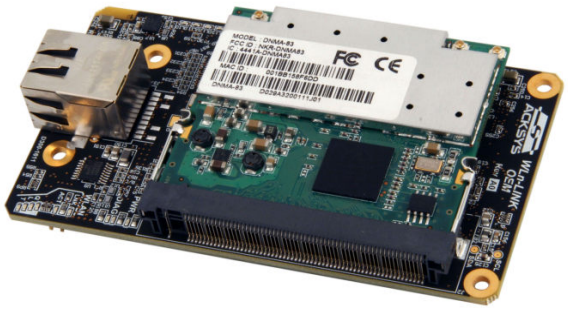


ETHERNET TO Wi-Fi GATEWAYS USER'S GUIDE

FOR 802.11A/B/G/H/N DEVICES

ACKSYS COMMUNICATIONS & SYSTEMS

Wi-Fi GATEWAY USER GUIDE

COPYRIGHT (©) ACKSYS 2014

REGISTERED TRADEMARKS ®

- ACKSYS is a registered trademark of ACKSYS.
- 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

DISCLAIMERS

ACKSYS ® gives no guarantee as to the content of the present document and takes no responsibility for the profitability or the suitability of the equipment for the requirements of the user.

ACKSYS ® will in no case be held responsible for any errors that may be contained in this document, nor for any damage, no matter how substantial, occasioned by the provision, operation or use of the equipment.

ACKSYS ® reserves the right to revise this document periodically or change its contents without notice.

REGULATORY INFORMATION AND DISCLAIMERS

Installation and use of this Wireless LAN device must be in strict accordance with local regulation laws and with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antennas) to this device 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.

ACKSYS COMMUNICATIONS & SYSTEMS
10, rue des Entrepreneurs
Z.A. Val Joyeux
78450 VILLEPREUX - France

Phone:	**+33 (0)1 30 56 46 46**
Fax:	**+33 (0)1 30 56 12 95**
Web site:	**www.acksys.fr**
Hotline:	**support@acksys.fr**
Sales:	**sales@acksys.fr**

TABLE OF CONTENTS

I INTRODUCTION

This reference guide applies to the following access points and bridges:

WLn-LINK-OEM-TTL
WLn-LINK-OEM-RJ
WLn-ABOARD family: /N, /24, /48, /72, /110, and /H4 option
WLn-xROAD
WLn_RAILBOX

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 version **2.4.3** of the product firmware.

- If your product contains an earlier version, you can download a firmware update from our Internet web site.
- If your product contains a more recent version, you can check our web site to download a documentation update.

The firmware change log (which you can download from the ACKSYS web site) explains which features are available depending on the firmware version.

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 ACKSYS.

ACKSYS provides this document "as is", without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose.

ACKSYS 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, ACKSYS 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

This line of products provides Wi-Fi connectivity for Ethernet devices. Thanks to its configuration possibilities, the ACKSYS products line is able to create different topologies see section "Wireless topologies examples" for more details.

II.2 Products common features

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

General services:

- Multi-interface bridging
- Router with DSCP retagging, NAT, firewall
- Optional DHCP server or client
- Events handler, alarms

Configuration and maintenance:

- HTTP and HTTPS Web browser configuration
- Acksys NDM compatibility
- SNMP agent for status and configuration
- Browser-based firmware upgrades
- Emergency upgrade mode

Wi-Fi capabilities:

- Modes: Access point, bridging client, repeater, 802.11s mesh, ad-hoc
- WME/WMM support
- Access point: optional client isolation, 802.11x authenticator, slow bit rates lockout, clients MAC filtering
- Client modes: "4 addresses" or MAC translation, 802.11r support
- Dual band (2.4 GHz and 5 GHz)
- Support 802.11n, 20 or 40 MHz channel width, MCS 0 to 15
- Backward compatible with 802.11a, b, g
- Security (depending on the mode): WPA2, 802.1x (RADIUS)
- A/B/G compatible security: WPA, WEP
- Fast roaming configurations
- Long-distance Wi-Fi

Ethernet capabilities:

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

II.3 Products range

Some features are available only on dual radio products. The following table shows in which range each product belongs.

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

Feature	WLn-ABOARD	WLn-LINK-OEM	WLn-xROAD	WLn-RAILBOX
Wi-Fi radios	2	1	1	1/2
802.11 spatial streams	2	2	3	3
Cellular radio				1, optional
Gigabit Ethernet	2	1	1	2
Serial port([1])	✓(RS422 /RS485)	✓ (TTL)		
C-Key	✓	✓ (TTL)		✓
Alarm([2])	✓			✓
Dual power supply	✓			option
PoE+				option
High power radio option	✓	✓		
Rugged enclosure	✓		✓	✓

([1]) Reserved for customized versions – not supported in the standard firmware
([2]) Not supported in all firmware versions

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.

The WLn series includes 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 behavior.

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.

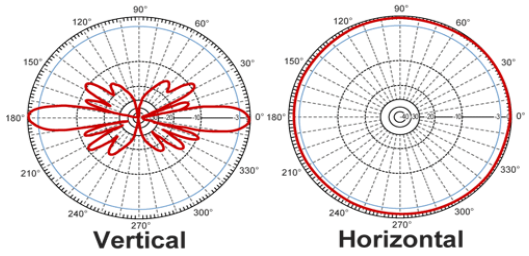
The radiation patterns shown in the next sections are given for example only and just provide a better understanding of each antenna type distinctiveness.

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.

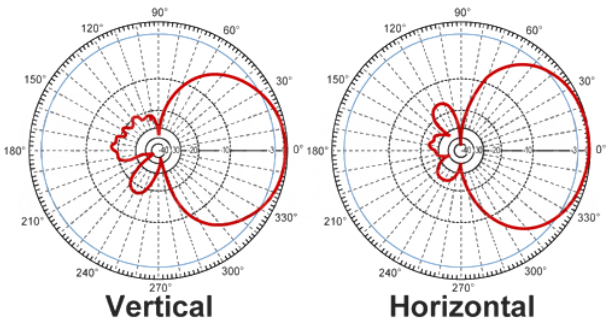
This type of antenna is used to cover a wide area all around the antenna.

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

Antenna	Radiation pattern
	

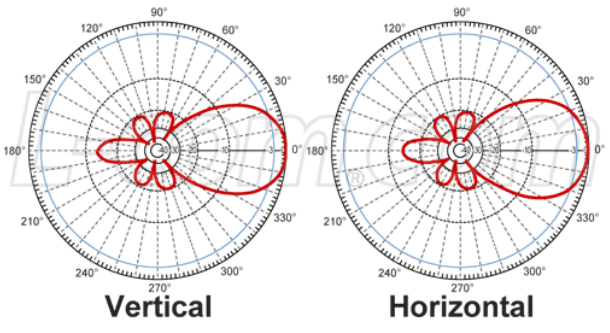
III.2.2 Patch antenna

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
	

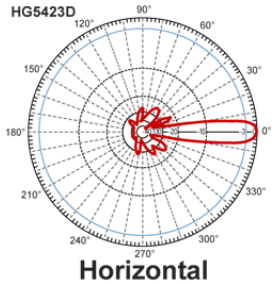
III.2.3 Yagi antenna

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 antenna are basically a set of several (usually 2 or 3) standard antenna 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

They are two major cases when considering antenna installation.

III.3.1 Non 802.11n 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:

- Use an antenna with a larger gain
- And / or
- Use a product with a larger radio output power.

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 table below explains what we mean by “line of sight”.

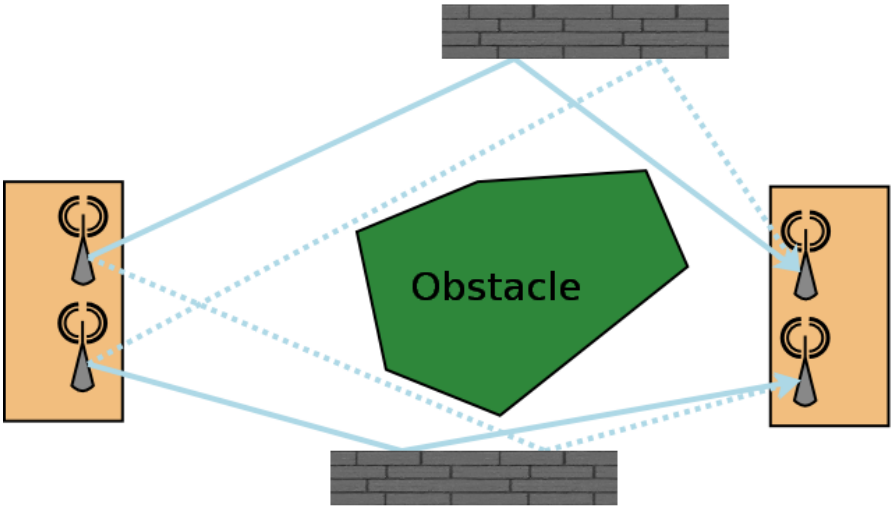
Product in line of sight (We can see the top of the mast where it is installed)

Product not in line of sight (the other product is nowhere to be seen clearly)

III.3.2 802.11n

With this norm, considerations about EIRP and RSSI are still relevant. But, the 802.11n 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 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 uses bounces to increase bandwidth, a line of sight outdoor application will have poor performances 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 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

Products performance is affected by the radio link quality (a.k.a. RSSI). The better the RSSI is, the better the throughput and error rate can be.

A preliminary site survey is strongly recommended to detect overloaded radio channels BEFORE buying band specific antenna.

An overloaded channel may strongly affects performances. It is recommended to use a free channel.

III.5 Regulatory domain rules

All around the world there are 2 major regulatory rules sets in wide use:

- ETSI: for European countries.
- FCC: for American countries

The other 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.6 Antenna gain and RF output power

If you plan to use a high gain antenna, it is possible you exceed the EIRP allowed in your country. In this case you must reduce manually the radio transmit power of your product (please see Advanced Settings tab in section VI.1.1.1a).

In the following section we give the FCC rules to adapt the product Tx power to the antenna used.

III.6.1 FCC rules for 2.4 GHz band

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)

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, if you make use of 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

If you make use of 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.6.2 FCC rules for 5 GHz band

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)

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	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.

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 the Acksys NDM software.

You can use any recent browser. Javascript must be enabled.

IV.2 Reset pushbutton

The RESET pushbutton 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 (> 2 seconds)while the product is running will reset it to factory settings.
- 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 NDM* or to reset to factory settings (see point 2).

IV.3 Acksys NDM

Acksys NDM can detect the WLn products, display their configuration and set their IP address even when they are incorrectly configured.

Acksys NDM should be used to set a correct IP address, compatible with your local network.

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

IV.4 Emergency upgrade

“Emergency upgrade” mode is entered only via the pushbutton. It allows to recover when a product was powered down during a regular firmware upgrade, or if the product experienced such conditions that it is completely non-operational.
“Emergency upgrade” mode is described in more details in its own chapter.

IV.5 SNMP agent

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

V TECHNICAL REFERENCE

V.1 Addressing in network protocols

In a device bearing multiple LAN interfaces the IP protocol can route data packets from LAN to LAN considering its final target that may be several "hops" farther.

If the LANs are compatible from the viewpoint of addresses and data frames structure, the device can also implement a bridge, moving blindly data frames without considering the final target.

Each of these levels of data transfer uses its own addressing scheme.

IP networks can be conceptually grouped into "zones" in order to assign common administrative policies to them.

V.1.1 TCP/IP network layers

V.1.1.1 TCP/IP protocols stack

TCP/IP is the name of the protocols 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.)

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.

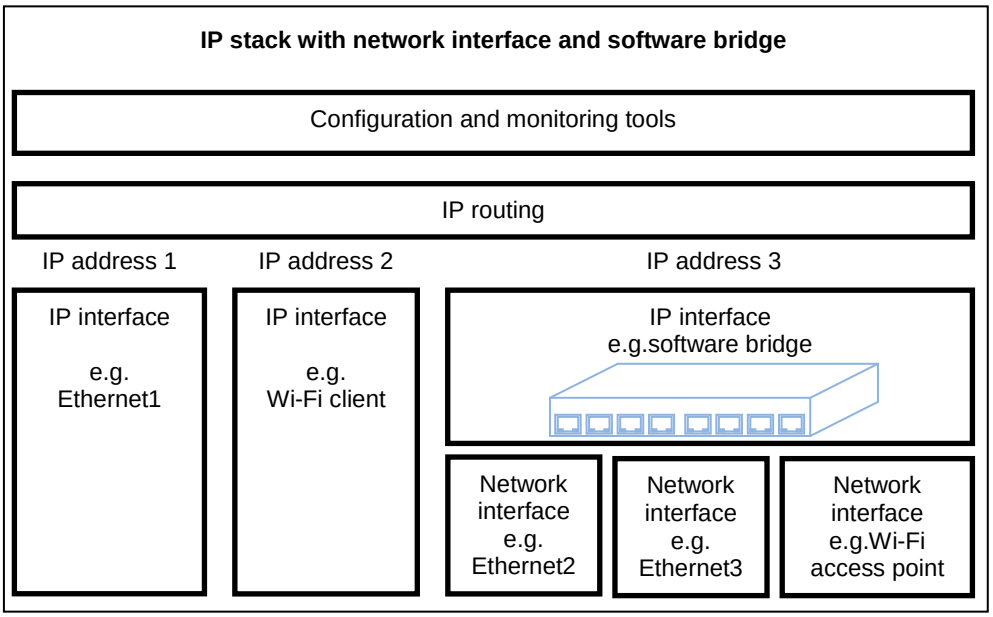
The **Network (IP) address** solves this problem by defining addresses which can be subject to routing. When the source and destination devices are not on the same LAN, the source device can send data to an intermediate router (also called gateway). The router has routing tables which allows it to forward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

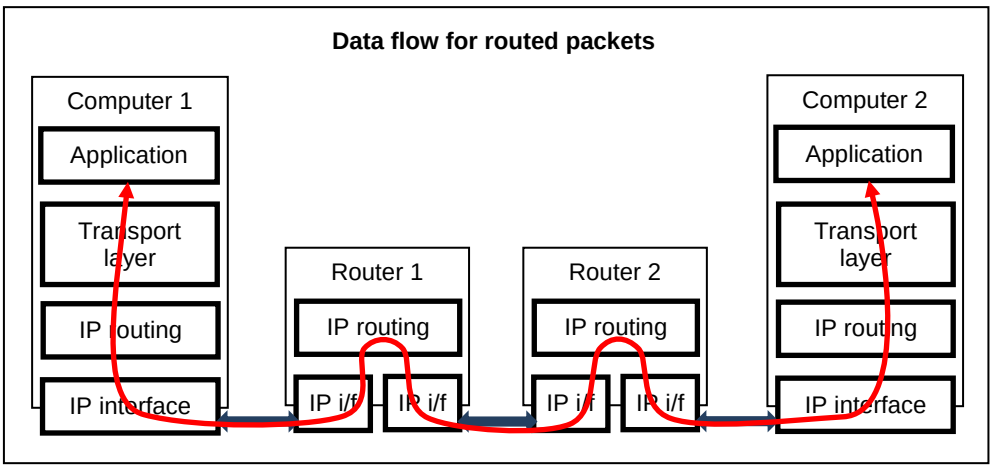
V.1.1.2 IP Networks

IP is the part of the TCP/IP stack that manages computer addresses and routing. Each network interface is seen by the IP 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. Within one computer, the IP protocol makes use of “IP network interfaces” to access the various LANs. An IP interface is thus the piece of software that drives one network hardware interface.



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 routed through 2 routers. The source and destination IP address never changes during the transit, contrary to the MAC addresses which change at each routing point.



V.1.2 LAN layer: network interfaces

In the context of TCP/IP networks, a network interface is a means of communicating with other computers. This means 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.

For the WLn products, network interfaces can be either Ethernet LANs or Wi-Fi subsystems described as “roles”: either access point, client, mesh point, and so on.

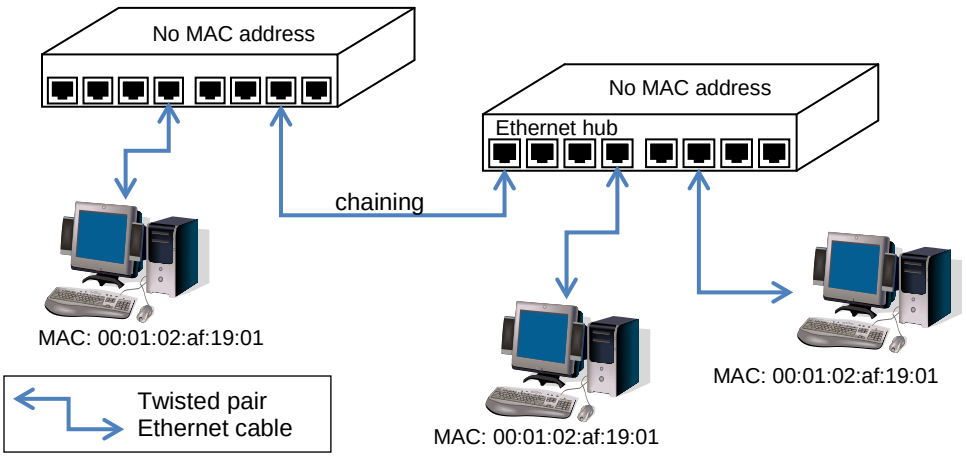
You can group compatible network interfaces inside bridges. Access points are commonly bridged with a Ethernet LAN to provide Ethernet access to its Wi-Fi clients. The IP protocol views the bridge as a single interface with a single IP address, just like if the bridge was an external hardware switch.

V.1.2.1 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).

Ethernet LAN example



V.1.2.2 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 wlans).

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.1.3 IP layer: IP addresses and routing

V.1.3.1 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	0	1	1	1	0	0	1	0	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	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.

I.1.1.1 Public and private addresses

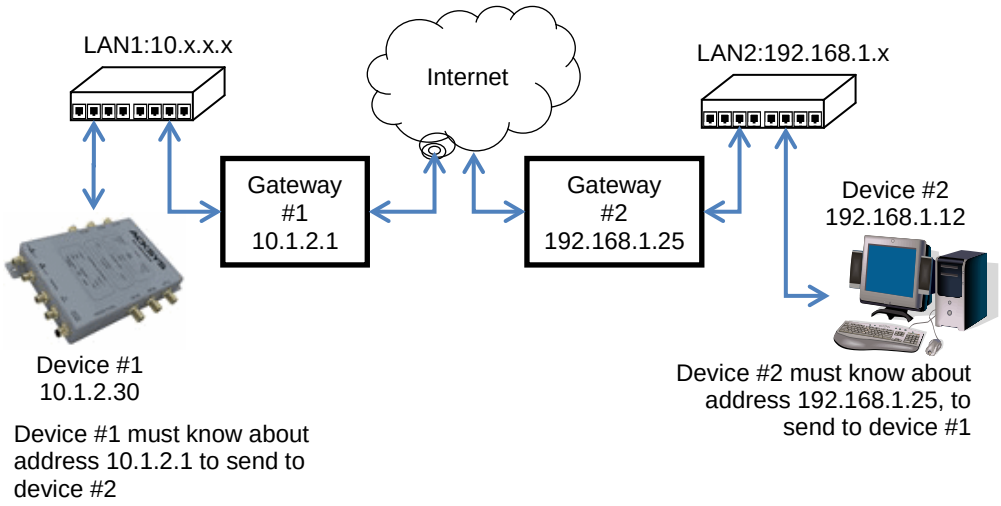
IP addresses can be private or public. Public ones are reserved to devices that require sending data over a public network, such as internet. They are usually purchased or leased from a local ISP.

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:

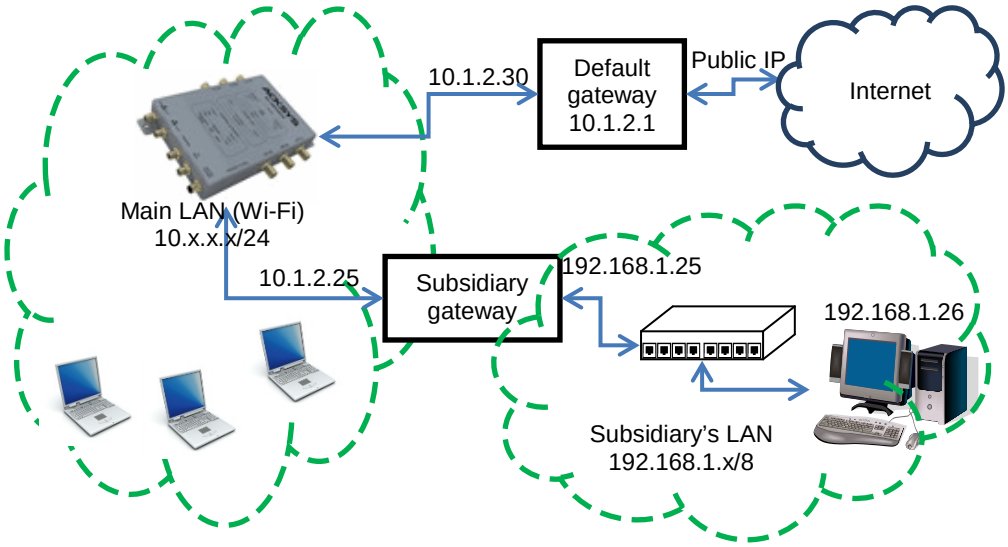
- Internally, organizations use only private addresses from a known set: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- Routers between private area and the Internet convert internal, private addresses to their own Internet public address, hence making the whole world believe that there is only one computer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

V.1.3.2 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.



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.

V.1.3.3 Zones

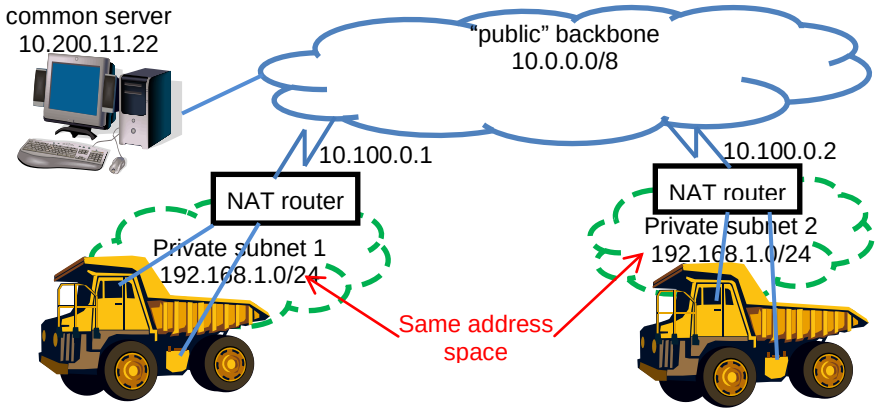
In a router, you may need to selectively block or allow traffic between network interfaces. A zone is an administrative concept which groups several IP interfaces in order to specify common extra processing:

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

V.1.3.4 NAT (network 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”.



A NAT router thus splits the network 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 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 router uses port numbers as extensions to the IP addresses. Hence, the NAT mainly works with UDP and TCP; it cannot handle generic ICMP routing, but only towards one private device at most.

The NAT 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 router is lower than the performance of a regular router, which is lower than the performance of a simple software bridge.

V.2 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.

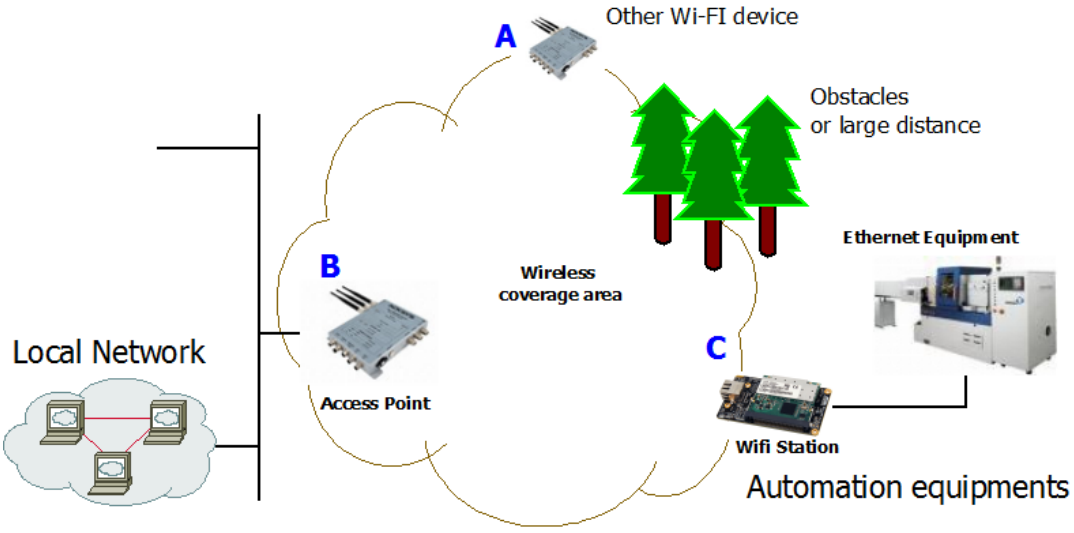
The stations in the group have in common a wireless network name which identifies the WLAN. The IEEE802.11 norm defines three architectures to communicate between Wi-Fi stations:

Infrastructure (roughly 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 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**.

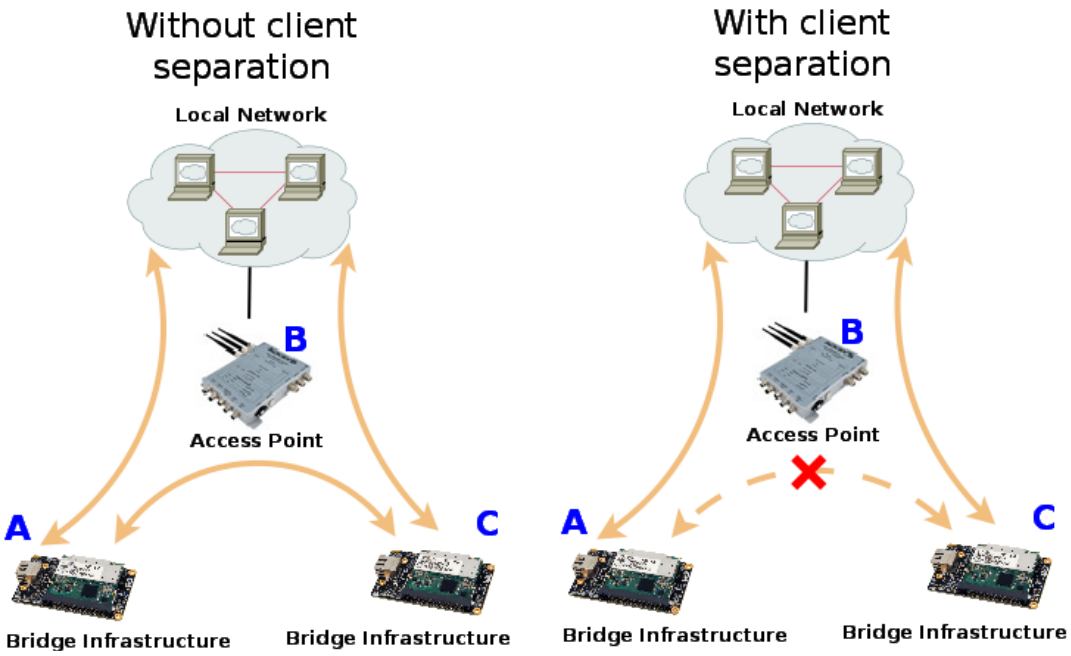
The infrastructure mode provides central connection points for WLAN clients and the AP may also bridge them to a wired network. Prior to any communication, the client must join the WLAN (wireless LAN) by selecting one access point, authenticating and possibly establishing encryption keys.

