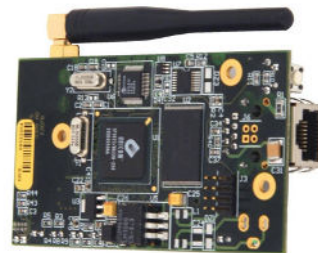


# 802.11A/B/G ACCESS POINTS/BRIDGES

## USER GUIDE





## TABLE OF CONTENTS

I	INTRODUCTION .....	5
II	DEVICE INSTALLATION ON THE NETWORK .....	7
III	NEW IP CONFIGURATION .....	7
IV	WEB ADMINISTRATION .....	9
IV.1	Web Configuration Structure .....	9
IV.2	Help .....	10
IV.3	LAN Settings .....	10
IV.4	Wireless Settings .....	12
IV.4.1	Bridge or Access Point mode .....	14
IV.4.1.1	Infrastructure mode .....	15
IV.4.1.2	Ad-hoc mode .....	16
IV.4.2	WDS mode .....	17
IV.4.2.1	WDS menu .....	18
IV.4.3	SSID .....	19
IV.4.3.1	Broadcasting the SSID .....	19
IV.4.4	802.11 mode .....	19
IV.4.5	Super G and Super AG .....	21
IV.4.6	Channels and international compatibility .....	21
IV.4.7	802.11b/g (2.4GHz) .....	22
IV.4.8	802.11a/h (5 GHz) .....	24
IV.5	Wireless security .....	25
IV.5.1	MAC ID filtering in access point mode .....	26
IV.5.1.1	MAC ADDRESS FILTER .....	26
IV.5.2	MAC ID Filtering in bridge infrastructure mode .....	29
IV.5.2.1	MAC ADDRESS FILTER .....	29
IV.5.3	WEP & WPA & WPA2 encryption .....	30
IV.5.3.1	WEP encryption .....	31
IV.5.3.2	WPA/WPA2 encryption .....	33
IV.5.3.2.1	Security in pre-shared key mode (PSK) .....	34
IV.5.3.2.2	EAP extensions under WPA- and WPA2- Enterprise .....	35
IV.5.3.3	802.1x menu in bridge mode .....	38
IV.6	Roaming mode .....	39
IV.7	NAT .....	43
IV.7.1	NAT menu .....	44
IV.8	Advanced Ethernet interface configuration .....	50
V	SNMP MONITORING AND MANAGEMENT .....	52
V.1	MIB (Management Information Bases) .....	53
V.2	SNMP community .....	53
V.3	SNMP trap .....	54
V.4	SNMP menu .....	54
V.5	SNMP filtering .....	55
V.6	Traps management .....	57
V.7	Enterprise MIB ACKSYS .....	59
VI	FACTORY DEFAULT SETTINGS .....	73
VII	DEVICE UPGRADE .....	74
VII.1	By the WEB interface .....	74
VII.2	By ACKSYS NDM .....	74
VII.3	Recovering a product after an upgrade problem .....	75



## I INTRODUCTION

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

- WLg-LINK
- WLg-LINK-OEM-RJ
- WLg-LINK-OEM-TTL
- WLg-LINK-OEM-EVAL
- WLg-ABOARD/N
- WLg-ABOARD/NP
- WLg-ACCESS-ATEX
- WLg-IDA/N
- WLg-SWITCH
- WLg-xROAD/N
- WLg-xROAD/NP

It covers product installation, online help (HELP menu of the WEB administration) and the quickstart guide included with your product.

This reference guide describes the latest version of the ACKSYS access point firmware. Please use the change log (can be downloaded from ACKSYS web site) to check which features are available for your firmware.

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 DEVICE INSTALLATION ON THE NETWORK

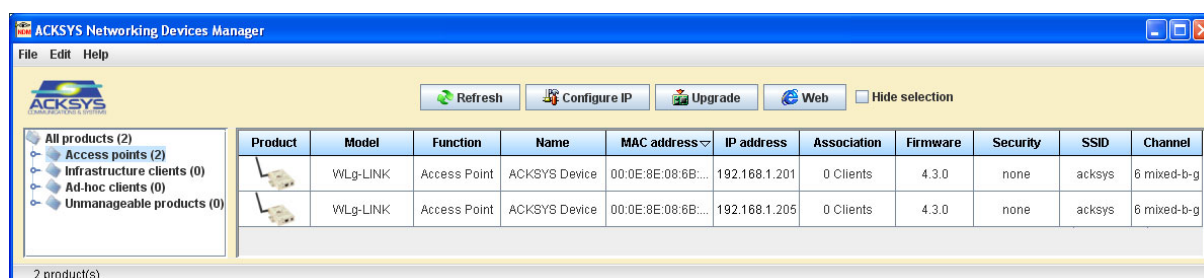
This first part is shown in the quick installation guide specific to each product. We invite you to read methodically the guide and follow all its recommendations.

## III NEW IP CONFIGURATION

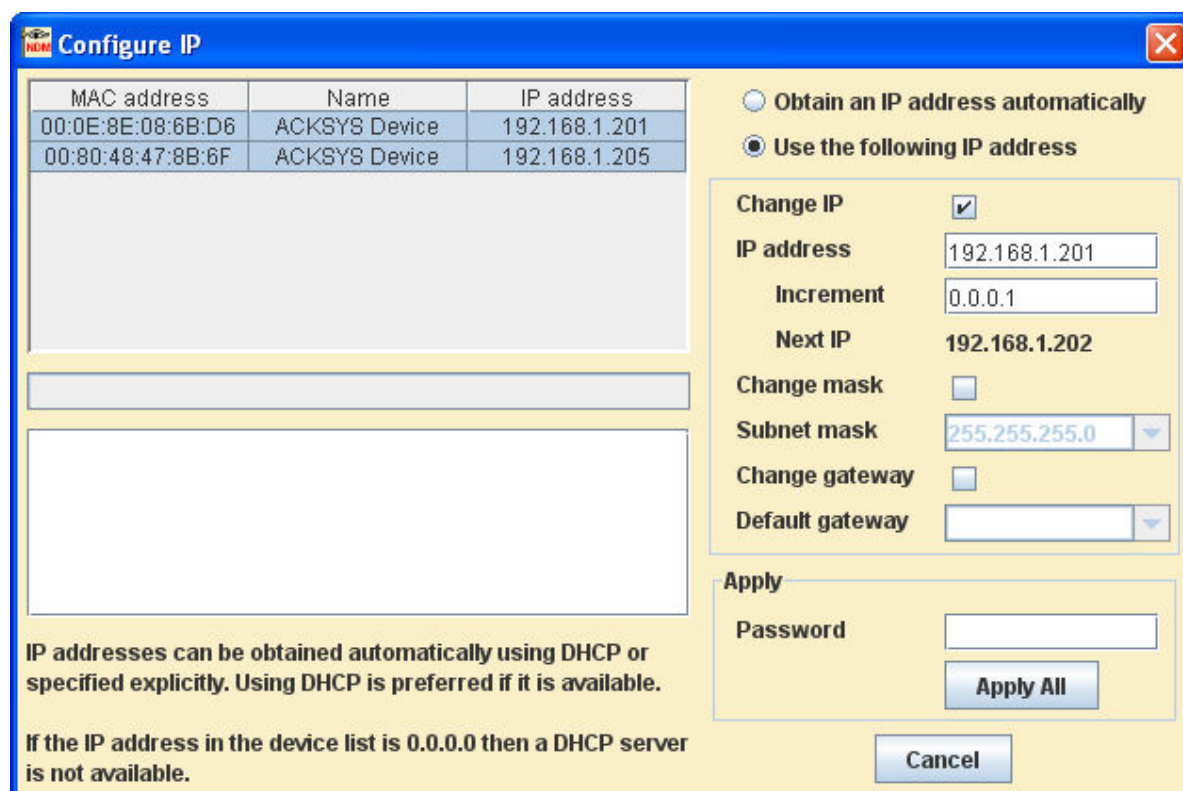
Once the device is attached to your network you will need to assign an IP address compatible with the network, unless the default IP address is already set (see paragraph « [Factory default settings](#) »).

In order to modify your device's IP address, you must use the ACKSYS NDM multi-platform application included in the CD-ROM included with the product.

From a P.C. on the network, run this application. The detected devices list will automatically appear.



The application detects all the ACKSYS products of the access point/bridge family on the local network. Select the product to configure and click on « Configure IP ».



If you only select one device before you click on « Configure IP », you must enter this device's IP parameters (IP address, subnet mask, default gateway). It can be done manually or automatically (the IP parameters will then be selected by the DHCP protocol). Then select « Apply ».

If you select several devices before you click on « Configure IP », a list of the selected devices to configure will appear in the configure IP window.

- If you wish to assign manually the IP parameters for each device (IP address, subnet mask, default gateway), select the product to configure, select your configuration and then click on « Apply ».
- If you wish to configure several products at the same time, select those products from the list, select your configuration and click on « Apply All ». All the selected products will be configured.

Once the devices have a suitable network IP address, you can use its embedded web server to configure them further.



## IV WEB ADMINISTRATION

Users can access and configure the device by selecting « web » or through a web browser interface. The device's login screen appears. The default username is « admin » and there is no password.



In order to proceed further you will need the following information :

- The wireless mode:
  - o Infrastructure
  - o Ad-hoc
- The wireless standard : 802.11a, 802.11b, 802.11g, 802.11b/g
- The wireless network SSID
- The wireless network channel
- The kind of wireless security to be used (WEP, WPA, WPA2, 802.1x, MAC ID filtering)
- The device's wireless mode
  - o **bridge infra** or **access point** for an infrastructure mode
  - o **bridge ad-hoc** for an ad-hoc mode

### IV.1 Web Configuration Structure

The web configuration user interface is structured thus :

- BASIC:
  - o WIZARD
  - o LAN: TCP/IP address settings.
  - o DHCP: embedded DHCP server settings (not available in bridge mode).
  - o WIRELESS: Wi-Fi settings.
  - o SNMP: SNMP agent settings.
- ADVANCED:
  - o MAC address filter: Settings for the MAC ID filter in access point mode.
  - o Advanced Wireless: Advanced wireless settings.
- TOOLS:
  - o ADMIN: Password settings for admin and users. You can also backup and restore all the settings in a file.
  - o TIME: Management of the time.

- SYSTEM: Restoration of the factory settings and to reboot the device.
- FIRMWARE: Shows the current firmware version or to upload new firmware.
- STATUS:
  - DEVICE INFO: Shows the device settings: IP address, wireless channel, SSID...
  - WIRELESS: Detected access points, connected wireless users.
  - LOGS: Shows device events.
  - STATISTICS: Displays received and transmitted packets passing through the device.
- HELP:
  - MENU: Describes all menus.
  - BASIC: Help for the basic menu.
  - ADVANCED: Help for the advanced menu.
  - TOOLS: Help for the tools menu.
  - STATUS: Help for the status menu.
  - GLOSSARY: Glossary of the technical terms used.

Search by selecting a menu or submenu title.

Some functions are specific to the ACCESS POINT or BRIDGE mode and will disappear depending on the selected mode. For example, the « BASIC→DHCP » and « ADVANCED→MAC ADDRESS FILTER » settings are not available in bridge mode.

## IV.2 Help

Provides an explanation on the overall settings of each menu and a detailed glossary.

## IV.3 LAN Settings

The LAN (Local Area Network) settings for the Access Point are **IP Address Mode**, **IP Address**, **Subnet Mask**, and **Default Gateway**. The device's local network (LAN) settings are configured using the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this Web-based management interface. This option is available in the "**BASIC→LAN**" page:

LAN SETTINGS	
IP Address Mode :	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IP Address :	<input type="text" value="192.168.1.253"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>
Gateway :	<input type="text" value="0.0.0.0"/>
Local Domain Name :	<input type="text"/> (optional)

***IP Address Mode***

Choose **DHCP (Dynamic)** 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.

Choose **Static IP (Manual)** 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 AP. In this case, you must also configure the fields shown above.

