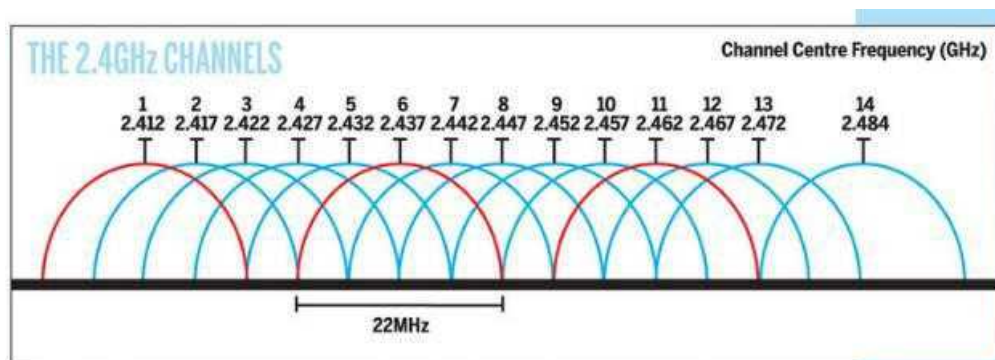
- First of all, local regulation rules that may forbid or limit using some channels;
- Transmit power on each channel, that may be limited by the legislation and by the hardware;
- Radio noise and interferences originating from other Wi-Fi devices operating on the same channel or non-Wi-Fi devices like microwaves oven, cordless telephones, Bluetooth devices, others wireless devices;
- Collisions due to the “hidden station” effect when all access points in your system use the same channel.

A preliminary site survey is strongly recommended to detect overloaded radio channels BEFORE buying band specific antenna. An overloaded channel may strongly affect performances. It is recommended to use a free channel.

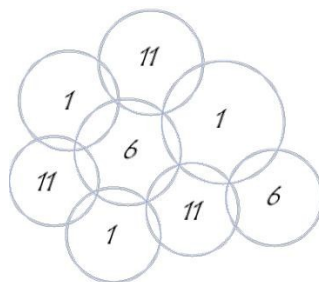
Wi-Fi performance also depends greatly on the radio link quality (a.k.a. RSSI). The better the RSSI is, the better the throughput and error rate can be. Signal quality is a function of distance, obstacles, narrow pathways, hygrometry, and antennas orientation.

III.4.1 GHz overlapping radio channels

The radio channel is only an indication of the central frequency in use. Modulation enlarges the channel to a 20-22 MHz band. This must be taken into account when several Wi-Fi cells are near to each other in 2.4GHz (5GHz channels do not overlap), otherwise the effective performance will decrease due to interferences. This point is especially important when you try to cover a geographic area with several access points.



Although the use of “non-overlapping” channels 1, 6, and 11 has limits when products are too close, the 1–6–11 guideline has merit. If transmitter channels are chosen closer than channels 1, 6 and 11 (for example, 1, 4, 7 and 10), overlap between the channels may cause unacceptable degradation of signal quality and throughput.



Picture III-1: Example of geographical implantation of non-overlapping channels

III.5 802.11 regulatory domain rules

To control the use of Wi-Fi radio channels, there are 3 major regulatory rules sets in wide use all around the world:

- ETSI: for European countries
- FCC: for American countries
- MKK/TELEC: for Asian countries

Specific regulatory domains (France, Brazil, Korean, Australia ...) derive from the major regulatory rules with several modifications.

The regulatory domain gives the rules to use each RF band.



To abide by your local laws, you must select the country where the product will be installed before activating the Wi-Fi card.

III.5.1 Antenna gain and RF output power

If you plan to use a high gain antenna, you might exceed the EIRP allowed in your country and UL / IEC / EN 60079-0 standards. In this case you must reduce manually the radio transmit power of your product (see [Advanced Settings tab](#) in section [VII.1.2 Wireless/Radio](#)).

In the following sections you will find the FCC and ETSI rules to adapt the product transmit power to the antenna used.

Definition of terms:

RF Output power: RF power radiated by the ACKSYS wireless device without the antenna

EIRP: RF power radiated by the ACKSYS wireless device with the antenna.

EIRP = RF OUTPUT POWER + ANTENNA GAIN (dBi)

III.5.2 FCC rules for 2.4 GHz band

2.4 GHz point to multipoint: MAX EIRP = +36 dBm (4 Watts)		
MAX RF Output POWER dBm (mW)	MAX Gain dBi	MAX EIRP dBm (W)
30 (1000)	6	36 (4)
27 (500)	9	
24 (250)	12	
21 (125)	15	
18 (62.5)	18	
15 (32)	21	
12 (16)	24	

In other words, when using antennas with a gain higher than 6dBi, for every 1 dBi gain over 6 dBi, the MAX RF output power must be reduced by 1 dB.

2.4 GHz point to point: MAX EIRP = special rules					
MAX RF Output POWER dBm (mW)		MAX Gain (dBi)	MAX EIRP dBm (W)		
30	(1000)	6	36	(4)	
29	(800)	9	38	(6.3)	
28	(630)	12	40	(10)	
27	(500)	15	42	(16)	
26	(400)	18	44	(25)	
25	(316)	21	46	(39.8)	
24	(250)	24	48	(63)	
23	(200)	27	50	(100)	
22	(160)	30	52	(158)	

When using antennas with a gain higher than 6dBi, for every 3 dBi gain over 6 dBi, the MAX RF output power must be reduced by 1 dB.

III.5.3 FCC rules for 5 GHz band

5 GHz point to multipoint: MAX EIRP = special rules						
BAND	Freq. (GHz)	Channels	Location	MAX RF output POWER (dBm/mW)	MAX Gain (dBi)	MAX EIRP (dBm/mW)
UNII	5.15-5.25	36, 40, 44, 48	Indoor & outdoor	16 / 40	6 ₍₁₎	22 / 160
UNII-2	5.25-5.35	52, 56, 60, 64	Indoor & outdoor	23 / 200	6 ₍₁₎	29 / 800
UNII-2 ext.	5.470-5.725	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Indoor & outdoor	23 / 200	6 ₍₁₎	29 / 800
UNII-3	5.725-5.825	149 to 161	outdoor	29 / 800	6 ₍₁₎	35 / 3.2 W

1 If antennas higher than 6dBi gain are utilized, a reduction of 1 dB of the MAX RF output POWER is required for every 1 dBi increase in the antenna gain above 6dBi.

5 GHz point to point: MAX EIRP = special rules						
BAND	Freq. (GHz)	Channels	Location	MAX RF output POWER (dBm/mW)	MAX Gain (dBi)	MAX EIRP (dBm/mW)
UNII	5.15-5.25	36, 40, 44, 48	Indoor	16 / 40	6	22 / 160
UNII-2	5.25-5.35	52, 56, 60, 64	Indoor & outdoor	23 / 200	6	29 / 800
UNII-2 ext.	5.470-5.725	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Indoor & outdoor	23 / 200	6	29 / 800
UNII-3	5.725-5.825	149 to 161	outdoor	30 / 1 W	23 ₍₂₎	53 / 200 W

2 If antennas higher than 23 dBi gain are utilized, a reduction of 1 dB of the MAX RF output POWER is required for every 1 dBi increase in the antenna gain above 23 dBi.

Some channels require DFS support; please, see section "[Radars detection overview \(DFS\)](#)".

III.5.4 ETSI rules for 2.4 GHz band

2.4 GHz point to multipoint: MAX EIRP = +20 dBm (100 mWatts)						
BAND	Freq. (GHz)	Channels	Location	MAX RF output POWER (dBm/mW)	MAX Gain (dBi)	MAX EIRP (dBm/mW)
ISM	2.4-2.483	1 to 13	Indoor/ outdoor	NA	NA	20 / 100

III.5.5 ETSI rules for 5GHz band

5 GHz point to multipoint: MAX EIRP = special rules						
BAND	Freq. (GHz)	Channels	Location	MAX RF output POWER dBm (mW)	MAX Gain (dBi)	MAX EIRP (dBm/mW)
UNII	5.15-5.25	36, 40, 44, 48	Indoor	NA	NA	23 / 200
UNII-2	5.25-5.35	52, 56, 60, 64	Indoor	NA	NA	If TPC 23 / 200 Else 20 / 100
UNII-2 ext.	5.470-5.725	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Indoor & outdoor	NA	NA	If TPC 30 / 1000 Else 27 / 500
UNII-3	5.725-5.825	149 to 161	Forbidden	NA	NA	NA

TPC means Transmit Power Control. It's a mechanism by which 2 devices initiating a communication will negotiate so that their respective power level is as low as possible, just loud enough to hear each other.

Some channels require DFS support; see section "[Radars detection overview \(DFS\)](#)".

III.5.6 Radars detection overview (DFS)

In some regions, it is important to ensure that wireless equipment does not interfere with certain radar systems in the 5 GHz band. If radar is detected, the wireless network automatically switches to a channel that does not interfere with the radar system. Freeing the channel when a radar is detected is called DFS (Dynamic Frequency Selection).

The radar detection is only required for a master device (AP, mesh node, ad-hoc). For a slave device (client), the radar detection is not required but the device must use a passive scan (listen only to join a network). Please notice that passive scan does not allow connection to hidden SSIDs (active scan is required). Actually, a client needs to send probes (active scan) in order to identify a hidden SSID AP.

Radar detection is a probabilistic activity, because radio signals can be distorted by distance, echoes and other hazards. The radio hardware compares the radio signal with known radar patterns. This mechanism can inherently fail in two ways:

- Not detecting a real radar pattern because it is distorted;
- Detecting a not-existent radar pattern because another radio signal is distorted resulting in something similar to a radar signal. This is called false detection.



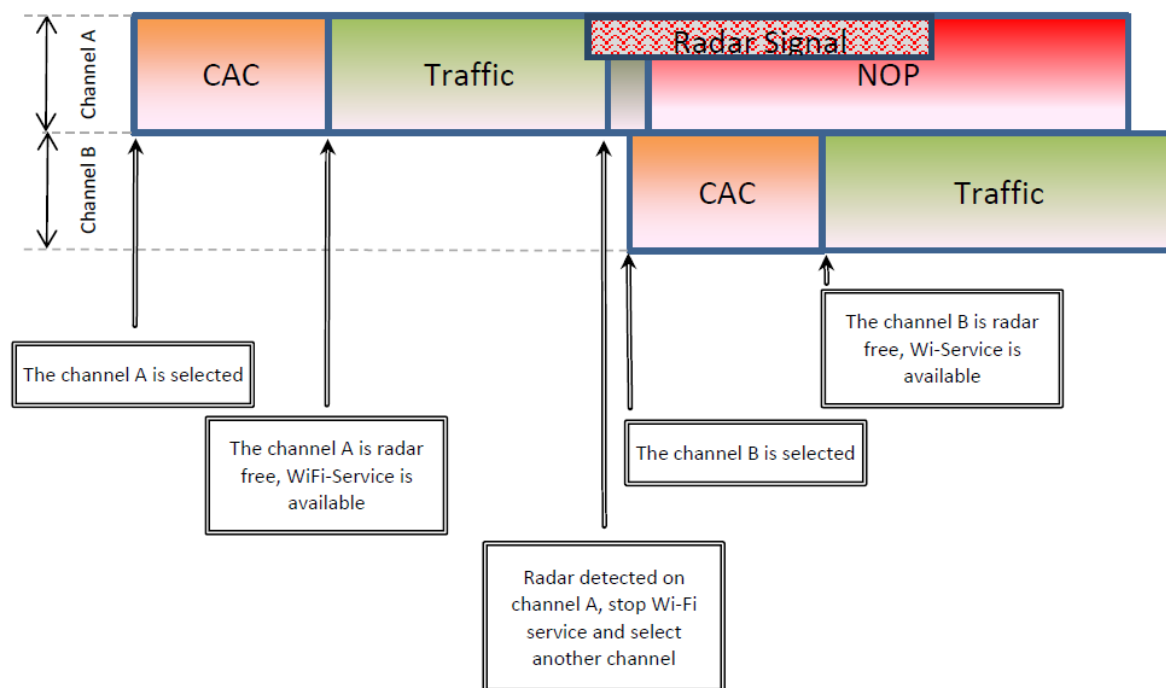
The detector makes its best to avoid these pitfalls but obviously cannot guarantee a 100% exact detection. And indeed, the standards do **not** require 100% detection success. This may result in false detections, and unexpected channel switching in some cases.

The ACKSYS product maintains a database of all applicable channels, where each channel is marked as "Radar Free", "Radar detected", "No radar detection". The product can only select a channel marked as "Radar free" or "No radar detection".

When the selected channel requires the DFS mechanism, the product starts the Channel Availability Check (CAC) period. During this period, the Wi-Fi service is not available because the product is checking if no radar is present on the channel. If a radar is detected during the CAC period, the channel is marked as "Radar detected", and the product will select another channel.

If the selected channel is "radar free", the product can operate it. During operation, the product continuously monitors the spectrum to search for radar patterns. If radar is detected, the product stops the Wi-Fi service, and will select another channel.

After radar detection, the channel is marked as "Radar detected" for a Channel Avoidance Period (NOP). During this period the product cannot select this channel.



Two lists of typical radar waveforms must be detected according to ETSI or FCC standards. Basically, a typical radar waveform is defined by different parameters like:

- Pulse Width
- Number of pulses per radar burst
- Time between pulses (Pulse Repetition Frequency or Pulse Repetition Interval)
- Number of bursts

The list of channels that require DFS are the following:

DFS in FCC			
Channels	BAND	CAC period	NOP period
36, 40, 44, 48	UNII	DFS is not required	
52, 56, 60, 64	UNII-2	1 min	30 min
100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	UNII-2 ext.	1 min	30 min
149 to 161	UNII-3	DFS is not required	

CAC and NOP periods are minimal values.

DFS in ETSI			
Channels	BAND	CAC period	NOP period
36, 40, 44, 48	UNII	DFS is not required	
52, 56, 60, 64	UNII-2	1 min	30 min
100, 104, 108, 112	UNII-2 ext.	1 min	30 min
116,120, 124, 128		10 min	30 min
132, 136, 140		1 min	30 min

CAC and NOP periods are minimal values.

NOTE: If the slave device (client) does not support the radar detection, the EIRP is limited to 23 dBm.

III.5.7 Specific DFS features for ACKSYS products range

The SOLEXY products support three master roles: AP, mesh node and ADHOC. Only the AP role supports DFS. Therefore, the two other master roles (mesh node, ad-hoc) can only use non-DFS channels.

In slave mode, SOLEXY products do not support radar detection but satisfy DFS requirements, because they use the passive scan mode. Be aware the EIRP must always be lower than 23 dBm.

The CAC period in ETSI mode for channel 116 is forced to 10 min whereas the minimum recommended value is 1mn. That enables to supporting HT40 with channels 116/120 and HT80 with channels 116/120/124/128.

The list of radar waveforms detected by SOLEXY products are listed in:

- *ETSI EN 301 893 standard*. The supported release is mentioned in the DFS test report/CE declaration of the product. New radar pulses are added with every version.
- *FCC part 15 sub part E*. The supported release is mentioned in the DFS test report.

IV ADMINISTRATION OVERVIEW

IV.1 Web interface

The primary means to fully configure the product is the web browser interface. It is described in more details in the [Web interface reference](#) chapter.

To get access to the product you may have to set its IP address first, this is done using either the *Acksys WaveManager* software.

You can use any recent browser except Microsoft Internet Explorer 11.

IV.2 Reset button

The RESET button has three uses:

- a short press (< 2 seconds) will reboot the product. The DIAG led will turn red steadily when the reboot takes place, until the product is operational.
- a long press while the product is running will reset it to factory settings. Press and hold the reset button until the DIAG led turns RED.
- a long press at startup time (either at power-up or very shortly after a reboot) will activate the “Emergency upgrade” mode. When the mode is activated the DIAG LED will blink quickly. This mode allows either to reload the firmware from *Acksys WaveManager* or to reset to factory settings with another press on the reset button (see above).

IV.3 Acksys WaveManager

Acksys WaveManager can detect these products, display their configuration and set their IP address, even when they are incorrectly configured, or an incorrect subnet.

Acksys WaveManager can also be used to set the SSID and WiFi operating frequency (radio channel)

Acksys WaveManager can also be used to reload the firmware when the product is in “Emergency upgrade” mode.

IV.4 Emergency upgrade

The “Emergency upgrade” mode is entered via the reset button. It allows recovery when a product was powered down during a regular firmware upgrade, or if the product experienced such conditions that it is completely non-operational.

The “Emergency upgrade” mode is described in more details in chapter [IX Firmware Upgrade](#)

IV.5 SNMP agent

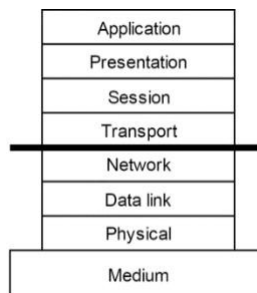
The product embeds a SNMP agent allowing configuration and monitoring from a SNMP manager like Acksys WaveManager, HP OpenView™ or net-snmp commands. The SNMP agent is described in more details in its own chapter.

V TECHNICAL REFERENCE

V.1 Networking components

V.1.1 OSI model

The discussion of the networking features will often refer to the Open Systems Interconnection (OSI) model. It is a conceptual view of communications systems standardized by the ISO. Please refer to <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html> or other resources for further explanations.



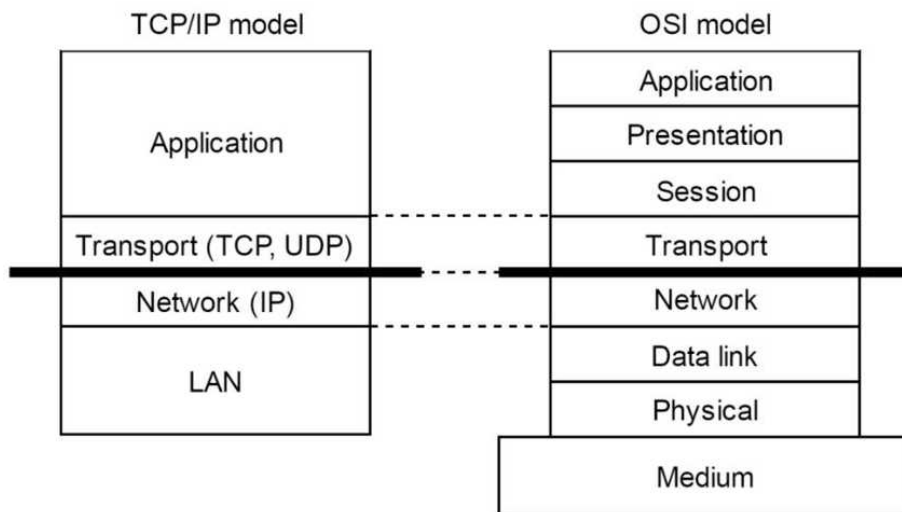
Picture V-1: The OSI layers

This user guide focuses on the three lower layers of the model: physical, data link and network.

V.1.2 TCP/IP model

TCP/IP is the protocols stack used by Internet and most Intranets.

In a device participating in a TCP/IP network, there are four software layers: the **application layer**, the **transport layer** (TCP or UDP), the **network layer** (IP), the **LAN layer** (Ethernet, Wi-Fi, point-to-point modems, etc.). Though the TCP/IP model is older than OSI, it is somewhat correlated since it is one of the origins of OSI.



Picture V-2: Comparison of TCP/IP and OSI models

Each layer has its own purpose and addressing scheme.

The **LAN layer address** allows a device to send data to another device connected to the same LAN. But there is not enough information in a LAN address to send to a device connected on another LAN through a router.

The **Network (IP) address** solves this problem by defining addresses which can be subject to routing. When the source and destination devices are not on the same LAN, the source device can send data to an intermediate router (also called gateway). The router has routing tables which allows it to forward data to the destination device, maybe through other gateways.

The **transport layer address**, called a “port”, is used inside a destination device to deliver data to the correct application process.

You can move packets between two physical links depending on their MAC addresses, without changing the packets: this is called bridging or switching. You can move packets between LANs by selecting their destination depending on the IP addresses: this is called routing. Routing offers additional features, like the possibility to masquerade IP addresses, or to selectively disable routing: this is firewalling.

V.1.3 LAN layer: network interfaces

In the context of TCP/IP networks, a network interface is a way to communicate with other computers. This way could be a piece of hardware and its software drivers, like an Ethernet LAN, or a pair of modems linking COM ports of two peer computers; it could also be a whole subsystem like a PABX, a Wi-Fi infrastructure, or a couple of Ethernet paired for redundancy.

In WaveOS, the network interface is implemented as a software object that conceptualizes a communication port. It provides communication between

- an upper software layer such as the IP networking layer or a bridge,
- and lower communication interfaces, such as physical media, tunnels, Wi-Fi “roles” or bridges.

You can group compatible network interfaces inside bridges. Access points are commonly bridged with an Ethernet LAN to provide Ethernet access to its Wi-Fi clients. The IP protocol views the bridge as a single interface with a single IP address, just like if the bridge was an external hardware switch.

Giving an IP address to a network interface attaches it to the IP layer.

V.1.4 Physical interface

A physical interface is a software object that relies on a hardware device like an Ethernet card or a Wifi radio card.

The [VII.1.1 Physical interfaces](#) submenu configures the physical interfaces.

V.1.5 Network segment

A network segment is a hardware assembly that interconnects two or more computers, and allows them to exchange physical “signals” without processing them. For example: a RJ45 cable, a coaxial Ethernet, or a handful of RJ45 cables linked by an Ethernet Hub.

The concept of network segment in Ethernet compatible networks is similar to the “collision domain”. It indicates which devices will always receive a frame sent and which devices must synchronize to access the media.

Note that a network switch splits the network into several segments, because it filters frames between its ports; conversely a legacy network hub maintains the view of several ports sharing a single segment because collisions can occur between ports.

V.1.6 Virtual interface

A virtual interface is a software object that implements special-purpose processing on data frames and that can be associated with a physical interface, or another virtual interface, or stand alone.

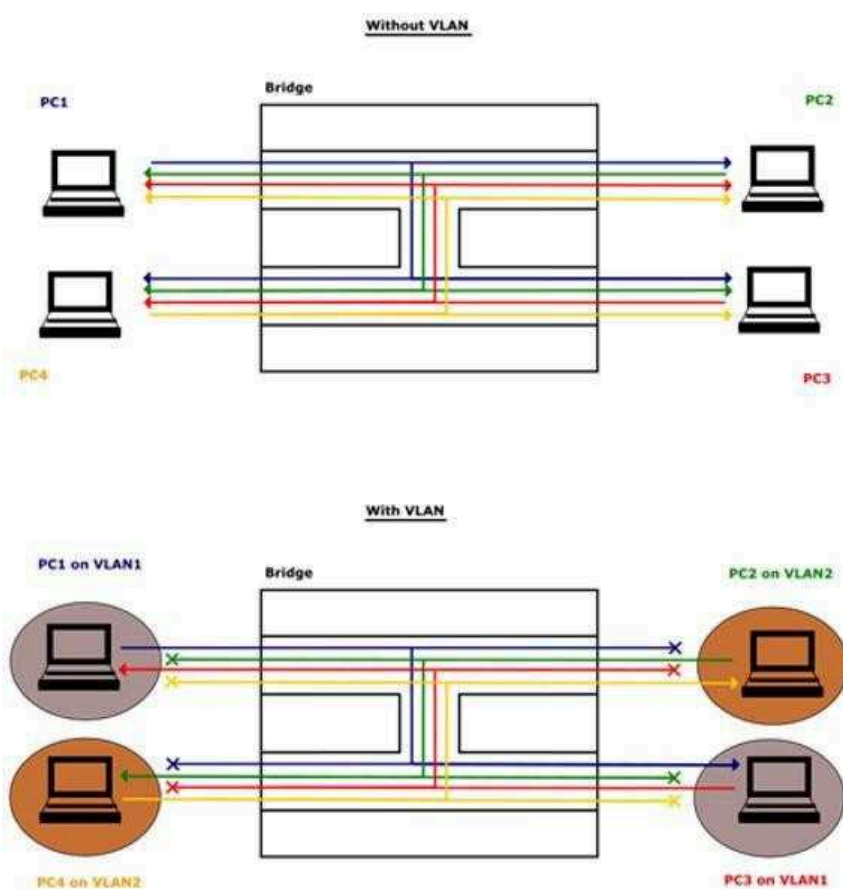
Virtual devices are commonly used to create tunnels or to multiplex several unrelated flows through one medium using VLANs.

V.1.7 VLAN

The **VLAN** (Virtual LAN) concept allows splitting up a broadcasting domain at the data link layer into several sub-domains, by assigning to each sub-domain a VLAN identifying number, the **VLAN_ID**.

VLANs have a number of advantages. They help reduce to a sub-domain the target of broadcast frames, isolate unrelated hosts which share the same physical network, and allow bridges to make different forwarding decisions based on VLAN IDs.

Picture V-3: Computers receive only from computers on the same VLAN



V.1.7.1 Frame tagging

When a network segment must convey frames for several VLANs, the frames are tagged with the corresponding **VLAN_ID**.

V.1.7.2 Vlan interface

A VLAN interface is a Virtual interface that filters a **VLAN_ID** of ingress traffic on a physical interface, then untags it by removing the **VLAN_ID**. Conversely, all egressing traffic of the VLAN interface will be tagged with the **VLAN_ID**.

The VLAN interfaces are achieved with the VIRTUAL INTERFACES / 802.1Q TAGS in submenu.

Please see: [VII.1.4.1 802.1q Tagging](#)

V.1.8 Bridge

A bridge is a device that connects two or more 802.1 compatible network segments and forwards frames selectively. Bridging is done at layer 2 (data link layer) of the OSI model: frames are forwarded based on their Ethernet address, rather than their IP address (unlike a router). Since forwarding is done at Layer 2, all layer 3 protocols can go transparently through a bridge.

Each network segment is connected to the bridge via a **port**. A port can be a physical or virtual interface.

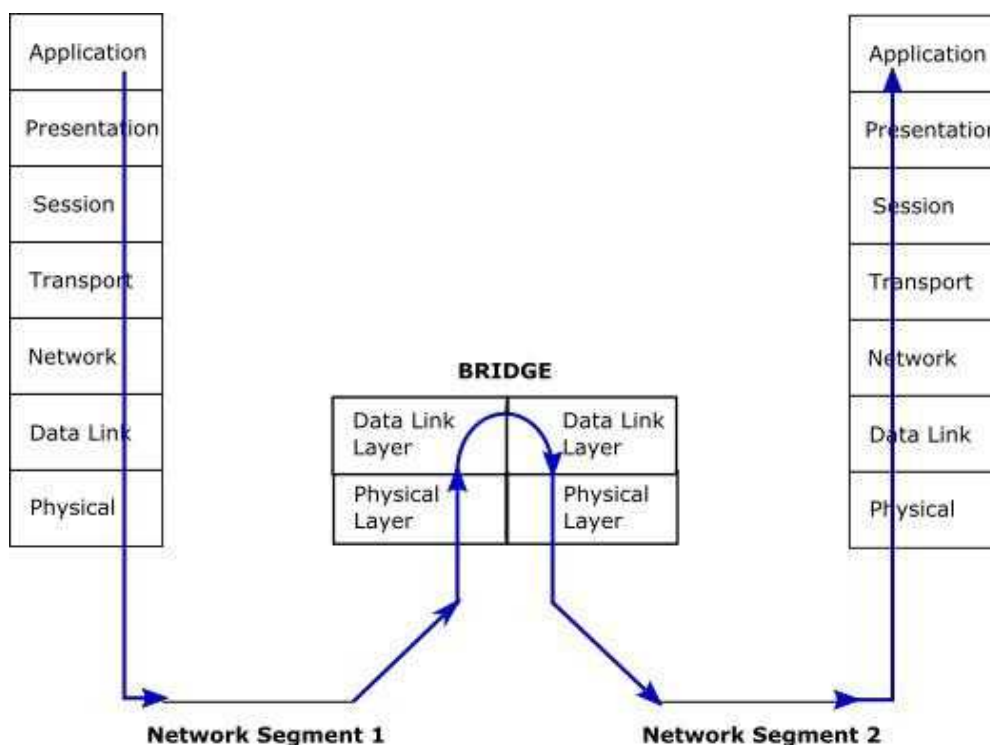
The bridge builds an internal list of MAC addresses in use on each attached network segment. When forwarding a frame, the bridge looks up the destination in its table and forwards only to the port bearing the address. If the destination address is not found in a table, the frame is duplicated and forwarded on every port but the originating one.

A bridge can appear as a distinct hardware called a “switch”. Alternately, a router can embed a “software bridge” which groups several ports in a single layer 2 interface to be configured at layer 3.



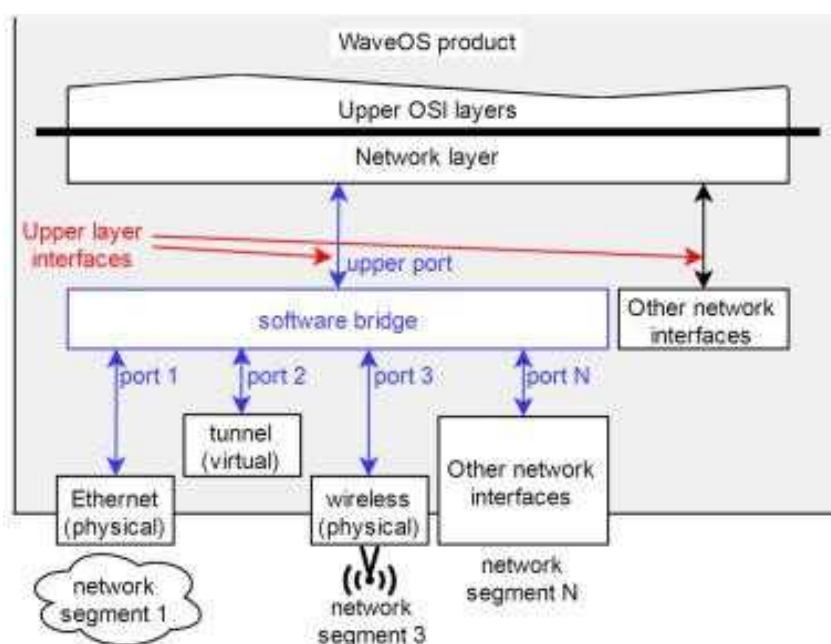
Picture V-4: An 8-ports switch

In order to bridge interfaces together, refer to [VII.1.5.1 Network configuration](#) and the **Interfaces Settings** submenu.



V.1.8.1 Bridge upper layer interface

The software bridges integrated in a router have one dedicated port through which the network upper layer services can route data to the underlying network segments or configure the bridge itself. This special port is called the upper layer interface.



Picture V-5: Upper layer interface in software bridges

V.1.8.2 Vlan bridging

There are 2 types of bridges in WaveOS:

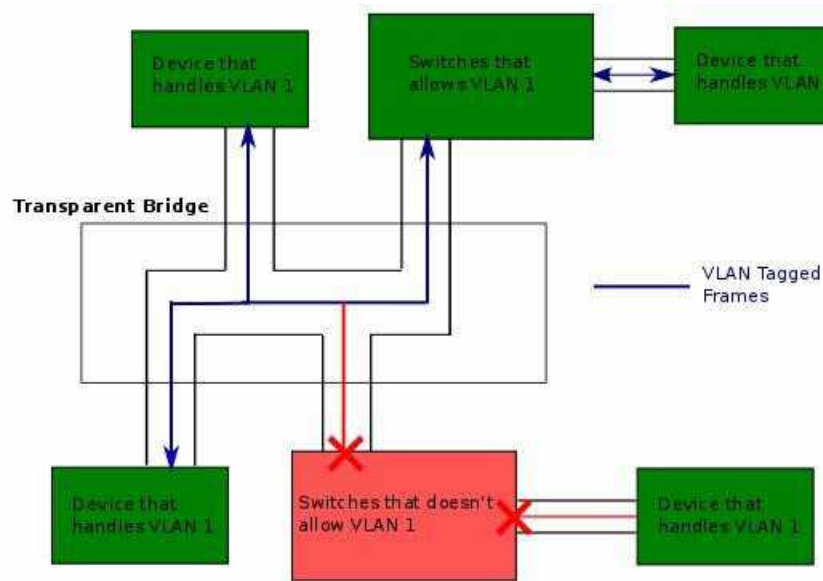
- Transparent Bridge: Bridge that does not handle VLANs.
- Bridge-VLAN: Bridge that handles VLANs.

Transparent bridges are less powerful but easier to set up. They can be tweaked to use a limited form of VLAN filtering.

a) Transparent Bridge

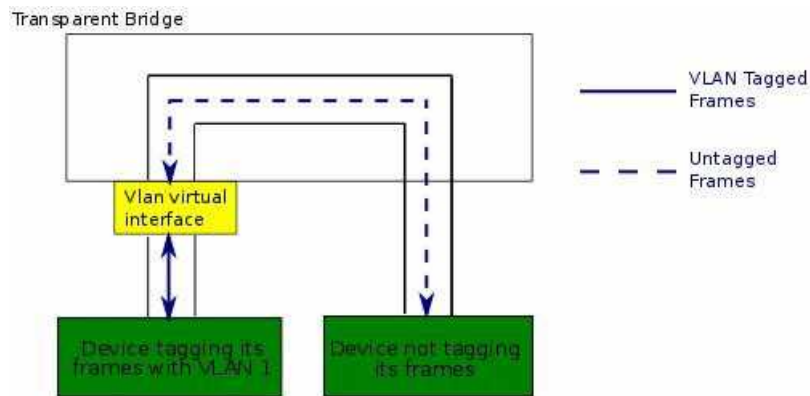
A transparent bridge does not consider VLANs or VLAN tags in frames. Frames are forwarded to any bridge port, only depending on their destination address. If an ingress frame contains a VLAN tag, it will egress unchanged.

So, a bridge port can potentially output both tagged and untagged frames. Manageable external switches connected to this bridge must be carefully set to filter or pass through the planned VLAN tags or untagged frames. See next picture.



Picture V-6: Transparent bridge forwards tagged frames unmodified

However you can create VLAN interfaces (see above) and plug them on the bridge ports. This enforces the use of tags, and allows converting from one VLAN to another:



Picture V-7: VLAN tag conversion using a virtual interface

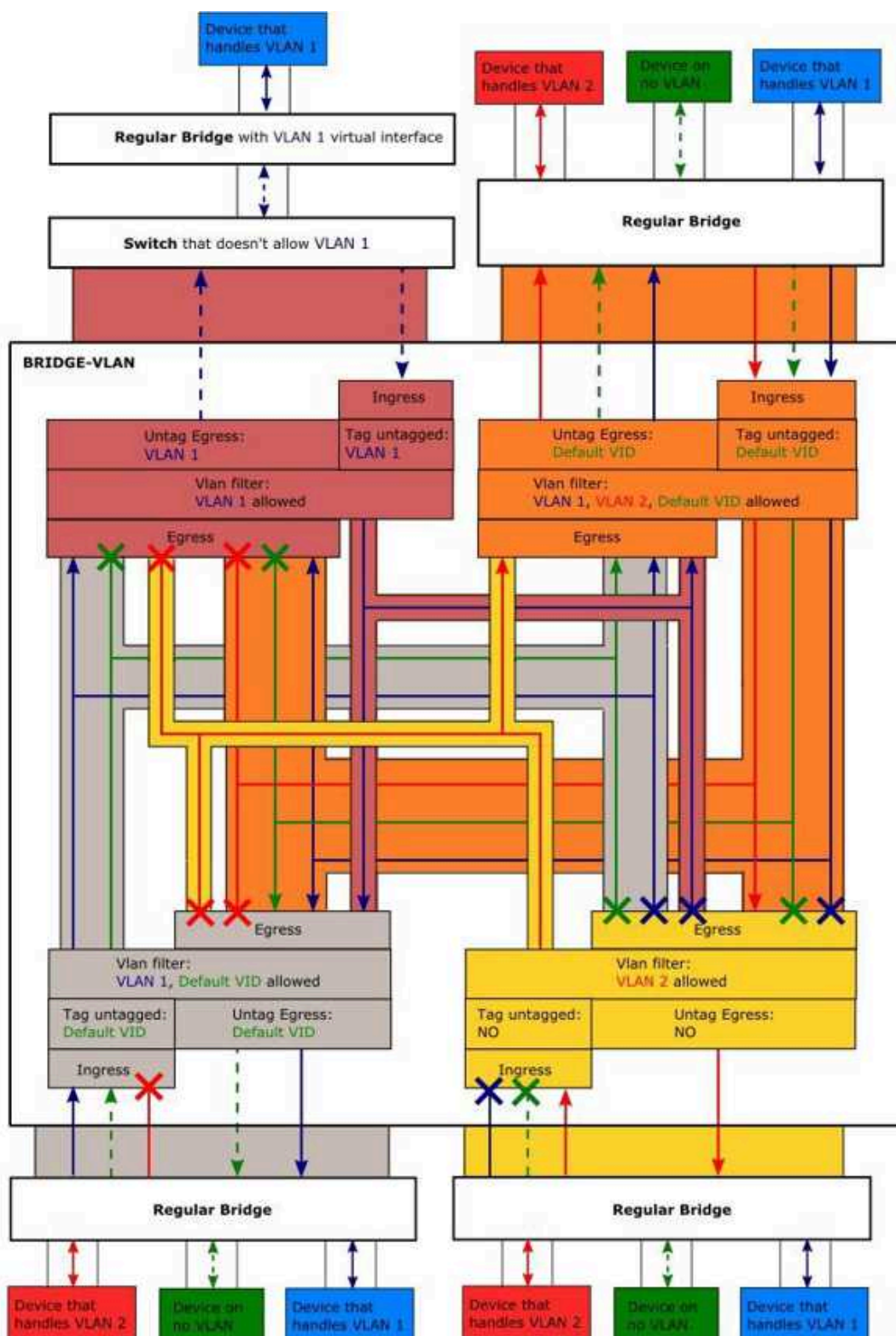
The VLAN interface drops untagged and wrongly tagged ingress frames. It untags properly tagged ingress frames before forwarding them to the bridge. In the other direction it tags egress traffic.

b) Bridge-VLAN

In a “bridge-vlan”, each interface has a list of authorized VLANs. VLANs that are not in this list cannot be forwarded via this interface.

Ingress untagged traffic is dropped and not forwarded by the bridge. Instead it can be tagged with a configurable Default VLAN_ID, so it can then be forwarded by the bridge.

Egress traffic can be tagged or untagged.



The bridges-vlans are achieved with the BRIDGING / VLAN MANAGEMENT submenu.

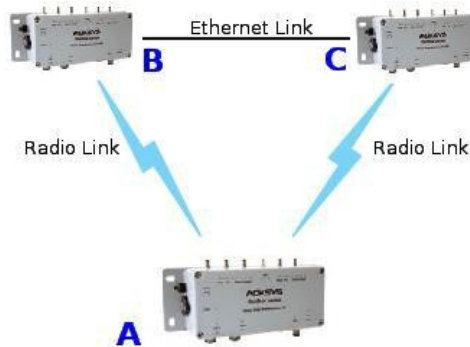
Please see: [VII.1.7.2 Vlan Management](#)

V.1.8.3 Spanning Tree Protocols (STP, RSTP)

a) Spanning Tree overview

Incentive

Interconnecting various switch devices and MAC bridges in a LAN may lead to network loops. For example (see picture below), say you have 3 bridges A, B and C, and there is a direct (Ethernet or Wi-Fi) connection between A and B, another between B and C, another between C and A; then when a device connected to A sends a broadcast, it will be resent by A to B and C, B will resend it to C and C will resend it to A. The broadcast frame is caught in a loop which will soon take a lot of the available bandwidth resulting in a so-called “broadcast storm”.



However, loops may be useful to create backup routes when a link fails. See [Point-to-point redundancy with dual band](#) section for an example.

Topology model and related terms

The STP/RSTP topology is built on physical network links interconnected by **bridges**. The whole structure is called a **Bridged LAN**. Examples of bridges are: Ethernet switches, manageable switches and the software bridge included in the product.

One physical network link may connect together several **end stations** and several bridges. Examples of such links are: the legacy Coaxial Ethernet, the Twisted Pair Ethernet hub, or a wireless Access Point. When there are exactly two bridges connected by the link, it is called a “point-to-point link” from the STP/RSTP point of view. A point-to-point link may connect end stations in addition to the two bridges.

The interface between the bridge and the physical network link is called a **port**. A bridge has several ports and its main function is to forward frames from one port to the others.

There are two ways to provide redundancy in a bridged LAN. First, a bridge may have several ports connected to the same physical network link, to guard against a port failure. Second, a group of bridges may form a loop (a mesh) to guard against a bridge failure.

Operation

When the STP protocol is activated on several interconnected bridges, they will exchange information to agree upon a unique path to transmit frames from one point to another.

The bridges will coordinate to set up a tree structure, thus avoiding loops, and this tree is capable of rearranging automatically when links are broken.

STP should be activated on all bridges participating in a LAN loop. The alternate protocol RSTP is an evolution of STP that reacts more rapidly to broken links in some cases, thus accelerating broken links recovery.



Warning: If the bridge contains **wireless** interfaces, some caution must be taken to ensure proper functioning of **STP/RSTP** on these interfaces:

- If the **wireless** interface is an **Access Point**: The number of clients connected to this Access Point must be limited to 1.
- If the **wireless** interface is a **Client**: The Bridging mode must be "**4 addresses format (WDS)**" (since ARP NAT cannot handle non-IP STP frames). Please note that this implies that the roaming functionality is compatible with ST/RSTP only if set to the [Connect before break](#) mode.

b) RSTP overview

RSTP is a network protocol defined in the standard 802.1d that ensures a loop-free topology in a bridged LAN (With WDS for wireless interface).

It also allows including alternate paths and backup ports in the network topology.

RSTP provides quick recovery of connectivity to minimize frame loss.

Packets named **BPDU** are used for RSTP negotiation between bridges, and for topology changes.

Protocol outlines

Root election

RSTP defines the network topology as a Spanning Tree (an inverted tree). It first selects a **Root bridge**, from which Ethernet/Wireless connections branch out to connect other switches.

After the root bridge is chosen, each other bridge in the network will have 2 types of links:

- **Upper links**: Links leading to the root bridge
- **Lower links**: Link not leading to the root bridge.

Then, each bridge will negotiate with its neighbors to state on which ports are attached to lower links: the **Designated ports**, and which ports are attached to upper links. From these, a single one will be selected as the **Root port**.

Port roles

If several ports in the bridge have an upper link, to avoid loops, RSTP will define these ports either as **backup** if they share the same medium as the root port, or **alternate** if they are on a different medium. It does so according to ports performance parameters.

Only Root and Designated ports are allowed to forward packets, Alternate and backup ports are not allowed to forward.

In case of failure on Root port, RSTP will change an Alternate or Backup port to Root port.

So RSTP defines 5 port roles for a bridge:

- **Root**
- **Designated**
- **Alternate**
- **Backup**
- **Disabled** (no link).

Port states

To avoid loops during RSTP port role definition, ports are allowed neither to forward traffic, nor to learn MAC addresses. After assigning roles, ports are allowed to learn MAC addresses but not yet to forward traffic. Eventually the ports transit to the forwarding state.

In RSTP, a port has 3 states:

- **Discarding**: It is not allowed to forward traffic.
- **Learning**: It is not allowed to forward traffic, but it is learning MAC addresses.
- **Forwarding**: It is allowed to forward traffic, and it is learning MAC addresses.

Topology change propagation

In RSTP, a topology change is generated if a root or designated port moves to forwarding state.

All bridges (root and non-root bridges) can generate and forward topology change information through BPDU to upper and lower links in the network, which allows RSTP to achieve shorter convergence time than STP.

Performance Improvements

Convergence speed

To speed up the transition to forwarding state, and so have a functional network, RSTP defines some performance parameters:

The Edge port type: a port attached to LAN with no other bridge attached. RSTP will make the edge ports transition directly to forwarding state.

The Point-to-Point link type: a direct link between two bridges (without any intermediate equipment like a hub between the two bridges). This will help designated port to transition faster to forwarding state.

The forward delay: The delay to transition Root and Designated Ports to Forwarding state.

Failure recovery speed

Some parameters act on the connectivity recovery speed in case of a bridge failure:

Hello period: Each bridge broadcasts on its designated ports a BPDU every “Hello_time” (by default = 2s), to notify its bridge neighbors of the RSTP statement and actual root. A lower-link bridge considers that it has lost connectivity with its upper-link neighbor if it did not receive 3 consecutive BPDUs (by default $3 \times 2s = 6s$).

Reducing the Hello time speeds up recovery in case of bridge failure, at the expense of greater bandwidth used for the BPDUs.

Best path enforcement

Automatic selection of the root bridge may lead to suboptimal routes for the traffic flows. So, priorities can be set to make RTSP use known best paths:

Bridge priority: The Root bridge is selected by first comparing bridges priorities, and secondly bridges MAC addresses. The user can enforce a known best path by setting the bridges priorities to enforce election of the desired Root bridge.

Port path cost and Port priority: When a bridge has several upper links, these parameters will permit to select which will be the root port on the bridge, and which will be the alternate or backup port.

Backward compatibility with STP:

RSTP will revert to legacy STP on an interface if a legacy version of an STP BPDU is detected on that port. This may lead to degraded performance. So, all bridges in a LAN should use RSTP, although the LAN will still recover (less quickly) with STP.

V.1.9 Tunneling

Tunneling is a way to encapsulate data frames to allow them to pass networks with incompatible address spaces or even incompatible protocols.

Generic Routing Encapsulation (GRE) tunnels are tunnels that can encapsulate unicast/multicast traffic.

GRE creates a bidirectional tunnel between a pair of endpoints (network devices). The source point encapsulates the packets and redirects them to the destination point that will de-encapsulate them, so the GRE tunnel will behave as a virtual point to point link.

The source and destination point are configured via a GRE virtual interface on each side of the GRE tunnel. Each GRE interface contains the IP address of the other side of the tunnel.

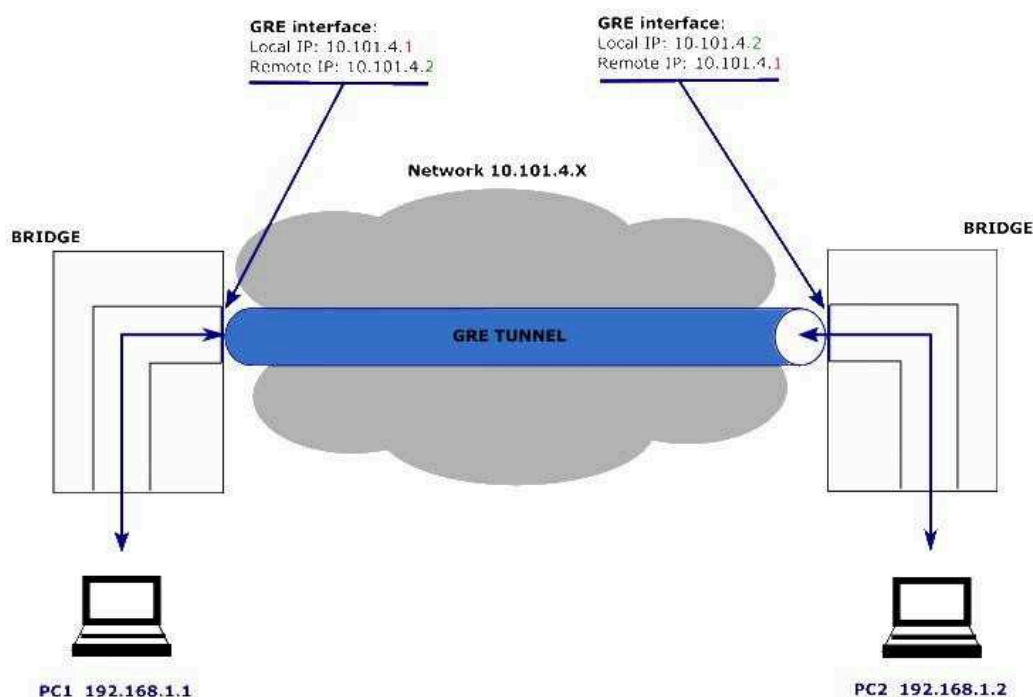
Packets that need to be encapsulated and delivered to some destination (**payload packets**) are encapsulated in GRE packets, then the GRE packet is encapsulated in some other protocol (the **delivery protocol**) and then forwarded.

The protocol type of the **payload packets** can be one of **ETHER TYPES** (see RFC1700).

WaveOS supports **IPV4** as **delivery protocol**.

GRE tunnels are stateless, they cannot change the source endpoint interface to down, if the destination endpoint is unreachable.

WaveOS supports **layer 2 tunneling over GRE** by **bridging the physical interface with a GRE tunnel interface**.



Layer 2 tunneling over GRE can be configured with the **VIRTUAL INTERFACES/L2 TUNNELS**.

Please see: [VII.1.4.4 L2 Tunnels](#)

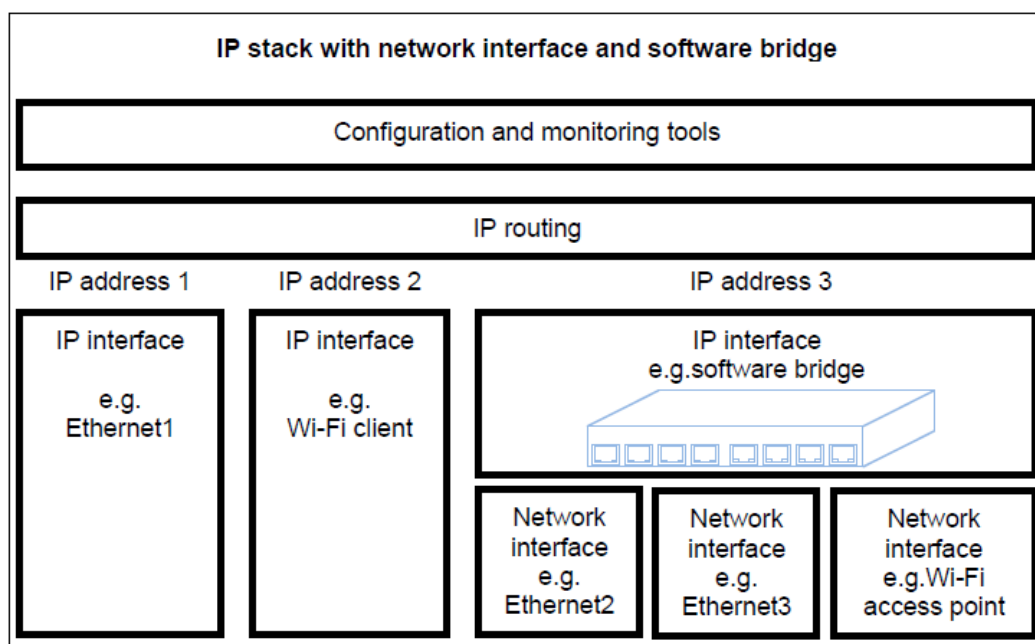
V.1.10 Unicast Routing in IP networks

Routing is the act of finding a path from one place to another, on which a packet can travel. It enables hosts that are not on the same local network to communicate with each other.

A router receives packets not aimed at itself, and selects a path for forwarding it packet, based on its address to the next intermediate router or final destination. To achieve the path selection, the router, uses a routing table built either automatically or by the user.

Routing is done at the layer 3 of the OSI model.

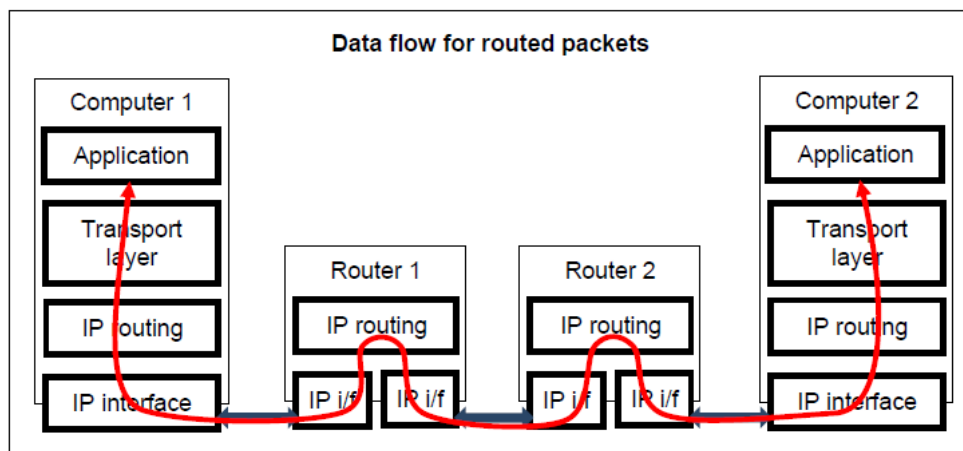
IP is the part of the TCP/IP stack that manages computer addresses and routing. Within one computer, the IP protocol sees each network interface as a separate LAN. Each LAN must have an IP address, something like “192.168.1.2”, to enable it to be used by IP. A network interface is thus the piece of software that drives one network hardware interface.



Picture V-8: Example of combined routing/bridging setup

The set of all the LANs that can communicate together by means of routers is an “internetwork”; the Internet itself is an example of such concept. Routers themselves are nothing more than a computer equipped with several network connections and used specifically to route packets.

Here is the path followed by a data packet traversing 2 routers. The source and destination IP address never change during the transit, contrary to the MAC addresses which change at each routing point.



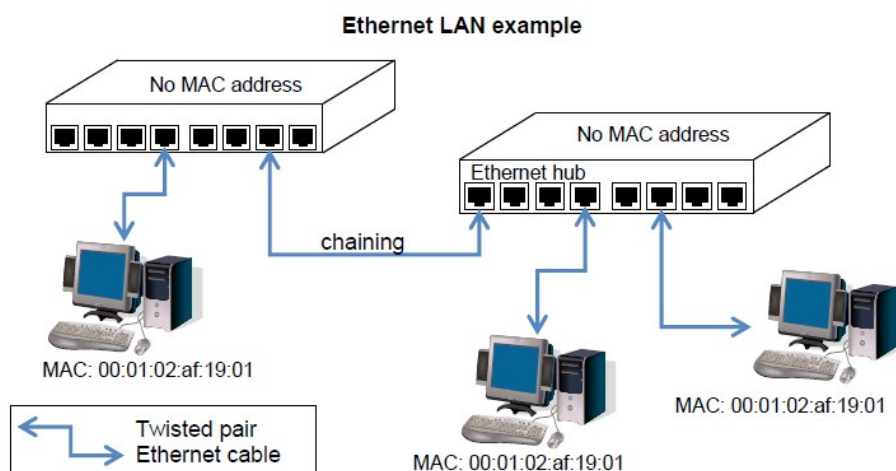
On **WaveOS**, routing is implied when several network interfaces are configured. It can be tuned further in the **ROUTING/FIREWALL** submenu. Please see: [Routing / Firewall](#) chapter.

V.1.11 Addressing in the Data Link Layer (OSI layer 2)

V.1.11.1 Ethernet Address

The Ethernet address is also referred to as the hardware address or MAC address. The first three bytes identify the hardware manufacturer, e.g. Hex 00:09:90 for an ACKSYS product. The last three bytes change in each product. This address is assigned at the factory and should not be changed.

An Ethernet LAN can be made of hubs, switches, bridges. These retransmit data packet without changes. You can think of hubs as mere electrical amplifiers, and you can think of switches as filtering hubs. They must not be confused with IP routers (see below).



V.1.11.2 Wi-Fi MAC Address

The Wi-Fi protocols use the Ethernet addresses format to identify radio cards and to distinguish various functions on the same card. These addresses are either factory assigned by the radio card maker, or dynamically computed, e.g. when the same radio card advertises two access point functions (two wlangs).

A Wi-Fi MAC address can also be used as the BSSID, an identifier which delimits which stations can talk together using only Wi-Fi techniques (e.g. using an Access Point but not TCP/IP or Ethernet)

V.1.12 Addressing in the IP layer (OSI layer 3)

V.1.12.1 IP addresses

This section focuses on IPv4 addresses.

The IP address is a 4 bytes (or 32 bits) number, unique to each device on the network, which hosts can use to communicate. The IP address is usually represented in the “decimal dotted notation” which consists of the decimal value of each of the four bytes, separated by dots.

The IP address is divided into two parts: network and host. The main purpose of this division is to ease the routing process. The set of bits constitutive of the network part is identified by a “network mask”. For example, the mask 255.255.255.0 selects the 24 upper bits of an address as the network address, and the lower 8 bits as the host address.

Another way to specify a netmask is to indicate the number of ‘1’ bits, assuming they all are the most significant. For example, in **192.168.1.0/24** the **/24** part means **netmask 255.255.255.0**

Example: Class C network address and netmask

1	1	0	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	0	0		
193								168								1								200							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0		
255								255								255								0							

Historical usage has named **Class A network** the networks **1.x.x.x/8** to **127.x.x.x/8**; **Class B** the networks **128.0.x.x/16** to **191.255.x.x/16**; **Class C** the networks **192.0.0.x/24** to **223.255.255.x/24**.

A host part with all bits set to 1 is the broadcast address, meaning “for every device”. A host part with all bits fixed to 0 addresses the network as a whole (for example, in routing entries). Addresses above 224.0.0.0 are used for multicast addressing.

V.1.12.2 *Public and private addresses*

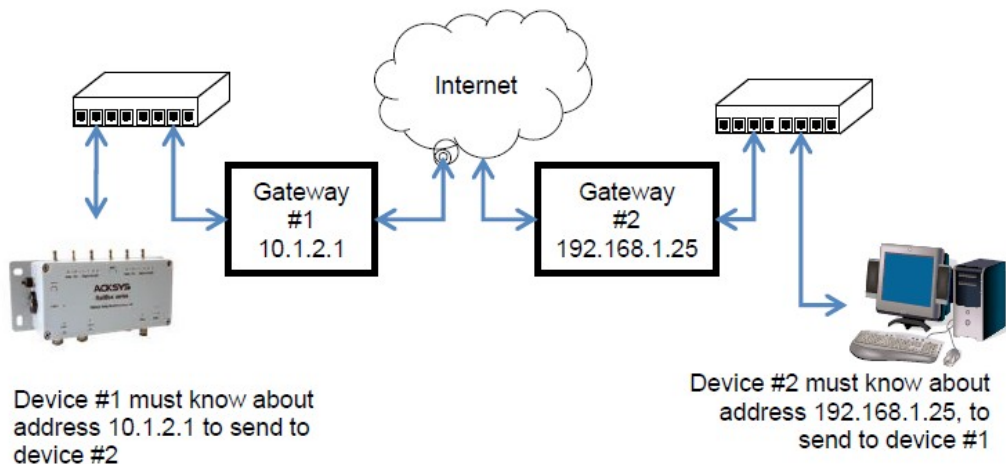
IP addresses can be private or public. Public ones are reserved to devices that require sending data over a public network, such as internet. They are usually purchased or leased from a local ISP.

Ideally each device in the world should have its own IP address so that they always can communicate together. In the real world, most organizations manage their own IP address space independently, so there are duplicates from one organization to another. Two rules help avoiding conflicts:

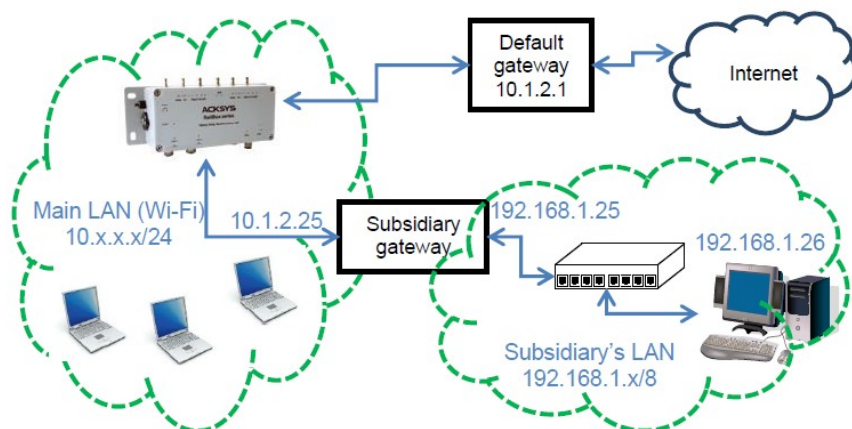
- Internally, organizations use only private addresses from a known set: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- Routers between private area and the Internet convert internal, private addresses to their own Internet public address, hence making the whole world believe that there is only one computer there, holding all the organization's computing resources. This conversion is called NAT
(Network Addresses Translation).

V.1.12.3 *Routers (a.k.a. gateways)*

Each network device communicating through routers **MUST** know the IP address of the gateway nearest to it. It will use this gateway to forward data to farther LANs. If a device does not know its gateway, it may receive data but may not return an answer. For example, this can forbid answering a PING even if the PING request makes its way to the device.



When several routers are available on a single LAN to access various remote LANs, the network devices on the LAN should know about each router's own address and the remote network addresses they lead to. Usually one of the routers is designated as "default", the other ones are treated as exceptions to this default route. Page 49 / 309



Network devices often use the DHCP protocol to get their IP address. The DHCP server may provide the address of the local router at the same time. To set your Acksys product as DHCP client, please refer to section VII.1.10.1 DHCP Server.

V.1.13 Multicast routing

Multicast traffic is used to distribute a single data packet to many receivers. Examples are video broadcasting (one sender, many receivers) or teleconferencing (many senders, many receivers). Multicast traffic normally uses the UDP transport protocol.

Multicast routing aims to broadcast at minimal cost a data flow to selected receivers. To achieve this goal:

- Bridges must forward multicast frames only to networks segments bearing local receivers or requiring IP routers;
- IP Routers must forward multicast packets only to network interfaces bearing either local receivers or requiring IP routers;
- IP routers must select the best path from the data sender to all receivers.

When it is known that the number of willing receivers is large against the total number of hosts in the network, multicast traffic can be flooded throughout the network. This so-called “dense mode” is simple but it takes a lot of network resources and is not scalable.

Usually, there are only a limited number of receivers, this is called “sparse mode”. Two features are required to limit the traffic:

- The receivers must advertise their will to receive
- The intermediate routers must build an optimal distribution tree, e.g. only one copy of the data is sent to a router on the same LAN than two receivers, and only one router distributes a multicast flow on one given LAN.

V.1.13.1 Multicast addresses

A multicast address is usually called a “group” since it does not point to any specific location in the network.

a Ethernet Data link layer

On Ethernet compatible networks (which includes Wi-Fi), group addresses have the least significant bit of the first byte set to 1 (this is the first bit to be transmitted in a frame). In this sense the broadcast address is also a multicast.

b Network layer

IPv4 reserves all 32-bits addresses beginning with binary “1110” for multicast. This covers the group range 224.0.0.0 to 239.255.255.255.

Groups in the range 224.0.0.0 to 224.0.0.255 are reserved for LAN delivery, and cannot be routed outside a LAN.

c Conversion between layers

When a IP multicast is sent out on an Ethernet network, in order for the Ethernet to multicast the frame, the IP group is converted to an Ethernet multicast address.

IPv4 groups are converted to “01:00:5E:” + 23 lower bits of the group.

IPv6 groups are converted to “33:33:” + 32 lower bits of the group.

Hence, two different groups may be received by a device expecting only one of them. The receiving network layer must filter out unexpected groups.

V.1.13.2 PIM-SM

WaveOS implements the Protocol Independent Multicast – Sparse Mode (PIM-SM) to establish the routing tables required for multicast traffic. PIM must run on all the intermediate routers between the data sources and their receivers. The main features of PIM-SM are:

- Manage “rendezvous points” (RP) routers, which are the central distribution points for any given multicast flow
- Identify and manage local multicast sources
- Identify local receivers
- Find routes for multicast flows
- Manage multicast routing tables
- Handle rendezvous points redundancy
- Handle routers redundancy

a Routers redundancy

When several multicast routers are available on a local network, they automatically negotiate and elect the “Designated Router” (DR) that will process multicast for this network. Periodical messages ensure the detection of the DR failure to trigger a new election.

b Local sources management

Multicast sources need no protocols to trigger multicast distribution. They just send out their data. Switches and bridges forward multicast traffic to both the local self-advertized receivers and local routers.

c Local receivers management

Initially, routers do not deliver multicast traffic on local networks until a local receiver advertises itself by broadcasting an “IGMP join” message. This triggers routing of the requested multicast flow from the outside world to the local network.

To account for possible receiver failures and IGMP frames losses, the multicast router periodically sends an “IGMP global query” to refresh its knowledge of local multicast receivers.

Intermediate switches and bridges in the local network may optimize local multicast traffic by using “IGMP snooping”. For this purpose, they may issue “IGMP global query” themselves. These messages differ from the routers’ in two points:

- Their source IP address is 0.0.0.0
- Based on this address, receiving bridges do not account the originator as a multicast router, and so will not forward multicast data to it.

When all local receivers cease to respond to queries for a group, the router stops forwarding this group on the LAN.

d Rendezvous points functions

To avoid configuring each router in the network with each possible source for a multicast flow, each multicast group is assigned one multicast router known as the “rendezvous point” for this group.

Data from a multicast source is encapsulated and sent (tunneled) by the local router (the sender’s DR) to the rendezvous point in unicast.

Requests from receivers are routed by the multicast routers to the rendezvous point.

After initial communication establishment, the rendezvous point may optimize the path, ensuring that the multicast traffic will flow directly from the source to the destinations.

e Rendezvous points selection

Any multicast router can be designated by static configuration as a rendezvous point for a group. After that, other routers come to know its existence by either:

- Static configuration in the other routers
- Dynamic negotiation with the BSR (Bootstrap router).

For redundancy, several rendezvous points may serve the same group. Priorities can be enforced, and in the event of equal priorities, an algorithm ensures that the same rendezvous point is used by all routers.

f BSR election

When rendezvous points are set up dynamically, a Bootstrap Router (BSR) is designated to broadcast periodically the table of currently active rendezvous points.

Any multicast router can be designated by static configuration as a BSR for the network. For redundancy, several BSR may be defined with various priorities. In this case they will elect a master BSR automatically.

g Multicast route selection

When routing *unicast*, the router receives a packet, extracts its *destination address* and forward depending on the destination. On the contrary, when routing *multicast*, the router receives a request for a group which is converted to a *source address* (the one of the rendezvous point). The router must make the request travel in the reverse path toward the source. This is known as Reverse Path Forwarding (RPF). Routers which are on the path of the request set their forwarding tables so that multicast data will travel in the opposite direction.

Several routers may exist on any given LAN; a Designated Router (DR) is elected so that the LAN will not receive duplicate packets for the same group. Also, PIM checks and prunes redundant routes between routers.

V.1.13.3 ***Multicast pitfalls and solutions***

Many details can make a seemingly good configuration fail at forwarding multicast traffic. Here we describe the most common and give directions to solve the issues.

a Router misconfiguration

A multicast router makes full use of its local unicast routing tables in order to compute RPF and SSM paths, and to join other routers. So the IP tables and routes must be correctly set up for unicast operation as well.

Solution: as a prerequisite, check that each router is correctly configured for unicast operation.

b Sender misconfiguration

The sender must be correctly configured for unicast operation. First,

If the sender's source IP is wrong, the local DR will not accept its multicast traffic

But the sender will nevertheless emit its multicast traffic since it is unacknowledged UDP traffic. Second,

The sender must know the route to deliver multicasts

Usually the sender's network configuration includes a default route and multicasts will egress through the network interface bearing the default route.

Solution: pay attention to set the sender IP address in the same subnet than the DR, and either to associate the group address with a local network interface, or to have a DR on the same LAN than the default unicast router.

c Small TTL

Multicast traffic has the capability to flood the network. In order to limit the potential for mistake,

Most standard multicast senders use a default TTL of 1

This is specially the case with software commonly used for network tuning and testing, like Videolan VLC, IPERF and JPERF.

According to the IP protocol, the TTL parameter constrains the number of local networks that a packet can cross. Hence TTL="1" means "only local delivery".

Solution: configure the sending software so that it uses a larger TTL.

The minimum value must take into account the shortest path between source and farthest destination, going either through the RP or directly.

Setting incorrect values will result in packets silently dropped by a certain router along the distribution path.

d MTU and DON'T_FRAGMENT option

This one is not specific to multicast but is prominent in this case, because UDP is generally used. If a packet is larger than the MTU of any subnetwork in the distribution path, the relevant router must fragment it. However,

Most senders default to using the IP Don't Fragment flag

This is specially the case with the Linux kernel, and consequently all application software running under Linux, if they do not provide a means to reset this IP option.