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 firmware revision, the WLn products implement 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 WLn 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.6: “Wired to wireless bridging in infrastructure mode”).

V.2.2 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).

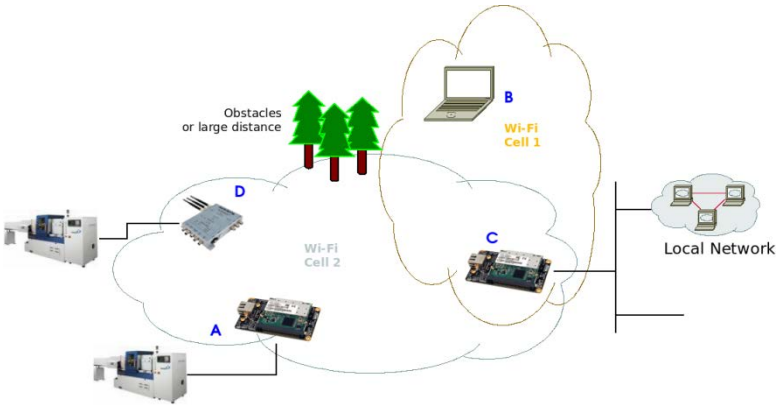
In addition, all wireless adapters on the ad-hoc network must use the same SSID and the same channel number.

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 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.

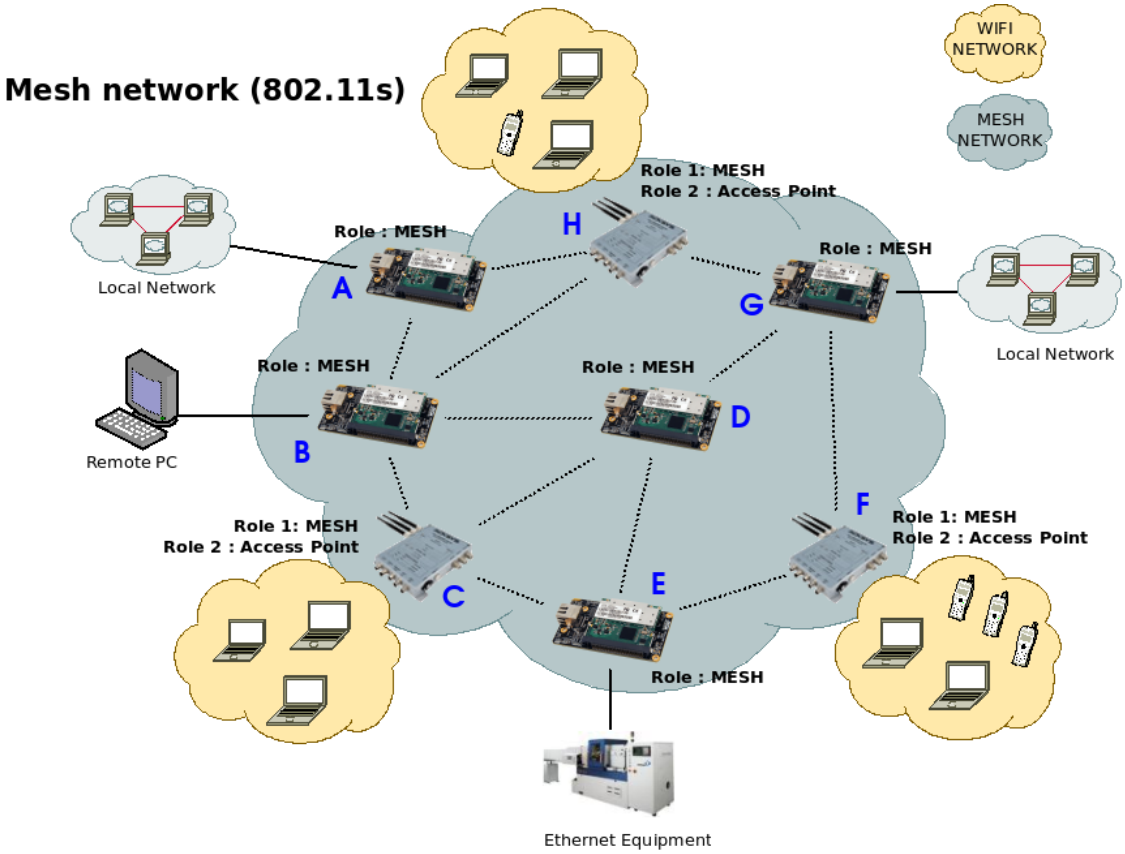
Product **C** cannot relay from **A, D** to **B**.

V.2.3 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.

All ACKSYS “WLn” 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. ACKSYS devices implement HWMP.

Security protocols

802.11s networks can use either no security, or the SAE security described in section “Preauthentication”. This security is roughly similar to infrastructure WPA/PSK.

V.2.4 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.2.5 Virtual AP (multi-SSID) and multifunction cards

The WLn 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.

Until firmware v2.2.x the multifunction limits are 4 virtual AP, one client, one mesh point and one ad-hoc station simultaneously per card. Starting with firmware v2.4.0 the limits are indicated on the web interface, page “Setup / Physical interfaces Overview”.

V.3 802.11 modes

There are 4 kinds of wireless transmission formats available: 802.11b, 802.11g, 802.11a and 802.11n.

V.3.1 802.11b

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.3.2 802.11g

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.3.3 802.11a

The 802.11na 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.3.4 802.11n

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). WLn products handle 1 to 3 streams depending on the model. Here are the physical bit rates achievable with one and two streams:

Maximum bit rate (Mbps)

	1 stream	
Channel width	20 MHz	40 MHz
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	
Channel width	20 MHz	40 MHz
MCS 8	14.4	30
MCS 9	28.9	60
MCS 10	43.3	90
MCS 11	57.8	120
MCS 12	86.7	180
MCS 13	115.6	240
MCS 14	130.0	270
MCS 15	144.4	300

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.4 802.11 channels & international compatibility

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. See appendix for further details about radio channels.

Depending on the location of the product (indoor/outside), not all wireless channels are available. Refer to local regulation (which is constantly liable to change).

Region/country

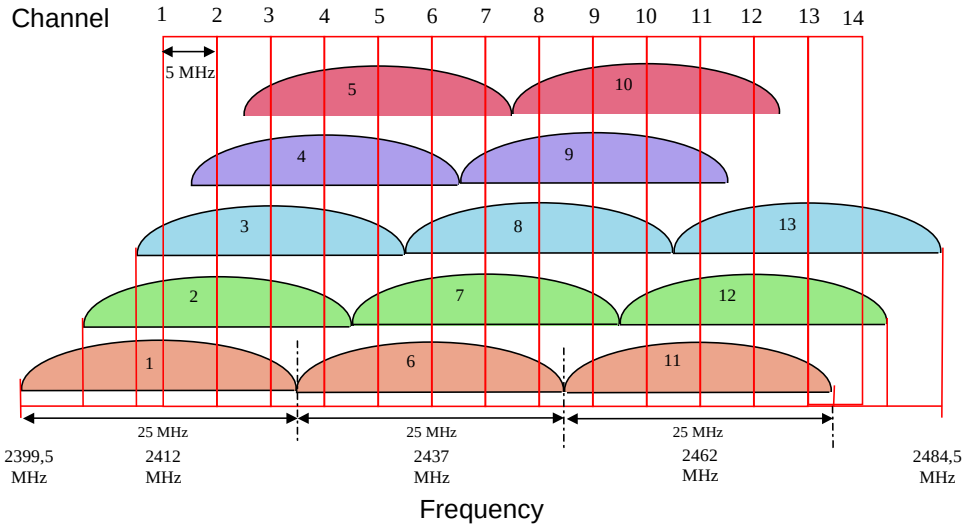
Channels availability varies by countries, constrained in part by how each country allocates radio spectrum to various services.

Broadly speaking, the world is divided into the 3 main regions:

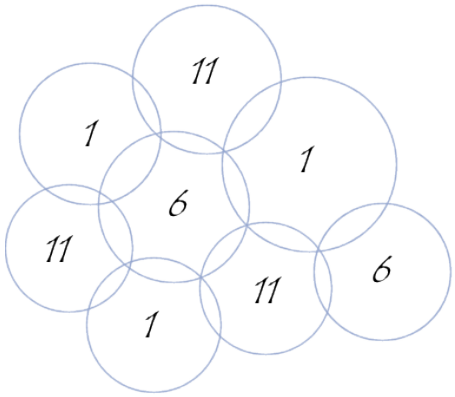
- Europe, regulated by the ETSI (European Telecommunications Standards Institute)
- US, regulated by the FCC (Federal Communications Commission)
- Asia, regulated by the MKK/TELEC

2.4GHz Overlapping radio channels

The radio channel is only an indication of the central frequency in use. Modulation enlarges the channel to a 25 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.



Example of geographical implantation of non-overlapping channels

V.5 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.5.1 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.** 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.

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:

I) The client station sends an authentication request to the Access Point.
II) The Access Point sends back a clear-text challenge.
III) The client has to encrypt the challenge text using the configured WEP key and send it back in another authentication request.
IV) 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.5.2 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	AES	RC4-CCMP
WPA2	AES (default)	AES-CCMP

V.5.3 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.

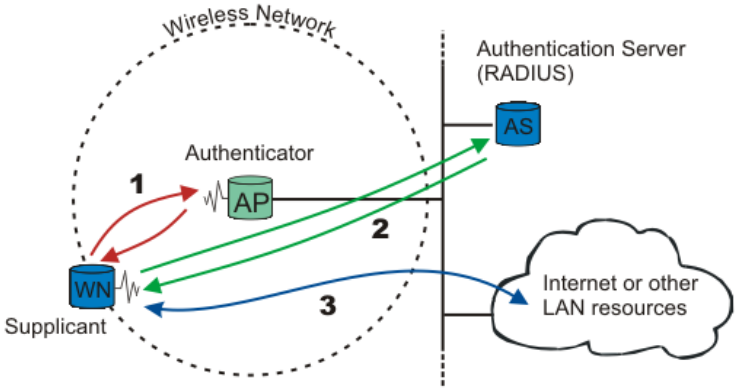
V.5.4 Enterprise mode (802.1x, RADIUS)

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. WLn clients always use preauthentication when the AP offers it.

Pre-authentication makes the client store communication keys before it needs it. The WLn 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 WLn clients, the keys are kept in a cache table whose lifetime is configurable.

V.5.5 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.5.6 Mesh Secure Authentication of Equals (SAE)

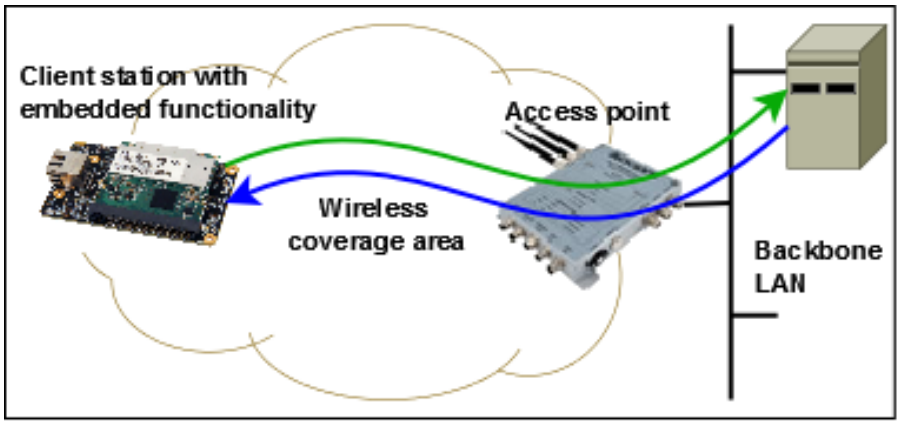
In 802.11s mesh mode, no mesh node has a special identification role, all nodes are considered equal in privileges. When SAE is used, all nodes must have a preset common key. Each time a node comes in reach of another node in the same mesh, it will verify that the peer node knows the key. The encryption 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.6 Wired to wireless bridging in infrastructure mode

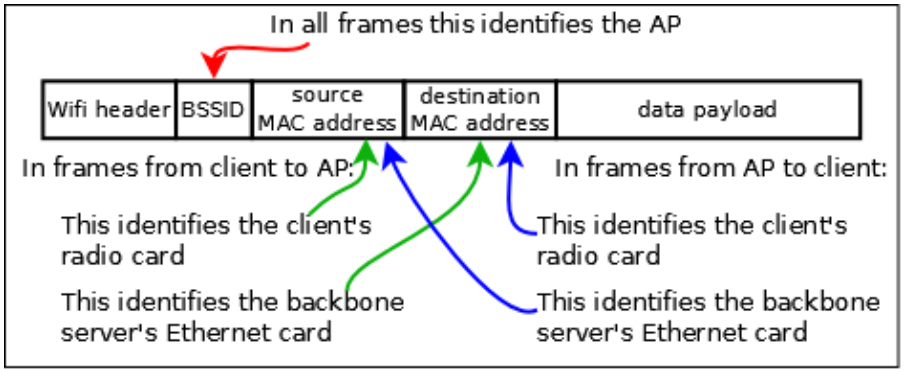
V.6.1 The problem

As outlined in section V.2.1, 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.



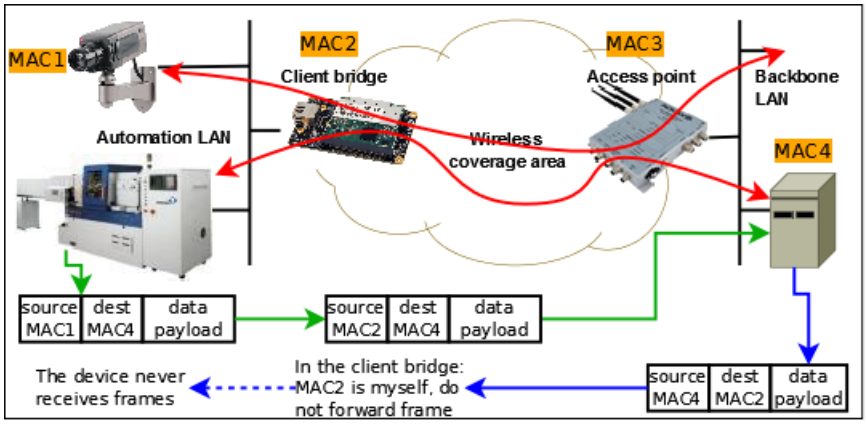
Bridging several devices with a single wireless client

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.6.2 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 WLn products “**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 though (Supported since firmware version 2.4.0).
- 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 WLn products, as several Linux-based clients and APs, support this mode described in section V.6.2.2 below.

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

V.6.2.1 Masquerading (ARPNAT)

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, an 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**. 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.

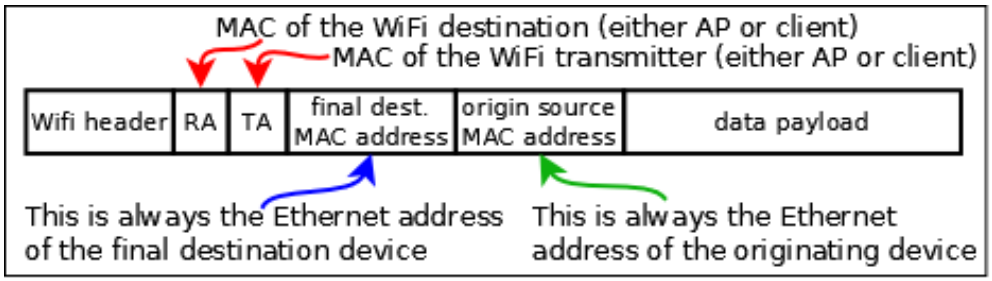
5) ARP is a protocol used to discover MAC addresses. The ARP frames contain MAC addresses both in their headers and in their data. Special processing is done in the bridge to convert these frames.
CISCO and others can set up a “proxy ARP server” in their APs. This means that the AP itself converts IP 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.

V.6.2.2 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 has the big advantage of being independent of the layer 3 IP addresses:

1) This mode can bridge protocols other that 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, is should be used only between products of the same brand or range, or when you know that the AP and client use compatible software.

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 WLn access points (AP) always support both standard and transparent clients simultaneously. The WLn client bridges must be set up as either standard clients or transparent clients.

V.6.2.3 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 WLn 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 WLn product clones the source MAC address from the first incoming frame after a reboot. So, there should be only one device connected to the WLn LAN.

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 WLn product is turned on, to be sure the WLn 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.7 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.

V.7.1 Mono-channel vs. multichannel roaming

The WLn client 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 WLn 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 WLn 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.7.2 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 WLn 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 reassociation 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.

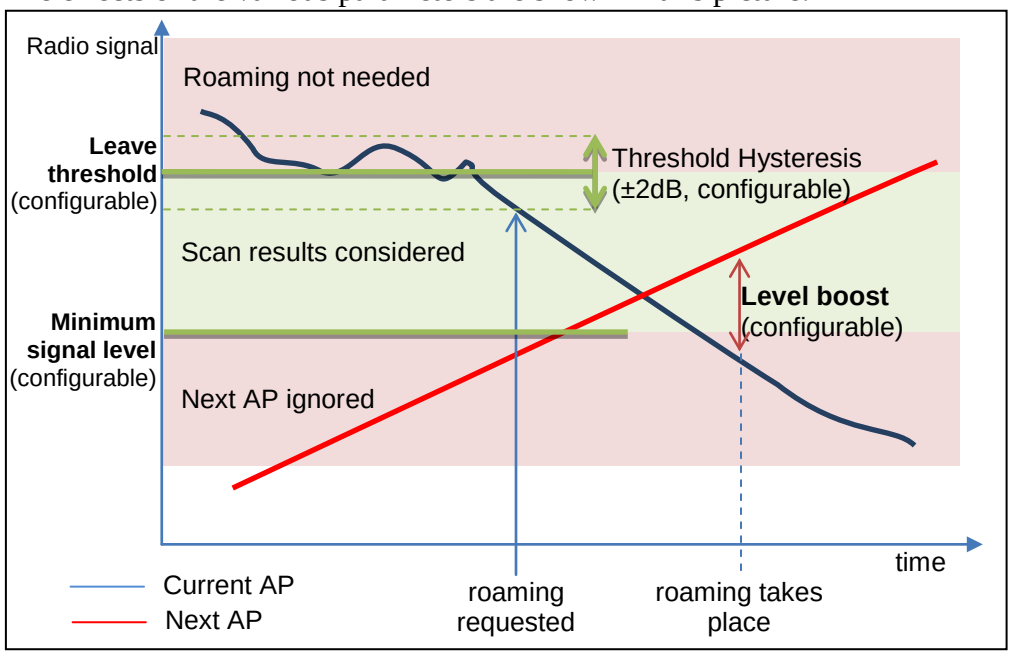
Configuration

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 reassociation periods. To account for this, crossing the limit is subject to a hysteresis (currently, 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 reassociation.

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.7.3 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 WLn client's "sight" due to moving objects in the field, climatic changes, AP powerdown 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.7.4 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.

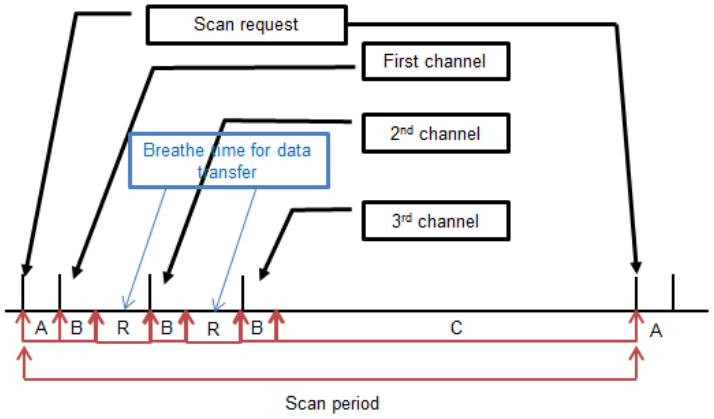
The probe request contains the SSID among other data. Any AP capable of serving this SSID will answer. The signal quality at which the response is received is used to select the best AP.

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 it adds to the scan period, as shown in the following diagram, showing the background scan.

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 breathe time “R” in the diagram is shortened to 0, resulting in a slightly faster scan cycle.

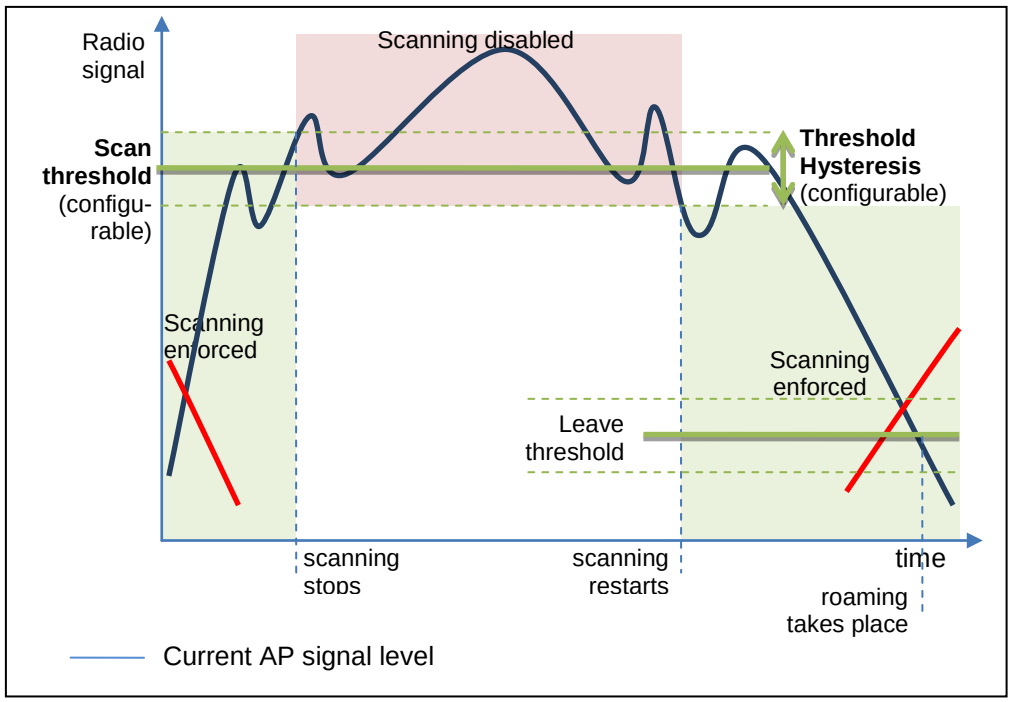


A: Initialization = a few ms
B: Channel scan = 56ms
C: Padding = configurable by steps of 250ms
R: Breathe time = 200ms
The 'R' delay is removed in reactive (foreground) scan cycles, thus shortening them while the client is not connected to an AP.
NOTE: the 'B' delay is configurable in versions 2.4.3 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 interrupted 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.

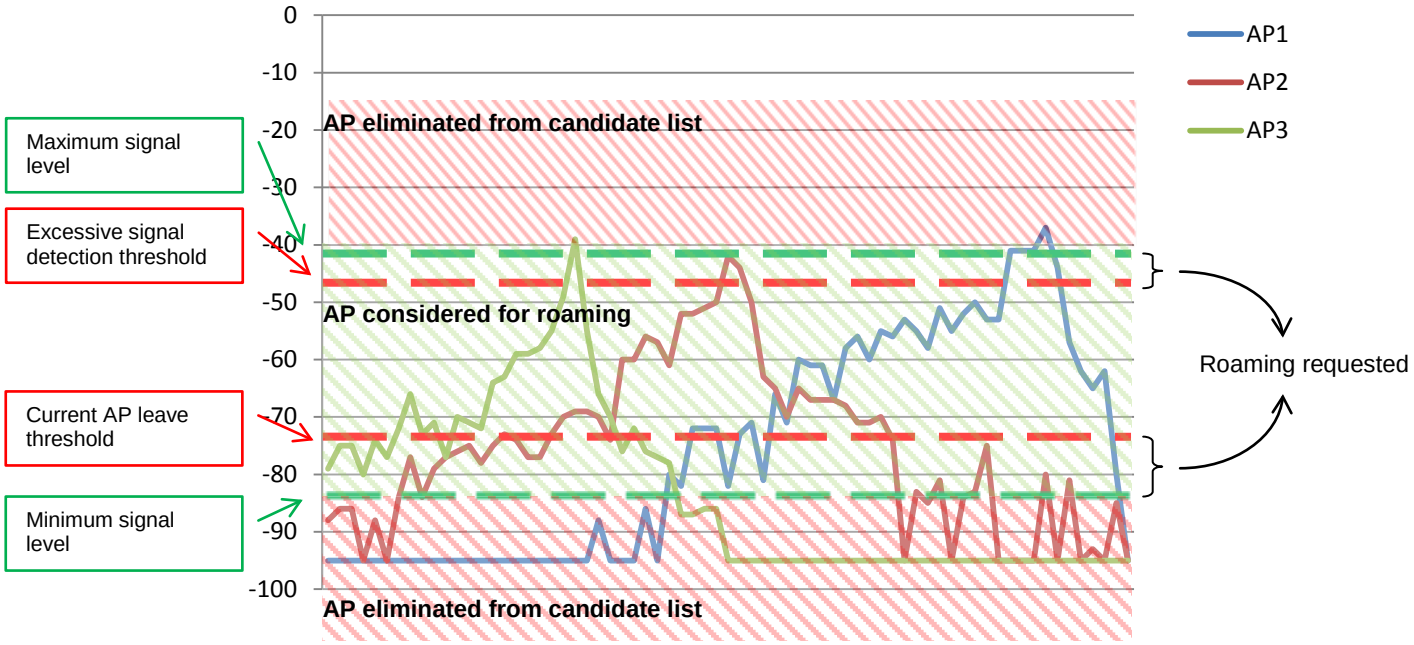
V.7.5 Advanced Roaming settings

In several situations the basic roaming settings are not sufficient.