Note that you cannot choose **DHCP (Dynamic)** if you have enabled the **DHCP Server** option on the DHCP page; the AP cannot be both a DHCP client and a DHCP server.

***IP Address***

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.

***Subnet Mask***

The subnet mask of the local area network.

***Gateway***

The IP address of the router on the local area network. It is only used by the administration services (Web interface, SNMP...) if they must cross the gateway to communicate with the administration host.

***Local Domain Name***

This entry is optional. Enter a domain name for the local network. The AP's DHCP server will give this domain name to the computers on both wireless and wired LANs. So, for example, if you enter mynetwork.net here, and you have a wireless laptop called 'alan', that laptop will be known as alan.mynetwork.net. Note, however, that if the AP's settings specify a **DHCP (Dynamic)** address, and the router's DHCP server assigns a domain name to the AP, that domain name will override any name you enter here.

## IV.4 Wireless Settings

Wireless settings for your device may be configured here. Please note that any changes made in this section may also need to be duplicated on your Wireless Client. To protect your privacy, use the wireless security mode to configure the wireless security features.

This device supports three wireless security modes: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires a RADIUS authentication server.

### **Enable Wireless Radio**

This option enables the wireless connection feature of the Access Point. When you set this option, the following parameters are displayed;

**BASIC WIRELESS SETTINGS**

**Wifi Mode :** ☐ Bridge ☒ Access Point

**Enable WDS :** ☐

**Wireless Network Name :**  (Also called the SSID)

**Visibility Status :** ☒ Visible ☐ Invisible

**802.11 Mode :**  ▼

**Super G H™ Mode :**  ▼

**Region / Country :**  ▼

**Auto Channel Select :** ☒

**Channel :**  ▼

**Antenna :**  ▼

**Transmission Rate :**  ▼ (Mbit/s)

### **Wireless Network Name**

When you are browsing for available wireless networks, this name will appear in the list (unless Visibility Status is set to Invisible, as described below). This name is also referred to as the SSID. For security purposes we highly recommend changing the pre-configured network name.

### **Visibility Status**

The Invisible option allows you to not appear on your wireless network. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then other computers could connect to your network. When Invisible mode is enabled, you must manually enter the Wireless Network Name (SSID) on the client to connect to the network.

### **Auto Channel Select**

If you select this option, the Access Point automatically finds the channel with the least interference and uses that channel for wireless networking. If you disable this option, the Access Point uses the channel that you specify with the following **Channel** options.

**Channel**

A wireless network uses specific channels on the 2.4 GHz wireless spectrum to handle communication between clients. 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.

**Transmission Rate**

By default, the fastest possible transmission rate will be selected. If necessary, you may modify the speed.

**802.11 Mode**

If all of your devices can connect in 802.11g Mode, you can change the mode to "802.11g only". If you only have some devices that are 802.11b, leave the setting at Mixed.

**Super G™ Mode**

**Super G without Turbo:** Performance enhancing features such as Packet Bursting, FastFrames and Compression.

**WEP**

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, WEP is not as secure as WPA encryption. To gain access to a WEP network you must know the key.

#### IV.4.1 Bridge or Access Point mode

The device's default mode is « ACCESS POINT ». If you want to switch to bridge mode you need to select « BRIDGE ».

The device will then reboot. The next time you access the device's web server, you will see the bridge's mode banner instead of the access point's banner . Bridge mode's specific parameters can now be modified.

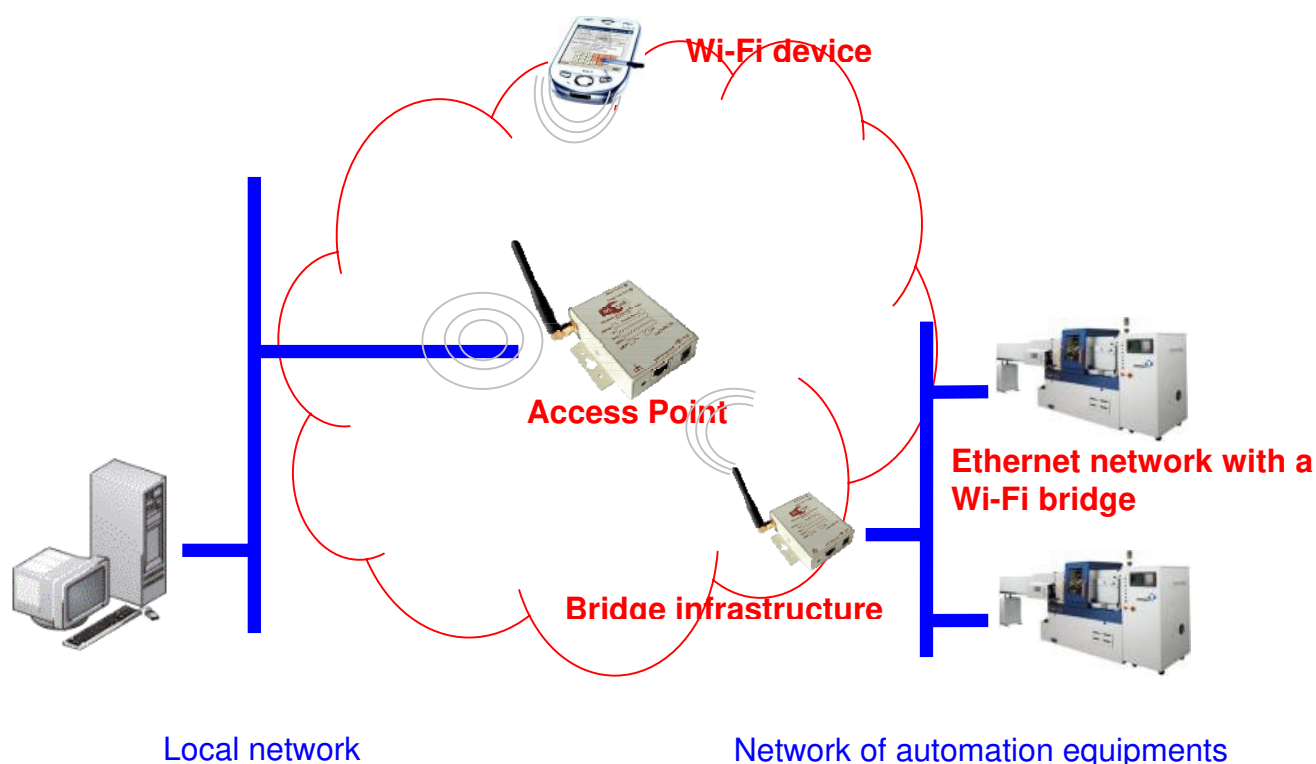
Once in bridge mode, the « Wireless Mode » parameters become available.

**Wireless Mode :** ☐ Infrastructure ☒ Ad-Hoc

#### IV.4.1.1 Infrastructure mode

In such a network there are 2 kinds of devices:

- The access point
- Client Wi-Fi devices that connect to the access point (the ACKSYS access point supports up to 20 clients). They can be Wi-Fi devices with embedded Wi-Fi or devices connected to a Wi-Fi bridge by an Ethernet cable.



The ACKSYS device can be :

- **Access point** (select **ACCESS POINT** mode).
- **Bridge** (select **BRIDGE** mode together with the **infrastructure** Wireless mode)

Infrastructure wireless mode networking connects a wireless network to a wired Ethernet network. Infrastructure wireless mode also supports central connection points for WLAN clients.

A wireless access point (AP) is required for infrastructure wireless mode networking. To join the WLAN, the AP and all wireless clients must be configured to use the same SSID. The AP is then cabled to the wired network to allow wireless clients access, for example, to Internet connections or printers. Additional APs can be added to the WLAN to increase the reach of the infrastructure and support any number of wireless clients.

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

#### IV.4.1.2 Ad-hoc mode

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

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

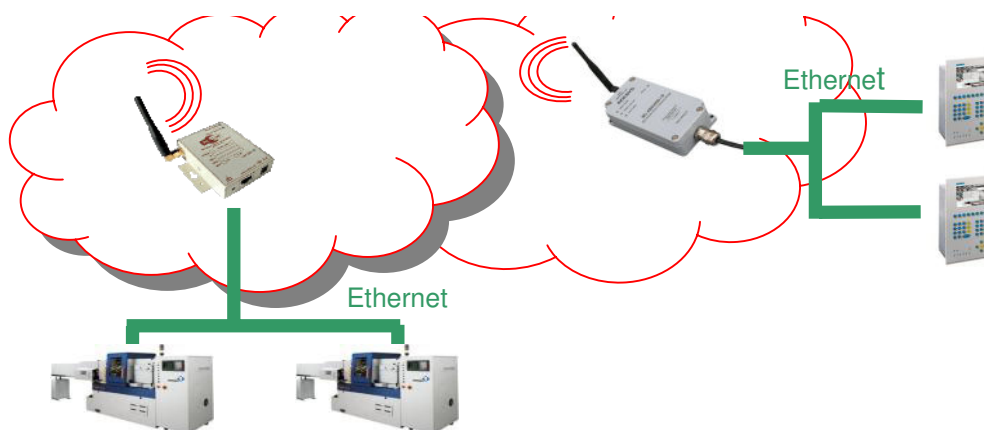


In addition, all wireless adapters on the ad-hoc network must use the same SSID and the same channel number.

An ad-hoc network tends to feature a small group of devices in very close environment. In order to communicate, all the cells of the devices **must overlay**.

Ad-hoc mode only works in 802.11b, with or without a WEP key (no WPA or WPA2)

All cells share the same wireless channel and the same SSID. They must overlay each other. There is no way to establish a route in order to link 2 remote products.





## IV.4.2 WDS mode

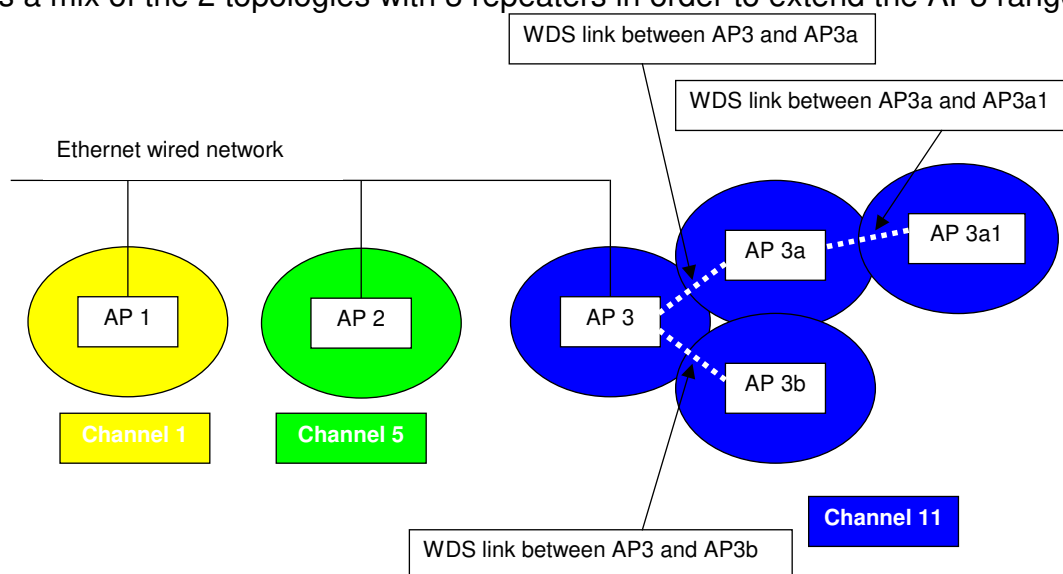
A WDS (Wireless Distribution System) is a system that enables the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them, as is traditionally required. The notable advantage of WDS over other solutions is that it preserves the MAC addresses of client packets across links between access points.

An access point can either be a main, relay or remote base station. A main base station is typically connected to the wired Ethernet. A relay base station communicates data between remote base stations, wireless clients or other relay stations to either a main or another relay base station. A remote base station accepts connections from wireless clients and passes them to relay or main stations. Connections between "clients" are made using MAC addresses rather than by specifying IP assignments.