Using large packet sizes will usually result in packets silently dropped by a certain router along the distribution path. Often it will be the sender's DR since it must encapsulate traffic to the RP, thus reducing the MTU.

Solution: configure applications to use the maximum frame size that do not need fragmentation; or configure the sender to clear the Don't Fragment flag.

e Wireless slow multicast traffic

The 802.11 infrastructure mode is asymmetric by essence. When an Access Point sends data to a station, it uses a data rate appropriate for this station. When it sends to many stations as in multicast, 802.11 states that:

the AP must send multicast using the lowest rate available, which is 1

or 6 Mbps depending on the radio band.

When a station sends multicast frames to the AP, it uses the best rate, but in order to make the frame available to other stations, the AP immediately re-broadcasts the frames at the lowest rate.

This results in

- very slow multicast traffic over Wireless,
- great waste of bandwidth for other traffic.

Solution: Make multicast traffic pass the wireless link while encapsulated in a tunnel. This can be for example a GRE tunnel configured for this purpose, or you can take advantage of the encapsulation between the sender's DR and the RP (in which case you must forbid the RP to switch to the shortest path, which would bypass the tunnel).

f Wireless transmitting traffic permanently

The radio channel is a sparse resource. On another hand,

the multicast sender blindly sends to its DR,

and this DR quite blindly sends to the RP (except that the RP can request a temporary suspension when it has no receivers).

Solution: the path between the sender and its DR should not cross a wireless LAN. The path between the sender and its RP should not cross a wireless LAN, though this requirement is less stringent. If you refer to the previous pitfall item, an optimal system has the sender and the RP on the same side of the wireless LAN, and use a GRE tunnel to transfer multicast data to the other side.

g

Wireless transmitting unwanted multicast traffic

An Access Point connected to an Ethernet segment conceptually extends the Ethernet to the associated stations.

Unwanted multicasts reaching the AP from the Ethernet will be forwarded to the stations at very low speed, wasting bandwidth.

In WaveOS this can occur if the AP is added to a bridge together with other interfaces.

Solution: if you know in advance that no wireless station is interested in some multicast group, you can set bridge filters to forbid outgoing multicast traffic. See [Bridge filter](#) in the web interface chapter.

h Access points and multicast routers

When the multicast router starts it enumerates the available network interfaces.

If one of them is an access point, it may be that this AP is not yet started because it is configured to search for a channel (ACS function) or because the chosen channel is subject to DFS delays (CAC or NOP). In this case the multicast router cannot establish various negotiations, and this network interface will stay ignored forever.

Access point are delayed by ACS and DFS

Solution: Put the AP all alone in its own bridge. The multicast router will consider that the bridge itself is available, whatever the AP state.

i Long delays at startup

While running, the multicast router reacts to various events in a timely manner. However, users will go through unexpectedly long delays when WaveOS starts up.

This normal behavior comes from:

- a number of protocols (IGMP, DR election, BSR election, RP election, RPF establishment),
- starting simultaneously,
- depending on each other,
- each having large retry timers.

The resolutions of the timers used in PIM (5 s) compounds this effect.

Solution: Only broad indications can be given here. Keep in mind that the problem is only at startup though.

On one hand you must balance between a slightly faster startup by tweaking various timers (IGMP querier, HELLO and RD-Candidate messages), the extra load put on the network and compatibility with alien multicast routers; and on another hand, you must balance between static RP list configuration, and the extra administration burden.

j **Associating VRRP and PIM**

When using a VRRP router as multicast router, VRRP will resume or suspend the PIM router depending on the VRRP state being master or backup. This behavior is configurable by linking VRRP to multicast routing in the [VRRP configuration page](#), in case you do not use PIM on the same interfaces as VRRP.

Several points must be kept in mind when dealing with complex configurations.

- 1 The multicast router is all-or-nothing: either it runs and manages all configured interfaces, or it stops and manages none. If a part of the network interfaces is not involved in VRRP, these interfaces will be unmanaged nevertheless when VRRP transitions to backup state.
- 2 When the VRRP backup transitions to master state, PIM restarts. This means that the takeover delay is the same as for a startup, which means, much longer for the multicast traffic than for the unicast traffic.

V.1.14 **Firewall**

Network interfaces can be conceptually grouped into “zones” in order to assign common administrative policies to them. *Firewall*

The firewall permits to set rules that are applied to each packet, and that decides if a packet must be forwarded or blocked.

In WaveOS, the firewall feature can be tuned in the ROUTING/FIREWALL/NETWORK ZONES submenu.

Please see: [Firewall](#)

V.1.15 **Zones and Network Address Translation (NAT)**

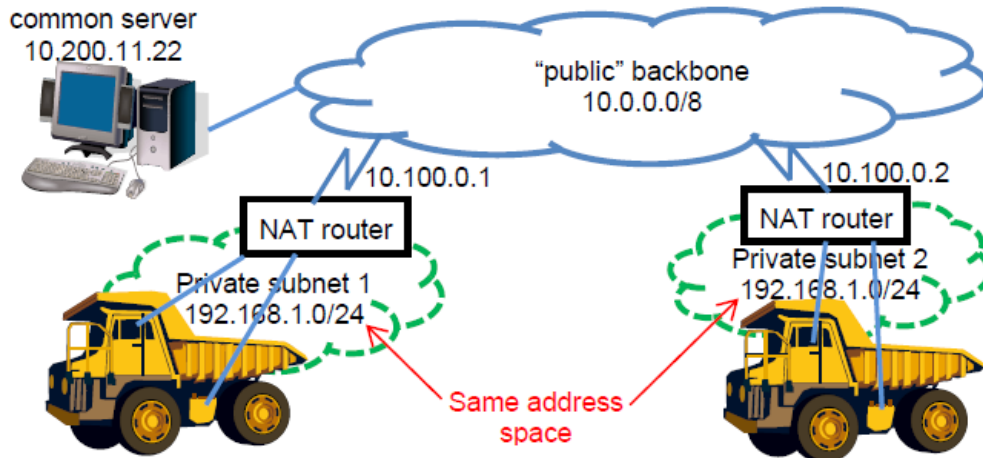
In a router, you may need to selectively block or allow traffic between network interfaces. A zone is an administrative concept which groups several IP interfaces in order to specify common extra processing:

- Firewall rules
- IP address conversion rules (to implement NATs).

V.1.15.1 **NAT/PAT (Network/Port Addresses Translation) routers**

When a global network is composed of several networks managed by independent administrators and connected together, the same IP addresses could potentially be assigned inside the subnetworks. This is customarily seen in the Internet which serves as a backbone to connect together the private networks of many companies. This could be used also when many identical subnetworks must be set up and connected to a root backbone.

In this kind of setup, each subnetwork has a router which is the gateway to and from the subnetwork. The routers are interconnected by the backbone. To avoid IP addresses duplicates, the routers convert the subnetwork IP addresses to backbone IP addresses, hence the name “NAT”.



In the case of a NAT/PAT router, the network is split in two “**zones**”: the **public zone** which is materialized by the backbone, and where a central administration gives out “public” IP addresses; and the **private zone** where the administrator can assign IP addresses without the knowledge of IP addresses outside.

Then the NAT/PAT router changes all outgoing (from private to public) IP datagrams to masquerade the source private IP address into its own unique, public IP address. It also changes the incoming (from public to private) IP datagrams replacing the destination address, which is the router’s public address, to the private IP address of some device in the private network. In order to keep offering a wide address space as seen from the public side, the NAT/PAT router uses port numbers as extensions to the IP addresses. Hence,

the NAT/PAT mainly works with UDP and TCP; it cannot handle generic ICMP routing, but only towards one private device at most.

The NAT/PAT router must manage incoming connection calls as well as outgoing connection calls. It uses two main conversion tables:

- A configurable table which assigns a private destination IP to selected destination ports in the incoming calls
- An internal conversion table which tracks which ports are assigned to which (private IP, private port) couple for outgoing datagrams.

Due to the various processing involved, the performance of a NAT/PAT router is lower than the performance of a regular router, which is lower than the performance of a simple software bridge.

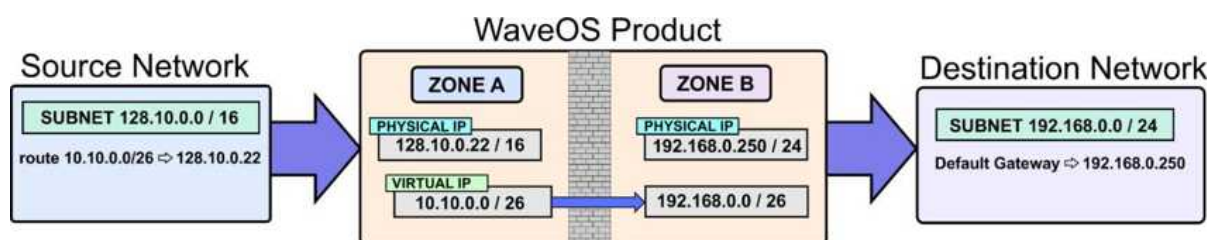
V.1.15.2 NAT 1:1

In the case of 1:1 NAT, the translations are still carried out by routing between different zones, but there is no longer any notion of private and public zones. The idea here is to create virtual subnets, associated with a given zone (Source zone), and to perform translations from these virtual subnets to the real subnets of another zone (Destination zone). We can thus translate either unique IP addresses or entire subnets.

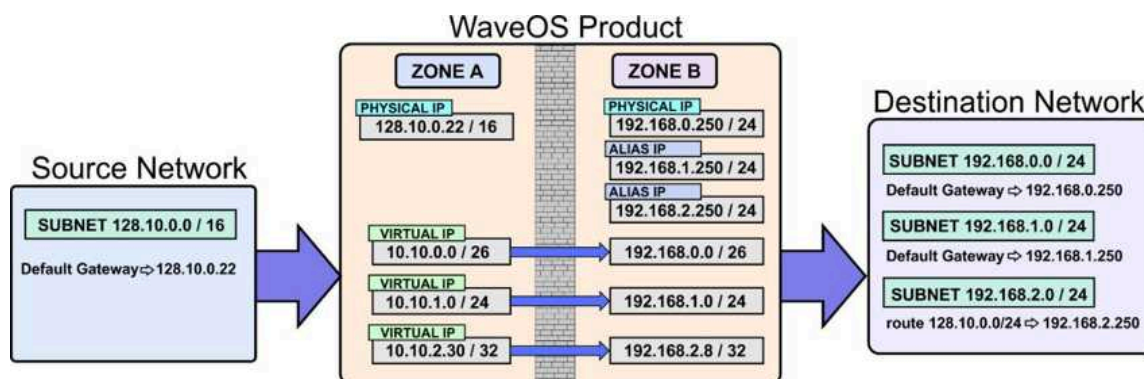
In the following example, we have a source network on subnet 128.10.0.0/16, and a destination network on subnet 192.168.0.0/24.

From the source network, we want to access the 64 lower addresses of subnet 192.168.0.0 of the destination network (192.168.0.0 to 192.168.0.63).

To do this, we create a virtual subnet in Zone A (source zone), which will be defined in the source network by a static route. In the WaveOS product, we will then be able to define a rule for translating this virtual subnet to the physical addresses of the destination network. To restrict translation to the first 64 addresses of the subnet, the subnet mask on the virtual IP must be 255.255.255.192 (or /26 CIDR notation)



Now if we want to add access to the whole 192.168.1.0 subnet and reach a unique 192.168.2.0 subnet address, we just need to add the virtual addresses and define the proper translation rules. However, it will be necessary to create on the destination interface an alias of the IP address of the product for each of the subnets, in order to be able to define the return path, via static routes, or default gateways.



V.2 Wireless concepts in 802.11

V.2.1 Wireless architectures

A wireless LAN (WLAN) is a group of Wi-Fi capable stations. They communicate with each other by following rules specified for a given architecture.

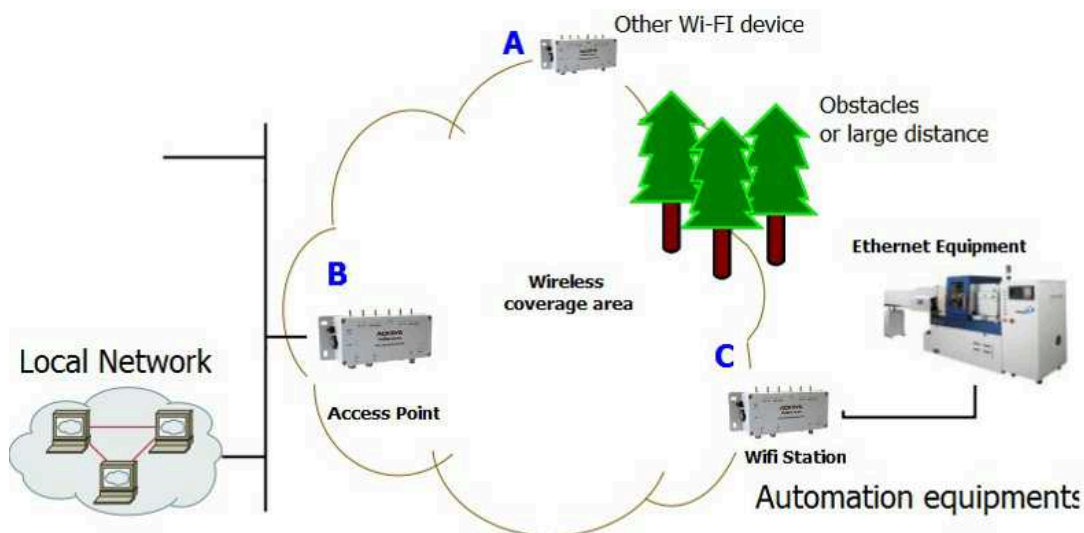
The stations in the group have in common a wireless network name which identifies the WLAN. The IEEE802.11 norm defines three architectures to communicate between Wi-Fi stations:

- Infrastructure (a client/server where the AP relays all traffic)
- Ad-hoc (peer to peer multipoint communication, no relaying)
- Mesh network (all stations are involved in relaying traffic)

V.2.1.1 Infrastructure Mode

In an infrastructure network there are 2 kinds of devices (called **stations**):

- The access points (APs)
- Client Wi-Fi devices (client stations) that connect to an access point to gain access to other Wi-Fi devices or LAN devices.



Products **A**, **B**, **C** can communicate with each other.

Product **B** relays data between products **A** and **C**.

Product **B** relays data between the LAN and products **A** and **C**.

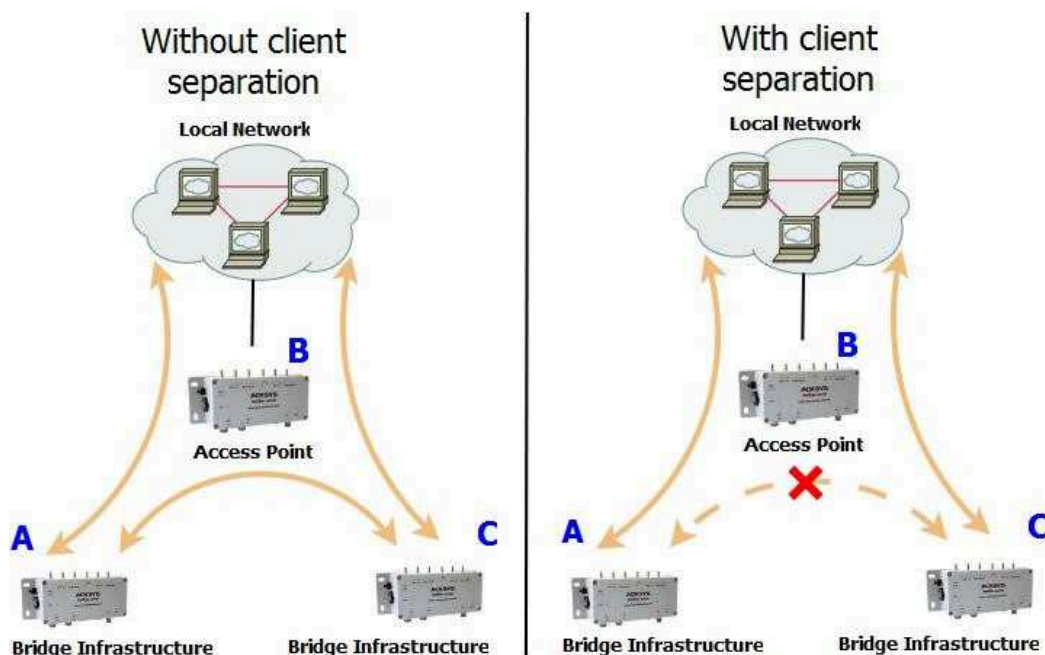
The infrastructure mode provides central connection points for WLAN clients and the AP may also bridge them to a wired network. Prior to any communication, the client must join the WLAN (wireless LAN) by selecting one access point, authenticating and possibly establishing encryption keys.

The AP and its associated clients form a Basic Service Set (BSS) identified by a BSSID, in the form of a MAC address automatically forged by the AP. More APs can be added to the WLAN to increase the reach of the infrastructure and support any number of wireless clients. The whole WLAN is identified by the SSID, a string of 1 to 32 bytes, usually a human-readable text. All wireless stations and APs in the same WLAN must be configured to use the same SSID.

The APs in the WLAN are then cabled to a common wired LAN to allow wireless clients access, for example, to Internet connections or printers.

Compared to the alternative ad-hoc wireless networks, infrastructure mode networks offer the advantage of scalability, centralized security management and improved reach.

Since the 1.4.2 revision, the firmware implements the “clients isolation” feature which allows the AP to block communication between clients. In this case product A will be able to communicate with product B and the “local network” but not with product C (according to the figure below). Product C will also be able to communicate with product B and the “local network” but not with product A. The picture shows the access point behavior with and without the Separation Client option.



In the infrastructure mode concept, a client is supposed to be a single unit. However the wireless client can bridge several Ethernet devices to a BSS towards the AP, and it still appears as only one device, by converting MAC addresses on the fly (see section [V.2.6 Wired to wireless bridging in infrastructure mode](#)).

V.2.1.2 Ad-hoc Mode

On wireless computer networks, ad-hoc mode is a way for wireless devices to directly communicate with each other. Operating in ad-hoc mode allows all wireless devices, within range of each other, to see each other and communicate in peer-to-peer fashion without involving central access points (including those built into broadband wireless routers).

To set up an ad-hoc network, each wireless adapter must be configured for ad-hoc mode (as opposed to the alternative infrastructure mode).

In addition, all wireless adapters on the ad-hoc network must use the same SSID and the same channel number.

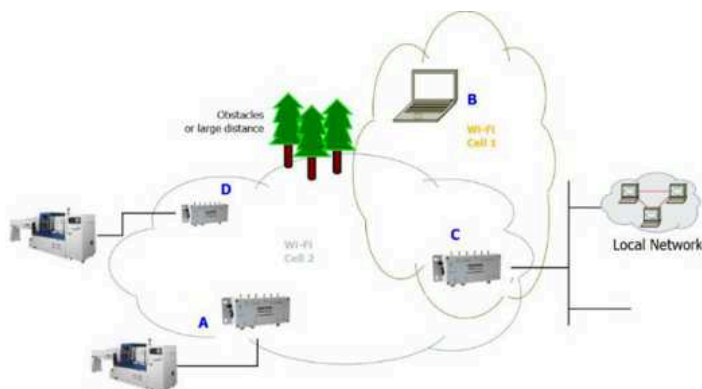
An ad-hoc network tends to feature a small group of devices in very close environment. All communicating devices must share the same cell. There is no way to establish a route in order to link 2 remote products.



Without security, Ad-hoc mode works in 802.11abgn/ac mode.

With WEP security, Ad-Hoc mode works in 802.11abg mode

Ad-Hoc mode does not support WPA/WPA2 security.



Products **A**, **C**, **D** can communicate with each other.

Products **B**, **C** can communicate with each other.

Products **B**, **D** cannot communicate, obstacle on the way.

Products **A**, **B** cannot communicate, they are too far away.

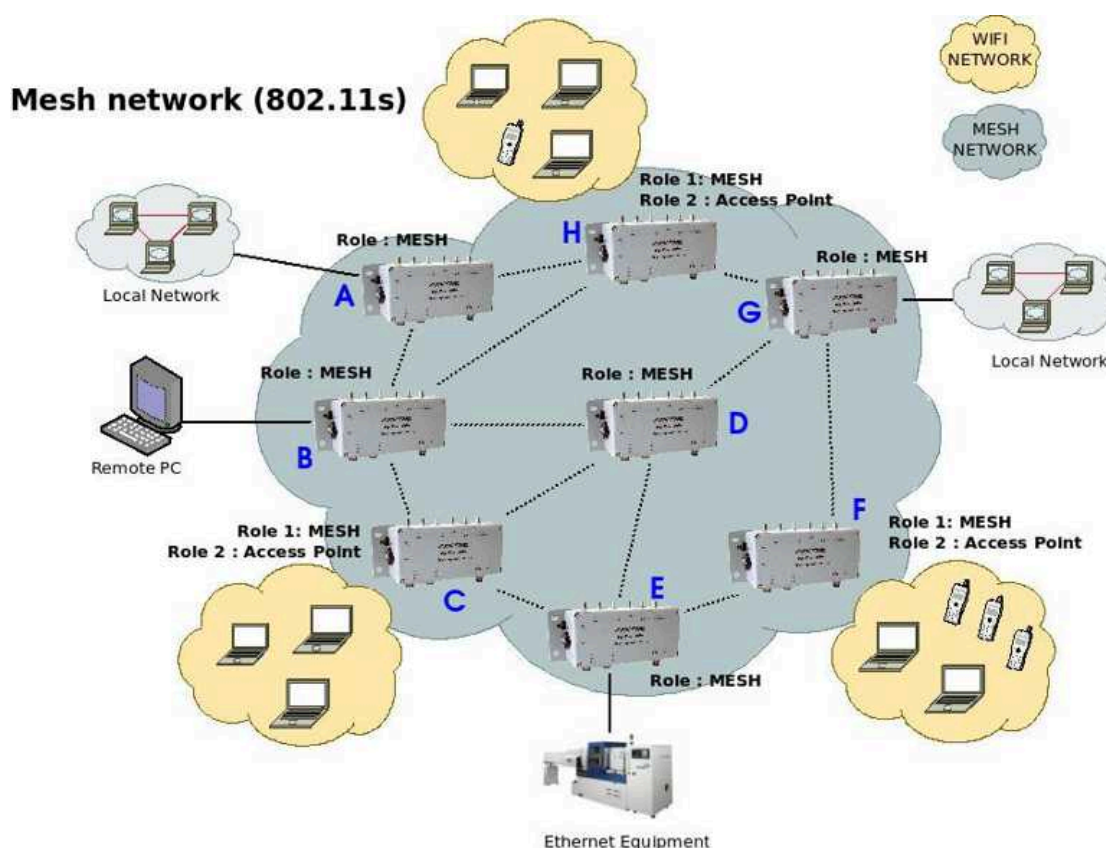
Product **C** cannot relay from **A**, **D** to **B**.

V.2.1.3 Mesh (802.11s) Mode

In a 802.11s mesh network there are 3 kinds of devices. They all participate in the process of packet relaying:

- A **mesh station** has a functionality of its own (i.e. a laptop computer).
- A **mesh access point** provides both “mesh” and “basic access point” facilities, bridging non-mesh Wi-Fi devices to the mesh network.
- A **mesh portal** allows other network types to be bridged to the mesh network. For example, a portal would bridge Ethernet to Wi-Fi mesh.

SOLEXY products currently implement “station” and “portal” functions. Products equipped with two radio cards can be used as mesh access points.



Products **A** to **H** can communicate with each other.
 Products **A, B, D, E, G** provide Mesh portal functionality.
 Products **C, F, H** provide Mesh AP functionality.

Routing protocols

To determine the transmission path between two mesh points, a routing protocol must analyze the network. 802.11s defines HWMP as a mandatory

protocol, and it has provisions to plug in other third-party routing protocols. SOLEXY devices implement HWMP.

Security protocols

802.11s networks can use either no security, or the SAE security described in section [V.2.5.7 Mesh Secure Authentication of Equals \(SAE\)](#). This security is roughly similar to infrastructure WPA/PSK.

V.2.1.4 *Wireless Network Name*

This name is also referred to as the SSID and serves as a wireless network identifier.

A service set identifier, or SSID, is a name used to identify the specific 802.11 wireless LAN to which a user wishes to access. A client device will receive broadcast messages from all access points within range, advertising their SSIDs, and can choose one to connect to, based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one.

Devices participating in a Wi-Fi communication must all use the same SSID. When you are browsing for available wireless networks, this name will appear in the list. For security purposes we highly recommend changing the pre-configured network name.

The SSID used in 802.11s Mesh mode is called “mesh ID”. It takes the same form as the infrastructure SSID, but is a separate parameter: if you use the same string for an infrastructure SSID and a mesh ID, they are considered as two distinct WLANs.

V.2.1.5 *Virtual AP (multi-SSID) and multifunction cards*

The products can handle several virtual functions (interfaces)) on a single radio card, within certain limits. For example, one radio device can be used to advertise several SSID, simulating several real APs at once, together with one mesh point.



When one radio card supports simultaneous virtual interfaces **they must all be set to the same channel** (hence the client scanning must be restricted to the channel you selected, and multichannel roaming is impossible). The **channel bandwidth is therefore shared** between all interfaces.

The multifunction limits are indicated on the web interface, page “Setup / Physical interfaces Overview”.

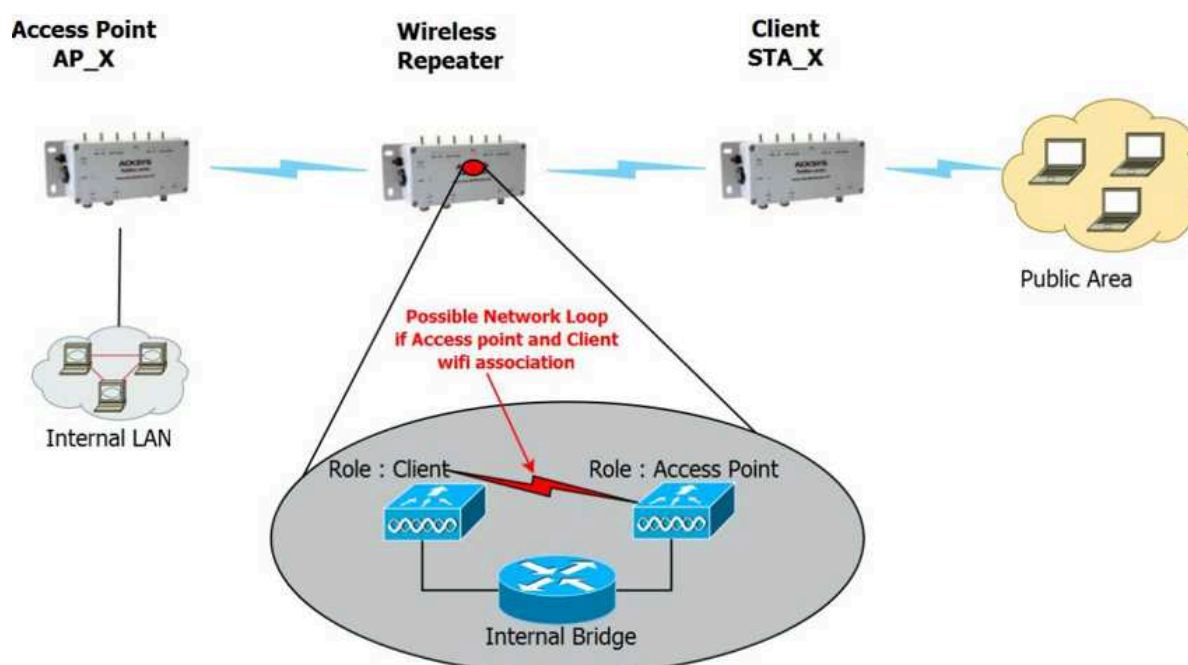
V.2.1.6 Wireless repeater

When the distance between an Access point **AP_X** and a Wireless Station **STA_X** is too long for a direct connection, a **wireless repeater** is used to bridge the gap.

The wireless repeater has 2 roles:

- ➔ Client Role to relay data from/to the Access point AP_X.
- ➔ Access point Role to relay data from/to the Wireless Station STA_X.

These 2 roles will be bridged together in the same switch. Thereby, several configurations are possible for a repeater.



Special caution should be taken when configuring the Repeater to avoid the client repeater association with the Access point repeater (when they have the same SSID), which will then generates a network loop.

There are two ways to avoid this network loop:

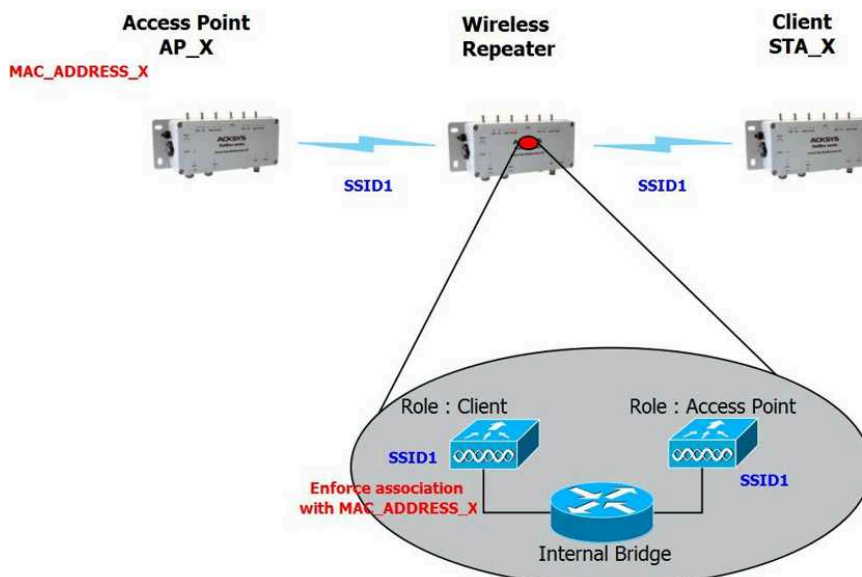
- ➔ Set the same SSID on client role and Access point role of the repeater, but enforce the client role to associate with the BSSID of the AP_X. Use the "multiple SSID" feature of the client role to unlock BSSID configuration.

Advantage:

Service continuity: the repeater will extend the current network with the same SSID. So, the end user can keep the same SSID in all the network locations

Drawback:

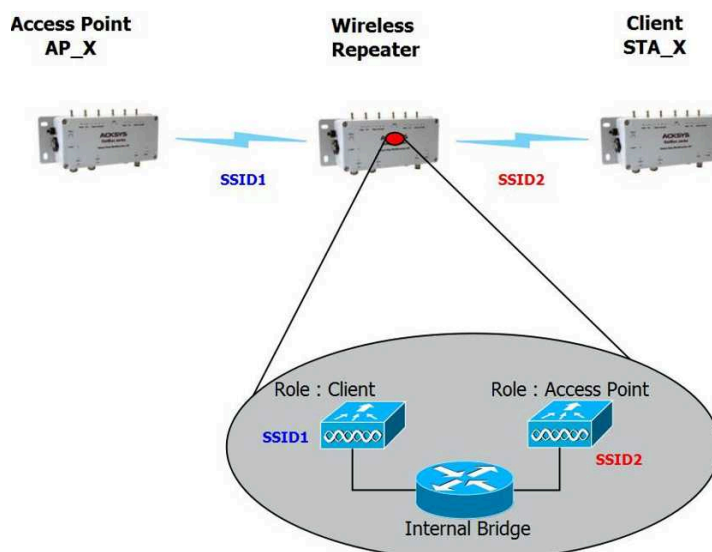
When AP_X is replaced, the client role of the repeater must be reconfigured, so that it only associates with the new BSSID.



➔ Set a different SSID on client role and Access point role of the repeater. Advantage:

No need to reconfigure the repeater if we change the AP_X. Drawback:

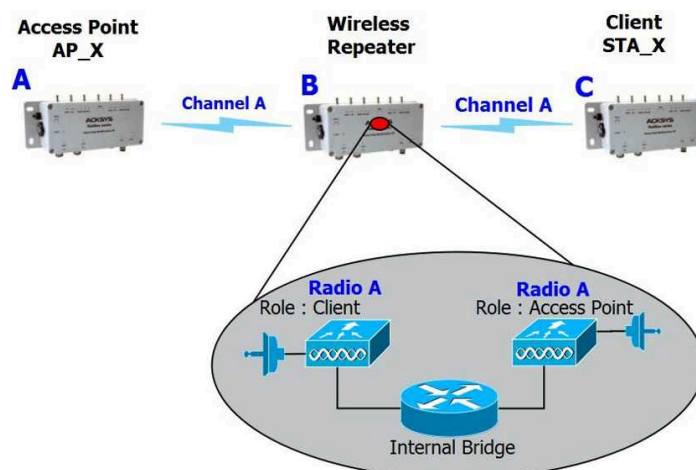
It requires the end users to use multiple SSIDs, as the network extension has now a different SSID.



Impact on Throughput:

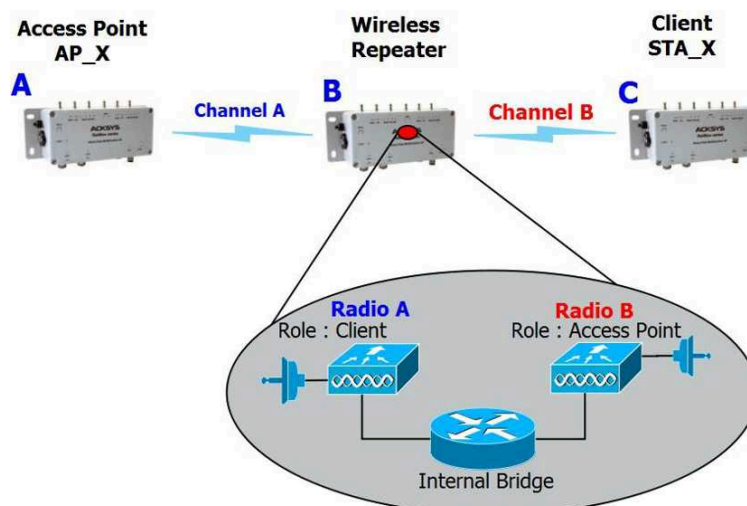
A repeater uses one radio card to perform the 2 roles, Client+Access point, and to perform the transmissions from AP_X to Repeater, and then Repeater to STA_X (and vice-versa).

Since the repeater, having only one radio card, cannot receive and transmit at the same time, the throughput is reduced by at least 50%.



High performance Repeater:

To enhance throughput, a dual radio repeater can use one radio for the AP role and the other radio for the client role, using a different channel on each radio card, so it can transmit and receive at the same time.



Advantage:

Doubles the available bandwidth; also solves the loop problem.

Drawback:

The end users must search several channels for the SSID.

V.2.2 Modulation and coding

There are 5 kinds of wireless transmission formats available: 802.11b, 802.11g, 802.11a, 802.11n and 802.11ac.

V.2.2.1 802.11b

802.11b is supported for compatibility with old devices. Using it will lower the throughput for all devices in the radio range, because 802.11b uses a lot of bandwidth for little throughput.

Op. Frequency	Typical throughput	Bit Rate (Max)
2.4 GHz	4.5 Mbit/s	11 Mbit/s

Note: actual throughput and bitrate depends on the distance between stations, antennas quality and radio conditions

802.11b has a maximum raw data rate of 11 Mbit/s and uses the same media access method defined in the original standard. 802.11b devices suffer interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include: microwave ovens, Bluetooth devices, baby monitors and old cordless telephones.

V.2.2.2 802.11g

This transmission standard works in the 2.4 GHz band (like 802.11b) but operates at a maximum raw data rate of 54 Mbit/s, or about 20 Mbit/s mean throughput. 802.11g hardware is fully backward compatible with 802.11b hardware.

Op. Frequency	Typical throughput	Bit Rate (Max)
2.4 GHz	20 Mbit/s	54 Mbit/s

Note: actual throughput and bitrate depends on the distance between stations, antennas quality and radio conditions

Like 802.11b, 802.11g devices suffer interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include: microwave ovens, Bluetooth devices, baby monitors and old cordless telephones.

V.2.2.3 802.11a

The 802.11a operates in 5 GHz band with a maximum raw data rate of 54 Mbit/s, which yields a realistic mean throughput in the mid-20 Mbit/s.

Op. Frequency	Typical throughput	Bit Rate (Max)
5 GHz	20Mbit/s	54Mbit/s

Note: actual throughput and bitrate depends on the distance between stations, antennas quality and radio conditions

Since the 2.4 GHz band is often saturated, using the relatively unused 5 GHz band gives 802.11a provides a significant advantage. However, this high carrier frequency also brings a slight disadvantage: The effective overall range of 802.11a is slightly less than that of 802.11b/g; 802.11a signals cannot penetrate as far as those for 802.11b because they are absorbed more easily by walls and other solid objects in their path.

V.2.2.4 802.11n

802.11n can operate on either the 2.4 GHz or 5 GHz band. According to the chosen one, the above notes about range and band saturation also apply.

802.11n also allows using a channel width of either 20 MHz or 40 MHz to double bandwidth. "HT20" refers to the standard single channel operation; "HT40" refers to the extended double channel operation.

802.11n hardware may allow transmission of more than one data stream (so-called "spatial streams") simultaneously. In order for the streams not to interfere with each other, the radio signal must bounce on obstacles in various directions, or the antennas must be polarized. Both cases result in lower range due to power losses, but faster transmission.

The number of spatial streams must not be confused for the number of antennas. Furthermore, antennas can be dedicated to emission or reception only. Hence an 802.11n radio specification must include three numbers: number of transmitters, number of receivers, and number of spatial streams.

In order to automatically adapt to radio conditions, the 802.11n uses various transmission parameters: number of streams, modulation, channel width and so on. The resulting transmission format is named Modulation and Coding Scheme (MCS). SOLEXY products handle 1 to 3 streams depending on the model. Here are the physical bit rates achievable with one, two and three streams:

Maximum bit rate (Mbps)

Channel width	20 MHz	40 MHz
1 stream		
MCS 0	7.2	15
MCS 1	14.4	30
MCS 2	21.7	45
MCS 3	28.9	60
MCS 4	43.3	90
MCS 5	57.8	120
MCS 6	65.0	135
MCS 7	72.2	150
2 streams		
MCS 8 = 2xMCS0	14.4	30
MCS 9 = 2xMCS1	28.9	60
MCS 10 = 2xMCS2	43.3	90
MCS 11 = 2xMCS3	57.8	120
MCS 12 = 2xMCS4	86.7	180
MCS 13 = 2xMCS5	115.6	240
MCS 14 = 2xMCS6	130.0	270
MCS 15 = 2xMCS7	144.4	300
3 streams		
MCS 16 = 3xMCS0	21.7	45
MCS 17 = 3xMCS1	43.3	90
MCS 18 = 3xMCS2	65.00	135
MCS 19 = 3xMCS3	86.7	180
MCS 20 = 3xMCS4	130	270
MCS 21 = 3xMCS5	173.3	360
MCS 22 = 3xMCS6	195	405
MCS 23 = 3xMCS7	216.7	450

Note 1: When the peer station cannot handle short guard intervals, the bit rate is reduced by about 10%. Guard interval is an 802.11n feature allowing shortening some idle times during transmission.

Note 2: As can be inferred from the above table, the bit rate is proportional to the number of streams. A 3 streams radio can transfer up to 450 Mbps.

Note 3: Actual bitrate and throughput depend on the distance between stations, antennas quality and radio conditions

For detailed information and relationship about MCS, bit rates, maximum transmit power and receiver sensitivity, refer to either the CDROM or the quick start guide appropriate for each product.

V.2.2.5 802.11ac

Compared to 802.11n, 802.11ac will add the 80 MHz channel size (wider channels increase speed), the 256-QAM modulation (and therefore 2 new MCS per stream), and will support 5GHz band only.

Here are the physical bit rates achievable with 1, 2 and 3 streams:

Maximum bit rate (Mbps)

Channel width	20 MHz	40 MHz	80 MHz
1 stream			
MCS 0	7.2	15	32.5
MCS 1	14.4	30	65
MCS 2	21.7	45	97.5
MCS 3	28.9	60	130
MCS 4	43.3	90	195
MCS 5	57.8	120	260
MCS 6	65	135	292.5
MCS 7	72.2	150	325
MCS 8	86.7	180	390
MCS 9	n/a	200	433.3
2 streams			
MCS 0	14.4	30	65
MCS 1	28.9	60	130
MCS 2	43.3	90	195
MCS 3	57.8	120	260
MCS 4	86.7	180	390
MCS 5	115.6	240	520
MCS 6	130.3	270	585
MCS 7	144.4	300	650
MCS 8	173.3	360	780
MCS 9	n/a	400	866.7
3 streams			
MCS 0	21.7	45	97.5
MCS 1	43.3	90	195
MCS 2	65	135	292.5
MCS 3	86.7	180	390
MCS 4	130	270	585
MCS 5	173.3	360	780
MCS 6	195	405	n/a
MCS 7	216.7	450	975
MCS 8	260	540	1170
MCS 9	288.9	600	1300

V.2.3 Radio channels and national regulation rules

A wireless network uses specific channels on the 2.4 GHz or 5 GHz radio spectrum to handle communication between stations. Some channels in your area may suffer from interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.

Region/country

Every country controls and limits available radio frequencies. The broadly named 802.11 2.4 GHz and 5 GHz bands are further limited to allow sharing with other radio devices (radars, weather devices). You must set the country where you will operate the product; then, the channels proposed in the menus will be limited to the ones available in the selected country.

In the “AP” role, the product will insert the country rules in its beacons as required by the 802.11d protocol. In the “client” role, the product uses the country rules provided by the AP using the 802.11d protocol.

For further details about radio regulation areas, refer to chapters [802.11 regulatory domain rules](#), and [Appendix – 802.11 Radio channels](#)

Automatic channel selection

In Access Point mode, the product can select the best channel among a list, or among all channels available in the country. At startup (note that this occurs only once), the AP chooses the best channel depending on the measured noise and occupancy of each possible channel. This noise analysis postpones the end of the product startup for around 0.5 second per analyzed channel.

Roles other than AP do not recognize this option. For repeater, mesh and ad-hoc roles you must set one channel only. For the client role, all available channels are scanned except when proactive roaming mode is selected.

V.2.4 Wireless security

There are many technologies available to counteract wireless network intrusion, but currently no method is absolutely secure. The best strategy may be to combine a number of security measures.

Possible steps towards securing a wireless network include:

1. All wireless LAN devices need to be secured
2. All users of the wireless network need to be trained in wireless network security
3. All wireless networks need to be actively monitored for weaknesses and breaches

Available wireless security protections are:

- Not broadcasting the SSID (access point only feature)

- WEP encryption

- WPA or WPA2 – PSK (“Pre-Shared Key”)

- WPA or WPA2 – Enterprise, also known as 802.1x or RADIUS.

WEP encryption vs. WPA and WPA2 encryption

The encryption depends on the wireless topology. In ad-hoc mode, only WEP encryption is available, because WPA requires a point-to-point link in order to establish the cryptographic keys. In infrastructure mode, there is a point-to-point link between each station and its associated Access Point, and you can use WEP or WPA/WPA2.

V.2.4.1 *WEP encryption*

WEP is a method of encrypting data for wireless communication and is intended to provide the same level of privacy as a wired network. However, due to progress in crypto science, **WEP is not considered secure anymore, and cannot be used altogether with 802.11N/AC modes.** To gain access to a WEP network you must know the key. The key is a string of characters that you create. When using WEP you will need to determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption.

Keys are defined by entering a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format.

ASCII format is provided so that you can enter a string that is easier to remember. The ASCII string is converted into HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

V.2.4.2 *WEP authentication*

Two methods of authentication can be used with WEP: *Open System authentication* and *Shared Key authentication*.

In *Open System authentication*, the WLAN client need not provide its credentials to the Access Point during authentication. Thus, any client, regardless of its WEP keys, can authenticate itself with the Access Point and then attempt to associate. In effect, no authentication (in the true sense of the term) occurs. After the authentication and association, WEP can be used for encrypting the data frames. At this point, the client needs to have the right keys.

In *Shared Key authentication*, WEP is used for authentication. A four-way challenge-response handshake is used:

1. The client station sends an authentication request to the Access Point.
2. The Access Point sends back a clear-text challenge.
3. The client has to encrypt the challenge text using the configured WEP key and send it back in another authentication request.
4. The Access Point decrypts the information and compares it with the clear-text it had sent. Depending on the result of this comparison, the Access Point sends back a positive or negative response. After the authentication and association, WEP can be used for encrypting the data frames.

At first glance, it might seem as though Shared Key authentication is more secure than Open System authentication, since the latter offers no real authentication. However, it is quite the reverse. It is possible to derive the static WEP key by capturing the four handshake frames in Shared Key authentication. Hence, it is advisable to use Open System authentication for WEP authentication, rather than Shared Key authentication. (Note that both authentication mechanisms are weak).

V.2.4.3 **WPA/WPA2 encryption**

WPA greatly increases the level of over-the-air data protection and access control on existing and future Wi-Fi networks. It addresses all known weaknesses of Wired Equivalent Privacy (WEP), the original native security mechanism in the 802.11 standard.

WPA not only provides strong data encryption to correct the weaknesses of WEP, it adds user authentication that was largely missing in WEP. WPA is designed to secure all versions of 802.11 devices, including 802.11b, 802.11a, and 802.11g, multi-band and multi-mode.

WPA is the older standard (which, due to progress in crypto science, **is not considered secure anymore**); select this option if the Access Point only supports the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard.

The cipher type is the encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block-based encryption.

You can choose from 2 security options:

WPA Mode	Cipher Type	Security solution
WPA	RC4	RC4-TKIP
WPA2	AES	AES-CCMP

V.2.4.4 **Pre-shared key mode (PSK)**

In Pre-Shared Key mode (PSK, also known as personal mode), each Access Point client must provide a password to access the network. The password may be from 8 to 63 printable

ASCII characters. Most operating systems allow the password to be stored to avoid re-typing. The password must also remain stored in the Wi-Fi access point.

All Wi-Fi devices on your Wi-Fi cell must have the same Pre-Shared Key.

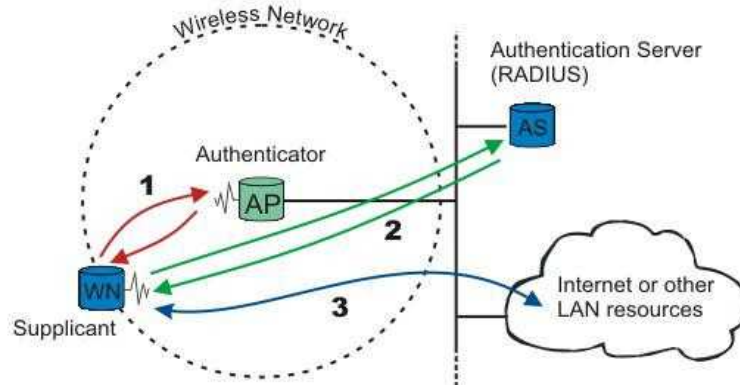
V.2.4.5 Enterprise mode (802.1x, RADIUS)

WPA/WPA2-Enterprise, or 802.1x, provides authentication to devices trying to attach to a private network through a boundary Access Point, establishing the access point as the gateway to LAN resources, or preventing access from that device if authentication fails.

NOTE: since in a chain of repeaters the farthest ones would depend on the nearest ones to access the 802.1X server, this security is not available in repeater mode. WPA/WPA2-PSK can still be used.

The authentication process is organized around several agents:

- User, also called supplicant or Wireless Node (WN),
- Wireless access point or authenticator,
- Authentication server, most often a RADIUS (Remote Authentication Dial-In User Service) server,
- Authentication modus operandi.



When a wireless node (WN) requests access to a LAN resource, the first step is the physical association between the client and the access point, defining a so-called “access port” (number 1 on the diagram).

The access point (AP) asks for the WN's identity. Then it establishes a point-to-point EAP tunnel between the WN and the authentication server (number 2 on the diagram). *No other traffic other than EAP is allowed until the WN is authenticated (the “port” is closed).* Until authenticated the client cannot access the LAN.

Once the authentication server informs the authenticator that the WN is authenticated, the traffic to the LAN is allowed (number 3 on the diagram): the “port” is open. Otherwise the “port” stays closed.

Note: 802.1x also offers a system to exchange keys which will be used to encrypt communications and to check integrity.

Authentication modus operandi

802.1x uses one of the EAP (Extensible Authentication Protocol) methods. The most commonly used ones are:

- EAP-PEAP
- EAP-TLS
- EAP-TTLS

The EAP method used is transparent to the access point. On another hand the access point clients, like bridges, must be aware of the authentication method. The choice of method must take into account the capabilities of the server/supplicant couple as well as the level of security needed.

For example, a Windows XP SP2 supplicant allows:

- PEAP authentication with login and password (called MSCHAP V2)
- Use of certificates.

Preauthentication

A client is said to preauthenticate when it is authenticating with a new AP through the currently associated AP. This aims to speed up the association time when the client decides to roam to the preauthenticated AP, because it will remove the important overhead of the 802.1x protocol.

Preauthentication must be enabled in the AP to allow the client to use it. The Client role in these products always uses preauthentication when offered by the AP.

Pre-authentication makes the client store communication keys before it needs it. The client can keep many keys in advance, allowing roaming from one AP to another to another... and back to the first, without re-executing the 802.1 x protocol.

In the client, the keys are kept in a cache table whose lifetime is configurable.

V.2.4.6 *Protected management frame (802.11w)*

This feature protects your device from a hacker DoS (Deny of Service) attack.

By default, the management frames are not protected. Anyone can send a DEAUTH frame to a client or to the AP.

In this situation, a hacker can gather AP information using a Wi-Fi sniffer and then send to a legacy client a DEAUTH frame with the AP mac address. The client receives this frame, and then closes the connection with the AP.

The 802.11w adds a field in the frame to authenticate the frame sender.

If the Wi-Fi equipment receives a management frame from an incorrect sender, it will discard the frame.

V.2.4.7 Mesh Secure Authentication of Equals (SAE)

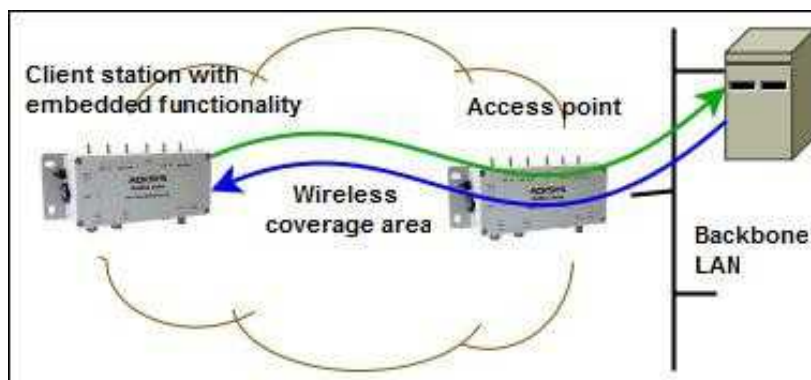
In 802.11s mesh mode, no mesh node has a special identification role, all nodes are considered equal in privileges. When SAE is used, all nodes must have a preset common key. Each time a node comes in reach of another node in the same mesh, it will verify that the peer node knows the key. The encryption uses the WPA2 protocols suite (AES/CCMP).

The password key can be from 8 to 63 printable ASCII characters. The same password must remain stored in all the mesh nodes.

V.2.5 Wired to wireless bridging in infrastructure mode

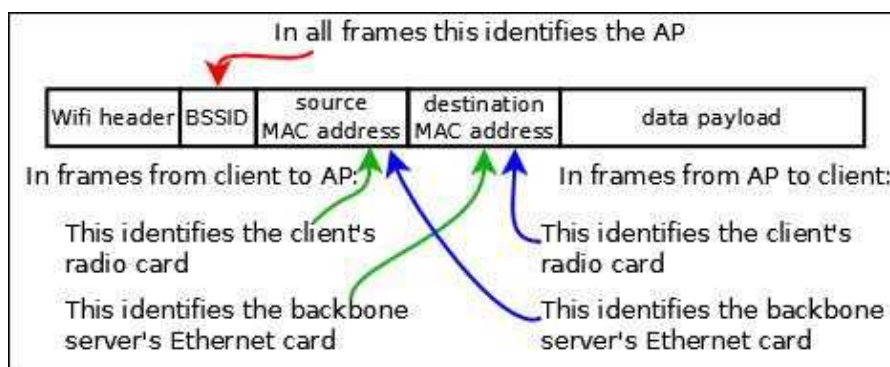
V.2.5.1 The problem

As outlined in section [V.2.1.1](#), in the 802.11 standard **an infrastructure client is supposed to be a single unit with a single MAC address**. The AP forwards data to/from the client, from/to other clients or wired devices. In this respect the AP is similar to an Ethernet switch.



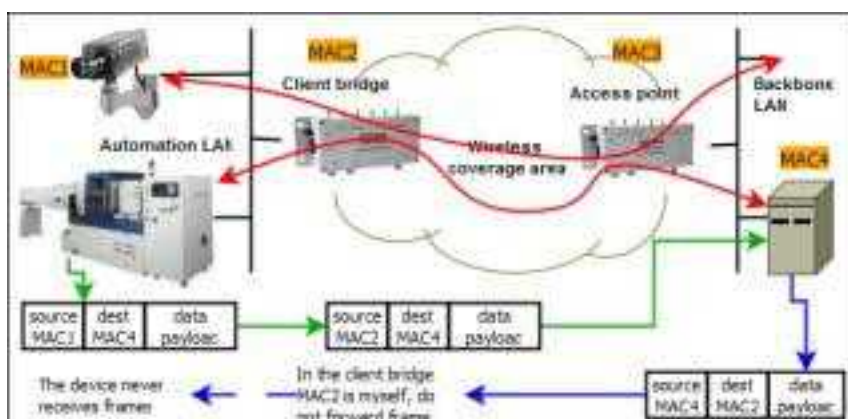
Bridging several devices with a single wireless client

To allow the AP to forward data, each frame includes a source MAC and a destination MAC.



Standard infrastructure data frames (3 addresses)

When using a client station to bridge a wired network to an AP, the situation is different. What appears to the AP as a single device with a single MAC address (that of the radio card), is hiding several wired devices, each of them having its own MAC address. Since they do not participate in the association process to the AP, they did not authenticate, hence the AP will not accept frames containing their MAC address as a source. If the client changes the source MAC address to its own, other problems appear, see picture below.



Sample problem bridging several devices with a single wireless client

V.2.5.2 The solutions

There are four ways to overcome this limitation and allow bridging the devices behind the client station:

- Routing. Let the wired LAN on the client side be an IP subnetwork, and let the client be a router or a NAT. This is a very clean solution but needs to manage the subnetwork. Strictly spoken, this is routing (layer 3 networking), not bridging (layer 2 networking).
- Masquerading. Let the client change the wired devices MAC address to its own and back, an approach also known as "Level 2.5 NAT" or
- "ARPNAT". This is the default operation in the "**client (infrastructure)**" mode. It is described in more details in section [Masquerading \(ARPNAT\)](#) below.
- Cloning. Let the client use the MAC address of the wired device. This is limited to one wired device.
- Using the "**client (infrastructure)**" and "**4 addresses format**" bridging mode, involving a more sophisticated frame format. The 802.11 standard provides a "4-addresses" frame format to solve this kind of issues but it does not fully specify it; hence this mode is not always compatible between clients and APs from different vendors. The ACKSYS products, as well as several Linux-based clients and APs, support this mode described in section b below.

Note that the mesh mode (not an infrastructure mode) also allows bridging.

a Masquerading (ARP NAT)

In this solution to the bridging problem, the client bridge keeps a table to convert devices MAC addresses to and from their IP addresses.

In frames sent to the AP, the bridge replaces the devices source MAC address with its own and remembers the MAC/IP correspondence of the frame.

When a frame comes back from the AP its destination MAC address is the one of the bridge. The bridge finds the IP address in the frame, finds out the corresponding device MAC address, pokes it in the destination MAC of the frame, and sends it to the wired LAN side.

This solution is compatible with any third-party AP since all processing is done on the client side. However, there are special behaviors to keep in mind:

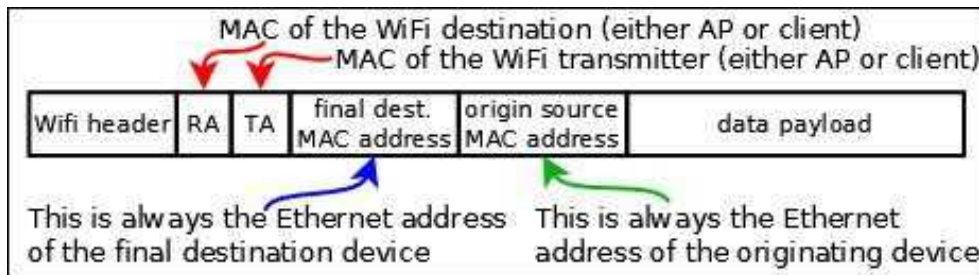
1. The conversion table handles MAC/IP conversions only. This means that **only the TCP/IP protocols suite** (TCP, UDP, IP, ICMP, ARP, DHCP and so on) can be bridged.
2. The conversion table is updated only by frames from the LAN to the Wi-Fi. This is usually not a problem because prior to any data transfer, a broadcast ARP request/reply exchange must take place. But if the client bridge is powered down, when it comes up again, the ARP exchange is not necessarily restarted by the devices on the backbone side. Then, when the bridge receives a data frame from the AP, its conversion table is empty and the frame is not forwarded. In this case, the bridge itself initiates an ARP for the destination IP address mentioned in the frame, triggering from the LAN device a response that will update the table, so that the next frame can be forwarded.
3. Equipment on **the backbone cannot use an IP gateway (a router or a NAT) located on the client LAN side, except if the product is the gateway and if the destination subnet is directly routable by the product.** The reason is that the destination IP address in the frames received from the AP are not the one of the gateway, but the address of an equipment farther beyond the gateway; but the MAC address needed is that of the gateway. So, the address conversion is not possible.
4. DHCP is a protocol used to set up IP addresses. The wired device MAC address is conveyed not only in the DHCP frame header, but also in the data payload. The address conversion causes an address mismatch at the DHCP server. To satisfy the DHCP server requirements, the bridge advertises itself as a DHCP relay agent, resolving the mismatch. For this to work, **a DHCP server located on the AP side must be able to send unicast IP packets to the bridge.** This means that the bridge must have an IP address reachable from the DHCP server prior to serving IP addresses to the devices behind the bridge.
5. ARP is a protocol used to discover MAC addresses. The ARP frames contain MAC addresses both in their headers and in their data. Special processing is done in the bridge to convert these frames. CISCO and others can set up a "proxy ARP server" in their APs. This means that the AP itself converts IP to MAC addresses on behalf of the

backbone equipment. The proxy ARP server can get confused because all devices on the bridged LAN appear to have the same MAC address (the one of the bridge radio card) but different IP addresses. The solution is to **disable the proxy ARP server on the AP side**. In the CISCO product this is called “passive client mode”.

6. More generally, applications or protocols running on the backbone side and relying on MAC addresses to identify devices, will encounter problems in this mode. Fortunately, such software is hardly used.

b Infrastructure client using 4 addresses format (WDS)

When the client is in 4 addresses format bridging mode, it uses a special frame header where both Wi-Fi and LAN MAC addresses are indicated. This is called the “4-addresses frame format”. By conveying both the client MAC and the wired device MAC in the wireless frame, the client can correctly route Wi-Fi frames to its LAN while the AP can know that it sends to an authenticated client.



4-addresses frame format

In this solution to the bridging problem, the client bridge and the AP encapsulate both data and Ethernet MAC addresses in the Wi-fi frame, adding both the AP and the client Wi-Fi MAC addresses. So, the frame can reach its Wi-Fi destination, which removes the Wi-Fi addresses and retrieves the original frame unchanged. The same process takes place both ways.

This solution is independent of the layer 3 IP addresses:

1. This mode can bridge protocols other than TCP/IP.
2. It transfers DHCP and ARP frames unchanged, avoiding most verification issues on the AP side, like proxy ARP or DHCP servers.
3. It allows using an IP gateway either on the AP side or on the bridge side, accessible from either side.

But since this solution relies on unspecified 802.11 features, it should be used only between products of the same brand or range, or when you know that the AP and client use compatible software.

Please note that 4-addresses frame format is not compatible with the roaming feature.

Final note: The 4-addresses frame format is sometimes called WDS (wireless distribution system). This acronym designates a frame format that can be used in a variety of ways. It does NOT designate a specific Wi-Fi architecture (like infrastructure or mesh).

Configuration

The access point role (AP) always supports both standard ARP NAT and 4-addresses clients simultaneously. The client bridges can be set up either in ARP NAT or 4-addresses format.

c Cloning

The ARPNAT solution loses the MAC address information from the wired devices when bridging frames to the wireless interface. Most devices do not care about MAC address substitution because they use the IP protocol in Layer 3 and ARPNAT takes care of IP addresses.

But some devices do not use IP in layer 3 (PROFINET equipment, LAN video camera...) and the MAC address is the unique ID identifying the equipment correctly.

With the cloning feature, the product can use the MAC address of a wired equipment as the source MAC address on the wireless interface. The cloned address is used for all wireless transactions: association, authentication and data exchange. The original MAC address of the radio card is ignored.



To set up the wireless MAC address, the product clones the source MAC address from the first incoming frame after a reboot or the configured MAC address. So, there should be **only one** device connected to the LAN of the product.

If you mix the non-IP device with other IP devices, you must ensure that the non-IP device will send the first frame after the product is turned on, to be sure the product will clone the correct MAC address. To avoid this problem with a PROFINET equipment you should use the "PROFINET cloning", in which case the first PROFINET frame source MAC address will be used for cloning.

V.2.6 **Fast roaming features**

In order to keep network connectivity when a client product is installed in a quickly moving vehicle, you can adjust some configuration parameters. Please note that the fast roaming feature is not compatible with 4-addresses format, and therefore not compatible with STP/RSTP.

V.2.6.1 ***Mono-channel vs. multichannel roaming***

The client role can either look for APs on one channel only, or it can scan several channels. Each way has its pro's and con's.

Mono-channel

All the APs compete for the air media, so that the available bandwidth is reduced for all clients and APs. But the client is informed of the APs presence and condition at all times, and can communicate with its current AP at all times. Also, if one of the APs is near a source of interference on the selected channel, all APs must be switched to another channel.

Multi-channel

You can arrange for APs which are in radio range of each other to use different channels. In this way they will not compete for air bandwidth. You should not choose channels

which are too close to each other, since they might interfere. The client must scan each chosen channel in its turn. For this it must go “off-channel” for a small time, leaving the channel of its currently associated AP; during this time, it cannot exchange data. The data is then buffered under certain limits. This reduces data throughput for the client.

Configuration

After activating the proactive roaming feature, you must adjust the list of channels scanned by the client. You can select one or several channels.

If proactive roaming is not activated, all channels allowed in the country are scanned; this maximizes the chance of finding a matching AP, but slows down data transfers.

V.2.6.2 *Proactive roaming vs. reactive roaming*

Reactive

Reactive roaming takes place when the client can no more communicate with its AP. When too many failures take place, the client disconnects from its current AP and begins to search a new one. Reactive roaming is the default mode, because there is nothing to configure in this case. In this mode, channel scanning; also called “foreground scan”, does never take place during data transfers, leaving all the bandwidth available for data transfers. But the roaming process is slow (it must wait for the end of the scan) and data cannot be transmitted during this time. Whenever a client cannot associate to any AP, it enters reactive roaming.

Proactive

Proactive roaming means that the client will search, select and switch to another AP before signal level is so low that a lot of errors can happen. By selecting appropriate parameters, the change from one AP to another will take place before data throughput is affected, and the re-association process will be quick if the new AP is in sufficient radio range. Hence few data (if any) will be lost.

To enable proactive roaming the client must search for APs while it is already associated and potentially exchanging data. This process is called “background scan” and somewhat reduces data throughput.

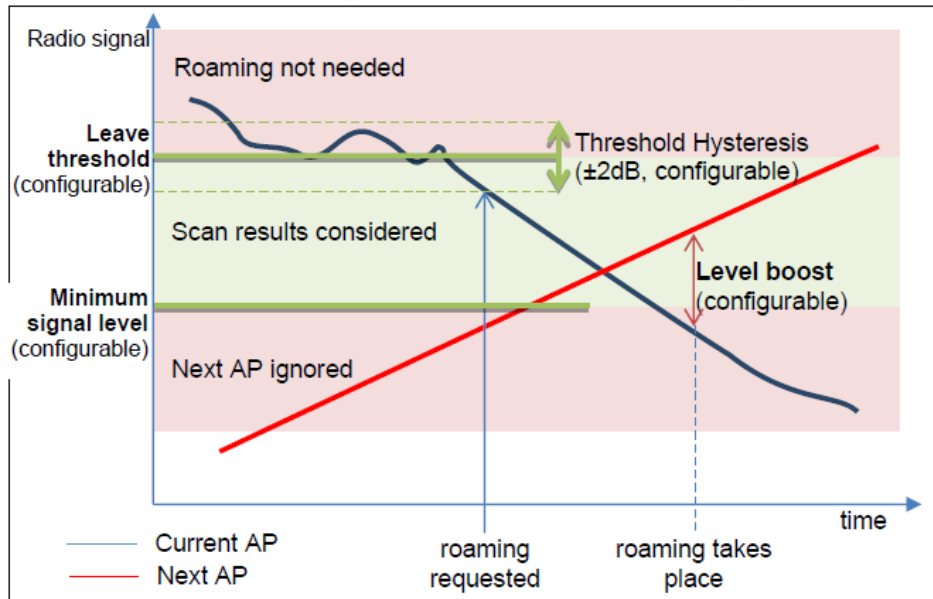
Configuration

You must configure the radio signal level threshold at which you consider that the link quality is insufficient for your throughput requirements.

But radio signal reception level is not a stable measurement; it varies under many unforeseen parameters (moving objects, humidity...). When the AP signal is near the threshold, it can go back and forth around the limit. You do not want to switch from AP to AP too often, since this means you cannot transfer data during these re-association periods. To account for this, crossing the limit is subject to a hysteresis called “required level boost” (default: 6 dB).

Finally, even when the threshold is crossed, you do not want to reassociate with a worse AP, but you do not want to lose the current bad AP either. The “required level boost” configuration parameter specifies how much better you want the new AP to be in order to begin re-association.

The effects of the various parameters are shown in this picture.



NOTE: the threshold hysteresis is configurable in versions 2.2.7 and later. The “leave threshold” is called “minimum level” in earlier firmwares.

V.2.6.3 *What happens when the current AP fails*

Contrary to wired LANs, the Wi-Fi medium is not limited in width, in sources of interferences or in obstacles. Hence the currently associated AP may abruptly disappear from the client’s “sight” due to moving objects in the field, climatic changes, AP power down and so on.

The client has four ways to know its AP is available:

- Checking that beacons from the AP are regularly received,
- Receiving data,
- Receiving acknowledges for data sent,
- Receiving responses to probes sent.

If the failure is short-lived, data is retransmitted, and a few missing beacons is allowed. Conversely, long-lived absence of beacons or data acks triggers a disconnection. If another AP previously detected is still around, the client will switch to it; else the client will enter reactive roaming. To properly distinguish short-lived from long-lived failures, this process is reacting more slowly than proactive roaming, depending on your configuration.

Configuration

On the client side you can configure the number of missing beacons that will trigger the roaming process. The delay will depend on the beacon frequency that was configured in the AP. Please bear in mind that losing a frame or two is very common in Wi-Fi, and the missing beacons count should not be set below 3.

On the AP side you can set the beacon interval. The smaller the interval, the faster failures are detected; but beacons are transmitted at the lowest allowed bit rate, and consume more bandwidth than data frames.

V.2.6.4 Scanning

Scanning is the process used by the client station to find the APs around, in order to associate with one of them. Scanning takes place periodically. During each period, the client will successively switch to configured scan channels, send a broadcast “probe request” frame and wait for responses.