For example, if the Wi-Fi client is embedded on a train, and a directional antenna is fixed on the roof, 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.

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.

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.

V.7.5.1 Smoothing factor

Various parameters are meant to trigger events:

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

For the purpose of threshold crossing detection, all this 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 $1/16^{th}$. 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 antepenultimate 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 $16/16^{th}$) means that only the most recent beacon is used in the comparisons.

V.7.5.2 Off-channel configuration

You can shorten the duration of the off-channel probe request/response sequences (the 'B' parameter in the "scan period" picture above). This solves the situation where a great 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 (1) a switching delay (very quick), (2) a synchronization delay (ensuring that our probe will not collide with another transmitter on the channel), (3) probe request transmission (at the lowest rate available), (4) response waiting delay.

Also, the scanner can switch from channel to channel, without returning to the current channel. This is limited to one beacon interval, though.

You can configure items (2) and (4) of the sum, and you can define the overall off-channel duration.

V.7.6 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.

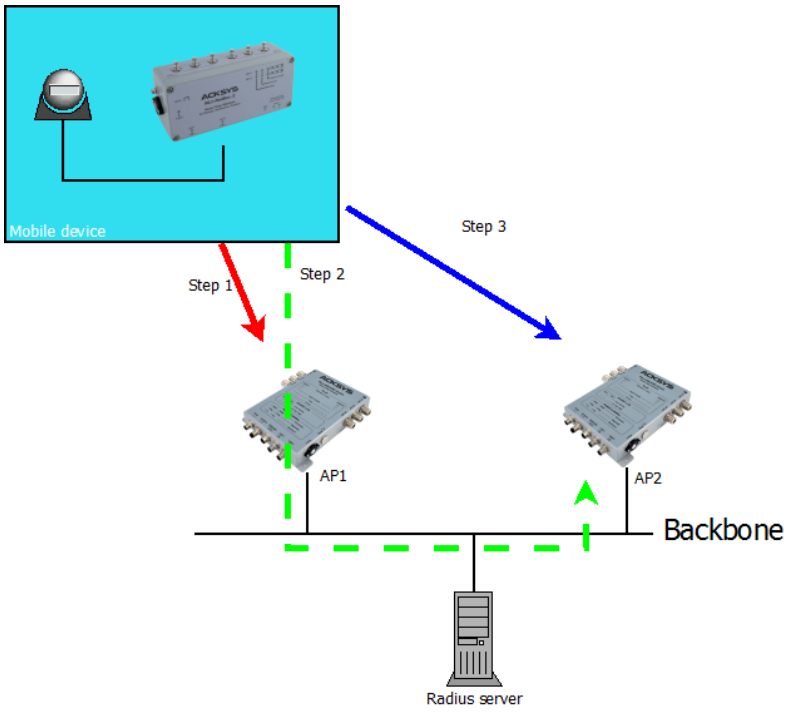
V.7.6.1 Pre-authentication / PMK caching

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

The AP signals its pre-authentication / PMK caching capabilities in its beacons. If a client supports at least of these, it can use the corresponding ones.

The Wln 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.

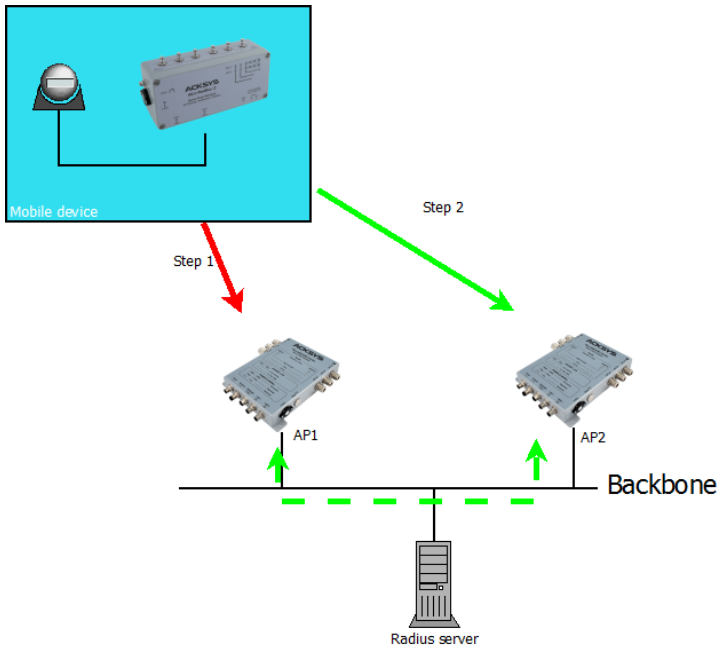
V.7.6.2 Fast Transition Support (802.11r)

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

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

The WLn products support the 802.11r only in client mode.

The picture below explains the different 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.8 ACKSYS MIB and SNMP agent

V.8.1 Access methods

The SNMP agent described here is available since firmware version 1.6.0. At the time of writing, requests to SNMP agent can use SNMP V1 or V2c. the community is “public”.

Recommended tools

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

V.8.2 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.

Relevant OIDs

The Acksys MIB covers a large range of devices. Hence all OIDs are not relevant to all products.

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 the WLn products. Please refer to the MIB to find out numeric OID values and specific description for each item.

acksysProductID	a code identifying the product.
network-product.administration	core administration functions: adminReset, adminSave, adminApply, adminResetFactory
c-key-management	management functions to save and restore configuration from/to the C-Key. Also provides test utility.
networkStatus	current (running) state of the Wi-Fi devices: statusIfWlanTable, statusPhyWifiTable
networkConfiguration	next-to-be-applied network parameters of the product, see details below.
servicesConfiguration	next-to-be-applied services configuration of the product. Only configDhcpTable is supported in firmware v1.6.0, and only one row is allowed.

Changing the configuration

When items in networkConfiguration or servicesConfiguration are changed, changes are not saved to permanent memory until ‘1’ is written to the adminSave OID. Reading this OID let you know if there are any pending (unsaved) changes.

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

Applying the configuration

To make the saved changes current, 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. This is not considered an error.

V.8.3 Managing configuration tables

Many configurations details are held in tables. Here is a summary showing how you can use each table.

Table name	Description	Number of rows
configIpSubnetTable	IP subnets IP parameters: IP address and so on	Fixed, 1 subnet
configPhyWifiTable	Radio cards configuration Parameters common to all wireless lans	Fixed, # of rows = # of radio cards
configInterfaceTable	Logical interfaces and their relationship	Fixed by agent, depends on other tables
configIfStaTable	List of Wi-Fi client interfaces	User-defined
configIfAPTable	List of VAP (virtual AP) interfaces	User-defined
configIfMeshTable	List of mesh point interfaces	User-defined, max one per radio
configIfBridgeTable	List of bridge modules (equivalent to an internal switch device)	Fixed, 1 bridge
configRadiusTable	List of radius servers	User-defined
configDhcpTable	List of DHCP pools served	Fixed, 1 pool

Fixed: user cannot insert or delete rows
User-defined: user can insert or delete row using the SNMPV2c procedure

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

- The index to 'configRadiusTable' may be used in 'configIfAPTable.configIfAPRadiusIndex', whose value will not be updated in case of insertions or deletions.
- 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.
- Currently, 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.
- Currently, the SNMP agent does not recognize repeaters created with the web interface. A workaround is shown in the examples below.

V.8.4 Using SNMP notifications (traps)

Your product support 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

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.8.5 Examples

These example scripts use snmpset (provided in the Linux net-snmp package). They are meant to run under Linux. Use them as a guideline for other cases.

The following 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 aestkip
CFGSET  192.168.1.253  configIfStaKey.\"radio0w0\"  s  "shared  psk
key"
# set bridge type to L25NAT (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.9 C-KEY handling

Some products of the product line can be equipped with a C-KEY.
The following applies to these products, when equipped with firmware version 2.2.0 or greater.

Warning: Unlike the “WLg” products series, the C-KEY is never saved or updated automatically in the “WLn” products.

V.9.1 Factory settings

Since the firmware 2.4.0 the out of box C-KEY state has changed.
In this state (Factory state) the C-KEY LED is turned off and the C-KEY contain not useable data.
After the C-KEY is initialized, there is no way to put back the C-KEY in this state.

V.9.2 Understanding configurations and their signature

A C-Key contains:

- a product model identifier;
- an archive of the configuration files appropriate for the model;
- a signature for the archive (the C-Key signature, a MD5 sum).

The product keeps an internal copy of the configuration files, so that it can work with the C-Key removed. The internal copy also has a signature (the internal signature), which is updated in 3 cases:

- when the product is reset to factory settings, the internal signature is cleared before rebooting;
- when the user copies the internal configuration to the C-Key, the internal signature is recomputed so that it is the same as the newly created C-Key signature;
- at boot time, when the C-Key signature is found different from the internal signature, the C-Key configuration and its signature are copied to the internal configuration (you can disable this copy using either the web interface or SNMP).

This procedure has several consequences.

- After a reset-to-factory-settings action, the product reboots and copies the C-Key contents, if valid; to its internal configuration, and uses it immediately; this is a sure path to ensure that the product is using the C-Key configuration;

- if you change the internal configuration, since the internal signature is unchanged, the next reboot will not load from the C-Key; instead it will use the changed configuration; this situation is shown with a warning in the web interface; it is useful for lab testing;
- if you replace the C-Key with another one containing a different configuration (hence a different signature), it will clear and replace your internal configuration at next power-on. This will not happen if you have previously disabled the C-Key function.

V.9.3 Not using the C-Key

To make sure that the C-Key is never used, you should blank it out ("erase" configuration function). The C-Key LED will then light up in red; you can configure it to disable it.

V.9.4 Replacing a product on the field

Let's imagine a product which is installed, in use and its configuration has been backed up on its C-Key. Now let's imagine that the product was damaged and needs replacement. Here is the procedure that will transfer the configuration from the damaged product "**DP**" to the new one "**NP**".

Requirements: a small screwdriver to unplug and plug back the C-Key.

1) Remove the C-Key on **NP** (if any) and keep it apart; it won't be used.
2) Power off **DP**, disconnect cables and unscrew from its support.
3) Dismount the C-Key from **DP**.
4) Plug the C-Key into **NP** and screw it.
5) Mount **NP** in its location, reconnect the cables.

   If **NP** has been used previously, and you are unsure whether its configuration disables the C-Key:

6) Power up **NP**, wait for the "Diag" LED to turn green.
7) 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 both "Diag" and "C-Key" LEDs turn green.

V.9.5 Working with the C-Key in the lab

In the lab you may not know exactly the internal configuration or the C-Key contents.

You can use the product with the C-Key plugged or unplugged. Always power off the product before plugging or unplugging the C-Key.

We suggest that you disable the C-Key, but let it mounted, while testing various configurations. When you are satisfied with your configuration you can save it to the C-Key. The "C-Key disable" flag itself is not saved to the C-Key.

Remember that a reset to factory settings will clear the "C-Key disable" flag.

Only a configuration action (saving or erasing) will change a C-Key contents.

V.9.6 Programming a set of identical C-Keys

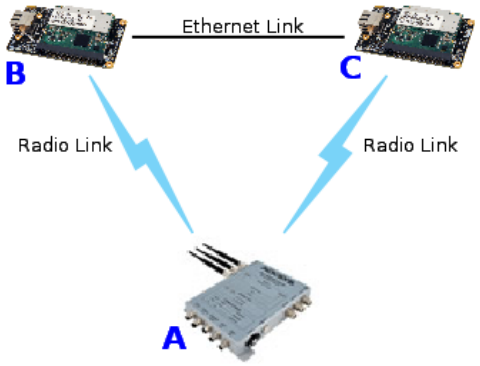
Dedicate a product to prepare the configuration and program the C-Keys.

1) Remove the C-Key from the powered-off product.
2) Reboot and configure the product as needed.
3) In “Tools/Set config/C-Key management”, select “Ignore C-Key settings” and “save option”.
4) Save and power off
5) Install a C-Key and turn power on. Wait until the diag LED turns green. Remember that after reboot the product will use its new IP address.
6) In “Tools/Set config/C-Key management” menu, click “Copy”
7) Power off the product, remove the programmed C-Key, return to step 5.

V.10 Spanning Tree Protocol (STP)

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.

Operation

When the STP protocol is activated on several interconnected bridges, they will exchange information to agree upon a unique way 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.

VI WEB INTERFACE REFERENCE

VI.1 Setup Menu

With this menu you can configure the wireless interface(s) and the networking properties.

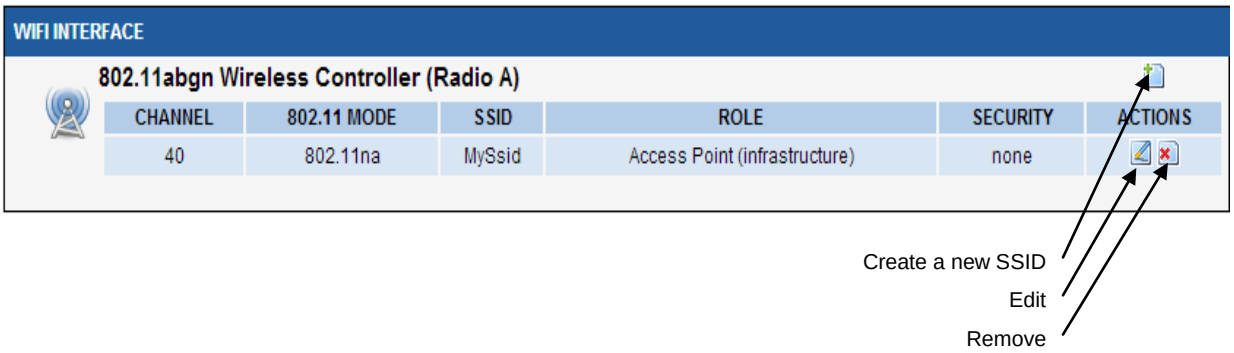
At the bottom of most “setup” pages, there are two buttons or three buttons.

After changing parameters, press “**Save**” to record in permanent memory the parameters changed in this page.
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”)

VI.1.1 Physical interfaces

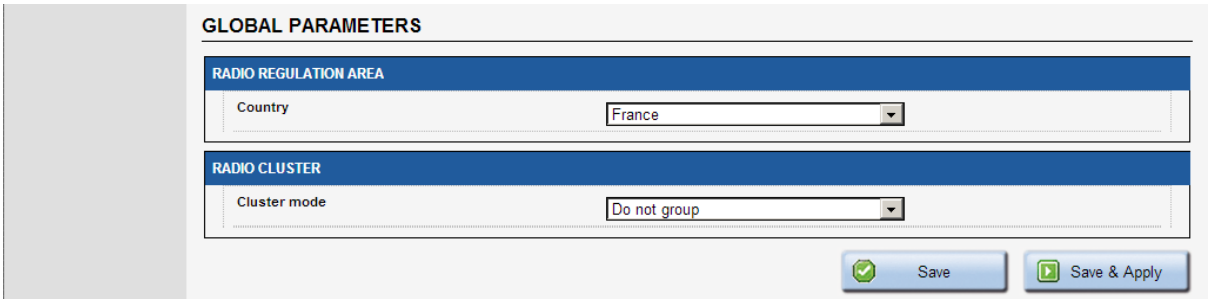
Wireless overview section:

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.



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:



Country:
The regulation rules of the selected country will determine the channels and transmission powers you can use.

Cluster mode: (only for the products with multiple radio cards)
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.

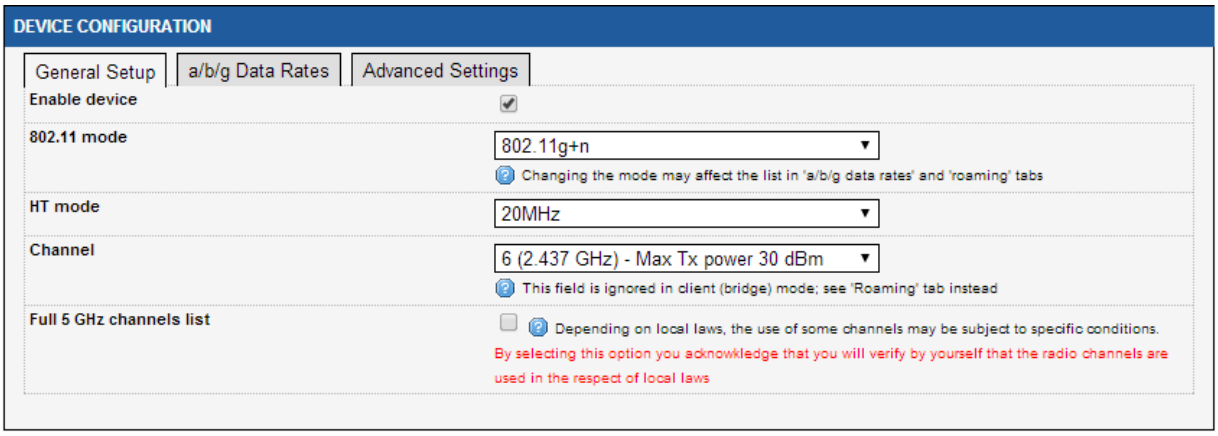
In this mode, the roaming parameters are taken from the configuration of the radio card used for data transfers.

VI.1.1.1 Wireless / Radio

a. Device Configuration

General Setup tab:

This section gathers all the settings that are common to each SSID you may create on this radio card.



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:

802.11b, 802.11g and 802.11a represent the 802.11 mode described in the "802.11 modes" section.

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.

Note: a product configured in 802.11a+n cannot communicate with another one configured in 802.11g+n because they are using different frequency ranges.

HT mode:

In 802.11n (a+n or g+n) you can use 2 adjacent channels in order to increase the bandwidth. One of the channels is the one selected in the "**Channel**" section (see below). The second one may be the one directly below or directly above.

If you choose "20 MHz", the HT mode will be disabled.

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).

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. Use the "roaming" tab to force the scan channel. See also section V.2.5: "Virtual AP (multi-SSID) and multifunction cards"

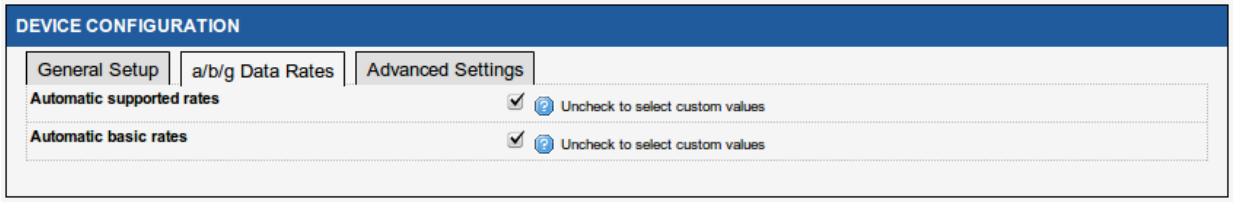
See chapter XI: "Appendix – Radio channels list" for more details on the available channels.

Full 5 GHz channel list (since 2.4.0):

The WLn series do not support the DFS. The DFS is required in several regions to use the 5 GHz band. By default this check box is uncheck and your product only allows the channels authorized in your country.

You can check this check box to use the full 5 GHz channels list, but in this case you must verify by yourself that the radio channels are used in the respect of local laws.

a/b/g/n Data Rates tab:



Automatic supported rates:

This option allows you to restrict the rates that your Access Point advertises as supported to the clients.

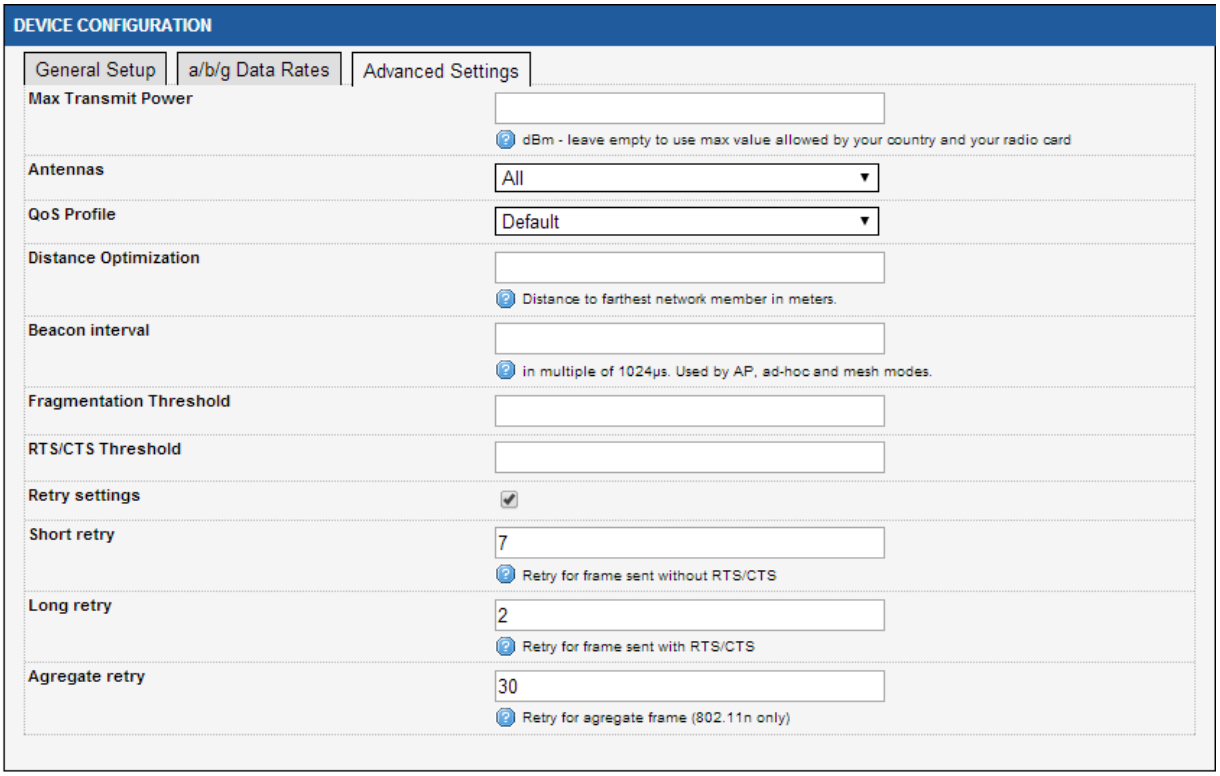
Automatic basic rates:

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.

Advanced Settings tab:



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).

b. 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.

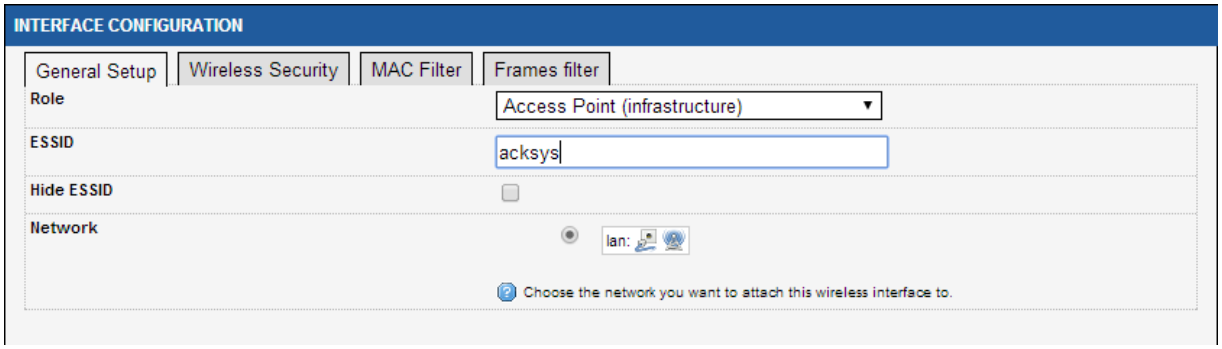
Loops pitfall in products with more than one radio

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 are 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 tab:



Role:

Supported roles are:

- Access point
- Isolating Access Point
- Client (connecting to an Access Point)
  Note: 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.
- Repeater (combination of an AP and a client targeting the next AP)
- Mesh 802.11s
- Point to multipoint station (ad-hoc mode)

See a detailed description of the modes in section V.2.

Multiple ESSIDs (only in client mode):

When this is checked, a multi-selection field 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 VI.1.2.2 – Wireless SSID.

ESSID:

This is the wireless network name. See section "802.11 modes" for more details.

Hide ESSID (only in Access point mode):

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.

Mesh ID (only in Mesh mode):

This option replaces the ESSID when the Mesh mode is selected. It has the same purpose.

BSSID of the next repeater (only in Repeater mode):

In Repeater mode, devices must be chained. This option represents the BSSID of the next link in the chain.

Wireless network nicknames (only in client mode):

On this list you have all SSID configured previously. Please see section VI.1.2.2 – Wireless SSID for more details.

The client interface will associate with one of the SSIDs selected in this list, at a time.

Network:

This option allows selecting the network where the interface is added. Please see section Network for more details on network management.

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
- WPA2-PSK
- WPA-PSK/WPA2-PSK Mixed Mode
- WPA-EAP
- WPA2-EAP
- WPA-LEAP
- WPA2-LEAP

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

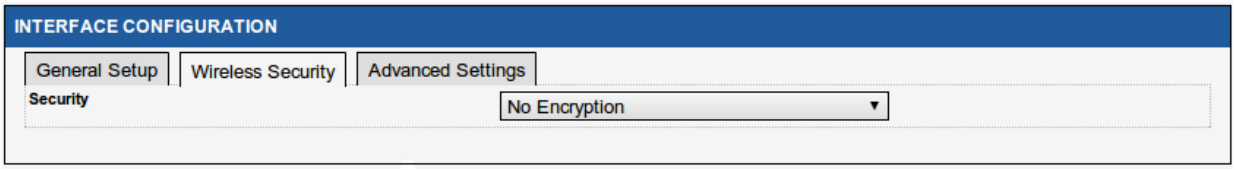
According to the choice you've made, some properties will appear or disappear.

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.