All base stations in a Wireless Distribution System must be configured to use the same radio channel and share WEP keys if they are used. They can be configured to different service set identifiers.

WDS may also be referred to as repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging). It should be noted, however, that throughput in this method is inversely proportional to two raised to the power of the number of "hops", as all traffic uses the same channel. For example, client traffic going through one relay station before it reaches the main access point will see at most half the maximum throughput that a directly connected AP would experience and a client two hops from the directly connected AP will see at most one quarter of the maximum throughput seen at the directly connected AP.

Here is a mix of the 2 topologies with 3 repeaters in order to extend the AP3 range



The picture shows 3 WDS links, of which only two links are with the AP3.  
 The AP3 must know the AP3a and the AP3b MAC addresses and vice versa.  
 The AP3a must know the AP3a1 MAC address and vice versa.

Note: there must be no link between AP3a and AP3b because it would create a loop on the network. The product default settings include a STP (Spanning Tree Protocol) implementation which avoid the creation of faulty links.

ACKSYS access point can memorize up to 6 different MAC IDs.

#### IV.4.2.1 WDS menu

**BASIC WIRELESS SETTINGS**

Wifi Mode : ☐ Bridge ☒ Access Point

**Enable WDS :** ☒

Wireless Network Name :  (Also called the SSID)

Visibility Status : ☒ Visible ☐ Invisible

802.11 Mode :

Super AG™ Mode :

Region / Country :

Auto Channel Select : ☒

Channel :

Antenna :

Transmission Rate :  (Mbit/s)

The above picture shows the “Enable WDS” checkbox which enables the WDS feature. Should you select this option, the following menu appears :

**WDS SETTING**

Disable STP : ☐

WDS AP MAC Address : 1:   
 2:   
 3:   
 4:   
 5:   
 6:

(Leave blank to disable WDS for that slot)

**“Disable STP”** : if selected, the STP protocol is disabled.

Note : When this option is used, you must manage the links between your access points in order to avoid loops on the network.

**“WDS AP MAC Address”** : The next six parameters define which access points will be able to establish a WDS link with the current access point. Fill in the fields with the MAC address of the desired access points.

For the AP3, the AP3a and the AP3b MAC addresses will have to be entered.

### IV.4.3 SSID

A service set identifier, or SSID, is a name used to identify the specific 802.11 wireless LANs to which a user wishes to be connected. 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.

#### IV.4.3.1 Broadcasting the SSID

By default the network name is sent, with the beacon frame, in order to allow wireless devices to join the network.

This option can be disabled by selecting the « invisible » button in visibility status. This will not protect your network. In this case, connection to the network can only be made by manually entering the correct SSID .

This should not be used to protect a wireless network against determined hackers. Other forms of authentication should be used; WPA being the most accepted. However it should still be turned on because it increases the difficulty of making unauthorized access to a wireless network. It is the first layer of a layered security setup.

### IV.4.4 802.11 mode

There are 3 kinds of wireless networks available:

#### ➤ 802.11b

Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)	Range (Outside)
2.4 GHz	4.5 Mbit/s	11 Mbit/s	~35 m	~150 m

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.

## ➤ 802.11g

Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)	Range (Outside)
2.4 GHz	26 Mbit/s	54 Mbit/s	~30 m	~75 m

This works in the 2.4 GHz band (like 802.11b) but operates at a maximum raw data rate of 54 Mbit/s, or about 19 Mbit/s mean throughput. 802.11g hardware is fully backward compatible with 802.11b hardware.

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.

## ➤ 802.11a

Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)	Range (Outside)
2.4 GHz	30Mbit/s	54 Mbit/s	~10 m	~50 m

The 802. operates in 5 GHz band with a maximum raw data rate of 54 Mbit/s, which yields realistic mean achievable throughput in the mid-20 Mbit/s.

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.

#### IV.4.5 Super G and Super AG

Super G is Atheros' owned frame-bursting, compression and channel bonding technology to improve IEEE 802.11g wireless LAN performance. The throughput transmission speed limit when using Super G is claimed to be up to 40Mbit/s-60Mbit/s at a 108Mbit/s signaling rate, which is achieved through the bonding of two 54Mbit/s 802.11g channels.

Super G products from different vendors are all interoperable in Super G mode.

Atheros has also used this technology to their 802.11a/g chipsets, marketing it as Super AG.

In order to use Super AG, all Wi-Fi devices must use Atheros or interoperable chipsets.

Super AG can be used :

- Without turbo
- With Dynamic turbo: the network automatically selects if a turbo should be enabled
- With Static turbo : the turbo is always enabled

The available rates with these options are : 108 Mbps, 96 Mbps, 72 Mbps, 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps and 6 Mbps.

#### IV.4.6 Channels and international compatibility

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

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

Available channels are modified when you select your country or region in the « region/country » menu.

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

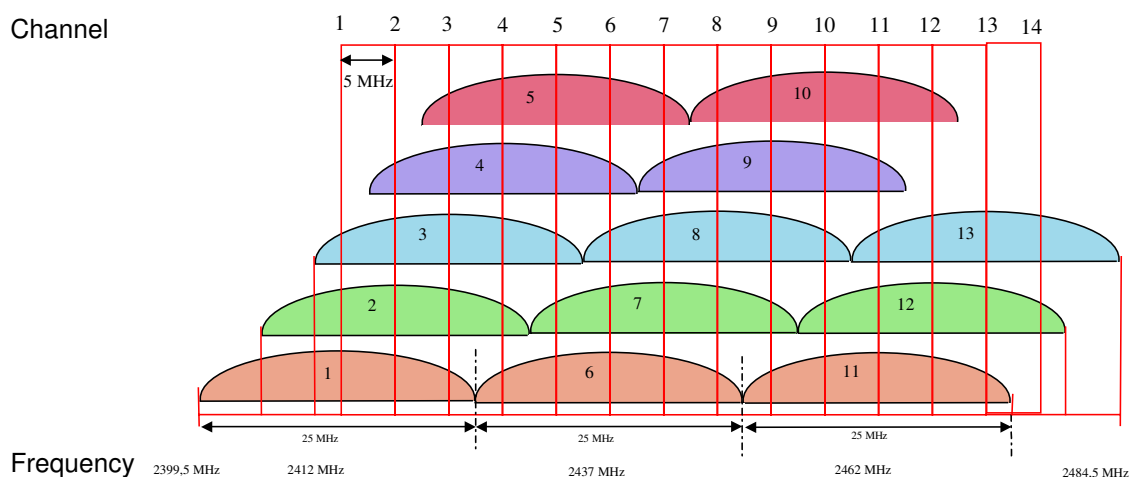
#### IV.4.7 802.11b/g (2.4GHz)

These networks use the ISM (Industrial Scientific and Medical) radio band on the [2.3995-2.4965] spectrum.

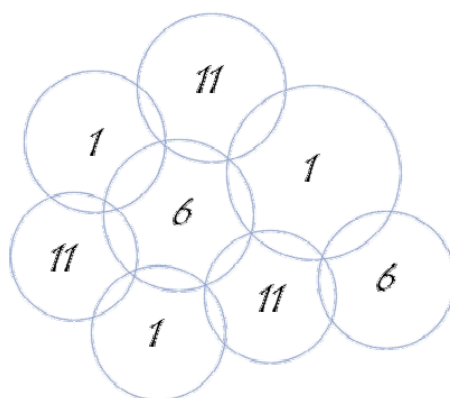
Channel (25 MHz)	Central frequency (GHz)	Allowed by
1	2,412	Asia MKK, Europe ETSI, US FCC
2	2,417	Asia MKK, Europe ETSI, US FCC
3	2,422	Asia MKK, Europe ETSI, US FCC
4	2,427	Asia MKK, Europe ETSI, US FCC
5	2,432	Asia MKK, Europe ETSI, US FCC
6	2,437	Asia MKK, Europe ETSI, US FCC
7	2,442	Asia MKK, Europe 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  $\pm 11$  MHz from the center frequency, the sense in which channels are effectively 22 MHz wide. One consequence is that stations can only use every fourth or 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  $\pm 22$  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.



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.



#### IV.4.8 802.11a/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]



## IV.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, see paragraph IV.4.3.1.
- MAC ID filtering
- WEP encryption
- WPA with 802.1x authentication or PSK
- WPA2 with 802.1x authentication or PSK

## IV.5.1 MAC ID filtering in access point mode

ACKSYS access points contain a MAC ID filter that allows the administrator to permit access only to computers having certain MAC IDs. This can be helpful, however it must be remembered that MAC IDs over a network can be faked.

The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adaptor(s). It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacturer of the network adaptor.

The ACKSYS access point uses the list of MAC addresses and works as follows :

- **“only allow listed machines”** : a configuration where the MAC addresses in the list are allowed. In this case, only clients on the list will be able to connect to the access point.
- **“only deny listed machines”** : a configuration where the MAC addresses in the list are denied. In this case, only clients not on the list will be able to connect to the access point.

### IV.5.1.1 MAC ADDRESS FILTER

This menu is only available in access point mode.

#### **Enable MAC Address Filter**

When this is enabled, computers are granted or denied network access depending on the mode of the filter.

**ADVANCED**  
MAC ADDRESS FILTER  
ADVANCED WIRELESS

**MAC ADDRESS FILTER**  

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.

Save Settings
Don't Save Settings

**ENABLE**  
Enable MAC Address Filter : ☒





**FILTER SETTINGS**  
Mode : 
Filter Wireless Clients : ☒
Filter Wired Clients : ☒

**ADD MAC ADDRESS**  
Enable : ☒
MAC Address : 
Computer Name : 

Copy Your PC's MAC Address

Save
Clear

**MAC ADDRESS LIST**  
Deny access to all except the machines in this list (subject to "Filter Settings"):  

Enable	MAC Address	Computer Name	
<input checked="" type="checkbox"/>	06:70:80:10:11:70	WLG-LINK	 
<input checked="" type="checkbox"/>	00:50:70:D7:03:11	myComputer	 

**NOTE** Incorrectly configuring this feature prevents machines from accessing the network. In this case, you can regain access by activating the factory defaults button on the Access Point itself.

## Mode

When "only allow listed machines" is selected, only computers with MAC addresses listed in the AC Address List are granted network access. When "only deny listed machines" is selected, any computer with a MAC address listed in the MAC Address List is refused access to the network.

## Filter Wireless Clients

When this option is selected, the MAC address filters will be applied to wireless network clients.

## Filter Wired Clients

When this option is selected, the MAC address filters will be applied to wired network clients.

## Add MAC Address

In this section, you can add entries to the MAC Address List below or edit existing entries.

## Enable

MAC address entries can be activated or deactivated.

**MAC Address**

Enter the MAC address of the desired computer or connect to the Access Point from the desired computer, and then select 'Copy Your PC's MAC Address'.

**Save**

Saves the new or edited MAC Address entries in the list. When you finish updating the MAC Address List, you must still select 'Save Settings' at the top of the page to activate the changes.

**MAC Address List**

The section lists the current MAC Address filters. A MAC Address entry can be changed by selecting 'Edit' or deleted by selecting 'Delete' . When you select 'Edit' , the item is highlighted, and the "Edit MAC Address" section is activated for editing.

## IV.5.2 MAC ID Filtering in bridge infrastructure mode

ACKSYS bridges contain a MAC ID filter that allows the administrator to refuse or authorize access points.

The ACKSYS access point uses a list of MAC address which works as follows :

- **“only allow listed machines”** : a configuration where the MAC addresses in the list are allowed. In this case, only the access points on the list will be able to connect to the bridge.
- **“only deny listed machines”** : a configuration where the MAC addresses in the list are denied. In this case, the access points that are not on the list will be able to connect to the bridge.

### IV.5.2.1 MAC ADDRESS FILTER

The MAC ADDRESS FILTER configuration is available in the “ADVANCED/MAC ADDRESS FILTER” menu.