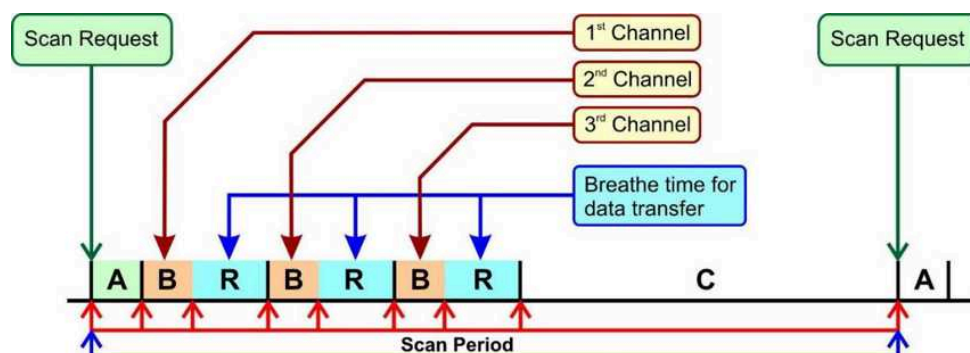
The probe request contains the SSID among other data. Any AP capable of serving this SSID will answer. The signal quality at which the response is received is used to select the best AP.

When the scanned channel is not the one of the current AP, the client is said “off-channel” and it cannot transmit nor receive data during this time; the data is buffered meanwhile. To inform the AP that it cannot receive, the client sends a “power save mode” indication to the AP before going off-channel, so that the AP can buffer frames in the meanwhile. Configuring too many scan channels will result in loss of throughput and/or loss of data. To allow sufficient time for buffered data to flow out, you can configure the delay between two scan periods.

Configuration

The two scan parameters are the list of scan channels and the delay between scans. Warning! This delay is not the scan period, but increases the scan period, as shown in the following diagram, showing the background scan (C parameter).

NOTE: when the client is not associated to any AP (after a client restart, or if the current AP suddenly disappears), there is no data to exchange, hence the breath time “R” in the diagram is shortened to 0, resulting in a slightly faster scan cycle.



A: Initialization = a few ms

B: Channel scan = 56ms

C: Padding = configurable by steps of 4 ms

R: Breathe time = 200ms

(C is the "Delay between two successive scan cycles" in the web interface)

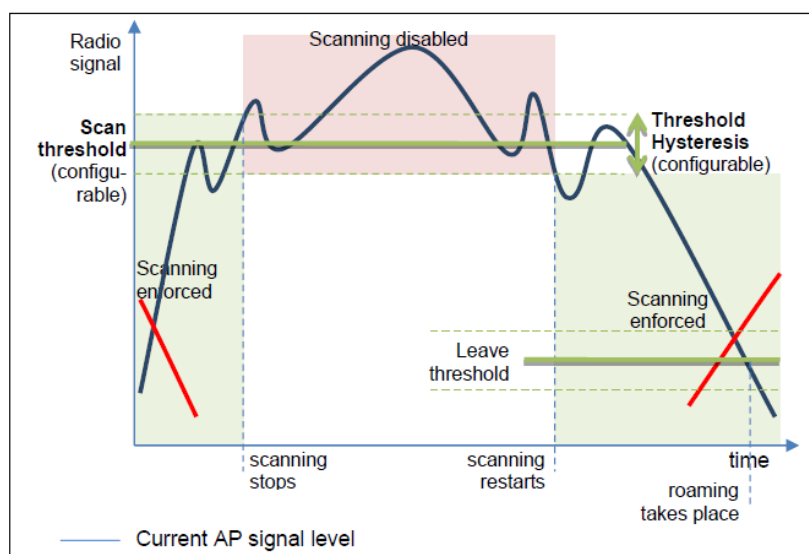
The 'R' delay is removed in reactive (foreground) scan cycles, thus shortening them while the client is not connected to an AP.

NOTE: the 'B' delay is configurable in versions 2.4.3 and later. See next section.

Scanning itself normally takes place unconditionally. To gain extra throughput when the signal level is good, you can configure a "scan threshold". This parameter sets the signal level above which you estimate that no roaming is ever necessary. Setting the "scan threshold" to zero disables this feature (default).

When set, the scan threshold is compared to the power received from the current AP. When the power is greater than the threshold, the scan process is stopped at the next scan period. When the power received is lower than the threshold, the scan process is restarted.

To avoid oscillation effects due to a received power rapidly changing around the threshold, a hysteresis is implemented. Its value is the same as the hysteresis used for the "leave threshold".



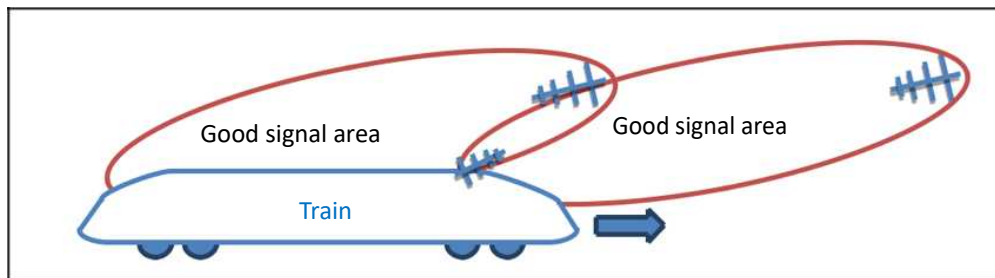
NOTE: the scan threshold is configurable in versions 2.2.7 and later.

V.2.6.5 Advanced Roaming settings

In several situations the basic roaming settings are not sufficient. This includes directional antennas handling, fine tuning of the mean signal decay rate and fine tuning of the bandwidth used for scanning.

a Directional AP handling

If the Wi-Fi client is, say, embedded on a train, and a directional antenna is fixed on the roof (see picture), a high signal level means that the AP will soon be on the other (bad) side of the directional antenna soon, hence it is a good time to roam to another AP farther ahead, with a lower reception level.



Train soon losing current AP despite good signal

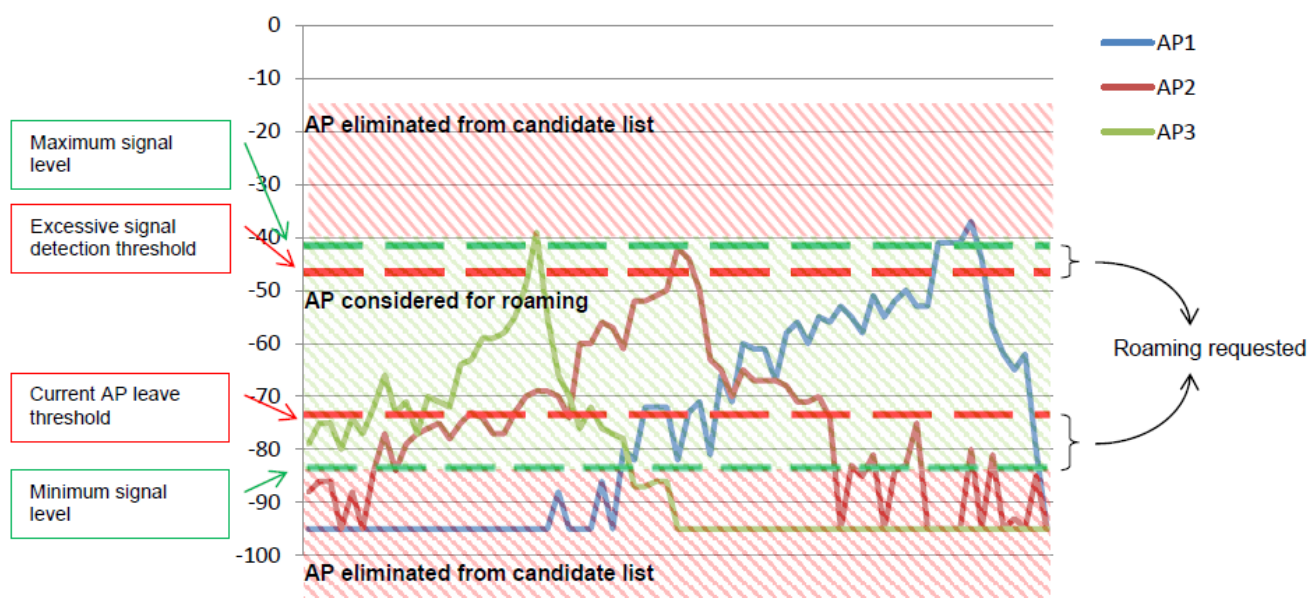
In this case when the AP is seen with a high signal level it is likely that the client will lose the association in the next few seconds.

The **Excessive signal detection threshold** parameter drives the decision of dynamically leaving the current AP when its level becomes too high. The **Maximum signal level** parameter drives the static elimination of APs with high signal level as candidates for the next association; the check is performed after each scan.

Good stability places some constraints on these parameters:

- When both parameters are used, you must set the threshold level lower (less powerful) than the max level.
- These parameters are incompatible with the **Current AP scan threshold**, which is another way of managing high signal level Aps.
- The **excessive** threshold also uses the **Threshold hysteresis** parameter
- The max level is not checked during the first scan after association, to avoid leaving an AP which just became current.

Configuration



At the end of scan process, the product chooses a candidate AP. The candidate AP is the AP where you will roam if the roaming is requested.

Roaming won't occur before the **Minimum roaming interval** has elapsed since the last association. In areas where several APs are received with about the same signal quality, this parameter helps avoid frequent roaming due to slight signal variations.

Roaming won't occur to an AP that was left recently before the **No-return delay** has elapsed. This parameter helps enforce roaming to a sequential succession of APs, even if signal bounces make a previous AP appear temporarily as more desirable.

b Smoothing factor (RSSI decay rate)

Various parameters are meant to trigger events:

- scan threshold
- leave threshold
- excessive signal detection threshold.

For the purpose of threshold crossing detection, all these parameters are compared to the RSSI of the current AP.

The RSSI of the current AP is defined as an exponential moving average computed over the most recent beacons received from the current AP. So, the comparison is done, not against the current signal level, but against an average. Note that only the beacons signal levels are used, since they are transmitted at a stable bit rate and power level and they are received with homogenous receiver sensitivity.

In order to favor more or less the recent beacons against the older ones in the computed RSSI average, you can set the exponential factor of the moving average. This factor is called the “RSSI smoothing factor”. It represents the percentage attached to the most recent beacon in the computation.

The smoothing factor is a value between 0 and 1 in steps of $1/16^{\text{th}}$. For example, a value of $3/16$ means that the signal power levels of the previous beacons are used like this:

- for the most recent beacon, $\frac{3}{16} = 18.75\%$ of the signal value,
- for the penultimate beacon, $\frac{3}{16} \times \frac{13}{16} = 15\%$
- for the penultimate beacon, $\frac{3}{16} \times \frac{13}{16} \times \frac{13}{16} = 12\%$
- and so on.

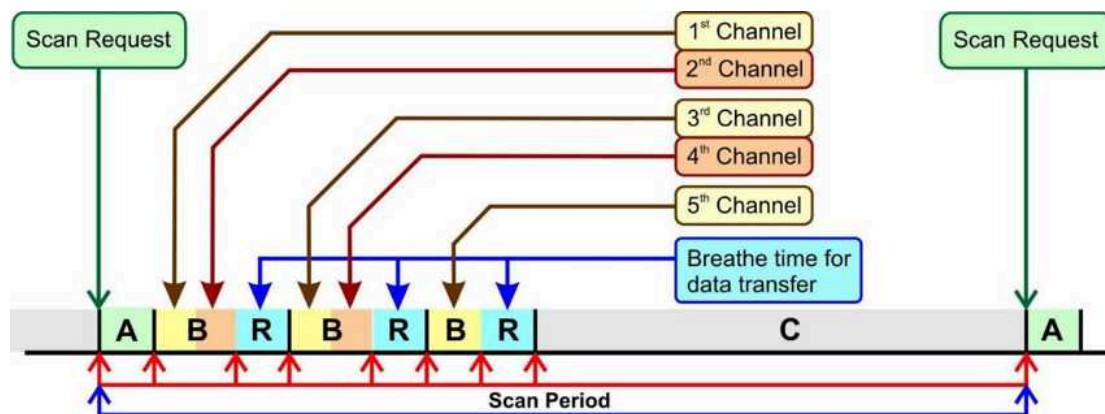
Configuration

In the browser interface the factors are expressed as the percentage attached to the last beacon. As an extreme case, using 100% (or $16/16^{\text{th}}$) means that only the most recent beacon is used in the comparisons.

c Off-channel configuration

You can shorten the duration of the off-channel probe request/response sequences (the ‘B’ parameter in the “scan period” picture). This solves the situation where a large data flow is entering the AP which cannot forward it to the client because it is scanning another channel, and the AP has insufficient buffers. The ‘B’ delay is the sum of (B1) a switching delay (very quick), (B2) a synchronization delay (ensuring that our probe will not collide with another transmitter on the channel), (B3) probe request transmission (at the lowest rate available), (B4) response waiting delay.

Also, the scanner can switch from channel to channel, without returning to the current channel. In the next picture, 5 channels must be scanned. During one scan sequence 'B', the delays (B2)-(B3)-(B4) are repeated without returning to the data channel, until either the parameter "Maximum time off-channel" or the current AP beacon interval is exhausted. This behavior saves some of the switching delays (B1) and improves mean throughput at the expense of the instant throughput.



Configuration

You can configure items (B2) with the "Offchannel adaptation delay" and (B4) with "Per channel probe response delay", and you can define the overall off-channel duration of one 'B' scan sequence with the "Maximum time off-channel" parameter. All these parameters are defined ± 4 ms.

Default values

The default parameters allow probing 2 channels per scan sequence, as displayed in the picture. The default "maximum time off-channel" is 125 ms, but since most AP have a beacon period of 100 ms, this parameter is usually automatically reduced to 100 ms. The two other default parameters are set to 30 ms, but are actually rounded down to 28 ms.

If the channel list includes DFS channels, the delay indicated in "Maximum time off-channel" must take into account the minimum value of "Per channel probe response delay" in the DFS case.

For example, if we scan channel 36 (not DFS) and 52 (DFS):

The "Maximum time off-channel" must be at least "Offchannel adaptation delay" + 108. Note that when we leave this parameter empty, it displays 125 in the background but it is automatically adjusted to: 125 + "Offchannel adaptation delay"

With "Offchannel adaptation delay" = 30 (rounded to 28); "Per channel probe response delay" = 30 (rounded to 28); "Maximum time off-channel" = 150, the scan cycle is: channel 36 (approx 56 ms) then return to the operating channel (200 ms) then channel 52 (approx 138 ms) then "Delay between two successive scan cycles" and we start again.

We see that the maximum delay of 150ms is never used to the maximum, the maximum interruption of service is 138 ms.

Setting a value a little greater than 138 makes it possible to absorb the peaks of CPU usage of the router. For example if, at the same time, it does multicast routing, encrypted VPN, etc. In fact, in this example, up to $138 + 56 + (56-4) = 246$ ms, the scan cycle will be identical.

To scan the 2 channels consecutively, you can set "Offchannel adaptation delay" = 30 (rounded to 28); "Per channel probe response delay" = 30 (rounded to 28); "Maximum time off-channel" = 200 (i.e. $138 + 56 + 6$ ms of margin), the scan cycle will then be: channel 36 (approx 56 ms) then directly channel 52 (approx 138 ms) then "Delay between two successive scan cycles" and we start again.

V.2.6.6 Authentication speed up

In the association task, the AP and the client must exchange several frames. The number of frames increases with the security level.

In the WPA protocol, the PMK (Pairwise Master Key) is used to generate the temporally keys which will be used to encrypt the data.

- WPA/WPA2-PSK: The PMK is derived from the Pre-Shared Key.
- WPA/WPA2-EAP: The PMK is distributed by the radius server.

The table below gives the number of frames vs the security level

Security policy	Number of frame
Open (without security)	4 frames - 4 Authentication frames
WEP	4 frames - 4 Authentication frames
WPA/WPA2-PSK	8 frames - 4 Authentication frames - 4 Key exchange frames
WPA/WPA2-EAP (with radius server)	> 8 frames - 4 Authentication frames - Several radius authentication frames - 4 key exchange frames

The "4 Authentication frames" are mandatory by the 802.11 protocol.

The "4 Key exchange frames" are necessary to exchange the temporally key.

The “several radius authentication frames” are necessary to authenticate the Wi-Fi client with the radius server. The numbers of frame are depending of the authentication method.

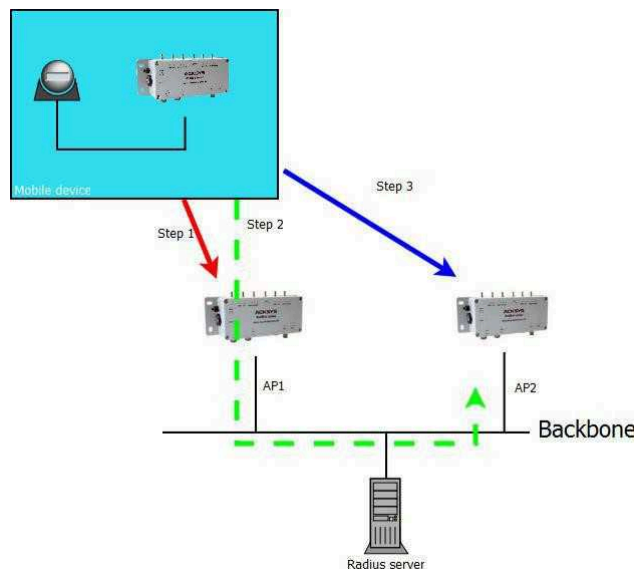
a Pre-authentication / PMK caching

With this feature, the authentication with WPA/WPA2-EAP policy is reduced to 8 frames (as in PSK mode).

The AP beacons convey its pre-authentication / PMK caching capabilities. A client can choose between them the capabilities it supports and use them.

The products support both features and automatically use them if the roaming is enabled.

The picture below shows the 3 steps of the pre-authentication process:



Step 1: The Wi-Fi client associates with AP1 for the first time. In this step the client does a full authentication. The radius server sends the PMK to both AP1 and the Wi-Fi client. AP1 and the Wi-Fi client store the PMK in their local cache.

At the end of this step, the Wi-Fi client is connected to AP1

Step 2: The Wi-Fi client discovers AP2 by scan process. It uses the secured link with AP1 to process a pre-authentication with AP2. During this step, the radius server sends the PMK to AP2 and the Wi-Fi client. They both store the PMK in their local cache.

At the end of this step, the Wi-Fi client is still connected with AP1.

Step 3: The Wi-Fi client roams to AP2. Both AP2 and the Wi-Fi client check if the PMK in their local cache is correct.

If the PMK is correct, AP2 starts the WPA handshake with the Wi-Fi client.

If the PMK is not correct, the AP starts a radius authentication.

At the end of this step, the Wi-Fi client is connected with AP2.

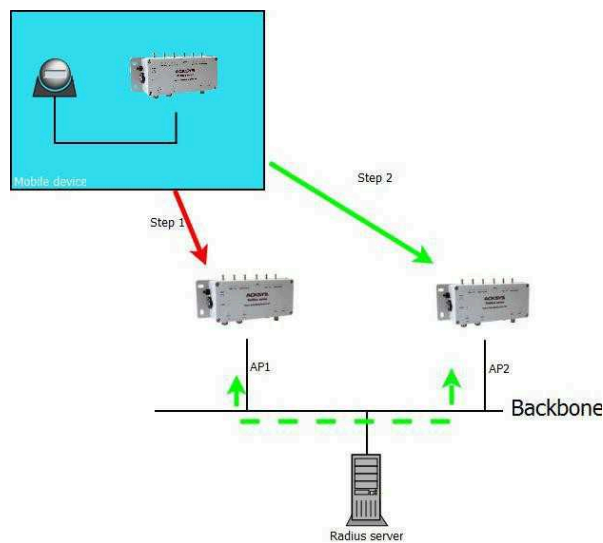
b Fast Transition Support (802.11r)

With this feature, the authentication with all WPA/WPA2 policies is reduced to 4 frames (as in open mode).

With the 802.11r, the temporal key is distributed through the back bone between the different APs.

The products support the 802.11r only in client mode.

The picture below shows the steps of an 802.11r authentication:



Step 1: The Wi-Fi client does a full authentication with AP1. AP1 stores the PMK and temporally keys. This full authentication process produces data that will be stored by the Wi-Fi client for the next step.

Step 2: The Wi-Fi client roams on AP2 and uses data stored in the previous step in its authentication request. With these data, AP2 knows that this Wi-Fi client is successfully authenticated with AP1. AP2 directly requests the temporally keys from AP1 (using the back bone). If AP1 gives all the needed keys to AP2, the Wi-Fi client is allowed to finish the association process with AP2. In the other case, the Wi-Fi client starts a full authentication with AP2.

V.2.6.7 **Connect before break**

As we have seen previously, the roaming process, even when it relies on the use of two radio cards, always implies that the Wi-Fi client physically disconnects from the current AP before being able to reconnect to the next AP. This means that there is necessarily a time, even a very short one, during which the client is completely disconnected from the network, and the mechanisms put in place to stop packets transmission this period can't fully guarantee the absence of packet loss.

To meet the needs of certain applications for which packet loss during handover is critical, Acksys has developed a particular roaming mode, called "Connect Before Break", which makes it possible to drastically reduce the packet loss rate, and this even with very data throughput.

The operating principle of Connect Before Break is based on the use of a 'ghost' WiFi client, which is actually a clone of the effective client, operating in parallel with the latter by connecting to the same Access Point, but which, instead of ensuring data exchange, will be responsible for carrying out the function of detecting the surrounding Access Points (scanning). We therefore have at any times two perfectly identical clients, one that we will call the **active client**, which provides traffic with the AP, and the other, called **passive client**, which analyzes the environment in search of compatible Access Points.

When the signal level of the current AP drops below the roaming threshold, as soon as the **passive client** has detected a new AP meeting the roaming criteria, it will leave the current AP and initiate the connection process to this new one. During this time, the **active client** remains connected to the current AP and can continue to exchange data packets. It will only disconnect from the current AP when the **passive client** has established the connection with the new AP, after advertising the handover request to the entire network, via ARP exchanges, and after checking that the buffers of the current AP and the **active client** are empty.

When the **active client** has been disconnected, the two clients will swap their roles: the **passive client** becomes the **active client** and vice versa.



Please note that, unless your product is configured as a NAT router, Connect Before Break requires the use of the [4 addresses format \(WDS\)](#). This implies that the access points to which he can connect can only be WaveOS Acksys products

Also note that Connect Before Break can operate on a single radio card, but in this case, **you can only use one channel**.

For the implementation of Connect before Break, we strongly recommend that you consult the application note [APNUS0016 Connect Before Break](#)

V.3 High availability features

V.3.1 Router redundancy with VRRP

In networks such as a transportation system (train, tramway...) which uses Wi-Fi links to communicate with the ground, redundant routing allows setting up a double route, main and secondary, and to detect failures of the main route in order to activate the secondary one. During normal operation of the main route, the secondary route can also be used to transfer data of lesser importance or to implement static load balancing.

When a product is used in IP router mode, you can set up a secondary product to serve as a backup router. This feature uses the VRRP protocol to decide on which product is routing traffic at any given time. The “master” (or “primary”)

router is normally used, and the “slave” (or “backup”, or “secondary”) router is used when the master fails.

In the devices around, only one gateway address is set. Depending on availability, this gateway IP address will address either the master or the slave router. Together they form a cluster called “virtual router”.

You can also set up two virtual routers, corresponding to two gateway addresses A and B, and designate one router as master for A and backup for B, and conversely set the other router as master for B and backup for A, thus providing high-availability load-sharing.

Detected failures include Ethernet cable wrenching, Ethernet coupler burnout, Wireless card failure, remote access point failure (in client mode), and of course, power failure of the master. Network breakages between two remote nodes (e.g. two remote switches indirectly connected to the products) are not detected: hence the rest of the network must be redundant as well.

Any detected failure makes the backup router:

- Take over the existing connections
- Advertise the remote devices around that the MAC address of the IP gateway has changed.

When the default is fixed in the master, it resumes, taking back the routing from the backup router.

Three services cooperate to support failover: VRRP detects failures and switches the addressing; connection tracking synchronizes TCP connections between the primary and backup routers; the event manager reports failures.

V.3.1.1 VRRP

The VRRP service handles hardware failures detection and route switching. It implements RFC3768 with slight changes. The VRRP protocol is straightforward: a VRRP master multicasts periodic advertisement frames which inhibit the VRRP backup(s). When the backup ceases to receive the advertisement, it uses gratuitous ARP to inform the network of the new location for the gateway IP address. Then, as the new “master”, it sends “advertisement” frames periodically.

When the master recovers, it negotiates with the backup through the advertisement frames and the real master takes back the routing function.

So, in the master router, the VRRP service detects hardware failures, in the slave, it also monitors the master’s health.

Note that the backup can detect the presence of the master, but the master cannot detect the presence of an inactive backup. This is very important because, if the network hardware is only half-functioning (for example the

Ethernet link of the master can receive frames but not send them), the system could end up with two active routers at the same address (the master sees no default, and the backup becomes active since it receives no advertisements from the master). The solution to this is instance grouping.

The duration between failure and take-over by the backup depends on many parameters:

- Time to detect the failure (1 to 2 seconds for an Ethernet linkdown, depend on roaming parameters for Wi-Fi failure)
- Advertisement interval. The backup waits up to 4 times the interval before taking over
- Time to reload the connections in the backup (a few ms)
- Time to broadcast the “gratuitous ARP” frame to the network so that switches and hosts know the new MAC address associated to the gateway IP address
- Traffic load. A high network traffic may slow down noticeably the take-over.

VRRP instances

A VRRP instance is the entity that manages one gateway IP address in one router. It is bound to one subnet.

By this definition, a VRRP instance has the following properties:

- ID a virtual address identification number, common to the master and the backup. The ID associated to an IP must be unique on the subnet (in case you have several distinct gateways using VRRP)



- Virtual IP address The address managed by the instance. It must be different from any other IP address assigned to the device, either static or DHCP-provided
- Netmask Routing information for the virtual IP address
- Network interface The physical (Ethernet...) or logical (bridge...) subnet to which the virtual IP address is bound

Several other properties are inherited from the group the instance belongs to: the priority (in backup state), the master advertisement period (in master state) and the initial state.

A network interface can be bound to several IP addresses. Typically, one is static and is used for management purposes (to configure and monitor the router) and the other is the virtual gateway address, used by hosts to route packets to other subnets.

VRRP Groups

An IP router interconnects several subnets (LANs). A failure on one subnet must be reported to the other subnets as well, so that remote hosts on all attached subnets stop using the router. To achieve this, the VRRP service manages groups of interdependent subnets. When one subnet fails in the group, it acts as if all subnets had failed and stops advertising on all grouped subnets.

In order to ease configuration, some instances properties are defined at the group level.

- Name a gateway identification string, can differ from the same group name used in the backup (but using different names is discouraged since it leads to human errors).
- Initial state The state of all instances at service start, this speeds up the initial state stabilization. Normally the master is initially master and the backup is initially backup, but this is not mandatory.
- Advertisement period This VRRP parameter is given to the VRRP instances in the group
- VRRP instances list The instances which are part of the group.
- Connection tracking If the router is NAT/PAT, VRRP should synchronize connections when the backup becomes active. The connection tracking service should be enabled and configured separately.

The group properties must be identical in the master and in the backup, except maybe for the initial state.

RFC changes

Three enhancements are added to RFC3768:

- Timers are in centiseconds instead of seconds; this feature is taken from VRRP V3 (RFC5798).
- A new “fault” state allows tracking of partial hardware failures. The genuine VRRP protocol only handles complete router shutdowns.
- The master and backup routers have different MAC addresses, i.e. virtual MAC addresses are not supported. Hence, devices using the virtual router must handle the ARP protocol, which is the vast majority, if not all, of IP network devices.

V.3.1.2 *Connection tracking*

The “connection tracking” service is rather a “connection tracking and replication” service. When the router is in NAT/PAT mode, the connection tracking service synchronizes connection knowledge between the master and the slave. The connection information is sent from the master to the slaves as soon as possible (the order of magnitude is tens of milliseconds but the actual figure depends on the product and network load); there is a slight possibility that a connection which was open just before failure, is not transmitted to the backup router. The user’s application software should be prepared to this and should retry the connection.

A dedicated network link can, and should, be used to transfer connection data: for example, the secondary Ethernet available on some products.

The service is awakened each time a TCP connection is set or torn down, or when an UDP flow is stabilized. Depending on the user’s application there can be a lot of such events. They are grouped together and sent (replicated) in an UDP multicast packet to the backup system that replicates the connection list. The grouping avoids overflowing the network when many connections are present, but induces some delay in the replication.

V.3.1.3 *Failures reporting*

When the routers change state, an internal event is generated, and you can set the event to generate various actions with the generic “alarms/events” service. You can trigger an action when any given instance or group enter or leaves any given state. When you associate events and actions, you must remember that SNMP actions need a working subnet to propagate.

V.3.1.4 *Miscellaneous questions*

a Access points configuration

The access points must allow clients to use several IP addresses and to change them from time to time. ***This requirement rules out some forms of proxy ARP.***

b Throughput

In load sharing, you must consider the possibility of a failure, where, after takeover, all the data will be routed by one router only. In such a configuration it is therefore advisable to restrain the throughput to half the acceptable throughput.

Note that reducing the timeouts make the system faster to react, but reduces the useful throughput, because of the additional load placed upon the CPU and the network.

c Wi-Fi bandwidth occupation

VRRP and Connection tracking rely on MULTICAST frames. You must consider how this affects air bandwidth:

1. All VRRP frames are transmitted 3 times on the air. In the Master (Wi-Fi client)→ AP direction, they are transmitted twice: once in UNICAST to the AP which rebroadcasts them (at low bitrate) to the other potential clients of this AP;
2. in the AP→ Backup (Wi-Fi client) direction they are broadcast once at low bitrate.
3. Multicast / broadcast frames from an AP are transmitted at the lowest modulation rate available (1 Mbps in the 2,4 GHz band, or 6 Mbps in the 5 GHz band). You can speed up multicasts by disabling the lowest bitrates (see documentation).
4. As noticed earlier, it is not advisable to use Wi-Fi for connection tracking and replication. The bandwidth is one more reason to avoid this.

The shorter the VRRP period, the more the bandwidth is occupied, the less it is available for useful data exchange.

d Influence of Wi-Fi handover (roaming) on VRRP takeover delay

In the “client” Wi-Fi function, when the roaming mode is enabled, two kinds of short interruptions of the transmission will occur. The duration of these interruptions must be taken into account when configuring the VRRP “Advertisement periods”, so that no unwanted takeover will take place due, not to a breakdown, but merely to roaming latency.

1. Interruptions due to multichannel scan

They are periodic and systematic. They are configurable within some limits, using three parameters in the “advanced roaming” tab:

Maximum time off-channel, Maximum time off-channel, Per channel probe response delay. With a standard AP and the default parameters, the interruption will not exceed 65 ms.

2. Interruptions due to handover from one AP to another

The interruption duration in this case depends on a large number of factors, such as the kind of security parameters, AP capacity and AP swiftness. Depending on various factors, the duration can vary from 14 ms (no security, fast AP) to more than 300 ms (WPA, RADIUS dialog, certificates control, slow AP...)

The handover process inhibits the detection of Wi-Fi disconnections by the VRRP service: when another AP is available for fast roaming, disconnection detection is disabled, in the assumption that a reconnection to the other AP will quickly follow. If the quick reconnection fails, a timer expires and makes VRRP handle the disconnection. The timer, which represents the maximum time between the loss of the current AP and VRRP failover decision, is computed as follows:

- If the scan cycle period is greater than 2 seconds, Timer =
(scan interval parameter) + 2s.
- Else, on the assumption the timer is
Timer = 2 × (scan interval parameter)

e Influence of the priority field on VRRP takeover delay

VRRP is designed to handle more than one backup. The “priority” field adjusts the priority between the potentially many backups. The timers which detect a failure of the master depend on this priority field. The higher the priority, the faster the takeover; but for reliability reasons in the priority negotiation, you are advised to use large intervals between values assigned to each device of the VRRP instance (i.e., between the master and the backup). The waiting time for the “advertisement” frames from the master is computed as:

$$\text{Timeout (in ms)} = ((256 - \text{priority}) / 256) \times 1000 + 3 \times \text{AdvertisementPeriod}$$

For example, if the initial role of the product is “backup” and Advertisement period = 100 ms, the default timeout will be

$$(256 - 200) / 256 \times 1000 + 3 \times 100 = 519 \text{ ms } (\pm 4 \text{ ms})$$

f Takeover caused by a Ethernet link loss

Due to limitations in the software and hardware components used, detection of an Ethernet link loss may take up to 2 seconds. Obviously in this case the takeover cannot take place before that delay.

g Packets are not routed from wireless to wired interfaces! What is wrong?

The advanced settings/bridging mode setting was left to ARP NAT mode. As explained in section [V.2.6.2a](#), only a non-bridged wireless interface can route incoming data. The

“network” holding the wireless interface must be set to non-bridging, or the client bridging mode must be 4-addresses.

h **SNMP**

SNMP OIDs are not yet defined for VRRP configuration. Therefore, it is not possible to configure VRRP using SNMP.

However, SNMP traps are defined and can be configured and sent.

V.3.2 **Link layer redundancy with RSTP**

WaveOS features the STP and RSTP protocols. As link layer protocols they are handled by the bridge component. See section [V.1.8.3 Spanning Tree Protocols \(STP, RSTP\)](#)

V.4 **SNMP agent and ACKSYS MIB**

The SNMP protocol defines the dialogue between a management station and a SNMP agent. An SNMP agent runs on each managed system and reports information via SNMP to the managing systems.

With SNMP you can:

- ❖ Get the device state
- ❖ Change the product configuration
- ❖ Manage events

V.4.1 **SNMP security**

V.4.1.1 **SNMP V1 and V2c**

Under SNMP V1 and V2c, the security relies on an IP-based access control, mapped to a **Community String**. Authentication of clients is performed with the **community string**, in effect a type of password, which is transmitted in clear text.

The SNMP V1/V2c Communities can be configured in the SNMP AGENT submenu. Please see: [SNMP Agent](#)

V.4.1.2 **SNMP V3**

The SNMP v3 protocol provides more sophisticated security mechanisms than SNMP v1 and SNMP v2c. SNMP v3 implements a user-based security model (**USM**) that authenticates and encrypts the requests sent between agents and their managers, and provides user-based access control.

SNMP V3 splits the security into 2 pieces, the authentication / encryption and the authorization.

a The User based Security Model (USM):

USM provides authentication and privacy (encryption) functions and operates at the message level.

In USM, the administrator can create a list of users:

- Each user has a name (called a **Security Name**), an authentication type (**NONE, MD5 or SHA**) and a privacy protocol (**NONE, DES or AES**) for data encryption.

WAVEOS supports AES128 as AES encryption.

For more details on **USM**, please see “RFC 3415”.

The SNMP V3 users can be configured in SNMP AGENT submenu.

Please see: [SNMP Agent](#)

b The View based Access Control Model (VACM):

VACM determines whether a given user is allowed to access a particular MIB object to perform specific functions and operates at the PDU level.

In VACM, the administrator can:

- Assign for each user (or SNMPv1/v2c communities) a **security model**:

- ❖ **V1** community based security model
- ❖ **V2c** community based security model
- ❖ **USM**

and will then attribute for each pair of “**Security Model, Security Name**” a **Group Name**.

- Define “**Views**” containing a set of MIB objects, where MIB sub trees can be included or excluded.
- Set the **Access Policy** for each **Group**: **Read/write** permissions for a given **View**:
 - ❖ Each tuple “**Group Name, Context Name, Security Model, Security Level**” can be assigned a **Read/Write** permission for a given **View**.
 - ❖ **Security Level** can be:
 - No authentication.
 - Authentication and no privacy (data encryption).
 - Authentication and privacy (data encryption).



For security model V1 and V2c, security level must be “No authentication”.

The Context Name used by WAVEOS inside the agent is always the default context name, which is an **empty string** (For more details on SNMP context please see RFC 5343).

For more details on **VACM**, please see “RFC 3415”.

The users’ access rights can be configured in SNMP AGENT submenu.

Please see: [SNMP Agent](#)

V.4.2 Access methods

Requests to SNMP agent can use SNMP V1, V2c or V3, depending on which SNMP security rules have been configured on **WAVEOS**

For SNMP V1 and V2C, the “public” community is configured per default as read/write, and you can manage communities via the Web interface.

Recommended tools

- ❖ Net-SNMP, available at <http://www.net-snmp.org/>
- ❖ Ireasoning™ MIB browser, available at <http://ireasoning.com/mibbrowser.shtml> (requires JAVA)

V.4.3 Using the Acksys MIB

Obtaining the MIB

The Acksys MIB is included in the *firmware update package* available in the download section of www.acksys.com. The ACKSYS MIB file is self-documented. To read the OIDs documentation please use a text file editor or MIB browser.

Relevant OIDs

The Acksys MIB covers a large range of devices. Hence all OIDs are not relevant to WaveOS. Every OID description contains a firmware tag identifying the firmware which is relevant to this OID. Firmware type and minimum version required are included in the tag, like “[WaveOS Firmware Version 2.8.0.1]”.

All the OIDs described below are relative to the Acksys MIB root:

- ❖ .1.3.6.1.4.1.28097
- ❖ iso.org.dod.internet.private.enterprises.acksys

The following OIDs are meaningful for WaveOS. Please refer to the MIB to find out numeric OID values and specific description for each item.

acksysProductID	a code identifying product model.
acksysProductSerialNumber	unique identifier assigned to a product.
network-product.administration	core administration functions: adminReset, adminSave, adminApply, adminResetFactory
c-key-management	management functions to erase, save/ restore configuration from/to the C-Key, turn off the C-KEY status led permanently and ignore C-KEY settings. This part also provides a test utility reserved for Acksys production.
networkStatus	current (running) network states, please see section V.4.4
networkConfiguration	next-to-be-applied network parameters of the

serviceStatus	product, see section V.4.5 current (running) state of services.
servicesConfiguration	next-to-be-applied services configuration of the product, see section V.4.6

Changing the configuration

When items in `networkConfiguration` OR `servicesConfiguration` are changed, changes are not saved to permanent memory. Reading the `adminSave` OID let you know if there are any pending (unsaved) changes: `saveNotRequired` means no unsaved changes; `saveRequired` means pending changes exists, you can save them to permanent memory by writing '1' to `adminSave`.

On another hand, setting `adminResetFactory` to '1' clears any previous configuration, either saved or not, and reboots the product, thus resetting it to factory settings. The firmware version is kept unchanged, however.

Applying the configuration

To apply the current saved changes, you can either set `adminApply` to 'enable' (this will not reboot the product), or set `adminReset` to '1' (which reboots the product). **Warning:** applying a network configuration change may not get an answer from the agent, since the product networking subsystem is stopped and restarted. If the new modified network is not reachable by the SNMP client, you cannot get an answer from the agent. This is not considered an error.

V.4.4 Understanding network status tables

Current network states of the product are summarized in the tables described below:

- `statusIfWlanTable`: lists running wireless interface states, like BSSID, channel, security information, connection state, signal level, etc. `statusIfWlanChannel` OID displays the current channel used by the wireless interface. Channel "-1" indicates that the process of channel selection is in progress. It's the same with 0 (in MHz) as frequency in the `statusIfWlanFrequency` OID.
By default, the `statusIfWlanPreSharedKey` OID is under protection of SNMP V3, only `admin_acksys_group` can see its result. And, of course, you can modify this configuration in the SNMP AGENT submenu. Please see: [SNMP Agent](#)
- `statusPhyWifiTable`: displays the current state of the radio card, like radio card label, enable/disable state, cluster mode, etc.
- `statusPhyWifiScanTable`: Acksys MIB provides wireless scan service by writing '1' to the `statusPhyWifiScanTableStart` OID. After starting a scan, you can read the `statusPhyWifiScanUpdateTbl` OID to know if current scan is finished: `inprogress` means the scan isn't finished yet; `available` means the scan is stopped, and then you can see the result in the `statusPhyWifiScanTable`.

The *statusPhyWifiScanTable* summarizes all available wireless devices in range, on all wireless channels, like access points, mesh points or ad-hoc stations. In this table you can find some useful information like SSID, BSSID, signal level, frequency (in MHz), security, etc. The *statusPhyWifiScanSignal* OID displays the signal level in dBm taken from probe and beacon frames only, which are sent at the lowest available rate. In general, the signal level found for these frames is better than the one from data frames.

- *statusSpanningTreeTable*: it displays current states of the STP/RSTP bridges, if there are bridges with STP/RSTP enabled in the product.
- *statusSpanningTreePortTable*:
This table includes the *statusSpanningTreeTable* and extra information about spanning tree port.

V.4.5 Managing network configuration tables

Network configuration management contains 3 parts which represent 3 layers of OSI model: IP layer (tcpip), Data Link layer (netif) and Physical layer (netphy). You can find out relevant OIDs at each layer.

Note that there is no “repeater” table since this feature is a combination of an AP and a STA (client) with common parameters.

To insert a row in one of the relevant tables, you must set to ‘createAndGo’ the ‘rowStatus’ item indexed by the index to be created. To remove a row, you must set to ‘destroy’ the ‘rowStatus’ item indexed by the index to be deleted.

CAVEATS:

- It is not recommended to make configuration changes simultaneously with SNMP and the web interface. Changes may take several seconds to propagate from one of these two services to the other.
- SNMP agent does not recognize repeaters created with the web interface. A workaround is shown in the examples below.
- WEB interface does not support wpa-mixed (mixed WPA/WPA2) except mixed WPA/WPA2 PSK for AP. It also doesn’t support WPA cipher modes tkip, aes or tkip+aes. Be aware that if you configure one of these modes via SNMP, the WEB interface will display “No encryption”.
- The default WPA cipher of AP is AES for WPA2-PSK and WPA2-EAP modes, and TKIP+AES for WPA-PSK and WPA-EAP modes. In the case of client, default cipher is AES for WPA/WPA2-EAP-TLS modes, and TKIP+AES for the other modes. You can also configure other WPA cipher but be aware of WEB interface.

V.4.5.1 *OIDs relevant to IP layer*

The OIDs that concern IP layer are about IP settings, routing and firewall management. In the OID tables described below, user can insert or delete rows using the SNMPV2c procedure.

- configIpSubnetTable: lists configurable network interfaces with an IP setting. By default, a network interface can specify only one interface among wireless interface, Ethernet interface, virtual interface, or L2 tunnel GRE interface by using *configIpSubnetInterface*. In order to add multi interfaces in a network, you have to set the network as bridge by writing '2' to the *configIpSubnetBridgeEnable* OID, and then add interfaces by managing *configInterfaceTable* (see *configInterfaceDepends* in [section V.4.5.2](#)).
- configIpZonesTable: general settings of user defined network zones. In this table, you can also enable NAT/PAT (IP Masquerading) then go to *configIpNatIpForwardTable* for further configuration.
- configIpNatIpForwardTable: allows to redirect the input traffic on one zone to a device on private zone when the *configIpZoneNAT* is enabled.
- configIpFirewallTable: used to manage integrated firewall rules on specified zone. The firewall can drop, reject or forward the input traffic from one chosen zone to another device or zone.
- configIpRoutesTable: list of static routes. The static routes indicate over which interface and gateway certain host or network can be reached.
- configIpZoneForwardTable: list of inter-zone forwarding rules. It allows to set the forwarding policies between one zone and other zones. This table is used only for the zone which disables IP Masquerading.
- configIpDscpTaggingTable: list of DSCP tagging rules applied on each incoming frame. The incoming frames matching all the rules in this table will be tagged on DSCP tag. Only routed frames forwarded from one IP network to another can be tagged.

Acksys MIB provides also management of DOS protection: enabled par default

- synfloodprotection: enable/disable SYN-flood protection
- dropinvalidpacket: drop/accept invalid frames or frames without active connection

V.4.5.2 *OIDs relevant to Data Link layer*

Configuration details about wireless interface, virtual interface and bridge are relevant to Data Link layer. In the following described OID tables except *configInterfaceTable*, user can insert or delete rows using the SNMPV2c procedure.

- configFilterGroupTable: allows to manage layer 2 bridge filter group, see *configFilterGroupRuleTable* for more filter rule details.
- configFilterGroupRuleTable: lists filter rules of all filter groups. Each filter group may contain one or several filter rules. The frames which match at least one rule will be dropped.
- configInterfaceTable: All logical interfaces are listed in this table. The rows are fixed by agent, depend on the following tables. User cannot insert or delete rows. You can

manage the network relationship between these interfaces by using *configInterfaceDepends* OID. The network relationship is a dependency between one bridge interface and one or several non-bridge interfaces. In *configInterfaceDepends* OID, you can specify a bridge under one or several non-bridge type interface interfaces like wireless interface, Ethernet interface, L2 tunnel GRE interface or VLAN interface. If you don't respect this rule, the SNMP agent will reject your configuration by sending an error message.

And also, you can configure the filter group in each interface by setting *configInterfaceFilterGroupIndex* and *configInterfaceFilterGroupDir* OIDs.

All the interfaces listed in *configInterfaceTable* come from the following tables. You can find further configurations there.

- *configIfMeshTable*: List of configurable Mesh points. Mesh point supports only SAE as security mode for now.
- *configIfBridgeTable*: List of MAC bridge networks. You can configure STP/RSTP for your bridges with STP/RSTP activated.
- *configIfVlanTable*: List of configurable VLAN interfaces.
- *configIfStaTable*: List of infrastructure clients. In this table you can find the general configurations of client, advanced configurations of security and roaming.
Each security mode has exclusive configurations. When you define a security mode, you must not forget to set these configurations and you must ignore the configurations of other security modes. Here is a summary about specified security configurations:

SECURITY	SPECIFIED CONFIGURATION	DESCRIPTION
WEP	configIfStaWepKey1 - 4	WEP KEY #1- #4 defined in HEX (characters 0-9, A-F) or ASCII format string.
	configIfStaWepKey	Indicates which one of the 4 WEP keys is currently selected
WPA(2)-PSK	configIfStaKey	Pre-Shared Key with a length from 8 to 63 characters. If its length is 64 characters it will be used directly as hexadecimal format
	configIfStaFastBSSTransitionActivated	Fast transition support (802.11r)
WPA(2)-EAP	configIfStaKey	Password In TLS mode: password associated to the chosen Private Key
	configIfStaEapType	EAP method: TLS, PEAP, LEAP
	configIfStaFastBSSTransitionActivated	Fast transition support (802.11r)
	configIfStaIdentity	Identify only for LEAP/PEAP mode
	configIfStaPrivateKey	You can upload the content of Private key file in PEM format (only in TLS mode) by SNMP-SET. The result is shown by SNMP-GET: 0 : key not set 1 : key is uploaded
	configIfStaCACert	You can upload the content of CA-Certificate file in PEM format (only in TLS mode) by SNMP-SET. The result is shown by SNMP-GET: 0 : key not set 1 : key is uploaded
	configIfStaUserCert	You can upload the content of uploaded User-Certificate file in PEM format (only in TLS mode) by SNMP-SET. The result is shown by SNMP-GET: 0 : key not set 1 : key is uploaded
	configIfStaAuthentication	Authentication type for phase 2 only in PEAP mode
	configIfStaWpaKeyCacheLifeTime	how long the conversation keys are retained in case the client roams back to an already authenticated AP. (in second)

The following OIDs cover configurations exclusive to roaming mode, they can help you configure the roaming client further. Ignore them if the client doesn't enable roaming.

OID NAME	DESCRIPTION
configIfStaRoamingEnable	Client roaming mode activation <i>[All OIDs below are taken into account when this OID is set to '2']</i>
configIfStaRoamingEnableDBM	If the RSSI of the current AP falls below this value (in dBm), the client will try leaving the current AP and roaming to another AP.
configIfStaRoamingRequiredBoost	Roaming occurs only if the potential AP signal is above the current AP's plus this value (in dBm).
configIfStaRoamingScanPeriod	Delay between two successive scan cycle (in millisecond)
configIfStaRoamingRssiSmoothingFactor	The RSSI of the current AP is computed over the last few beacons received. Select the importance of the last beacon relative to older ones: the RSSI smoothing factor is a value between 1 and 16 that indicates the step of 1/16 (e.g. 3/16, 5/16, 16/16) <i>In WEB interface it is in percentage format: 6%(1), 13%(2), 19%(3), 25%(4), 31%(5), 38%(6), 44%(7), 50%(8), 56%(9), 63%(10), 69%(11), 75%(12), 81%(13), 88%(14), 94%(15), 100%(16)</i> <i><u>Default:19%(3)</u></i>
configIfStaRoamingBeaconTimeout	Beacon interval unit
configIfStaRoamingCurrentApScanThreshold	When the current AP signal is above this level (in dBm), the client ceases to scan. Set to 0 to scan unconditionally. <i>Incompatible with <code>configIfStaRoamingMaxSignalLevel</code>.</i>
configIfStaRoamingMinimumStaLevel	The AP's signal is below this level (in dBm), it will not be roaming candidate, but it will still be used if there is no current AP nor better AP. '0' to disable this configuration
configIfStaRoamingAboveLevelThreshold	When the perceived signal level of the current AP passes above this limit (in dBm), the client will try to roam to another AP. '0' to disable this configuration
configIfStaRoamingMaxSignalLevel	APs which are above this level (in dBm) have less priority when choosing the next AP to roam to.
configIfStaRoamingMinRoamDelay	Roaming won't occur before this delay (in ms) has elapsed since the last association.
configIfStaRoamingNoReturnDelay	Roaming won't occur to an AP that was left recently. (in ms, max 180000 ms)
configIfStaRoamingThresholdHysteresis	This value (in dBm) will be added and subtracted to each threshold to set the corresponding threshold hysteresis interval.
configIfStaRoamingOffChanMaxDelay	Maximum delay offchannel during which data must be buffered by the associated AP (in ms)
configIfStaRoamingOffChanProbeDelay	Delay (in ms) for collision avoidance after a channel switch, before sending the probe request
configIfStaRoamingPerChanProbeDelay	Time (in ms) to wait for an answer from the AP.

- configIfAPTable: List of configurable access points. You can find all configurations about general AP settings, securities, MAC filter and frames filter in the table.

As in the *configIfStaTable*, each security has specified configurations. Focus on the configuration of the security you selected and ignore the other security configurations.

SECURITY	SPECIFIED CONFIGURATION	DESCRIPTION
WEP	configIfAPWepKey1 - 4	WEP KEY #1- #4 defined in HEX (characters 0-9, A-F) or ASCII format string.
	configIfAPWepAuthentication	WEP type: open, share
	configIfAPWepKey	currently used WEP key, a value between 1 and 4 that indicates select one of four WEP keys
WPA(2)-PSK	configIfAPKey	Pre-Shared Key with a length from 8 to 63 characters. If its length is 64 characters it will be used directly as hexadecimal format
	configIfAPPreAuthentication	802.11w security feature activation
	configIfAPWpaGroupRekey	Time interval for rekeying the GTK (broadcast/multicast encryption keys) in seconds.
	configIfAPWpaPairRekey	Time interval for rekeying the PTK (unicast encryption keys) in seconds.
	configIfAPWpaMasterRekey	Time interval for rekeying the GMK (master key used internally to generate the GTK) in seconds.
WPA(2)-EAP	configIfAPKey	Shared Secret with a length from 8 to 63 characters.
	configIfAPPreAuthentication	802.11w security feature activation
	configIfAPWpaGroupRekey	Time interval for rekeying the GTK (broadcast/multicast encryption keys) in seconds.
	configIfAPWpaPairRekey	Time interval for rekeying the PTK (unicast encryption keys) in seconds.
	configIfAPWpaMasterRekey	Time interval for rekeying the GMK (master key used internally to generate the GTK) in seconds.
	configIfAPRadiusIndex	Selected index of configRadiusTable entry

- configRadiusTable: sub-table of Radius server prepared for AP security configuration. It can cover several Radius servers. You can select one Radius server for your AP.

The selection of the Radius server for an AP is different between the web interface and the SNMP agent. If you change the Radius server in both services, the web interface will prevail. To recover the Radius configuration set by SNMP, first use the web interface to change the AP to a non-Radius mode.

- configDetailsNasId: NAS common identifier for radius servers. It is used for AP in WPA-EAP mode.

V.4.5.3 **OIDs relevant to Physical layer**

`configPhyWifiTable` gathers all the physical parameters about a radio card. User cannot insert or delete rows. Number of rows depends on radio card installed in the product.

'0' in `configPhyWifiChannel` indicates that the radio card is configured for multiple channels or automatic channel selection. Please see `configPhyWifiChannelList` for more channel details. `configPhyWifiChannelList` can contain one or several channels, separated by spaces. 'auto' or '0' in `configPhyWifiChannelList` indicates automatic channel selection.

If the radio card is configured in client roaming mode, `configPhyWifiChannel` and `configPhyWifiChannelList` are ignored, see `configIfStaScanChannels` instead.

V.4.6 **Managing service configuration tables**

Service configuration management gathers the service parameters about web server, DHCP server, DNS relay.

Web server: this part allows you to activate and configure HTTP and HTTPS servers.

DHCP: DHCP service is provided separately by network. One DHCP server independent and ready to setup is prepared for each network interface. Static leases table allows to assign always the same predefined IP address according to the client MAC address.

DNS relay: it is about activation of DNS protection attack.

V.4.7 **Using SNMP notifications (traps)**

Your product supports the SNMP V2c traps (also called notifications).

The Acksys MIB lists the available SNMP traps under the OID .1.3.6.1.4.1.28097.11 (notification).

To use a trap, you need to configure the trap settings of an event (see section "Alarms/events" in the Web interface).

The table below shows the mapping between events and traps.

Event name	Notification name	OID
LAN link	linkAlarm	.1.3.6.1.4.1.28097.11.1
Wireless link	linkAlarm	.1.3.6.1.4.1.28097.11.1
Input power	powerAlarm	.1.3.6.1.4.1.28097.11.3
Digital input	digitalInput	.1.3.6.1.4.1.28097.11.4
Temperature limit	tempExceededAlarm	.1.3.6.1.4.1.28097.11.5
Wireless client assoc.	clientLinkAlarm	.1.3.6.1.4.1.28097.11.6
VRRP state change	vrrpAlarm	.1.3.6.1.4.1.28097.11.7

Variables may be bound in the notification to provide detailed information about the event. Available variables are listed in the MIB for each affected event. You can find these variables under OID .1.3.6.1.4.1.28097.11.255 (notificationBindings).

V.4.8 Examples

These example scripts use SNMP-SET (provided in the Linux net-snmp package). They are meant to run under Linux. Use them as a guideline for other cases.

This script changes the product IP address, and applies the changes:

```
# define a shell macro for snmpset
alias CFGSET="snmpset -m ACKSYS-WLG-MIB -c public -v2c"
# configure it with a new address and netmask
CFGSET 192.168.1.253 configIpSubnetIPv4Addr.\lan\ a 10.0.1.2 CFGSET 192.168.1.253
configIpSubnetIPv4Mask.\lan\ a 255.0.0.0
# save and apply without rebooting
CFGSET 192.168.1.253 adminSave.0 i 1 CFGSET 192.168.1.253
adminApply.0 i 2
```

The following script replaces the factory-defined AP interface on radio A, by a Wi-Fi client bridged to the internal bridge, and sets a WPA-PSK key:

```
# define a shell macro for snmpset
alias CFGSET="snmpset -m ACKSYS-WLG-MIB -c public -v2c"
# delete existing AP interface
CFGSET 192.168.1.253 configIfAPRowStatus.\radio0w0\ i 6
# add a client interface
CFGSET 192.168.1.253 configIfStaRowStatus.\radio0w0\ i 4
# configure it with WPA/WPA2-PSK
CFGSET 192.168.1.253 configIfStaSsid.\radio0w0\ s myNewSsid
CFGSET 192.168.1.253 configIfStaSecurityMode.\radio0w0\ i 3
CFGSET 192.168.1.253 configIfStaWpaVersion.\radio0w0\ i 1
CFGSET 192.168.1.253 configIfStaWpaCipher.\radio0w0\ i aeskip
CFGSET 192.168.1.253 configIfStaKey.\radio0w0\ s "shared psk key"
# set bridge type to L2SNAT (therefore, not WDS)
CFGSET 192.168.1.253 configIfStaWds.\radio0w0\ i disable
# save and apply without rebooting
CFGSET 192.168.1.253 adminSave.0 i 1 CFGSET 192.168.1.253
adminApply.0 i enable
```

The following creates the equivalent of a repeater, starting with the already factory-defined AP:

```
# define a shell macro for snmpset
alias CFGSET="snmpset -m ACKSYS-WLG-MIB -c public -v2c"
# configure the existing AP interface
CFGSET 192.168.1.253 configIfStaWds.\radio0w0\ i enable
# add a client interface
CFGSET 192.168.1.253 configIfStaRowStatus.\radio0w1\ i 4
# configure it
CFGSET 192.168.1.253 configIfStaSsid.\radio0w1\ s "acksys"
CFGSET 192.168.1.253 configIfStaSecurityMode.\radio0w1\ i none
CFGSET 192.168.1.253 configIfStaWds.\radio0w1\ i enable
# set MAC address of next AP
CFGSET 192.168.1.253 configIfStaBssid.\radio0w1\ x 90a4de214f85
# save and apply without rebooting
CFGSET 192.168.1.253 adminSave.0 i 1 CFGSET 192.168.1.253
adminApply.0 i enable
```

V.5 QOS Traffic Class Management

V.5.1 Traffic Classification

Traffic classification corresponds to the categorization of a traffic by a network layer into a number of traffic classes. Each resulting traffic class can be treated differently in order to differentiate the service implied for the user.

The product will act as a network scheduler that will classify packets in a traffic stream based on the content of some portion of the packet header of a particular protocol, into separated individual flows and queues that have different priorities in term of packet egressing.

The product will manage the traffic classes defined in the standard IEEE 802.1p (for Vlan priority) at the Ethernet layer, in the DiffServ standard at the IP layer, and in WMM of IEEE 802.11e standard for IEEE 802.11 networks (WLAN).

V.5.1.1 802.1p traffic classes

The IEEE 802.1p standard defines the class of service (CoS) as a 3-bits field called the Priority Code Point (**PCP**) within an Ethernet frame header when using VLAN tagged frames as defined by the IEEE 802.1Q standard. It specifies a priority value of between 0 and 7 inclusive that can be used by QoS disciplines to differentiate traffic.

PCP	Traffic Types	Product Internal Traffic classes
0	Best Effort	Depends on Diffserv (see below)
1	Background	1
2	Spare	2
3	Excellent Effort	3
4	Controlled Load	4
5	Video	5
6	Voice	6
7	Network Control	7

The product will map the IEEE 802.1p priorities 1 → 7 to the internal traffic classes 1 → 7.

The IEEE 802.1p priority 0 will be considered as no priority set, and then the Diffserv priority will be used instead.

V.5.1.2 DiffServ traffic classes

DiffServ uses a 6-bit differentiated services code point (DSCP) in the 8-bit Differentiated services Field (DS field) in the IP header for packet classification purposes. The DS field and ECN field replace the outdated IPv4 TOS field.

The product will only use the first 3 bits of DS field which represent the Class selector of DiffServ, to map to the internal traffic classes 0 → 7.

In case that IEEE 802.1p priority > 0 is present, the Diffserv priority will not be used.

Class Selector Values		Product Internal Traffic classes
DS field	Class	
000XXXXX	CS0	0
001XXXXX	CS1	1
010XXXXX	CS2	2
011XXXXX	CS3	3
100XXXXX	CS4	4
101XXXXX	CS5	5
110XXXXX	CS6	6
111XXXXX	CS7	7

V.5.1.3 WMM Traffic Classes

WMM defines 4 Access Categories for **802.11** networks (WLAN) to handle the QoS data traffic, with 4 levels of priorities 0→3 (with 0 being the highest priority and 3 the lowest one):

WMM Access Categories	Priority
AC_BK (background)	3
AC_BE (best effort)	2
AC_VI (video)	1
AC_VO (voice)	0

WMM also specifies a mapping between the LAN's Layer 2 (802.1d) Class of Service and the WLAN's WMM access categories.

802.1p PCP	WMM Access Categories	
	WMM Access Categories	Priority
0	AC_BE (best effort)	2
1	BK (background)	3
2	BK (background)	3
3	AC_BE (best effort)	2
4	AC_VI (video)	1
5	AC_VI (video)	1
6	AC_VO (voice)	0
7	AC_VO (voice)	0

The product adds the following mapping between the LAN's Layer 3 Diffserv field and the WLAN's WMM access categories, that will be used when 802.1p priority = 0, and when there is no VLAN but there is Diffserv field.

Diffserv Class	WMM Access Categories	
	WMM Access Categories	Priority
CS0	AC_BE (best effort)	2
CS1	BK (background)	3
CS2	BK (background)	3
CS3	AC_BE (best effort)	2
CS4	AC_VI (video)	1
CS5	AC_VI (video)	1
CS6	AC_VO (voice)	0
CS7	AC_VO (voice)	0

V.5.2 Traffic Class to Queue Mapping

V.5.2.1 Queue definition

When the network scheduler wants to classify a packet that cannot egress due to traffic congestion, it puts it in a queue.

Each interface on the product has its own queues where packets are stored before egressing.

Each **queue** has its own **priority** in term of packet egressing:

Packets in a Queue with a better priority will be sent first.

V.5.2.2 Queues of Ethernet Interfaces

Ethernet Interfaces manage **8** queues in parallel, **Queue 0→7 with priorities 0→7**, with 0 the highest priority and 7 the smallest one.

V.5.2.3 *Queues of Wireless interfaces*

Wireless Interfaces manage **4** queues in parallel, **Queue 0→3 with priorities 0→3**, with 0 the highest priority and 3 the smallest one.

V.5.2.4 *Queue mapping*

The queue mapping defines the association between a traffic class and a queue priority.

The queue priority will permit to the network scheduler to know the order in which the packets are sent to the network.

**For Wireless interfaces, WMM imposes the traffic class to queue mapping.
The queue priority corresponds to the WMM access categories priorities.**

V.5.3 Queue Management

As in a same queue, we can have several traffic classes, and in a traffic class we can have several streams of different origins, we may also need to deal with the bandwidth sharing inside a same queue.

The queue management corresponds to how to deal with traffic in the same queue.

The product offers 2 types of queue management:

- **FIFO** Queue: the packets exit the queue in the same order they entered it, without worrying about bandwidth sharing.
- **FAIR** Queue: the traffic inside a queue is divided in multiple flows, and then all flows are fairly served for egress.

V.5.4 GRE Tunnels

The product manages the traffic class inheritance of the packets encapsulated by the GRE Tunnels.

If a GRE tunnel encapsulates VLAN with a VLAN priority (PCP) > 0, it will convert the encapsulated VLAN priority to a DiffServ Class for its own enclosing IP packets.

If the VLAN priority (PCP) = 0, or if the encapsulated packet is not a VLAN, it will inherit the encapsulated Diffserv field.

VI SECURITY MANAGEMENT

You should ensure that the network access to your product is secured and so avoid unauthorized access of a hacker.

To achieve this, you should configure your product to restrict access to your product to a network segment or a group of authorized users.

VI.1 HTTP/HTTPS server

You have the possibility to protect the access to the web interface with a password:

- Username: root
- Password: Per default there is no password set

You can also activate the HTTPS server so that the data exchange with the server is encrypted.

A default low security self-signed certificate is used if you do not provide one.

We strongly recommend to upload your own certificate (It must be a PEM file containing both the certificate and its unencrypted private key).

Please see [VII.1.10.8 Web Server](#) for product configuration.

VI.2 Bridge mode

In bridge mode, you can control the access to the product with the bridge vlan management:

Use a vlan for the configuration management of the product in the network segments that contain the authorized users.

Allow this vlan only on the port connected to this network segment, and on the bridge upper layer interface.

Please see [Enable the Bridging VLAN](#) for product configuration.

VI.3 Router mode

In router mode, you can control the access to the product with:

The acceptance policy for local services. You should set it to disabled for Network zones that don't contain authorized users.

Firewall to block the input traffic that is destined to your product.

Please see [VII.1.8 Routing / Firewall](#) for product configuration.

VI.4 SNMP access

Per default, there is no security activated on the SNMP agent, and every SNMP v1/v2c user can access all the public and private OIDs.

To protect the SNMP access, you have to change the SNMP access configuration, for example by limiting the “view” read/write rights to certain OIDs.

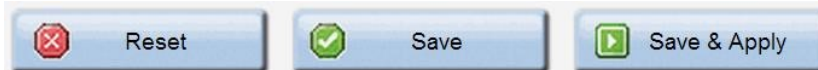
You can also create a SNMP v3 secured user.

Please see [VII.1.10.5 SNMP Agent](#) for product configuration.

VII WEB INTERFACE REFERENCE

VII.1 Setup Menu

With this menu you can configure the wireless interface(s) and the networking properties. At the bottom of most **SETUP** pages, there are two or three buttons:



After changing parameters, press **Save** to record in permanent memory the parameters changed in this page. In this case the changes will not be applied immediately, but only after a restart, or after a subsequent **Save & Apply**.

Press **Save & Apply** to record the parameters, and then apply all configuration changes made in any page up to now.

Press **Reset** (if available) to revert the data in the form to previous values (the values displayed after the last **save**)

VII.1.1 Physical interfaces

Wireless overview section:

This page lists the most significant properties of the radio cards, organized by SSID. In the bottom of the page you can change global Wi-Fi properties.

PHYSICAL INTERFACES

WiFi 1

WiFi 2

LAN 1

LAN 2

VIRTUAL INTERFACES

NETWORK

VLAN

BRIDGING

ROUTING / FIREWALL

QOS

SERVICES

SETUP

TOOLS

STATUS

WIRELESS INTERFACES OVERVIEW

You can set up to 8 simultaneous roles (wifi interface types) per radio card, among the following combinations:

Combination	Channel selection	Can use DFS	Max number of interfaces			
			Access point	Infrastructure client	Mesh point	Ad-hoc
Multiple access points	single, auto, multiple	yes	8			
Client / bridge	single, auto, multiple, roaming*	yes		1		
SRCC	single	yes	auto	auto		
Other / Ad-hoc	single	no			unsupported	unsupported

When using several roles, they all use the same shared channel, in this case, the client role must not be set to multichannel roaming.

Repeater mode is a combination of two roles: access point + client.

* The roaming feature is not yet available for IEEE802.11ac cards.

WIFI INTERFACE

WiFi 1: Wi-Fi 5 (802.11ac) Wireless interface

CHANNEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
Automatic	802.11ac+n	acksys1	Access Point (infrastructure)	none	

WIFI INTERFACE

WiFi 2: Wi-Fi 5 (802.11ac) Wireless interface

CHANNEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
Automatic	802.11ac+n	acksys2	Access Point (infrastructure)	none	Interface disabled

GLOBAL PARAMETERS

RADIO REGULATION AREA

Country: United States

RADIO CLUSTER

Cluster mode: Do not group

Save & Apply

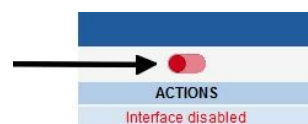
Save

The **WIFI INTERFACE** frame summarizes the main settings of each WiFi interface

WIFI INTERFACE						
802.11abgn Wireless Controller (Radio A)						
	CHANNEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
	40	802.11na	MySsid	Access Point (infrastructure)	none	  

Create a new SSID
Edit
Remove

By default (factory settings), the radio cards are disabled.
It's your responsibility to activate them with this button:



Enabling or disabling a radio card will only be applied after a **Save & apply**

Click the **Remove** button to delete this SSID. Click the **Edit** button to open the radio window and edit this SSID properties.

Global parameters section:

GLOBAL PARAMETERS	
RADIO REGULATION AREA	
Country	United States
RADIO CLUSTER	
Cluster mode	Do not group

Country:

The regulation rules of the selected country will determine the channels and transmission powers you can use. Additionally, in client role the product will use the country provided by the AP in its beacons.

Cluster mode:

You can cluster the radio cards so that one radio is used to scan multiple channels while the other connects to AP's and transfers data. In this mode, the scanning process does not disturb data transfers, but the scanner radio is reserved for this use.

When **Group for scanning** is selected, the scan for APs occurs on one radio card. The results are given to the other radio card so that it can select the best AP for roaming

purposes. This implies that the AP signal levels must be the same for both cards; hence **their antennas positions, polarities and cabling must be very close to each other**. The roaming trigger level boost should not be set too small, to account for residual differences.