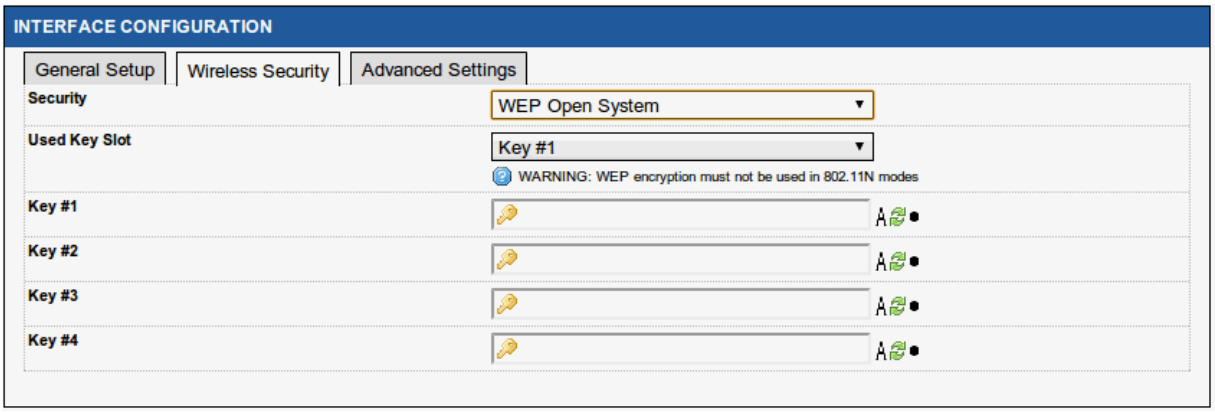
You need to properly configure the APs, their mobility domain and NAS ids to take advantage of this feature.

Wireless Security tab, No Encryption mode:



Nothing to configure here.

Wireless Security tab, WEP Open System & WEP Shared Key:



Use Key Slot:

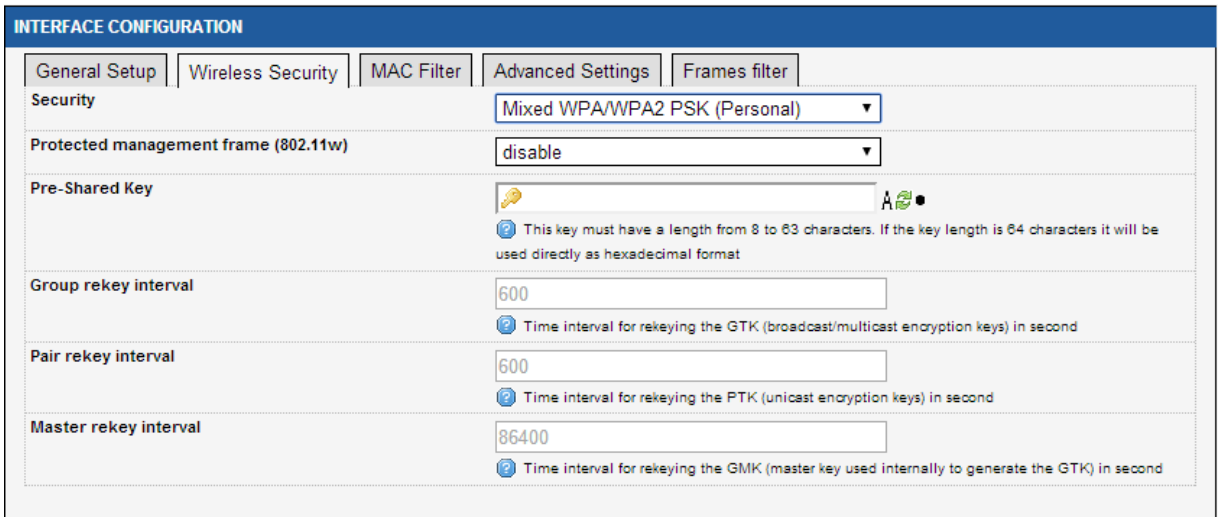
This field selects the currently used WEP key.

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 (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.

Wireless Security tab, WPA-PSK, WPA2-PSK & WPA-PSK/WPA2-PSK Mixed Mode:



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).

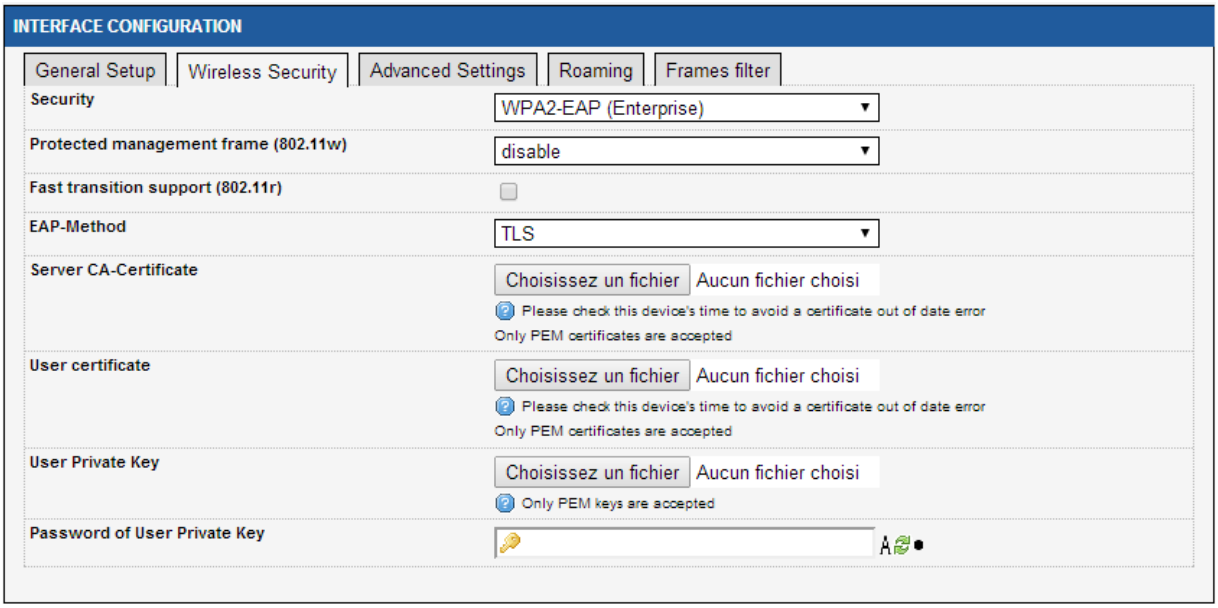
The green arrow icons on the right allow to display the key in clear text while you are typing it in.

Group rekey (AP mode only): interval: Time interval for rekeing the GTK (broadcast/multicast encryption keys) in seconds.

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):



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)

Key cache life time:
In any of the EAP modes, this indicates how much time the conversation keys are retained in case the client roams back to an already authentified AP. This reduces the roaming delay by removing most of the authentication overhead.

You need to properly configure the APs to take advantage of this feature.

EAP-Method:
This field contains the EAP-Method to be used.
Available methods are: TLS, PEAP, LEAP

Server CA-Certificate:
Selects the location of the CA-Certificate file to be uploaded. Only PEM certificates are allowed (see below for details).

User certificate:

Selects the location of the user certificate file to be uploaded. Only PEM certificates are allowed (see below for details).

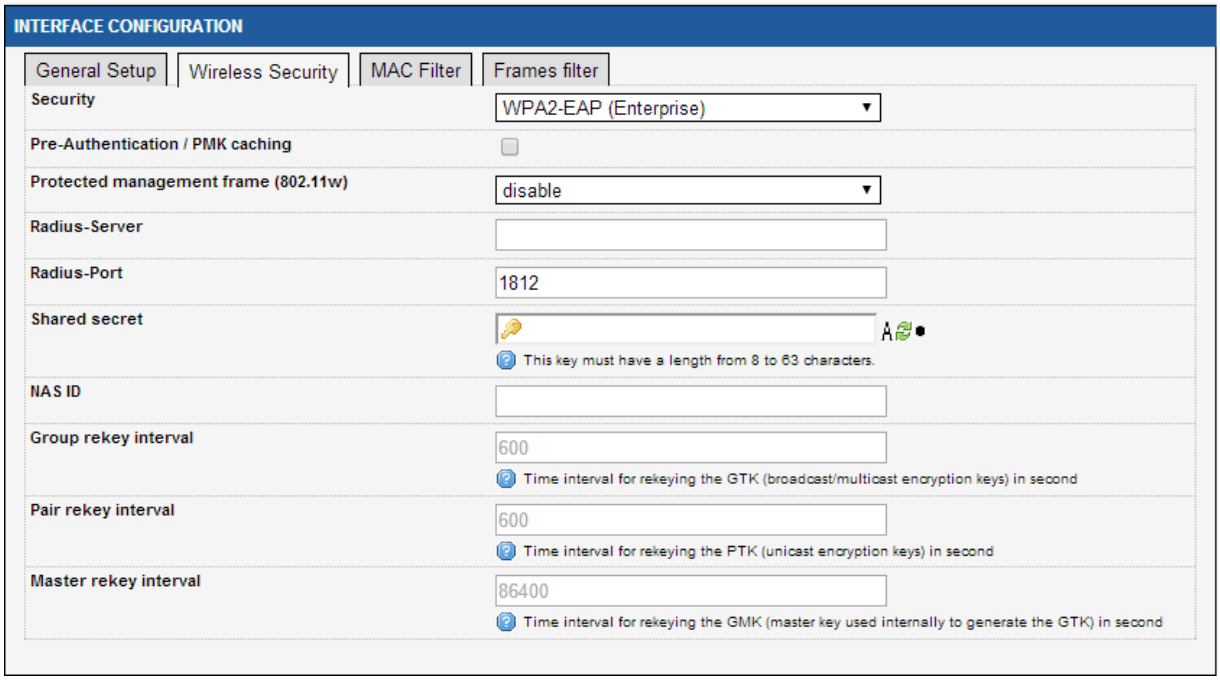
User Private Key (only in TLS mode):
Selects the location of the Private Key file to be uploaded. Only PEM private keys are allowed (see below for details).

Password of User Private Key (only in TLS mode):
Password associated to the chosen Private Key.

Authentication:
This field contains the Authentication method.
Available methods are: PAP, CHAP, MSCHAP, MSCHAPV2, Custom

NOTE : Certificates and keys must be provided in PEM format. This format is defined by the OpenSSL project. It is a text file recognizable by a starting line beginning with "-----BEGIN" and the binary data encoded using the base64 method. See http://www.openssl.org/docs/HOWTO/certificates.txt for more details.

Wireless Security tab, WPA-EAP Mode (in access point mode):



Pre-Authentication / PMK caching :
In any WPA/WPA2-EAP mode, check this box to allow use of pre-authentication / PMK caching.
For more information, please 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.

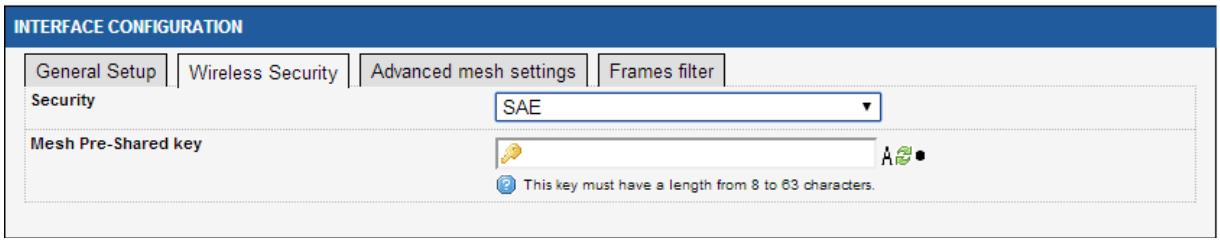
NAS ID: Network Access Server ID. This value may be used by the radius server instead of the IP address.

Group rekey: interval: Time interval for rekeing 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.

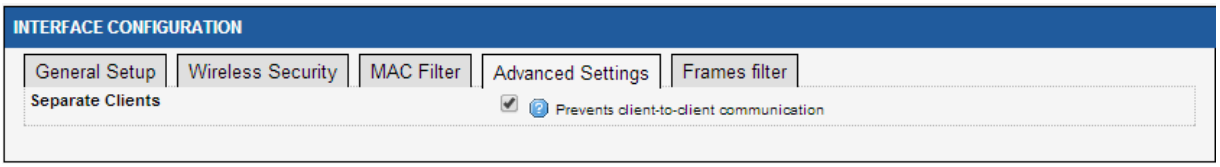
Wireless Security tab, SAE Mode (in mesh mode):



Mesh Pre-Shared key:
This option allows configuring the mesh network shared key.

Advanced Settings tab:

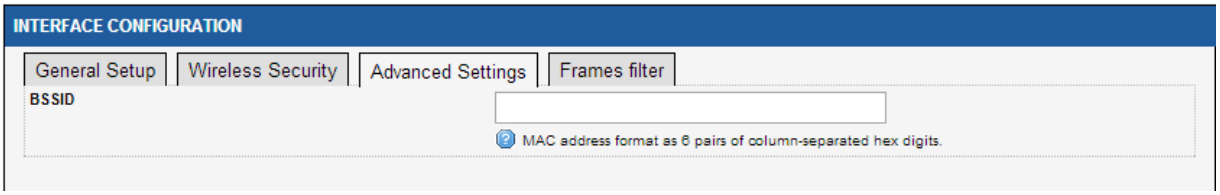
Advanced settings tab in "Isolating Access point" mode



Separate Clients:

If this option is checked, wireless clients won't be able to communicate between them. This option is only available when the "Isolating Access Point" role is selected. The "Access point" mode cannot separate clients. See section "Infrastructure Mode" for more details.

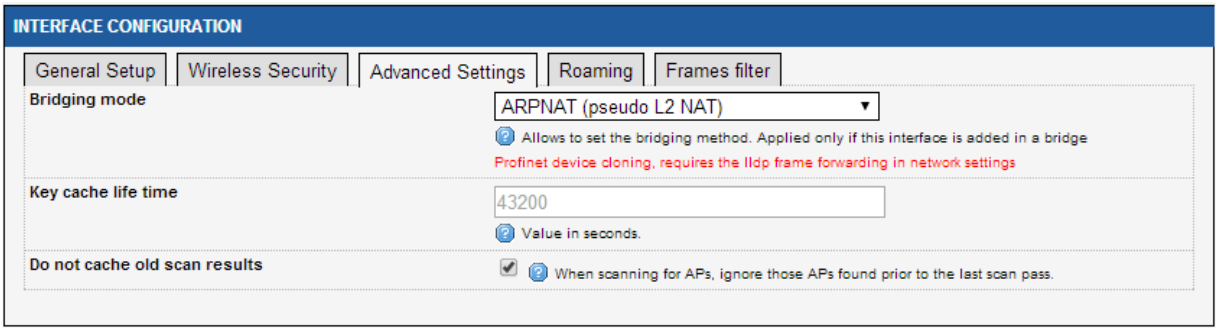
Advanced settings tab in “Point to multipoint station (ad-hoc)” mode



BSSID:

This option allows setting the BSSID for this interface.

Advanced settings tab in “Client” mode



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. This feature requires LLDP forwarding. Please read the section Network configuration for more details.

Please read the section Cloning for more details on cloning mode.

Key cache life time:

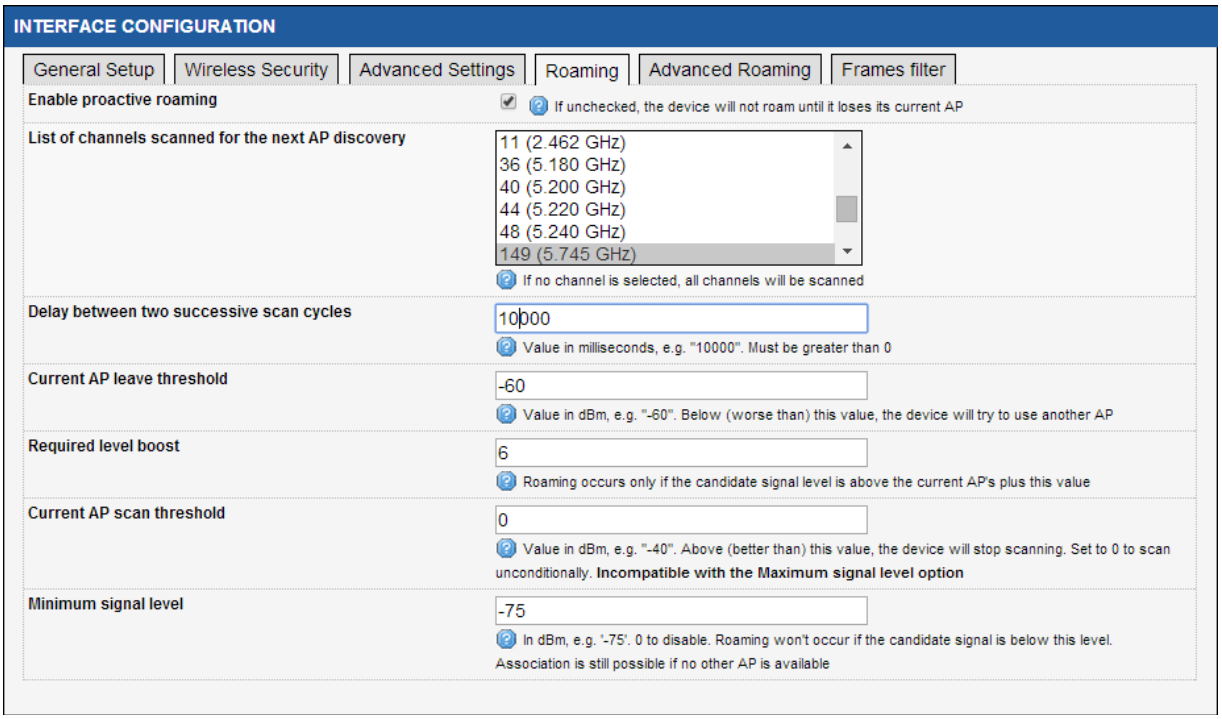
If your AP supports the Opportunistic key caching (OKC) or the pre-authentication, this option allows configuring the life time for each PMK.

The default value is 43200 seconds (12 hours).

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.

Roaming tab (only in Client mode):



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.

Using more than one channel allows a denser repartition of the Access Points, as they will not interfere with each other. But 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.

To achieve the best throughput we recommend using only one channel.

Delay between two successive scan cycle:
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.

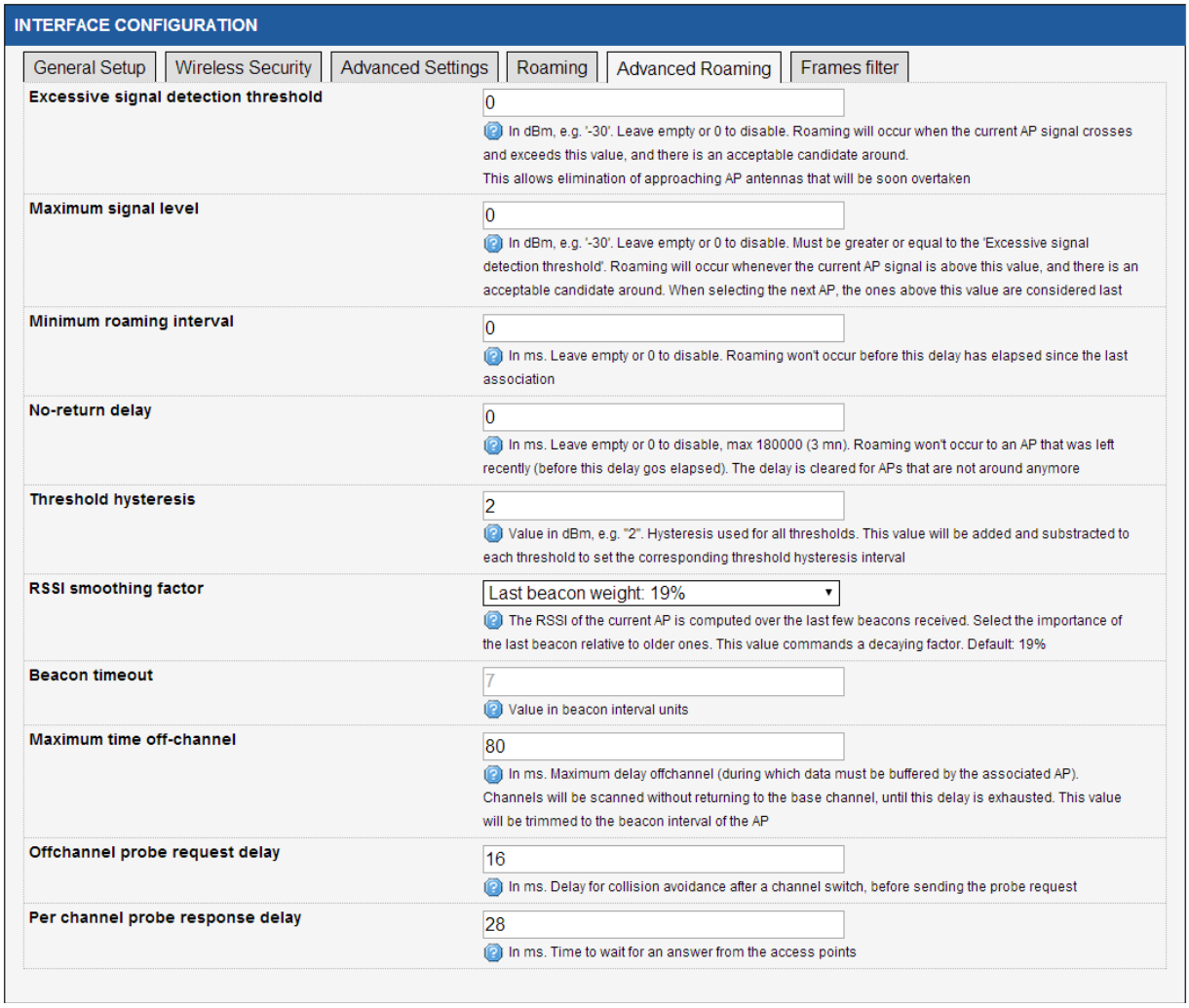
Note: in previous versions this parameter was named “Current AP minimum signal level”.

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 in Client mode):



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.

Minimum roaming interval:
If you want to avoid continual roaming when all the APs have about the same low signal level (below the leave level), you can enforce a minimum delay between two successive roaming processes.

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 are far, you can add a delay here.

Threshold hysteresis:
In order to avoid oscillating behaviors 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 ± 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.

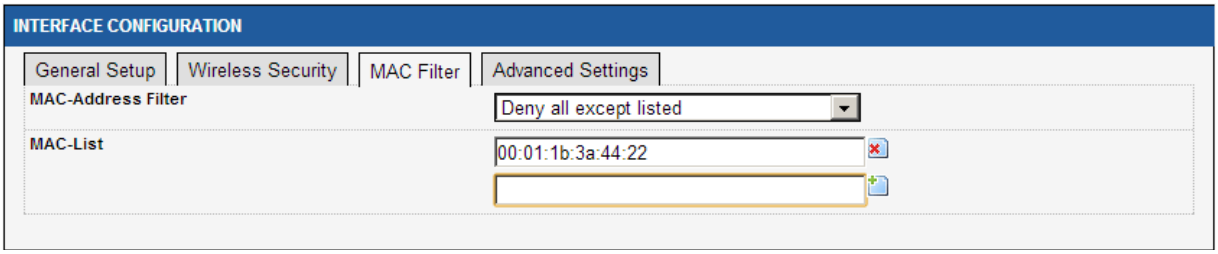
Maximum time off-channel:
When scanning another channel, the current AP is told to buffer incoming data until the client returns to the channel of the AP. Some APs have insufficient buffers and loose data in the meantime. This parameter limits the duration where the scanner is scanning on other channels, so the 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 probe request delay:
When switching to another channel, the radio must listen silently to synchronize with existing devices already using the new channel. The probe request is sent after this delay elapses after the channel switch.

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.

MAC filter tab (only in Access Point modes):

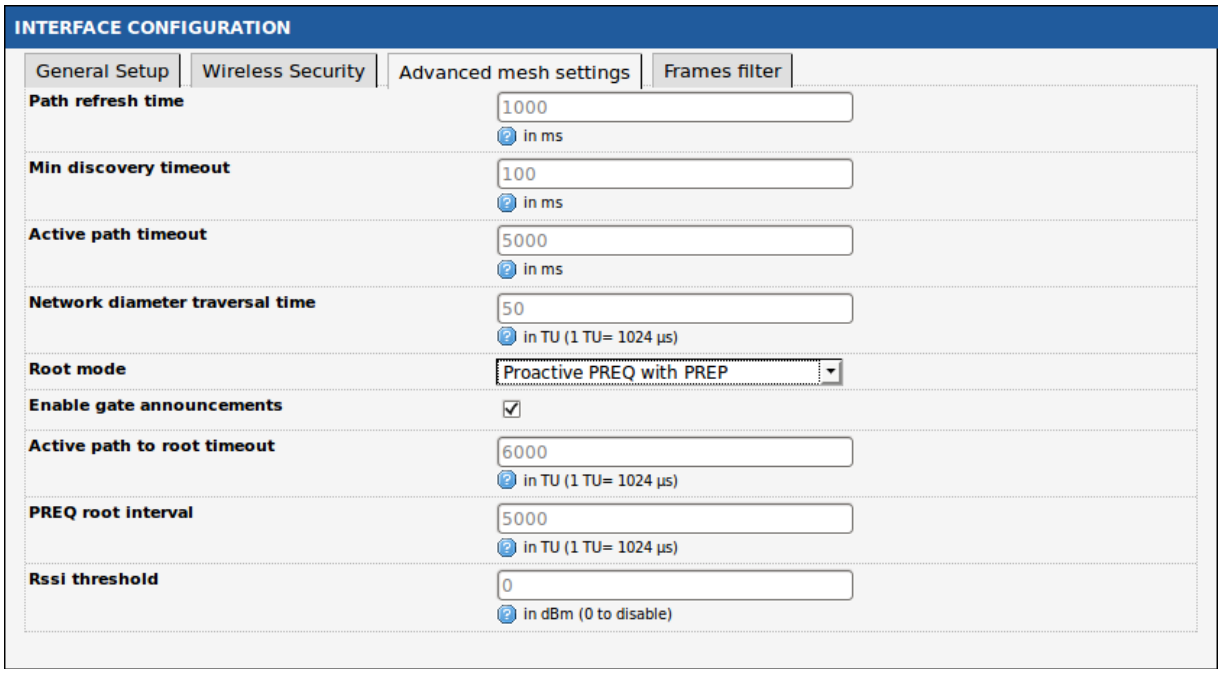


MAC-Address filter:
You can specify a list of client MAC addresses that will be either allowed or denied. Let the filter disabled if you do not require it. **WARNING**: this must not be used alone as an effective security feature, since MAC addresses are is easy to masquerade.

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):



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 timout 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 reduces 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 a 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.