**ADVANCED**  
ADVANCED WIRELESS  
ADVANCED ETHERNET  
MAC ADDRESS FILTER

#### MAC ADDRESS FILTER

The MAC (Media Access Controller) Address filter option is used to control network association based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This Feature can be configured to ALLOW or DENY association.

#### ENABLE

Enable MAC Address Filter : ☒

#### FILTER SETTINGS

Mode :

#### ADD MAC ADDRESS

Enable : ☒  
MAC Address :   
Computer Name :

#### MAC ADDRESS LIST

Allow association to all except the access point in this list (subject to "Filter Settings"):

Enable	MAC Address	Computer Name	
<input checked="" type="checkbox"/>	00:0e:8e:08:68:28	Computer1	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

### IV.5.3 WEP & WPA & WPA2 encryption

The encryption depends on the device mode :

In **Infrastructure mode** (access point or bridge) :

WIRELESS SECURITY MODE	
Security Mode :	<input checked="" type="radio"/> None <input type="radio"/> WEP <input type="radio"/> WPA/WPA2-PSK <input type="radio"/> WPA/WPA2

- None : no security
- WEP : WEP encryption
- WPA/WPA2-PSK : WPA or WPA2 encryption without 802.1x authentication
- WPA/WPA2 : WPA or WPA2 encryption with 802.1x authentication

In **Bridge Ad-Hoc** :

WIRELESS SECURITY MODE	
Security Mode :	<input checked="" type="radio"/> None <input type="radio"/> WEP <input type="radio"/> WPA/WPA2-PSK <input type="radio"/> WPA/WPA2

- None : no security
- WEP : WEP encryption

The security parameters described in this document are available in BASIC\WIRELESS menu.

### IV.5.3.1 WEP encryption

**WEP**

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the Access Point and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length: 64 bit (10 hex digits) ▼ (length applies to all keys)

WEP Key 1: ••••••••••

WEP Key 2: ••••••••••

WEP Key 3: ••••••~•••

WEP Key 4: ••••••~•••

Default WEP Key: WEP Key 1 ▼

Authentication: Open ▼

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, WEP is not as secure as WPA encryption. 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.

#### 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).



### IV.5.3.2 WPA/WPA2 encryption

**WPA**

WPA requires stations to use high grade encryption and authentication. NOTE: WDS will not function with WPA security.

**WPA Mode :** WPA ▼

**Cipher Type :** TKIP ▼

**Group Key Update Interval :** 3600 (seconds)

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 WEP's weaknesses, it adds user authentication which 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; select this option if clients that will be used with the Access Point only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the “WPA2” option, the Access Point tries WPA2 first, but falls back to WPA if the client only supports WPA. With the “WPA2 Only” option, the Access Point associates only with clients that also support WPA2 security.

The encryption algorithm used to secure the data communication is the cipher type. 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. With the “TKIP and AES” option, the Access Point negotiates the cipher type with the client, and uses AES when available.

You can choose from 4 security options:

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

In Access point mode, the interval for updating the group key used for broadcast and multicast data can be modified at all times by selecting ‘Group Key update interval’

#### IV.5.3.2.1 Security in pre-shared key mode (PSK)

Pre-shared key mode (PSK, also known as personal mode) is designed for home and small office networks that do not require the complexity of an 802.1x authentication server. Each user must enter a password to access the network. The password may be from 8 to 63 printable ASCII characters or 64 hexadecimal digits (256 bits). Most operating systems allow the password to be stored to avoid re-entry. The password must remain stored in the Wi-Fi access point.



PRE-SHARED KEY	
Pre-Shared Key :	••••••••

All Wi-Fi devices on your network must have the same Pre-Shared Key (PSK).

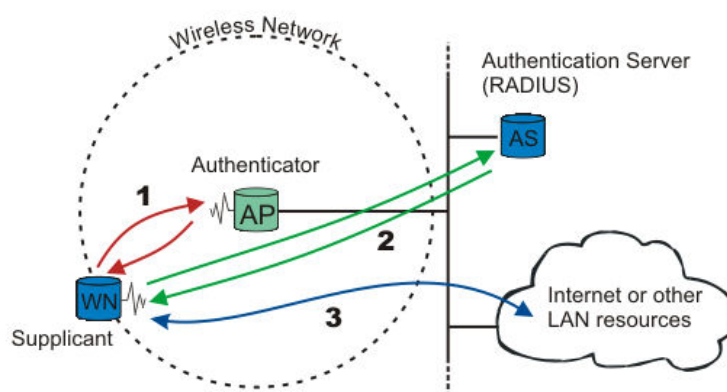
#### IV.5.3.2.2 EAP extensions under WPA- and WPA2- Enterprise

WPA/WPA2 (or WPA/WPA2-Enterprise) use 802.1x. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails.

When a new wireless node (WN) requests access to a LAN resource, the access point (AP) asks for the WN's identity. *No other traffic other than EAP is allowed before the WN is authenticated (the "port" is closed).*

The authentication process is organized around several agents:

- User, also call 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.



The first step is the physical association between the client and the access point (number 1 on the diagram).

Until authenticated the client cannot access the LAN. Only authenticated traffic is allowed and sent to the RADIUS server through the authenticator (number 2 on the diagram).

Once the client is authenticated, the traffic to the LAN is allowed (number 3 on the diagram).

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

#### IV.5.3.2.2.1 Authentication modus operandi

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

- EAP-MD5
- EAP-TLS
- EAP-TTLS
- EAP-PEAP

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 couple server/supplicant as well as the level of security needed.

For example, a Windows XP SP2 supplicant allows :

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

ACKSYS access points allow the 4 authentication methods. The next image shows the "EAP (802.1x)" menu when the product is configured in access point mode and working as AUTHENTICATOR.

In bridge (infrastructure) mode, ACKSYS products can use the MSCHAP Version 2 when the unit works as SUPPLICANT. Detailed description of the corresponding menu is available in chapter : IV.5.1.5

#### IV.5.3.2.2.2 EAP (802.1x) in access point mode

**The EAP (802.1x) menu is only available if WPA/WPA2 is selected.**

This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting authentication to the Server through this access point (the Gateway, from the 802.1x point of view). Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.

The  button allows a 2<sup>nd</sup> radius server configuration.

**EAP (802.1X)**

When WPA enterprise is enabled, the Access Point uses EAP (802.1x) to authenticate clients via a remote RADIUS server.


**Authentication Timeout :**  (minutes)

**RADIUS server IP Address :**

**RADIUS server Port :**

**RADIUS server Shared Secret :**

**MAC Address Authentication :** ☒



Optional backup RADIUS server:

**Second RADIUS server IP Address :**

**Second RADIUS server Port :**

**Second RADIUS server Shared Secret :**

**Second MAC Address Authentication :** ☒

**Authentication Timeout:** Amount of time before a client will be required to re-authenticate.

**RADIUS Server IP Address:** The IP address of the authentication server.

**RADIUS Server Port:** The port number used to connect to the authentication server.

**RADIUS Server Shared Secret:** A password that must match the authentication server's.

**MAC Address Authentication:** If selected, the user must connect from the same computer whenever logging into the wireless network.

### IV.5.3.3 802.1x menu in bridge mode

This option is only available with second version of the product. This feature requires some hardware improvements.

To access the “802.1x Configuration” menu, select the “WPA/WPA2” radio button in the “Wireless security” menu :

WIRELESS SECURITY MODE	
Security Mode :	<input type="radio"/> None <input type="radio"/> WEP <input type="radio"/> WPA/WPA2-PSK <input checked="" type="radio"/> WPA/WPA2

This menu can configure the SUPPLICANT bridge to allow authentication with a RADIUS server.

Note : Only one EAP method is available here : the EAP-PEAP with authentication by login and password (MS-CHAP V2) :

802.1X CONFIGURATION	
PEAP-MSCHAP V2 Authentication requires login and password.	
Username :	<input type="text"/>
Password :	<input type="password"/>

“**Username**” : this field contains a valid username registered on your radius server.

“**Password**” : this field contains the password associated with the above username.

## IV.6 Roaming mode

The roaming mode allows a wireless mobile client (the bridge infrastructure mode in the ACKSYS product) to switch from an access point to another without losing the network connection.

*If disabled*, the ACKSYS bridge will not connect to another access point until connection has been lost with the current Access Point. *The change will otherwise take place* when the current RSSI reaches a predefined threshold. Once this threshold is reached, the bridge must have already found another access point with a better RSSI than the current one. In this case, the bridge will disconnect from the current access point and immediately connect with the new one.

The **roaming time** (the time necessary for the bridge to switch from one access point to another that is already available) is between [10-300ms].

When the roaming mode is enabled, the bridge has to scan radio channels to set up a valid access point list in case the current connection decreases under the RSSI threshold.

Since the radio channel scan disrupts the current connection (the current connection on channel X will be temporarily stopped to allow the bridge to scan channel Y), it is recommended to use only one channel when roaming is enabled (also called mono-channel mode). In this case, the bridge will not stop looking for better access points by scanning the beacons sent by the others access points (this mode is called passive mode scan). It will also periodically send probe requests to find access points that were not seen during the passive mode scan (this is the active mode scan). The period can be specified by the user and is called **scan period**.

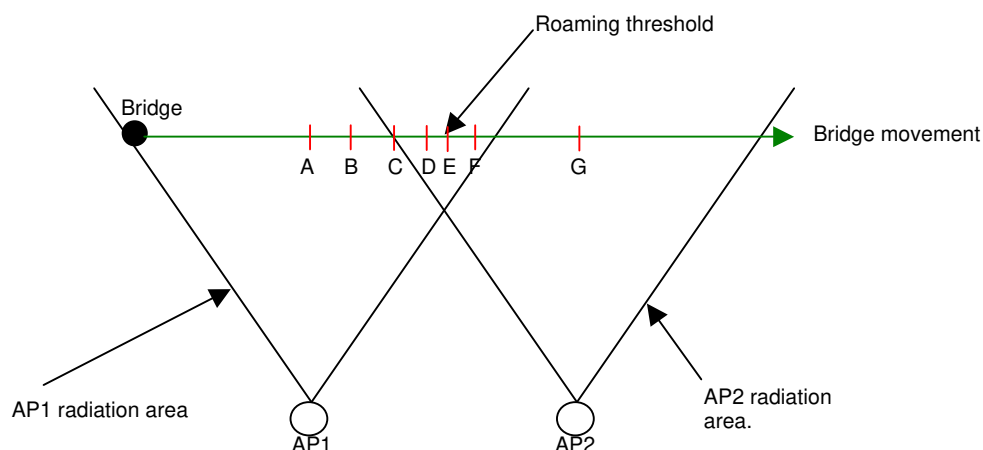
However, when 2 or more channels are used (multichannel mode), it is not advisable to keep scanning at the same rate as in the monochannel mode. This is why some new options are available in the multichannel mode :

- The **RSSI Threshold**: any level below this threshold and the scan is activated (it doesn't make sense to scan other channels while the connection with the access point is excellent). This threshold must be higher than the roaming threshold.
- The **scan duration**. During this time, both passive and active mode scans are used.

In the multichannel mode, there is a different radio channel scanned at each scan period.

**Attention - the shorter the scan period or the longer the scan duration , the more the current connection bandwidth is affected.**

**The more channels you have to scan, the longer the access point discovery time will take.**



In the above diagram :

Scan threshold : 50% of maximum RSSI

Roaming threshold : 45% of the maximum RSSI

The following table shows the RSSI (in %) evolutions between the bridge and AP1, and between the bridge and AP2.