In this mode, the roaming parameters are taken from the configuration of the radio card used for data transfers.

When **Group for scanning** is selected, you can choose the card that will be used for scanning with the **Scanner card** radio buttons.

RADIO CLUSTER	
Cluster mode	Group for scanning
Scanner card	☒ WiFi 1 ☐ WiFi 2

When **Group for connect before break** is selected, the behaviour of the two radio cards is quite similar to that of **Group for scanning** mode, but the functions of the two cards will be swapped, completely transparently, each time a roaming occurs. This operating mode is detailed in section [Connect before break](#).

The WiFi 1 interface is selected by default as the primary card, but since it's a temporary state, this has, in most cases, no incidence on the operation.

RADIO CLUSTER	
Cluster mode	Group for connect before break
Primary data card	☒ WiFi 1 ☐ WiFi 2
Secondary data card	☐ WiFi 1 ☒ WiFi 2

In this mode, it is possible to ask the same radio card to perform both functions, but note that in this case, you can only roam on a single radio channel.

For dual radio products, simply select the same radio card for both functions:

☒ WiFi 1 ☐ WiFi 2
☒ WiFi 1 ☐ WiFi 2

Configuration for single radio products:

RADIO CLUSTER	
Cluster mode	Group for connect before break
Primary data card	☒ WiFi
Secondary data card	☒ WiFi

Case of 802.11ac Wave 2 products:



WI-FI INTERFACE

Wi-Fi 5 (802.11ac Wave 2) Wireless interface

5GHz band Warning: Saving a change of band reboots immediately

CHANNEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
Automatic	802.11ac+n	acksys	Access Point (infrastructure)	none	 

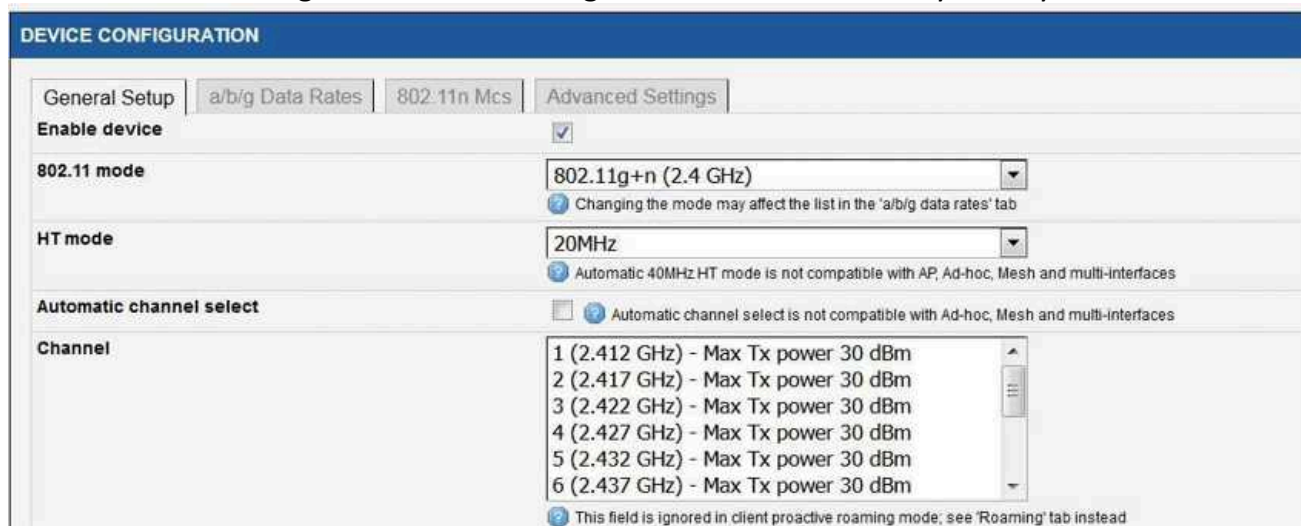
You must select the frequency band (5GHz or 2.4GHz) before proceeding with the Wireless configuration.

VII.1.2 Wireless/Radio

VII.1.2.1 SETUP/PHYSICAL INTERFACES/WIRELESS SETTINGS/DEVICE CONFIGURATION

General Setup tab:

This section gathers all the settings common to each SSID you may create on a radio card.



DEVICE CONFIGURATION

General Setup | a/b/g Data Rates | 802.11n Mcs | Advanced Settings

Enable device ☒

802.11 mode 802.11g+n (2.4 GHz)
Changing the mode may affect the list in the 'a/b/g data rates' tab

HT mode 20MHz
Automatic 40MHz HT mode is not compatible with AP, Ad-hoc, Mesh and multi-interfaces

Automatic channel select ☐ Automatic channel select is not compatible with Ad-hoc, Mesh and multi-interfaces

Channel

- 1 (2.412 GHz) - Max Tx power 30 dBm
- 2 (2.417 GHz) - Max Tx power 30 dBm
- 3 (2.422 GHz) - Max Tx power 30 dBm
- 4 (2.427 GHz) - Max Tx power 30 dBm
- 5 (2.432 GHz) - Max Tx power 30 dBm
- 6 (2.437 GHz) - Max Tx power 30 dBm

This field is ignored in client proactive roaming mode; see 'Roaming' tab instead

Enable device:

If this checkbox is checked, the radio card is enabled and is able to communicate. Uncheck it to disable the radio card.

802.11 mode:

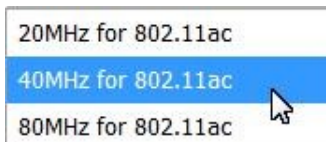
- The 802.11g+n mode operates in the 2.4GHz band (802.11g) and is compatible with 802.11g and 802.11n devices.
- The 802.11a+n mode operates in the 5GHz band (802.11a/h) and is compatible with 802.11a/h and 802.11n devices.
- The 802.11ac+n mode operates in the 5GHz band and is compatible with 802.11ac, 802.11a/h and 802.11n devices.

Note: a product configured in 802.11a+n/ac+n cannot communicate with another one configured in 802.11g+n because they are using different frequency ranges.

HT (High Throughput) mode:

In 802.11n and 802.11ac mode, you can use the default **HT20** mode, which uses a single 20MHz channel, just like the legacy 802.11a & 802.11g modes. But to increase the bandwidth, you have the possibility to aggregate two or four consecutive 20MHz channels, to work respectively on a 40MHz (HT40) or 80MHz (HT80) channel.

In **802.11ac** mode, you can aggregate two or four 20MHz channels. The primary channel, which is the channel on which

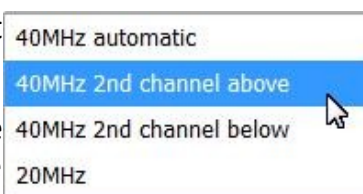


20MHz for 802.11ac
40MHz for 802.11ac
80MHz for 802.11ac

the AP sends its beacons to signal itself is automatically determined.

In **802.11n** mode you can aggregate only two adjacent 20MHz channels, to work on a 40MHz channel.

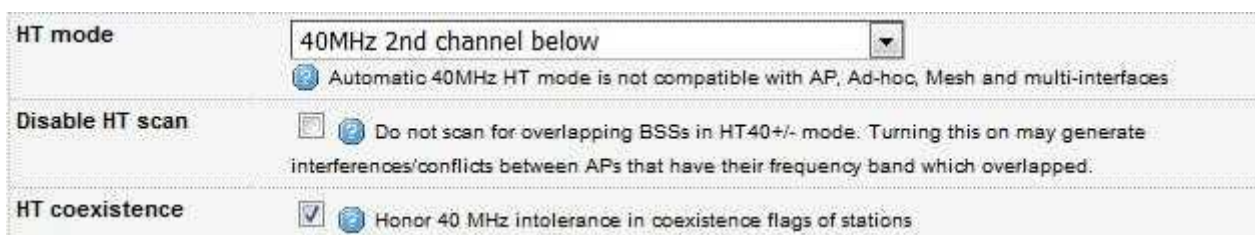
The primary channel is selected in the **Channel** section (see below). You can choose to fix the secondary channel as the one immediately above the primary channel, or as the one immediately below the primary channel. You can also set 40MHz automatic, and let the unit make the choice.



40MHz automatic
40MHz 2nd channel above
40MHz 2nd channel below
20MHz

40MHz automatic is not compatible with AP, Ad-hoc, Mesh and multi interfaces.

When HT40 mode is selected, two additional options appear:



HT mode: 40MHz 2nd channel below
☒ Automatic 40MHz HT mode is not compatible with AP, Ad-hoc, Mesh and multi-interfaces
 Disable HT scan: ☐ Do not scan for overlapping BSSs in HT40+/- mode. Turning this on may generate interferences/conflicts between APs that have their frequency band which overlapped.
 HT coexistence: ☒ Honor 40 MHz intolerance in coexistence flags of stations

Disable HT scan:

When this option is activated, the system will not check for the presence of other APs on the 40MHz width of the operating channel, which can favor the appearance of interference and degrade the quality of the communication.

HT coexistence:

With this option, the system will abandon the aggregation to free the secondary channel if it is used by other APs

Automatic channel select (ACS):

Depending on the product role, the channel can be selected automatically:

- AP role: At startup, the AP will select the channel among all the ones allowed in your country. In order to limit the choice to specific channels, do not check ACS, but use the channels multi-selection box instead.
- Client role: The client will scan all channels allowed in your country. In order to limit the channel scan list, do not check ACS, but use the channels multi-selection box instead. If the client is set in roaming mode, this channel list is superseded by the one in the roaming tab.
- Other roles: The other roles (mesh portal, ad-hoc) support only one channel, this parameter is not available and you must select a channel from the dropdown box.

Note: ACS is unavailable in “40 MHz second channel below” mode.

Channel:

According to the selected **802.11 mode** and the regulation rules of the selected country, a list of channels is available for selection. **This is not used for infrastructure client modes**, as they use all the allowed channels for scanning (possibly limited by roaming parameters).

In some cases, a single radio card can handle multiple Wi-Fi roles simultaneously. In this case any “client” function must be set to only scan the common channel. See also section [V.2.1.5 Virtual AP \(multi-SSID\) and multifunction cards](#)

See chapter [Appendix - 802.11 Radio channels](#) for more details on the available channels.

You can select several channels so that the AP will select the cleanest one, and will be able to switch to another if a radar is detected on the current one. To select multiple channels on classic browsers, use the Ctrl+click shortcut.

Note: remember that channels subject to DFS incur a checking delay (CAC time) before use. See section [V.2.4 Radio channels and national regulation rules](#) for more information.

a/b/g Data Rates tab:



Automatic supported rates:

This option allows you to restrict the rates that your Access Point advertises as supported to the clients.

Automatic basic rates:



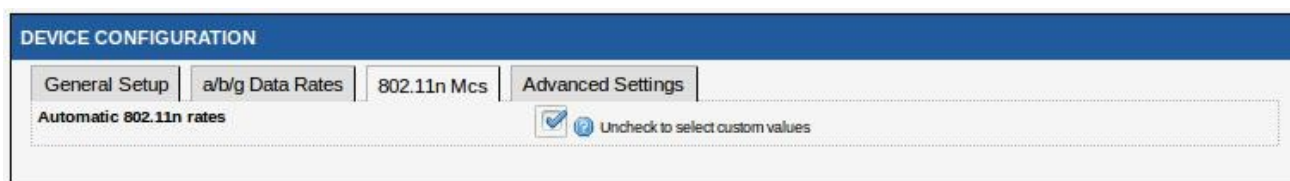
This option allows you to modify the rates that must be supported by others devices to be able to communicate with your Access Point. **Warning:** every basic rate must also be in the supported rates set.

NOTE ON DESELECTING THE LOWEST RATES:

Management, broadcast and multicast frames are sent using the lowest basic rate selected. You can increase performance with this type of frame by only selecting rates higher than the default but this will affect the area coverage (see the output power table given in your product Quick Start guide).

Since the radio card does not try low rates, retransmissions (when a frame is lost) will happen faster and will take less bandwidth. After association with the Access Point, the auto-adaptive rate control algorithm (MINSTREL algorithm) will converge faster as well.

802.11n MCS tab:



This option allows you to restrict the MCSs that your Access Point advertises as supported to the clients.

In the same manner as a/b/g rates, only selecting highest MCSs in a stream allows to increase performances for broadcast and multicast frame. The drawbacks are also the same as the a/b/g case.

This option is not available with 802.11ac radio cards.

Advanced Settings tab:

DEVICE CONFIGURATION		
General Setup	a/b/g Data Rates	Advanced Settings
Max Transmit Power	<input type="text"/> <small>dBm - leave empty to use max value allowed by your country and your radio card</small>	
Antennas	<input type="text" value="All"/>	
QoS Profile	<input type="text" value="Default"/>	
Distance Optimization	<input type="text"/> <small>Distance to farthest network member in meters.</small>	
Beacon interval	<input type="text"/> <small>In multiple of 1024µs. Used by AP, ad-hoc and mesh modes.</small>	
Fragmentation Threshold	<input type="text"/>	
RTS/CTS Threshold	<input type="text"/>	
Retry settings	☒	
Short retry	<input type="text" value="7"/> <small>Retry for frame sent without RTS/CTS</small>	
Long retry	<input type="text" value="2"/> <small>Retry for frame sent with RTS/CTS</small>	
Agregate retry	<input type="text" value="30"/> <small>Retry for aggregate frame (802.11n only)</small>	

Max transmit power:

The transmit power is normally computed automatically based on the regulation rules for the given channel and the capabilities of the radio card. This option sets an upper bound on the transmit power. Note that the transmit power is distributed between the configured antennas.

Antennas:

Unused antennas can be disabled here, thus concentrating transmit power on the remaining antennas. You can disable the third antenna, or both the second and third. In order to take advantage of 802.11n multiple spatial streams, you must use at least as many antennas as spatial streams. The transmit power is distributed between the configured antennas.

QoS Profile:

This option allows choosing between the two QoS profiles defined in the SETUP/QOS/WMM page:

- Default: uses the factory defaults for all WMM parameters
- User: allows you to use the user defined WMM parameters

Distance Optimization:

Use this option if your link is larger than 300 meters. This option will update some Wi-Fi internal timeouts but will not increase or decrease the output power. The distance to the farthest device should be used.

Beacon interval:

This option allows configuring the interval between two beacon frames.

Beacons are used by APs, mesh nodes and ad-hoc stations to advertise their capabilities and settings (HT mode, SSID...) to other devices.

The default settings depend on the 802.11 mode.

If you decrease the Beacon interval you consume more bandwidth on the channel, and you can decrease the global Wi-Fi performance; but you will detect connection losses faster.

Fragmentation Threshold:

This option configures the maximum 802.11 frame size in 802.11a/b/g mode in bytes. Frames that exceed this threshold are fragmented.

RTS/CTS Threshold:

The Wi-Fi standard uses the RTS/CTS protocol to avoid collisions in the air.

This option defines the size of the 802.11 a/b/g frames subject to this protection. Frame exceeding this size are sent under CTS/RTS protocol.

Use CTS/RTS when you have much interference on your channel and a poor performance on the Wi-Fi; or when you have hidden stations (e.g. in an exchange between stations A and B, a third station which is visible by A but not by B, hence interfering with B when it sends to A). On other case this protection decreases the global Wi-Fi performance.

Retry settings:

Unicast data frames are normally acknowledged. If the transmitter does not receive the acknowledgment, it must resend the frame.

In 802.11n, several frames can be aggregated into one big frame called an A-MPDU. Independent frames are acknowledged by an individual ACK frame, while A-MPDU frames are acknowledged by a single "block acknowledge" frame containing one acknowledgment for each subframe in the A-MPDU. Unacknowledged frames are resent in a later A-MPDU.

When you check this option, you can control the number of retries.

Short retry:

This is the number of retries for a physical data frame (single or A-MPDU).

Long retry:

This is the number of retries for a physical data frame (single or A-MPDU) sent with the RTS/CTS protocol.

Aggregate retry:

This option configures the number of retries for a frame aggregated into an A-MPDU (each 802.11 frame sent in A-MPDU frame).

VII.1.2.2 SETUP/PHYSICAL INTERFACES/WIRELESS SETTINGS/INTERFACE CONFIGURATION

This section is duplicated for each SSID. Settings only apply to the selected SSID.

Note: Various roles in the **Interface configuration** section have an **Advanced settings** tab, which you must not confuse with the **Advanced settings** for the **Device configuration** section just above.

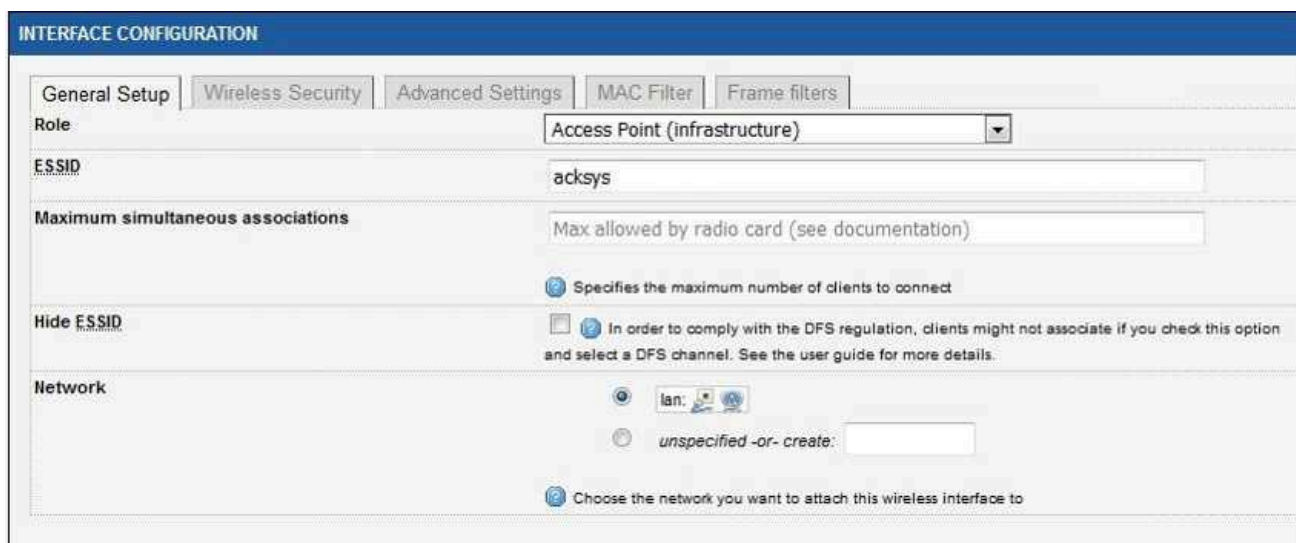
Loops pitfall in products with more than one radio

In products equipped with more than one radio card, you can create a wireless loop by activating one radio as Access Point with some SSID, and the other radio as Client with the same SSID.

Since the factory default is to have both radios bridged together internally and set to AP role, with the same SSID, you can fall in this trap by simply activating both radios and changing one of them from AP role to client role.

The product quickly enters a high-priority data transfer radio 1/wireless/ radio 2/internal bridge/radio 1. Then, the only way to recover is to reset the product to factory settings.

General Setup, Access Point Mode



INTERFACE CONFIGURATION

General Setup | Wireless Security | Advanced Settings | MAC Filter | Frame filters

Role: Access Point (infrastructure)

ESSID: acksys

Maximum simultaneous associations: Max allowed by radio card (see documentation)

Hide ESSID: ☐ In order to comply with the DFS regulation, clients might not associate if you check this option and select a DFS channel. See the user guide for more details.

Network: lan

unspecified -or- create:

Choose the network you want to attach this wireless interface to

Role: Supported roles are:

- Access point
- Isolating Access Point
- Client (connecting to an Access Point)
- Mesh (802.11s)
- Point to multipoint station (ad-hoc)
- SRCC

See a detailed description of the modes in section [V.2 Wireless architectures](#) for SRCC.

ESSID:

This is the wireless network name. See section [V.2 Wireless architectures](#) for more details.

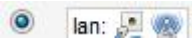
Maximum association:

Specifies the maximum number of clients allowed to connect on the Access Point.

Hide ESSID:

This option allows you to not broadcast the SSID on the network. This means that your clients need to know the SSID beforehand, since scanning will not reveal the SSID of the AP. Please check section [Radars detection overview \(DFS\)](#) for more details about hidden SSID and DFS considerations.

Network:

This option allows selecting the network where the interface is added. In the default factory settings, all the physical interfaces (Ethernet and radio ports) are bridged in the **lan** network The image shows a network selection interface with a dropdown menu currently set to "lan". To the right of the dropdown is a small icon of a globe.

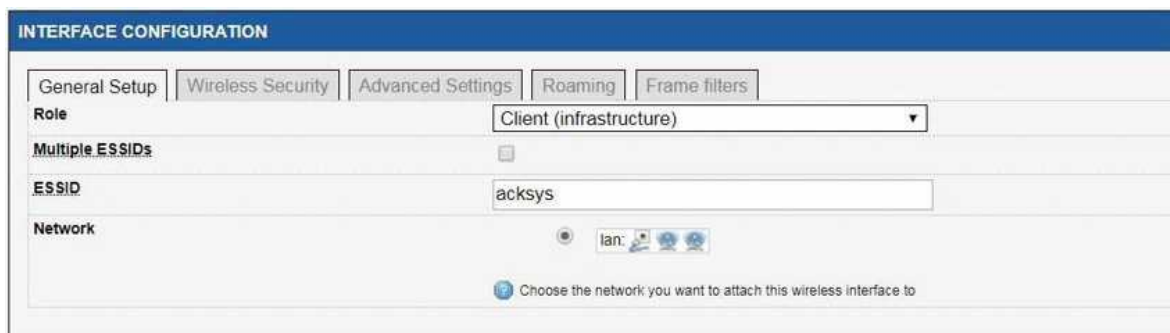
If you fill in the field to the right of  and validate, this will create a new network. In this case, your radio interface will be automatically added to this new network and removed from the current one, so please be careful and only use this feature if you have a very clear idea of what you want to do.

Please see section [Network](#) for more details on network management.

Mesh ID (only in Mesh mode):

This option replaces the ESSID when the Mesh mode is selected. It has the same purpose.

General Setup tab, Client mode

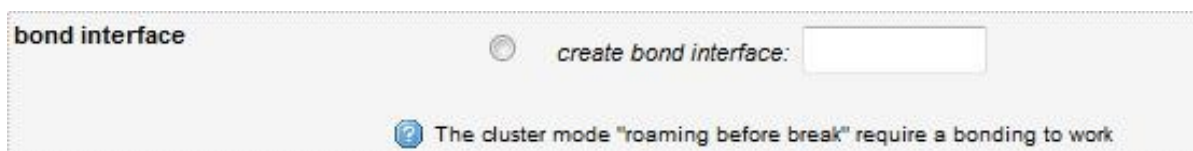


Multiple ESSIDs:

When this is checked, a multi-selection field, Wireless network nicknames, replaces the single ESSID field. You can select several SSIDs with their security parameters, and the client will associate to any AP advertising one of these combinations. In case several matching APs are in range, you can prioritize the SSIDs.

When using multiple ESSIDs, the roaming features are not available, and the security is defined together with the corresponding ESSID in a separate menu. See section [VII.1.4.3 Wireless SSIDs](#).

When **Connect before Break** is selected in the **Cluster mode** from the **Global Parameters**, the **Network** field is replaced by **bond interface**. You must give a name to this interface.



Wireless Security tab:

This menu allows you to choose the type of wireless security you want to apply on this SSID. The different security schemes are described in the [Wireless security](#) section.

Security:

Supported modes are:

- No Encryption
- WEP Open System
- WEP Shared Key
- WPA-PSK (Personal)
- WPA2-PSK (Personal)
- WPA-PSK/WPA2-PSK Mixed Mode (Personal)
- WPA-EAP (Enterprise)
- WPA2-EAP (Enterprise)
- WPA-LEAP (Enterprise)
- WPA2-LEAP (Enterprise)



NOTE 1: The Enterprise client automatically adapts to any kind of WPA/WPA2 Enterprise access point, except in one case: Using the EAP-TLS method with WPA2-Enterprise enforces the use of the CCMP protocol; it connects only to a WPA2-Enterprise access point offering CCMP.

According to the choice you've made, some properties will appear or disappear.

Fast Transition Support (802.11r):

This box appears only for clients in any of the WPA/WPA2 modes. Check this box to allow use of the 802.11r protocol against APs that support it, resulting in a reduction of the time necessary to authenticate when roaming.

You need to properly configure the APs, their mobility domain and NAS ids to take advantage of this feature.

Wireless Security tab, No Encryption mode:

INTERFACE CONFIGURATION

General Setup
Wireless Security
Advanced Settings

Security
No Encryption

Nothing to configure here.

Wireless Security tab, WEP Open System & WEP Shared Key:

INTERFACE CONFIGURATION

General Setup
Wireless Security
Advanced Settings
MAC Filter
Frame filters

Security
Used Key Slot

WEP Shared Key
Key #1

WARNING: WEP encryption must not be used in 802.11N modes
The following keys may be given as 10- or 26-digits hexadecimal strings,
or 5- or 13-character strings converted to their hex value.

Key #1		A
Key #2		A
Key #3		A
Key #4		A

Use Key Slot:

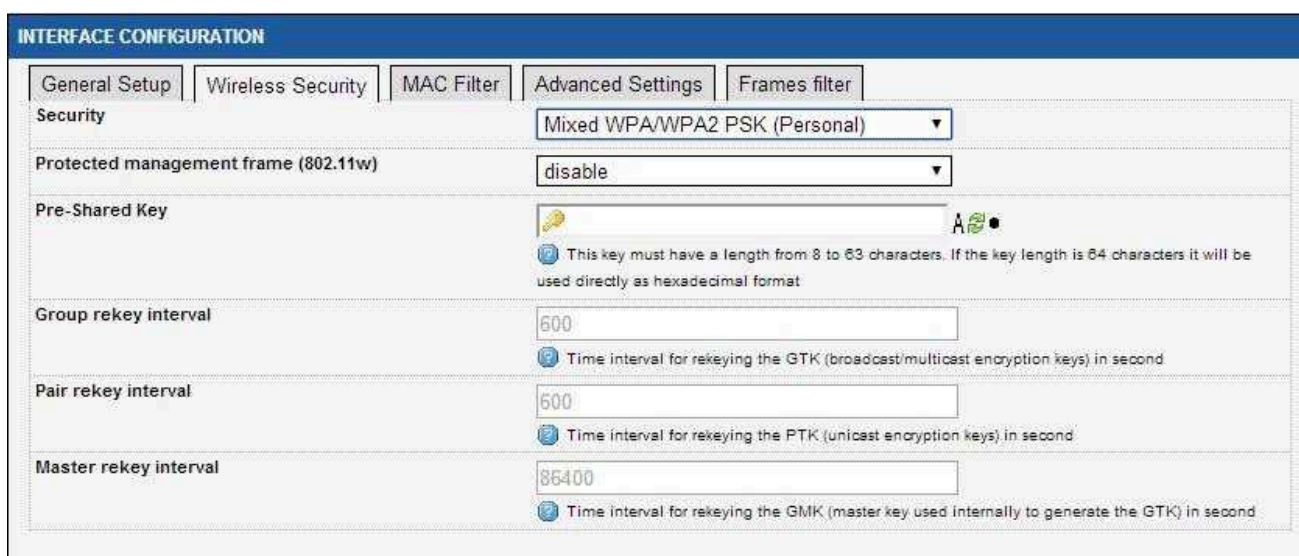
This field selects the currently used WEP key.

Key #1 to #4:

Contain the WEP key. Keys are defined by entering a string in HEX (hexadecimal - using characters 0-9, A-F), or ASCII (alphanumeric characters) format.

ASCII format is provided so that you can enter a string that is easier to remember. The ASCII string is converted into HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

Wireless Security tab, WPA-PSK, WPA2-PSK & WPA-PSK/WPA2-PSK Mixed Mode:



The screenshot shows the 'INTERFACE CONFIGURATION' window with the 'Wireless Security' tab selected. The 'Security' dropdown is set to 'Mixed WPA/WPA2 PSK (Personal)'. The 'Protected management frame (802.11w)' is set to 'disable'. The 'Pre-Shared Key' field is empty, with a green arrow icon on the right and a tooltip stating: 'This key must have a length from 8 to 63 characters. If the key length is 64 characters it will be used directly as hexadecimal format'. The 'Group rekey interval' is set to '600' with a tooltip: 'Time interval for rekeying the GTK (broadcast/multicast encryption keys) in second'. The 'Pair rekey interval' is set to '600' with a tooltip: 'Time interval for rekeying the PTK (unicast encryption keys) in second'. The 'Master rekey interval' is set to '86400' with a tooltip: 'Time interval for rekeying the GMK (master key used internally to generate the GTK) in second'.

Protected management frame (802.11w):

Enable/disable the 802.11w security feature. For more information, please read section [Protected management frame \(802.11w\)](#)

Pre-Shared-Key:

The pre-shared key may be from 8 to 63 printable ASCII characters or 64 hexadecimal digits (256 bits). The green arrow icons on the right allow to display the key in clear text while you are typing it in.

Group rekey (AP mode only):

interval: Time interval, in seconds, for rekeying the GTK (broadcast/multicast encryption keys).

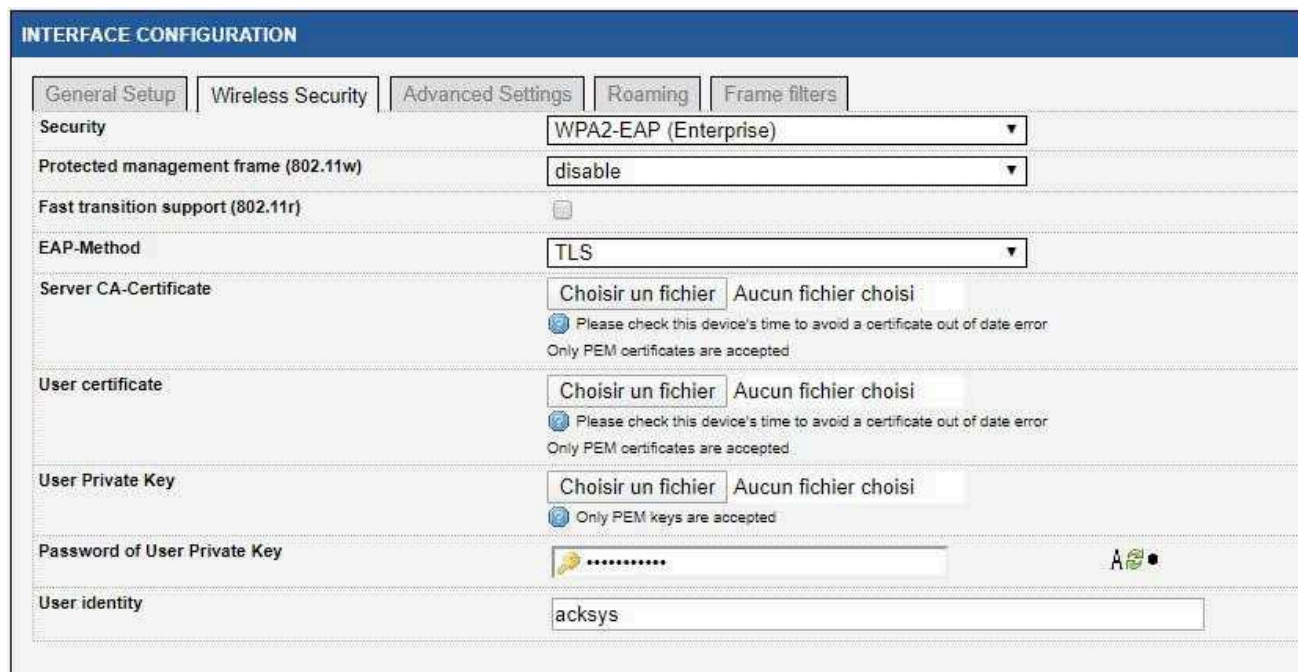
Pair rekey interval (AP mode only):

Time interval for rekeying the PTK (unicast encryption keys) in seconds.

Master rekey interval (AP mode only):

Time interval for rekeying the GMK (master key used internally to generate the GTK) in seconds.

Wireless Security tab, WPA-EAP Mode (in client mode):



INTERFACE CONFIGURATION

General Setup | **Wireless Security** | Advanced Settings | Roaming | Frame filters

Security: WPA2-EAP (Enterprise) ▼

Protected management frame (802.11w): disable ▼

Fast transition support (802.11r): ☐

EAP-Method: TLS ▼

Server CA-Certificate: Choisir un fichier | Aucun fichier choisi
Please check this device's time to avoid a certificate out of date error
Only PEM certificates are accepted

User certificate: Choisir un fichier | Aucun fichier choisi
Please check this device's time to avoid a certificate out of date error
Only PEM certificates are accepted

User Private Key: Choisir un fichier | Aucun fichier choisi
Only PEM keys are accepted

Password of User Private Key: 

User identity: acksys

Protected management frame (802.11w):

Enable/disable the 802.11w security feature. For more information please read section [Protected management frame \(802.11w\)](#)

Fast Transition Support (802.11r):

In any of the WPA/WPA2 modes, check this box to allow use of the 802.11r protocol against APs that support it, resulting in a reduction of the time necessary to authenticate when roaming. You need to properly configure the APs, their mobility domain and NAS ids to take advantage of this feature.

For more information, please refer to section [Fast Transition Support \(802.11r\)](#)

Server CA-Certificate:

Selects the location of the CA-Certificate file to be uploaded. Certificates and keys must be provided in PEM format. *This format is defined by the OpenSSL project. It's a text file identifiable by its first line beginning with "-----BEGIN" and the binary data encoded using the base64 method.*

EAP-Method:

This field contains the EAP-Method to be used.
Available methods are: TLS, PEAP, LEAP.

NOTE: The Enterprise client automatically adapts to any kind of WPA/WPA2 Enterprise access point, except in one case: Using the EAP-TLS method with WPA2-Enterprise enforces the use of the CCMP protocol; it connects only to a WPA2-Enterprise access point offering CCMP.

EAP-Method TLS:

User certificate:

Selects the location of the user certificate file to be uploaded. Must be provided in PEM format.

User Private Key:

Selects the location of the Private Key file to be uploaded. Only PEM private keys are allowed.

Password of User Private Key:

Password associated to the chosen Private Key.

User identity:

This field gives the login to use during EAP-TLS authentication. In this authentication method, this field is rarely used by the RADIUS server. The default value is *acksys*

EAP-Method PEAP:

EAP-Method	PEAP
Anonymous identity	incognito
<small>This identity is used during the authentication phase 1. It is recommended to set a different value than user identity.</small>	
Server CA-Certificate	Choisir un fichier Aucun fichier choisi
<small>Please check this device's time to avoid a certificate out of date error. Only PEM certificates are accepted</small>	
Authentication (phase 2)	MSCHAPV2
User identity	acksys
Password	*****

Anonymous identity:

This value allows to configure the identity that will be sent in phase 1 of the protocol. It's not used by the RADIUS server, but it's a necessary element for the establishment of the TLS tunnel. As this field is clear on the network, we recommended, for security reasons, to set a value different from the login used for authentication.

If this field is left empty, the identity used by the authentication method (User identity) will be used.

Authentication (phase 2):

This field contains the Authentication method. To date, only MSCHAPV2 is available

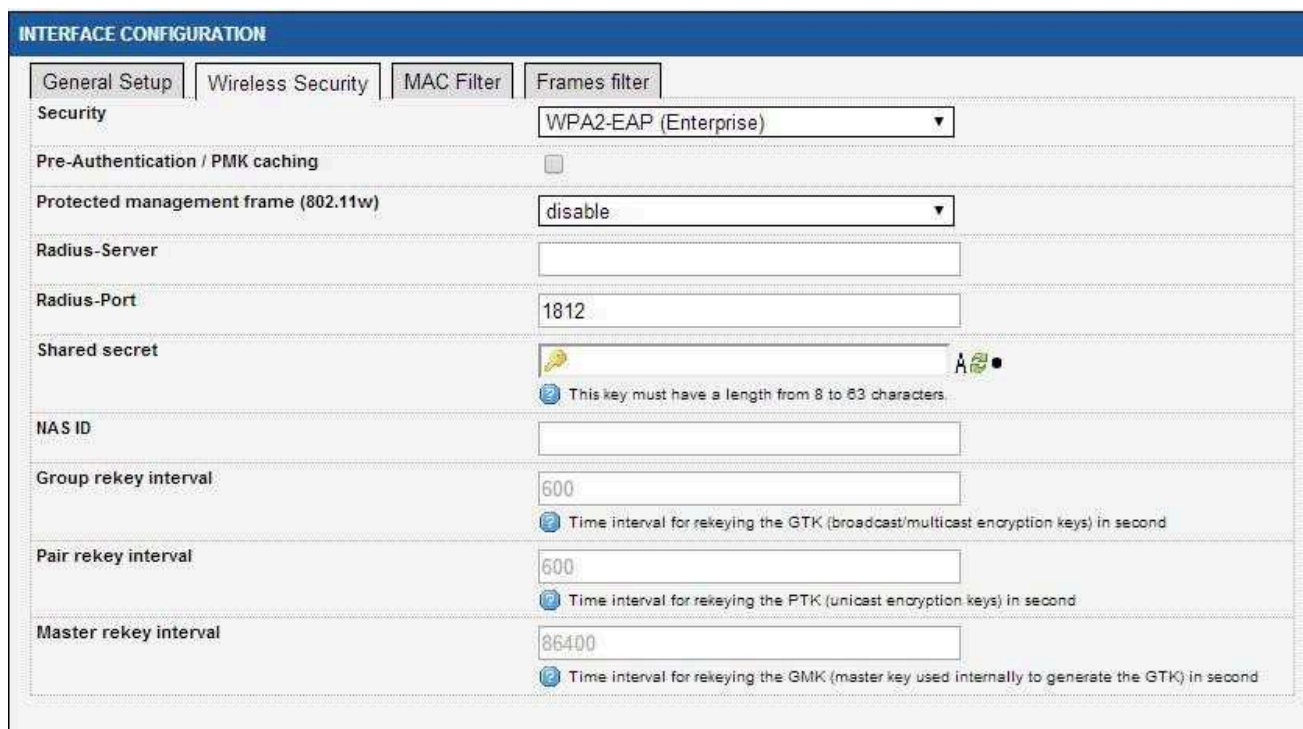
User identity:

Identity used for the authentication.

Password:

Password associated to the User identity

Wireless Security tab, WPA-EAP Mode (in access point mode):



The screenshot shows the 'INTERFACE CONFIGURATION' window with the 'Wireless Security' tab selected. The 'Security' dropdown is set to 'WPA2-EAP (Enterprise)'. The 'Pre-Authentication / PMK caching' checkbox is unchecked. The 'Protected management frame (802.11w)' dropdown is set to 'disable'. The 'Radius-Server' field is empty. The 'Radius-Port' field contains '1812'. The 'Shared secret' field contains a masked password with a strength indicator. The 'NAS ID' field is empty. The 'Group rekey interval' is set to '600' seconds. The 'Pair rekey interval' is set to '600' seconds. The 'Master rekey interval' is set to '86400' seconds. Each interval field has a tooltip explaining its purpose.

Field	Value
Security	WPA2-EAP (Enterprise)
Pre-Authentication / PMK caching	☐
Protected management frame (802.11w)	disable
Radius-Server	
Radius-Port	1812
Shared secret	[Masked Password]
NAS ID	
Group rekey interval	600
Pair rekey interval	600
Master rekey interval	86400

Pre-Authentication / PMK caching:

In any WPA/WPA2-EAP mode, check this box to allow use of pre-authentication / PMK caching. For more information, refer to [Pre-authentication / PMK caching](#)

Protected management frame (802.11w):

Enable/disable the 802.11w security feature. For more information please read section [Protected management frame \(802.11w\)](#)

Radius-Server: IP address or URI of the radius server.

Radius-Port: Radius server UDP port.

Shared secret: Password shared between the access point and the radius server.

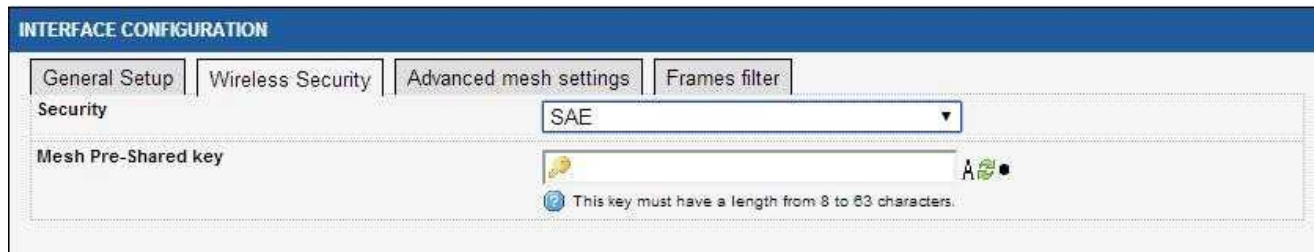
NAS ID: Network Access Server ID. This value may be used by the radius server instead of the IP address.

Group rekey: interval: Time interval for rekeying the GTK (broadcast/multicast encryption keys) in seconds.

Pair rekey interval: Time interval for rekeying the PTK (unicast encryption keys) in seconds.

Master rekey interval: Time interval for rekeying the GMK (master key used internally to generate the GTK) in seconds.

Wireless Security tab, SAE Mode (in mesh mode):

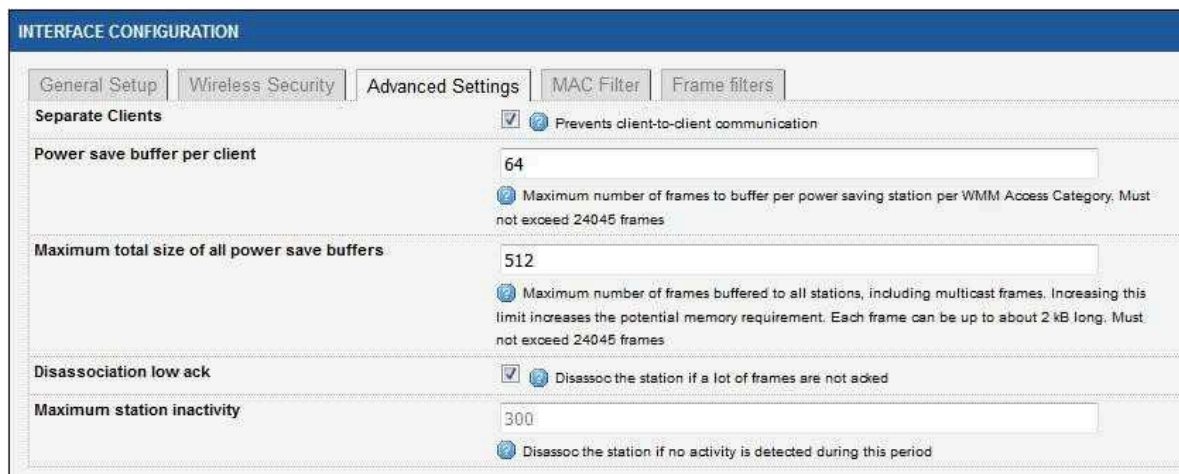


The screenshot shows the 'INTERFACE CONFIGURATION' window with the 'Wireless Security' tab selected. The 'Security' dropdown is set to 'SAE'. Below it, there is a 'Mesh Pre-Shared key' field with a password icon and a green checkmark. A tooltip indicates: 'This key must have a length from 8 to 63 characters.'

Mesh Pre-Shared key:

This option allows configuring the mesh network shared key.

Advanced settings tab in Access point mode



The screenshot shows the 'INTERFACE CONFIGURATION' window with the 'Advanced Settings' tab selected. The 'Separate Clients' checkbox is checked, with a tooltip: 'Prevents client-to-client communication'. The 'Power save buffer per client' is set to 64, with a tooltip: 'Maximum number of frames to buffer per power saving station per WMM Access Category. Must not exceed 24045 frames'. The 'Maximum total size of all power save buffers' is set to 512, with a tooltip: 'Maximum number of frames buffered to all stations, including multicast frames. Increasing this limit increases the potential memory requirement. Each frame can be up to about 2 kB long. Must not exceed 24045 frames'. The 'Disassociation low ack' checkbox is checked, with a tooltip: 'Disassoc the station if a lot of frames are not acked'. The 'Maximum station inactivity' is set to 300, with a tooltip: 'Disassoc the station if no activity is detected during this period'.

Separate Clients:

This option is only available when the **Isolating Access Point** role is selected. When **Separate Clients** is checked, wireless clients won't be able to communicate between them (this is not possible in **Access point** mode). See section [Infrastructure Mode](#) for more details.

Power Save buffer per client:

Define the maximum number of frames that can be queued for each client

Maximum total size of all power save buffers:

Maximum number of frames that can be buffered for all the stations

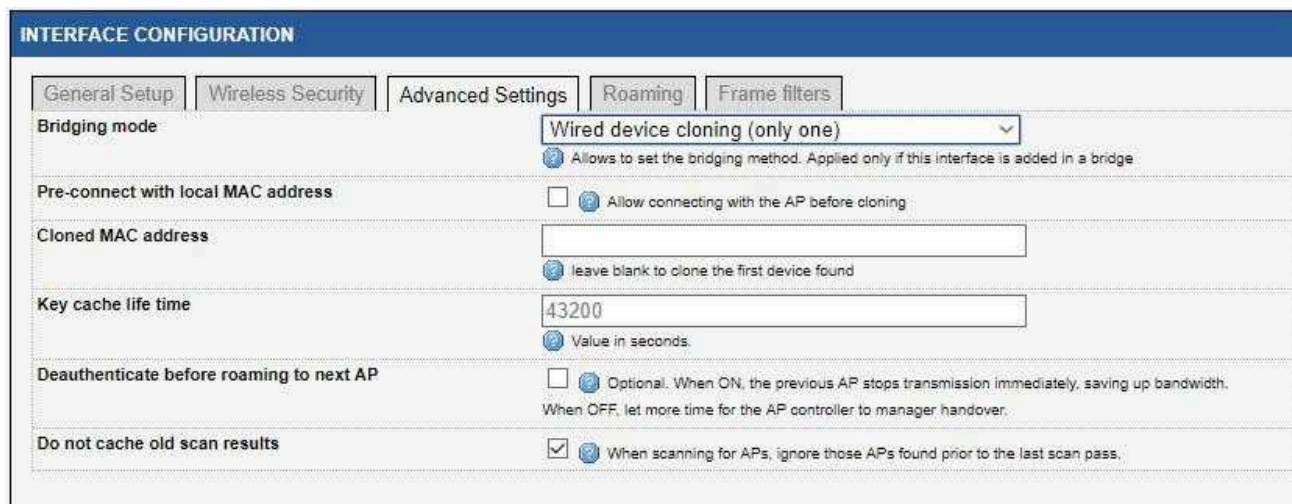
Disassoc low ack:

With this option set, when more than 50 packets sent by the AP are not acknowledged by the client, the client is disconnected.

Maximum station inactivity:

Idle time in seconds after which the client will be disconnected.

Advanced settings tab in Client mode



The screenshot shows the 'INTERFACE CONFIGURATION' window with the 'Advanced Settings' tab selected. The 'Bridging mode' is set to 'Wired device cloning (only one)'. The 'Pre-connect with local MAC address' option is unchecked. The 'Cloned MAC address' field is empty. The 'Key cache life time' is set to 43200 seconds. The 'Deauthenticate before roaming to next AP' option is unchecked. The 'Do not cache old scan results' option is checked.

Setting	Value / Status
Bridging mode	Wired device cloning (only one)
Pre-connect with local MAC address	☐
Cloned MAC address	
Key cache life time	43200
Deauthenticate before roaming to next AP	☐
Do not cache old scan results	☒

Bridging mode:

This option allows selecting the bridging method (Please see section [Wired to wireless bridging in infrastructure mode](#) for more details) that will be used if this interface is added to a bridge (please see section [Network](#) for more details).

The available methods are:

- ARPNAT (default value)
- 4 addresses format (WDS)
- Wired device cloning
- PROFINET device cloning.

When **Connect before Break** is selected in the **Cluster mode** from the **Global Parameters**, you must select [4 addresses format \(WDS\)](#).

Please read the section [Cloning](#) for more details on cloning mode.

Pre-connect with local MAC address:

This option exists only with Wired device cloning or Profinet device cloning. If checked, this allows the product association to an Access Point with the local Wireless adapter MAC address when no Ethernet or Profinet equipment is detected. In this case, if cloning to the Ethernet or Profinet equipment occurs some time later, the ARP table of the remote devices will no longer be valid. So, these remote devices won't be able to access to the product until the ARP table is refreshed.

Cloned MAC addr:

This field exists only with Wired device cloning or Profinet device cloning. Fill this field, if you want to force the MAC address used for the cloning. Leave blank to clone the first device found.

Key cache life time:

This field exists only with WPA/WPA2 EAP. If your AP supports the Opportunistic key caching (OKC) or the pre-authentication, this option allows configuring the life time for each PMK. The default value is 43200 seconds (12 hours).

Deauthenticate before roaming to next AP:

When this option is selected, the client can de-authenticate the current access point before the client roam to the next access point, which frees up the frequency more quickly. This option can be left unchecked to allow more time for an access point controller to handle the transfer, or to ensure compatibility with previous versions of WaveOS.

Do not cache old scan results:

When checked, the scan results of the previous scan cycle is not merged with the results of the current scan cycle. This option is checked by default.

Advanced settings tab in Point to multipoint station (ad-hoc)



The screenshot shows the 'INTERFACE CONFIGURATION' window with four tabs: 'General Setup', 'Wireless Security', 'Advanced Settings', and 'Frames filter'. The 'Advanced Settings' tab is selected. Under the 'BSSID' label, there is a text input field. Below the input field, a small icon and text indicate the MAC address format: 'MAC address format as 6 pairs of column-separated hex digits.'

BSSID:

This option allows setting the BSSID for this interface.

Roaming tab (only in Client mode):

INTERFACE CONFIGURATION
General Setup
Wireless Security
Advanced Settings
Roaming
Advanced Roaming
Frames filter

Enable proactive roaming
☒
If unchecked, the device will not roam until it loses its current AP

List of channels scanned for the next AP discovery

11 (2.462 GHz)
36 (5.180 GHz)
40 (5.200 GHz)
44 (5.220 GHz)
48 (5.240 GHz)
149 (5.745 GHz)

☒ If no channel is selected, all channels will be scanned

Delay between two successive scan cycles
10000
☒ Value in milliseconds, e.g. "10000". Must be greater than 0

Current AP leave threshold
-60
☒ Value in dBm, e.g. "-60". Below (worse than) this value, the device will try to use another AP

Required level boost
6
☒ Roaming occurs only if the candidate signal level is above the current AP's plus this value

Current AP scan threshold
0
☒ Value in dBm, e.g. "-40". Above (better than) this value, the device will stop scanning. Set to 0 to scan unconditionally. Incompatible with the Maximum signal level option

Minimum signal level
-75
☒ In dBm, e.g. "-75". 0 to disable. Roaming won't occur if the candidate signal is below this level. Association is still possible if no other AP is available

If the bridging mode is set to **4 addresses format (WDS)**, Proactive Roaming must be enabled **ONLY** when the Connect before Break mode is selected.

Enable proactive roaming:

Check this checkbox to enable the fast roaming features.

List of channels scanned for the next AP discovery:

Choose here the channels that will be scanned for AP discovery. This selection supersedes the list of channels from the Device configuration box above.

Using more than one channel allows a denser repartition of the Access Points, as they will not interfere with each other. But, unless you are using a dual radio product, this will reduce the data throughput for the client, because the scanning process must periodically leave the AP channel (and thus stop transmitting) in order to scan other channels.

With single radio products, the best throughput will be achieved if you use only one channel. If possible, do not select more than three or four channels.

Delay between two successive scan cycles:

This value represents the time (in milliseconds) between scan cycles.

Current AP leave threshold:

If the RSSI of the current AP falls below this value (in dBm), the client will try leaving the current AP and roaming to another AP.

Note: in previous versions this parameter was named *Current AP minimum signal level*.

Required level boost:

Minimum improvement in signal level that the new (target) AP must exhibit over the old (current) one, to allow roaming to actually occur.

Current AP scan threshold:

When the current AP signal is above (better than) this level, the client ceases to scan for better APs.

Minimum signal level:

APs whose perceived signal is below this level will not be candidates for roaming, i.e., they will never be preferred to the currently associated AP. But it will still be used if there is no current nor better AP.

Advanced Roaming tab (only Client with proactive roaming enabled):

INTERFACE CONFIGURATION	
General Setup Wireless Security Advanced Settings Roaming Advanced Roaming Frame filters	
Excessive signal detection threshold	<input type="text" value="0"/> <p><small>In dBm, e.g. -30. Leave empty or 0 to disable. Roaming will occur when the current AP signal crosses and exceeds this value, and there is an acceptable candidate around. This allows elimination of approaching AP antennas that will be soon overtaken.</small></p>
Maximum signal level	<input type="text" value="0"/> <p><small>In dBm, e.g. -30. Leave empty or 0 to disable. Must be greater or equal to the 'Excessive signal detection threshold'. Roaming will occur whenever the current AP signal is above this value, and there is an acceptable candidate around. When selecting the next AP, the ones above this value are considered last.</small></p>
Maximum time above maximum level	<input type="text" value="0"/> <p><small>In number of scan cycles. Leave empty or 0 to disable. Maximum time allowed with a signal level superior to Maximum without a disconnection when no other APs are available for roaming. Furthermore, when this option is activated, the client will not connect to any AP superior to Maximum.</small></p>
Maximum time under minimum level	<input type="text" value="0"/> <p><small>In number of scan cycles. Leave empty or 0 to disable. Maximum time allowed with a signal level inferior to Minimum without a disconnection when no other APs are available for roaming. Furthermore, when this option is activated, the client will not connect to any AP inferior to Minimum.</small></p>
Minimum roaming interval	<input type="text" value="0"/> <p><small>In ms. Leave empty or 0 to disable. Roaming won't occur before this delay has elapsed since the last association.</small></p>
No-return delay	<input type="text" value="0"/> <p><small>In ms. Leave empty or 0 to disable, max 180000 (3 min). Roaming won't occur to an AP that was left recently (before this delay has elapsed). The delay is cleared for APs that are not around anymore.</small></p>
Threshold hysteresis	<input type="text" value="2"/> <p><small>Value in dBm, e.g. -2. Hysteresis used for all thresholds. This value will be added and subtracted to each threshold to set the corresponding threshold hysteresis interval.</small></p>
RSSI smoothing factor	<div> <input type="text" value="Last beacon weight: 19%"/> <input type="button" value="v"/> </div> <p><small>The RSSI of the current AP is computed over the last few beacons received. Select the importance of the last beacon relative to older ones. This value commands a decaying factor. Default: 19%.</small></p>
Beacon timeout	<input type="text" value="7"/> <p><small>Value in beacon interval units.</small></p>
Probe on beacon timeout	☒ <p><small>When beacon time out occurs, probe the current AP for the last time in the hope that deauthentication won't be needed if the AP answers.</small></p>
Maximum time off-channel	<input type="text" value="125"/> <p><small>In ms. Maximum delay offchannel (during which data must be buffered by the associated AP). Several channels will be scanned without returning to the base channel, until this delay is exhausted. An upper limit of 10 times the beacon interval of the current AP is enforced.</small></p>
Offchannel adaptation delay	<input type="text" value="30"/> <p><small>In ms. Adaptation delay after a channel switch, before sending the probe request or accepting beacons. Reducing below 30 ms speeds up scanning but decreases AP detection likelihood.</small></p>
Per channel probe response delay	<input type="text" value="30"/> <p><small>In ms. Time to wait for an answer from the access points. For DFS channels, where probes are forbidden, a floor value of 100 ms is enforced to ensure beacon detection.</small></p>
Roaming log info	<div> ☐ Display scan process while associated ☐ Display scan process while un-associated ☐ Display best based selection comparison ☐ Display roaming parameters ☐ Log filtered table of APs used to select the best AP (limited to line buffer available space) ☐ Include unfiltered APs in the above table (show all APs seen) ☐ Rise log level used to display reasons for filtering out APs ☐ Display roaming state changes </div> <p><small>Select the roaming log info will show in product log. To show the log you must set the wireless client log level to roaming or more and general log level to notice or more in 'log settings' section.</small></p>

Excessive signal detection threshold:

When the perceived signal level of the current AP passes above this limit, the client will try to roam to another AP, in the assumption that the current one will soon suddenly drop, due perhaps to the use of directional antennas.

Maximum signal level:

APs that are above this level have less priority when choosing the next AP to roam to.

Maximum time above maximum level:

Maximum time allowed, in number of scan cycles, with a signal level superior to Maximum without a disconnection when no other APs are available for roaming. Furthermore, when this option is activated, the client will not connect to any AP superior to Maximum.

Maximum time under minimum level:

Maximum time allowed, in number of scan cycles, with a signal level inferior to Minimum without a disconnection when no other APs are available for roaming. Furthermore, when this option is activated, the client will not connect to any AP inferior to Minimum.

Minimum roaming interval:

This parameter allows to impose a minimum delay, in milliseconds, between the last association to an AP and the next roaming.

No-return delay:

In areas with many walls, an AP that was left because it became too far away, may appear very good for a short time, due to radio waves bounces. To avoid roaming back to this kind of APs, which you know to be far, you can add a delay here.

Threshold hysteresis:

In order to avoid oscillating behaviours when the measured received signal is unstable (which is usually the case), the scan, leave and excessive thresholds are, in fact, interpreted as intervals of width $\pm$ hysteresis centered on the threshold.

RSSI smoothing factor:

Thresholds are compared to the average power of the beacons received from the current AP. The smoothing factor adjusts the pace at which old beacons are forgotten in the moving average calculation.

Beacon timeout:

The number of consecutive missing beacons from the current AP that will cause disassociation and search for a new AP. The corresponding duration depends on the beacon interval set in the AP.

Probe on beacon timeout:

When set, before disassociation due to missing beacons, the client will send a short data frame and will not disassociate if this frame is acked.

Maximum time off-channel:

When scanning another channel, the current AP is told to buffer incoming data until the client returns to the channel of the AP. Some APs have insufficient buffers and loose data in the meantime. This parameter limits the duration where the scanner is scanning on other channels, so it returns to the AP channel before the AP buffers are exhausted. This duration must be set greater than the sum of the two next parameters. It will be further reduced automatically to the duration of the AP beacon interval. Its precision is about 10 ms.

If this parameter is large enough, the scanner can switch channels and send probes several times before returning to the current AP channel.

Off-channel adaptation delay:

Adaptation delay, in ms, after a channel switch, before sending the probe request or accepting beacons. Reducing below 30 ms speeds up scanning but decreases AP detection likelihood.

Per channel probe response delay:

The time the scanner will stay on the scanned channel after sending a probe request, waiting for probe responses or beacons. To tune this parameter, you must account for the traffic on the channel and the swiftness of the AP (or its controller) at answering probe requests.

For DFS channel, where probes are forbidden, a floor value of 108ms is enforced to ensure beacon detection.

Roaming log info:

Select the roaming information that must be displayed. Please note that the Wireless log level must be set to **Roaming** or higher (see section 0 Log settings)

MAC filter tab (only in Access Point modes):

INTERFACE CONFIGURATION	
General Setup	Wireless Security
MAC Filter	Advanced Settings
MAC-Address Filter	Deny all except listed
MAC-List	00:01:1b:3a:44:22

MAC-Address filter:

You can specify a list of client MAC addresses that will be either allowed or denied. Let the filter disabled if you do not require it. **WARNING:** this must not be used alone as an effective security feature, since MAC addresses are is easy to masquerade.

MAC-List:

Enter the client MAC address to deny or allow. Enter MAC addresses as hexadecimal strings, with a separating column every two digits.

Click the  **add** icon on the right of the last field to add a new address. Click the  **remove** icon on the right of any field to remove it from the list.

Advanced mesh settings tab (only in 802.11s mode):

INTERFACE CONFIGURATION	
General Setup	Wireless Security
Advanced mesh settings	Frames filter
Path refresh time	1000 in ms
Min discovery timeout	100 in ms
Active path timeout	5000 in ms
Network diameter traversal time	50 in TU (1 TU= 1024 μ s)
Root mode	Proactive PREQ with PREP
Enable gate announcements	☒
Active path to root timeout	6000 in TU (1 TU= 1024 μ s)
PREQ root interval	5000 in TU (1 TU= 1024 μ s)
Rssi threshold	0 in dBm (0 to disable)

Path refresh time:

When data is sent through a previously discovered path which is due to expire soon (i.e., in less than the *path refresh time* parameter), an early discovery is started, so that the path will be already renewed when it should have expired. This removes data latency due to expired path renewal. *path refresh time* must be less than *active path timeout*.

Min discovery timeout:

When a path discovery request is sent, it will be resent if no response is received after min *discovery timeout*. This discovery timeout is doubled after each successive timeout for the same path. This value must be greater than twice the “network diameter traversal time”, so that the timeout covers both a request and its response crossing the largest possible path in the network.

Active path timeout:

This is the delay during which a path is considered valid, i.e. it can be kept in cache tables and used before a renewal becomes mandatory. The target of a path discovery inserts this value in its response to the requester. The requester can use the path during this time at most, after which it must renew the discovery (in case the target has moved).

Network diameter traversal time:

This is an estimate of the time needed for an HWMP frame to propagate across the mesh.

Rssi threshold:

This is the threshold (in dBm) below which a plink will be closed if already established or not allowed to start the peering process if not. Enter 0 to disable this feature.

Root mode:

This indicates whether this station is a root node, and how it advertises this fact to other stations. A root node sends periodical broadcasts to inform all the other nodes of its existence. This can speed up routing decisions in some cases. Several stations can be set in root mode in the same mesh, but the broadcast messages overhead reduce useable bandwidth.

Three root modes are available. For details on how they work, see the IEEE 802.11-2012 standard, chapter 13.

- Proactive PREQ: the root station periodically sends out a broadcast HWMP PREQ frame that establishes a data path from any node to the root.
- Proactive PREQ with PREP: the root station periodically sends out a broadcast HWMP PREQ frame that establishes a data path from any node to the root, and requires the nodes to answer back with a HWMP PREP frame that establishes the reverse data path from the root to any node.

- Proactive RANN: the root station periodically sends out a broadcast HWMP RANN frame advertising its address (receiving stations then request a path to the root with an unicast PREQ).

The next parameters vary depending on the exact root mode.

Enable gate announcements (root mode only):

This flag should be set if this product has access to a network outside the mesh, which holds always true since bridging networks is the purpose of these products. The flag is sent to all other nodes to advertise the fact that MAC addresses outside the mesh might be reached through this root node.

Active path to root timeout (root mode only):

This is the same as **Active path timeout** but is used only in proactive PREQ sent by this root node.

PREQ root interval (PREQ root modes only):

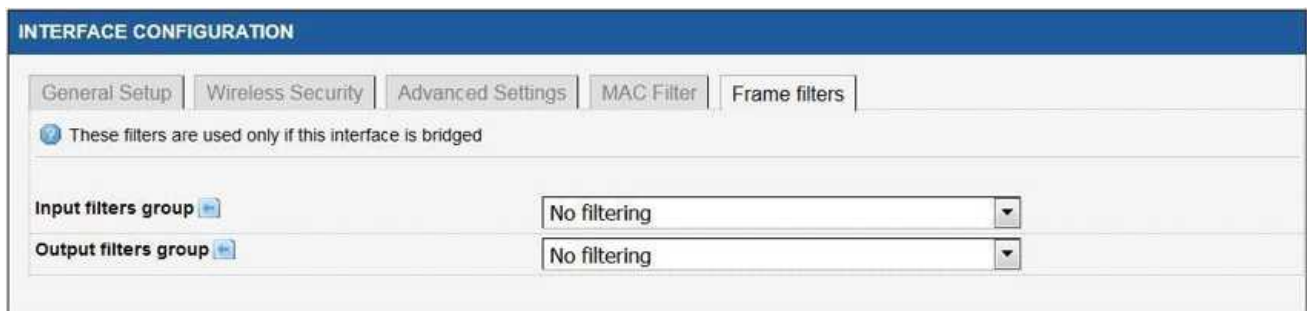
This value represents the time between proactive PREQ broadcasts.

RANN root interval (RANN root mode only):

This value represents the time between proactive RANN broadcasts.

Frames filter tab:

Wireless interfaces included in a bridge-type network interface can filter frames as they pass along.



Input filter group/Output filter group:

Choose one of the filters prepared in routing/firewall/bridge filter section.
For more information about filters group, please see [Bridge filter](#)

SRCC configuration

In order for SRCC to work correctly, all the parameters (except the product type) in the two following sections must be identical on every product of a train.

General Setup:

INTERFACE CONFIGURATION
General Setup
Frames filter
Advanced SrcC

Role
Srcc

Network
lan:

Choose the network you want to attach this wireless interface to:

Product type
Type A

2 devices from the same side of the coach must have the same type

Link establishment threshold
-50

in dBm.

Below this threshold, a potential peer is ignored

Link establishment duration
60

in seconds

Broken link threshold
-70

in dBm.

Below this threshold during more than "Broken link duration", a link will be closed.

Broken link duration
660

in seconds

Wifi band
802.11a band (5 GHz)

Use VHT80 ieee802.11ac

First link channel
36 (5.180 GHz)

This channel cannot be subject to DFS

Second link channel
100 (5.500 GHz) (DFS)

Network: The network to which SRCC will add its wireless interface.

Product type: All products on the same coach edge must have the same product type (whatever it is).

Link establishment threshold & Link establishment duration:

A potential partner is considered valid if its signal level stays over **Link establishment threshold** during more than the **Link establishment duration**.

Broken link threshold and Broken link duration:

If an established link's signal drops below **Broken link threshold** during more than **Broken link duration**, the link is considered broken, and SRCC start its wireless detection process again.

The broken link duration includes the DFS CAC time. This explains the 660s default value which is 600s (European CAC time for weather channels) and 60s (for the broken link duration itself). You can reduce this value according to your current DFS CAC time, see [III.5.6 Radars detection overview \(DFS\)](#) for usual values.



SWAA / SWSA User Guide

The parameters below allow the user to configure the final wireless link:

Wi-fi band:

The Wi-Fi frequency range for the final links. Choose 802.11a for the 5GHz band and 802.11g for the 2.4GHz band.

Use VHT80 ieee802.11ac:

If you choose the 802.11a band, click this checkbox to use the 802.11ac VHT80 channel feature. This will dramatically increase the link bandwidth. If unchecked, ieee802.11ac VHT40 is selected.

First link channel:

This is the wireless channel associated with the first SRCC final link. DFS channels have been removed from the list since SRCC uses it for its wireless discovery. This way, the discover process will not be stopped by a DFS event.

Second link channel:

This is the wireless channel associated with the second SRCC final link. Even if the products are configured in non-redundant topology, both channels are required.

Advanced SRCC parameters:

These settings are for experienced users only. Change them with great care.

INTERFACE CONFIGURATION

General Setup
Frame filters
Advanced SRCC

Ethernet discover scan duration
120
in seconds

Mixed redundancy mode
☐

Wi-Fi discover ap ssid
ACK_SRCC_DISC

Wi-Fi pre-shared key magic
Ceci est un magic tres complique
This key magic must have a length from 8 to 63 characters.

Peer table timeout
20
in seconds

Target table timeout
120
in seconds

Peer acknowledge timeout
120
in seconds

Peer reconfiguration timeout
200
in seconds

Internal L2 GRE interface ip prefix
192.168.40.0
The netmask for this ip network is 255.255.255.0. Thus the first 3 octets only are meaningful

Ethernet discover scan duration:

This is the global duration of the Ethernet topology discovery scan. As explained in the technical reference section, all the SRCC devices in the same coach must be powered up at the same time. If this is not the case, this parameter will help you adjust the time window where all SRCC devices can scan each other during the power-up sequence.

Mixed redundancy mode:

Activate the Mixed redundancy mode.

Mixed redundancy mode boost:

This is the gain in per cent added to the target metric. min=1; maximum=65535

Wi-Fi discover ap ssid:

This is the SSID used by the wireless scan process to discover other potential partners.

Wi-Fi pre-shared key magic:

This key allows the user to define his own key, so that it can be different for each user.