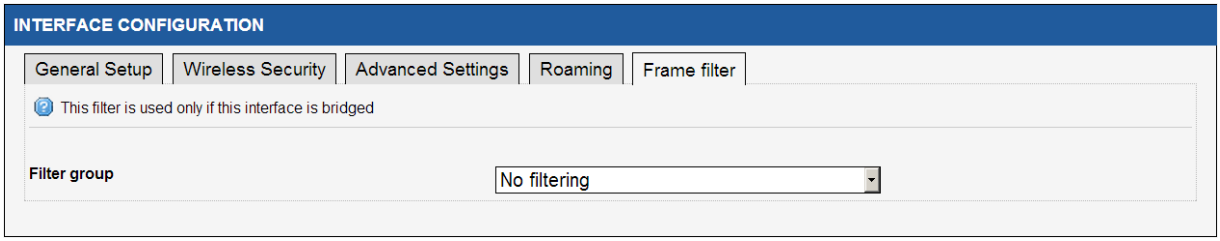
Active path to root timeout (root mode only):
This is the same as “Active path timeout” but is used only in proactive PREQ sent by this root node.

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.



Filter group:
Choose one of the filters prepared in routing/firewall → bridge filter section.

VI.1.2 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.

VI.1.2.1 802.1q Tagging

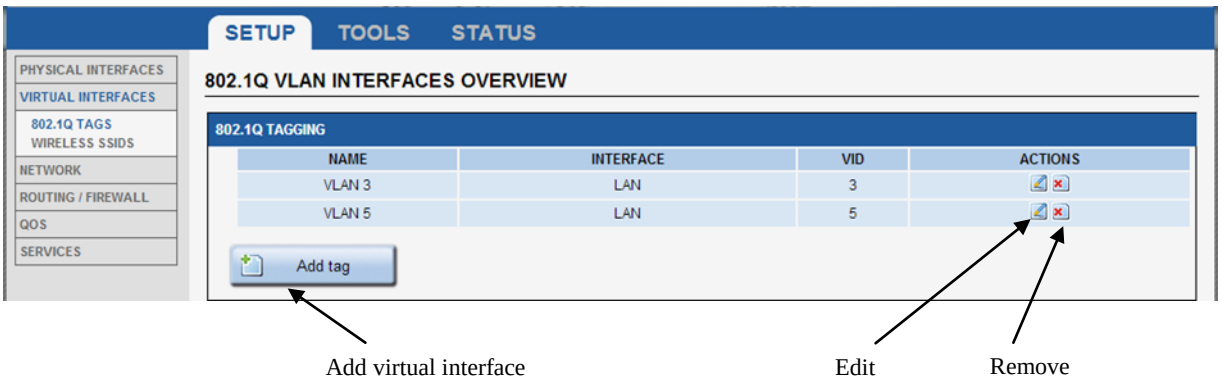
802.1q tags are used to split a common physical link into several virtual LANs (VLANs) in order to isolate the traffics pertaining to groups of devices. Each group is given a different VLAN ID which is used to mark the data frames exchanged within the group. Then, only devices configured to use the VLAN 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.

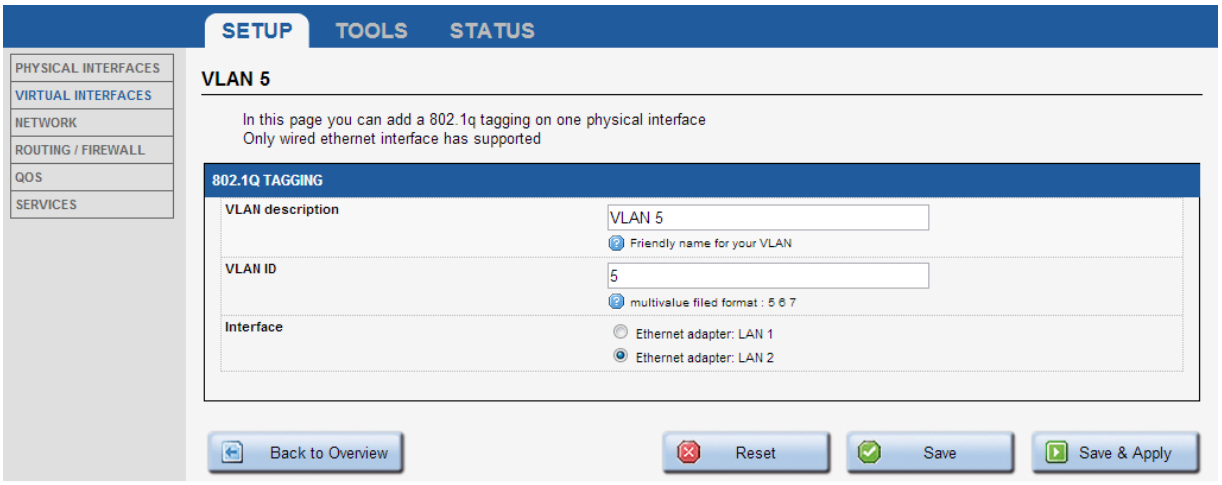
a. <u>VLAN Overview:</u>

This page displays the list of actual virtual interfaces created.



Click the "**Remove**" button to remove the virtual interface.
Click the "**Edit**" button to open the virtual interface configuration page.
Click the "**Add network**" button to create a new virtual interface.

b. VLAN configuration:



VLAN description
Enter a friendly name for this interface (optional).

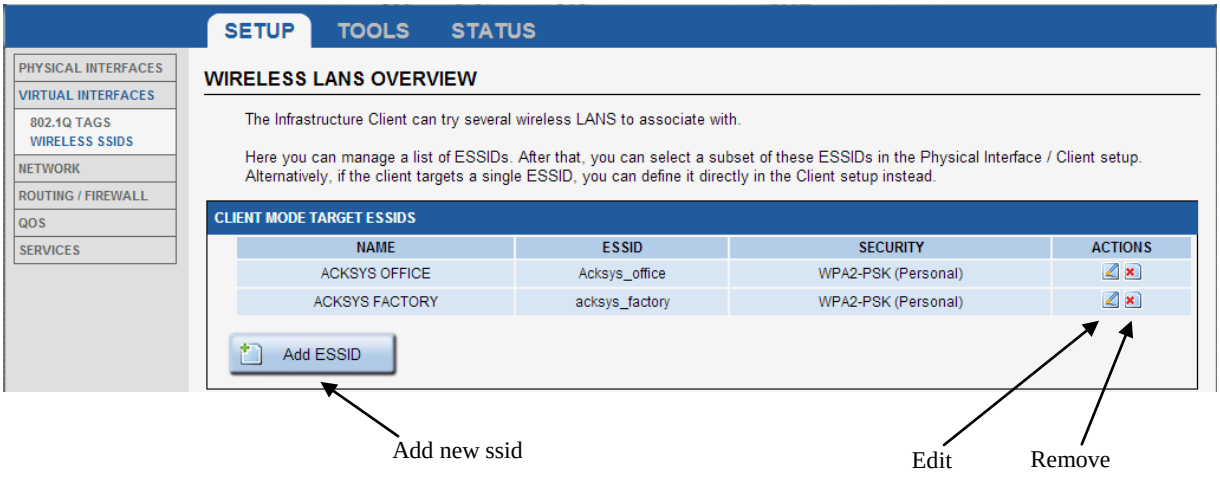
VLAN ID
Enter the id for virtual interface. If you need to create several VLAN IDs on top of the same physical interface, you can use the space character to separate the IDs. Example: 5 10 120

Interface
Select the physical interface on which you create the virtual interface.

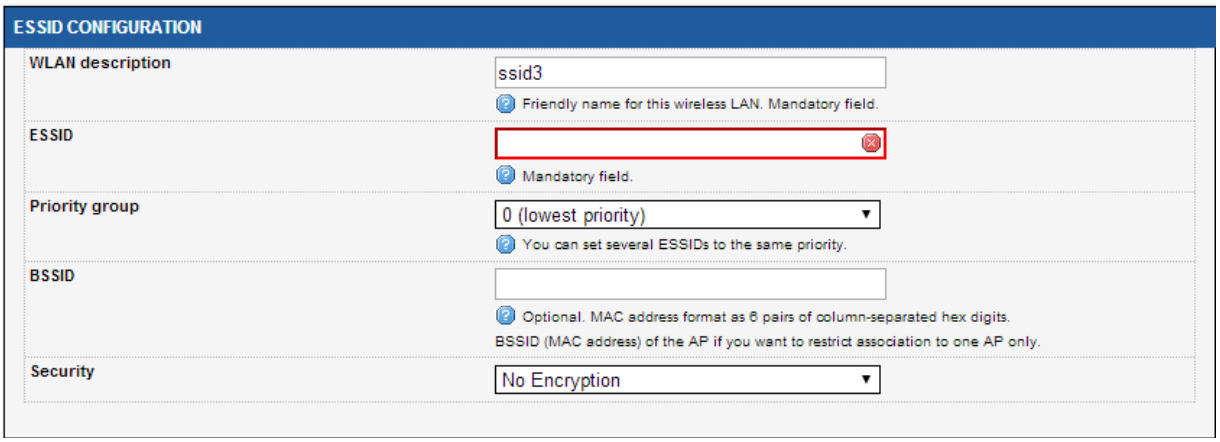
VI.1.2.2 Wireless SSIDs

The wireless SSID section is used to configure several SSID and enable it on Wireless interface.

a. Wireless SSID overview



b. Wireless SSID configuration



WLAN description (optional):
Enter a friendly name for this SSID.

ESSID:
Network name (also called SSID).

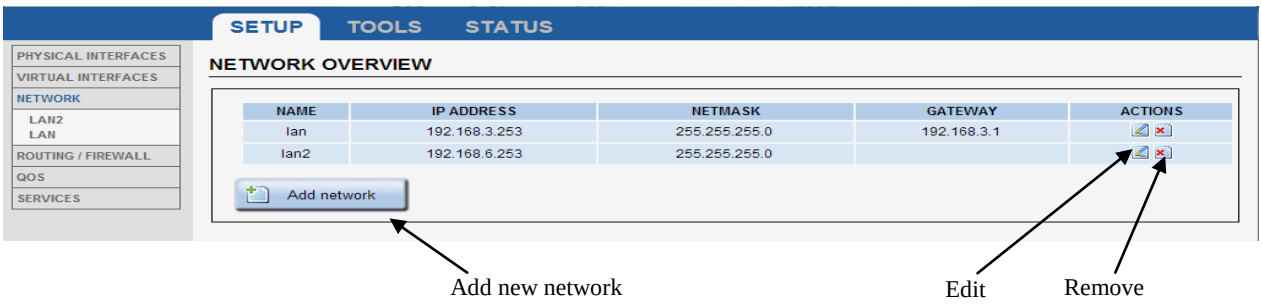
Priority group:
The scan process will choose the AP with the SSID of highest priority. If you have several APs advertising SSIDs of the same priority, the product will choose the AP with the best signal.

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:

VI.1.3 Network

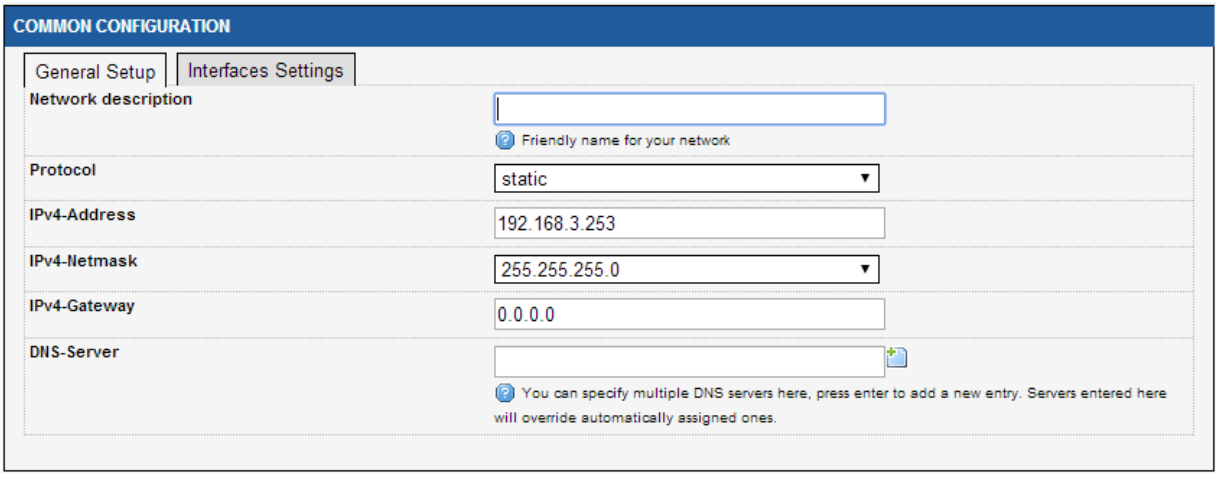
This page displays the actual network configuration.



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.

VI.1.3.1 Network configuration

General Setup:



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 AP. In this case, you do not need to fill in the fields shown above except possibly "**DNS-Server**" and "**Enable STP**".

Choose "s**tatic"** 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.

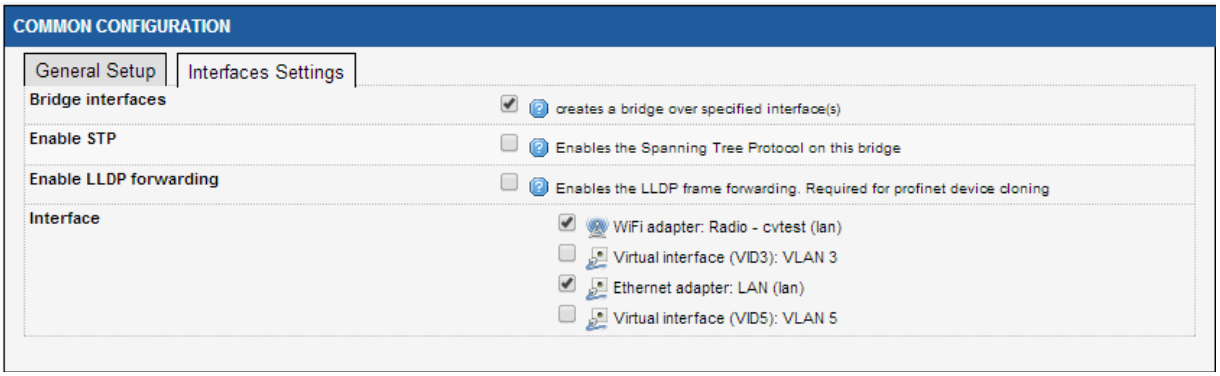
IPv4-Address (only in static mode):
The IP address of the AP on the local area network. Assign any unused IP address in the range of IP addresses available for the LAN. For example, 192.168.0.1.

IPv4-Network (only in static mode):
The subnet mask of the local area network.

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.

DNS-Server:
The IP addresses of the DNS server(s) you want to use.

Interfaces Settings:



Bridge interfaces:
If checked, all interfaces in this network are linked with the software equivalent of an Ethernet switch.

Enable STP:
If checked, the STP (Spanning Tree Protocol) will be activated on this bridge. If you choose to not use STP, you have to set up your devices to avoid network loops by yourself.

Enable LLDP forwarding:
Check this box if the internal bridge must forward the LLDP Multicast frame.
This option is mandatory if you want to use the "Profinet cloning" on Wi-Fi interface.

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.

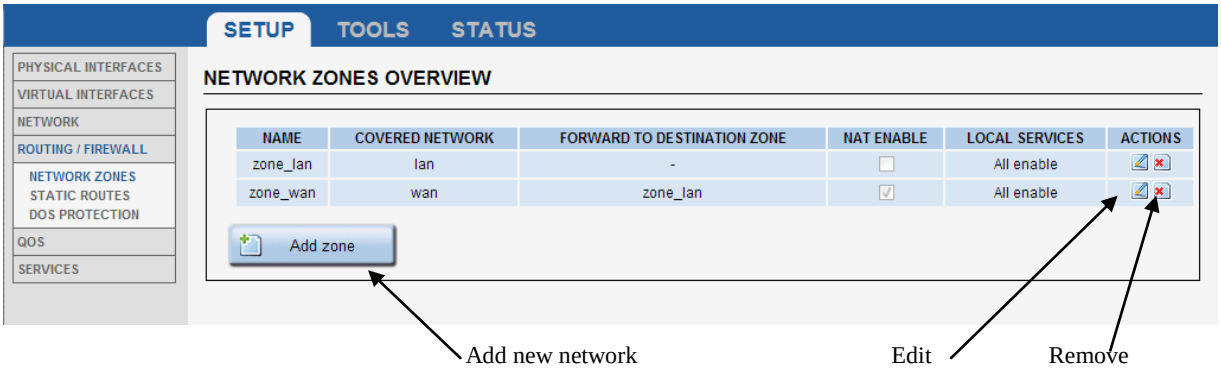
VI.1.4 Routing / Firewall

VI.1.4.1 Network zones

The routing rules are applied on a network zone. Zones are aggregates of networks which share the same forwarding rules. You can define zones and distribute networks between them.
In each network zone you can:

- Set the forwarding rules towards other zones
- Set the NAT filtering rules
- Set the firewall rules

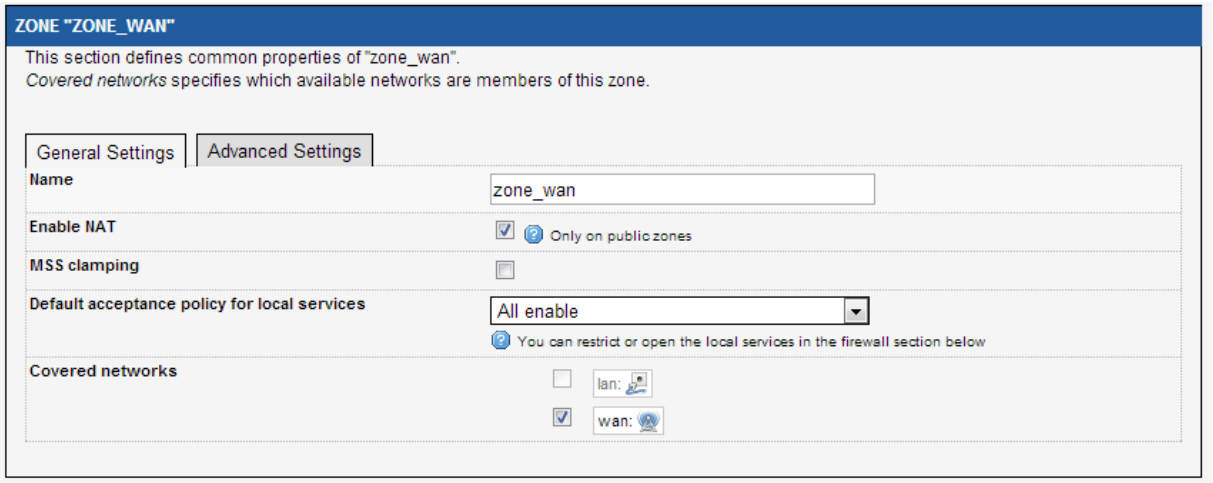
a. Zones Overview



Click the "**Add zone**" button to create a new zone.
Click the "**Edit**" button to open the zone configuration page.
Click the "**Remove**" button to remove the zone.

b. General Zones settings

General Settings



Name:
Friendly name for the zone.

Enable NAT:

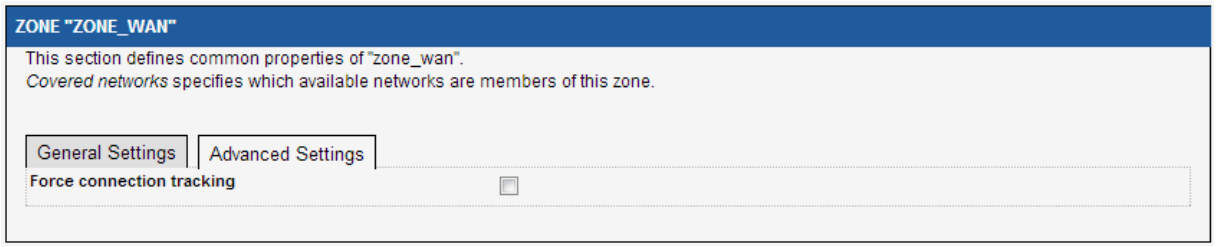
Enables NAT on this zone. Check this option only on zones which contains public interfaces.

MSS clamping:
Reduces the MSS 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.

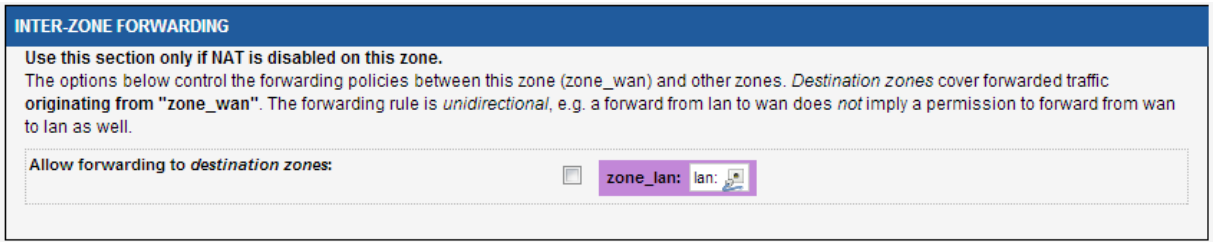
Advanced Settings



Force connection tracking:
By default the firewall disables the connection tracking for a zone if the NAT 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.

c. Inter-zone forwarding

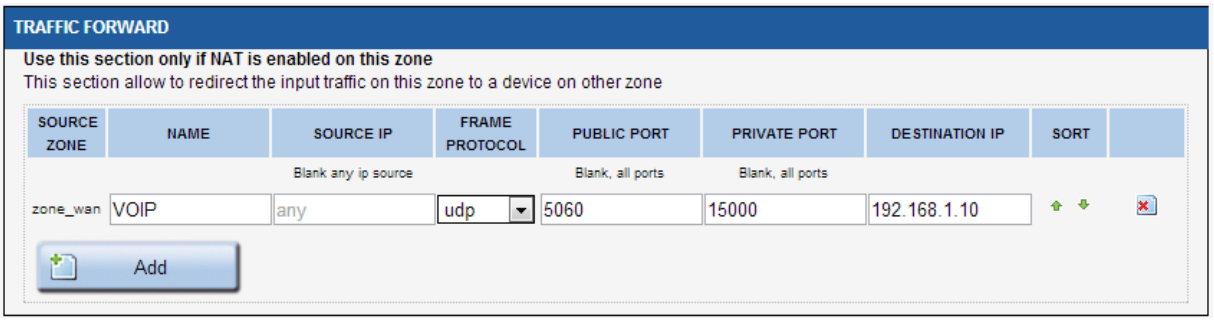
This section is used only if NAT is disabled on this zone.



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.

d. Traffic forwarding

Use this section to forward traffic to the private side when the NAT it 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.

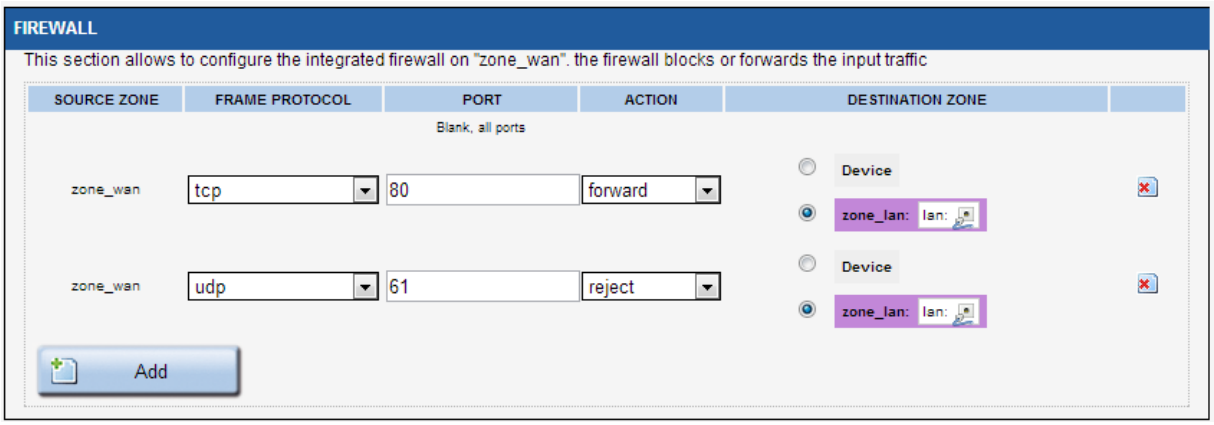
Public port:
Sets the expected destination port of the input frame on this zone. You can specify either a single port or a port range (using a dash "-" between the starting and ending ports). If this field is blank, any port will match.

Private Port:
The NAT 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 width.

Destination IP:
The NAT 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**.

e. Firewall

This section it used to restrict or allow the use of services provided on the device (locally in the product) or in other zone.



Frame protocol:
The protocol type: TCP, UDP, TCP & UDP, ICMP, all

Port:
The destination port of the traffic. The port identifies the service.

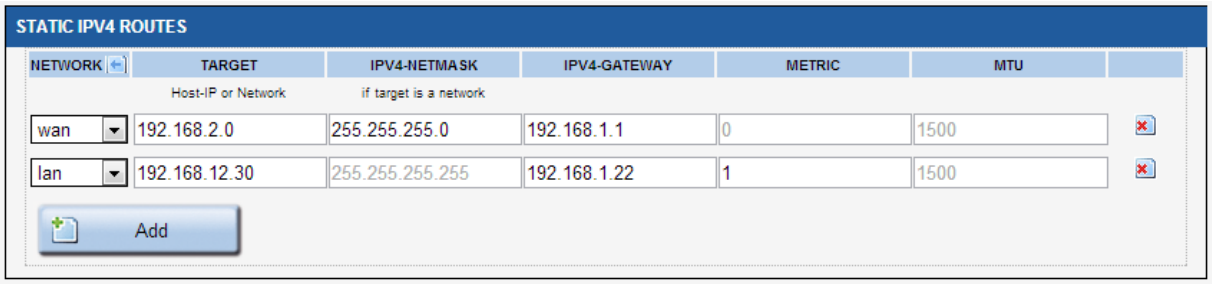
Action:
One of:

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.

VI.1.4.2 Static routes

In this section you can add a static route in the device.



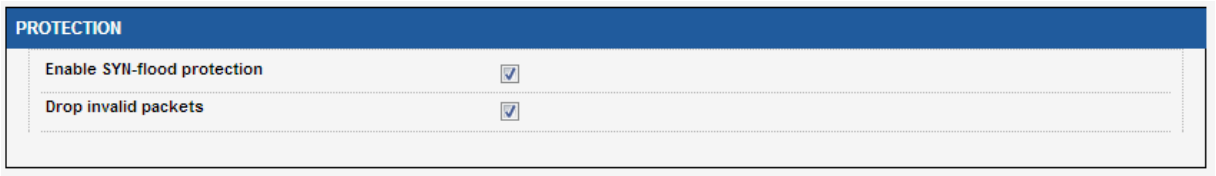
Target:
Destination host or network IP address.