	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>	<b>F</b>	<b>G</b>
<b>RSSI with AP1</b>	100%	50%	40%	30%	20%	10%	0%
<b>RSSI with AP2</b>	0%	0%	10%	20%	30%	40%	100%

In the illustration above :

- Step A : the communication with AP1 is perfect. Since the current RSSI is greater than the scan threshold(50%), there will be no scan.
- Step B : RSSI with AP1 is under 50% so the scan process is engaged.
- Step C : the bridge enters AP2 radiation diagram.
- Step D : the bridge reaches the roaming threshold but has not found a better access point.
- Step E : AP2 RSSI is better than AP1 RSSI so the bridge will roam to AP2 and disconnect from AP1.
- Step F : The scan process still runs because the new RSSI (with AP2) is under the scan threshold..
- Step G : The bridge stops the scan because the current RSSI (with AP2) is higher than the scan threshold.



The roaming mode can be activated using the following option :

WIRELESS ROAMING MODE	
Roaming Mode :	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

If « Enable » is set, the « Basic Roaming Settings » will appear. However, the « Auto channel select » option (located in the « Basic wireless setting » menu) must be cleared. You can select one or more channels available in the channel list.

Once the channels are selected, only the access points using the same channels will be seen by the bridge.

Auto channel select : ☐

Channel :

5.180 GHz - CH 36	▲
5.200 GHz - CH 40	☰
5.220 GHz - CH 44	▼
5.240 GHz - CH 48	
5.260 GHz - CH 52	▼

To make multiple selections/deselect from the list, use Ctrl+Click

The roaming configuration menu is shown below :

BASIC ROAMING SETTINGS	
<p>The roaming mode allows a mobile WiFi bridge to roam between several AP without network connection loss.</p> <p>When the roaming mode is enabled, the bridge will only switch from an AP to an other one if :</p> <ul style="list-style-type: none"> <li>• The RSSI with the current AP is lower than the roaming threshold</li> <li>• A new AP has been detected with a RSSI higher than the RSSI with the current AP.</li> </ul>	
Threshold unit :	<input type="radio"/> dBm <input checked="" type="radio"/> %
RSSI roaming threshold :	<input type="text" value="83"/>

This menu will allow you to set the roaming threshold. It can be entered in percent or in dBm.

The bridge will roam from AP1 to AP2 if :

$$(RSSI_{(AP1)} < RSSI_{(AP2)}) \text{ AND } (RSSI_{(AP1)} < \text{threshold})$$

So, it is impossible to roam to an access point that would offer a worse RSSI than the current one.

If more than one channel is selected, new parameters will appear in the « Advanced Wireless Tab » :

ADVANCED ROAMING SETTINGS	
In multichannel roaming mode, set the "RSSI scan threshold" and "Scan Duration" values to manage the AP scan process :	
<ul style="list-style-type: none"> <li>• <b>RSSI scan threshold</b> : While RSSI with the current AP is higher than this threshold, the bridge will not proceed to any AP scan. Once the RSSI with the current AP drops under this threshold, the AP scan process will start immediatly.</li> <li>• <b>Scan duration</b> : Set the maximum amount of time allowed for a single channel AP scan.</li> </ul>	
In all roaming modes, the "Scan Period" specifies the time interval between two AP scans.	
Threshold unit :	<input type="radio"/> dBm <input checked="" type="radio"/> %
RSSI scan threshold :	<input type="text" value="100"/>
Scan Period (s) :	<input type="text" value="5"/>
Scan Duration (ms) :	<input type="text" value="100"/>

These parameters must be set with care because wrong values can cause some loss of bandwidth or even disconnections.

« **Threshold unit** » : This option sets the unit for the « RSSI scan threshold » value (dBm or percent). This field is only available in the multichannel mode. Percent value is selected by default.

« **RSSI scan threshold** » : This option sets the threshold above which no scan will be made. This field is only available in the multichannel mode. By default, the RSSI scan threshold is set to 100%.

« **Scan Period** » : This option sets the scan process period. This value must be chosen according to the bridge moving speed. This field is always available regardless of the number of channels.

- In the multichannel mode, it sets the interval between two scan periods (active or passive).
- In the monochannel mode, it sets the interval between two active scan periods.

By default, the scan interval is set to 5 seconds.

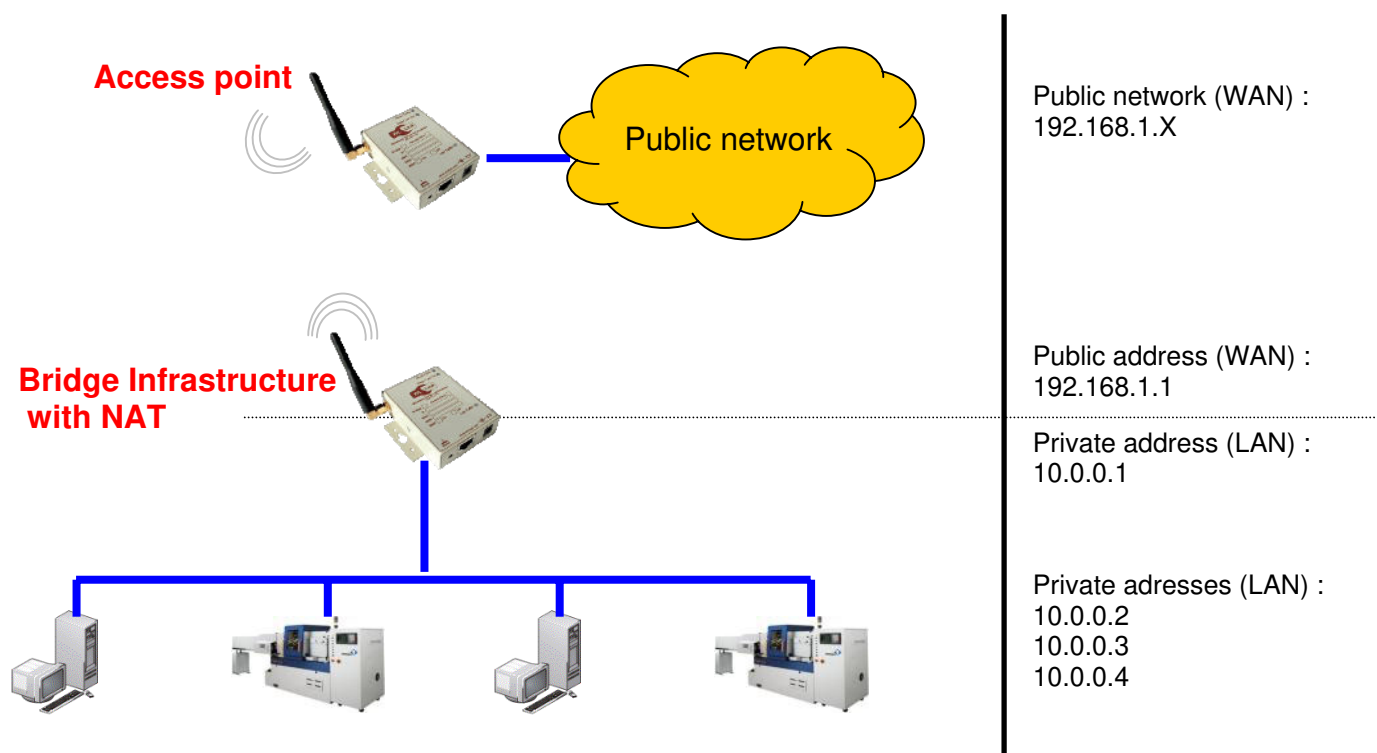
« **Scan duration** » : This option specifies the amount of time spent searching new access points on a given channel. If it is too short new access points may not be found. This field is only available in the multichannel mode. By default, the scan duration value is set to 100ms.

## IV.7 NAT

The NAT (Network Translation Address) is used to multiplex private network addresses (called LAN) into a single external public address (called WAN).

This method saves IPv4 addresses on the public network. This feature implies the following:

- devices in the private network cannot be accessed from a public network.
- only the WAN interface of the bridge will be visible from a public network.
- the traffic from the private network to the public network is allowed by using the bridge as a gateway.



It can be compared to a multiplexer that outputs one public address from several private addresses.

**Attention: NDM ACKSYS software placed on a public network cannot find a bridge using NAT.**

### IV.7.1 NAT menu

The NAT feature is only available in the bridge infrastructure mode with the 4.4.0 firmware version.

The NAT configuration menu is located in the BASIC section. By default, the NAT is disabled. To enable it, select the following :

NAT ENABLE	
Enable NAT :	<input type="checkbox"/>

When enable NAT is set, detailed configuration options are available. These options will configure the following features :

- internal servers (adminweb, snmp)
- WAN interface configuration
- port forwarding rules editing
- port triggering rules editing

When NAT is enabled, the LAN IP address must be static in order to use the “port forwarding” feature.

#### Internal servers :

INTERNAL SERVERS CONFIGURATION	
Enable ping from WAN :	<input checked="" type="checkbox"/>
Enable internal web server from the WAN :	<input checked="" type="checkbox"/>
Web server port :	<input type="text" value="80"/>
Enable internal SNMP server from the WAN :	<input checked="" type="checkbox"/>
SNMP server port :	<input type="text" value="161"/>

« **Enable ping from WAN** » : this option, if enabled, will make the product answer to ICMP ping requests coming from its WAN interface.

« **Enable internal web server from the WAN** » : if enabled, this option allows the internal web server to answer requests from the WAN on the Ethernet port specified by the field « **Web server port** ».

« **Web server port** » : This option configures the TCP Ethernet port used to access the internal web server.

« **Enable internal SNMP server from the WAN** » : if enabled, this option allows the internal SNMP agent to answer requests from the WAN on the Ethernet port specified by the field « **SNMP server port** ».

« **SNMP server port** » : This option configures the TCP Ethernet port used to access the internal SNMP agent.

### **WAN IP configuration :**

WAN IP CONFIGURATION	
IP Address Mode :	<input type="radio"/> Static <input checked="" type="radio"/> DHCP
IP Address :	192.168.1.38
Subnet Mask :	255.255.255.0
Gateway :	192.168.1.1

« **IP Address Mode** » : Selects the WAN IP configuration method. By default, the automatic configuration by **DHCP** is enabled. Manual configuration way can be selected by choosing « **Static** ».

« **IP Address** » : If the **Static** configuration mode is used then this field contains the WAN IP address.

« **Subnet Mask** » : If the **Static** configuration mode is used then this field contains the WAN subnet mask.

« **Gateway** » : If the **Static** configuration mode is used then this field contains the WAN gateway.

## Port Forwarding :

PORT FORWARDING

**Enable :** ☒

**Name :**

**IP Address :**

**Public TCP Ports :**  (ie : 100-200,588)

**Private TCP Ports :**  (ie : 100-200,588)

**Public UDP Ports :**  (ie : 100-200,588)

**Private UDP Ports :**  (ie : 100-200,588)

A server located in the private network (LAN) cannot be accessed by a client located in the public side (WAN).

The port forwarding feature can solve this problem by redirecting public incoming requests on a specified port to a unique private IP address.

Note : this feature allows only one forward rule by public port.

« **Enable** » : If selected, this option marks the rule as active as soon as you click the « Save » button. If not, you will have to enable the rule manually in the “**Port forwarding rules list**” menu.

« **Name** » : Contains the rule's name. This name is used to identify the rule in the “**Port forwarding rules list**” menu.

« **IP Address** » : This field contains the IP address to where the WAN request will be redirected.

« **Public TCP ports** » : This field contains the TCP port or port range which will be redirected to the private network. It is possible to enter more ports or port ranges (separated by a comma). It is possible to leave this field blank if only UDP ports are used.

« **Private TCP ports** » : This field contains the TCP port or port range to which the ports contained by the « Public TCP Port » will be redirected. The syntax used for this field must be the same as the one used for the “Public TCP Ports”.

### Examples :

Public TCP Port	Private TCP Port	NAT behavior
4000	22	TCP public port 4000 is redirected to TCP private port 22.

1000-1002	10-12	TCP public ports 1000, 1001, 1002 are respectively redirected to TCP private ports 10, 11, 12.
68,18-20	100,200-202	TCP public port 68 is redirected to TCP private port 100. And TCP public ports 18, 19, 20 are respectively redirected to TCP private ports 200, 201, 202.