Peer table timeout:

During the wireless discover process, if a potential partner's signal level is correct (over the Link establishment threshold) and suddenly disappears, this partner will be erased from the partner (peer) list after a Peer table timeout duration.

Target table timeout:

This is the same as peer table timeout, but expressed for the whole cell – the group of wireless peers on the other carriage. See SRCC technical reference for more details. If the cell is not valid for more than Target table timeout, it will be removed from the list.

Peer acknowledge timeout:

This is the duration the Master waits for the answer from all partners after sending its proposed cell architecture.

Peer reconfiguration timeout:

This is the duration the Master waits for all the partners to switch to their final roles.

Internal L2 GRE interface IP prefix:

SRCC's internal uses a GRE L2 tunnel. This GRE interface is configured with a C class IPV4 address. This parameter offers the user a way to customize the IP in case of conflict between the default IP address and its network.

This parameter represents the GRE interface IP prefix. Only the first three bytes are significant (the last one is ignored). If the final role is AP, the last digit will replace with 1 and with 2 in case of client final role.

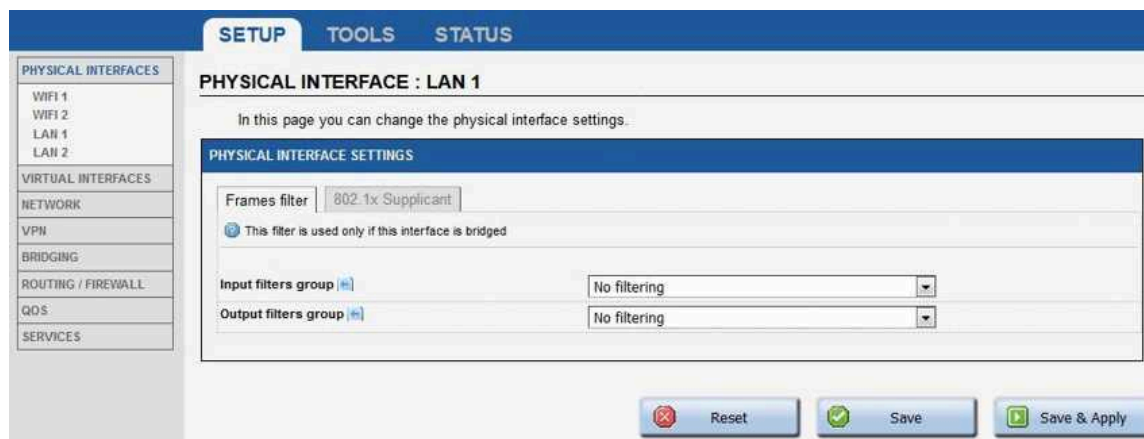
For example:

User prefix: A.B.C.D

Final Role	IP
AP	A.B.C.1
Client	A.B.C.2

VII.1.3 Physical Interface: LAN

Frames filter



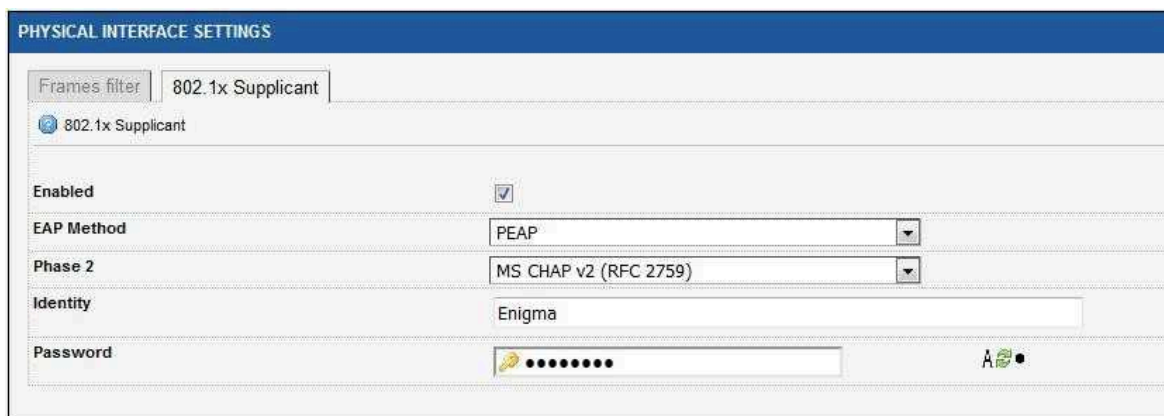
This page allows to apply input or output filters on the Ethernet interfaces of the product.

Input/Output filters group:

Choose one of the filters prepared in *routing/firewall/bridge filter* section. For more information about filters group, please see [Bridge filter](#)

802.1x Supplicant

In this tab you can activate 801.1x authentication on the Ethernet ports. To date, only the supplicant mode is supported.



EAP-Method:

Select the EAP-Method to be used, PEAP or TLS

Phase 2:

This field contains the Authentication method. Only MSCHAPV2 is available.

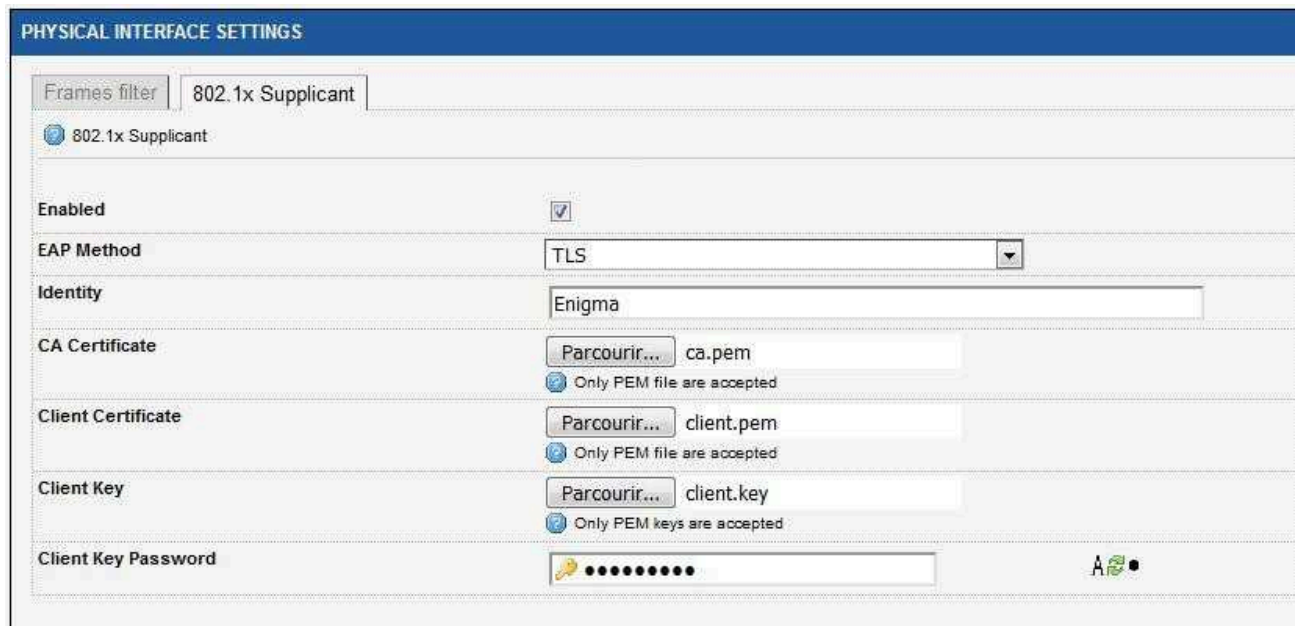
Identity:

Identity used for the authentication.

Password:

Password associated to the User identity

EAP-Method TLS:



The screenshot shows the 'PHYSICAL INTERFACE SETTINGS' window. At the top, there's a 'Frames filter' set to '802.1x Supplicant'. Below it, a section for '802.1x Supplicant' is visible. The main configuration area includes: 'Enabled' (checked), 'EAP Method' (set to 'TLS'), 'Identity' (set to 'Enigma'), 'CA Certificate' (file path 'ca.pem' with a note 'Only PEM file are accepted'), 'Client Certificate' (file path 'client.pem' with a note 'Only PEM file are accepted'), 'Client Key' (file path 'client.key' with a note 'Only PEM keys are accepted'), and 'Client Key Password' (a masked password field).

Identity:

This field gives the login to use during EAP-TLS authentication.

CA-Certificate:

Selects the location of the CA-Certificate file to be uploaded. Certificates and keys must be provided in PEM format (see note below).

Client certificate:

Selects the location of the Client certificate file to be uploaded. Must be provided in PEM format.

Client Key:

Selects the location of the Key file to be uploaded. Only PEM private keys are allowed.

Client Key password:

Password associated to the Client Key.

NOTE: The PEM format is defined by the OpenSSL project. It's a text file identifiable by its first line beginning with "-----BEGIN" and the binary data encoded using the base64 method.

VII.1.4 Virtual interfaces

This section allows managing virtual interfaces.

A virtual interface is attached to a physical interface.

You can add a several virtual interfaces on one physical interface.

For 802.1q tagging, the virtual interface adds a 802.1q tag on egress traffic and removes the tag on ingress traffic.

VII.1.4.1 802.1q Tagging

802.1q tags are used to split a common physical link into several virtual LANs (VLANs) in order to isolate the traffics pertaining to groups of devices. Each group is given a different VLAN ID which is used to mark the data frames exchanged within the group. Then, only devices configured to use the VLAN tag can communicate with other devices inside the group.

From a physical LAN interface in the product, you can define virtual interfaces that are used just like an independent physical LAN interface.

After creating the virtual interface, you must add it to a network to use it.

VLAN Interfaces overview:

This page displays the list of actual virtual interfaces created.

802.1Q VLAN INTERFACES OVERVIEW					
802.1Q TAGGING					
NAME	INTERFACE	VID	PRIORITY	ACTIONS	
VLAN5	LAN 1	5	Video (5)		
VLAN3	LAN 1	3	Voice (6)		
					

Click the **Remove** button to remove the virtual interface 

Click the **Edit** button to open the virtual interface configuration page 

Click the **Add tag** button to create a new virtual interface.

VLAN configuration:

802.1Q INTERFACE: VLAN5

In this page you can add a 802.1q tagging on one physical interface
For Wifi interface, you can create a VLAN interface only for Mesh and Client Role, this interface can then only be routed (it can not be bridged)

802.1Q TAGGING

General Setup | Filtering

VLAN description: VLAN5

Friendly name for your VLAN

VLAN ID: 5

VLAN priority: Video (level 5)

The priority that will be assigned to tagged egress traffic from this port

Interface:

- Ethernet adapter: LAN 1
- Ethernet adapter: LAN 2
- Wi-Fi adapter: WIFI 1 - RadioTest
- Wi-Fi adapter: WIFI 2 - acksys

VLAN description

Enter a friendly name for this interface (optional).

VLAN ID

Enter the id for virtual interface. If you need to create several VLAN IDs on top of the same physical interface, you can use the space character to separate the IDs.

Example: 5 10 120

VLAN priority

Select the priority that will be assigned to tagged egress traffic from this port.

Interface

Select the physical interface on which you create the virtual interface.

For Wi-Fi interface, you can create a VLAN interface only for Mesh and Client Role. This interface can then only be routed (it cannot be bridged with other interfaces).

802.1Q TAGGING

General Setup | Filtering

These filters are used only if this interface is bridged

Input filters group: No filtering

Output filters group: No filtering

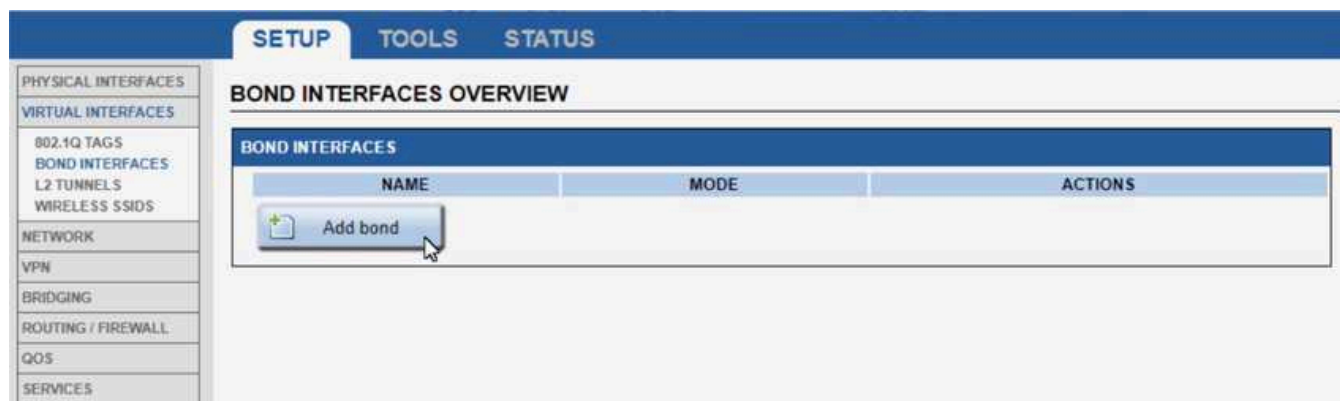
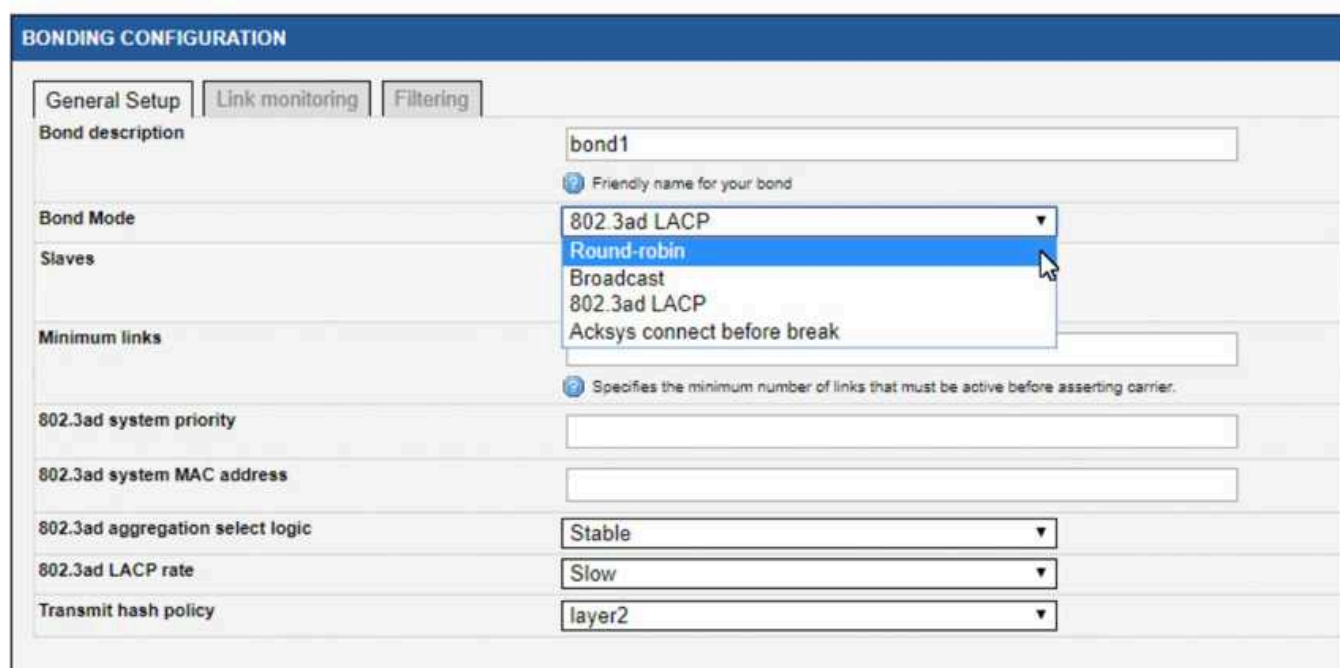
Input filter group/Output filter group:

Choose one of the filters prepared in routing/firewall/bridge filter section.

For more information about filters group, please see [Bridge filter](#)

VII.1.4.2 BOND INTERFACES

Bonding makes it possible to aggregate several network cards so as to increase bandwidth and have "high availability". A bonding interface is also created automatically when using Connect Before Break mode. Click **Add bond** to add a new bond interface.

Bond description:

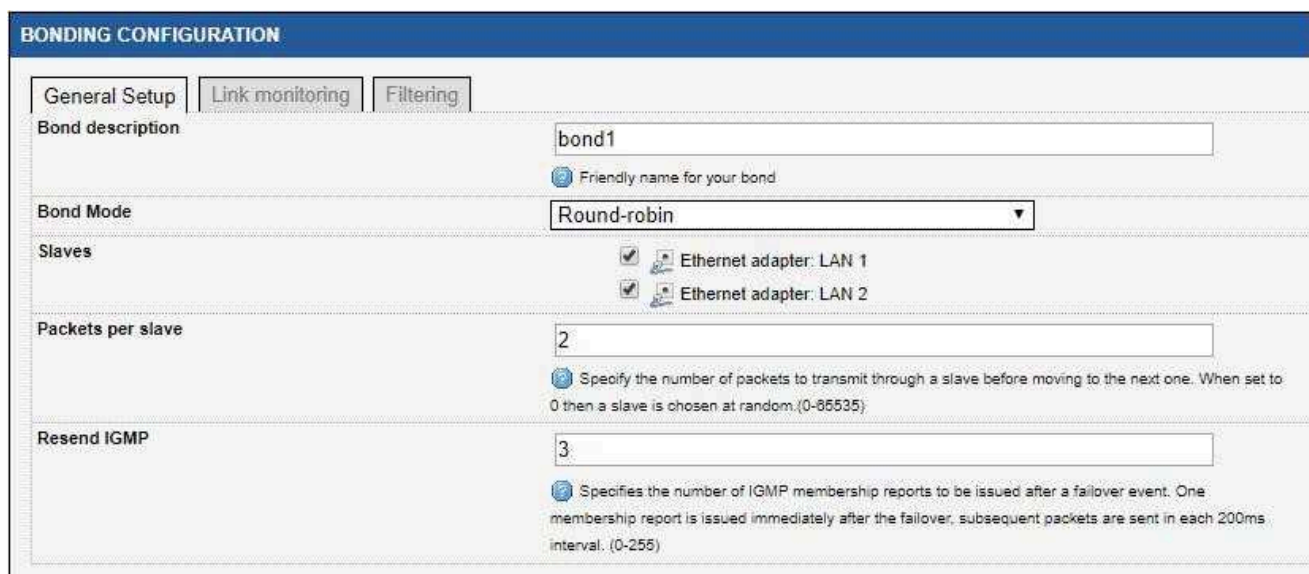
Symbolic name of you bond interface.

Bond Mode:

Selection of the required bond mode: Round Robin, Broadcast, 803.3ad LACP, Connect before break. These modes are described in the following pages.

Round-Robin Mode

Round-Robin mode is used for load balancing. The transmission of packets is done sequentially on each of the cards active in the aggregate. This mode increases bandwidth and manages fault tolerance.



The screenshot shows the 'BONDING CONFIGURATION' window with three tabs: 'General Setup', 'Link monitoring', and 'Filtering'. The 'General Setup' tab is active. It contains the following fields and options:

- Bond description:** A text field containing 'bond1'. Below it is a help icon and the text 'Friendly name for your bond'.
- Bond Mode:** A dropdown menu set to 'Round-robin'.
- Slaves:** Two checkboxes are checked: 'Ethernet adapter: LAN 1' and 'Ethernet adapter: LAN 2'.
- Packets per slave:** A text field containing '2'. Below it is a help icon and the text 'Specify the number of packets to transmit through a slave before moving to the next one. When set to 0 then a slave is chosen at random. (0-65535)'.
- Resend IGMP:** A text field containing '3'. Below it is a help icon and the text 'Specifies the number of IGMP membership reports to be issued after a failover event. One membership report is issued immediately after the failover, subsequent packets are sent in each 200ms interval. (0-255)'.

Slaves:

The two Ethernet interfaces (LAN 1 and LAN 2) must be selected.

Packets per slave:

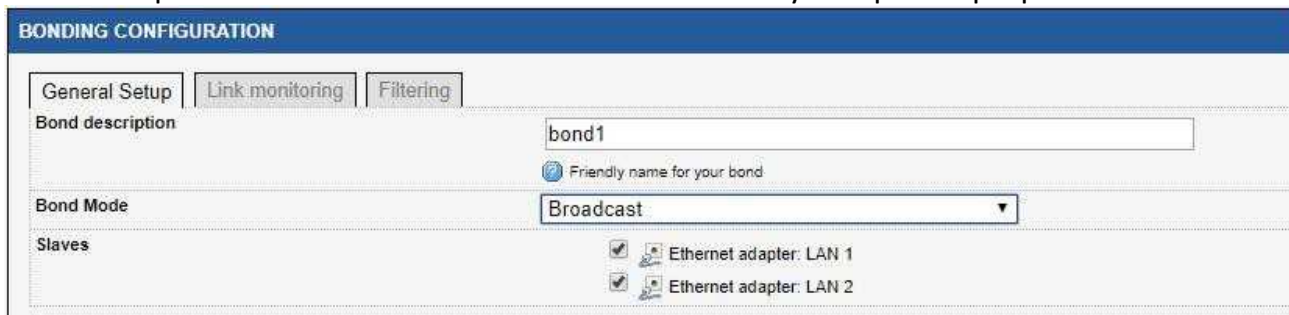
Specify the number of packets sent on a slave interface before moving to the next. The value can vary from 1 to 65535. The default value is 1. If you enter 0, the value will be chosen randomly.

Resend IGMP:

Specifies the number of IGMP membership reports to be issued after a failover event. One membership report is issued immediately after the failover, subsequent packets are sent in each 200ms interval. (0-255)

Broadcast Mode

This method is based on broadcast policy which consists in transmitting everything on all slave interfaces. It provides fault tolerance. This can be used only for specific purposes.



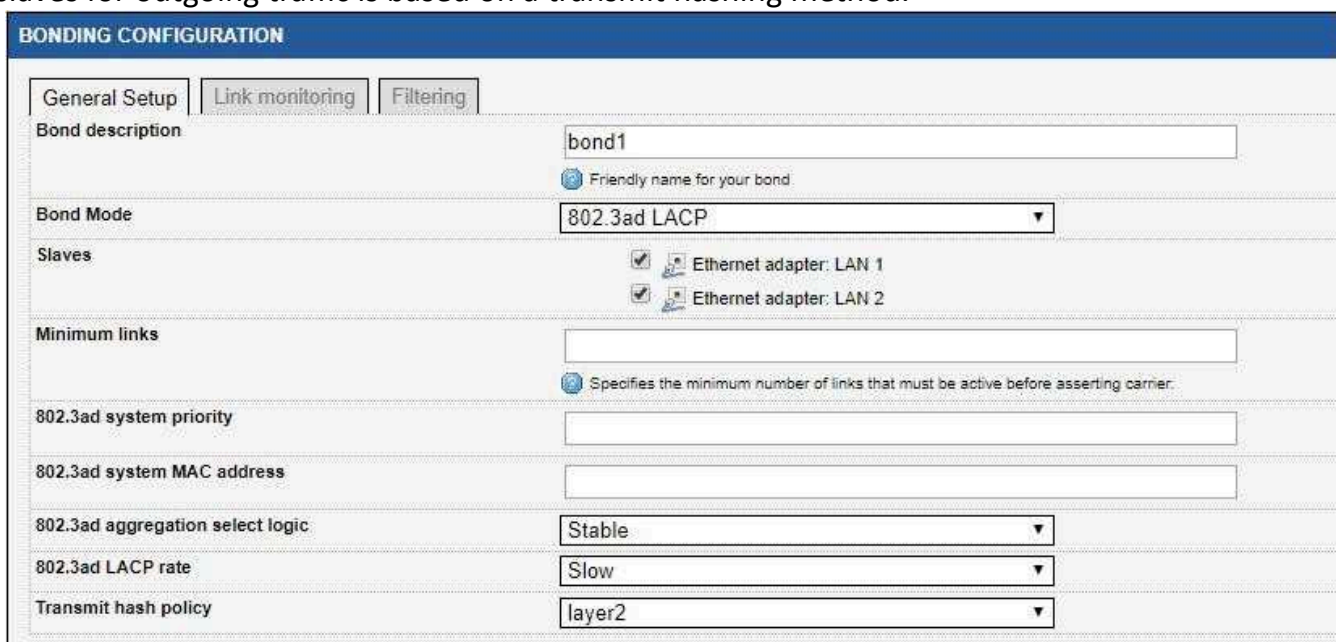
The screenshot shows the 'BONDING CONFIGURATION' window with the 'General Setup' tab selected. The 'Bond description' field contains 'bond1'. The 'Bond Mode' dropdown is set to 'Broadcast'. Under the 'Slaves' section, both 'Ethernet adapter: LAN 1' and 'Ethernet adapter: LAN 2' are checked.

Slaves:

The two Ethernet interfaces (LAN 1 and LAN 2) must be selected.

802.3ad LACP

This mode is known as Dynamic link aggregation mode which creates aggregation groups having the same speed. It requires a switch that supports IEEE 802.3ad dynamic link. The selection of slaves for outgoing traffic is based on a transmit hashing method.



The screenshot shows the 'BONDING CONFIGURATION' window with the 'General Setup' tab selected. The 'Bond description' field contains 'bond1'. The 'Bond Mode' dropdown is set to '802.3ad LACP'. Under the 'Slaves' section, both 'Ethernet adapter: LAN 1' and 'Ethernet adapter: LAN 2' are checked. The 'Minimum links' field is empty. The '802.3ad system priority' field is empty. The '802.3ad system MAC address' field is empty. The '802.3ad aggregation select logic' dropdown is set to 'Stable'. The '802.3ad LACP rate' dropdown is set to 'Slow'. The 'Transmit hash policy' dropdown is set to 'layer2'.

Minimum links:

Specifies the minimum number of physical links that must be active for the bonding interface carrier to be mounted. The default value is 1 and must remain at 1.

802.3ad system priority:

Allows to define the priority of the link, which will be managed by the 802.3ad switch. The highest priority is 1, and the lowest 65535. The default is 65535.

802.3ad system MAC address:

By default, the virtual MAC address of the bonding interface is used. This field allows to define another value.

802.3ad aggregation select logic:

Specifies the 802.3ad aggregation selection logic to use. The possible values and their effects are:

Stable The active aggregator is chosen by largest aggregate bandwidth. Reselection of the active aggregator occurs only when all slaves of the active aggregator are down or the active aggregator has no slaves.

Bandwidth The active aggregator is chosen by largest aggregate bandwidth. Reselection occurs if:

- A slave is added to or removed from the bond
- Any slave's link state changes
- Any slave's 802.3ad association state changes
- The bond's administrative state changes to up

Count The active aggregator is chosen by the largest number of ports (slaves). Reselection occurs as described under the "bandwidth" setting, above.

The bandwidth and count selection policies permit failover of 802.3ad aggregations when partial failure of the active aggregator occurs. This keeps the aggregator with the highest availability (either in bandwidth or in number of ports) active at all times.

802.3ad LACP rate:

Option specifying the rate at which we will ask our link partner to transmit LACPDU packets in 802.3ad mode. The possible values are

- **Slow** : Request partner to transmit LACPDUs every **30 seconds**
- **Fast** : Request partner to transmit LACPDUs every **1 second**

Transmit hash policy:

This parameter allows to define the strategy that will be used to choose which port will be selected for each type of exchange:

Layer2 All bonding ports are used if the data flow consists of packets with different source MAC addresses or different destination MAC addresses.

Layer2+3 All bonding ports are used if the data flow consists of packets with different source MAC addresses or different destination MAC addresses, or different source IP addresses or different destination IP addresses

Layer3+4 All bonding ports are used if the data flow consists of packets with different MAC source addresses or different MAC address destinations, different

source IP addresses or different destination IP addresses, different source ports or different destination ports

Encap2+3 Same as Layer 2+3, but if we detect that the packet is encapsulated in a tunnel protocol (GRE for example), data will be extracted from the tunnel to be processed

Encap3+4 Same as Layer 3+4, but if we detect that the packet is encapsulated in a tunnel protocol (GRE for example), data will be extracted from the tunnel to be processed

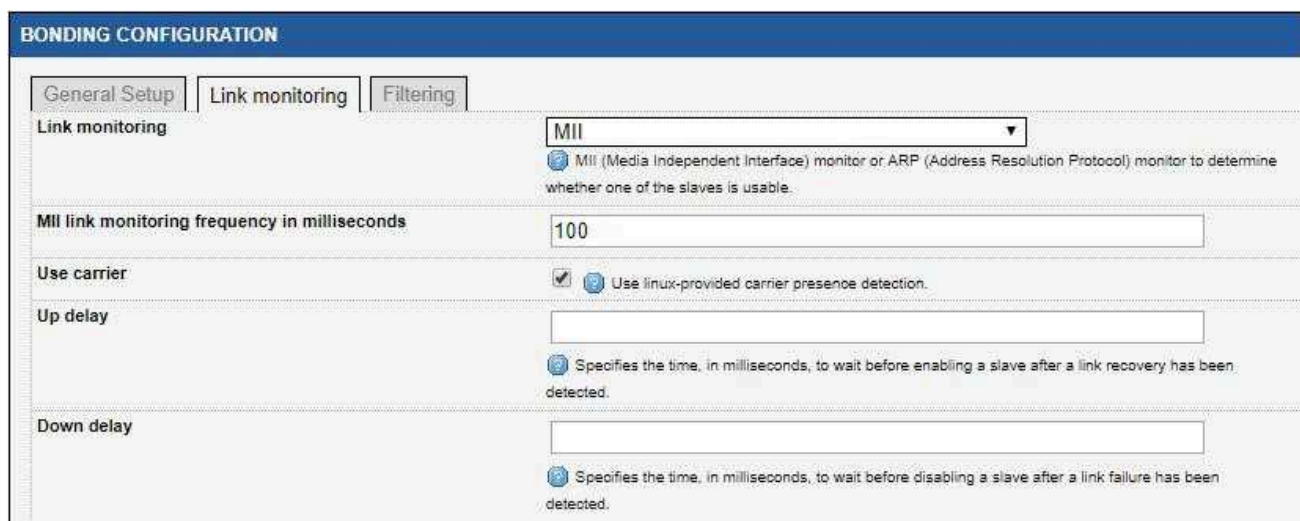
Connect before break

The bond for connect before break is usually created via the *SETUP/Physical interface* page, please refer to [Global parameters/Cluster Mode](#)



Link monitoring using MII

The Link Monitoring tab is used to define the parameters for monitoring the links of the slave ports of the bonding interface. When choosing the MII option, the physical link of the interfaces is tested



MII link monitoring frequency in milliseconds:

Defines the frequency at which the physical link of each port is tested. Default is 100ms.

Up delay:

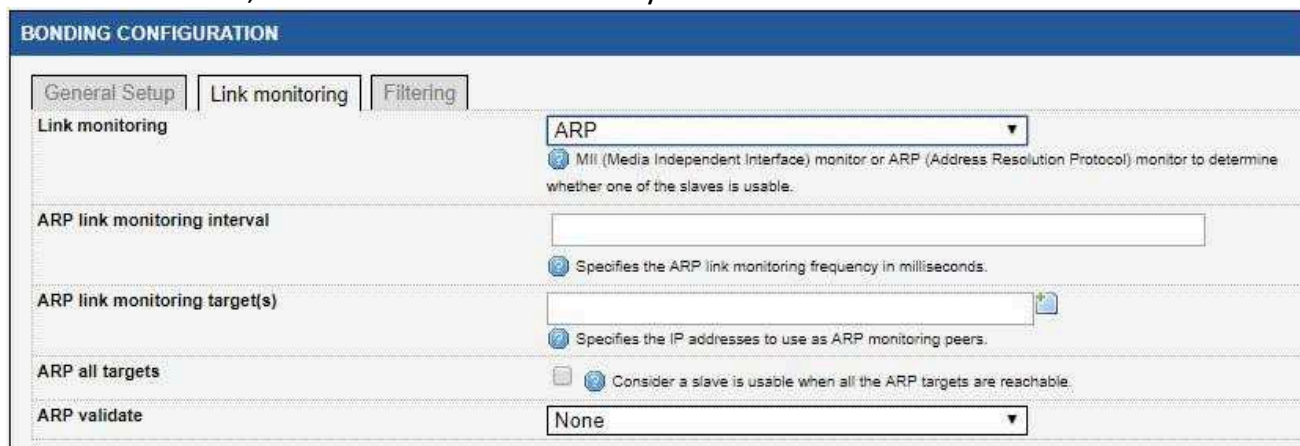
Specifies the time, in milliseconds, to wait before enabling a slave port, after detection of the recovery of the physical link.

Down delay:

Specifies the time, in milliseconds, to wait before disabling a slave port, after detection of a physical link failure.

Link monitoring using ARP (only in Round Robbin or Broadcast mode)

In this case, the control of the continuity of the links is based on ARP traffic.



The screenshot shows the 'BONDING CONFIGURATION' window with the 'Link monitoring' tab selected. The 'Link monitoring' section has a dropdown menu set to 'ARP'. Below it, there is a text box for 'ARP link monitoring interval' and a text box for 'ARP link monitoring target(s)'. The 'ARP all targets' checkbox is checked. The 'ARP validate' dropdown menu is set to 'None'.

ARP link monitoring interval:

Specifies the time intervals at which ARP requests are sent, in milliseconds.

ARP link monitoring target(s):

Here we define the IP addresses to which we must send ARP requests to monitor the links.

ARP all targets:

If this box is checked, it means that a slave will be considered usable only if all the specified IP addresses respond to the ARP requests.

ARP validate:

Here we define the criteria that will allow to decide if an interface is usable. The slave interface which gave its MAC address to the bonding interface is called the **active interface**. The other slaves are called **backup interfaces**. The different options are:

None: (default): We check if there has been incoming and outgoing ARP traffic recently on the interface to determine if it is usable

Active: We look if there has been incoming and outgoing ARP traffic recently on the interface, and for the active interface, we examine the content of incoming and outgoing ARP

Backup: We check if there has been incoming and outgoing ARP traffic recently on the interface, and for the backup interface, we examine the content of incoming and outgoing ARP

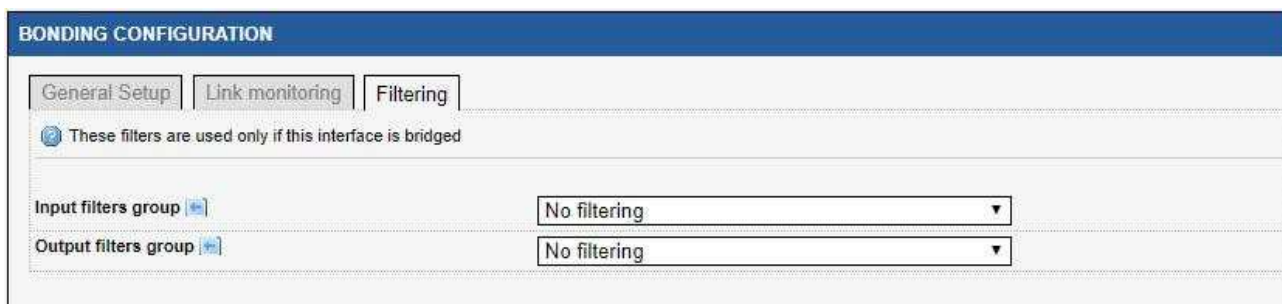
All: We examine all ARPs on all bonding interfaces to determine if they are usable.

Filter: We check if there has been recent ARP traffic entering the interface to determine if it is usable

Filter active: We check if there has been recent incoming ARP traffic on the interface, and for the active interface, we examine the content of incoming and outgoing ARPs.

Filter backup: We check if there has been incoming ARP traffic recently on the interface, and for the backup interface, we examine the content of incoming and outgoing ARPs.

Filtering tab



The screenshot shows the 'BONDING CONFIGURATION' window with the 'Filtering' tab selected. It contains three sub-tabs: 'General Setup', 'Link monitoring', and 'Filtering'. A note states: 'These filters are used only if this interface is bridged'. Below this, there are two rows: 'Input filters group' and 'Output filters group'. Each row has a dropdown menu currently set to 'No filtering'.

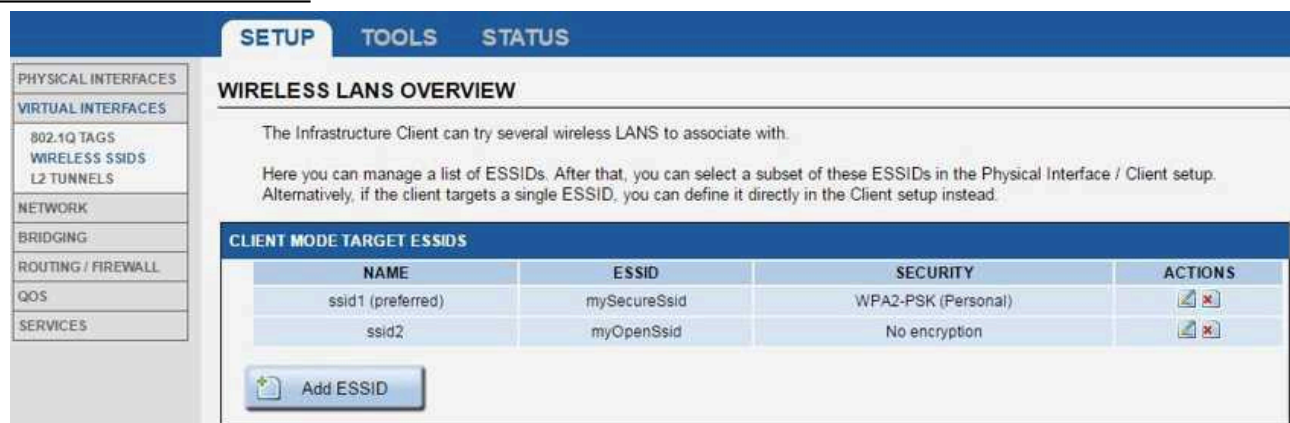
Input filter group/Output filter group:

Choose one of the filters prepared in routing/firewall/bridge filter section.
For more information about filters group, please see [Bridge filter](#)

VII.1.4.3 Wireless SSIDs

The wireless SSID section is used to configure several SSIDs and enable them on the client role of the Wireless interface.

Wireless SSID overview



SETUP TOOLS STATUS

WIRELESS LANs OVERVIEW

The Infrastructure Client can try several wireless LANs to associate with.

Here you can manage a list of ESSIDs. After that, you can select a subset of these ESSIDs in the Physical Interface / Client setup. Alternatively, if the client targets a single ESSID, you can define it directly in the Client setup instead.

CLIENT MODE TARGET ESSIDS			
NAME	ESSID	SECURITY	ACTIONS
ssid1 (preferred)	mySecureSsid	WPA2-PSK (Personal)	 
ssid2	myOpenSsid	No encryption	 

 Add ESSID

Use the  Add ESSID button to add a SSID specification

Use  button to edit the parameters, use  to suppress an SSID specification

Wireless SSID configuration



SETUP TOOLS STATUS

SSID1

ESSID CONFIGURATION

WLAN description
 Friendly name for this wireless LAN. Mandatory field.

ESSID
 Mandatory field.

Priority group
 You can set several ESSIDs to the same priority.

BSSID
 Optional. MAC address format as 6 pairs of column-separated hex digits.
BSSID (MAC address) of the AP if you want to restrict association to one AP only.

Security

Deauthenticate before roaming to next AP ☒  Optional. When ON, the previous AP stops transmission immediately, saving up bandwidth. When OFF, let more time for the AP controller to manager handover.

WLAN description (optional):

Enter a friendly name for this SSID.

ESSID:

Network name (also called SSID).

Priority group:

The scan process will choose the AP with the SSID of highest priority. If you have several APs advertising SSIDs of the same priority, the AP with the best signal will be chosen.

BSSID (optional):

Set the BSSID of the AP if you want to restrict association to one AP only.

Security:

Select the security policy. For more information on the security parameter please read the section [Wireless Security tab](#):

VII.1.4.4 L2 Tunnels

In this section, you can configure Layer 2 tunneling with GRE.

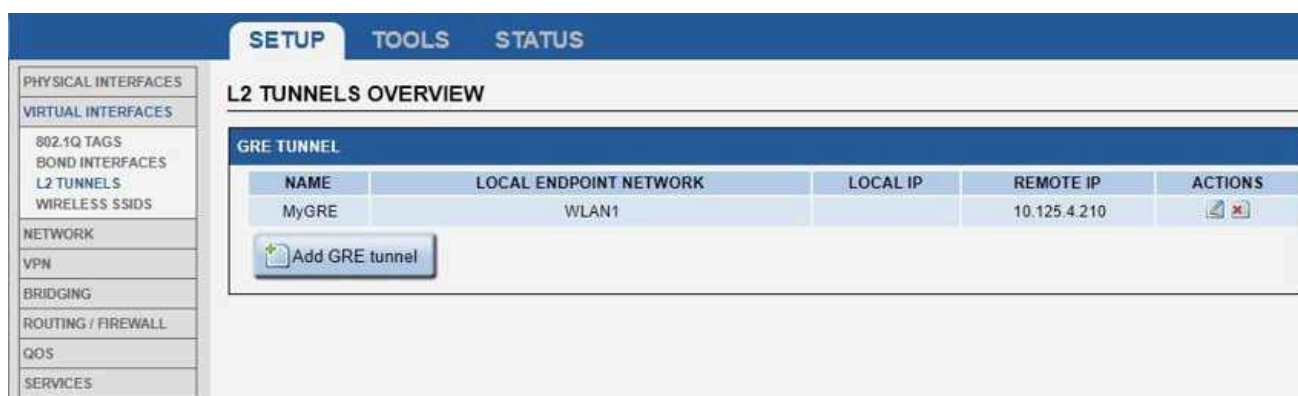
The GRE encapsulation adds L2, L3 and GRE headers to the original L2 frame. This overhead will reduce the network MTU (Because the L2 frame is limited to 1524 octets on 802.3 networks).

NOTE: The 802.11 networks support a larger frame than 802.3 networks. If your GRE tunnel traverses 802.11 networks only, it is recommended to increase the MTU on the GRE interface and the network bearing the 802.11 physical interface, to allow using the maximum 802.3 MTU for the original L2 frame.

For example, setting the GRE and WiFi interfaces MTU to 2000 is sufficient to encapsulate frame sizes up to the 802.3 MTU.

L2 TUNNELS Overview

In this page, you can create a GRE tunnel:



Use  button to add GRE interface

Use  button to edit GRE tunnel parameters

Use  button to suppress GRE tunnel

GRE TUNNEL configuration page

In this page, you can configure the GRE tunnel

General Setup tab

GRE TUNNEL

General Setup

Filtering

GRE interface description

GRE protocol version

Remote IP V4

MTU

Network

QoS

Local GRE endpoint

Local endpoint Network

Static route to remote GRE endpoint

Friendly name for your GRE

This remote IP is used to find the remote GRE endpoint

☒ lan:

☐ VLAN1:

☐ VLAN2:

☐ WLAN0:

Choose the network you want to attach this GRE interface to.

Choose the network you want to bind with the local GRE endpoint

☒ Enable static route to join remote GRE endpoint via the Local endpoint Network.

WARNING: This option is mandatory when Local endpoint Network has no IP address configured and that it will be affected later a virtual IP address by a network services ex: VRRP.

GRE interface description

Friendly name for your GRE interface

GRE protocol version

Always GRE IPV4

GRE Remote IPV4

IP of the remote endpoint of the tunnel

MTU (Maximum transmit unit)

The maximum size of L2 frames encapsulated in the GRE tunnel

Network

Add GRE tunnel interface in selected network.

Local GRE endpoint

Choose between:

- **Configure with IP V4 address**
- ❖ **Local IP V4:** This local IP is used to find the local GRE endpoint.

WARNING: if this IP is not valid when GRE interface is created, tunnel will be routed via a default Gateway. This case can be encountered when this IP correspond to the IP of a wireless interface or a virtual interface that is created after the GRE tunnel.

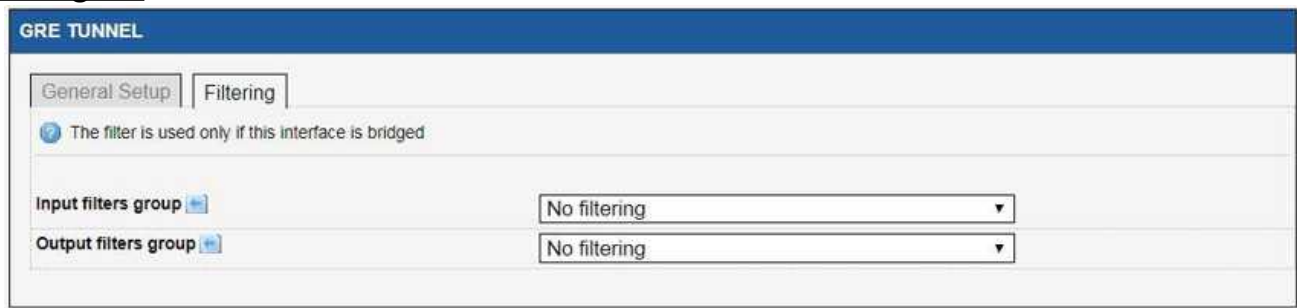
The solution is instead of using a local IP for the local endpoint configuration, we bind the Local endpoint of the tunnel to a Network that contains the given interface with the given IP (see section below).

➤ **Configure with Network:**

- ❖ **Local endpoint Network:** Choose the network you want to bind with the local GRE endpoint
- ❖ **Static route to remote GRE endpoint:** Enable static route to join remote GRE endpoint via the Local endpoint Network.

WARNING: This option is mandatory when Local endpoint Network has no IP address configured and that it will be affected later a virtual IP address by a network services ex: VRRP.

Filtering tab



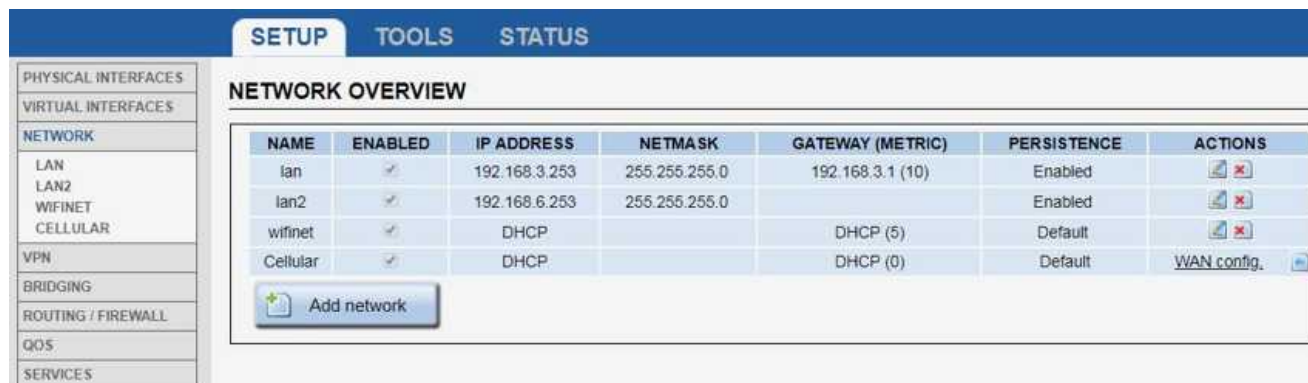
The screenshot shows the 'GRE TUNNEL' configuration window with the 'Filtering' tab selected. It includes a note: 'The filter is used only if this interface is bridged'. Below this, there are two rows: 'Input filters group' and 'Output filters group', each with a dropdown menu currently set to 'No filtering'.

Input filter group/Output filter group:

Choose one of the filters prepared in routing/firewall/bridge filter section.
For more information about filters group, please see [Bridge filter](#)

VII.1.5 Network

This page displays the current network configuration.



NAME	ENABLED	IP ADDRESS	NETMASK	GATEWAY (METRIC)	PERSISTENCE	ACTIONS
lan	☒	192.168.3.253	255.255.255.0	192.168.3.1 (10)	Enabled	
lan2	☒	192.168.6.253	255.255.255.0		Enabled	
wifinet	☒	DHCP		DHCP (5)	Default	
Cellular	☒	DHCP		DHCP (0)	Default	WAN config.

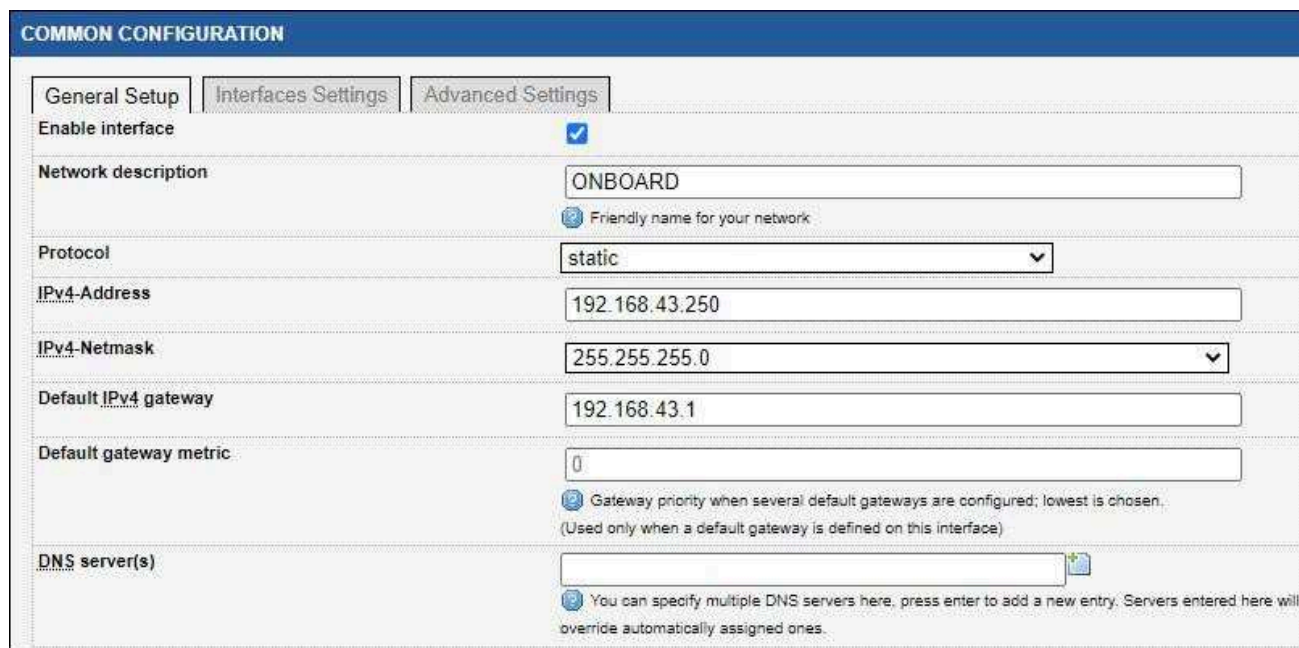
Click the **Remove**  button to remove the network.

Click the **Edit**  button to open the network configuration page.

Click the **Add network** button to create a new IP network.

VII.1.5.1 Network configuration

General setup:



COMMON CONFIGURATION

General Setup | Interfaces Settings | Advanced Settings

Enable interface ☒

Network description:
 Friendly name for your network.

Protocol:

IPv4-Address:

IPv4-Netmask:

Default IPv4 gateway:

Default gateway metric:
 Gateway priority when several default gateways are configured; lowest is chosen.
 (Used only when a default gateway is defined on this interface)

DNS server(s):
 You can specify multiple DNS servers here, press enter to add a new entry. Servers entered here will override automatically assigned ones.

Enable interface

This checkbox allows you to temporarily disable the LAN interface without losing your configuration.

Network description

Friendly name for your network.

Protocol

Choose **DHCP** if you have a DHCP server in the network and you want to assign an IP address to the device. In this case, you do not need to fill in the fields shown above except possibly **DNS-Server**

Choose **static** if you do not have a DHCP server in the network or if, for any other reason, you need to assign a fixed address to the interface. In this case, you must also configure the fields shown below.

Note that you cannot choose **DHCP** if you have enabled the **DHCP Server** option on the DHCP page; the AP cannot be both a DHCP client and a DHCP server.

IPv4-Address (only in static mode)

The IP address of the AP on the local area network. Assign any unused IP address in the range of IP addresses available for the LAN. For example, 192.168.0.1.

IPv4-Network (only in static mode)

The subnet mask of the local area network.

Default IPv4-Gateway (only in static mode)

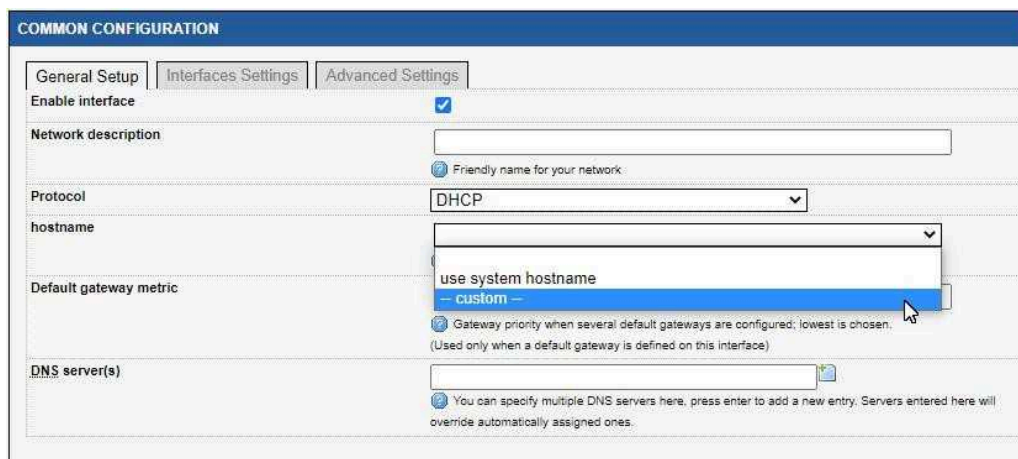
The IP address of the router on the local area network. Use 0.0.0.0 if no gateway is defined.

Default Gateway Metric

When several Networks are configured, with their own gateway, the *Default Gateway Metric* allows to introduce a priority between these gateways. The gateway with the lowest Metric will be chosen.

DNS-Server:

The IP addresses of the DNS server(s) you want to use. If you selected the DHCP protocol, you can choose to use the value defined in the menu TOOLS/System, or you can define a new Hostname, specific to this network.



COMMON CONFIGURATION

General Setup | Interfaces Settings | Advanced Settings

Enable interface ☒

Network description

Protocol **DHCP**

hostname **use system hostname** **custom**

Default gateway metric

DNS server(s)

Gateway priority when several default gateways are configured; lowest is chosen. (Used only when a default gateway is defined on this interface)

You can specify multiple DNS servers here, press enter to add a new entry. Servers entered here will override automatically assigned ones.

IP Alias:

IP aliases can be useful if you need an access to your device from different networks, for example when your product is configured in router mode, and acts as a gateway for different subnets

IP ALIASES

NATed VRRP networks warning
The following applies to NATed networks which use the VRRP protocol:

- Public-side NAT MUST NOT define IP aliases; else the NAT might use the alias IP as public address instead of the VRRP IP
- Conversely, Private-side NAT SHOULD define a private IP alias to allow connection tracking replication



To add an IP alias, enter a mnemonic and click Add, then enter the desired IP address, and the associated subnet mask.

IP ALIASES

NATed VRRP networks warning
The following applies to NATed networks which use the VRRP protocol:

- Public-side NAT MUST NOT define IP aliases; else the NAT might use the alias IP as public address instead of the VRRP IP
- Conversely, Private-side NAT SHOULD define a private IP alias to allow connection tracking replication

CONTROL 

General Setup

IPv4-Address

192.168.1.250

IPv4-Netmask

255.255.255.0

CAMERAS 

General Setup

IPv4-Address

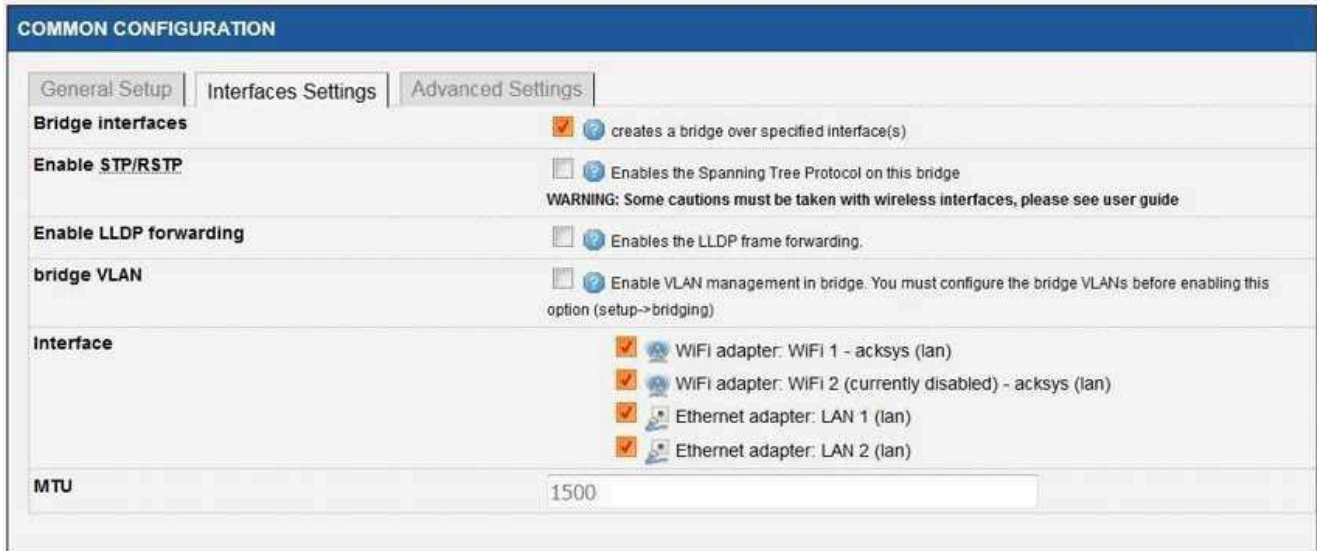
192.168.2.8

IPv4-Netmask

255.255.255.0



Interfaces Settings:



COMMON CONFIGURATION

General Setup | **Interfaces Settings** | Advanced Settings

Bridge interfaces ☒ creates a bridge over specified interface(s)

Enable STP/RSTP ☐ Enables the Spanning Tree Protocol on this bridge
WARNING: Some cautions must be taken with wireless interfaces, please see user guide

Enable LLDP forwarding ☐ Enables the LLDP frame forwarding.

bridge VLAN ☐ Enable VLAN management in bridge. You must configure the bridge VLANs before enabling this option (setup->bridging)

Interface

- ☒ WiFi adapter: WiFi 1 - acksys (lan)
- ☒ WiFi adapter: WiFi 2 (currently disabled) - acksys (lan)
- ☒ Ethernet adapter: LAN 1 (lan)
- ☒ Ethernet adapter: LAN 2 (lan)

MTU 1500

Bridge interfaces:

If checked, all interfaces in this network are linked with the software equivalent of an Ethernet switch.

Enable STP/RSTP:

If checked, the STP/RSTP (Spanning Tree Protocol) will be activated on this bridge. If you choose to not use STP/RSTP, you have to set up your devices to avoid network loops by yourself.



Some cautions must be taken with wireless interfaces, please see [Spanning Tree Protocols \(STP, RSTP\)](#).

Enable LLDP forwarding:

Check this box if the internal bridge must forward the LLDP Multicast frame.

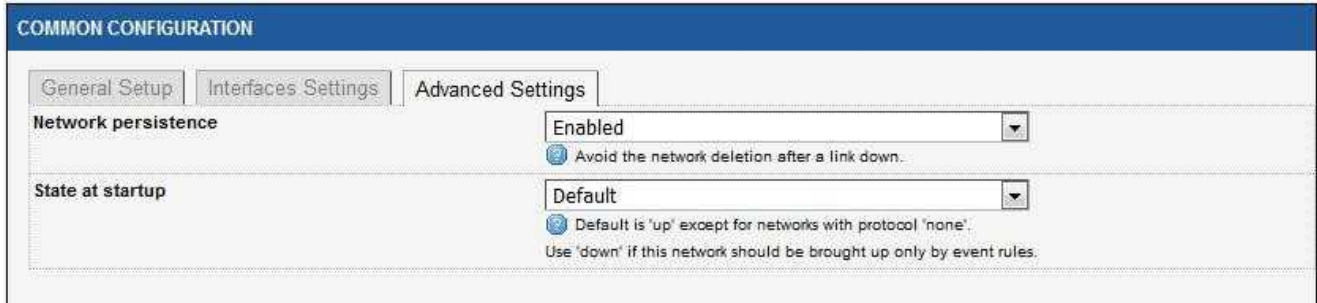
Bridge VLAN:

Enable VLAN management in the bridge. Please see: [Vlan Management](#)

Interface:

This is the list of available network interfaces. Disabled (greyed) interfaces are already used in another network. For bridge networks, select all the interfaces you want to bridge together into the LAN being configured. For simple networks, select the one interface to configure.

Advanced Settings:



COMMON CONFIGURATION

General Setup | Interfaces Settings | **Advanced Settings**

Network persistence Enabled
Avoid the network deletion after a link down.

State at startup Default
Default is 'up' except for networks with protocol 'none'.
Use 'down' if this network should be brought up only by event rules.

Network Persistence:

When this option is enabled, the IP setting (routes, gateway, virtual interfaces, etc.) remains persistent when the physical interface loses its connection. This makes it possible, for example, to avoid systematic sending of DHCP requests when an interface loses the link.

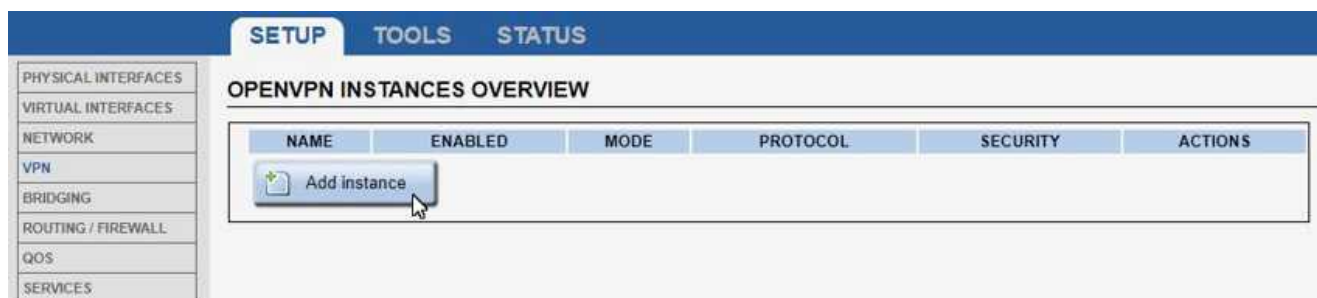
Default value is *enabled* for static protocol (fixed IP) and *disabled* for all the other protocols (DHCP, VRRP).

State at startup

Gives the network status at startup. The default state is "Up", except for networks whose protocol is "none". Use "Down" only if this network is to be activated by an event

VII.1.6 VPN

This page allows to create a VPN interface



NAME	ENABLED	MODE	PROTOCOL	SECURITY	ACTIONS
Add instance					

To create a new VPN instance, click on **Add instance**, this will open the OpenVPN configuration page.

OPENVPN Configuration

OPENVPN - VPN1

OpenVPN can work in server mode, waiting for a number of clients to call in, or in client mode, where it connects to a predefined OpenVPN server address.

CONFIGURATION

Tunnel settings	Auth/Crypto	Client settings
Enable virtual network	☒	
State at startup	Default	
<small>Default is 'up' except for networks with protocol 'none'. Use 'down' if this network should be brought up only by event rules.</small>		
OpenVPN instance description	vpn1	
<small>Friendly name for this VPN instance</small>		
Role	Client (calling)	
Protocol	UDP	
<small>Favor UDP, as TCP leads to potential conflicts in the TCP over TCP redundancy mechanisms</small>		
Listener port	1194	
<small>UDP or TCP port that the server will listen to, and that the client will call</small>		
Data channel compression	☐ Use fast LZO compression	
Tunnel type	L3 (IP) tunnel	
<small>Only L3 tunnels are supported</small>		
VPN subnet local IP address	10.8.0.1	
<small>IP address of the local VPN endpoint, not used in TLS client mode since it is pulled from server</small>		
VPN subnet mask	255.255.255.0	
<small>Subnet mask of the VPN subnet, not used in TLS client mode</small>		
Tunnel MTU	1500	
<small>Encapsulated MTU, adjust to avoid fragmentation; the default of 1412 allows the default SHA1 digest</small>		
Keepalive period	10	
<small>Keepalive period (seconds). Every such time, a packet is sent to each peer to elicit a response.</small>		
Keepalive timeout	30	
<small>Keepalive timeout (seconds). Connection terminates if no traffic is received from the peer for such time.</small>		

State at startup

Gives the VPN network status at startup. The default state is "Up", except for networks whose protocol is "none". Use "Down" only if this network should be brought up only by event rules.

OpenVPN instance description

This is the friendly name you give to this VPN instance.

Role

The role can be Server or Client. The server waits for clients to call in. The Client calls the server to initiate the connection.

Protocol

Protocol can be UDP or TCP. Favor UDP, as TCP leads to potential conflicts in the TCP over TCP redundancy mechanisms. You must ensure that the routers between the Client and the Server open the ports necessary to authorize the packets of the selected format.

Listener port

This is the UDP or TCP port listened by the Server, waiting for a Client to call. Default is 1194.

Data channel compression

Check this box if you want the data passing through the tunnel to be compressed. Fast LZO compression is used.

Tunnel Type

Only L3 tunnels are supported.

VPN subnet local IP address

Virtual IP address of this VPN endpoint.

VPN subnet mask

The subnet mask associated to the IP address of this VPN endpoint.

Tunnel MTU

Encapsulated MTU, should be adjusted to avoid fragmentation; the default of 1419 bytes allows the default SHA1 digest.

Keepalive period

The keepalive mechanism verifies that the VPN link is always valid. A probe is sent by each peer at the frequency defined by this parameter. The keepalive period is given in seconds.

Keepalive timeout

This is the Keepalive timeout value, in seconds. The connection is closed if no packet is received for a period longer than this period of time. The **Keepalive timeout** value must be greater than the **Keepalive period**

LOCAL ROUTES

LOCAL ROUTES

This section is used in both Server and Client modes. It lists the routes to be installed in the local IP stack.

- In the client, it lists the server subnets reachable using the server as gateway,
- In the server, it lists the client subnets reachable using the client as gateway.

If the gateway is not indicated, it defaults to the VPN remote address.

TARGET NET	NETMASK	GATEWAY	METRIC	SORT
192.168.23.0	255.255.255.0	10.8.0.2	Default: 0	<div> <div>↑</div> <div>↓</div> <div>✖</div> </div>


Add

This section allows to define the routes to be installed in the local IP stack.

TARGET NET:

Destination subnet.

NETMASK:

Destination subnet mask.

GATEWAY:

The gateway that must be used to reach the target network. If left blank, the gateway defaults to the VPN remote address.

METRIC:

Sets the metric for this route.

USERS VALIDATION

USERS VALIDATION

This section is used in Server mode only; it lists users allowed to connect to this VPN instance. Optionally you can enable routing from the server to a client-side subnet.

USERNAME	PASSWORD	SUBNET	NETMASK	DESCRIPTION	SORT
Acksys		 Client subnet		Allowed user	<div> <div>↑</div> <div>↓</div> <div>✖</div> </div>


Add

This section is used in Server mode only; it lists users allowed to connect to this VPN instance. Optionally you can enable routing from the server to a client-side subnet.

CLIENTS ROUTES

CLIENTS ROUTES

This section is used in Server mode only. It lists the routes enforced by the server in the client at connection time. If the gateway is not indicated, it defaults to the server's address.

TARGET NET	NETMASK	GATEWAY	METRIC	SORT
This section contains no values yet				

 Add

This section is used in Server mode only. It lists the routes enforced by the server in the client at connection time. If the gateway is not indicated, it defaults to the server's address.



Warning, the routes can only be enforced by the server with TLS VPN authentication: you must choose **PKI certificate** in the **Auth/Crypto** tab described below.