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.

VI.1.4.3 Denial Of Service (DOS) protection



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

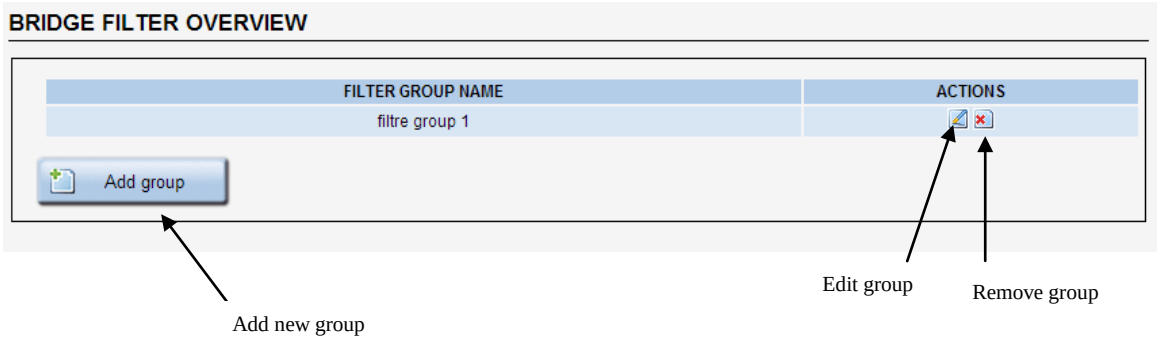
Drop invalid packets:
Drop invalid frames or frames without active connection.

VI.1.4.4 Bridge filter

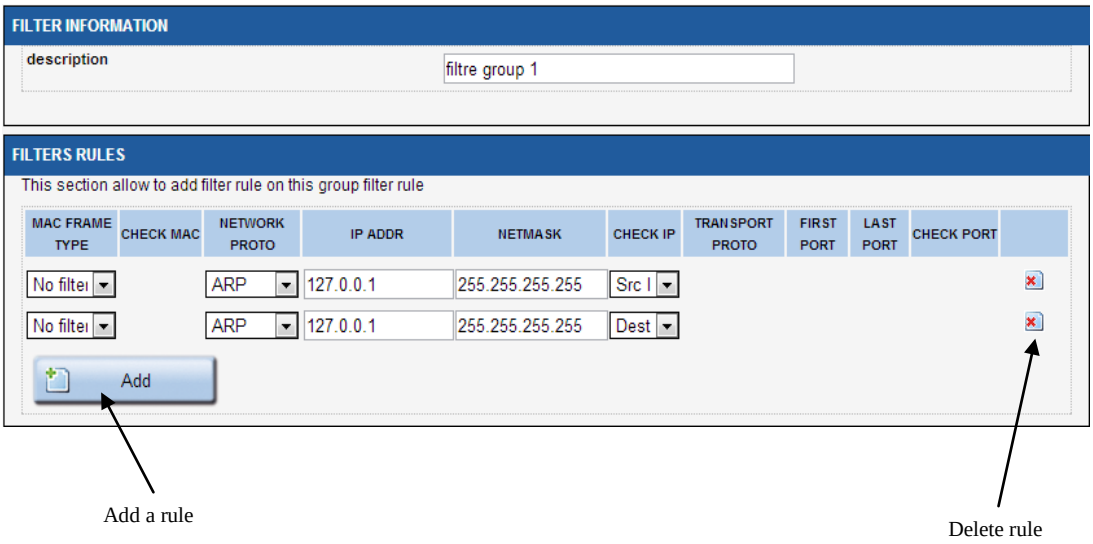
In this section you can manage layer 2 (link-level) filter groups.
Each filter group may contain several rules and may be affected to one or more Ethernet or Wireless interfaces, provided they are included in a bridge.

The filter drops the frame if one rule matches in group.

a. Add group



b. Edit group



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 uncast 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 of *no filter*

- Src Addr: Check the frame type on source MAC address field
- Dest Addr: Check the frame type on destination Mac address field

Network Proto:
Select the layer 3 protocoles

- 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 adresse 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

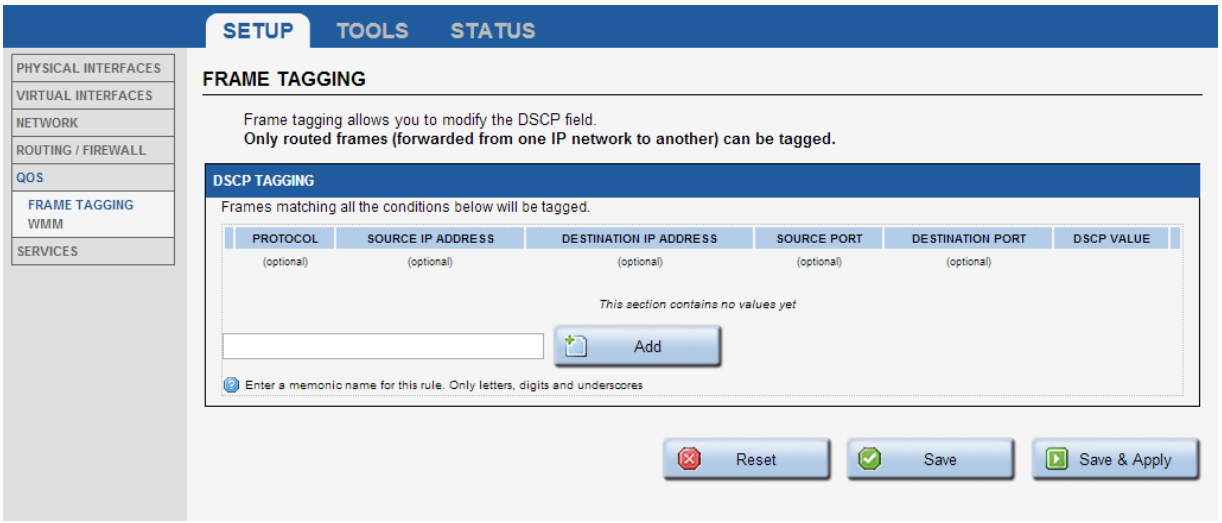
First port & Last port
These fields are visible only if the transport protocol (Layer 4) is set to UDP or TCP.
Check if the frame used the port between first and last port.

Check Port
This field is visible only if the Transport protocol (Layer 4) et set to UP or TCP.

- Src: Check on source port.
- Dest: Check on destination port.

VI.1.5 QOS

VI.1.5.1 Frame tagging



DSCP 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.

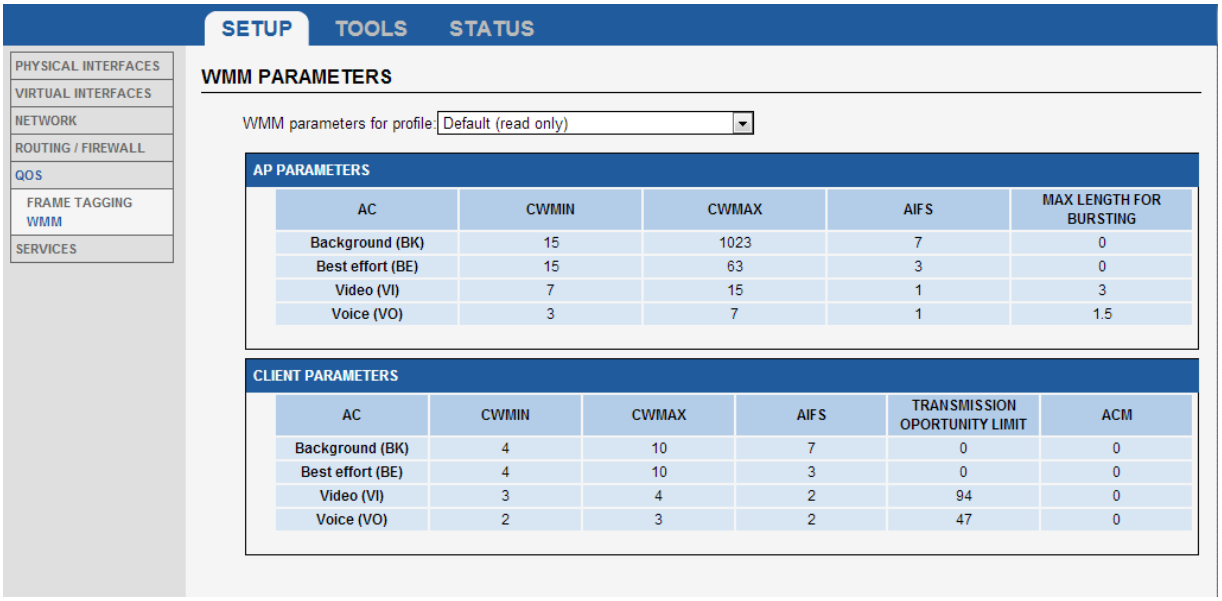
SOURCE PORT:
The source port of the incoming frame. This parameter is valid for TCP & UDP protocols only (see above). You can specify either a single port or a port range (using a dash "-" between the starting and ending ports).

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 (using a dash "-" between start port and end port).

DSCP VALUE:
The value to be written in the DSCP field (6 bits) of the IP frame.
You can use the following table below 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)

VI.1.5.2 WMM



The page displays the WMM parameters for the selected profile. WMM (a.k.a. WME) is always available.

Profile selection:

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 4 AP 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.

STA Parameters:

This table allows you to change the WMM parameters sent by the AP 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.

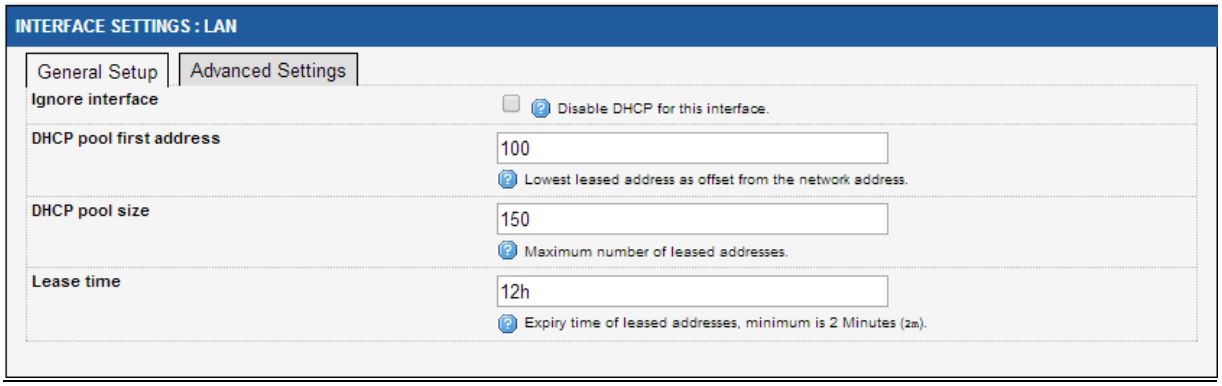
AIFS:
Defines the arbitration inter-frame spacing value for the current queue (expressed in number of time slots). Allowed values are 1 to 255.

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.

VI.1.6 Services

VI.1.6.1 DHCP Server



Interface settings: LAN: General Setup:

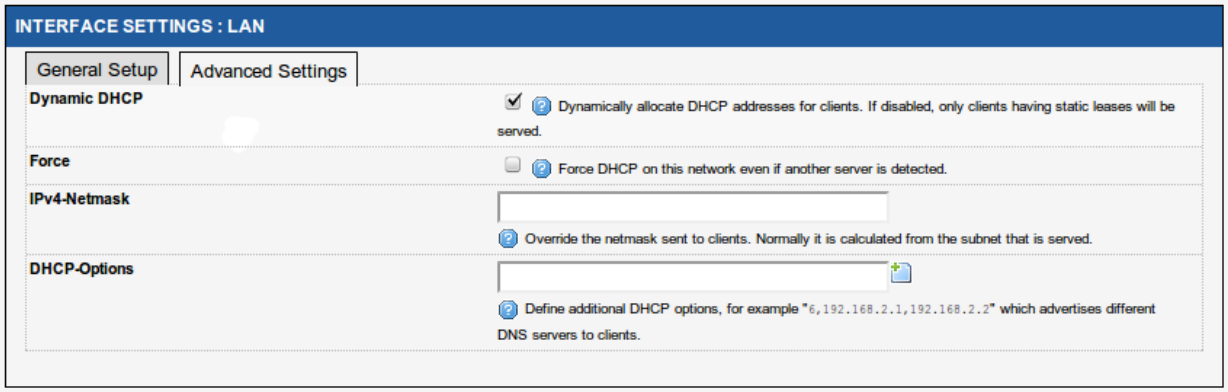
Ignore interface:
If checked, the DHCP server is disabled for this interface.

DHCP pool first address (if DHCP enabled):
First IP address of the DHCP pool. ATTENTION: this is interpreted as an offset relative to network address.

DHCP pool size (if DHCP enabled):
Maximum number of leased addresses.

Lease time (if DHCP enabled):
This represents the time during which a given IP address remain valid. After that time, the client needs to renew his lease.

Interface settings: LAN: Advanced Settings:



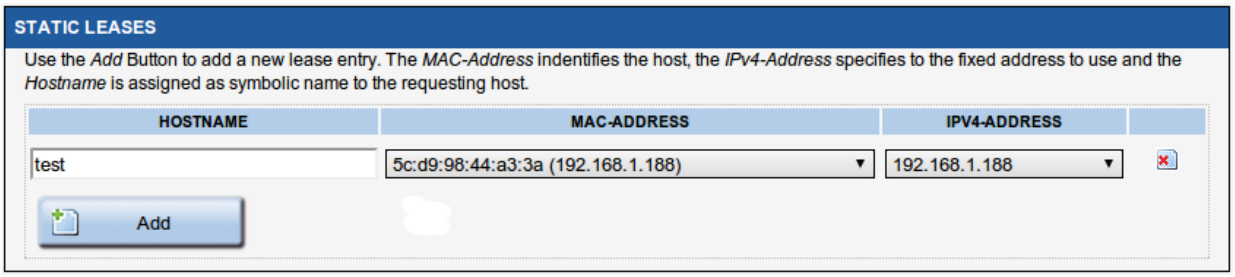
Dynamic DHCP:
If unchecked, only static leases will be authorized (see section "DHCP Server").

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 another server before start.

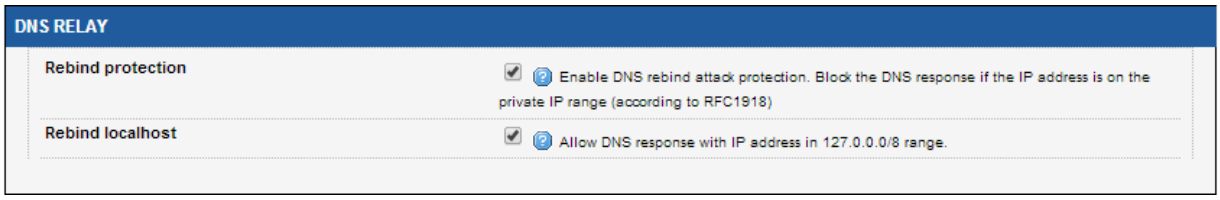
Ipv4-Netmask:
This option override the default netmask value sent to DHCP clients.

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 Lease:
This option allows to always give the same predefined IP address according to the client MAC address.

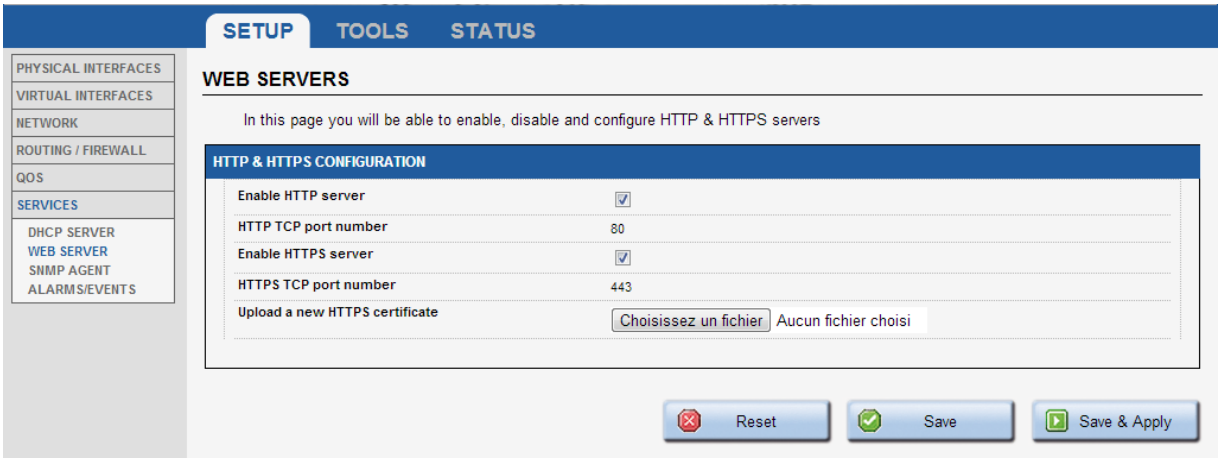


DNS relay
These options enable DNS protection Attack.



VI.1.6.2 Web Server

This menu allows you to activate and configure HTTP and HTTPS servers.



For the HTTPS server, you can give a web certificate file and upload it using the "**Upload Certificate**" button.

VI.1.6.3 SNMP Agent

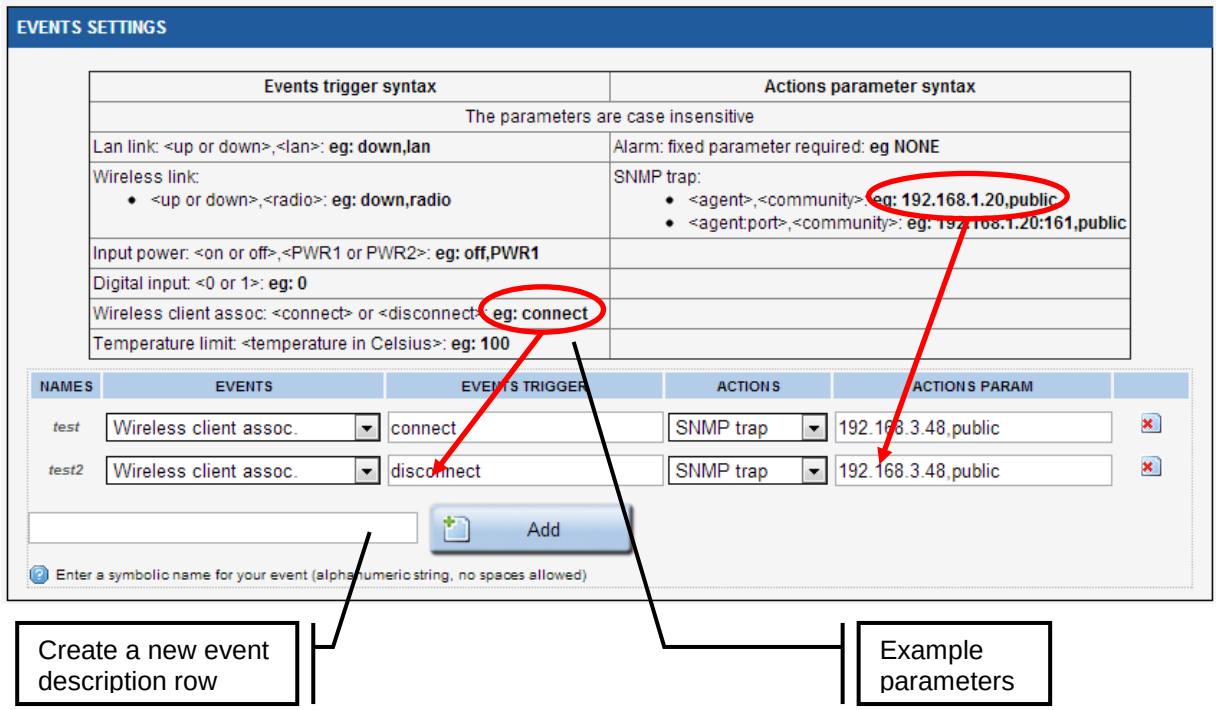
The SNMP agent is enabled by default and allows access, using the "**public**" community, to the MIB-II and ACKSYS MIB. Further configuration of the agent itself is not yet available – coming soon.

The Aksys MIB file is self-documented. To read the OIDs documentation please use a text file editor or MIB browser.

VI.1.6.4 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.

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.

Wireless client assoc: The event can be linked only with the 'SNMP trap' action. 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.

Actions:

The "snmp" action, when triggered, will send the relevant trap to the specified manager address using the specified community.

The "alarm" action only exists in some products. When triggered, the alarm contact will be activated as specified in the product "quick installation guide".

VI.2 Tools Menu

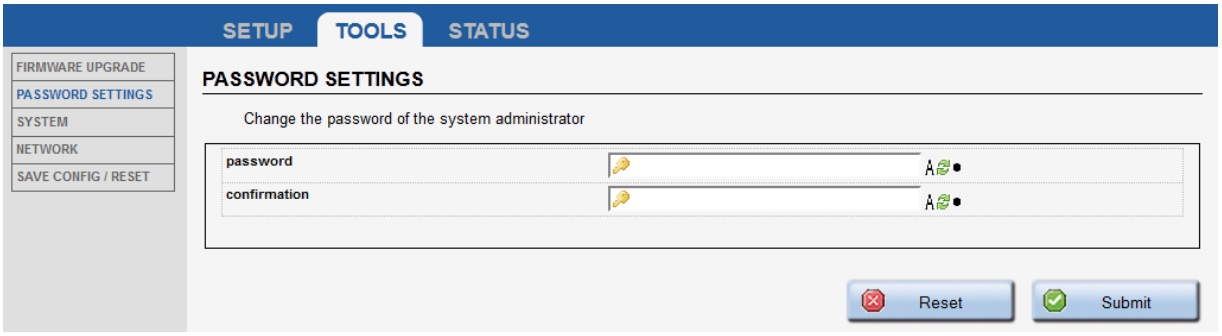
This menu allows you to administrate your product. A set of menu is provided and offers simplified the following possibilities:

VI.2.1 Firmware upgrade

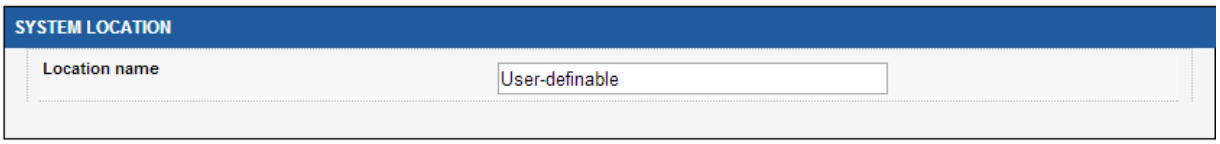
Firmware upgrade has its own section in this user manual: "Firmware Upgrade".

VI.2.2 Password Settings

In this menu, you can modify the product's password.

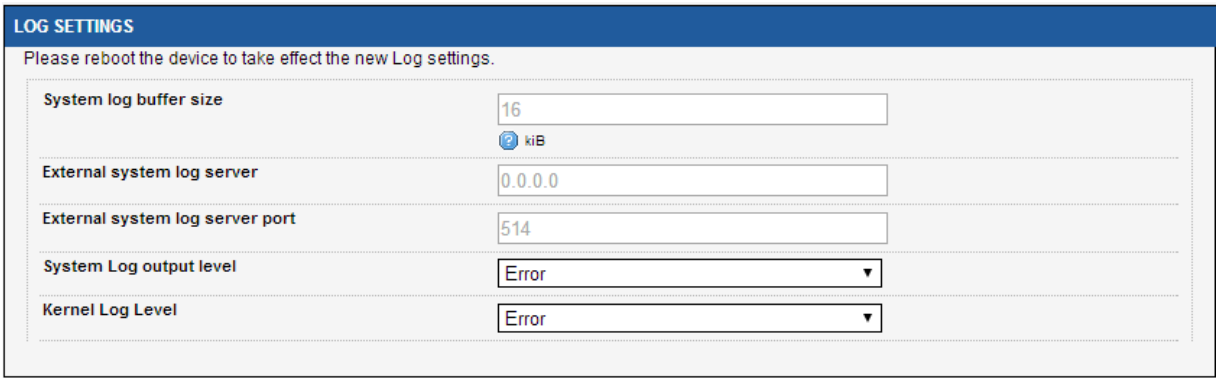


VI.2.3 System



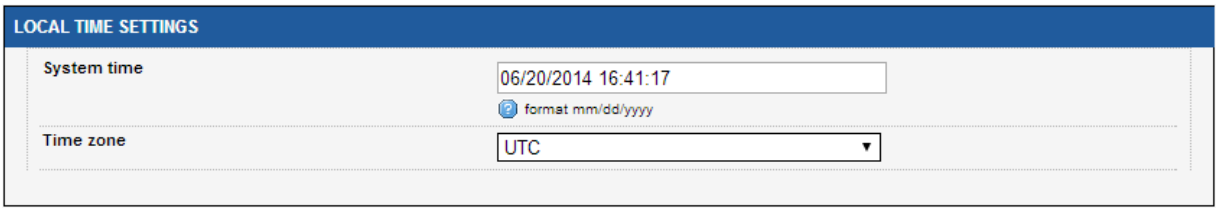
Location Name

With this panel, you can set the location name of the product. This text will be shown in the NDM 'Location' column.



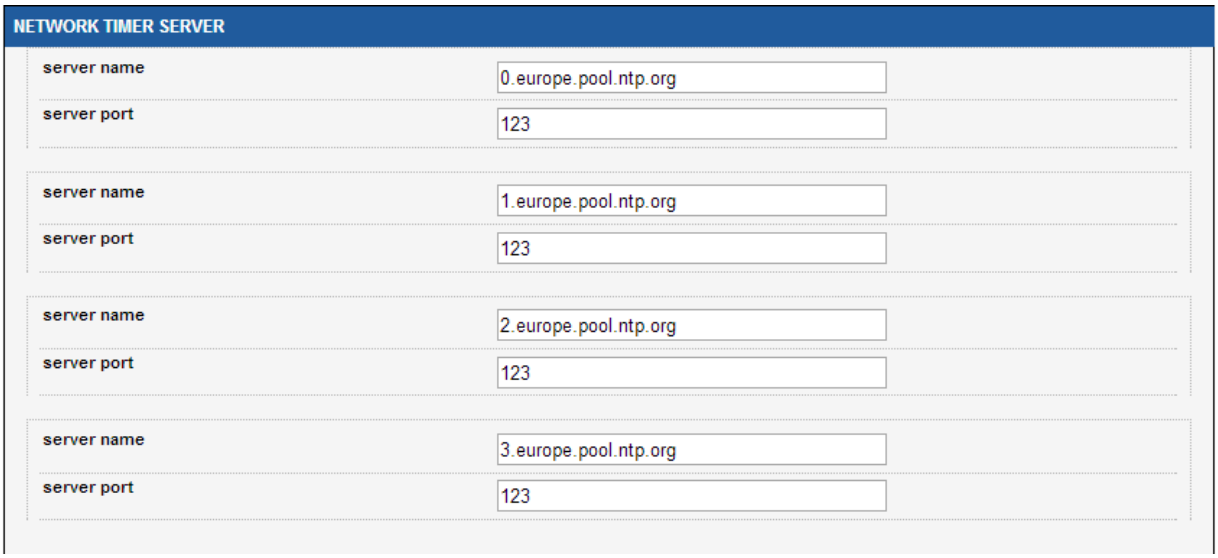
Log Settings
This frame allows you to set the product log parameters.