« **Public UDP ports** » : This field contains the UDP ports or port range which will be redirected to the private network. It is possible to enter more port or ports ranges by entering them separated by a comma. It is possible to leave this field blank if only TCP ports are used.

**Champ « Private UDP ports »** : This field contains the TCP port or port range to which the ports contained by the « Public TCP Port » will be redirected. The syntax used for this field must be the same as the one used for the “Public TCP Ports”.

Examples :

Public UDP Ports	Private UDP Port	NAT behavior
4000	22	UDP public port 4000 is redirected to UDP private port 22.
1000-1002	10-12	UDP public ports 1000, 1001, 1002 are respectively redirected to UDP private ports 10, 11, 12.
68,18-20	100,200-202	UDP public port 68 is redirected to UDP private port 100. And UDP public ports 18, 19, 20 are respectively redirected to UDP private ports 200, 201, 202.

The « **Save** » button validates the whole set of port-forward rule parameters. Once selected, this rule will be added to the “Port forwarding rules list”.

The « **Cancel** » button will clean each port-forward rule parameter and set it to its default value. This can be used to cancel rule editing.

### The port forward rules list

PORT FORWARDING RULES LIST						
Enable	Name	IP Address	Public TCP ports	Private TCP port	Public UDP ports	PrivateUDP ports
<input checked="" type="checkbox"/>	ssh	10.0.0.38	4022	22		

This list summarizes all the port-forwarding rules previously entered. For each rule, it shows every parameter entered.

“**Enable**” : This option, if checked, enables the rule located on the same row. If the checkbox is not checked, the rule will be disabled.

## **Port triggering :**

This feature handles a dynamic port-forwarding. The trigger is set by a request on a specified private port (Trigger port range) and will open one or more predefined public ports (Input ports).

When the trigger port is closed, the public ports will be closed at the end of their communication.

**PORT TRIGGERING RULES**

Enable : ☒

Name :

Trigger Port Range :  (ie : 100-200,588)

Trigger Protocol :

Input Port Range :  (ie : 100-200, 588)

Input Protocol :

« **Enable** » : If selected, the rule is marked as active as soon as 'Save' is clicked. If not, you will have to enable the rule manually in the "**Port triggering rules list**" menu.

« **Name** » : Contains the rule's name. This name is used to identify the rule in the "**Port triggering rules list**" menu.

« **Trigger port Range** » : This field contains the private ports that will be used to trigger the opening of public ports. It is possible to enter more ports or port ranges (separated by a comma).

« **Trigger Protocol** » : This parameter allows definition of whether the '**Trigger port Range**' is UDP, TCP or both.

« **Input port Range** » : This field contains the public ports or port range to be opened. It is possible to enter more ports or port ranges (separated by a comma).



« **Input Protocol** » : This parameter allows definition of whether the « **Input port Range** » is UDP, TCP or both.

The « **Save** » button validates the whole set of port-triggering rule parameters. Once selected, the rule will be added to the "Port triggering rules list".

The « **Cancel** » button will clean each port triggering rule parameter and set it to its default value. This can be used to cancel rule editing.



## Port triggering rules list

PORT TRIGGERING RULES LIST				
Enable	Name	Trigger Protocol/Ports	Input Protocol/Ports	
<input checked="" type="checkbox"/>	FTP	TCP 20	TCP 21	 

This list summarizes all the port-triggering rules previously entered. For each rule, it shows every parameter entered.

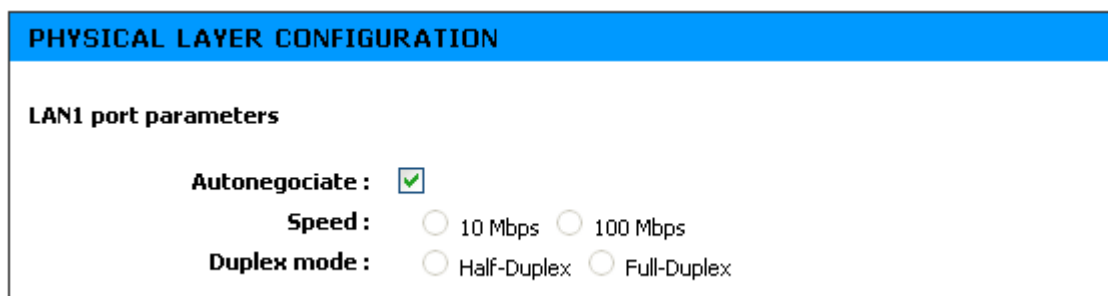
**“Enable”** : This option, if checked, enables the rule located on the same row. If not checked, the rule will be disabled.

## IV.8 Advanced Ethernet interface configuration

Since 4.2.0 release, the firmware allows access to an advanced LAN interface configuration menu. This menu is available in the Advanced section of the « Advanced Ethernet » menu.

Depending on the range of your product, two pages are available.

For a product from the WLg-LINK range :



The screenshot shows a configuration window titled "PHYSICAL LAYER CONFIGURATION" in a blue header. Below the header, the text "LAN1 port parameters" is displayed. Under this, there are three settings: "Autonegociate" with a checked checkbox, "Speed" with two radio buttons for "10 Mbps" and "100 Mbps", and "Duplex mode" with two radio buttons for "Half-Duplex" and "Full-Duplex".

« **Autonegociate** » : This option is activated by default and allows detection of the communication speed and the duplex type.

« **Speed** » : This option allows selection of the Ethernet interface speed (10Mbps or 100Mbps).

« **Duplex mode** » : this option allows selection of the duplex mode for the Ethernet interface (half duplex or full duplex).

For a product from the WLg-ABOARD range :

PHYSICAL LAYER CONFIGURATION	
<b>LAN1 port parameters</b>	
<b>Autonegociate :</b>	<input checked="" type="checkbox"/>
<b>Speed :</b>	<input type="radio"/> 10 Mbps <input type="radio"/> 100 Mbps
<b>Duplex mode :</b>	<input type="radio"/> Half-Duplex <input type="radio"/> Full-Duplex
<b>LAN2 port parameters</b>	
<b>Autonegociate :</b>	<input checked="" type="checkbox"/>
<b>Speed :</b>	<input type="radio"/> 10 Mbps <input type="radio"/> 100 Mbps
<b>Duplex mode :</b>	<input type="radio"/> Half-Duplex <input type="radio"/> Full-Duplex
<b>Common settings</b>	
<b>Allow large frames :</b>	<input checked="" type="checkbox"/> Uncheck this to make frames larger than 1518 bytes illegal

« **Autonegociate** » : This option is activated by default and allows detection of the communication speed and the duplex type.

« **Speed** » : This option allows selection of the ethernet interface speed (10Mbps or 100Mbps).

« **Duplex mode** » : This option selection of the duplex mode for the ethernet interface (half duplex or full duplex)

« **Allow large frames** » : If set, this option allows a frame size bigger than 1518 bytes. The larger frame will then be 1540 bytes long. If unset, this option sets any frames bigger than 1518 bytes as invalid.

Products with two or more LAN ports implement the « Port mirroring » feature. It allows the product to copy the Ethernet traffic from one port to another. This can be accessed from the « Advanced Ethernet » menu :

PORT MIRRORING	
<b>Mirror to port :</b>	<input type="text" value="None"/> ▼
<b>Mirror from :</b>	<input type="checkbox"/> LAN1 port <input type="checkbox"/> LAN2 port <input type="checkbox"/> Wi-Fi and local product traffic

« **Mirror to port** » : This field contains the destination port of the port mirroring. The selected traffic will be copied to this port.

« **Mirror from** » : This field contains the mirrored port.

## V SNMP MONITORING AND MANAGEMENT

In typical SNMP usage, there are a number of systems to be managed, with one or more systems managing them. A software component called “agent” runs on each managed system and reports information via SNMP to the managing systems.

With SNMP you can :

- See the device state
- Define the device setting
- Manage events

The 4.2.0 update includes a SNMP V2c agent. The agent can however handle SNMP V1 requests. The SNMP version is automatically handled by the product.

For example :

- If a valid SNMP V2c request is received by the product, the response frame will be a SNMP V2c frame.
- If a valid SNMP V1 request is received by the product, the response frame will be a SNMP V1 frame.

The product can also send SNMP V1 or V2c traps to a supervisor.

## V.1 MIB (Management Information Bases)

SNMP does not define which information (which variables) a managed system should offer. SNMP uses an extensible design, where management information bases (MIBs) define the available information. MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID). Roughly speaking, each OID identifies a variable that can be read or set via SNMP.

Your device uses the following groups in MIB II:

- System, OID .1.3.6.1.2.1.1, contain device information.
- IP, OID .1.3.6.1.2.1.4.20.1.4.2, contain device IP information.

There is also a specific MIB: « Enterprise MIB ».

The ACKSYS « Enterprise MIB » root OID is « **.1.3.6.1.4.1.28097** ». More details are available further on in this document.

The MIB file is on the CDROM or can be downloaded on our web site.

## V.2 SNMP community

Devices and management stations running SNMP belong to a SNMP community. This helps define the information destination. The community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities.

### V.3 SNMP trap

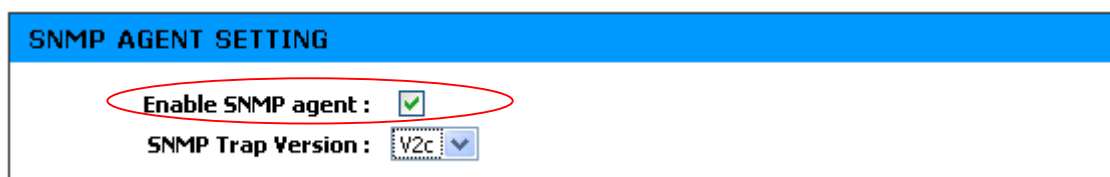
A trap is an alert that is sent to a management station by agents.

ACKSYS devices can issue the following traps:

- ColdStart: Device start
- Linkdown: Wireless link where the access point is broken (only in bridge infrastructure mode).
- LinkUp: Wireless link where the access point is established (only in bridge infrastructure mode).
- Power1 On: Power supply is up (only for WLg-ABOARD/xx).
- Power1 Off: Power supply is off (only for WLg-ABOARD/xx).
- Power2 On: Power supply is up (only for WLg-ABOARD/xx).
- Power2 Off: Power supply is off (only for WLg-ABOARD/xx).

### V.4 SNMP menu

Since the 3.8.0 firmware update, the SNMP agent is enabled by default. If your product's firmware version is before 2.2.0, this can be enabled by selecting « Enable SNMP agent » ,available in the BASIC\SNMP menu.



**SNMP AGENT SETTING**

Enable SNMP agent : ☒

SNMP Trap Version : V2c

## V.5 SNMP filtering

The 4.2.0 firmware update allows community creation as well as links to filter SNMP requests.

First create one or more communities using the « SNMP communities setting » :

**SNMP COMMUNITIES SETTING**
  
  
 Community Name : 
  
 Rights Type :

**SNMP COMMUNITIES LIST**

Enable	Community	Rights	
<input checked="" type="checkbox"/>	private	Read-Write	
<input checked="" type="checkbox"/>	public	Read-Only	
<input checked="" type="checkbox"/>	other	Read-Restricted	

### Add a community :







Enter the community name in the « **Community Name** » field, then select the type of right desired, then select « **Save** ». The new community will be added to the community list.

There are 3 types of rights that can be chosen for a community :

- Read Only : the members of this community will not be able to modify the OID value
- Read Write : the members of this community will be able to read and modify the OID value.
- Read Restricted : the members of this community will not be able to modify the OID value nor to read “sensible” OID (such as WEP / WPA keys).



Each community can have an authorized IP address range. The « **SNMP IP Filtering Rules** » menu can be used to configure this filtering feature.