AUTH/CRYPTO

These pages allow define the credentials, encryption and authentication methods for your VPN tunnel. For more information about the definitions of these fields, please refer to the OpenVPN documentation:

<https://community.openvpn.net/openvpn/wiki/SecurityOverview>

CONFIGURATION

Tunnel settings

Auth/Crypto

Client settings

Key type

PKI certificate

Root CA certificate

Choisir un fichier

Aucun fichier choisi

Root CA certificate (PEM file format). WARNING: Synchronize time between server and clients!

Local certificate

Choisir un fichier

Aucun fichier choisi

Local certificate (PEM file format)

Local private key

Choisir un fichier

Aucun fichier choisi

Local private key (PEM file format)

Revoked certificates list

Choisir un fichier

Aucun fichier choisi

CA-issued list of revoked certificates

TLS channel HMAC protection

Choisir un fichier

Aucun fichier choisi

Optional additional TLS channel HMAC protection

Authenticate using username/password

☐

Check client username/password against predefined server list

Data channel encryption algorithm

AES-256

Data channel encryption algorithm. The chosen algorithm must be supported at both sides of the VPN.

Data channel authentication digest

SHA1 (OpenVPN default)

Data channel authentication algorithm. Adds overhead to frames size and processing time.

CONFIGURATION

Tunnel settings

Auth/Crypto

Client settings

Key type

Pre-shared key (entails P2P operation)

Data channel encryption algorithm

AES-256

Data channel encryption algorithm. The chosen algorithm must be supported at both sides of the VPN.

Data channel authentication digest

SHA1 (OpenVPN default)

Data channel authentication algorithm. Adds overhead to frames size and processing time.

Pre-shared key

Choisir un fichier

Aucun fichier choisi

Pre-shared key (PEM file format)

CONFIGURATION

Tunnel settings

Auth/Crypto

Client settings

Key type

No key (entails P2P, cleartext, no auth)

Data channel authentication digest

SHA1 (OpenVPN default)

Data channel authentication algorithm. Adds overhead to frames size and processing time.

Client settings

CONFIGURATION

Tunnel settings

Auth/Crypto

Client settings

Remote OpenVPN server address

110.25.250.16

Remote OpenVPN server address

Remote OpenVPN server address:

This is the remote OpenVPN server address.

Server settings

CONFIGURATION

Tunnel settings

Auth/Crypto

Server settings

Maximum number of simultaneous clients

Maximum number of simultaneous clients

Maximum number of simultaneous clients:

This setting allows you to limit the number of clients that can connect to your server simultaneously. This allows to optimize the use of the physical resources of your product.

VII.1.7 Bridging

In this section, you can configure the bridging services integrated in your product.

VII.1.7.1 STP/RSTP

In this section, you can configure STP/RSTP for your Network Ports and Bridges.
To configure STP/RSTP on a given Network, Bridge must be enabled.

STP/RSTP overview

NETWORK	BRIDGE STATUS	STP/RSTP STATUS	BRIDGED INTERFACE	ACTIONS
Ian	Enabled	Disabled	WiFi adapter: WiFi 1 - Acksys WiFi adapter: WiFi 2 - Service Ethernet adapter: LAN 1 Ethernet adapter: LAN 2	

Click edit button  to change the STP/RSTP parameters for the given bridged network

STP/RSTP Bridge settings

BRIDGE SETTINGS	
Max age	<input type="text" value="20"/>  The range is 6 to 40s
Forward delay	<input type="text" value="15"/>  The range is 4 to 30s and must have: $2 * (\text{Forward Delay} - 1 \text{ second}) \geq \text{Max Age}$
Max hops	<input type="text" value="20"/>  The range is 6 to 40
Hello time	<input type="text" value="2"/>  The range is 1 to 10s
Hold count	<input type="text" value="6"/>  The range is 1 to 10
Priority	<input type="text" value="8"/>  The range is 0 to 15 (802.1d values divided by 4096)

Max age

The maximum age of the information transmitted by the Root Bridge.

Forward delay

The delay to transition Root and Designated Ports from Discarding to Learning or from Learning to Forwarding states.

Max hops

The maximum number of hops the BPDU can be forwarded.

Hello time

The interval between periodic transmissions of Configuration Messages by Designated Ports.

Hold count

The maximum number of BPDUs that can be sent in one second

Priority

Bridge priority in the STP/RSTP topology, the range is 0 to 15, with 0 the highest priority and 15 the smallest one. It will permit to select the root bridge.

STP/RSTP Port settings

PORT SETTINGS					
INTERFACE	PATH COST	EDGE PORT	BPDU GUARD	P2P MAC	PRIORITY
<small>The range is 0 to 200000000, 0 is for auto</small> <small>Range: 0 to 15 (802.1d values divided by 16)</small>					
WiFi 2 (currently disabled) - acksys	0	auto	false	auto	8
WiFi 1 - acksys	0	auto	false	auto	8
LAN 1	0	auto	false	auto	8
LAN 2	0	auto	false	auto	8

Path Cost

The Port's contribution, when it is the Root Port, to the Path Cost to reach the Root Bridge. When set to 0, the value will be calculated automatically depending on the port speed. The port offering the lowest cost to the root bridge will become the root port, and all other redundant paths will be placed into blocking state.

Edge Port

Initial edge state of the port. If set to true, initial state will be set to edge port, if set to false, the initial state will be set to non-edge port, and if set to auto, the product will detect automatically the port type. The RSTP will make transition the edge ports directly to forwarding state.

BPDU Guard

Set it to true on edge ports (port attached to a LAN with no other bridge attached), if you want the port to be disabled upon the reception of a BPDU.

P2P Mac

This will set the initial point-to-point link state. If set to true, the initial link state will be set to point-to-point link (Direct link between two bridges (without an intermediate equipment like a hub between the two bridges)), this will help designated port to transition faster to forwarding state. If set to auto, the product will detect automatically the link type

Priority

Port priority inside the bridge. If in the bridge, several ports offer the same path cost, STP/RSTP will use the port priority to elect the root port. The range is 0 to 15, with 0 the highest priority and 15 the smallest one.

VII.1.7.2 Vlan Management

In this page you can manage the 802.1q tagging on the bridged ports.

For each interface included in a bridge you can specify the supported VLANs.

VLAN Interfaces overview

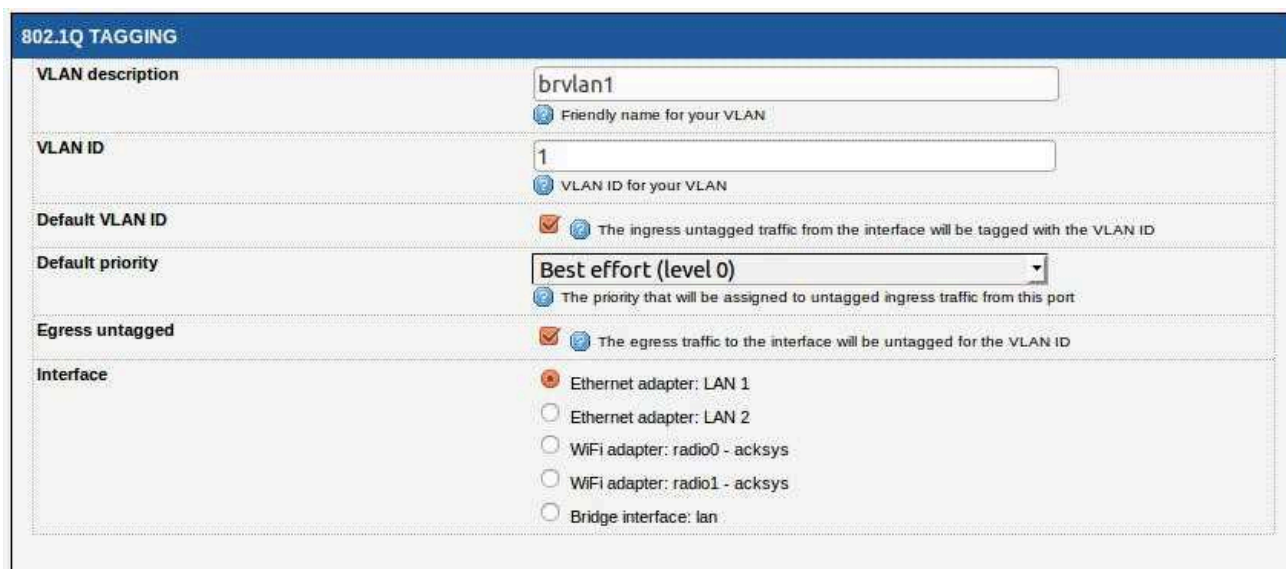
The overview lists all configured combinations of ports and VLANs.



Click on **Add tag** button to add VLAN configuration on one port.

Click the Edit button  to define or change the VLAN properties

Port configuration page



VLAN description:

Friendly name for the setting.

VLAN ID:

The VLAN ID.

Default VLAN ID:

If checked, all ingress untagged traffic will be placed in the VLAN. Only one VLAN per port can be the default.

Default priority:

Select the priority. This option is available only if default VLAN ID is checked.

Egress untagged:

If checked, the VLAN tag will be removed from the frame before forwarding.

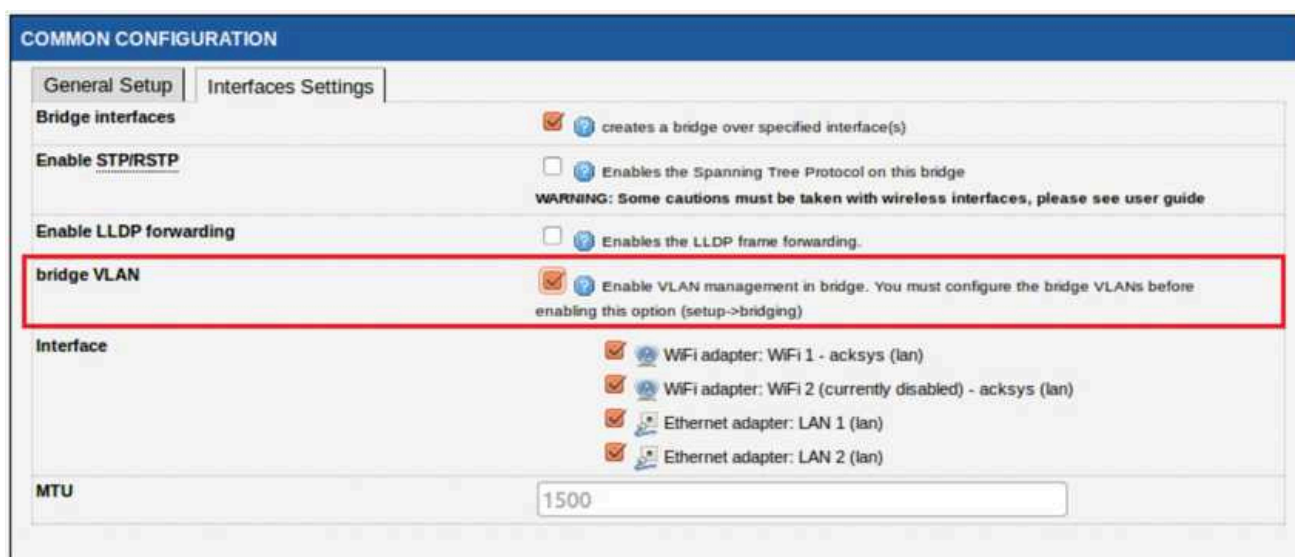
Interface:

Selects the port to apply the VLAN settings to.

All relevant VLANs should be configured on every interface of the bridge.

Enable the Bridging VLAN

You can enable Bridge VLAN in the submenu **NETWORK/Interface Settings**.



When you enable the Bridge VLAN, the untagged frames will be dropped for security reasons. All untagged frames should be placed in a specific VLAN by configuring a default VLAN on the originating port.

If you want to access the product through a port without VLAN tags:

Add VLAN on the **Bridge interface** itself (bridge upper layer interface), check **default VID** and **egress untagged** option on the required port

Add the same VLAN on all interfaces where you want access the product. Check the **default VID** and “egress untagged” option.

This VID value must not be in use by another VLAN (or its traffic will be mixed with non VLAN traffic).

The pictures below show a simple configuration to have a product access from LAN 1 or LAN 2 without VLAN.

802.1Q TAGGING						
NAME	INTERFACE	VID	PRIORITY	DEFAULT VID	EGRESS UNTAGGED	ACTIONS
brvlan2	Ethernet adapter: LAN 1	1	Best Effort (level 0)	☒	☒	 
brvlan3	Ethernet adapter: LAN 2	1	Best Effort (level 0)	☒	☒	 
brvlan1	network: lan	1	Best Effort (level 0)	☒	☒	 

 Add tag

VII.1.7.3 Bridge filter

In this section you can manage layer 2 (link-level) filter groups.

Each filter group may contain several rules and may be affected to one or more Ethernet or Wireless interfaces, provided they are included in a bridge.

The filter drops the frame if one rule matches in group.

Add group

BRIDGE FILTER OVERVIEW

FILTER GROUP NAME	ACTIONS
filtre group 1	 

 Add group

Edit group

FILTER INFORMATION										
description		<input type="text" value="filtre group 1"/>								

FILTERS RULES										
This section allow to add filter rule on this group filter rule										
MAC FRAME TYPE	CHECK MAC	NETWORK PROTO	IP ADDR	NETMASK	CHECK IP	TRANSPORT PROTO	FIRST PORT	LAST PORT	CHECK PORT	
<input type="text" value="No filter"/>		<input type="text" value="ARP"/>	<input type="text" value="127.0.0.1"/>	<input type="text" value="255.255.255.255"/>	<input type="text" value="Src I"/>					
<input type="text" value="No filter"/>		<input type="text" value="ARP"/>	<input type="text" value="127.0.0.1"/>	<input type="text" value="255.255.255.255"/>	<input type="text" value="Dest"/>					

 Add

Description:

You can assign a symbolic name to the group.

Mac frame type:

Select the layer 2 frame type.

- No filter: No test on mac layer
- Unicast: Check if the frame is unicast type.
- Broadcast: Check if the frame is broadcast type.
- Multicast: Check if the frame is multicast type.

Check MAC:

This field is visible, only if Mac frame type is different from *no filter*

- Src Addr: Check the frame type on source MAC address field
- Dest Addr: Check the frame type on destination MAC address.

Network Proto:

Select the layer 3 protocol

- No filter: No test on Layer 3
- ARP: Check if it is an ARP frame
- IP: Check if it is an IP frame
- Custom: Enter the protocol number. For example, 0x800 for IP frame.

IP addr & Netmask

These fields are visible only if the Layer 3 protocol is set to IP or ARP.

With these fields you can select the par of IP address.

IP address	Netmask	Result
192.168.1.3	255.255.255.255	The frame match only for frame with IP address 192.168.1.3
10.10.0.0	255.255.0.0	The frame match for all IP address in 10.10.x.x
127.0.0.1	255.255.255.255	The frame match for the IP address assigned to the product on this interface

Check IP:

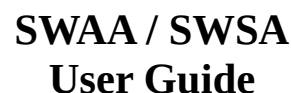
This field is visible only if the layer 3 protocol is set to IP or ARP.

- Dest IP: Check on the destination IP field in the frame. For ARP protocol the *Target IP address* field was used.
- Src IP: Check on the source IP field in the frame. For ARP protocol the *Sender IP address* field was used.

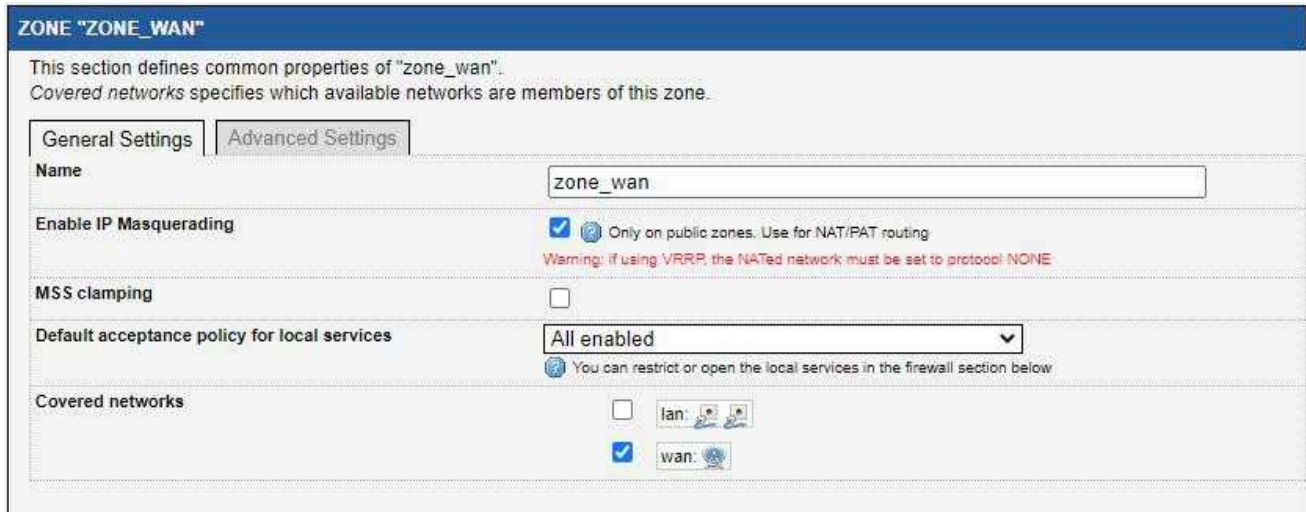
Transport proto:

This field is visible only if the layer 3 protocol is set to IP.

- UDP: Check if the transport protocol is UDP
- TCP: Check if the transport protocol is TCP
- ICMP: Check if the transport protocol is ICMP



General Zones settings



The screenshot shows the 'ZONE "ZONE_WAN"' configuration page. It has two tabs: 'General Settings' (selected) and 'Advanced Settings'. The page contains the following fields and options:

- Name:** A text box containing 'zone_wan'.
- Enable IP Masquerading:** A checked checkbox. A tooltip says 'Only on public zones. Use for NAT/PAT routing'. A warning message below reads: 'Warning: if using VRRP, the NATed network must be set to protocol NONE'.
- MSS clamping:** An unchecked checkbox.
- Default acceptance policy for local services:** A dropdown menu set to 'All enabled'. A tooltip says 'You can restrict or open the local services in the firewall section below'.
- Covered networks:** Two checkboxes. 'lan' is unchecked, and 'wan' is checked.

Name:

Friendly name for the zone.

Enable IP Masquerading:

Enables NAT/PAT on this zone. Check this option only on zones which contains public interfaces.

MSS clamping:

Reduces the MSS (Maximum Segment Size) if the interface uses a smaller MTU.

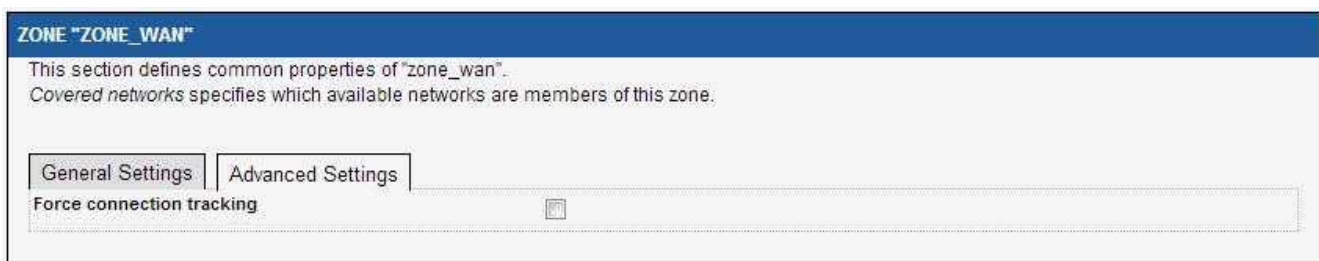
Default acceptance policy for local services:

Enables or disables the local services from this zone. You can restrict or open the local service in the firewall section.

Covered networks:

Select the networks covered by this zone by checking the relevant boxes.

Advanced Settings



The screenshot shows the 'ZONE "ZONE_WAN"' configuration page, 'Advanced Settings' tab. It contains the following field:

- Force connection tracking:** An unchecked checkbox.

Force connection 00:

By default, the firewall disables the connection tracking for a zone if the NAT/PAT (IP Masquerading) is not enabled.

Disabling the connection tracking increases the routing performance.

Check this option to enable connection tracking on this zone. You should do this only with customized versions of the firmware that require it.

Inter-zone forwarding

INTER-ZONE FORWARDING

Use this section only if IP Masquerading is disabled on this zone.

The options below control the forwarding policies between this zone (%s) and other zones. *Destination zones* cover forwarded traffic originating from %q. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forwarding to destination zones: ☐ zone_lan lan:  

This section is used only if IP Masquerading is disabled on this zone.

Select the zones where all traffic from this zone is forwarded without restriction. If you want to forward only part of the traffic use the firewall section.

Traffic forwarding

TRAFFIC FORWARD

Use this section only if IP Masquerading is enabled on this zone.

This section allow to redirect the input traffic on this zone to a device on other zone

SOURCE ZONE	NAME	SOURCE IP	FRAME PROTOCOL	PUBLIC PORT	PRIVATE PORT	DESTINATION IP	SORT	
zone_wan	VOIP	any	udp	5060	1500	192.168.1.10		 

 Add

Use this section to forward traffic to the private side when the NAT/PAT (IP Masquerading) is enabled.

For each frame received by this zone with matching source IP, frame protocol and public destination port, the frame's destination port and destination IP address will be rewritten as specified.

Name:

Rule name. You can assign a symbolic name to the rule.

Source IP:

Sets the expected source IP of the input frame. If this field is blank, any IP match.

Frame Protocol:

Sets the expected protocol type: UDP, TCP, TCP & UDP or all.

Public port:

Sets the expected destination port of the input frame on this zone. You can specify either a single port or a port range (using a dash "-" between the starting and ending ports). If this field is blank, any port will match.

Private Port:

The NAT/PAT will replace the original destination port by this private port in the frame before sending it on the private side. If this field is blank, the port (or port range) is left unchanged. If a public port range is used, the private port must be a port range of the same width.

Destination IP:

The NAT/PAT will replace the original destination IP address by this private IP address in the frame before sending it on the private side. **This field cannot be blank.**

NAT 1:1

NAT 1:1

Use this section only if IP Masquerading is disabled on this zone.

This section allow to redirect the input traffic on a virtual address to a device on other zone

SOURCE ZONE	SOURCE IPV4 NETWORK	DESTINATION ZONE	DESTINATION IPV4 NETWORK	NETWORK MASK
Source IP starting address for the 1:1 mapping.	Destination Zone	Destination IPv4 Network	Common Network Mask	
zone_wan	10.10.1.0	zone_lan	192.168.1.0	255.255.255.128
<div>Add</div>				

Use this section to define the virtual IVPV4 networks that will be used to forward traffic from the source zone to the defined destination zone network. IP Masquerading must be disabled to use NAT1:1.

Source IPV4 Network:

Define the starting virtual address used for the 1:1 mapping.

Destination Zone:

Select here the destination zone among the different zones previously created.

Destination IPV4 Network:

Define the physical destination IPV4 Network. This subnet must be accessible in the destination zone.

Network Mask:

The network mask defines the size of the translated network:

255.255.255.255	1 translated IP addresses
255.255.255.192	64 translated IP addresses
255.255.255.128	128 translated IP addresses
255.255.255.0	256 translated IP addresses
255.255.0.0	65 536 translated IP addresses
255.0.0.0	16 777 216 translated IP addresses

Please note that, on the source network, it is necessary to define the router as the default gateway, or to create a static route to the router, to be able to access the translated subnets of the destination zone.

On the destination networks, the return path to the source network must also be defined in the same way. Creation of IP aliases may be required for this purpose.

Firewall

FIREWALL

This section allows to configure the integrated firewall on "zone_wan". the firewall blocks or forwards the input traffic.
Rules are processed in the listed order.

SOURCE ZONE	SOURCE IP	DESTINATION IP	FRAME PROTOCOL	PORT	ACTION	DESTINATION ZONE	SORT
☐ Device ☒ zone_wan ☐ net1	<input type="text" value="192.168.3.9"/>	<input type="text"/>	<input type="text" value="tcp"/>	<input type="text" value="80"/>	<input type="text" value="forw"/>	☐ Device ☒ zone_lan ☐ net1	
☐ Device ☒ zone_wan ☐ net1	<input type="text"/>	<input type="text" value="10.90.5.4"/>	<input type="text" value="udp"/>	<input type="text" value="61"/>	<input type="text" value="reject"/>	☐ Device ☒ zone_lan ☐ net1	

This section it used to restrict or allow the use of services provided on the device (locally in the product) or in another zone.

Source IP:

The IP source address of the packets to be filtered.

Destination IP:

The IP destination address of the packets to be filtered.

Frame protocol:

The protocol type: TCP, UDP, TCP & UDP, ICMP, GRE, all

Port:

The destination port of the traffic. The port identifies the service.

Action:

One of:

Forward: Forward traffic to the destination zone or device

Reject: Drop packet and send ICMP message to the traffic source

Drop: Drop packet without ICMP message.

Destination zone:

Zone where traffic will be forwarded.

VII.1.8.2 Static routes

In this section you can add a static route in the device.

STATIC IPV4 ROUTES						
NETWORK	TARGET	IPV4-NETMASK	IPV4-GATEWAY	METRIC	MTU	SPECIFIC
Host-IP or Network: if target is a network:						
VLAN1	1.2.3.5	255.255.255.255		0	1500	GRE=gre1
lan	192.168.12.30	255.255.255.255	192.168.1.22	1	1500	
wan	192.168.2.0	255.255.255.0	192.168.1.1	0	1500	
						

Target:

Destination host or network IP address.

IPv4-netmask:

If the target is a network, you must set this field to the correct netmask.

If the target is a host, you can leave this field blank.

Metric:

Sets the metric for this route. Leave blank to use the default of 64.

MTU:

Set the MTU for this route. Leave blank to use the computed value.

Specific:

This column indicates the static routes that are automatically created by network services.

WARNING: modifying/deleting routes marked as SPECIFIC could prevent corresponding services to work properly.

VII.1.8.3 Multicast routing

In this page you configure the PIM-SM multicast router.

PHYSICAL INTERFACES

VIRTUAL INTERFACES

NETWORK

BRIDGING

ROUTING / FIREWALL

NETWORK ZONES

STATIC ROUTES

MULTICAST ROUTING

DOS PROTECTION

QOS

SERVICES

SETUP

TOOLS

STATUS

PIM-SM MULTICAST ROUTER SETTINGS

RP: RendezVous point, the server where outgoing flows are sent, and where receivers join requests ultimately arrive.
DR: Designated router, the elected router among the potentially several ones on a given subnetwork.
Group: Multicast community identified by a multicast address.
Group prefix: the high-order bits of a multicast address, identified by an IP address and a number of relevant bits.

GENERAL SETTINGS

Basic Setup

RendezVous Points

Shortest Path

IGMP Settings

Advanced Settings

Enable Multicast routing

☒

Log level

Error

Enable RendezVous point Bootstrap Service

☒

If disabled, you must set some static RP's below.

RendezVous point Candidate

☒

Advertise to the bootstrap servers as a candidate RP for the groups detailed below.

LOCAL RENDEZVOUS POINT CONFIGURATION

Multicast groups manageable by the local RP

MULTICAST GROUP PREFIX
<div>CIDR format: IPAddress/MaskLength</div> <div>230.0.0.0/8</div> <div>Add</div>

REMOTE RENDEZVOUS POINTS CONFIGURATION

Multicast groups manageable by well-known remote RP's

MULTICAST GROUP PREFIX	RENDEZVOUS POINT
<div>CIDR format: IPAddress/MaskLength</div> <div>239.0.0.0/8</div> <div>Add</div>	<div>IP Address</div> <div>10.10.150.48</div>

LOCAL NETWORKS CONFIGURATION

NETWORK	HANDLE MULTICAST	TTL THRESHOLD	DR PRIORITY	PREFERENCE	METRIC	IGMP
Min TTL allowing forwarding: 1-255 HELLO priority, higher is better: 1-4,000,000,000 ASSERT preference: 1-255 ASSERT metric: 1-1024						
onboard	☒	2		default	default	v2
backside	☐	1		default	default	v3
GRE-tunnel	☒	1		default	default	v3

Reset

Save

Save & Apply

The **General settings** section sets various router options.

The **Local rendezvous points configuration** section sets the list of multicast groups that this device is willing to handle as their rendezvous point.

The **Remote rendezvous points configuration** section associates groups to remote rendezvous points addresses, so that this device does not need a BSR to provide this association.

The **Local networks configuration** lists the local network interfaces available for multicast routing. It is a mirror of the list in the **setup/network** overview page. It allows disabling some interfaces, or changing various performance details.

General settings Basic setup tab

Enable multicast routing:

Check this to enable the multicast router and all the dependent functionalities.

Log level:

Adjusts the quantity of messages sent to the system log. Warning: the system log must be set to at least the same level in order to handle the messages.

Enable Bootstrap Service:

Check this to allow this device to be a BSR candidate.

RendezVous Point candidate:

Check this to allow this device to be a RP for the groups listed in the **local rendezvous point configuration** section.

Rendezvous Points tab

GENERAL SETTINGS	
Basic Setup	RendezVous Points
Shortest Path	IGMP Settings
Advanced Settings	
Bootstrap Server Candidate priority	5
	0 to 255.
Bootstrap Server Candidate advertized local address	
	Optional. If empty, defaults to highest local IP address.
Bootstrap Server messages periodicity	60
	Number of seconds between Bootstrap messages.
RendezVous point Candidate priority	20
	0 to 255.
RendezVous point Candidate advertized local address	
	Optional. If empty, defaults to highest local IP address.
RendezVous point Candidate messages periodicity	60
	Number of seconds between Candidate messages.

BSR candidate priority:

Priority in election process if several candidates are present (highest priority wins).

BSR local address:

Routers are multi-homed, they have several IP addresses. This is the IP address that will be used for the purpose of the BSR protocol. Leave blank to use the default value which is the highest IP address of the enable interfaces.

BSR message periodicity:

Also called [BS_Period]. Association between a multicast group and its RP is cached in the routers. The duration of this cache is normally 2.5 times the periodicity of RP

messages (allowing to lose two messages over 3). But if this duration is smaller than [BS_Period], it will be adjusted to $2.5 \times [\text{BS_Period}]$ to respect RFC5059 constraints

RP candidate priority:

Priority in election process if several candidates are present (highest priority wins).

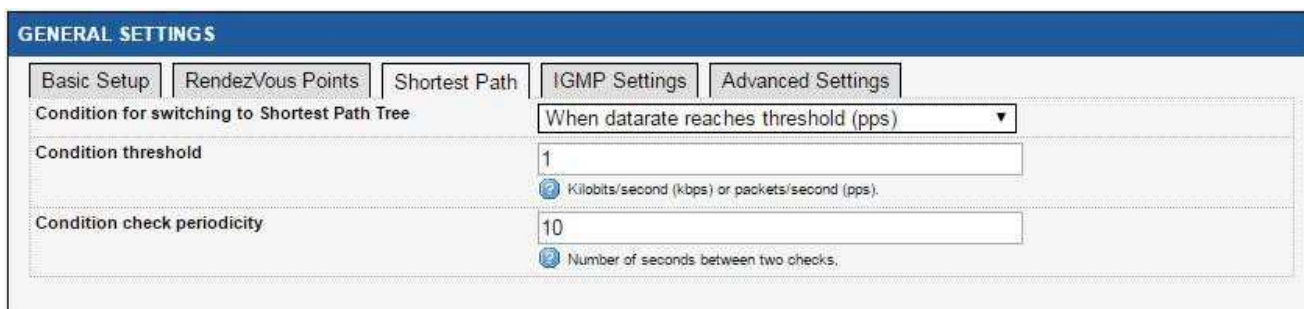
RP local address:

Routers are multi-homed, they have several IP addresses. This is the IP address that will be used for RP election in the BSR protocol. Leave blank to use the default value which is the highest IP address of the enable interfaces.

RP candidate messages periodicity:

duration between two successive **RP-Cand** PIM messages (advertising willingness to handle configured groups).

Shortest path tab



The screenshot shows the 'GENERAL SETTINGS' window with the 'Shortest Path' tab selected. The 'Condition for switching to Shortest Path Tree' is set to 'When datarate reaches threshold (pps)'. The 'Condition threshold' is set to 1, with a unit selector set to 'Kilobits/second (kbps) or packets/second (pps)'. The 'Condition check periodicity' is set to 10, with a unit selector set to 'Number of seconds between two checks'.

Condition for switching:

switching the path from RP traversal to shortest can be triggered when throughput exceeds a configured value. Choose the trigger type: it can be **never** (no switching), or expressed in packets per second or bits per second.

Condition threshold:

which throughput will trigger the switch to SPT. The unit depends on the above choice.

Condition check periodicity:

the maximum delay between the time the trigger condition becomes true and the time the SPT switch is initiated.

IGMP settings tab

GENERAL SETTINGS	
Basic Setup	RendezVous Points
Shortest Path	IGMP Settings
Advanced Settings	
Query interval	12
Number of seconds between two IGMP General Query messages.	
Other querier present timeout	42
Number of seconds before taking over the querier role. Should be 2.5 or 3.5 times the query interval.	

Condition threshold:

which throughput will trigger the switch to SPT. The unit depends on the above choice.

Query interval:

the delay between two successive IGMP queries.

Other querier present timeout:

the delay after the last IGMP query was seen on a network interface, before this router takes over the IGMP querier role on this interface, in the assumption that the previous querier went down.

Advanced settings tab

GENERAL SETTINGS	
Basic Setup	RendezVous Points
Shortest Path	IGMP Settings
Advanced Settings	
Hello messages periodicity	30
Number of seconds between PIM HELLO messages.	
Default route metric	1024
For PIM ASSERT messages. 1 to 1024.	
Default route preference	101
For PIM ASSERT messages. 1 to 255.	
Debug classes	mrt
Classes of messages used at the debug loglevel. Reserved for advanced support.	

Hello periodicity:

duration between two successive "HELLO" PIM messages (advertising existence and priority of a PIM router).

Default route metric:

the route metric value sent in ASSERT messages if no metric is set for the network interface where ASSERT is sent.

Default route preference:

the preference metric value sent in ASSERT messages if no preference is set for the network interface where ASSERT is sent.

Debug classes:

when the log level is set to "Debug", this comma-separated field indicates the classes of debug messages sent to the log. This field is reserved for advanced technical support.

Local rendezvous point configuration

Here you enter the list of groups for which this router plays the rendezvous point role.



ADD button:

click here to add a new block of groups.

Red cross buttons:

click here to delete a block of groups.

Multicast group prefix:

in each line, write the prefix (the common beginning) of group IP addresses, followed by a "/" and the number of significant bits in the prefix.

This router will handle all groups beginning with one of the prefixes in the list.

Remote rendezvous points configuration

Here you list groups that are handled by a remote RP but you cannot rely on a BSR to advertise it. BSR is still used for other groups.



ADD button:

Click here to add a new block of groups.

Red cross buttons:

click here to delete a block of groups.

Multicast group prefix:

the common beginning of group IP addresses, followed by a "/" and the number of significant bits in the prefix.

Rendezvous point:

enter the address of the rendezvous point managing this group block.

This router preloads the list at startup and uses these associations to find the remote RP for the designated groups. For the purpose of RP election, these static associations have a priority of 1 (highest).

Local networks configuration

Here you give parameters related to each network interface.

LOCAL NETWORKS CONFIGURATION						
NETWORK	HANDLE MULTICAST	TTL THRESHOLD	DR PRIORITY	PREFERENCE	METRIC	IGMP
		Min TTL allowing forwarding, 1-255	HELLO priority, higher is better, 1-4,000,000,000	ASSERT preference, 1-255	ASSERT metric, 1-1024	
onboard	☒	2		default	default	v2 ▼
trackside	☐	1		default	default	v3 ▼
GRE-tunnel	☒	1		default	default	v3 ▼

Network: the friendly name of the network interface.

Handle multicast:

whether the PIM router will ignore this network.

TTL threshold:

drop outgoing multicast data with a lower TTL.

DR priority:

this router's priority for Designated Router election on this network.

Preference:

the preference metric value sent in ASSERT messages. Defaults to the value set in the **advanced settings** tab.

Metric:

the route metric value sent in ASSERT messages; represents the distance between this router and the RP being targeted. Defaults to the value set in "advanced settings" tab.

IGMP: set to **v2** to enforce IGMPv2 compatibility.

VII.1.8.4 Denial Of Service (DOS) protection

PROTECTION	
Enable SYN-flood protection	☒
Drop invalid packets	☒

Enable SYN-flood protection:

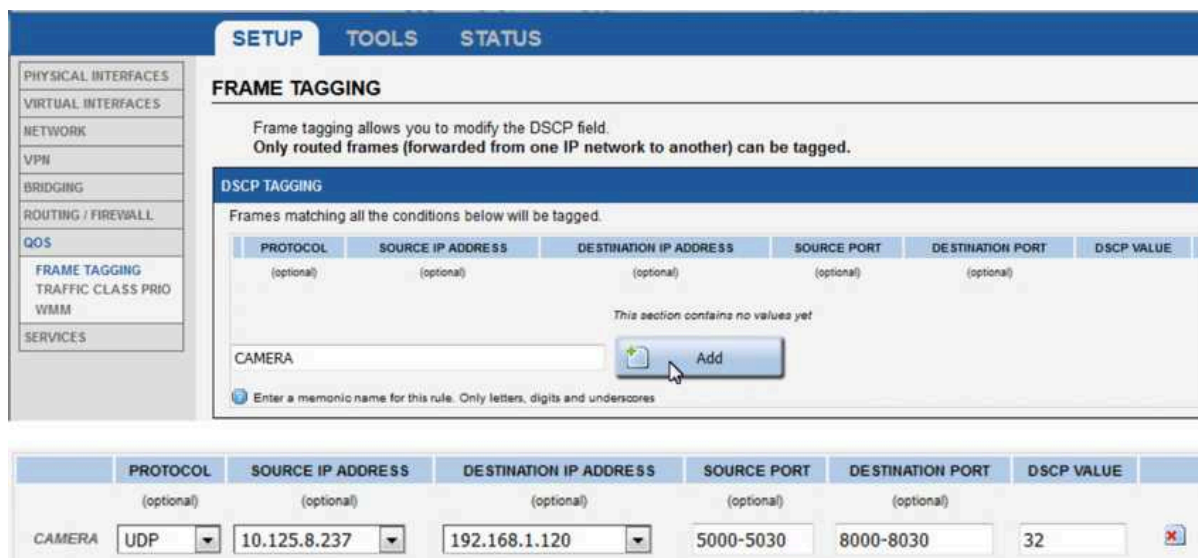
The syn-flood attack consists in filling the victim's resources by creating many half-opened connections. It is explained in details on http://en.wikipedia.org/wiki/SYN_flood

Drop invalid packets:

Drop invalid frames or frames without active connection.

VII.1.9 QOS

VII.1.9.1 Frame tagging



The DSCP tag applies on each incoming frame (from any interface) that matches the following criterions:

PROTOCOL:

The IP protocol type. This can be TCP, UDP or ICMP.

SOURCE IP ADDRESS:

The source IP address of the incoming frame. Wildcards are not allowed.

DESTINATION IP ADDRESS:

The destination IP address of the incoming frame. Wildcards are not allowed.

SOURCE PORT:

The source port of the incoming frame. This parameter is valid for TCP & UDP protocols only (see above). You can specify either a single port or a port range

DESTINATION PORT:

The destination port of the incoming frame. This parameter is valid for TCP & UDP protocols only (see above). You can specify either a single port or a port range

DSCP VALUE:

The value to be written in the DSCP field (6 bits) of the IP frame.

You can use the following table to set WMM valid tags:

WMM valid tags	
DSCP field value	WMM Queue
8 or 16	Background (BK)
0 or 24	Best effort (BE)
32 or 40	Video (VI)
48 or 56	Voice (VO)

VII.1.9.2 Traffic Class Priorities

This submenu allows configuring the QoS traffic class management.

SETUP

TOOLS

STATUS

PHYSICAL INTERFACES

VIRTUAL INTERFACES

NETWORK

VPN

BRIDGING

ROUTING / FIREWALL

QOS

FRAME TAGGING

TRAFFIC CLASS PRIORITY

WMM

SERVICES

TRAFFIC CLASSES' PRIORITIES PER INTERFACE

In this section, you can configure the traffic classes' priorities:

The IEEE 802.1Q priorities 1→7 are mapped to traffic class0→7.
The IEEE 802.1Q priority 0 is considered as no priority set.
If no IEEE 802.1Q priority is set, then the DSCP classes 0→7 are mapped to traffic class 0→7.

TC = Traffic Class
Queue = In case of traffic congestion, the packets that can not be sent are stored in a buffer named queue.
→ Interfaces that manage N Queues, have the Queue 0 with the highest priority, and Queue N-1 with the lowest one.
→ Packets in a Queue with a better priority will be sent first.

Queue Management = How to deal with traffic in the same queue:
→ FIFO Queue: The First packet which enter the queue, is the first which exit it, without worrying about bandwidth sharing.
→ FAIR Queue: Algorithm that divides the traffic inside a queue in multiple flows, then assures that all flows are fairly served.

Traffic Class to queue mapping

ETHERNET INTERFACES

For Ethernet interfaces, the traffic classes 0→7 can be mapped to 8 levels of priorities / Queues 0 →7.

INTERFACE	ENABLE	TC 0	TC 1	TC 2	TC 3	TC 4	TC 5	TC 6	TC 7
LAN1	☒	7	6	5	4	3	2	1	0
LAN2	☒	7	6	5	4	3	2	1	0

WI-FI INTERFACES

For Wi-Fi interfaces, QOS is always active (in regards to WMM).
The WMM standard also imposes the traffic class to priority mapping, with 4 levels of priorities / Queues 0 →3.

INTERFACE	TC 0	TC 1	TC 2	TC 3	TC 4	TC 5	TC 6	TC 7
WiFi - E-Test	2	3	3	2	1	1	0	0
WiFi - o/test	2	3	3	2	1	1	0	0

To map a traffic class to a given queue/priority, check the **enable** box and select the Queue number for each TCx traffic class. For Wi-Fi interfaces, WMM is always active and the queue mapping is imposed and cannot be changed

Queue management

QUEUE MANAGEMENT: ETHERNET INTERFACE

Management of Ethernet queues

INTERFACE	QUEUE 0	QUEUE 1	QUEUE 2	QUEUE 3	QUEUE 4	QUEUE 5	QUEUE 6	QUEUE 7
LAN1	FAIR	FAIR	FAIR	FAIR	FAIR	FAIR	FAIR	FAIR
LAN2	FAIR	FIFO	FAIR	FAIR	FAIR	FAIR	FAIR	FAIR

FAIR

QUEUE MANAGEMENT: WI-FI INTERFACE

Management of Wi-Fi queues

INTERFACE	QUEUE 0	QUEUE 1	QUEUE 2	QUEUE 3
WiFi - E-Test	FAIR	FAIR	FAIR	FAIR

To select the queue management type, select the queue type for each QUEUE x

VII.1.9.3 WMM

SETUP
TOOLS
STATUS

PHYSICAL INTERFACES
VIRTUAL INTERFACES
NETWORK
ROUTING / FIREWALL
QOS
FRAME TAGGING
WMM
SERVICES

WMM PARAMETERS

WMM parameters for profile: Default (read only)

AP PARAMETERS

AC	CWMIN	CWMAX	AIFS	MAX LENGTH FOR BURSTING
Background (BK)	15	1023	7	0
Best effort (BE)	15	63	3	0
Video (VI)	7	15	1	3
Voice (VO)	3	7	1	1.5

CLIENT PARAMETERS

AC	CWMIN	CWMAX	AIFS	TRANSMISSION OPPORTUNITY LIMIT	ACM
Background (BK)	4	10	7	0	0
Best effort (BE)	4	10	3	0	0
Video (VI)	3	4	2	94	0
Voice (VO)	2	3	2	47	0

The page displays the WMM parameters for the selected profile. WMM (a.k.a. WME) is always available.

WMM parameters for profile :

This listbox allows you to select **User** or **Default** QoS parameters. Default QoS parameters are given for reference and cannot be modified.

AP PARAMETERS:

This table allows you to change the WMM parameters for the four Access Point Tx queues (BK, BE, VI, VO).

CWMIN:

Defines the minimum contention window size (expressed in number of time slots).
Allowed values are 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023.

CWMAX:

Defines the maximum contention window size (expressed in number of time slots).
Allowed values are 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023.

AIFS:

Defines the arbitration inter-frame spacing value for the current queue size (expressed in number of time slots). Allowed values are 0 to 255.

MAX LENGTH FOR BURSTING:

Defines the maximum burst length (expressed in milliseconds with precision of 0.1 ms).
Allowed values are 0 to 100000ms.

CLIENT Parameters:

This table allows you to change the WMM parameters sent by the CLIENT in its management frame.

CWMIN:

Defines the minimum contention window size (expressed in number of time slots).
Allowed values are 0 to 12.

CWMAX:

Defines the maximum contention window size (expressed in number of time slots).
Allowed values are 0 to 12.

AIFS:

Defines the arbitration inter-frame spacing value for the current queue (expressed in number of time slots). Allowed values are 1 to 255.

TXOP_LIMIT:

Defines the tx opportunity limit duration (expressed in number of time slots).
Allowed values are 0 to 65535.

ACM:

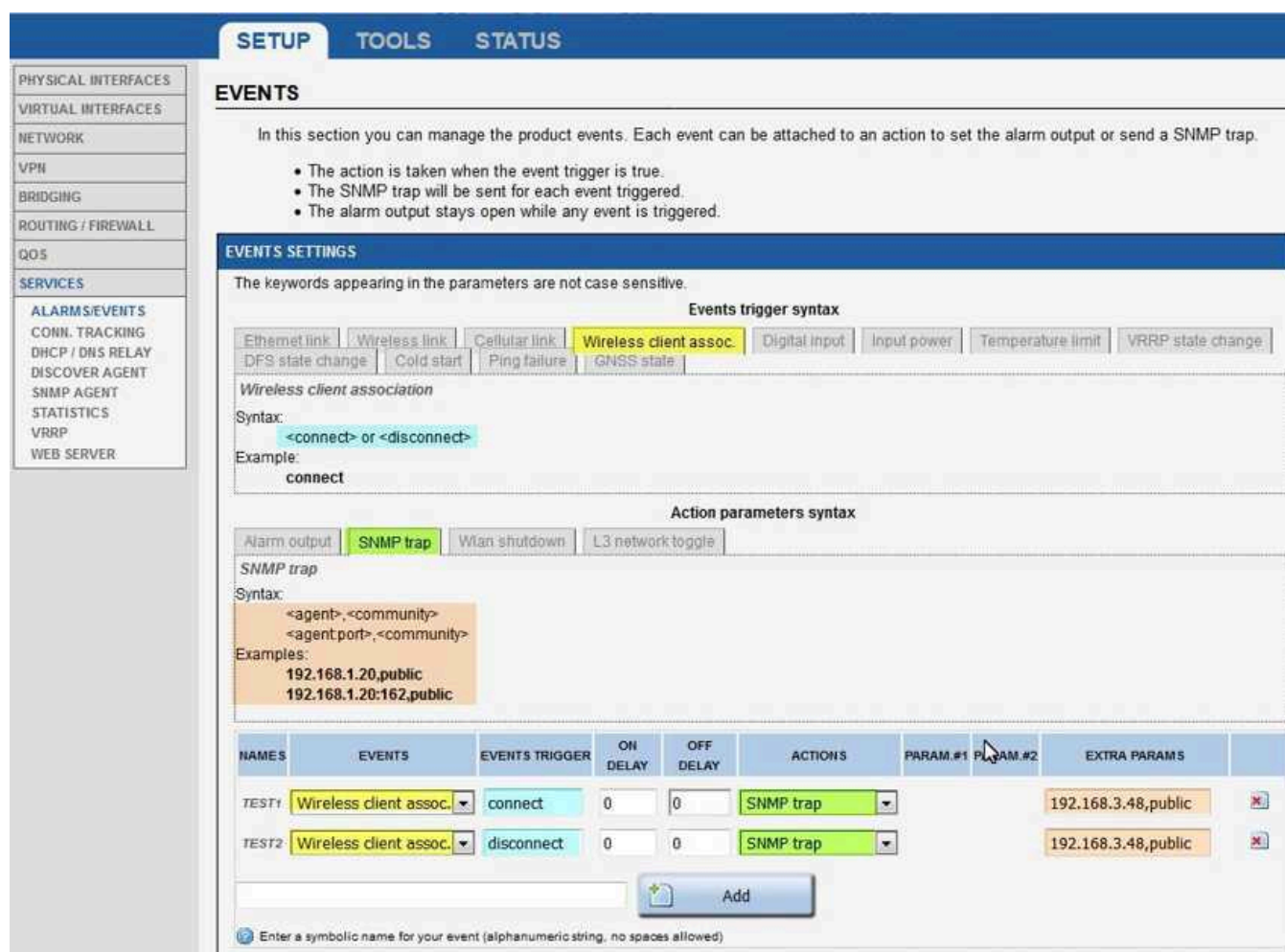
Defines the Admission Control Mandatory for the current queue. Allowed values are 0 and 1.

VII.1.10 Services

VII.1.10.1 Alarms / events

This page allows you to monitor various events in order to trigger actions. Using the **Add** button, you can define several triggers and give them mnemonic names.

Once trigger names have been created, you can set their event source and their associated action. The event source and the action may need extra parameters depending on their type. A summary help is displayed above the events table.



The screenshot shows the 'EVENTS' configuration page. On the left is a sidebar menu with categories: PHYSICAL INTERFACES, VIRTUAL INTERFACES, NETWORK, VPN, BRIDGING, ROUTING / FIREWALL, QOS, and SERVICES. Under SERVICES, 'ALARMS/EVENTS' is selected. The main content area has tabs for SETUP, TOOLS, and STATUS, with 'EVENTS' being the active tab. Below the tabs, there's a section titled 'EVENTS' with a description: 'In this section you can manage the product events. Each event can be attached to an action to set the alarm output or send a SNMP trap.' It lists three bullet points: 'The action is taken when the event trigger is true.', 'The SNMP trap will be sent for each event triggered.', and 'The alarm output stays open while any event is triggered.'

Below this is the 'EVENTS SETTINGS' section. It states: 'The keywords appearing in the parameters are not case sensitive.' It then shows 'Events trigger syntax' with a list of event sources: Ethernet link, Wireless link, Cellular link, Wireless client assoc. (highlighted), Digital input, Input power, Temperature limit, and VRRP state change. Below this, it shows 'Wireless client association' with a syntax example: '<connect> or <disconnect>' and an example: 'connect'.

Next is 'Action parameters syntax' with a list of actions: Alarm output, SNMP trap (highlighted), Wlan shutdown, and L3 network toggle. Below this, it shows 'SNMP trap' with a syntax example: '<agent>, <community>' and examples: '192.168.1.20,public' and '192.168.1.20:162,public'.

At the bottom is a table with columns: NAMES, EVENTS, EVENTS TRIGGER, ON DELAY, OFF DELAY, ACTIONS, PARAM.#1, PARAM.#2, and EXTRA PARAMS. It contains two entries: TEST1 and TEST2. Both are configured with 'Wireless client assoc.' as the event source, 'connect' and 'disconnect' as triggers, and 'SNMP trap' as the action. The extra parameters for both are '192.168.3.48,public'. An 'Add' button is located below the table.

Enter a symbolic name for your event and click the Add button to add a new entry.

Events:

Lan link: The state is up when the link is up on the physical interface.

Wireless link (in Access Point mode): The state is up when one client is connected on any of the access points running on the product.

Wireless link (in Client mode): The state is up when the bridge is connected to one Access point.

Input Power (Only on product with 2 input powers): The state is on, when the input power is powered.

Digital input (Only on product with digital input): The state is 1 when the digital input is active. Some products, such as the Airbox, have several Digital Input.

Wireless client assoc: The event can be linked only with the **SNMP trap** action. It sends a notification when a client associates or dissociates with one access point.

Temperature limit: The event is triggered when the temperature exceeds the trigger.

DFS state change: The event is triggered when the DFS status changed.

Cold start: The event is triggered when the product has finished booting.

Pinger: An ICMP ECHO Request (ping) is periodically sent to a remote host. If no ICMP ECHO Response is received for several consecutive periods, the event is triggered.

Actions:

SNMP: The **SNMP Trap** action, when triggered, will send the relevant trap to the specified manager address using the specified community.

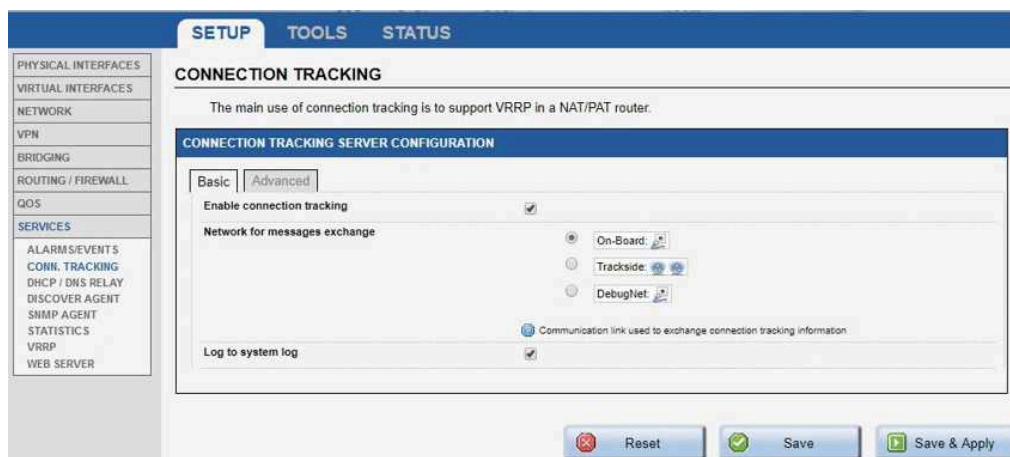
Alarm: The **Alarm** action only exists in some products. Some products, such as the Airbox, have several digital outputs that can be programmed as alarms. When triggered, the alarm contact will be activated as specified in the product [quick installation guide](#).

Wlan shutdown: the **Wlan shutdown** action, when triggered, will shut down the associated radio interface.

VII.1.10.2 Connection tracking

This page enables the connection tracking and replication service.

When connection tracking is required in the VRRP configuration page, you must enable and configure it here.



Basic tab

Enable connection tracking:

this enables the connection replication service.

Network for messages exchange:

network device used to send connection descriptions to the backup router. You can use either a subnet used by VRRP, or a dedicated network. Since this link must be reliable, a dedicated link is preferred, and a wired link is preferred over a wireless link.

Log to system log:

event messages are sent to the system log to be read later by an administrator.

Advanced tab

Multicast IPv4 address:

the multicast destination address used to send connection replication messages. It can be changed if some other user application uses the same multicast address.

Contrack group:

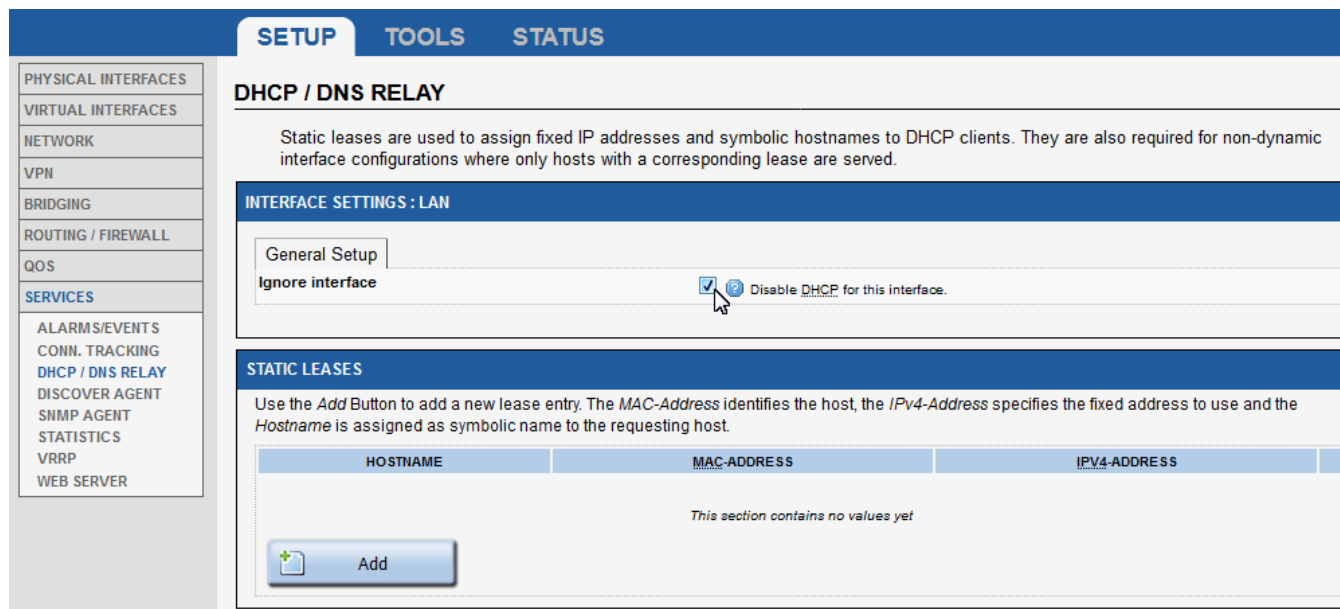
the replication service uses a standard protocol named contrack. If several instances of this service exist in other devices of the subnet, you can tag messages for your backup by dedicating a "group number".

Process priority:

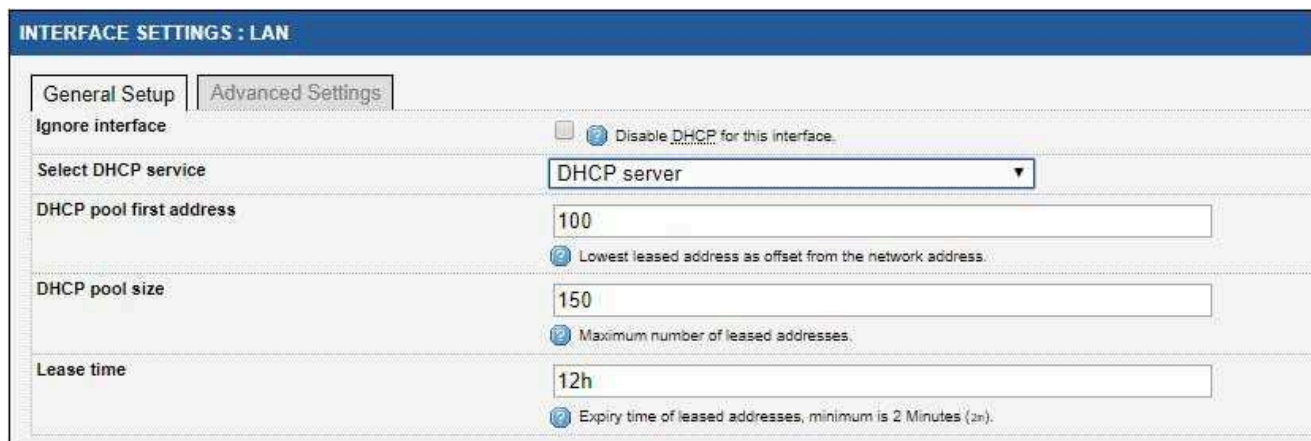
the higher the priority, the faster the replication, but also the higher the network load dedicated to replication. Also, a high priority with many connections may adversely affect the roaming delay.

VII.1.10.3 DHCP/DNS RELAY

To activate service DHCP server or DHCP relay, uncheck the **Ignore Interface** box:



Interface settings: DHCP Server General Setup:



Select DHCP service:

Allows to choose service DHCP server or DHCP relay. Default is DHCP server

DHCP pool first address:

First IP address of the DHCP pool. ATTENTION: this is interpreted as an offset relative to the network address.

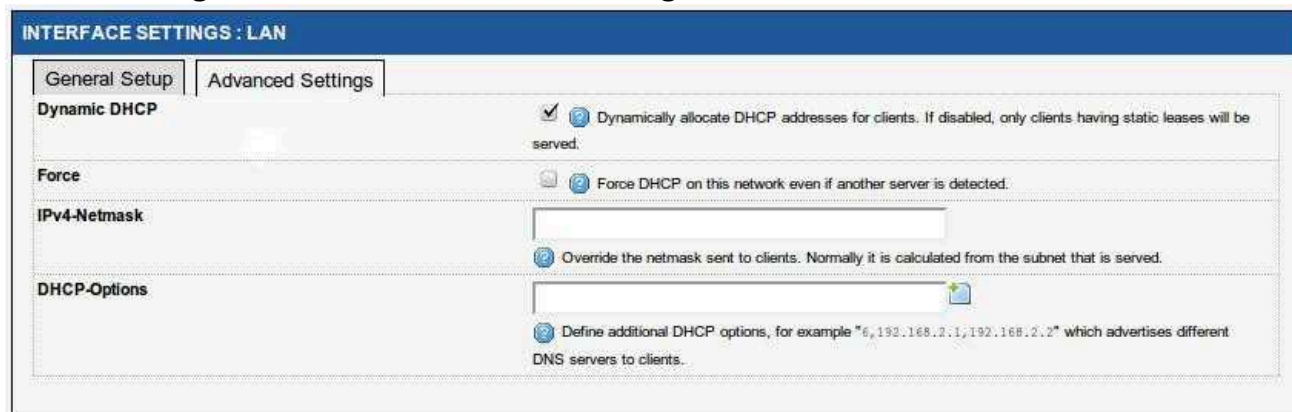
DHCP pool size:

Maximum number of leased addresses.

Lease time:

This represents the time during which a given IP address remains valid. After this time, the client needs to renew his lease.

Interface settings: DHCP Server Advanced Settings:



INTERFACE SETTINGS : LAN

General Setup | **Advanced Settings**

Dynamic DHCP ☒ Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

Force ☐ Force DHCP on this network even if another server is detected.

IPv4-Netmask Override the netmask sent to clients. Normally it is calculated from the subnet that is served.

DHCP-Options Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.

Dynamic DHCP:

If unchecked, only **static leases** will be authorized (see below)

Force:

By default, the DHCP service doesn't start if it detects the presence of another DHCP server on the network. If this option is checked, the DHCP server won't check for the presence of another server before starting.

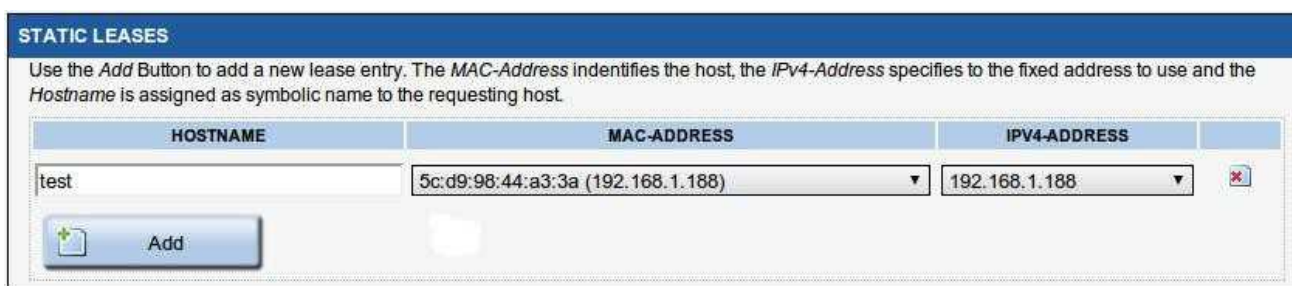
IPv4-Netmask:

This option override the default netmask value sent to DHCP clients.

DHCP-Options:

This field allows you to enter an additional DHCP option (enclosed into quotes). Syntax depends on the option itself. See DHCP RFCs for more information about DHCP options.

STATIC LEASES:



STATIC LEASES

Use the *Add* Button to add a new lease entry. The *MAC-Address* identifies the host, the *IPv4-Address* specifies to the fixed address to use and the *Hostname* is assigned as symbolic name to the requesting host.

HOSTNAME	MAC-ADDRESS	IPV4-ADDRESS
test	5c:d9:98:44:a3:3a (192.168.1.188)	192.168.1.188

 **Add**

Active only in DHCP server mode, this option allows to always give the same predefined IP address according to a given client MAC address.

DHCP RELAY

INTERFACE SETTINGS : LAN

General Setup

Ignore interface

☐
☒ Disable DHCP for this interface.

Select DHCP service

DHCP relay

Add/Remove DHCP relay

Please see DHCP relay section

DHCP RELAY

Use the Add Button to add a new DHCP relay entry.
The Relayed interface must have a static IP address. The DHCP Server/Relay must be able to reach back the network where the initial client's request originated from.

RELAYED INTERFACE	DHCP SERVER IPV4-ADDRESS	TRUSTED INTERFACE	SORT
Where DHCP request are received (from clients)	Where DHCP requests are sent (to server)	Where DHCP replies are received (from server)	
lan	192.16.1.1	all	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="X"/>

Use the Add button to add a new DHCP relay entry

RELAYED INTERFACE

The interface (defined in SETUP/NETWORK) on which the DHCP clients are connected. DHCP requests are received on this interface

DHCP SERVER IPV4-ADDRESS

The IP address of the DHCP server. DHCP requests from clients are forwarded to this address

TRUSTED INTERFACE

This is the interface (defined in SETUP/NETWORK) on which we authorize the reception of responses to DHCP requests. In the general case, we will choose "all"

DNS relay

These options enable DNS protection Attack.

DNS RELAY

Rebind protection

☒
☒ Enable DNS rebind attack protection. Block the DNS response if the IP address is on the private IP range (according to RFC1918)

Rebind localhost

☒
☒ Allow DNS response with IP address in 127.0.0.0/8 range.

VII.1.10.4 Discover Agent

This page will be able to configure the discover agent included in WaveOS. This agent is used by Acksys Network Device Manager to automatically find the Acksys products.

DISCOVER AGENT

In this section you will be able to configure the acksys discover agent. This agent is used by the Acksys network management tools

password	<input type="password" value="....."/>	
----------	--	---

Password

Enter your password. This password will be used for example when you will set the product IP by Acksys NMS.

VII.1.10.5 SNMP Agent

The SNMP agent is enabled by default and allows read/write access, using the **public** community, to the MIB-II and ACKSYS MIB.

The ACKSYS MIB file is self-documented. To read the OIDs documentation please use a text file editor or MIB browser.

Please read the SNMP security chapter before configuring the SNMP users and access rights: V.6.1 SNMP security

AGENT PROTOCOL CONFIGURATION

AGENT PROTOCOL CONFIGURATION	
Protocol	<input type="text" value="UDP"/>
Port number	<input type="text" value="161"/>
Snmp version	<input type="text" value="v1/v2c/v3"/>
SNMP V3 Engine ID	<input type="text" value="default"/>
<small> Warning: if you change this value and you already have set some SNMP V3 user, you should revalidate the user password. If you set the value to 'Motherboard ID' you can't export this SNMP configuration to another device</small>	

In this section you can change:

Protocol:

The agent access method (UDP/TCP)

Port number:

The agent port number

SNMP version:

- ❖ **v1/v2c:** This will allow **security model v1, v2c** and **usm** (please see chapter)
- ❖ **v3:** This will allow only **usm security model**.

SNMP V3 Engine ID

- ❖ **Default:** The default Engine ID is the same for all devices. In this configuration, the SNMP settings can be shared between several devices. If you change this value while you already have SNMP V3 users, you must revalidate the user password on each device.
- ❖ **MotherboardID:** Use the Motherboard ID as EngineID. This ID is unique, so each device with this setting will have a different engine ID. In this setting, you cannot share the SNMP settings between several products. You should revalidate the user password on each device.

COMMUNITY CONFIGURATION

In this section, you can find the list of communities, their access rights and restrictions on who use them. It relies on the SNMP v1/v2c **community based security model**.

Warning: if you change the public community properties, you must ensure that any SNMP client is set up accordingly. For example, the *Acksys WaveManager* software has a menu to change communities on a per-device basis.