It is possible to send the LOG to an external log server (syslog).



Local Time Settings
This frame allows you 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.



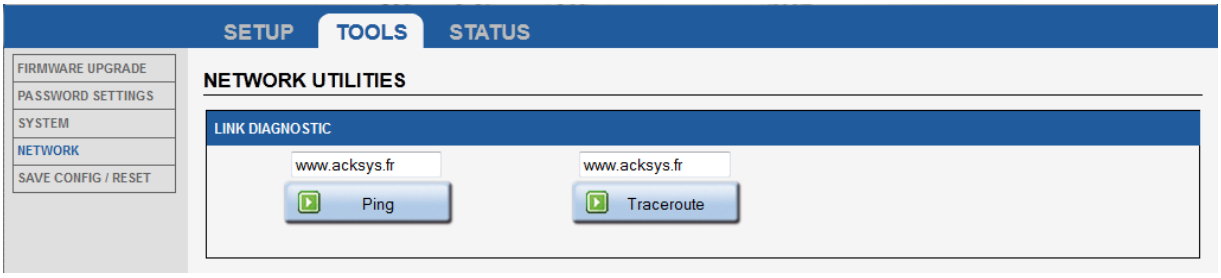
Network Timer Server

If a NTP server is reachable on the network, the product can use it to configure the local time.

The first server name/server port pair will be used and in case of non-responding server, it will fall back on the next pair.

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.

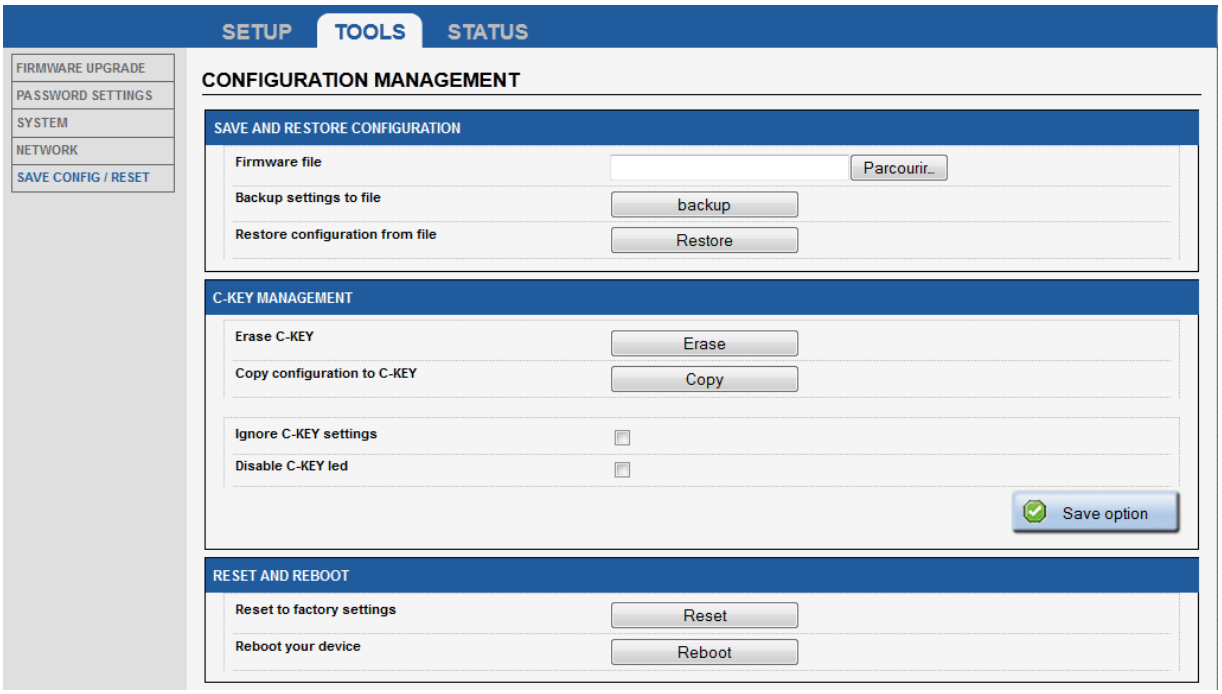
VI.2.4 Network



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.

VI.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 previous configuration is kept 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.

"**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:

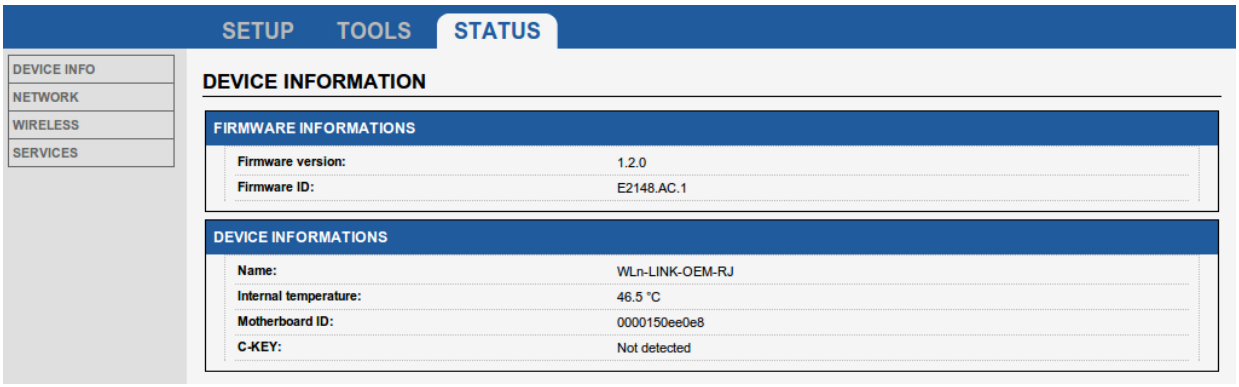
"**Reset to factory settings**":
This option will restore the default product settings.

"**Reboot your device**":
As its name suggests, a click on this button will reboot the device.

VI.3 Status Menu

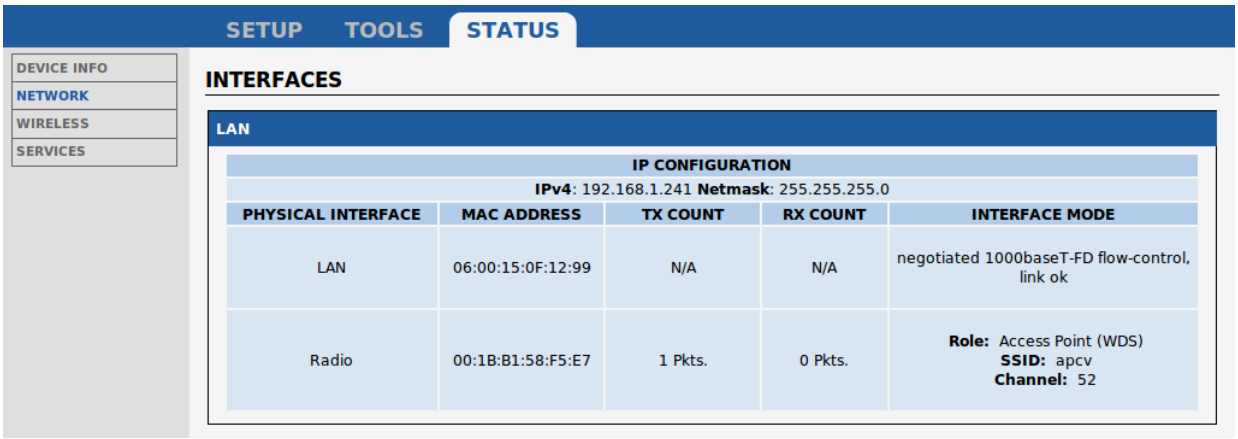
VI.3.1 Device Info

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.



VI.3.2 Network

This page summarizes the network interfaces configuration and display Tx & Rx packets counters.



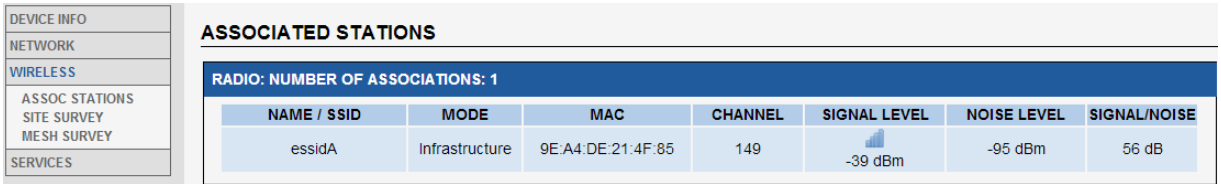
VI.3.3 Wireless

VI.3.3.1 Associated Stations (in access point mode)

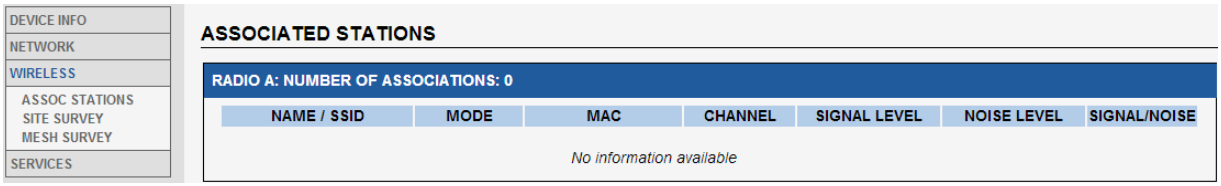
This panel lists the clients connected to this access point and displays RF signal properties.

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.



One associated station



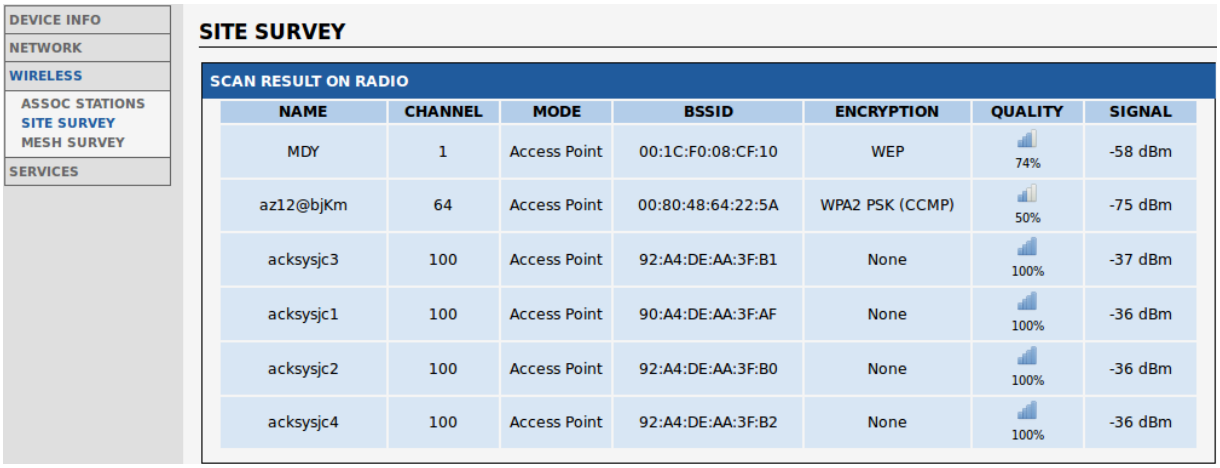
No associated station

VI.3.3.2 Site Survey

This panel summarizes all the access point available.

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.

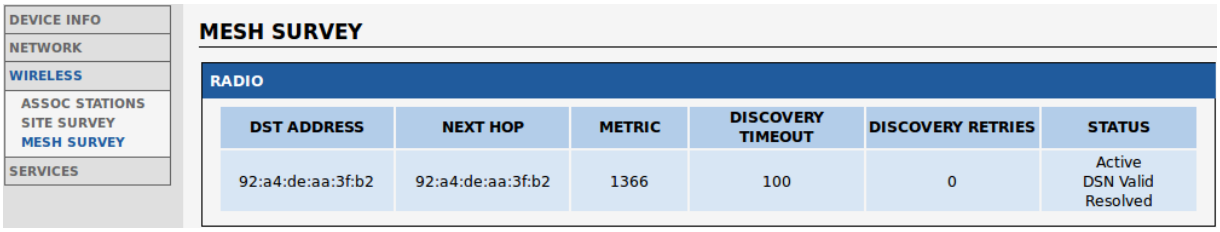


NAME	CHANNEL	MODE	BSSID	ENCRYPTION	QUALITY	SIGNAL
MDY	1	Access Point	00:1C:F0:08:CF:10	WEP	74%	-58 dBm
az12@bjKm	64	Access Point	00:80:48:64:22:5A	WPA2 PSK (CCMP)	50%	-75 dBm
acksysjc3	100	Access Point	92:A4:DE:AA:3F:B1	None	100%	-37 dBm
acksysjc1	100	Access Point	90:A4:DE:AA:3F:AF	None	100%	-36 dBm
acksysjc2	100	Access Point	92:A4:DE:AA:3F:B0	None	100%	-36 dBm
acksysjc4	100	Access Point	92:A4:DE:AA:3F:B2	None	100%	-36 dBm

NOTE: The signal level 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.

VI.3.3.3 MESH Survey

This panel summarizes properties for all 802.11s Mesh Points currently available.



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:

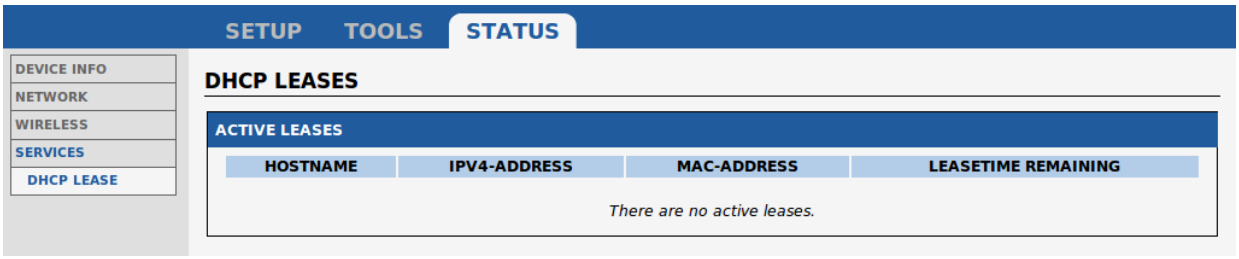
Displays the mesh path current state.
Must be one of the following:

- 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

VI.3.4 Services

VI.3.4.1 DHCP Lease

This panel summarizes the properties of all the current DHCP leases.



VI.3.5 LOG

This panel allows to visualize the product logs.
You can see the Kernel logs (logs from linux kernel) and system logs (logs from running daemons).

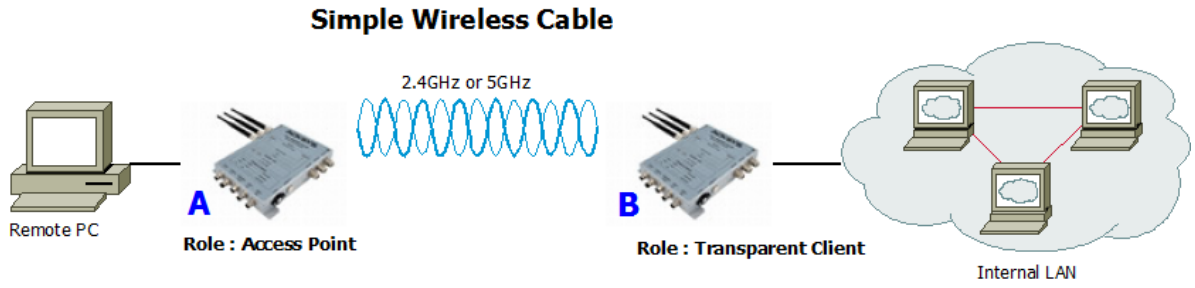
VII WIRELESS TOPOLOGIES EXAMPLES

The WLn series are 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.

VII.1 Simple "Wireless cable"

In this mode, an access point and an infrastructure bridge pair just replaces an existing Ethernet cable.



Configuration summary:

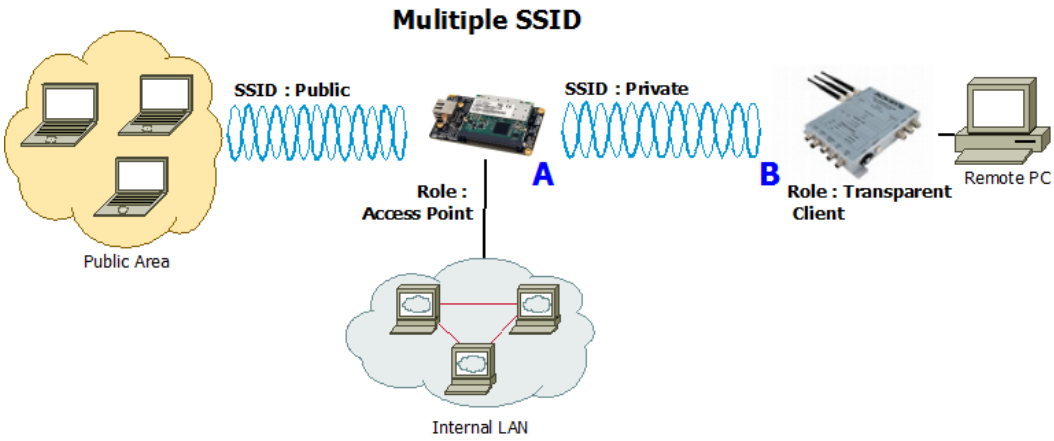
In this example, we are using 802.11a with 20MHz HT mode, channel 36, country code FR and ACKSYS as ESSID. You can obviously change any of these parameters as long as your choice makes sense.

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	any
Interface Configuration 1	
Parameter	***Value***
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A

VII.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.

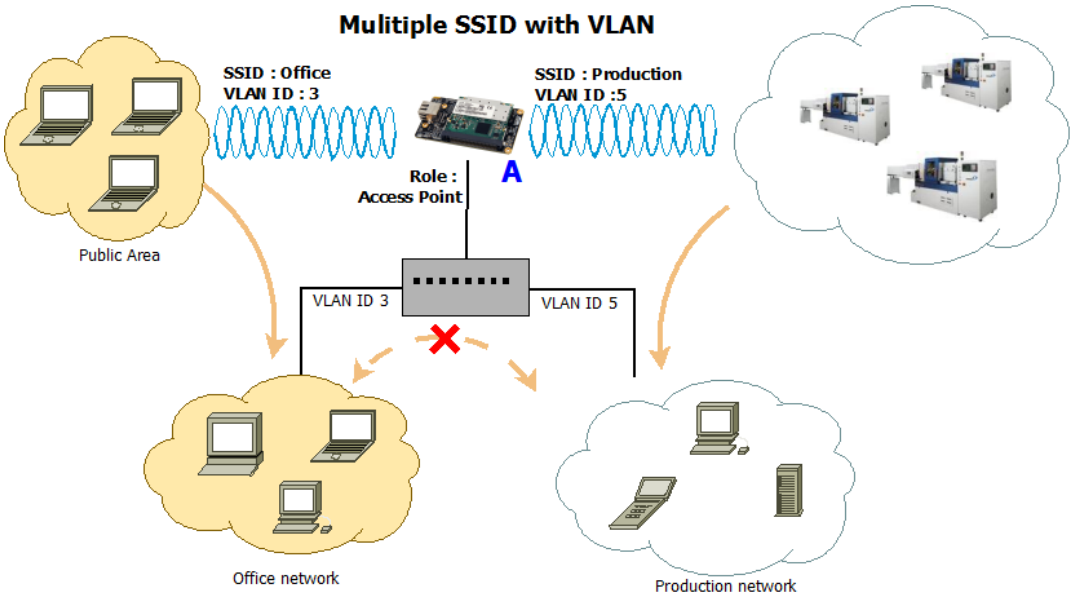
Product A	
Device Configuration	
Parameter	***Value***
Enable device	on
802.11 mode	802.11na
HT mode	40 MHz above
Channel	36
Country code	FR
Interface Configuration 1 (Public)	
Parameter	***Value***
Role	Access point
ESSID	SYSKCA
Interface Configuration 2 (Private)	
Parameter	***Value***
Role	Access 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	any
Interface Configuration 1	
Parameter	***Value***
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A private ESSID

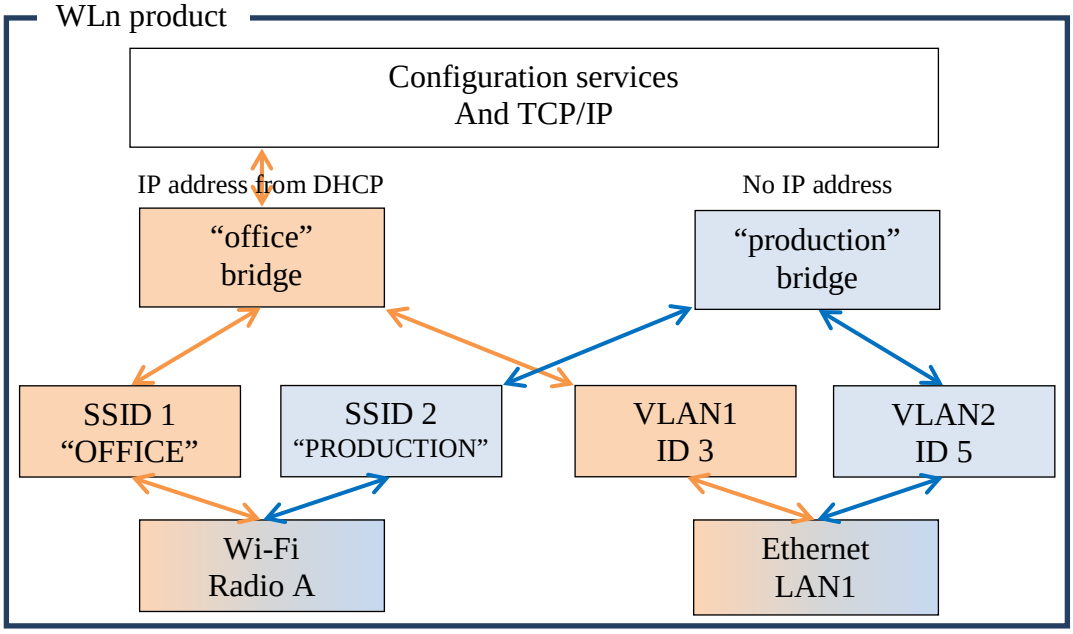
VII.3 Multiple SSID with VLAN

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 traffics share the same LAN interface. You can isolate SSID traffics 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.



In order to support this setting, the internal architecture of product “A” is as follows:



Internal architecture for SSID/VLAN association

Configuration summary:

Product A	
Device Configuration	
Parameter	***Value***
Enable device	on
802.11 mode	802.11na
HT mode	40 MHz above
Channel	36
Country code	FR
Interface Configuration 1 (Office)	
Parameter	***Value***
Role	Access point
ESSID	OFFICE
Interface Configuration 2 (Production)	
Parameter	***Value***
Role	Access point
ESSID	PRODUCTION

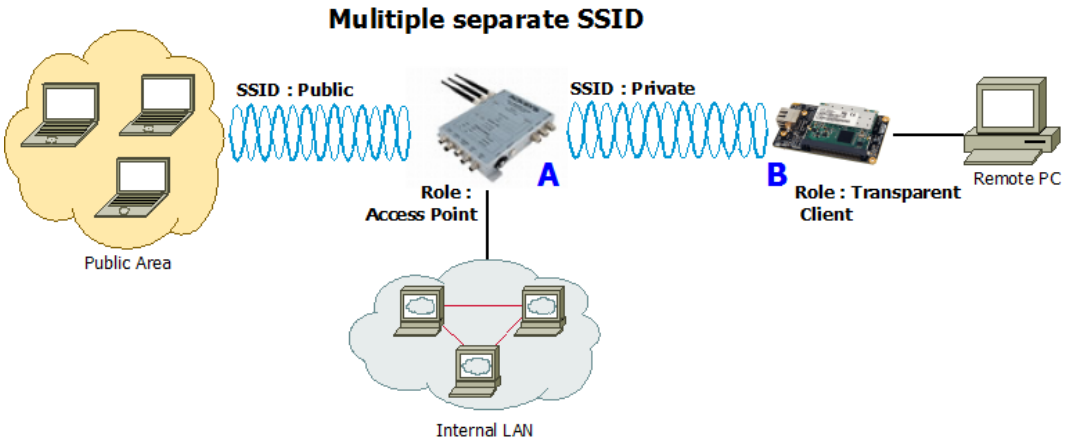
Virtual interface (VLAN 3)	
Parameter	***Value***
VLAN ID	3
Interface	LAN
Virtual interface (VLAN 5)	
VLAN ID	5
Interface	LAN
Network (office)	
Protocol	DHCP
Bridge interfaces	Checked
Interfaces	LAN.3 and “office” Wi-Fi adapter
Network (Production)	
Protocol	None
Bridge interface	Checked
Interfaces	LAN.5 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.

VII.4 Multiple separate SSID

In this mode, a single WLn-ABOARD 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.

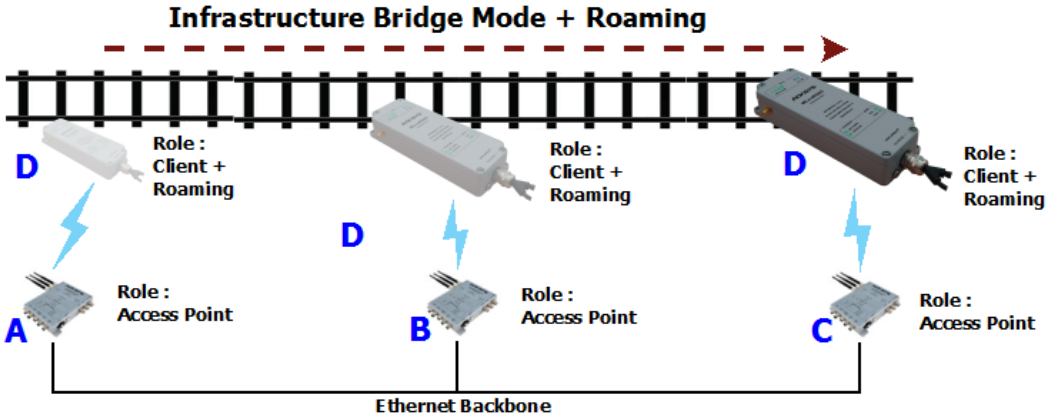
For Radio B (Private side):
Mode: 802.11na, HT mode: 40MHz above, channel: 44, country code: FR, ESSID: SYSKCA. You can obviously change any of these parameters as long as your choice makes sense.