SNMP IP FILTERING RULES SETTING	
Community :	<input type="text" value=""/>
IP Interval Start :	<input type="text" value="0.0.0.0"/>
IP Interval Stop :	<input type="text" value="255.255.255.255"/>
<input type="button" value="Save"/> <input type="button" value="Clear"/>	

SNMP IP FILTERING RULES LIST					
Enable	Community	Rights	Ip start	Ip stop	
<input checked="" type="checkbox"/>	private	Read-Write	192.168.1.30	192.168.1.30	 
<input checked="" type="checkbox"/>	public	Read-Only	192.168.1.31	192.168.1.80	 
<input checked="" type="checkbox"/>	other	Read-Restricted	192.168.1.81	192.168.1.254	 

To specify an IP address range you will need to :

- Choose a community in « Community »
- Enter the granted IP range start value
- Enter the granted IP range end value
- Click the “Save” button to validate previous values

Once the “Save” has been selected, the rule appears in the “SNMP IP filtering rules list” menu. Rules can then be deleted by selecting «  » or edited by clicking on the «  » icon.

Any SNMP request coming from an unknown IP address (not in the rules) will be discarded.



## V.6 Traps management

The SNMP trap configuration can be found in the “Basic / SNMP” menu.

**The SNMP agent must be enabled.**

You will first need to set the SNMP version used to send SNMP traps. Select the correct value (V2c or V1) in the « SNMP Trap Version » combobox.

SNMP Trap Version : 

You can now add, remove and edit SNMP traps using the following menu :

SNMP TRAP SETTING

Enable trap : ☒



Trap type : ColdStart

Trap receiver IP :

Community : public

Save
Clear

SNMP TRAP LIST

Enable	Trap type	Trap receiver IP	Community	
<input checked="" type="checkbox"/>	LinkDown	10.0.0.1	public	 
<input checked="" type="checkbox"/>	LinkUp	10.0.0.2	private	

### Add a trap

This can be done in the « SNMP TRAP SETTING » window:

- Enable: Uncheck this box to disable this trap
- Trap type: Select the required trap (ColdStart, Linkdown, LinkUp)
- Trap receiver IP: IP of the management station to where the Trap should be sent
- Community: Trap community

Click on save. The new trap is added in the « SNMP TRAP LIST » window.

### Comments:

- You can have up to 5 traps.
- The same trap can be configured several times.
- Each trap can have a specific destination IP.
- Each trap can have a specific destination community.
- Destination community can be different from the agent.

### Delete a trap

To remove a trap, click on the «  » trap icon and confirm your choice.

## Modify a trap

To modify a trap setting, click on the «  » trap icon.

SNMP TRAP SETTING









Enable trap : ☒

Trap type : ColdStart ▼

Trap receiver IP :

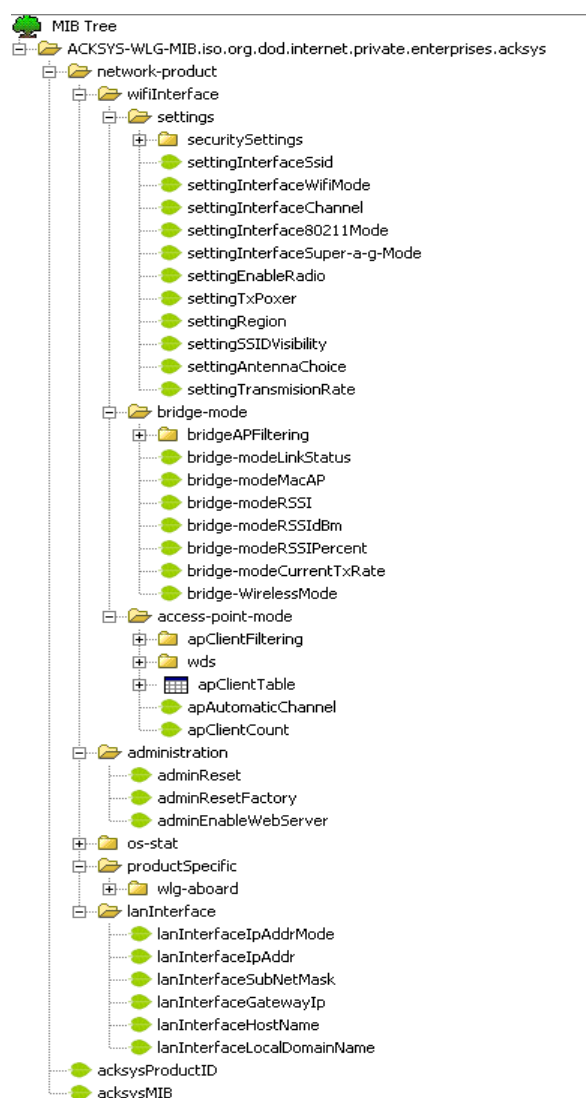
Community :

Save
Clear

SNMP TRAP LIST					
Enable	Trap type	Trap receiver IP	community		
<input checked="" type="checkbox"/>	ColdStart	192.168.1.47	public		
<input checked="" type="checkbox"/>	ColdStart	192.168.1.50	private		
<input checked="" type="checkbox"/>	LinkDown	192.168.1.50	public		
<input checked="" type="checkbox"/>	LinkUp	192.168.1.50	public		

Trap settings can be modified in « SNMP TRAP SETTING » . Once done, select save. The trap list is updated.

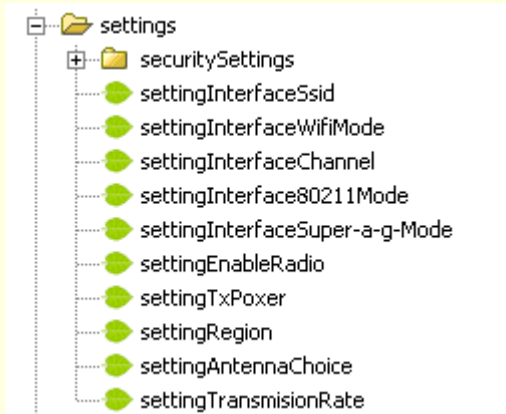
## V.7 Enterprise MIB ACKSYS



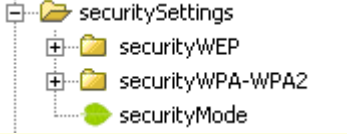

### Comments:

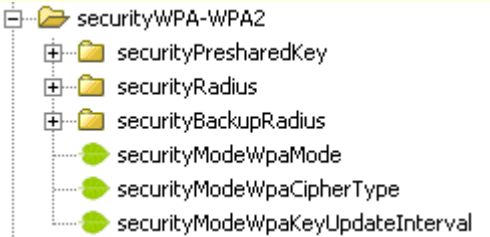
- Depending on the mode that is used (Access point or Bridge), you can only access « bridge-mode » or « access-point-mode » parameters.
- Changes will be enabled only after a reboot.
- The device can be rebooted by SNMP; to do this, write '1' in the OID .1.3.6.1.4.1.28097.1.2.1.0.



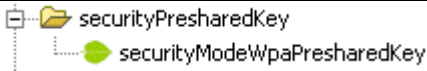
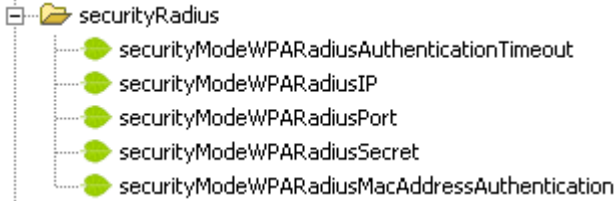
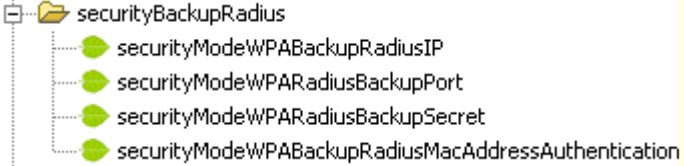
OID	Access	Name	Description	Values
.1.3.6.1.4.1.28097.1		ACKSYS-WLG-MIB	MIB for access points and bridge WIFI 802.11 a/b/g/h.	
.1.3.6.1.4.1.28097.3.0	Read	acksysProductID	Product identification code	1 : WLg-LINK 2 : WLg-ABOARD/N 3 : WLg-LINK-V2 4 : WLg-ABOARD/N-V2
.1.3.6.1.4.1.28097.2.0		acksysMIB		
.1.3.6.1.4.1.28097.1.1		wifiInterface	Part of the MIB dedicated to the wifi interface.	
.1.3.6.1.4.1.28097.1.1.1				
				
		<b>setting</b>	<b>WLAN settings</b>	
.1.3.6.1.4.1.28097.1.1.1.1.0	Read Restricted Write	Setting InterfaceSsid	WLAN SSID	Character string (up to 33 characters)
.1.3.6.1.4.1.28097.1.1.1.2.0	Read Restricted Write	Setting InterfaceWifiMode	Wifi - mode	1 : Bridge 2 : Access point
.1.3.6.1.4.1.28097.1.1.1.3.0	Read Write	SettingInterfaceChannel	Wireless channel	Wifi channel number. Depends on the selected 802.11 mode : A, H or B/G (used only for Access

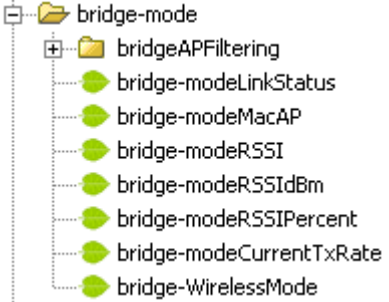
OID	Access	Name	Description	Values
				Point and Bridge ad-hoc)
.1.3.6.1.4.1.28097.1.1.1.4.0	Read Restricted Write	SettingInterface80211Mode	802.11x mode	1 : 802.11b only 2 : 802.11g only 3 : 802.11 b/g 4 : 802.11 a/h
.1.3.6.1.4.1.28097.1.1.1.5.0	Read Restricted Write	SettingInterfaceSuper-a-g-Mode	Super a/g mode	1 : Super a/g mode disable 2 : Super a/g without turbo. 3 : Super a/g with static turbo 4 : Super a/g with dynamic turbo
.1.3.6.1.4.1.28097.1.1.1.6.0	Read Restricted Write	SettingEnableRadio	Enables/disables wifi card	1 : Disables the radio card 2 : Enables the radio card
.1.3.6.1.4.1.28097.1.1.1.7.0	Read Restricted Write	SettingTxPower	Wireless radio power	1 : High (100 %) 2 : Medium (50 %) 3 : Low (25%)
.1.3.6.1.4.1.28097.1.1.1.8.0	Read Restricted Write	SettingRegion	Country	2 = Israel 4 = USA 5 = Hong Kong 6 = Canada 7 = Australia 10 = France outdoor 14 = Europe 17 = Japan 18 = Singapore 20 = Korea
.1.3.6.1.4.1.28097.1.1.1.10.0	Read Write	SettingAntennaChoice	Antenna port	1 : diversity 2 : main 3 : aux
.1.3.6.1.4.1.28097.1.1.1.11.0	Read Write	Setting Transmission Rate	Transmission rate	-1 : automatic 108,96,72,54,48,36,24,18,12,11,5 (5.5),2,1

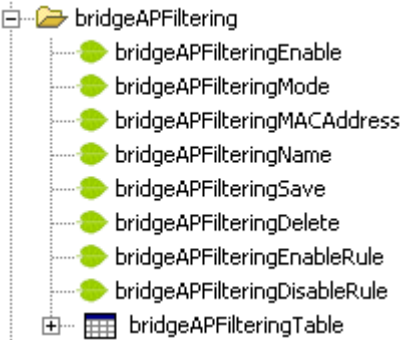
OID	Access	Name	Description	Values
<b>.1.3.6.1.4.1.28097.1.1.1.9</b> 		<b>Security Settings</b>	<b>WLAN security options</b>	
.1.3.6.1.4.1.28097.1.1.1.9.1.0	Read Restricted Write	Security Mode	WiFi security mode	1 : none 2 : WEP 3 : WPA-WPA2-PSK 4 : WPA-WPA2
<b>.1.3.6.1.4.1.28097.1.1.1.9.2</b> 		<b>Security</b> <b>WEP</b>	<b>WEP configuration</b>	