	COMMUNITY	SECURITY NAME	ACCESS IP BASE	ACCESS IP RANGE
public	public	rw	0.0.0.0	
private	private	rw	localhost	255.255.255.255

Add

Access rights are defined in the “community configuration” subsection. To add an access rights specification, type in a nickname for the specification and click on the **Add** button. The nickname must be composed of letters, numbers and underscores. The nickname is **not** the community name, it is an **access rights specification** name.

By default, the **private** community is defined but inaccessible, for historical compatibility reasons. You can redefine the default communities at will.

Community:

The identification name that must be provided to the SNMP client in order for it to identify against the agent. You can use the same as the nickname, if you need to.

Security Name:

The Security Name that will be used to set the access right in the **VACM** section.

Access IP base:

An IP address which is allowed to use this specification. If the DNS server is properly configured in the Setup/Network page, or obtained from a DHCP server, you can type a host name (a FQDN) instead.

Access IP range:

An IP mask which is applied to the IP base to determine the full range of allowed client IP addresses.

SNMP V3 USM user administration

In this section, you can create, delete or modify the security settings of a **SNMP v3** user based on the **USM** security model.



SNMP V3 USERS LIST

Create snmp v3 users

SECURITY NAME	AUTHENTICATION TYPE	PRIVACY PROTOCOL	ACTIONS
User_1	MD5	DES	 
User_2	SHA	AES	 

 Refresh  Add user  Apply config

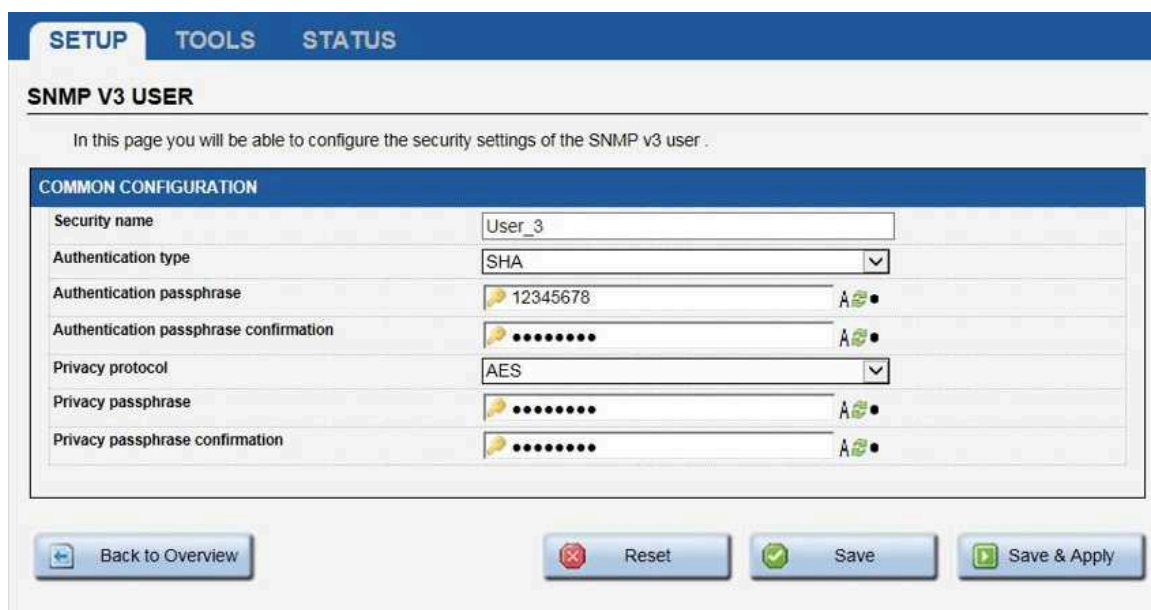
Refresh button:

Click on the refresh button, to synchronize with the user data base of the SNMP agent (since in SNMP v3, users can be created remotely with SNMP v3 commands).

This will also apply the saved changes on SNMP configuration.

Add user button:

Click on Add user button, to create a new SNMP v3 user.



SETUP TOOLS STATUS

SNMP V3 USER

In this page you will be able to configure the security settings of the SNMP v3 user .

COMMON CONFIGURATION

Security name	User_3		
Authentication type	SHA		
Authentication passphrase	12345678	A	
Authentication passphrase confirmation		A	
Privacy protocol	AES		
Privacy passphrase		A	
Privacy passphrase confirmation		A	

 Back to Overview  Reset  Save  Save & Apply



In this section, you can set the user credentials.

For security reasons, the stored passwords are encrypted and cannot be viewed later.

Authentication type:

Supported Authentication types are: SHA-512, SHA-384, SHA-256 and SHA-224

Supported Privacy protocols are AES-256, AES-192 and AES.

SHA1, MD5 and DES are also supported for compatibility, but marked as unsecure. They will certainly be removed in a future version, so we recommend not to use them.

Apply config button:

Click on this button to apply the saved changes. The saved changes that have not yet been applied for the SNMP v3 user list, are displayed in red:

SNMP V3 USERS LIST			
Create snmp v3 users:			
SECURITY NAME	AUTHENTICATION TYPE	PRIVACY PROTOCOL	ACTIONS
User_1	SHA-256	AES-256	 
User_2	SHA-512	AES-256	 
admin_acksys_user	SHA	AES	 
<div> Refresh</div> <div> Add user</div> <div> Apply config</div>			

Access control administration (VACM)

In this section, you can manage the access rights of SNMP v3 users or SNMP v1/v2c communities.

- 1) Add the user to a **Group** with its security model.

COMMUNITY CONFIGURATION

Map a SNMPv1 or SNMPv2c community string to a security name from a particular range of source addresses

	COMMUNITY	SECURITY NAME	ACCESS IP BASE	ACCESS IP RANGE	
PUBLIC	public	rw		0.0.0.0	
PRIVATE	private	rw	localhost	255.255.255.255	

Add

SNMP V3 USERS LIST

Create snmp v3 users

SECURITY NAME	AUTHENTICATION TYPE	PRIVACY PROTOCOL	ACTIONS
User_1	SHA-256	AES-256	
User_2	SHA-512	AES-192	
admin_acksys_user	SHA	AES	

Refresh Add user Apply config

GROUP CONFIGURATION

Map a Security Model and a Security Name into a named Group

GROUP	SECURITY MODEL	SECURITY NAME	
public	v1	ro	
public	v2c	ro	
public	usm	ro	
private	v1	rw	
private	v2c	rw	
private	usm	rw	
admin_acksys_group	usm	admin_acksys_user	
Group_V3	usm	User_1	
Group_V3	usm	User_2	

Add

- 2) Create a View on the OIDs that you need the rights.

VIEW CONFIGURATION

Define view with included/excluded OIDs

VIEW	TYPE	OID	
all	included	.1	
all	excluded	.1.3.6.1.4.1.28097.10.7	
admin_acksys_view	included	.1	
all	excluded	.1.3.6.1.4.1.28097.7.2.1.19	
For_auth_no_privacy	included	.1	
For_auth_no_privacy	excluded	.1.3.6.1.6.3	

Add

- Set the access rights on the View for the Group depending on the user security model and security level.

ACCESS CONFIGURATION					
Map group of users to a view depending on security level and type of access read/write					
GROUP	SECURITY MODEL	SECURITY LEVEL	READ	WRITE	
public	any	noauth	all	none	
private	any	noauth	all	all	
admin_acksys_group	any	priv	admin_acksys_view	admin_acksys_view	
Group_V3	usm	priv	all	all	
Group_V3	usm	auth	For_auth_no_privacy	For_auth_no_privacy	

Add

VII.1.10.6 Statistics

The system counters graphs display the product performance as a timing diagram by collecting data periodically.

PHYSICAL INTERFACES

VIRTUAL INTERFACES

NETWORK

VPN

BRIDGING

ROUTING / FIREWALL

QOS

SERVICES

ALARMS/EVENTS

CONN. TRACKING

DHCP / DNS RELAY

DISCOVER AGENT

SNMP AGENT

STATISTICS

VRRP

WEB SERVER

SETUP

TOOLS

STATUS

STATISTICS

In this page you can configure the statistics related services.

Warning: Some parameters can be changed by WaveManager

OVERALL SETTINGS

Enable statistics system ☒ To enable any statistics service, please enable this option.

WEB GRAPH

Allow to show the graph from status web pages

Enable statistics graph ☐

ACKSYS TELEMETRY

Allow to send information to WaveManager

Enable telemetry ☐

GPS STATISTIC

Allow to send GPS information to WaveManager

Enable GPS statistics ☐

WIRELESS ROAMING STATISTICS

Allow to send roaming information to WaveManager

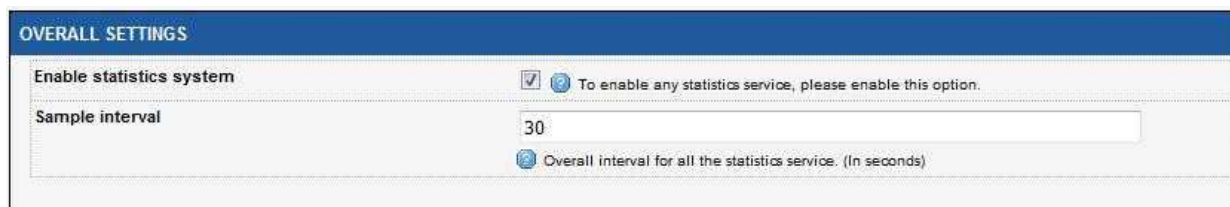
Enable wireless roaming statistics ☐ If enabled, wireless roaming status will be recorded. This data is asynchronous to overall sample rate.

WIRELESS INFO STATISTICS

Allow to send Wireless information to WaveManager

Enable wireless info statistics ☐ If enabled, wireless information (association list, connected AP ...) will be recorded.

Statistic related services are disabled by default. Please check Enable statistics system in the OVERALL SETTINGS to activate these functions.



OVERALL SETTINGS	
Enable statistics system	☒ To enable any statistics service, please enable this option.
Sample interval	30
	Overall interval for all the statistics service. (In seconds)

When statistical services are enabled, you can set the data collection interval (every 30 seconds by default).



WEB GRAPH	
Allow to show the graph from status web pages	☒
Enable statistics graph	☒

When graphs are enabled, the product collects the wireless signal level received by its wireless client from the AP, and tx/rx traffic data of network interfaces in real time. In the STATUS page, you can display collected data in graphical format with various display durations (see sections VII.3.2 Network and section VII.3.6.1 Associated Stations)

ACKSYS TELEMETRY

Allow to send information to WaveManager :

Enable telemetry ☒

Acksys telemetry server port

Output interval
Acksys telemetry will check if there is any new statistics data available at this frequency. To avoid data accumulation, this value should less than overall sample interval. (In seconds)

Max buffer size
This value will determine the size of buffer and also how much data will be stored in case connection with server is lost. (In bytes)

GPS STATISTIC

Allow to send GPS information to WaveManager :

Enable GPS statistics ☒

GPS server ip address
The ip address of a GPS server. If this product provides GPS service, please enter "127.0.0.1".

GPS server port

WIRELESS ROAMING STATISTICS

Allow to send roaming information to WaveManager :

Enable wireless roaming statistics ☒ If enabled, wireless roaming status will be recorded. This data is asynchronous to overall sample rate.

WIRELESS INFO STATISTICS

Allow to send Wireless information to WaveManager :

Enable wireless info statistics ☒ If enabled, wireless information (association list, connected AP ...) will be recorded.

The collection of telemetry information, GPS statistics, roaming statistics and GPS statistics is activated and automatically configured by WaveManager when it is launched or when these services are activated. It's possible to locally deactivate these services, but modification of the parameters is reserved for future functionalities not yet implemented.

VII.1.10.7 VRRP

In this page you will add the VRRP instances and their associated virtual IP address. Then you will create the VRRP groups, listing their instances and the properties common to all instances.

Before creating the instances, you must define all the needed subnets and their properties in the SETUP/NETWORK section.

If you are setting up a NAT or PAT router, you will need to enable the connection tracking service as well (see [Connection tracking](#)).

PHYSICAL INTERFACES

VIRTUAL INTERFACES

NETWORK

BRIDGING

ROUTING / FIREWALL

QOS

SERVICES

ALARMS/EVENTS

CONN. TRACKING

COUNTERS GRAPHS

DHCP / DNS RELAY

DISCOVER AGENT

SNMP AGENT

VRRP

WEB SERVER

SETUP

TOOLS

STATUS

VIRTUAL ROUTING REDUNDANCY PROTOCOL SETTINGS

VRRP instances are entities that send and receive VRRP advertisement frames through one network interface. VRRP groups enforce a common state (alive or dormant) for all instances in the group.

VRRP GLOBAL SETTINGS

multicast group

IPV4 multicast group used for VRRP advertisement

VRRP IN STANCES CONFIGURATION

VIRTUAL ROUTER ID	ENABLE NETWORK	VIRTUAL IPV4 ADDRESS	NETMASK	UNICAST PEER IP
101	☒ on-board	192.168.200.1	24	Multicast advertisement used
102	☒ on-board	192.168.200.2	24	Multicast advertisement used
201	☒ trackside	192.168.4.252	24	192.168.4.1
202	☒ trackside	192.168.4.253	24	Multicast advertisement used

Add

SYNCHRONIZED SUBNETS GROUPS CONFIGURATION

routeA

Enable

Initial state: Backup (dominant)

Advertisements period: 1000

Priority: default

Virtual router IDs: 101, 102, 201, 202

Support connection tracking: ☒

Services dependent on the state of this group: ☐

routeB

Enable

Initial state: Master (routing)

Advertisements period: 1000

Priority: default

Virtual router IDs: 101, 102, 201, 202

Support connection tracking: ☒

Services dependent on the state of this group: ☐

Ver. 0.9A

209 / 272

Subsection: VRRP global settings

Multicast group:

Set the multicast group that will be used by VRRP instance to send the advertisement.
Leave blank to use the default group.

Subsection: VRRP INSTANCES CONFIGURATION

Each virtual IP address is identified by a number between 1 and 255. To create an instance, enter a valid, unused number in the box at the bottom of the first subsection, then click the **Add** button.

The instance is created and you can set its properties:

Enable:

you must enable the instance to use it. If you are testing various configurations you can disable instances you do not use.

Networks:

choose the network interface to associate with the virtual IP. The interface can be either a network device or a software bridge; however broken links are not detected on software bridges.

Virtual IPV4 address:

choose the virtual IP address of your router for this subnet.

Netmask:

give the number of bits in the virtual address that hold the network part. (24 is the same as a 255.255.255.0 netmask, and so on).

Unicast peer IP:

VRRP can use unicast advertisement in place of multicast. The unicast IP address must be enabled during the master send the advertisement. Leave blank to use multicast advertisement.

Red cross:

with the red cross icon  you can delete an instance.

Subsection: SYNCHRONIZED SUBNETS GROUPS CONFIGURATION

Each instances group is given a name formed of letters, numbers and underscore sign. To create a group, enter a valid, unused name in the box at the bottom of the second subsection, then click the "Add" button. A group is created and you can set its properties:

Red cross:

with the red cross icon  you can delete a group.

Enable:

you must enable the group to use it. Disable it for tests.

Initial state:

this should reflect the intended role of the product for the group.

Advertisements period:

interval between two messages sent to the backup. A small value accelerates failure detection but increases network load.

Priority:

used for negotiation when several backups are set up. The default values assign a sensible value depending on the initial role.

Virtual router IDs:

a multi-selection box to select instances in the group.

Support connection tracking:

check to transfer connection information from the active router to the inactive one.

VII.1.10.8 Web Server

This menu allows to select and configure HTTP and HTTPS servers. Default is HTTP:



The other options available are:





For the HTTPS server, you can upload a web certificate file (PEM format). The certificate file is verified and uploaded when you **Save** or **Save & Apply**

VII.2 Tools Menu

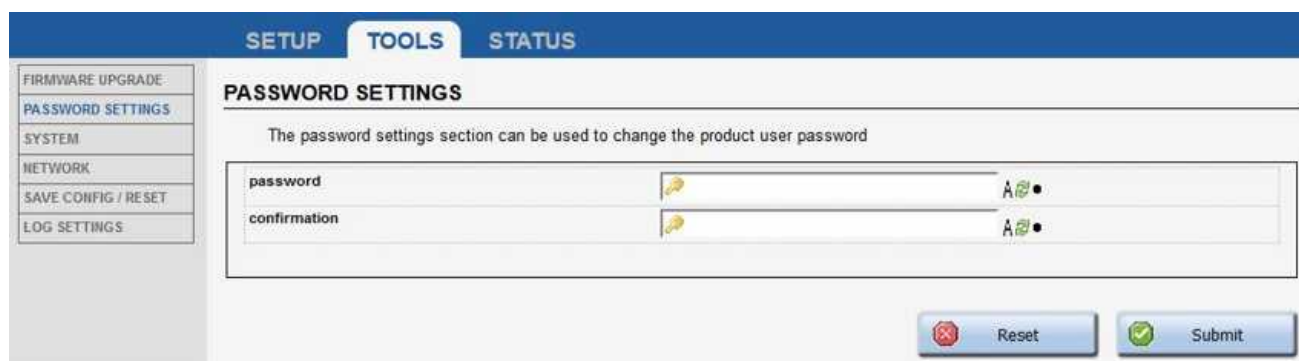
This menu allows you to administrate your product. A set of menu is provided and offers simplified the following possibilities:

VII.2.1 Firmware upgrade

Firmware upgrade has its own section in this user manual: [Firmware Upgrade](#).

VII.2.2 Password Settings

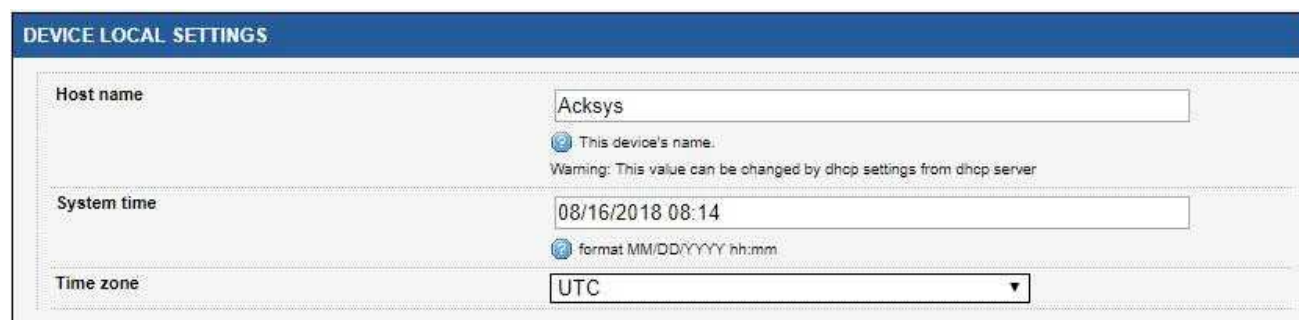
In this menu, you can modify the product's password.



The screenshot shows the 'PASSWORD SETTINGS' page. On the left is a sidebar menu with options: FIRMWARE UPGRADE, PASSWORD SETTINGS (selected), SYSTEM, NETWORK, SAVE CONFIG / RESET, and LOG SETTINGS. The main content area has a title bar with 'SETUP', 'TOOLS' (selected), and 'STATUS'. Below the title bar, the page is titled 'PASSWORD SETTINGS'. A descriptive text states: 'The password settings section can be used to change the product user password'. There are two input fields: 'password' and 'confirmation', each with a strength indicator (a yellow key icon and a green 'A' with a checkmark). At the bottom right, there are two buttons: 'Reset' (with a red 'X' icon) and 'Submit' (with a green checkmark icon).

VII.2.3 VII.2.3 System

VII.2.3.1 Device Local settings



The screenshot shows the 'DEVICE LOCAL SETTINGS' page. It has a title bar with 'DEVICE LOCAL SETTINGS'. The page contains three main settings: 'Host name' with a text input field containing 'Acksys', 'System time' with a text input field containing '08/16/2018 08:14', and 'Time zone' with a dropdown menu set to 'UTC'. Below the 'Host name' field, there is a warning message: 'Warning: This value can be changed by dhcp settings from dhcp server'. There are also small icons for 'This device's name' and 'format MM/DD/YYYY hh:mm'.

Host Name:

This is the name of the device. It can be changed the DHCP setting when the unit is configured as DHCP client. This text will be shown in the Device Info STATUS page.

System time and Time Zone:

Allows to set the current time and select your time zone.

ATTENTION: local time setting is lost at each reboot. No battery is provided to keep time accuracy during power off. Use a time server if needed.

VII.2.3.2 MIB-2 System Settings



MIB-2 SYSTEM SETTINGS

Device location:

this will appear in the MIB-2 'sysLocation' OID

Device Location:

This text will be shown in the WaveManager **Location** column, in the SNMP **sysLocation** value and in the browser caption.

VII.2.3.3 Network Timer Server



NETWORK TIMER SERVER

server name:

server port:

If the NTP server is reachable on the network, the product can use it to configure its local time.

One can use either IP address or domain name but the use of domain name requires configuring one or more DNS server addresses in the [Network configuration](#) section.

VII.2.4 Network Utilities



SETUP TOOLS STATUS

NETWORK UTILITIES

LINK DIAGNOSTIC

BANDWIDTH TEST

MODE	PROTOCOL	DELAY (\$)	DISPLAY (\$)
Server	TCP		1

LINK DIAGNOSTIC:

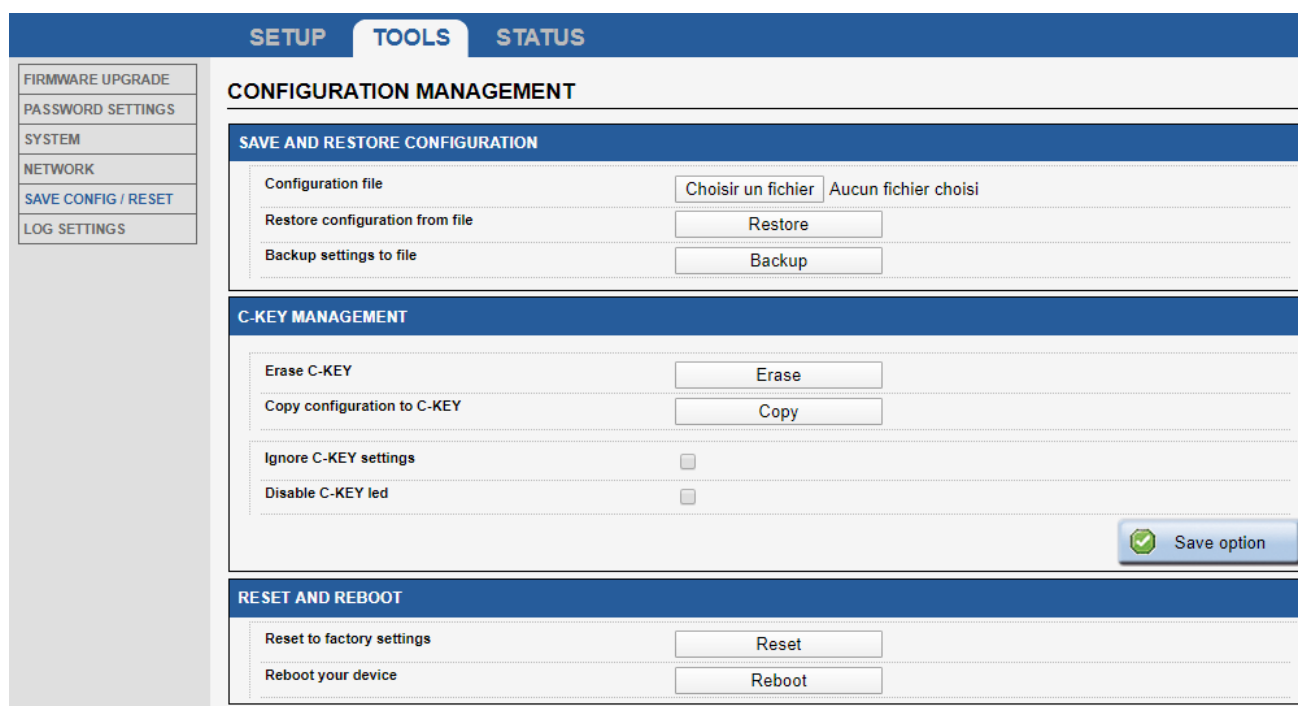
This panel provides two standard UNIX tools: ping and traceroute. Place the argument in the text field above the corresponding button and then click the button. The results will be displayed in a frame below.

You can use either an IP address or a domain name but the use of domain name requires to configure one or more DNS server addresses in the [Network configuration](#) section.

BANDWIDTH TEST:

Here you can perform an iPERF test, either in Server or Client mode, using TCP or UDP protocol. **DELAY** defines the duration of the test in seconds, while **DISPLAY** defines the status lines display interval in seconds.

VII.2.5 Save Config / Reset



Save And Restore Configuration:

With this panel, you can download the product configuration as file using the **backup settings to file**. The **Restore configuration from file** will ask for a previously saved configuration file and then restore it.

C-KEY Management:

Erase C-KEY:

This option will erase all the C-KEY contents. This has to be done before the first time you will copy configuration to the C-KEY.

Copy configuration to C-KEY:

This option will save your current configuration into the C-KEY. The configuration previously stored in the C-Key is kept in the C-Key as a backup; if the new configuration becomes damaged the backup will be loaded instead at boot time.



WARNING: the WPA keys and the various certificates (802.1x, HTTPS) will be copied as well. Anyone coming into possession of the C-Key can extract this information if no administration password has been defined.

Ignore C-KEY setting:

This option, if checked, will prevent the product from loading the C-KEY configuration at start-up. Otherwise the C-Key contents will overwrite the internal configuration files at boot time (default behavior).

Disable C-KEY led:

This option, if checked, will turn off the C-KEY status led permanently. This is useful if you don't have any C-KEY and do not want to see the permanently red C-KEY status LED. This can also be used to slightly reduce power consumption in case of embedded system.

Reset And Reboot:

Reset to factory settings:

This option will restore the default product settings.

Reboot your device:

As its name suggests, a click on this button will reboot the device.

VII.2.6 Log Settings

You can configure the log parameters on this page.

GENERAL SETTINGS			
System Log Output Level	Info ▼		
System Log Buffer Size	16		
	KiB		
External System Log Server	0.0.0.0		
External System Log Server Port	514		

WIRELESS ACCESS POINT LOG SETTINGS (WIFI)	
Wireless Log Level	Info ▼

VRRP SERVICE LOG SETTINGS	
VRRP log level	Error ▼

OPENVPN SERVERS LOG SETTINGS			
	NAME	MODE	VERBOSITY LEVEL
VPN1	vpn1	server	Errors ▼

General settings:

This section is about configuring the system log.

System Log Output Level:

Sets the minimum seriousness of a message to allow its insertion in the system log.

External System Log Server and Port:

Optional remote log server configuration. IP address and UDP port where the log messages will be sent using the syslog protocol. Leave empty to disable.

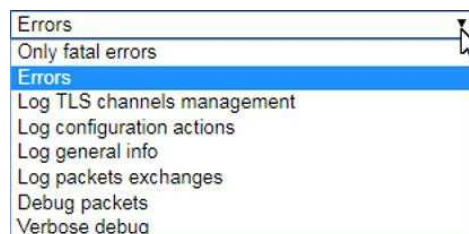
Log settings:

These sections are used to configure logging for various services. The messages are sent to the system log if their seriousness is above the configured level.

So, the log messages go through two rounds of filtering: one in the specific service and one in the syslog service. Please make sure the system log output level is high enough to display all required messages.

Verbosity Level:

Sets the minimum seriousness of a message relating to the OpenVPN server to allow its insertion in the system log.



VII.3 STATUS Menu

VII.3.1 Device Info

This page displays some useful information about the device. Providing the content of this page to the ACKSYS support team will speed up the technical support process.

SETUP	TOOLS	STATUS																				
DEVICE INFO NETWORK WIRELESS CELLULAR SERVICES LOGS	<h3>DEVICE INFORMATION</h3> <div> <h4>FIRMWARE INFORMATION</h4> <table border="1"> <tr> <td>WaveOS version:</td> <td>3.18.0.1</td> </tr> <tr> <td>Boot loader version:</td> <td>2.2.0.1</td> </tr> <tr> <td>Firmware ID:</td> <td>E2148.AC.1</td> </tr> </table> </div> <div> <h4>DEVICE INFORMATION</h4> <table border="1"> <tr> <td>Host name:</td> <td>MyHostName</td> </tr> <tr> <td>Model:</td> <td>RailBox/24A0</td> </tr> <tr> <td>Product version:</td> <td>V1</td> </tr> <tr> <td>Motherboard ID:</td> <td>0000177d21d8</td> </tr> <tr> <td>Product serial number :</td> <td>17234371</td> </tr> <tr> <td>C-KEY boot status:</td> <td>Factory state</td> </tr> <tr> <td>GNSS info:</td> <td>GNSS is disabled</td> </tr> </table> </div>		WaveOS version:	3.18.0.1	Boot loader version:	2.2.0.1	Firmware ID:	E2148.AC.1	Host name:	MyHostName	Model:	RailBox/24A0	Product version:	V1	Motherboard ID:	0000177d21d8	Product serial number :	17234371	C-KEY boot status:	Factory state	GNSS info:	GNSS is disabled
WaveOS version:	3.18.0.1																					
Boot loader version:	2.2.0.1																					
Firmware ID:	E2148.AC.1																					
Host name:	MyHostName																					
Model:	RailBox/24A0																					
Product version:	V1																					
Motherboard ID:	0000177d21d8																					
Product serial number :	17234371																					
C-KEY boot status:	Factory state																					
GNSS info:	GNSS is disabled																					

VII.3.2 Network

This page summarizes the network interfaces configuration and displays transmitted and received packets counts.

SETUP	TOOLS	STATUS																																																						
DEVICE INFO NETWORK ROUTES BRIDGES WIRELESS SERVICES LOG	<h3>INTERFACES</h3> <div> <h4>LAN</h4> <table border="1"> <thead> <tr> <th colspan="7">IP CONFIGURATION</th> </tr> <tr> <th colspan="7">IPv4: 192.168.2.252 Netmask: 24</th> </tr> <tr> <th>GRAPH</th> <th>PHYSICAL INTERFACE</th> <th>MAC ADDRESS</th> <th>TX COUNT (IN BYTES)</th> <th>RX COUNT (IN BYTES)</th> <th>INTERFACE MODE</th> <th>MTU</th> </tr> </thead> <tbody> <tr> <td></td> <td>WiFi 1</td> <td>04:f0:21:19:ea:8e</td> <td>2004</td> <td>0</td> <td>Role: Access Point (infrastructure) SSID: acksys Channel: 149</td> <td>1500</td> </tr> <tr> <td></td> <td>LAN 1</td> <td>02:00:17:7d:4b:2f</td> <td>19516</td> <td>7479</td> <td>Negotiated 1000 baseTX FD, link ok</td> <td>1500</td> </tr> <tr> <td></td> <td>LAN 2</td> <td>02:80:17:7d:4b:2f</td> <td>0</td> <td>0</td> <td>no link</td> <td>1500</td> </tr> </tbody> </table> </div> <div> <h4>VPN1 (VPN1)</h4> <table border="1"> <thead> <tr> <th colspan="4">CONNECTED PEERS</th> </tr> <tr> <th>COMMON NAME</th> <th>REAL ADDRESS</th> <th>BYTES RECEIVED</th> <th>BYTES SENT</th> </tr> </thead> <tbody> <tr> <td>Not available</td> <td>(null)</td> <td>0</td> <td>0</td> </tr> </tbody> </table> </div>		IP CONFIGURATION							IPv4: 192.168.2.252 Netmask: 24							GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU		WiFi 1	04:f0:21:19:ea:8e	2004	0	Role: Access Point (infrastructure) SSID: acksys Channel: 149	1500		LAN 1	02:00:17:7d:4b:2f	19516	7479	Negotiated 1000 baseTX FD, link ok	1500		LAN 2	02:80:17:7d:4b:2f	0	0	no link	1500	CONNECTED PEERS				COMMON NAME	REAL ADDRESS	BYTES RECEIVED	BYTES SENT	Not available	(null)	0	0
IP CONFIGURATION																																																								
IPv4: 192.168.2.252 Netmask: 24																																																								
GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU																																																		
	WiFi 1	04:f0:21:19:ea:8e	2004	0	Role: Access Point (infrastructure) SSID: acksys Channel: 149	1500																																																		
	LAN 1	02:00:17:7d:4b:2f	19516	7479	Negotiated 1000 baseTX FD, link ok	1500																																																		
	LAN 2	02:80:17:7d:4b:2f	0	0	no link	1500																																																		
CONNECTED PEERS																																																								
COMMON NAME	REAL ADDRESS	BYTES RECEIVED	BYTES SENT																																																					
Not available	(null)	0	0																																																					

Graph: graph availability

 : The history graph of the interface is unavailable because the function is disabled in the SETUP menu (SERVICES/COUNTER GRAPHS).

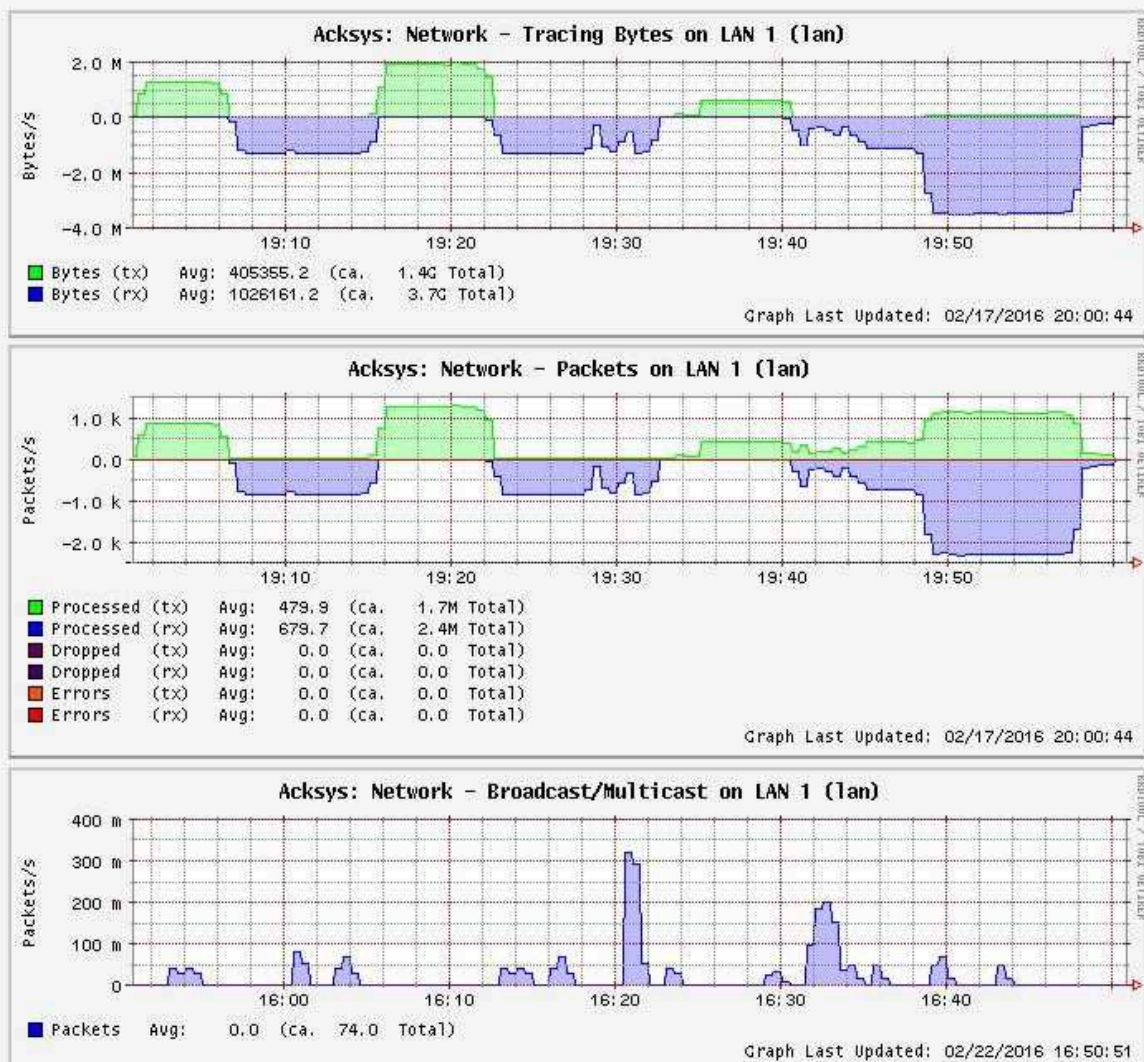
 : The history graph of the interface is available, click the icon to display the graph.

: The history graph of the bridged network is available, click to display the graph.

STATISTIC GRAPH : LAN 1 (LAN)

1hour

Display timespan »



This page displays the history graphs of the interface LAN 1:

Tracing bytes graph: displays the number of bytes sent (tx) and received (rx) on this interface.

Packets graph: displays the number of processed, dropped and error packets sent (tx) and received (rx) on this interface.

Broadcast/Multicast graph: displays the number of broadcast/multicast packets on this interface.

You can also configure the display duration to 10 minutes, 1 hours, 1 day, 1 week or 1 month.

VII.3.3 Routes

ACTIVE IPV4 ROUTES				
NETWORK	TARGET	IPV4-NETMASK	IPV4-GATEWAY	METRIC
lan	10.101.4.0	255.255.255.0	local	0

This page displays the active IPV4 routes on the product.

VII.3.4 Bridges

This page displays the port statuses of the STP/RSTP bridges, if there are bridges with STP/RSTP enabled in the product.

STP / RSTP										
LAN										
STP / RSTP STATUS										
Bridge Id: 8.000.02:00:17:7D:01:0C Designated Root: 8.000.02:00:17:7D:01:0C Root Port: none										
PHYSICAL INTERFACE	PORT ID	ROLE	STATE	PORT COST	DESIGNATED ROOT	DESIGNATED COST	DESIGNATED BRIDGE	DESIGNATED PORT	EDGE PORT	POINT TO POINT
LAN 1	8.001	Disabled	discarding	2e+8	8.000.02:00:17:7D:01:0C	0e+0	8.000.02:00:17:7D:01:0C	0.000	no	no
LAN 2	8.002	Designated	forwarding	2e+4	8.000.02:00:17:7D:01:0C	0e+0	8.000.02:00:17:7D:01:0C	8.002	no	yes
wlan0	8.003	Disabled	discarding	2e+8	8.000.02:00:17:7D:01:0C	0e+0	8.000.02:00:17:7D:01:0C	0.000	no	no

Physical interface: Port in the bridge

Port Id: Port identifier for the specified port, it is made up from the port priority and the interface number of the port.

Role: The Rapid Spanning Tree Algorithm assigns one of the following Port Roles to each Bridge Port: Root Port, Designated Port, Alternate Port, Backup Port, or Disabled Port.

The Disabled Port role is assigned if the port is not operational or is excluded from the active topology by management.

State: The port forwarding state:

For RSTP: it can be discarding, learning or forwarding.

For STP: it can be disabled, blocking, listening, learning or forwarding.

Port Cost: By default, it depends on the port speed, but it can be configured in the STP/RSTP settings.

Designated Root: Root Bridge for the Spanning tree. It is made up using the priority and base MAC address of the root bridge.

Designated Bridge: Bridge which contains the *Designated port*. It is made up from the priority and base MAC address of that bridge.

Designated port: Port that got the designated role among all bridge ports connected to this LAN (this includes the current port and the ports on the adjacent bridges). It is made up from the port priority and the interface number of the port.

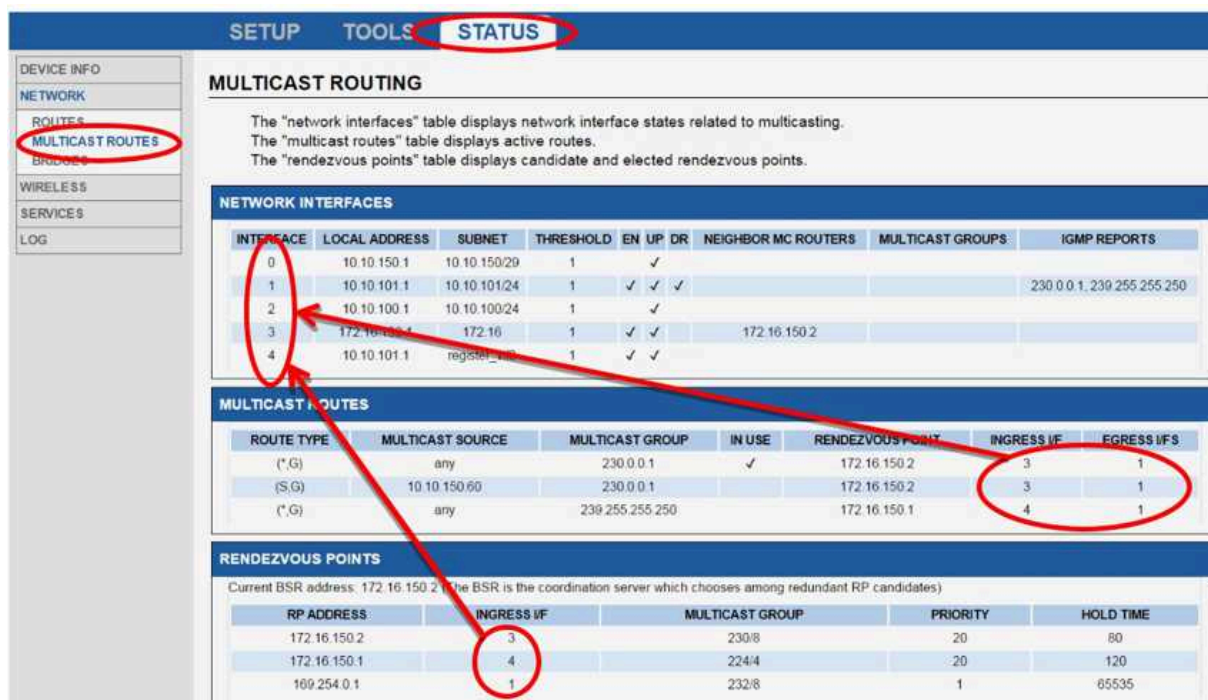
Designated Cost: Path cost to Root Bridge via the *Designated port* (Sum of ports costs of each root port on each bridge between the designated port and the Root Bridge)

Edge port: Set to true if the port is at the edge of the topology (connected to an end station), otherwise set to false.

Point to Point: Set to true if the port is connected to a point to point media (connected directly to another switch with a cable), otherwise set to false.

VII.3.5 Multicast routes

This page displays all available information about the running instance of the PIM multicast router.



MULTICAST ROUTING

The "network interfaces" table displays network interface states related to multicasting.
The "multicast routes" table displays active routes.
The "rendezvous points" table displays candidate and elected rendezvous points.

INTERFACE	LOCAL ADDRESS	SUBNET	THRESHOLD	EN	UP	DR	NEIGHBOR MC ROUTERS	MULTICAST GROUPS	IGMP REPORTS
0	10.10.150.1	10.10.150/20	1	✓					
1	10.10.101.1	10.10.101/24	1	✓	✓	✓			230.0.0.1, 239.255.255.250
2	10.10.100.1	10.10.100/24	1	✓					
3	172.16.150.1	172.16	1	✓	✓		172.16.150.2		
4	10.10.101.1	register_100	1	✓	✓				

ROUTE TYPE	MULTICAST SOURCE	MULTICAST GROUP	IN USE	RENDEZVOUS POINT	INGRESS I/F	EGRESS I/Fs
(*,G)	any	230.0.0.1	✓	172.16.150.2	3	1
(S,G)	10.10.150.60	230.0.0.1		172.16.150.2	3	1
(*,G)	any	239.255.255.250		172.16.150.1	4	1

Current BSR address: 172.16.150.2 (The BSR is the coordination server which chooses among redundant RP candidates)

RP ADDRESS	INGRESS I/F	MULTICAST GROUP	PRIORITY	HOLD TIME
172.16.150.2	3	230/8	20	80
172.16.150.1	4	224/4	20	120
169.254.0.1	1	232/8	1	65535

a Network interfaces section

Interface: network number referred to in ingress/egress columns.

Local address: Unicast IP address assigned to the network in Setup/Network page.

Subnet: the subnet this interface connects to, and the number of subnet bits. The [register_vif0](#) subnet is the special interface where senders send encapsulated data to their rendezvous point.

Threshold: Minimum TTL required to forward data to this interface.

EN: multicasting is enabled on this interface.

UP: this interface is available (e.g. the RJ45 connector is plugged in...).

DR: this router is Designated for this network.

Neighbor MC routers: other PIM routers directly connected to this network.

Multicast groups: PIM-SSM groups handled on this interface.

IGMP reports: list of groups for which receivers send join requests on this local network.

b Multicast routes section

Route type: (*,G) for any source to group, (S,G) for specific source to group.

Multicast source: source requested by the receiver: any or a specific IP address.

Multicast group: the group concerned by the route entry.

In use: this entry is actively used to forward data.

Rendezvous point: the IP address that was computed for the group.

Ingress I/F: interface where the multicast data is expected to arrive.

Egress I/F: interface list where the multicast data must be forwarded.

c Rendezvous points section

RP address: the IP address of the rendezvous point for this block of groups

Ingress I/F: interface toward the RP, hence, where data comes in.

Multicast group: the block of groups associated to this RP.

Priority: Priority of the RP for elections. Locally (statically) configured groups have a priority of 1.

Hold time: the delay after which this entry will become invalid if not refreshed in the meantime.

➤ Note that there is always an entry for the IP address 169.254.0.1 which is used internally to manage SSM routing.

VII.3.6 Wireless

VII.3.6.1 Associated Stations

If the radio card is in **access point mode**, this panel will list the clients connected to it and display RF signal properties.

If the radio card is in **client mode**, when it's associated with an access point, its RF details will be listed on this panel.

The signal level displayed is the one obtained from the **last frame received**, whatever its type (data or management) or modulation kind. So, **it is not comparable to the values appearing in the site survey**, which concern only probe and beacon frames.

Also, the signal level can vary a lot depending on the traffic. When data is received with a high MCS value, the signal can be low because typical transmitters are less powerful at high speeds; when no data is received the signal may raise because it is taken from low-rate beacons.

DEVICE INFO

NETWORK

WIRELESS

ASSOC STATIONS

SITE SURVEY

MESH SURVEY

CHANNEL STATUS

SERVICES

ASSOCIATED STATIONS

WIFI 1: NUMBER OF ASSOCIATIONS: 1

GRAPH	NAME / SSID	MODE	MAC	CHANNEL	SIGNAL LEVEL	NOISE LEVEL	SIGNAL/NOISE
	essidA	Infrastructure	96:A4:DE:AA:3F:AF	149	 -49 dBm	-107 dBm	58 dB

In client mode, the radio card associates with an access point

DEVICE INFO

NETWORK

WIRELESS

ASSOC STATIONS

SITE SURVEY

MESH SURVEY

CHANNEL STATUS

SETTINGS

ASSOCIATED STATIONS

WIFI 1: NUMBER OF ASSOCIATIONS: 1

GRAPH	NAME / SSID	MODE	MAC	CHANNEL	SIGNAL LEVEL	NOISE LEVEL	SIGNAL/NOISE
	essidA	Infrastructure	92:A4:DE:AA:3F:AF	149	 -79 dBm	0 dBm	-79 dB

In access point mode, one associated station.

DEVICE INFO

NETWORK

WIRELESS

ASSOC STATIONS

SITE SURVEY

MESH SURVEY

CHANNEL STATUS

ASSOCIATED STATIONS

WIFI 1: NUMBER OF ASSOCIATIONS: 0

GRAPH	NAME / SSID	MODE	MAC	CHANNEL	SIGNAL LEVEL	NOISE LEVEL	SIGNAL/NOISE
No information available							

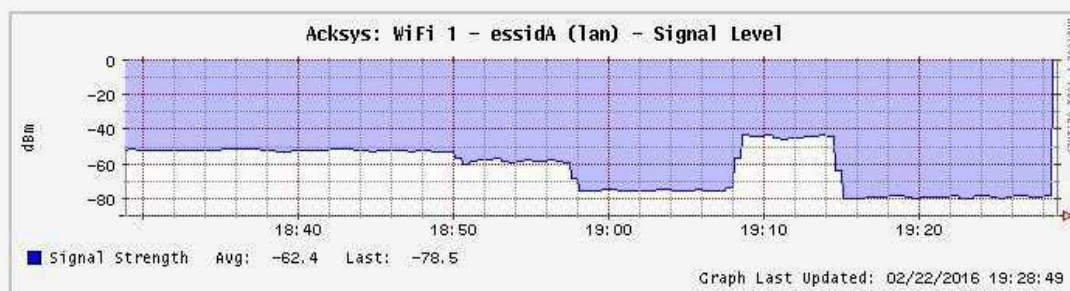
No associated station

You can display the statistic graph about signal strength by pressing the statistic graph icon . The statistic graph is only available for **client mode**. If the radio card is in **access point mode**, the statistic graph icon  will be disabled.

STATISTIC GRAPH : WIFI 1 - ESSIDA (LAN)

1hour

Display timespan »



This page displays the statistic graph of the wireless interface:

Signal Level graph: It displays signal level in dBm for wireless interface in real time.

You can also configure the display duration to 10 minutes, 1 hours, 1 day, 1 week or 1 month.

VII.3.6.2 Channel Status

This panel displays the availability of all wireless channels on each radio device.

DEVICE INFO	CHANNEL STATUS				
	WIFI				
NETWORK	CHANNEL	FREQUENCY	STATUS	DFS STATE	DFS CAC TIME
WIRELESS	1	2412 MHz	enabled	N.A	N.A
ASSOC STATIONS	2	2417 MHz	enabled	N.A	N.A
SITE SURVEY	3	2422 MHz	enabled	N.A	N.A
MESH SURVEY	4	2427 MHz	enabled	N.A	N.A
CHANNEL STATUS	5	2432 MHz	enabled	N.A	N.A
SERVICES	6	2437 MHz	enabled	N.A	N.A
LOG	7	2442 MHz	enabled	N.A	N.A
	8	2447 MHz	enabled	N.A	N.A
	9	2452 MHz	enabled	N.A	N.A
	10	2457 MHz	enabled	N.A	N.A
	11	2462 MHz	enabled	N.A	N.A
	12	2467 MHz	disabled	N.A	N.A
	13	2472 MHz	disabled	N.A	N.A
	14	2484 MHz	disabled	N.A	N.A
	36	5180 MHz	enabled	N.A	N.A
	40	5200 MHz	enabled	N.A	N.A
	44	5220 MHz	enabled	N.A	N.A
	48	5240 MHz	enabled	N.A	N.A
	52	5260 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
	56	5280 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
	60	5300 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
	64	5320 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
	100	5500 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
	104	5520 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
	108	5540 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
	112	5560 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
	116	5580 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
	120	5600 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
	124	5620 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
	128	5640 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
	132	5660 MHz	radar detection	unavailable (for 0d 00:01:16)	60000 ms
	136	5680 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
	140	5700 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
	149	5745 MHz	enabled	N.A	N.A
	153	5765 MHz	enabled	N.A	N.A
	157	5785 MHz	enabled	N.A	N.A
	161	5805 MHz	enabled	N.A	N.A
	165	5825 MHz	enabled	N.A	N.A

Status: channel constraints against the current Radio Regulation Area.

- Enabled: this channel is part of the current Regulation Area.
- Disabled: this channel is not part of the current Regulation Area.
- Radar detection: this channel is part of the current Regulation Area and Radar presence must be monitored.

DFS state: Dynamic Frequency Selection states for channels.

- Usable: The channel can be used, but channel availability check (CAC) must be performed before using it (Not in client mode, as it is the AP which manages the connection).
- Unavailable: A radar was detected on the channel, it cannot be used for the regulation-defined non-occupancy period (NOP).
- Available: The channel has been CAC checked and is available.

DFS CAC time:

The duration of the check for the presence of radar, before considering the channel as Available.

VII.3.6.3 MESH Survey

This panel summarizes properties for all 802.11s Mesh Points currently available.

DEVICE INFO NETWORK WIRELESS ASSOC STATIONS SITE SURVEY MESH SURVEY SERVICES	MESH SURVEY					
	RADIO					
	DST ADDRESS	NEXT HOP	METRIC	DISCOVERY TIMEOUT	DISCOVERY RETRIES	STATUS
	92:a4:de:aa:3f:b2	92:a4:de:aa:3f:b2	1366	100	0	Active DSN Valid Resolved

DST Address:

MAC address of the final destination.

Next Hop:

MAC address of the next mesh node in order to reach "DST Address".

Metric:

Represents the total cost of this mesh path (less is better).

Discovery Timeout:

Displays the current discovery timeout for this mesh path (in milliseconds)

Discovery retries:

As its name implies, displays the number of discovery retries.

Status:

Displays the mesh path current state.

Must be one of the following:

- Active : this mesh path can be used for forwarding
- Resolving : the discovery process for this mesh path is running
- Resolved : the discovery process ends successfully
- DSN Valid : the mesh path contains a valid destination sequence number

VII.3.6.4 Service status

DEVICE INFO NETWORK WIRELESS ASSOC STATIONS CHANNEL STATUS MESH SURVEY SERVICES STATUS SITE SURVEY SRCC STATUS SERVICES LOGS	SETUP TOOLS STATUS							
	SERVICES STATUS							
	WIFI 1							
	SERVICE	SSID	MAC	STATUS	CHANNEL	FREQUENCY	CHANNEL WIDTH	HT MODE
	Access Point	RadioTest	00:09:90:01:59:f2	ENABLED	36	5180 MHz	20 MHz (no HT)	NO HT

WIFI 2							
SERVICE	SSID	MAC	STATUS	CHANNEL	FREQUENCY	CHANNEL WIDTH	HT MODE
Access Point	Acksys	00:09:90:01:59:f3	ENABLED	44	5220 MHz	40 MHz	HT40+

Service status gives complementary information about the current state of the wireless interfaces. The STATUS field gives in particular useful information on the state of DFS channels.

VII.3.6.5 Site Survey

This feature allows to detect all access points within range. The results may depend on the mode the radio card is set to:

- When the radio card is in **client mode**, and a list of candidate channels is selected in the **Roaming** tab of the wireless setup, the survey will only include access points using the selected channels.
- When the radio card is in **access point mode**, the scan will disconnect associated clients.
- When the radio card is in **802.11s mesh mode**, some peers seem to appear and disappear at random because their beacon interval is large per the protocol definition, but the scan period is short.

On dual radio products, you can select the radio card with which you want to perform the site survey. Click on **Scan Radio** to start the survey. This operation may take a few minutes.

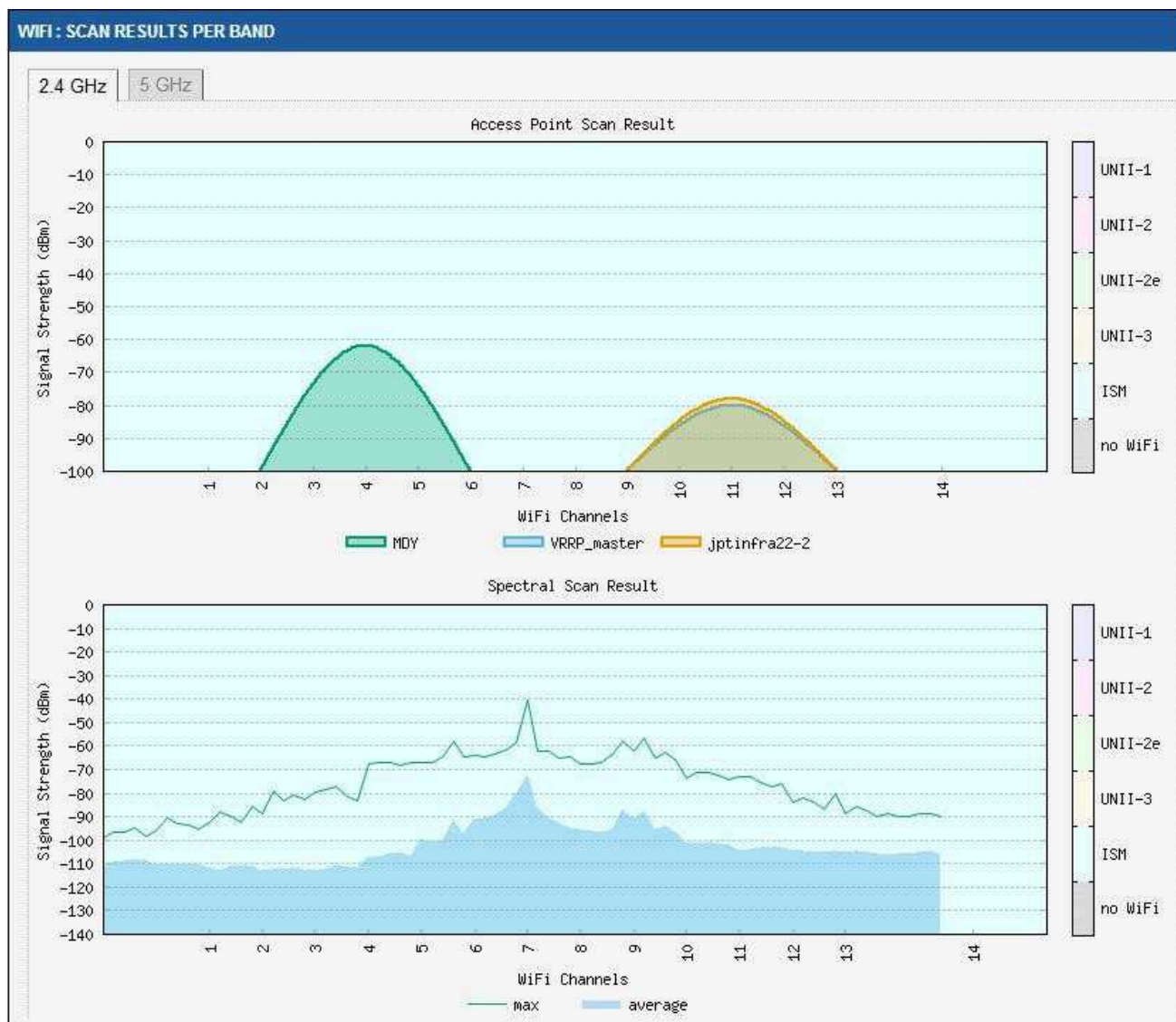


Please note that during the scan period, the radio card can no longer perform the function for which it is programmed. If, for example, it is configured as an Access Point, all associated clients will be temporarily disconnected. Also note that the site survey can work even when the radio card is not activated.

Attention, a disturbed environment can prevent the detection of certain Access Points, so it is not abnormal to have significantly different results between two successive site survey.

The first panel displays a radar view of the detected access points, and below the measured electromagnetic noise level. You can display the 2.4GHz band or the 5GHz band by clicking on the respective tabs.

We can see in the example below the presence of an electromagnetic noise around the frequency of channel 7. This noise is of non-Wi-Fi, because there is no access point on this frequency.



The lower table lists all the access points that could be detected.

WIFI 1 : SCAN RESULTS DETAILS

2.4 GHz - 5 GHz

NAME	CHANNEL	BANDWIDTH	ROLE	BSSID	ENCRYPTION	SIGNAL	
MDY	4	20 MHz	Access Point	00:1C:F0:08:CF:10	WPA2 PSK	-34 dBm	Join
VRRP_master	48	20 MHz	Access Point	04:F0:21:2C:6C:E3	None	-62 dBm	Join
jptinfra22-2	11	20 MHz	Access Point	04:F0:21:19:EB:95	WPA2 PSK	-75 dBm	Join
RADIOTEST	48	20 MHz	Access Point	00:09:90:00:C9:DA	None	-74 dBm	Join
RADIOTEST	48	20 MHz	Access Point	00:09:90:01:5A:17	None	-80 dBm	Join

Please note that the signal level of each detected Access Point is taken from probe and beacon frames only, which are sent at the lowest available rate. In general, the signal level found for these frames is better than the one from data frames.

WIFI 1 : SCAN RESULTS DETAILS							
2.4 GHz - 5 GHz							
NAME	CHANNEL	BANDWIDTH	ROLE	BSSID	ENCRYPTION	SIGNAL	
RADIOTEST	48	20 MHz	Access Point	00:09:90:00:C9:DA	None	-34 dBm	Join
RADIOTEST	48	20 MHz	Access Point	00:09:90:01:5A:17	None	-62 dBm	Join

The [Join](#) button in the right column of the result line does not appear if the SSID is hidden. You can click on this button to connect to this Access Point

WIFI 1 : SCAN RESULTS DETAILS							
2.4 GHz - 5 GHz							
NAME	CHANNEL	BANDWIDTH	ROLE	BSSID	ENCRYPTION	SIGNAL	
RADIOTEST	48	20 MHz	Access Point	00:09:90:00:C9:DA	None	-34 dBm	Join

Join with simplified configuration, if you want complete setup, please refer [setup page](#)

Wireless interface: WiFi 1 - RADIOTEST

SSID: RADIOTEST

Encryption: None

[Save & Apply](#)

RADIOTEST	48	20 MHz	Access Point	00:09:90:01:5A:17	None	-62 dBm	Join
-----------	----	--------	--------------	-------------------	------	---------	----------------------

Wireless interface allows to choose whether you want to replace the existing configuration or create a new instance on the radio card. This last option is not possible if the current configuration is already in the client (you cannot have more than one client role on a radio)

VII.3.6.6 SRCC Status

This page provides information on the status of the SRCC interface.

Here are some examples illustrating different stages of SRCC initialization:

Coach topology discovery

SRCC STATUS		
STATE: COACH TOPOLOGY DISCOVERY		
SRCC DISCOVER RESULT		
COACH SWITCH NODE LIST		
	MAC ADDRESS	SRCC TYPE

Wi-Fi neighbour discovery

SRCC STATUS		
STATE: WIFI NEIGHBOR DISCOVERY		
SRCC DISCOVER RESULT		
COACH SWITCH NODE LIST		
	MAC ADDRESS	SRCC TYPE
WIFI NEIGHBOR LIST		
	MAC ADDRESS	SIGNAL

Configuration complete

SRCC STATUS		
STATE: LINK CONFIGURED		
COACH CONFIGURATION		
POSITION IN COACH	MAC ADDRESS	SRCC TYPE
Local switch node	00:09:90:00:5a:f7	a
LINK CONFIGURATION		
MAC ADDRESS	ROLE	
00:09:90:00:5a:db	AP	
00:09:90:00:5a:f7	CLIENT	

VII.3.7 Services

VII.3.7.1 DHCP Lease

This panel summarizes the properties of all the current DHCP leases.

SETUP	TOOLS	STATUS
DEVICE INFO		
NETWORK		
WIRELESS		
SERVICES		
DHCP LEASE		

DHCP LEASES			
ACTIVE LEASES			
HOSTNAME	IPV4-ADDRESS	MAC-ADDRESS	LEASETIME REMAINING
There are no active leases.			

VII.3.7.2 VRRP

This panel displays the current state for the VRRP instances and groups configured in the product.

SETUP	TOOLS	STATUS
DEVICE INFO		
NETWORK		
WIRELESS		
SERVICES		
DHCP LEASE		
VRRP		
LOG		

VRRP			
ACTIVE INSTANCES AND GROUPS			
GROUP NAME	GROUP STATE	VRRP INSTANCE	VRRP STATE
routeA	backup	101	backup
		201	backup
routeB	master	102	master
		202	master

Here you can see that two virtual gateways are set up in this product. The first one is named "routeA" and groups virtual interfaces 101 and 201. It is currently inactive, because a master is detected on both interfaces.

The virtual gateway "routeB" is currently actively routing packets between virtual interfaces 102 and 202.

VII.3.8 Log

This panel allows visualizing the product logs.

The **Config log** displays a summary of the unit configuration, to verify that there are no inconsistencies in the configuration.

The **kernel log** displays log messages from the Linux kernel only. It is not filtered, i.e. it includes all recent messages sent by the kernel.

The **system log** displays log messages from both the kernel log and from the running services. The messages in this log are limited to the importance levels configured in the Setup/Tools/Log setting page.

In client mode, you can optionally display, in the system log, messages relating to the roaming process (see section VII.1.2 Advanced roaming tab). Please refer to the following table for the signification of the symbols surrounding the BSSID's (MAC addresses) displayed in these messages:

[B1:B2:B3:B4:B5:B6]	<i>BSSID of the current AP</i>
B1:B2:B3:B4:B5:B6	<i>BSSID of the AP selected for the next roaming</i>
/B1:B2:B3:B4:B5:B6/	<i>AP discarded by the 'matching SSID' test</i>
tB1:B2:B3:B4:B5:B6t	<i>AP discarded by the 'no return' test</i>
mB1:B2:B3:B4:B5:B6m	<i>AP laid aside by the 'minimum signal level' test</i>
MB1:B2:B3:B4:B5:B6M	<i>AP laid aside by the 'maximum signal level' test</i>

Note : An AP 'laid aside' can still be used if there is no other choice.

SYSTEM LOG

Save logs to file

```

Fri Nov 10 14:23:06 2017 daemon.notice wpa_supplicant[14834]: param low_ack = 50
Fri Nov 10 14:23:06 2017 daemon.notice wpa_supplicant[14834]: wlan0: acksys_roaming: oldstate DISCONNECTED -
Fri Nov 10 14:23:06 2017 daemon.notice wpa_supplicant[14834]: wlan0: autoscan_dualscan_init: reinitiated(scanon
Fri Nov 10 14:23:06 2017 daemon.notice wpa_supplicant[14834]: wlan0: autoscan_acksys_init: scan&associate
Fri Nov 10 14:23:06 2017 daemon.notice wpa_supplicant[14834]: wlan0: acksys_roaming: oldstate SCANONLY -> ne
Fri Nov 10 14:23:06 2017 daemon.notice wpa_supplicant[14834]: wlan0: autoscan_acksys_init: Init scan interva
Fri Nov 10 14:23:06 2017 daemon.notice netifd: radio0 (14087): adding wlan0 to wpa_supplicant: OK
Fri Nov 10 14:23:07 2017 daemon.notice wpa_supplicant[14834]: wlan0: autoscan_acksys: scan result notificati
Fri Nov 10 14:23:07 2017 daemon.notice wpa_supplicant[14834]: FG /04:f0:21:1b:5c:ed/ -71 -95 128 |
Fri Nov 10 14:23:07 2017 daemon.notice netifd: #####bridge_hotplug_add called
Fri Nov 10 14:23:07 2017 daemon.notice netifd: ##### bridge_create_member: create member wlan0
Fri Nov 10 14:23:07 2017 kern.warn kernel: [ 3042.616000] br_add_if: Add if wlan0 c4:93:00:07:78:7e
Fri Nov 10 14:23:07 2017 kern.info kernel: [ 3042.620000] device wlan0 entered promiscuous mode
Fri Nov 10 14:23:07 2017 daemon.notice netifd: radiol (14088): uci: Invalid argument
Fri Nov 10 14:23:07 2017 daemon.notice netifd: Network device 'wlan1' link is up
Fri Nov 10 14:23:07 2017 daemon.notice netifd: #####bridge_hotplug_add called
Fri Nov 10 14:23:07 2017 daemon.notice netifd: ##### bridge_create_member: create member wlan1
Fri Nov 10 14:23:08 2017 daemon.info Acksys discover: Daemon start
Fri Nov 10 14:23:08 2017 kern.info kernel: [ 3044.188000] br-lan: port 2(wlan1) entered forwarding state
Fri Nov 10 14:23:17 2017 daemon.notice wpa_supplicant[14834]: wlan0: autoscan_acksys: scan result notificati
Fri Nov 10 14:23:17 2017 daemon.notice wpa_supplicant[14834]: FG /04:f0:21:1b:5c:ed/ -73 -95 128 |

```

CONFIG LOG

Save logs to file

```

##### DEVICE LIST #####
Device_label Device_name Interface_name
-----
LAN 1 eth0 eth0
LAN 2 eth1 eth1
WiFi 1 phy0 radio0
WiFi 2 phy1 radiol

##### WIFI LIST #####
Interface_label Interface_name Network_included_in
-----
WiFi 1.RADIOTEST radio0w0 bond1
WiFi 2.RADIOTEST radiolw0 bond1

##### Check VLAN LIST #####
Nothing to report

##### VLAN LIST #####
vlan_description vlan_name Interface_attached_to vid Network_included_in interface_name
-----
Nothing to report

##### Check GRE/NETWORK LIST #####
Nothing to report

##### GRE LIST #####
gre_description gre_name gre_network local_endpoint_type tunlink
-----
Nothing to report

##### NETWORK LIST #####
network_description network_name network_proto network_type network_ifname
-----
loopback loopback static lo
lan lan static bridge eth0 eth1
bond1 bond1 bond ***N/A***

```

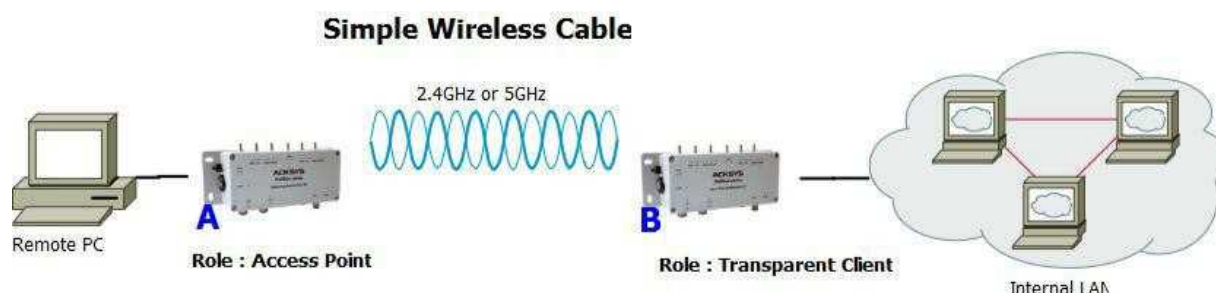
VIII WIRELESS TOPOLOGIES EXAMPLES

This products line has highly configurable devices allowing multiple wireless topologies. The followings sections describe the most used ones.