Product A	
Device Configuration 1 (Radio A)	
Parameter	***Value***
Enable device	on
802.11 mode	802.11na
HT mode	40 MHz 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	40 MHz 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	40 MHz above
Channel	44
Country code	FR
Interface Configuration 1	
Parameter	***Value***
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A private ESSID

VII.5 Infrastructure bridge + Roaming

In this mode an infrastructure bridge can switch from an access point to another without breaking connectivity.



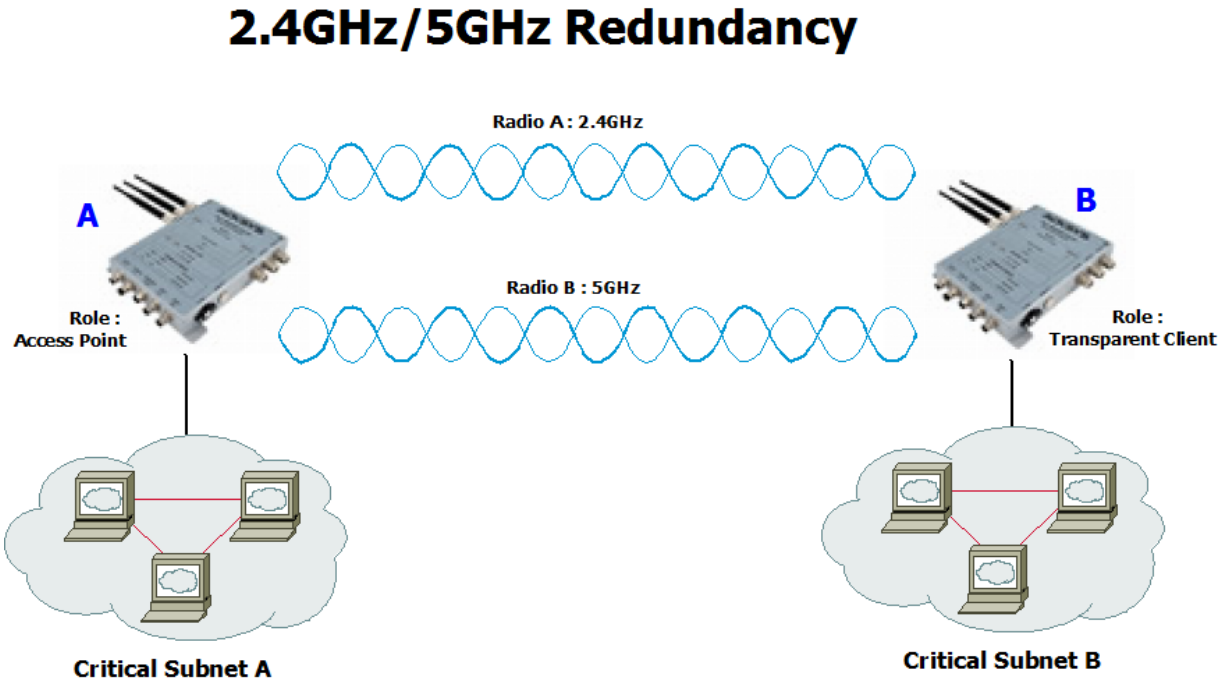
Configuration summary:
In this example, we are using the same parameters than previously with a roaming threshold set to -60dBm and a 5s scan cycle period.

Products 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	
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	any
Interface Configuration 1	
Parameter	***Value***
Role	Client
ESSID	same as product A
Roaming	
Parameter	***Value***
Enable proactive roaming	on
Channel	same as product A
Current AP minimum level	-60
Delay between 2 successive scan cycle	5000

VII.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.



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.

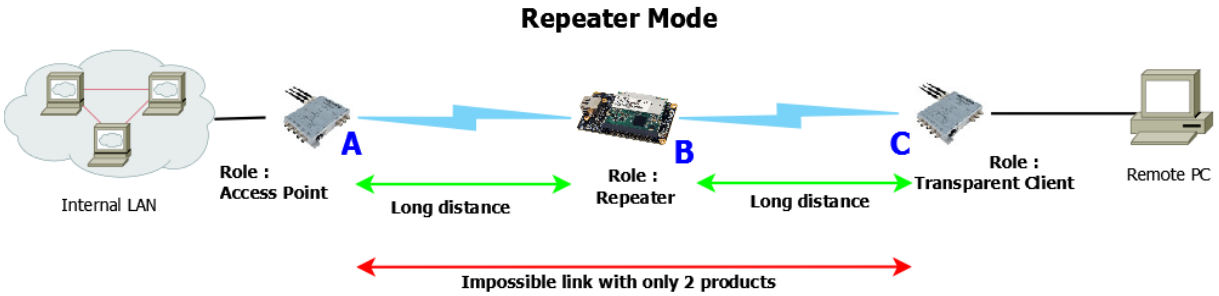
ATTENTION: This topology creates a network loop. You must provide a way to cut one of the two Wi-Fi links. This is usually done by using STP or RSTP inside the products. The WLn series provides STP since firmware 1.4.0 (RSTP is coming soon). STP must be activated in both Product A and Product B. See section "Spanning Tree Protocol (STP)" 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	any
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	any
Interface Configuration 1 (Radio B)	
Parameter	***Value***
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A

VII.7 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 must be seen as one access point and one bridge infrastructure in the same radio card. In the example above, Product **B** acts as a bridge with 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 as a transparent (4-addresses) client. This is the best way to achieve transparent communication. Other modes (like ARPNAT) would also work, but with caveats; see section V.6 – Wired to wireless bridging in infrastructure mode for more information.

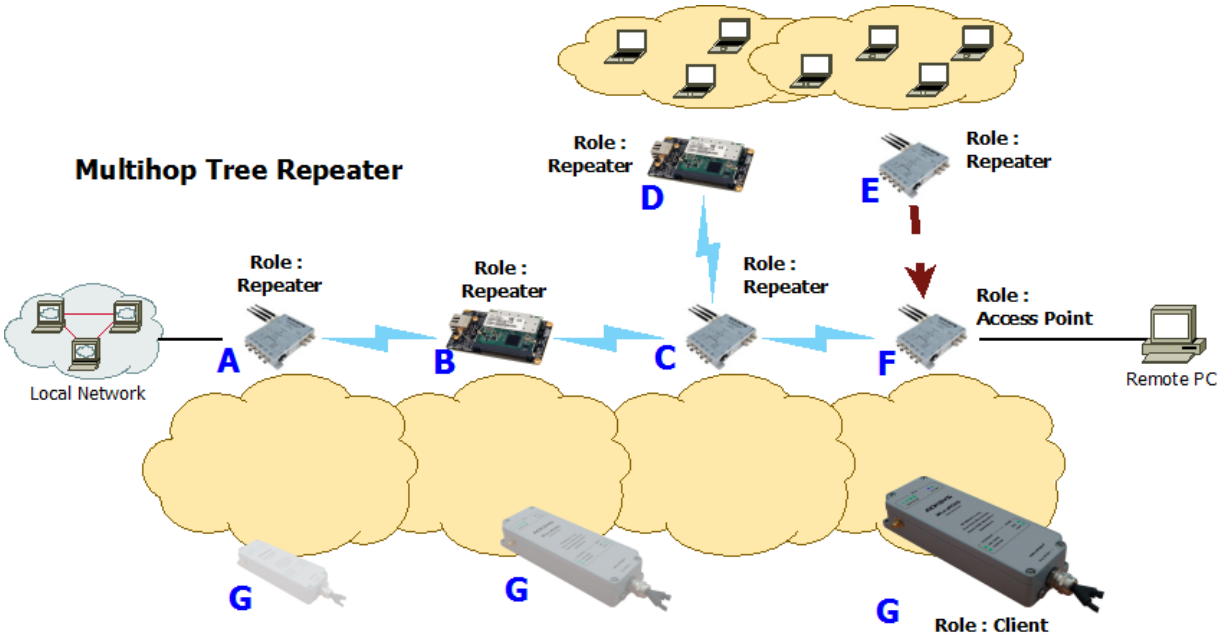
Product A	
Device Configuration (Radio A)	
Value	***Parameter***
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration 1(Radio A)	
Value	***Parameter***
Role	Access point
ESSID	ACKSYS

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	any
Interface Configuration 1 (Radio A)	
Parameter	***Value***
Role	Repeater
ESSID	same as product A
Next BSSID	Product A radio card MAC address

Product C	
Device Configuration (Radio A)	
Value	***Parameter***
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

VII.8 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.

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	Repeater
ESSID	ACKSYS
Next BSSID	Product B radio card MAC address

Product B	
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	Repeater
ESSID	same as product A
Next BSSID	Product C radio card MAC address

Product C	
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	Repeater
ESSID	same as product A
Next BSSID	Product F radio card MAC address

Product D	
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	Repeater
ESSID	same as product A
Next BSSID	Product C radio card MAC address

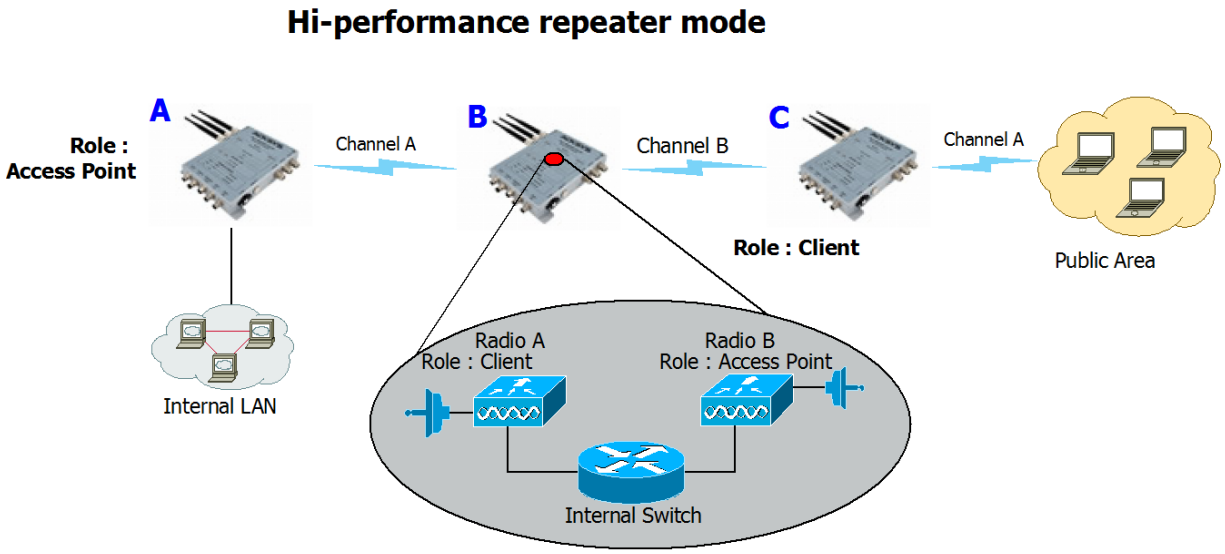
Product E	
Device Configuration	
Parameter	***Value***
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration	
Parameter	***Value***
Role	Repeater
ESSID	same as product A
Next BSSID	Product F radio card MAC address

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

Product 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	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A
Roaming	
Parameter	***Value***
Enable proactive roaming	on
Channel	same as product A
Current AP minimum level	-60
Delay between 2 successive scan cycle	5000

VII.9 High performance repeater

This mode takes advantage of the dual radio card device to implement a high-performance repeater.



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: ACKSYS1. 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.

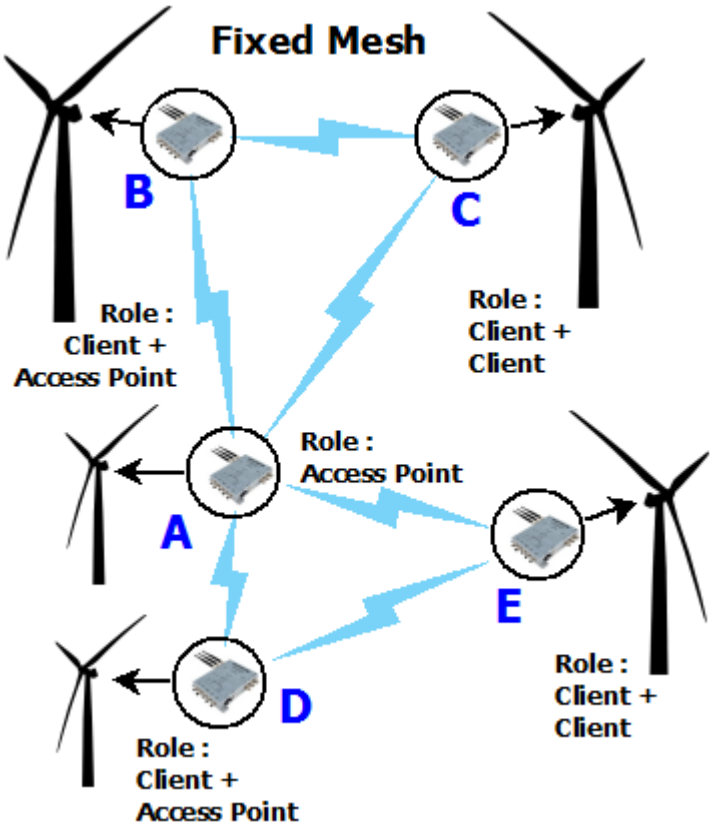
Product A	
Device Configuration (Radio A)	
Parameter	***Value***
Enable device	on
802.11 mode	802.11na
HT mode	40MHz above
Channel	36
Country code	FR
Interface Configuration 1(Radio A)	
Parameter	***Value***
Role	Access point
ESSID	ACKSYS1

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 1(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 1(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 1(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 1(Radio B)	
Parameter	***Value***
Role	Access point
ESSID	ACKSYS1

VII.10 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. The WLn series provides STP since firmware 1.4.0 (RSTP is coming soon). STP need to activated in each product. See section "Spanning Tree Protocol (STP)" for more details.

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 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	any
Interface Configuration (Radio A)	
Parameter	***Value***
Role	Client
Bridging mode	4 address format
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

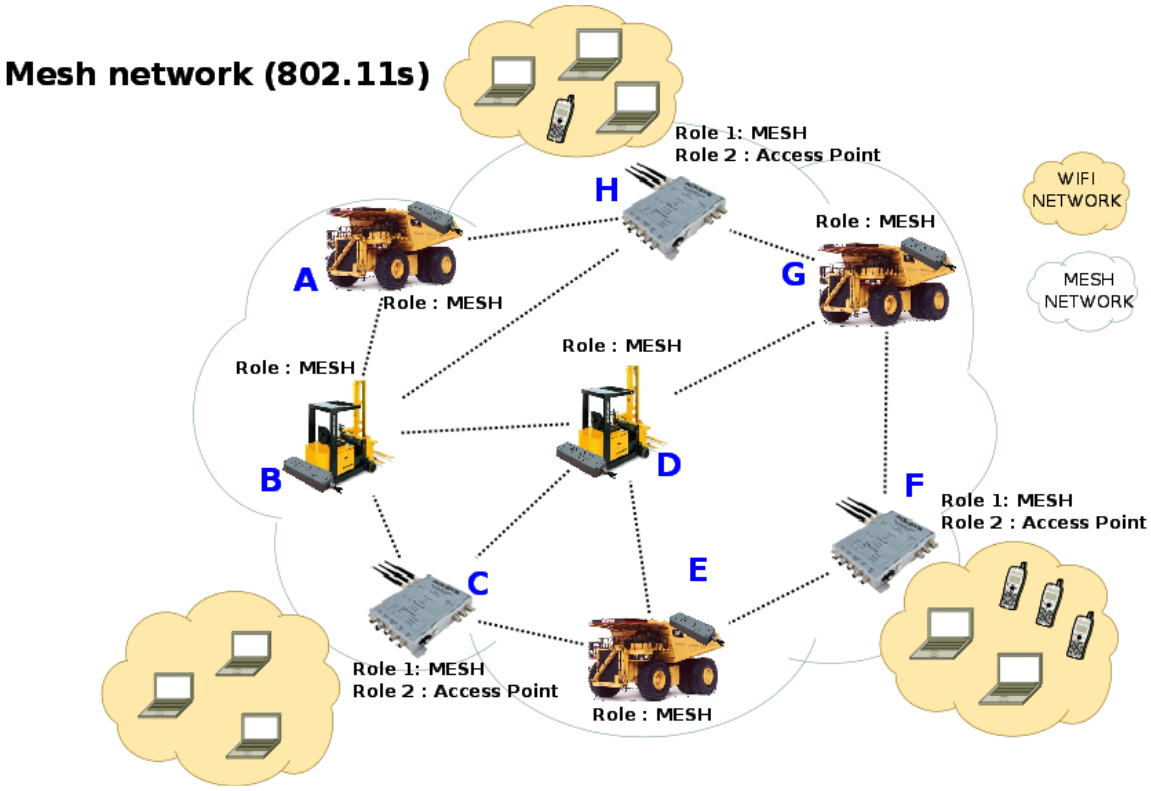
Product C	
Device Configuration (Radio A)	
Parameter	***Value***
Enable device	on
802.11 mode	Same as product A
HT mode	Same as product A
Channel	Same as product A
Country code	any
Interface Configuration (Radio A)	
Parameter	***Value***
Role	Client
Bridging mode	4 address format
ESSID	ACKSYS
Device 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	any
Interface Configuration (Radio B)	
Parameter	***Value***
Role	Client
Bridging mode	4 address format
ESSID	Same as product B (Radio B)

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	any
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	any
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 D (Radio B)
HT mode	Same as product D (Radio B)
Channel	Same as product D (Radio B)
Country code	any
Interface Configuration (Radio B)	
Parameter	***Value***
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	Same as product D (Radio B)

VII.11 802.11s Mesh

This topology uses the IEEE 802.11s standard. There is an overview of 802.11s in the section V.2.3: 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.

ATTENTION: 802.11s does not allow any security scheme for the Wi-Fi connection for the moment. We recommend the use of secured tunnels like VPNs to provide data confidentiality.

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 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	any
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 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	any
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

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	any
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

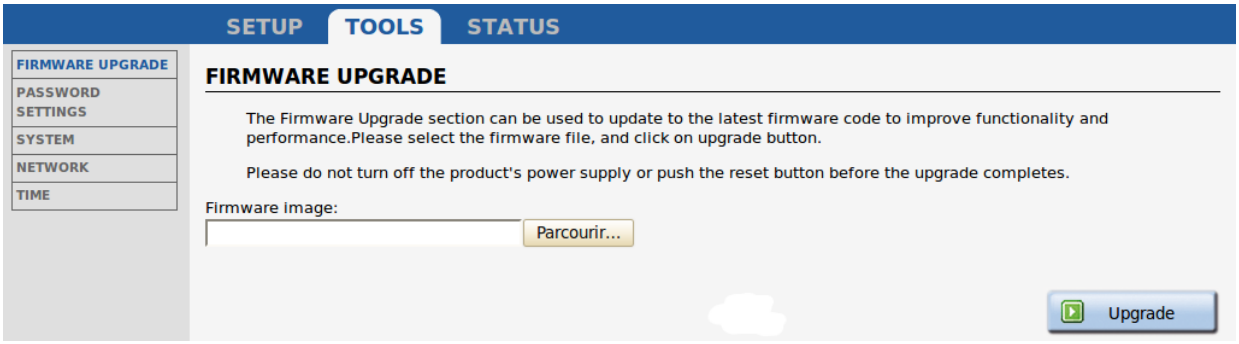
HT mode	20MHz
Channel	44
Country code	FR
Interface Configuration (Radio B)	
Parameter	***Value***
Role	Access Point
ESSID	ACKSYS2

HT mode	20MHz
Channel	48
Country code	FR
Interface Configuration (Radio B)	
Parameter	***Value***
Role	Access Point
ESSID	ACKSYS3

VIII FIRMWARE UPGRADE

VIII.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.

VIII.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

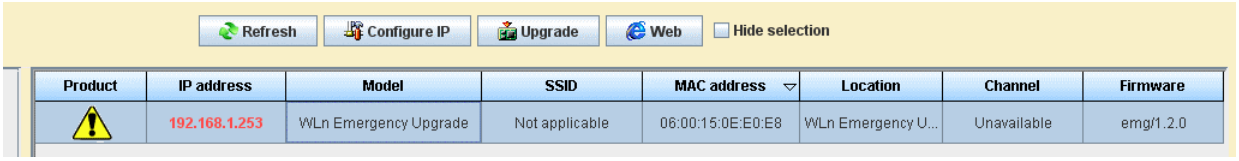
The bootloader upgrade package is available on our web site (www.acksys.fr) and may be applied using the TOOLS/FIRMWARE UPGRADE page in the internal web interface. The procedure uses the same upgrade process than the regular firmware upgrade :

- click the “Browse” button in order to select the upgrade file
- click the “Execute” button in order to perform the upgrade

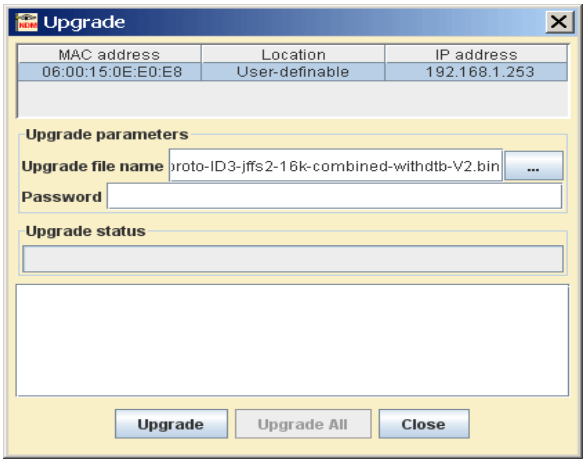
VIII.3 Emergency upgrade

Continually pressing the “reset” button during product start-up will enter a special failover mode called “Emergency upgrade”. The product will then execute a restricted service allowing only firmware uploads from the ACKSYS NDM software. You can recognize that the product is in this

failover mode because its DIAG LED will blink quickly. Remind that this LED is off in normal working mode.



Select in the list the products you wish to upgrade and click the “Upgrade” button.



Select the file to upload then click on “Upgrade”. If you wish to upgrade several products at once select them in the list and click “Upgrade All”.

All previous configuration changes will be left unchanged.

While the product is in “Emergency upgrade” mode it still allows to restore factory settings by pressing the reset button more than two seconds.

VIII.4 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.

IX 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.

IX.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.

IX.2 Check Network configuration

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 transparent client mode (since the 4-addresses format is not compatible with some AP providers).

X FREQUENTLY ASKED QUESTIONS

This section answers to various aspects of the WLn products operation.

X.1 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/

X.2 How many clients are handled by the access point function?

There can be as many as 2000 clients per AP, however, performance drops when more than 124 clients are connected to the same radio card using encryption.

X.3 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 WLn 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.

X.4 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.6.2.1 – “Masquerading (ARPNAT)”.

X.5 Fast roaming features

The figures indicated below are accurate for the firmware version 2.2.0 and will be updated as needed in future releases of this document.

X.5.1 What is the scan period when proactive roaming is enabled?

When the WLn 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 56ms + 0ms + 56ms + 200ms + 56ms + 200ms + 56ms + 3000ms = 3464ms. The radio cannot communicate while it is off-channel, in this case this is (3x56)/3464 = 4,8% of the time. The throughput decreases accordingly.

This figure is only an approximation and may vary under very heavy loads.

X.5.2 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 WLn 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 APPENDIX – GLOSSARY AND ACRONYMS

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.
BSS	Basic Service Set, the network formed by one AP and its clients.
Bridge	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. 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, a Ethernet switch is a hardware bridge, and the WLn products include a software bridge between their various interfaces such as Ethernet, multiple WLAN clients or APs, mesh, and so on.
BSSID	BSS identifier, usually the MAC address of the AP or a derivation thereof.
LAN	Local Area Network, a part of a network where devices can directly use MAC (OSI layer 2) addresses to communicate with each other.
MCS	Modulation and Coding Scheme, the way the bits are encoded in radio waves in 802.11n.
OSI	Open Systems Interconnection, an ISO standard to organize networking systems into specialized layers.
Repeater	In the WLn products, 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.
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.
VLAN	Virtual LAN, a LAN tunneled in another LAN by adding a VLAN tag to each frame in the VLAN.
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.

XII APPENDIX – RADIO CHANNELS LIST

XII.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.

XII.2 802.11a/h (5 GHz)

These networks use the 5 GHz radio band UN-II (Unlicensed-National Information Infrastructure).

Channel	Central frequency (GHz)	Power	Allowed by
34	5,170		Japan TELEC
36	5,180	40 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
38	5,190		Japan TELEC
40	5,200	40 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
42	5,210		Japan TELEC
44	5,220	40 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
46	5,230		Japan TELEC
48	5,240	40 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
52	5,260	250 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
56	5,280	250 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
60	5,300	250 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
64	5,320	250 mW (FCC), 200 mW (ETSI)	Europe ETSI, US FCC
100	5,500	1 W	Europe ETSI
104	5,520	1 W	Europe ETSI
108	5,540	1 W	Europe ETSI
112	5,560	1 W	Europe ETSI
116	5,580	1 W	Europe ETSI
120	5,600	1 W	Europe ETSI
124	5,620	1 W	Europe ETSI
128	5,640	1 W	Europe ETSI
132	5,660	1 W	Europe ETSI
136	5,680	1 W	Europe ETSI
140	5,700	1 W	Europe ETSI
149	5,745	1 W	US FCC
153	5,765	1 W	US FCC
157	5,785	1 W	US FCC
161	5,805	1 W	US FCC
165	5,825	1 W	US FCC

Summary:

US and Canada (FCC): 13 channels

- [5.150 to 5.250 GHz] (Called U-NII I)
- [5.250 to 5.350 GHz] (Called U-NII II)
- [5.725 to 5,825] (Called U-NII III)

Europe (ETSI): 19 channels

- [5.150 to 5.350 GHz]
- [5.5 to 5,725]

Japan (TELEC): 4 channels

- [5.150 to 5,250]