For every topology, the characteristic parameters for this topology are written in RED.

VIII.1 Simple “Wireless cable”

In this mode, an access point and an infrastructure bridge pair just replaces an existing Ethernet cable.



Configuration summary:

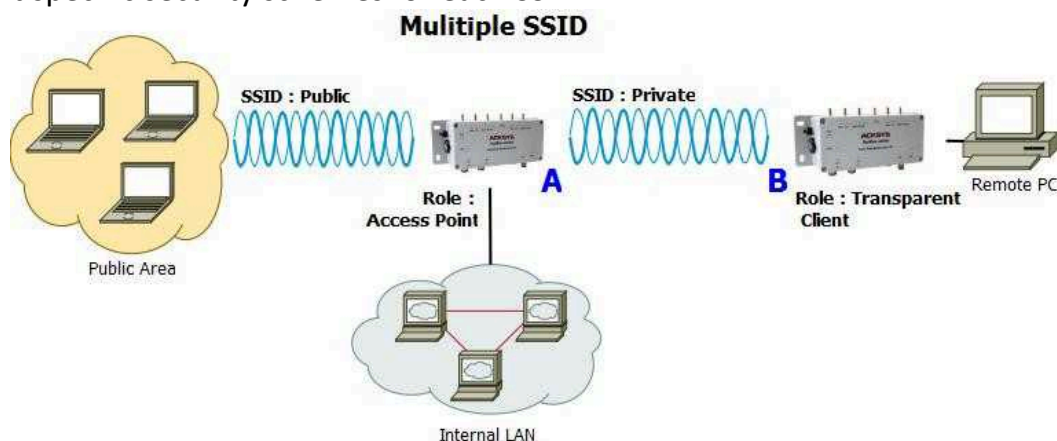
In this example, we are using 802.11a with 20MHz HT mode, channel 36, country code FR and ACKSYS as ESSID. You can obviously change any of these parameters as long as your choice makes sense.

Product A	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	802.11a
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration 1	
Parameter	Value
Role	Access Point
ESSID	ACKSYS

Product B	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	same as product A
Interface Configuration 1	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A

VIII.2 Multiple SSID

In this mode, a single access point provides multiple SSID at the same time in order to allow different specific security schemes for each SSID.



Configuration summary:

In this example, we are using 802.11na with 40MHz above HT mode, channel 36, country code FR, ACKSYS as private ESSID and SYSKCA as public ESSID. You can obviously change any of these parameters as long as your choice makes sense.

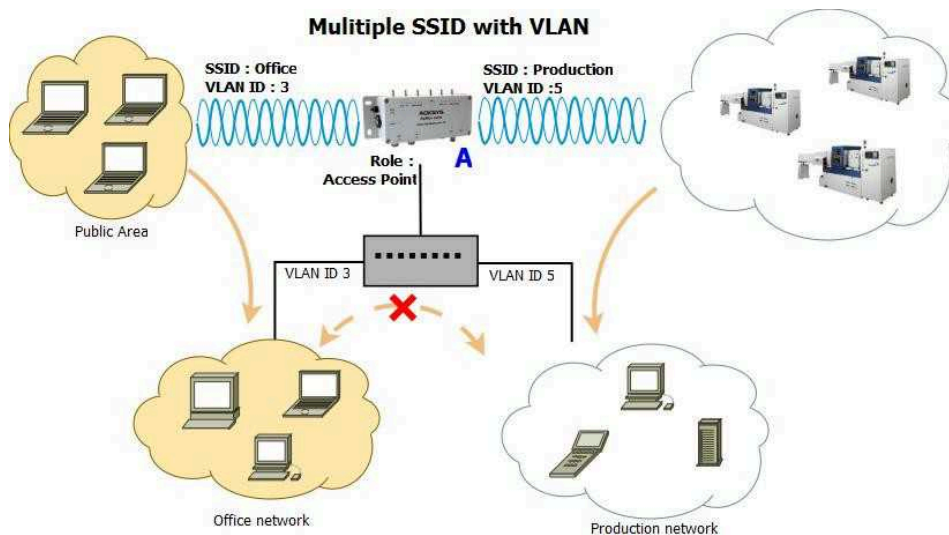
Product A	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	40MHz above
Channel	36
Country code	FR
Interface Configuration 1 (public)	
Parameter	Value
Role	Access Point
ESSID	SYSKCA
Interface Configuration 2 (Private)	
Parameter	Value
Role	Access Point
ESSID	ACKSYS

Product B	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	same as product A
Interface Configuration 1	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A private ESSID

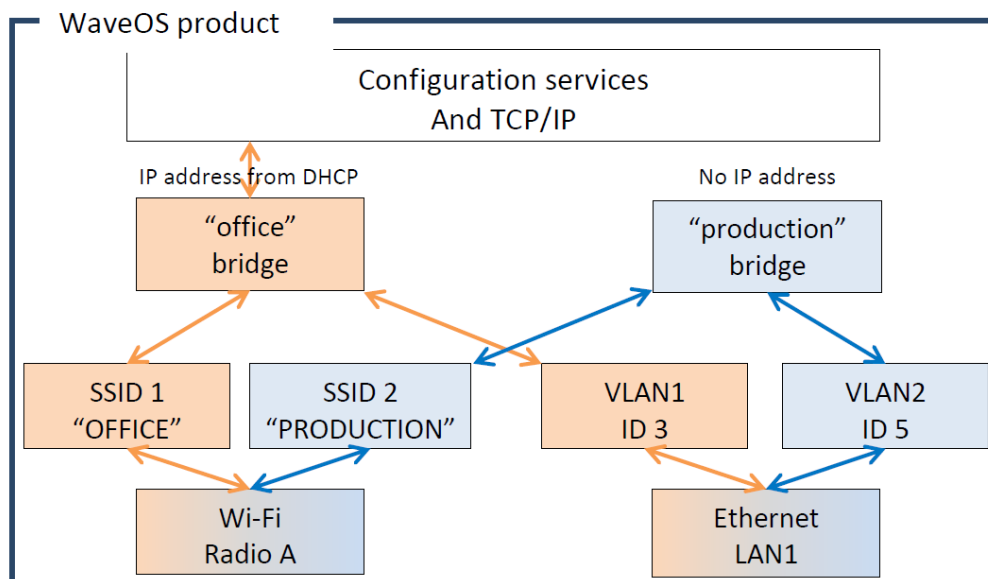
VIII.3 Multiple SSID with VLAN

In this configuration, a single access point provides multiple SSID at the same time in order to allow different security schemes for each SSID. All SSID traffic shares the same LAN interface. You can isolate SSID traffic from each other on the LAN using VLANs.

This mode adds a 802.1q tag in the frames sent to the LAN, and uses the tag in incoming LAN frames to forward data to the associated SSID. The tag itself is not transmitted over the Wi-Fi link.



The internal architecture of product “A” supporting this setting is:



Configuration summary:

Product A	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	40MHz above
Channel	36
Country code	FR
Interface Configuration 1 (Office)	
Parameter	Value
Role	Access Point
ESSID	OFFICE
Interface Configuration 2 (Production)	
Role	Access Point
ESSID	Production

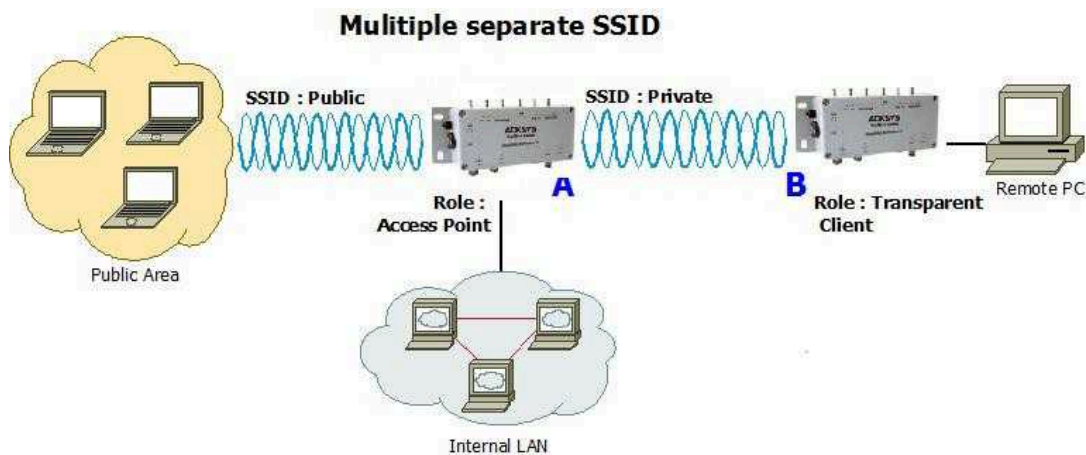
Virtual interface (VLAN 3)	
Parameter	Value
VLAN ID	3
Interface	LAN
Virtual interface (VLAN 5)	
VLAN ID	5
Interface	LAN
Network (office)	
Protocol	DHCP
Bridge interfaces	Checked
Interfaces	LAN.3 and "office" Wi-Fi adapter
Network (Production)	
Protocol	None
Bridge interface	Checked
Interfaces	LAN.5 and "production" Wi-Fi adapter

In order to achieve this configuration using the browser interface, you must change things in order:

- In the "virtual interfaces" menu, create the VLAN interfaces above the Ethernet LAN
- In the "physical interfaces" menu, set wireless radio settings and create one "access point" interface per needed SSID
- In the "network" menu, create one network per virtual network and use it to associate the VLAN from the Ethernet, with the SSID from the wireless radio.

VIII.4 Multiple separate SSID

In this mode, a single product uses its two radios to provide AP service simultaneously on two different channels or even radio bands, for better separation of functions (e.g. one channel for public access and one channel for SCADA).



Configuration summary:

In this example, we have two different configurations (one per radio card).

For Radio A (Public side):

Mode: 802.11na, HT mode: 40MHz above, channel: 36, country code: FR, ESSID: ACKSYS.
You can obviously change any of these parameters as long as your choice makes sense.

For Radio B (Private side):

Mode: 802.11na, HT mode: 40MHz above, channel: 44, country code: FR, ESSID: SYSKCA.
You can obviously change any of these parameters as long as your choice makes sense.



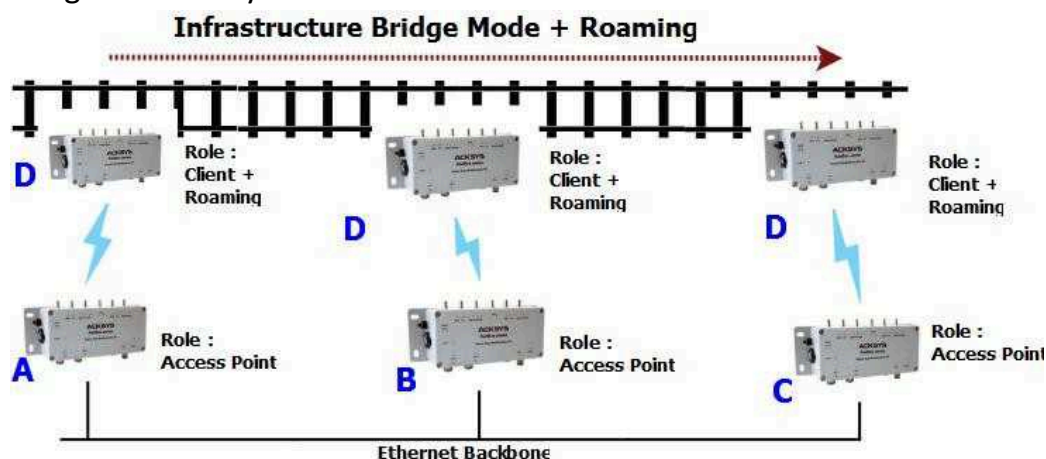
SWAA / SWSA User Guide

Product A	
Device Configuration 1 (radio A)	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	40MHz above
Channel	36
Country code	FR
Interface Configuration 1 (Radio A)	
Parameter	Value
Role	Access Point
ESSID	Private
Device Configuration 2 (Radio B)	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	40MHz above
Channel	44
Country code	FR
Interface Configuration 2 (Radio B)	
Parameter	Value
Role	Access Point
ESSID	Public

Product B	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	40MHz above
Channel	44
Country code	same as product A
Interface Configuration 1	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A private ESSID

VIII.5 Infrastructure bridge + Roaming

In this mode an infrastructure bridge can switch from an access point to another without breaking connectivity.



Configuration summary:

In this example, we are using the same parameters than previously with a roaming threshold set to -60dBm and a 5s scan cycle period.

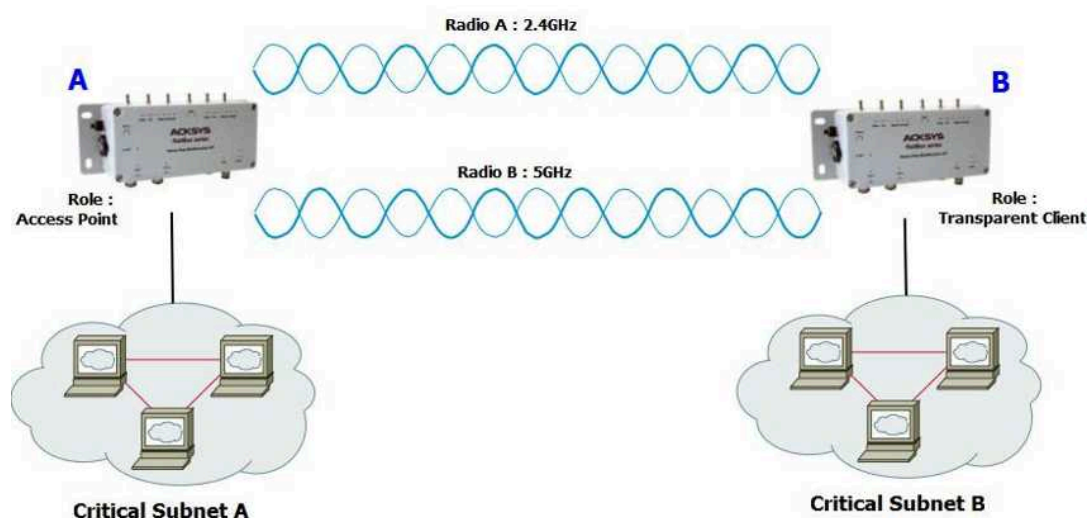
Product A, B, C	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	40MHz above
Channel	36
Country code	FR
Interface Configuration 1 (public)	
Parameter	Value
Role	Access Point
ESSID	ACKSYS

Product D	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	same as product A
Interface Configuration 1	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A private ESSID
Roaming	
Parameter	Value
Enable proactive roaming	on
Channel	same as product A
Current AP minimum level	-60
Delay between 2 successive scan cycle	5000

VIII.6 Point-to-point redundancy with dual band

In this mode, two dual radio products form a redundancy link by creating two wireless links on different channels. Only one link transfers data at a time. If one of the two links breaks down, the second one will replace it.

2.4GHz/5GHz Redundancy



Configuration summary:

In this example, we have two different configurations (one per radio card). You can obviously change any of these parameters as long as your choice makes sense.

For Radio A:

Mode: 802.11ng, HT mode: 20MHz, channel: 11, country code: FR, ESSID: ACKSYS1.

For Radio B:

Mode: 802.11na, HT mode: 20MHz, channel: 36, country code: FR, ESSID: ACKSYS2.

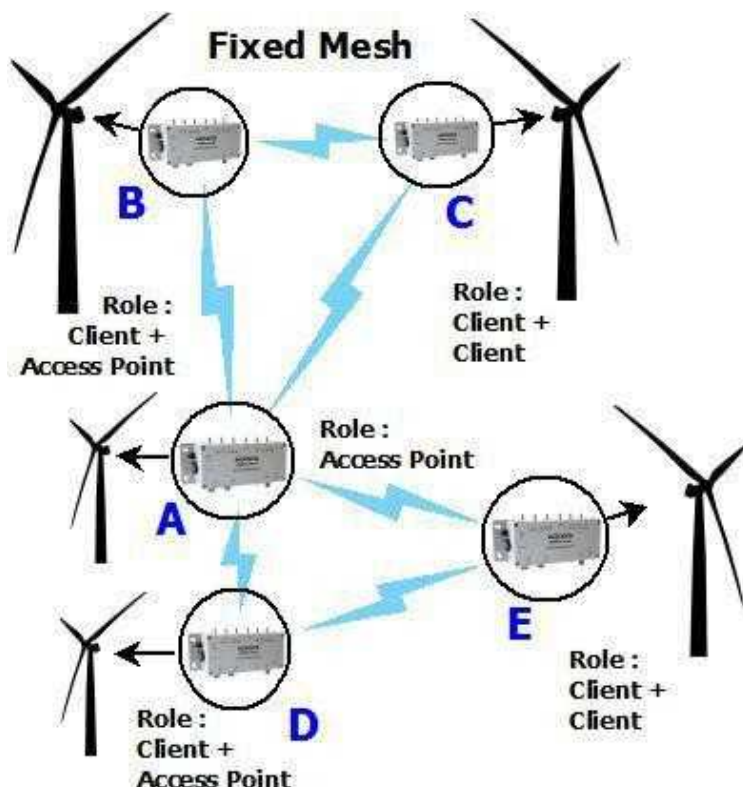
ATTENTION: This topology creates a network loop. You must provide a way to cut one of the two Wi-Fi links. This is usually done by using STP or RSTP inside the products. The product series provides STP since firmware 1.4.0 . STP must be activated in both Product A and Product B. See section “Spanning Tree Protocols (STP, RSTP)” for more details.

Product A	
Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	802.11ng
HT mode	20MHz
Channel	11
Country code	FR
Interface Configuration 1 (Radio A)	
Parameter	Value
Role	Access Point
ESSID	ACKSYS1
Device Configuration (Radio B)	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration 1 (Radio B)	
Parameter	Value
Role	Access Point
ESSID	ACKSYS2

Product B	
Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	same as product A
Interface Configuration 1 (Radio A)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A
Device Configuration (Radio B)	
Parameter	Value
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	same as product A
Interface Configuration 1 (Radio B)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A

VIII.7 Fixed Mesh

This topology provides a convenient way to handle loop/redundancy on your network.



Configuration summary:

You can obviously change any of these parameters as long as your choice makes sense.

Mode (Product **A** and Radio A for Products **B, C, D, E**): 802.11na, HT mode: 20MHz, channel: 36, country code: FR, ESSID: ACKSYS.

Mode (Radio B for Products **B, C**): 802.11na, HT mode: 20MHz, channel: 40, country code: FR, ESSID: ACKSYS2.

Mode (Radio B for Products **D, E**): 802.11na, HT mode: 20MHz, channel: 60, country code: FR, ESSID: ACKSYS3.

ATTENTION: This topology may create one or more network loop. You must provide a way to cut them. This is usually done by using STP or RSTP inside the products. This products series provides STP since firmware 1.4.0. STP needs to be activated in each product. See section [VII.1.5.1 Network configuration](#) for more details.



SWAA / SWSA User Guide

Product A	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration	
Parameter	Value
Role	Access Point
ESSID	ACKSYS
Product C	
Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	same as product A
Interface Configuration (Radio A)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	ACKSYS
Device Configuration (Radio B)	
Parameter	Value
Enable device	on
802.11 mode	same as product B (Radio B)
HT mode	same as product B (Radio B)
Channel	same as product B (Radio B)
Country code	same as product B (Radio B)
Interface Configuration (Radio B)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	Same as product B (Radio B)

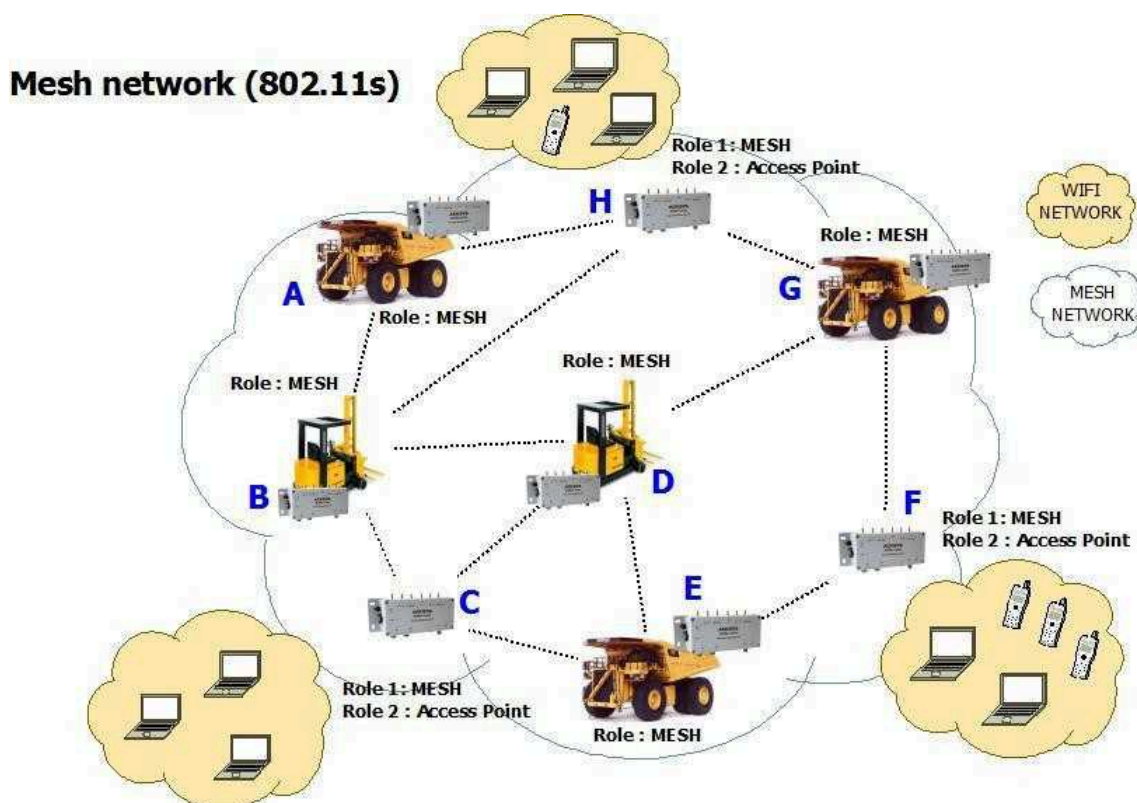
Product B	
Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	same as product A
Interface Configuration (Radio A)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	ACKSYS
Device Configuration (Radio B)	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	40
Country code	FR
Interface Configuration (Radio B)	
Parameter	Value
Role	Access Point
ESSID	ACKSYS2

Product D	
Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	same as product A
Interface Configuration (Radio A)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	ACKSYS
Device Configuration (Radio B)	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	60
Country code	FR
Interface Configuration (Radio B)	
Parameter	Value
Role	Access Point
ESSID	ACKSYS3

Product E	
Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	same as product A
Interface Configuration (Radio A)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A
Device Configuration (Radio B)	
Parameter	Value
Enable device	on
802.11 mode	Same as product D (Radio B)
HT mode	Same as product D (Radio B)
Channel	Same as product D (Radio B)
Country code	Same as product D (Radio B)
Interface Configuration (Radio B)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product D (Radio B)

VIII.8 802.11s Mesh

This topology uses the IEEE 802.11s standard. There is an overview of 802.11s in the section [V.2.1.3 Mesh \(802.11s\) Mode](#)



Configuration summary:

You can obviously change any of these parameters as long as your choice makes sense.

Mode (Products **A, B, E, D, G** and Radio A for Products **C, F, H**): 802.11na, HT mode: 20MHz, channel: 36, country code: FR, MESHID: ACKSYS.

Mode (Radio B for Products **C**): 802.11na, HT mode: 20MHz, channel: 40, country code: FR, ESSID: ACKSYS1.

Mode (Radio B for Products **F**): 802.11na, HT mode: 20MHz, channel: 44, country code: FR, ESSID: ACKSYS2.

Mode (Radio B for Products **H**): 802.11na, HT mode: 20MHz, channel: 48, country code: FR, ESSID: ACKSYS3.

Product A, B, E, D, G

Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration	
Parameter	Value
Role	Mesh (802.11s)
MESHID	ACKSYS

Product F

Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	same as product A
Interface Configuration (Radio A)	
Parameter	Value
Role	Mesh (802.11s)
MESHID	ACKSYS

Product C

Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	same as product A
Interface Configuration (Radio A)	
Parameter	Value
Role	Mesh (802.11s)
MESHID	ACKSYS
Device Configuration (Radio B)	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	40
Country code	FR
Interface Configuration (Radio B)	
Parameter	Value
Role	Access Point
ESSID	ACKSYS1
Product H	
Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	same as product A
Interface Configuration (Radio A)	
Parameter	Value
Role	Mesh (802.11s)
MESHID	ACKSYS



SWAA / SWSA User Guide

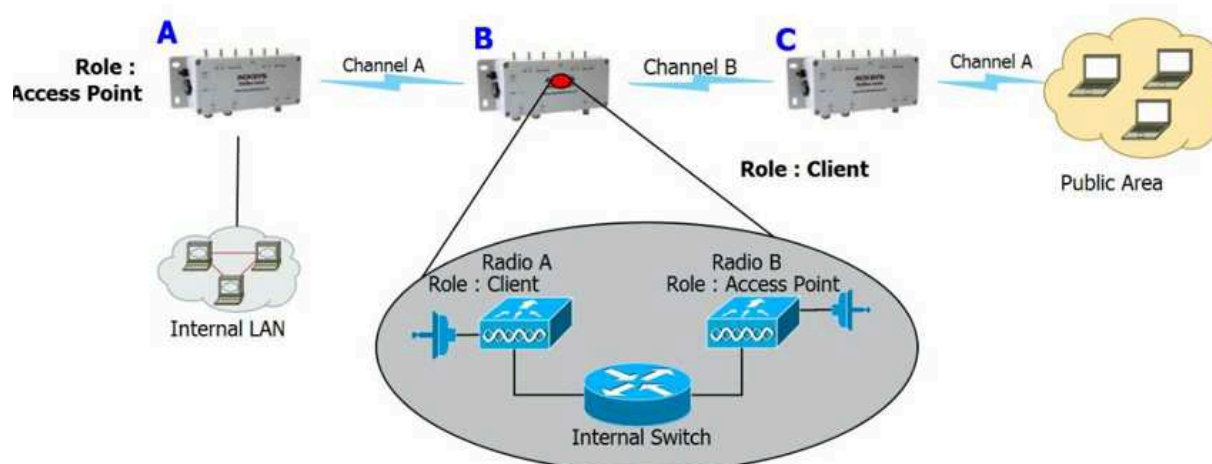
Device Configuration (Radio B)	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	44
Country code	FR
Interface Configuration (Radio B)	
Parameter	Value
Role	Access Point
ESSID	ACKSYS2

Device Configuration (Radio B)	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	48
Country code	FR
Interface Configuration (Radio B)	
Parameter	Value
Role	Access Point
ESSID	ACKSYS3

VIII.9 High performance repeater

This mode takes advantage of the dual radio card device to implement a high-performance repeater.

Hi-performance repeater mode



Configuration summary:

Mode (Product **A** to Product **B**): 802.11na, HT mode: 20MHz , channel: 36, country code: FR, ESSID: ACKSYS1. You can obviously change any of these parameters as long as your choice makes sense.

Mode (Product **B** to Product **C**): 802.11na, HT mode: 20MHz , channel: 44, country code: FR, ESSID: ACKSYS2. You can obviously change any of these parameters as long as your choice makes sense.

This configuration allows to not share the Wi-Fi channel. In this example, Radio A of Product **B** only communicates with Product **A** while Radio B of Product **B** only communicates with Product **C**.

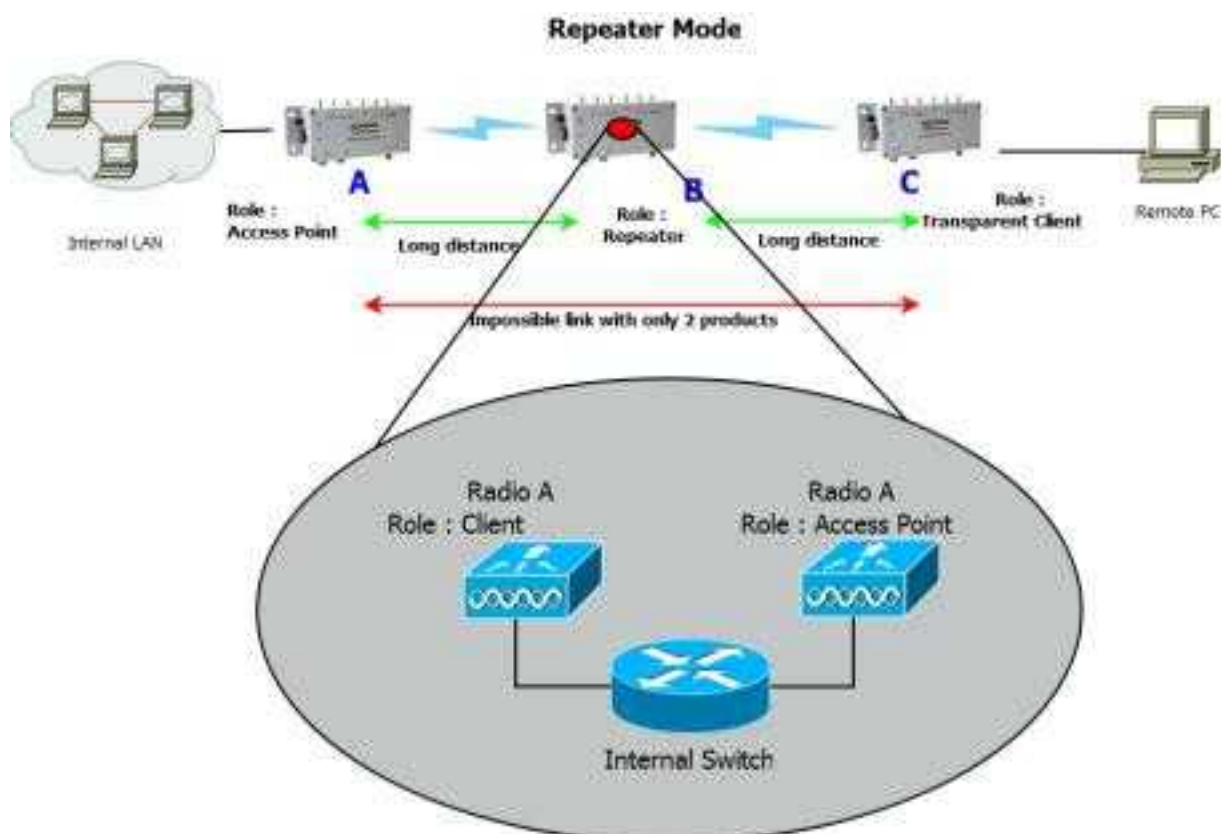
Attention: You must choose different channels for Radio A and Radio B.

Product A	
Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	40MHz above
Channel	36
Country code	FR
Interface Configuration 1 (Radio A)	
Parameter	Value
Role	Access Point
ESSID	ACKSYS1
Product B	
Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	40MHz above
Channel	36
Country code	FR
Interface Configuration (Radio A)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	ACKSYS1
Device Configuration (Radio B)	
Parameter	Value
Enable device	on
802.11 mode	802.11ng
HT mode	40MHz above
Channel	44
Country code	FR
Interface Configuration (Radio B)	
Parameter	Value
Role	Access Point
ESSID	ACKSYS2

Product C	
Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	40MHz above
Channel	44
Country code	FR
Interface Configuration (Radio A)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	ACKSYS2
Device Configuration (Radio B)	
Parameter	Value
Enable device	on
802.11 mode	802.11ng
HT mode	40MHz above
Channel	36
Country code	FR
Interface Configuration (Radio B)	
Parameter	Value
Role	Access Point
ESSID	ACKSYS1

VIII.10 Line topology repeater (single radio card)

Using this mode, you can extend the link distance by adding one or more intermediate repeater devices.



Configuration summary:

Mode: 802.11na, HT mode: 20MHz, channel: 36, country code: FR, ESSID: ACKSYS. You can obviously change any of these parameters as long as your choice makes sense.

The repeater role is equivalent to one access point and one bridge infrastructure in the same radio card. In the example above, product **B** acts as a client of product **A** and as an access point with product **C**.

Both products **A** and **B** have the same SSID; in order to avoid associating with itself, the repeater needs to know the BSSID of the access point with whom it must associate with (product **A** in this example).

Product **C** is set to 4-addresses bridging mode. This is the best way to achieve transparent communication. Other modes (like ARPNAT) would also work, but with caveats; see section [V.2.5 Wired to wireless bridging in infrastructure mode](#) for more information.

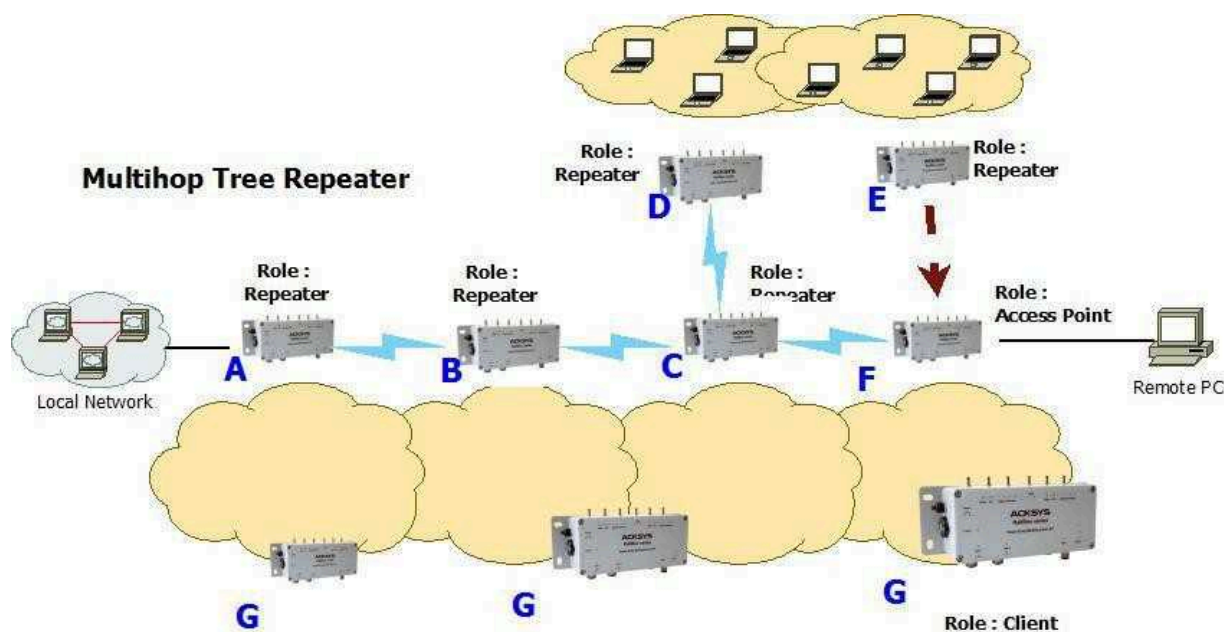
Product A	
Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration 1 (Radio A)	
Parameter	Value
Role	Access Point
ESSID	ACKSYS

Product C	
Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration 1 (Radio A)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A

Product B	
Device Configuration (Radio A)	
Parameter	Value
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	same as product A
Interface Configuration 1 (Radio A)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
Multiple ESSIDs	on
Wireless Network Nicknames	SSID_ACKSYS
ESSID Configuration (SSID_ACKSYS)	
Parameter	Value
WLAN description	SSID_ACKSYS
ESSID	same as product A
Priority group	7
BSSID	Product A radio card MAC address
Interface Configuration 2 (Radio A)	
Parameter	Value
Role	Access Point
ESSID	same as product A

VIII.11 Multihop tree repeater

You can also extend the coverage area in several directions and still get full connectivity by adding one or more intermediate repeater devices.



Configuration summary:

Mode: 802.11na, HT mode: 20MHz, channel: 36, country code: FR, ESSID: ACKSYS. You can obviously change any of these parameters as long as your choice makes sense.

This topology shows that repeaters interconnection is not limited to a line. Nevertheless, the repeaters interconnections are limited to a tree structure. However this does not limit data exchange, which can take place between any two devices in the tree.

Product **F** (the last product in the tree) must be set to access point mode. Theoretically, product **F** could be configured in repeater mode but the client portion of the repeater would consume radio bandwidth trying to associate.



SWAA / SWSA User Guide

Product A	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration 1 (Radio A)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
Multiple ESSIDS	on
Wireless Network Nicknames	SSID_ACKSYS
ESSID Configuration (SSID_ACKSYS)	
Parameter	Value
WLAN description	SSID_ACKSYS
ESSID	ACKSYS
Priority group	7
BSSID	Product B radio card MAC address
Interface Configuration 2 (Radio A)	
Parameter	Value
Role	Access Point
ESSID	ACKSYS
Product C	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration 1 (Radio A)	
Parameter	Value
Role	Client

Product B	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration 1 (Radio A)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
Multiple ESSIDS	on
Wireless Network Nicknames	SSID_ACKSYS
ESSID Configuration (SSID_ACKSYS)	
Parameter	Value
WLAN description	SSID_ACKSYS
ESSID	same as product A
Priority group	7
BSSID	Product C radio card MAC address
Interface Configuration 2 (Radio A)	
Parameter	Value
Role	Access Point
ESSID	same as product A
Product D	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration 1 (Radio A)	
Parameter	Value
Role	Client

Bridging mode	4 addresses format (WDS)
Multiple ESSIDS	on
Wireless Network Nicknames	SSID_ACKSYS
ESSID Configuration (SSID_ACKSYS)	
Parameter	Value
WLAN description	SSID_ACKSYS
ESSID	same as product A
Priority group	7
BSSID	Product F radio card MAC address
Interface Configuration 2 (Radio A)	
Parameter	Value
Role	Access Point
ESSID	same as product A
Product E	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration 1 (Radio A)	
Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
Multiple ESSIDS	on
Wireless Network Nicknames	SSID_ACKSYS
ESSID Configuration (SSID_ACKSYS)	
Parameter	Value
WLAN description	SSID_ACKSYS
ESSID	same as product A
Priority group	7
BSSID	Product F radio card MAC address
Interface Configuration 2 (Radio A)	

Bridging mode	4 addresses format (WDS)
Multiple ESSIDS	on
Wireless Network Nicknames	SSID_ACKSYS
ESSID Configuration (SSID_ACKSYS)	
Parameter	Value
WLAN description	SSID_ACKSYS
ESSID	same as product A
Priority group	7
BSSID	Product C radio card MAC address
Interface Configuration 2 (Radio A)	
Parameter	Value
Role	Access Point
ESSID	same as product A
Product F	
Device Configuration	
Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration	
Parameter	Value
Role	Access Point
ESSID	same as product A



SWAA / SWSA User Guide

<i>Parameter</i>	<i>Value</i>
Role	Access Point
ESSID	same as product A
Product G	
<i>Device Configuration</i>	
<i>Parameter</i>	<i>Value</i>
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR
<i>Interface Configuration</i>	
<i>Parameter</i>	<i>Value</i>
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A
<i>Roaming</i>	
<i>Parameter</i>	<i>Value</i>
Enable proactive roaming	on
Channel	same as product A
Current AP minimum level	-60
Delay between 2 successive scan cycle	5000

IX FIRMWARE UPGRADE

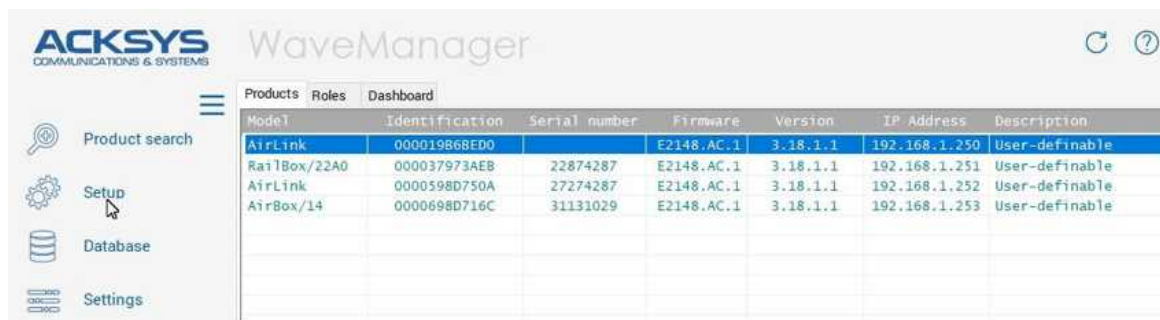
IX.1 Standard upgrade

Uploading a new version of the firmware is easily done from the web interface page **TOOLS→Firmware upgrade**



All previous configuration changes will be left unchanged.

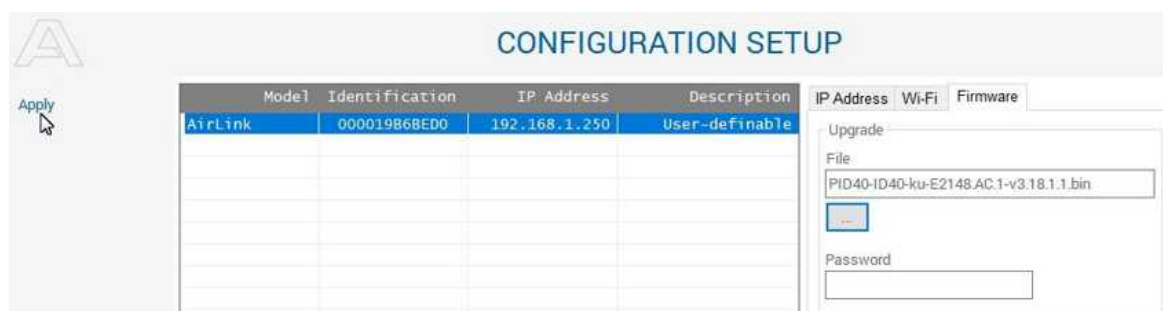
WaveManager is also a convenient way to upgrade your Acksys product. It's particularly interesting for batch updates. In the product list, select the unit you want to upgrade and click **Setup**



Model	Identification	Serial number	Firmware	Version	IP Address	Description
AirLink	000019868ED0		E2148.AC.1	3.18.1.1	192.168.1.250	User-definable
RailBox/22A0	000037973AEB	22874287	E2148.AC.1	3.18.1.1	192.168.1.251	User-definable
AirLink	0000598D750A	27274287	E2148.AC.1	3.18.1.1	192.168.1.252	User-definable
AirBox/14	0000698D716C	31131029	E2148.AC.1	3.18.1.1	192.168.1.253	User-definable

If the subnet of the product doesn't match the subnet of your computer, you can change its IP address before upgrading from this page.

Then, select the Firmware tab on the right, find the firmware binary file on your disk, enter the admin password if needed, and click **Apply**



Model	Identification	IP Address	Description
AirLink	000019868ED0	192.168.1.250	User-definable

Upgrade

File: PID40-ID40-ku-E2148.AC.1-v3.18.1.1.bin

Password:

Apply

If you want to upgrade several units (same model), you just need to make a multi-selection in both windows:



The screenshot shows the 'CONFIGURATION SETUP' window. On the left, there is an 'Apply' button. The main area contains a table with the following data:

Model	Identification	IP Address	Description
AirLink	000019868ED0	192.168.1.250	User-definable
AirLink	00001980750A	192.168.1.252	User-definable

On the right, there is a panel with tabs for 'IP Address', 'Wi-Fi', and 'Firmware'. The 'Firmware' tab is selected, showing an 'Upgrade' section with a 'File' input field containing 'PID40-ID40-ku-E2148.AC.1-v3.18.1.1.bin' and a 'Password' input field.

For more information, please refer to the WaveManager user's guide.

IX.2 Bootloader upgrade

The bootloader is a separate module which handles product bootup and emergency upgrade. Since it is so essential, this is a critical upgrade and the product might be damaged if a power failure happens during this upgrade. So, you should upgrade the bootloader only if requested by ACKSYS in order to avoid a product return.

Please respect the following recommendations:

- be sure to use a robust power supply
- choose a quiet desk instead of production line
- wait until the complete product reboot before trying to refresh the web page
- do not hesitate to contact the ACKSYS support team (support@acksys.fr) if you have any question

Please contact Acksys technical support to obtain the bootloader package corresponding to your product. The bootloader upgrade may be applied using the TOOLS/FIRMWARE UPGRADE page in the internal web interface. The procedure uses the same upgrade process than the regular firmware upgrade:

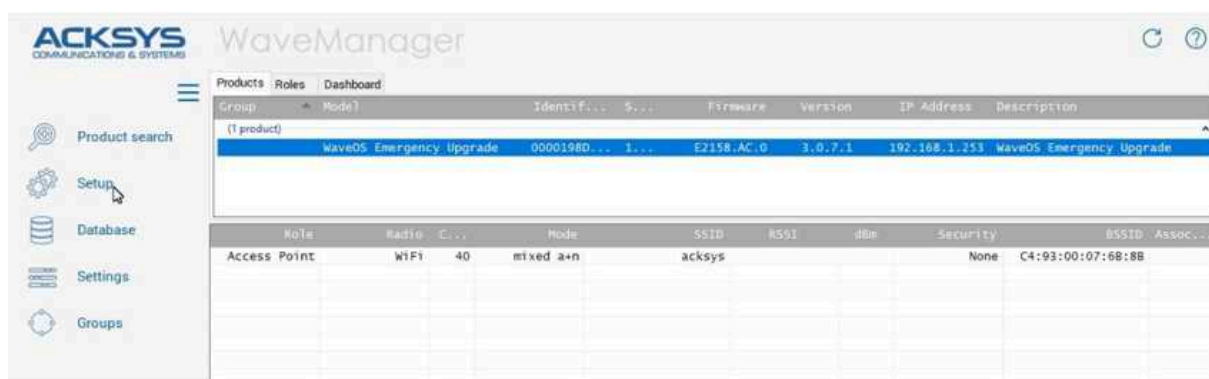
- click the **Browse** button in order to select the upgrade file
- click the **Execute** button in order to perform the upgrade

IX.3 Fallback after an interrupted upgrade operation

If the upgrade process fails due (for example) to an unexpected power supply failure during Flash EPROM programming, the product will automatically switch to failover mode.

At its next reboot the product will find out that the firmware is incomplete and the **Emergency upgrade** mode will start automatically. You can recognize that the product is in this failover mode because its **DIAG LED** will blink quickly (remind that this LED is green or OFF in normal working mode). The product will then execute a restricted service allowing only firmware uploads from the ACKSYS WaveManager software.

If a simple reset is not enough to exit Emergency Upgrade mode, it will be necessary to update the firmware from Wavemanager. Products in Emergency upgrade mode are clearly identifiable in WaveManager. Select the unit in the list, then click Setup and upgrade the unit as indicated chapter [IX.1](#) above.



While the product is in **Emergency upgrade** mode it still allows to restore factory settings by pressing the reset button more than two seconds.

You can voluntarily enter Emergency Upgrade mode: press and hold the reset button during product start-up, until the **Diag** led starts to blink

X TROUBLESHOOTING

This section gives indications on the checks to perform when things do not work as expected after configuration.

A network sniffer may prove very helpful when debugging network connections. We recommend WireShark, a free sniffer working on Windows and Linux.

X.1 Basic checks

Check power supply LED(s)

If the power supply LED is OFF, check that the power supply is correctly plugged at both ends; check that the delivered current and voltage is in the acceptable range. Products with dual power supply can work with only one source provided.

Check Diag LED

The Diag LED should go OFF (or green, on some models) 30 to 45 seconds after power up (depending on product model and configuration complexity). If it remains permanently fixed, the product is out of order. If it is blinking quickly, the device is in Emergency upgrade mode.

Check State LEDs

The State LED is OFF when the corresponding radio is disabled; it is blinking when the product tries to associate (or waits for association); it is steadily ON when associated.

If the product is set for infrastructure station mode, it will try to connect to an access point with corresponding configuration (channel, protocol, keys and SSID). During the search the Wlan status LED is blinking (red) and WLAN (blue) LED is off.

- Insure that the access point is in range
- Insure that the access point Wi-Fi and security parameters match the product Wi-Fi and security parameters.

Check WLAN LEDs

- The WLAN LED blinks whenever frames are sent or received. Even when no data transfers take place, management frames may make this LED blink.

X.2 Network configuration checks

Check IP address

Check IP addresses: the following assumes that all network devices are in the same LAN (the computer used for the tests, the product, the remote device):

- All network devices must be in the same IP subnet (**see RFC 950**). For example 192.168.1.253 and 192.168.1.10 are in the same subnet, but 192.168.1.253 and 128.1.1.10 are not (assuming a netmask of 255.255.255.0)
- All network devices must have the same netmask
- When changing the IP address of one device, the others keep the old address for several minutes in the ARP cache: clear it with "arp -d" (Windows O.S.) or by powering off the caching devices
- Windows (or other) firewalls may prevent communication.
- The web interface (in the Tools/Network menu) provides a "ping" feature which executes the ping command in background and then display the result on the web page. A traceroute tool is also available on the same page.

Check security parameters

Check security parameters: when installing, always disable all security parameters until everything else works correctly. Add security parameters at the end, when you are sure about the whole configuration parameters.

Check Wi-Fi parameters

Check Wi-Fi parameters: all the communicating devices must have matching Wi-Fi parameters. Check the SSID, the channel, the 802.11 mode (a, g, na, ng), the topology (infrastructure, mesh, repeater or ad-hoc). If in doubt, set the same given fixed channel on all communicating devices, and do not use the 4-addresses bridging mode, for this format is not compatible with some AP providers.

X.3 Multicast router checks

The following Reference configuration is used in this section:



Sender sends multicast traffic.

SDRRP is a multicast router, designated (sole) router on the right-side Ethernet and rendezvous point for the multicast group (Sender side Designated Router and Rendezvous Point).

RDR is a multicast router, designated (sole) router on the left-side Ethernet (Receive side Designated Router).

Receiver runs software that reads multicast traffic sent by **sender**.

Check unicast configuration

- From **Receiver**, can you ping each of **RDR**, **SDRRP**, **Sender**?
- From **Sender**, can you ping each of **SDRRP**, **RDR**, **Receiver**?
- From **RDR**, can you ping each of **Receiver**, **SDRRP**, **Sender**?
- From **SDRRP**, can you ping each of **Receiver**, **RDR**, **Sender**?

Run software

Run the sender and the receiver software now.

Check multicast configuration in SDRRP

- Are the “Enable multicast”, “Enable bootstrap” and “Rendezvous point candidate” checkboxes all checked?
- Does “local rendezvous point configuration” contain the proper group prefix?
- Are the two network interfaces reaching Ethernet and Wi-Fi enabled to handle multicast? Leave defaults for other parameters for now.

Now, if the multicast log level is set to Debug in **SDRRP**, you can see the following message every 10 seconds:

```
daemon.debug pimd[nnn]: move_kernel_cache: SG
```

Also, the “Status/network/multicast routes” may show, briefly from time to time, the **Sender** address in the multicast routes section. This indicates that join requests from **Receiver** do not reach **SDRRP** yet.

If the **Sender** address is steady and “in use” in the multicast routes section, see below the **Sender** checks.

- Look at the “Status/network/multicast routes” on **SDRRP**.
 - In the “network interfaces” section, does it show the IP address of **RDR** in the column “Neighbor MC routers” on the expected line?
Else either **RDR** is not enabled for the Wi-Fi link, or the link is not established or flickers.
 - In the “Rendezvous points” section, do you see your group? Is it associated with the address of **SDRRP**? Is the BSR address one of **RDR** or **SDRRP**?

Check multicast configuration in RDR

- Look at the “Status/network/multicast routes” on **RDR**.
 - In the “network interfaces” section, is the “DR” checkbox marked for the receiver side Ethernet network interface? Else there is another PIM router on this network.
 - In the “network interfaces” section, does it show the IP address of **SDRRP** in the column “Neighbor MC routers” on the expected line?
 - In the “network interfaces” section, does it show the multicast group in the column “IGMP reports” on the expected line? Else there is a problem with **Receiver**. Maybe it uses a unicast address instead of multicast, or a multicast in the range 224.0.0.x/24, or it uses IGMPv3 and you configured IGMPv2.
 - In the “multicast routes” section, does it show a route for the group? Is the “RP address” the one of **SDRRP**? Is the ingress interface the one where **Receiver** is attached?
 - In the “Rendezvous points” section, do you see your group? Is it associated with the address of **SDRRP**? Is the BSR address one of **RDR** or **SDRRP**? Else there is no BSR, and the rendezvous points and incorrectly configured.

Check IP options in Sender

These checks depend on the software you use, we can only give broad indications.

- Double check the TTL used by **Sender**. If possible, dump the Ethernet traffic with “tcpdump” (Linux) or “Wireshark” (Windows and Linux).
Display the TTL of outgoing frames.



- Double check the size of the frames. If possible, reduce it for a first try. 1000 bytes should pass quite anywhere. You can use “iperf” or “jperf” to generate multicast traffic with a known frame size.

Check UDP options in Sender and Receiver

- Do they use the same UDP port? The same data format?

XI FREQUENTLY ASKED QUESTIONS

This section answers questions to various aspects of the operation of the products.

- 1 Push the reset button steadily for at least 3 seconds, until the “Diag” LED turns back red; this resets the product to factory settings. Wait until “Diag” LED turn on.

XI.1 How to reset the device to factory settings?

You can reset to factory settings via the WEB interface (VII.2.5 Save Config / Reset), but in some cases, you will need to use the reset button for this purpose. Please refer to the product documentation to find the location of the reset button. Here is the procedure to restore the factory settings:

Push and hold the reset button steadily until the DIAG LED turns off, then release the button; Wait until the DIAG LED turns back on, then check with WaveManager that the IP address of the device has been reset to the factory default 192.168.1.253.

XI.2 I Can't find the Transparent Client mode

The old **Transparent Client** role is now a subset of the generic **Client (infrastructure)** role, and must be configured in the **Advanced settings** tab of the **Interface configuration** section (Bridging mode **4-addresses format (WDS)**).

XI.3 How is the Wi-Fi bit rate chosen?

The bit rate used to send a frame depends on several considerations and may have a large effect on both the throughput between two devices, and the bandwidth left for other devices.

Some frames are always sent at the lowest available bit rate: broadcasts and multicasts aim all stations hence they must reach the farthest possible distance; management frames are important and reception must be ensured as much as possible.

The lowest configured bit rate is supposed to always succeed. This bit rate will be used as a starting value after association. Then a dynamic adaptative algorithm named MINSTREL is used, quickly converging to the optimum rate while periodically checking for better throughput at other rates. The MINSTREL algorithm is described in:

<http://linuxwireless.org/en/developers/Documentation/mac80211/RateControl/minstrel/>

XI.4 What is the difference between WMM, WME, IEEE802.11e?

These are various names for the QoS function. IEEE802.11e is an extension of WME QoS, it adds APSD (automatic power save delivery) and HCCA, a rarely used protocol (QoS Wi-Fi usually uses EDCA). The products support WME, which consists of the mandatory features of IEEE802.11e. WMM is another name for WME.

The WME capability consists in having 4 priority classes (best-effort, background, video, voice). Each transmitted frame belongs to one class and the parameters for contention/collision resolution in the air media can be fine-tuned depending on the class.

XI.5 My CISCO access point rejects my client bridge?

We assume that SSID, channel and security are correctly set up. To allow bridging a LAN to a CISCO AP, the “passive mode” must be used on the CISCO AP, so that the proxy ARP server is disabled. See section [V.2.6.2a Masquerading \(ARPNAT\)](#).

XI.6 Fast roaming features

Figures given below are accurate for the firmware version 2.2.0 and will be updated as needed in future releases of this document.

XI.6.1 What is the scan period when proactive roaming is enabled?

When the client is connected, proactive roaming cycles through the activated channels. Each channel is scanned for a duration of around 56ms, during which the radio is deemed “off-channel” and no data can flow; then a 200ms pause is inserted between each channel scan to allow data transfers, and an extra delay can be configured between cycles in order to improve throughput by lowering CPU usage and off-channel time.

The 200 ms pause does not take place when the channel to scan is the one currently in use.

For example, for a 4-channels scan with a configured delay of 3000 ms, the scan period will be $56\text{ms} + 0\text{ms} + 56\text{ms} + 200\text{ms} + 56\text{ms} + 200\text{ms} + 56\text{ms} + 3000\text{ms} = 3464\text{ms}$. The radio cannot communicate while it is off-channel, in this case this is $(3 \times 56) / 3464 = 4,8\%$ of the time. The throughput decreases accordingly.

This figure is only an approximation and may vary under very heavy loads.

XI.6.2 What is the roaming delay when the current access point disappears suddenly?

This can occur when a big obstacle suddenly gets in the way of the radio waves: for example, turning around the corner of a tunnel. This can also happen if the AP is powered off or fails for whatever reason. The client product has several ways to find out:

- If the client is sending data to the AP and the AP no longer acknowledges it, the client will drop the association after 50 unacknowledged frames. Each frame is retried using the relevant retry procedures and appropriate (configurable) supported rates.
- If the client does not send data, it will rely on the beacons received from the AP. The client will detect when several consecutive beacons are missing; after which it will send two extra control frames (each retried 10 times) to further probe the AP. If the AP still does not respond, the client will drop the association. The number of missing beacons is configurable.

The total duration of this procedure depends on the configured number, the beacon interval duration set in the AP configuration, and the lowest configured basic rate (for the probe involving the control frames)

XI.7 The GRE tunnel does not forward data?

Provided that the GRE endpoints IP addresses are correct at both end of the tunnel, and each side can ping each other, this can happen in a corner case when

- The GRE tunnel local endpoint uses a wireless Access Point interface,
- The AP is configured in such a way that it cannot initialize quickly because of ACS or DFS delays,

In this case, at startup, the GRE tunnel searches for an outgoing route to the remote endpoint but cannot find it because it does not exist yet. It reverts to some default route potentially pointing in the wrong direction.

The solution is to either change the AP settings, or to include the AP network interface into a bridge. A software bridge has no startup delay and the GRE tunnel will always find it.

XI.8 Multicast

XI.8.1 Multicast route is unstable in the Web interface?

After configuring a multicast group and starting the corresponding multicast sender, you may experiment that the route comes and goes in the Web interface, page Status/Network/Multicast routes list.

One frequent cause is that the router receives the multicast flow but ignores it because no outgoing interface is configured.

Check the relevant interfaces in the “local networks configuration” section of the Setup/Routing/Multicast routing page.

Check that the IGMP reports from the receiver include the expected multicast group (see next FAQ below).

XI.8.2 Receiver device does not send its multicast group in its IGMP reports?

In Linux devices, IGMP messages are sent only on the interface defined by the routing table, which must include an appropriate routing entry such as

\$ route -n						
Destination	Gateway	Genmask	Flags	Metric	Ref	Use Iface
(...)						
224.0.0.0	0.0.0.0	240.0.0.0	U	0	0	0 eth0

XII APPENDIX – GLOSSARY AND ACRONYMS

802.11	An IEEE standard describing several variations of network layers 1 and 2 of a radio LAN.
802.11s	The part of the IEEE 802.11 standard that describes wireless mesh networks.
AP	Access point.
A-MPDU	Aggregated MAC protocol data unit. Several MAC frames concatenated in one big frame and handed to the Physical Layer for transmission in one chunk.
BSR	The Bootstrap Router is the multicast router responsible for dynamic selection and distribution of the mapping between RP's and multicast groups.
BSS	Basic Service Set, the network formed by one AP and its clients.
Bridge	<p>In the context of wireless applications, a bridge is a network component that transfers LAN (Ethernet) frames to the WLAN (Wi-Fi) media and vice-versa. When the WLAN is in infrastructure mode, the term “bridge” is used for the client of the AP, though, technically, the AP is also a bridge.</p> <p>In the broader context of networking, a bridge transfers layer 2 frames from one physical interface to another, without resorting to level 3 routing. For example, an Ethernet switch is a hardware bridge, and the products include a software bridge between their various interfaces such as Ethernet, multiple WLAN clients or APs, mesh, and so on.</p>
BSSID	BSS identifier, usually the MAC address of the AP or a derivation thereof.
GNSS	Global Navigation Satellite System, one of GPS (US), GLONASS (russian), Galileo (European) or BeiDou (Chinese).
IPv4	Internet Protocol version 4, a network layer in the TCP/IP protocol stack which is responsible for the delivery of packets to the correct target computer. IPv4 uses 32 bits sized addresses like “192.168.1.1”.
LAN	Local Area Network, a part of a network where devices can directly use MAC (OSI layer 2) addresses to communicate with each other.
MCC	Mobile Country Code, unique country identifier for cellular networks.
MCS	Modulation and Coding Scheme, the way the bits are encoded in radio waves in 802.11n.
MNC	Mobile Network Code, operator identifier for cellular networks in the designated country
OSI	Open Systems Interconnection, an ISO standard reference model to organize networking systems into specialized layers.
PSK	Pre-shared key, a symmetric crypto system where the same key is used at both ends of the link. This implies that the key must be previously transferred by a separate way from one end to the other (and this way could be a target for an

	attack).
Repeater	A combined client+AP on the same radio, linked together in a software bridge. Data received either by the AP or by the Ethernet LAN can be forwarded through the client to a remote AP, allowing setting up a chain.
RP	The Rendezvous Point is the multicast router responsible for distribution of a given multicast group.
RTS/CTS	An optional MAC protocol, that requires sending a small RTS frame that reserves the air medium for a long enough duration to send the next data frame. The receiver replies by sending a CTS frame that makes the same reservation. Therefore, all wireless stations in radio range of both the transmitter and the receiver, are informed of the data transmission that will take place.
SSID	Service Set Identifier, a string identifying the wireless network formed by a group of APs and their clients.
SSM	Source Specific Multicast is a variant of multicast routing where the receiver knows the address of the sender, so that there is no need to go through the RP.
USM	User-based Security Model, a way to define SNMP access permissions on a per-user basis.
VLAN	Virtual LAN, a LAN tunneled in another LAN by adding a VLAN tag to each frame in the VLAN.
Wi-Fi™	“Wireless Fidelity”. In this documentation, this term is used as a synonym for 802.11.
WLAN	Wireless LAN, a group of Wi-Fi stations sharing a common network name (SSID or Mesh ID), and a common authentication method, in order to exchange information with each other.

XIII APPENDIX – 802.11 RADIO CHANNELS

XIII.1 11b/g (2.4GHz)

These networks use the ISM (Industrial Scientific and Medical) radio band on the [2.3995-2.4965] spectrum.

Channel (25 MHz)	Central frequency (GHz)	Allowed by
1	2,412	Asia MKK, Europe ETSI, US FCC
2	2,417	Asia MKK, Europe ETSI, US FCC
3	2,422	Asia MKK, Europe ETSI, US FCC
4	2,427	Asia MKK, Europe ETSI, US FCC
5	2,432	Asia MKK, Europe ETSI, US FCC
6	2,437	Asia MKK, Europe ETSI, US FCC
7	2,442	Asia MKK, Europe ETSI, US FCC
8	2,447	Asia MKK, Europe ETSI, US FCC
9	2,452	Asia MKK, Europe ETSI, US FCC
10	2,457	Asia MKK, Europe ETSI, US FCC
11	2,462	Asia MKK, Europe ETSI, US FCC
12	2,467	Asia MKK, Europe ETSI
13	2,472	Asia MKK, Europe ETSI
14	2,484	Asia MKK

Besides specifying the center frequency of each channel, 802.11 also specifies (in Clause 17) a spectral mask defining the permitted distribution of power across each channel. The mask requires that the signal be attenuated by at least 30 dB from its peak energy at ± 11 MHz from the center frequency, so that the channels are effectively 22 MHz wide. One consequence is that stations can only use every fifth channel without overlap, typically 1, 6 and 11 in the Americas, 1-13 in Europe, etc. Another is that channels 1-13 effectively require the band 2401-2483 MHz, the actual allocations being for example 2400-2483.5 in the UK, 2402-2483.5 in the US, etc.

Since the spectral mask only defines power output restrictions up to ± 22 MHz from the center frequency to be attenuated by 50 dB, it is often assumed that the energy of the channel extends no further than these limits. It is more correct to say that, given the separation between channels 1, 6, and 11, the signal on any channel should be sufficiently attenuated to minimally interfere with a transmitter on any other channel. Due to the near-far problem, a transmitter can impact a receiver on a “non-overlapping” channel, but only if it is close to the victim receiver (within a meter) or operating above allowed power levels.

XIII.2 802.11a/h (5 GHz)

These networks use the 5 GHz radio band UN-II (Unlicensed-National Information Infrastructure).

UN-II uses four separate sub-bands: UN-II-1, 2, 2e and 3.

Band	Channel (20 MHz)	Central frequency (GHz)	Allowed by
U N II 1	34	5,170	Japan TELEC
	36	5,180	Europe ETSI, US FCC
	38	5,190	Japan TELEC
	40	5,200	Europe ETSI, US FCC
	42	5,210	Japan TELEC
	44	5,220	Europe ETSI, US FCC
	46	5,230	Japan TELEC
U N II 2	48	5,240	Europe ETSI, US FCC
	52	5,260	Europe ETSI, US FCC
	56	5,280	Europe ETSI, US FCC
	60	5,300	Europe ETSI, US FCC
U N II 2e	64	5,320	Europe ETSI, US FCC
	100	5,500	Europe ETSI, US FCC
	104	5,520	Europe ETSI, US FCC
	108	5,540	Europe ETSI, US FCC
	112	5,560	Europe ETSI, US FCC
	116	5,580	Europe ETSI, US FCC
	120	5,600	Europe ETSI, US FCC
	124	5,620	Europe ETSI, US FCC
	128	5,640	Europe ETSI, US FCC
	132	5,660	Europe ETSI, US FCC
	136	5,680	Europe ETSI, US FCC
U N II 3	140	5,700	Europe ETSI, US FCC
	144	5,720	Europe ETSI, US FCC
	149	5,745	US FCC
	153	5,765	US FCC
ISM	157	5,785	US FCC
	161	5,805	US FCC
ISM	165	5,825	US FCC

Summary:

Europe (ETSI): 19 channels

- UN-II 1 : 4 channels 36, 40, 44, 48
- UN-II-2 : 4 channels 52, 56, 60, 64
- UN-II-2e : 11 channels : 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140

US and Canada (FCC): 23 channels

- UN-II 1 : 4 channels 36, 40, 44, 48
- UN-II-2 : 4 channels 52, 56, 60, 64
- UN-II-2e : 11 channels : 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
- UN-II-3 : 4 channels : 149, 153, 157, 161

Japan (TELEC): 4 channels

- UN-II-1 : 4 channels : 34, 38, 42, 46