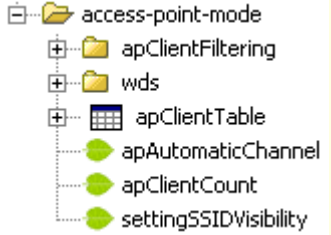
OID	Access	Name	Description	Values
.1.3.6.1.4.1.28097.1.1.1.9.2.1.0	Read Restricted Write	SecurityModeWepKeyLen	WEP Key length	64 or 128
.1.3.6.1.4.1.28097.1.1.1.9.2.2.0	Read Restricted Write	SecurityModeWepKey-1	WEP key number 1	WEP key in hex form
.1.3.6.1.4.1.28097.1.1.1.9.2.3.0	Read Restricted Write	SecurityModeWepKey-2	WEP key number 2	WEP key in hex form
.1.3.6.1.4.1.28097.1.1.1.9.2.4.0	Read Restricted Write	SecurityModeWepKey-3	WEP key number 3	WEP key in hex form
.1.3.6.1.4.1.28097.1.1.1.9.2.5.0	Read Restricted Write	SecurityModeWepKey-4	WEP key number 4	WEP key in hex form
.1.3.6.1.4.1.28097.1.1.1.9.2.6.0	Read Restricted Write	SecurityModeDefaultWepKey	Number of WEP keys	1,2,3,4
.1.3.6.1.4.1.28097.1.1.1.9.2.7.0	Read Restricted Write	SecurityModeWepAuthenticati on	Authentication mode	1 : open 2 : shared
<b>.1.3.6.1.4.1.28097.1.1.1.9.3</b> 		<b>SecurityWPA-WPA2</b>	<b>WPA security configuration</b>	
.1.3.6.1.4.1.28097.1.1.1.9.3.4.0	Read Restricted Write	SecurityModeWpaMode	WPA version	1 : WPA 2 : WPA2
.1.3.6.1.4.1.28097.1.1.1.9.3.5.0	Read Write	SecurityModeWpaCipherType	WPA cipher type	1 : TKIP 2 : AES
.1.3.6.1.4.1.28097.1.1.1.9.3.6.0	Read Restricted Write	SecurityModeWpaKeyUpdateI nterval	Time between two Group key changes.	duration in seconds (between 1 and 65535)
<b>.1.3.6.1.4.1.28097.1.1.1.9.3.1</b>		<b>SecurityPresharedKey</b>	<b>Preshared key configuration</b>	

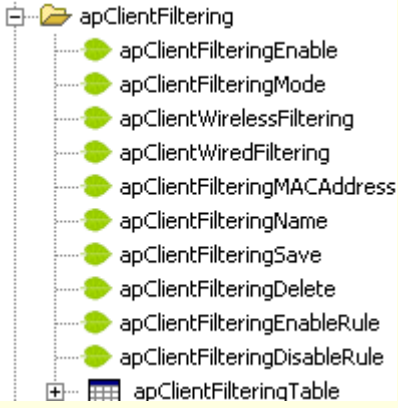


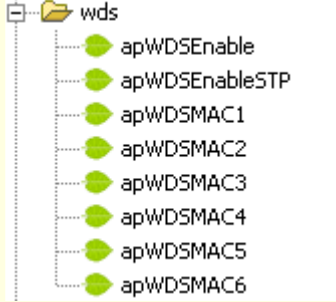
OID	Access	Name	Description	Values
				
.1.3.6.1.4.1.28097.1.1.1.9.3.1.1.0	Read Restricted Write	SecurityModeWpaPresharedKey	WPA Preshared key	Character string (between 8 and 33 characters)
<b>.1.3.6.1.4.1.28097.1.1.1.9.3.2</b> 		<b>SecurityRadius</b>	<b>WPA in radius mode configuration</b>	
.1.3.6.1.4.1.28097.1.1.1.9.3.2.1.0	Read Restricted Write	SecurityModeWpaRadiusAuthenticationTimeout	Maximum authentication time	Duration in minutes
.1.3.6.1.4.1.28097.1.1.1.9.3.2.2.0	Read Restricted Write	SecurityModeWpaRadiusIP	Radius server IP address	IP Address
.1.3.6.1.4.1.28097.1.1.1.9.3.2.3.0	Read Restricted Write	SecurityModeWpaRadiusPort	Radius server port used for authentication	1 to 65535
.1.3.6.1.4.1.28097.1.1.1.9.3.2.4.0	Read Restricted Write	SecurityModeWpaRadiusSecret	Password used in communications between the radius server and the access point.	Character string (between 1 and 33 characters)
.1.3.6.1.4.1.28097.1.1.1.9.3.2.5.0	Read Restricted Write	SecurityModeWpaRadiusMacAddressAuthentication	Using of the SUPPLICANT MAC address for Radius authentication	1 : disabled 2 : enabled
<b>.1.3.6.1.4.1.28097.1.1.1.9.3.3</b> 		<b>SecurityBackupRadius</b>	<b>WPA in radius mode with a backup server configuration</b>	

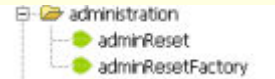
OID	Access	Name	Description	Values
.1.3.6.1.4.1.28097.1.1.1.9.3.3.1.0	Read Restricted Write	SecurityModeWpaBackupRadiusIP	Maximum authentication time	Duration in minutes
.1.3.6.1.4.1.28097.1.1.1.9.3.3.2.0	Read Restricted Write	SecurityModeWpaRadiusPort	Radius server IP address	IP address
.1.3.6.1.4.1.28097.1.1.1.9.3.3.3.0	Read Restricted Write	SecurityModeWpaBackupRadiusSecret	Radius server port used for authentication	1 to 65535
.1.3.6.1.4.1.28097.1.1.1.9.3.3.4.0	Read Restricted Write	SecurityModeWpaBackupRadiusMacAddressAuthentication	Password used in communications between the radius server and the access point.	Character string (between 1 and 33 characters)
<b>.1.3.6.1.4.1.28097.1.1.2</b> 		<b>bridge-mode</b>	<b>Bridge infrastructure configuration</b>  <u>NOTE:</u> The followings OIDs are not relevant in ad-hoc mode.	
.1.3.6.1.4.1.28097.1.1.2.1.0	Read	bridge-modeLinkStatus	Link status with the access point.	1 : « up », Wi-Fi link up 2 : « down », Wi-Fi link down
.1.3.6.1.4.1.28097.1.1.2.2.0	Read	bridge-modeMacAP	MAC address of the access point to which the bridge is connected.	
.1.3.6.1.4.1.28097.1.1.2.3.0	Read	bridge-modeRSSI	RSSI value (ATHEROS format)	
.1.3.6.1.4.1.28097.1.1.2.4.0	Read	bridge-modeRSSIdBm	RSSI value in dBm	
.1.3.6.1.4.1.28097.1.1.2.5.0	Read	bridge-modeRSSIPercent	RSSI value in percent	
.1.3.6.1.4.1.28097.1.1.2.6.0	Read	bridge-modeCurrentTxRate	Current transmission rate in bits/s	
.1.3.6.1.4.1.28097.1.1.2.7.0	Read Write	bridge-WirelessMode	Bridge mode.	1 : infrastructure 2 : ad-hoc

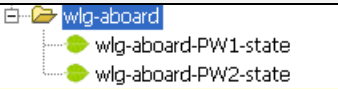
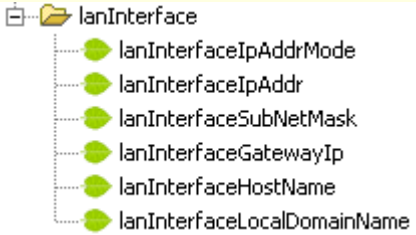
OID	Access	Name	Description	Values
<b>.1.3.6.1.4.1.28097.1.2.8</b> 		<b>bridgeAPFiltering</b>	<b>Access point filtering configuration</b>	
.1.3.6.1.4.1.28097.1.1.2.8.1.0	Read Write	bridgeAPFilteringEnable	Enables or disables the MAC filtering	1 : disabled 2 : enabled
.1.3.6.1.4.1.28097.1.1.2.8.2.0	Read Write	bridgeAPFilteringMode	Selects the filter mode	1 : allow 2 : deny
.1.3.6.1.4.1.28097.1.1.2.8.3.0	Read Write	bridgeAPFilteringMACAddress	MAC address of the access point	MAC Address
.1.3.6.1.4.1.28097.1.1.2.8.4.0	Read Write	bridgeAPFilteringName	Rule name	Character string (between 1 and 63 characters)
.1.3.6.1.4.1.28097.1.1.2.8.5.0	Write	bridgeAPFilteringSave	Write 1 at this OID will create a new rule with <b>bridgeAPFilteringMACAddress</b> et <b>bridgeAPFilteringComputerName</b> paramaters	1
.1.3.6.1.4.1.28097.1.1.2.8.6.0	Write	bridgeAPFilteringDelete	Removes the selected rule	Index of the rule to delete
.1.3.6.1.4.1.28097.1.1.2.8.7.0	Write	bridgeAPFilteringEnableRule	Enables the selected rule	Index of the rule to enable
.1.3.6.1.4.1.28097.1.1.2.8.8.0	Write	bridgeAPFilteringDisableRule	Disables the selected rule	Index of the rule to disable

OID	Access	Name	Description	Values
.1.3.6.1.4.1.28097.1.1.2.8.9		bridgeAPFilteringList	Access point filtering rules list	
.1.3.6.1.4.1.28097.1.1.2.8.9.1		bridgeAPFilteringListEntry	Single rule description.	
.1.3.6.1.4.1.28097.1.1.2.8.9.1.1	Read Restricted	bridgeAPFilteringListId	Rule index	
.1.3.6.1.4.1.28097.1.1.2.8.9.1.2	Read Restricted	bridgeAPFilteringListName	Rule name	
.1.3.6.1.4.1.28097.1.1.2.8.9.1.3	Read Restricted	bridgeAPFilteringListMAC	Access point MAC address	
.1.3.6.1.4.1.28097.1.1.2.8.9.1.4	Read Restricted	bridgeAPFilteringListEnable	Shows if the rule is selected or not	1 : enabled 2 : disabled
<b>.1.3.6.1.4.1.28097.1.1.3</b> 				
		<b>access-point-mode</b>	<b>Access point settings</b>	
.1.3.6.1.4.1.28097.1.1.3.1		apClientTable	Connected Client table	
.1.3.6.1.4.1.28097.1.1.3.1.1		apClientEntry	Single client description	
.1.3.6.1.4.1.28097.1.1.3.1.1.1	Read	clientMacAddr	Client MAC address	
.1.3.6.1.4.1.28097.1.1.3.1.1.2	Read	client80211Mode	Client WLAN mode	1 : 802.11b only 2 : 802.11g only 3 : 802.11 b/g 4 : 802.11 a/h
.1.3.6.1.4.1.28097.1.1.3.1.1.3	Read	clientTxRate	Client transmission rate in bits/s.	
.1.3.6.1.4.1.28097.1.1.3.1.1.4	Read	clientRssiPercent	Client RSSI in percent	
.1.3.6.1.4.1.28097.1.1.3.2.0	Read Write	apAutomaticChannel	Enables / disables automatic channel selection	1 : automatic channel selection is disabled 2 : automatic channel selection is enabled
.1.3.6.1.4.1.28097.1.1.3.3.0	Read	apClientCount	Number of client connected to the access point	
.1.3.6.1.4.1.28097.1.1.3.6.0	Read Write	SettingSSIDVisibility	Broadcasts or not the SSID	1 : SSID not visible 2 : SSID visible

OID	Access	Name	Description	Values
<b>.1.3.6.1.4.1.28097.1.1.3.4</b> 		<b>apClientFiltering</b>	<b>Client Filtering (MAC address filtering) configuration</b>	
.1.3.6.1.4.1.28097.1.1.3.4.1.0	Read Write	apClientFilteringEnable	Enables / disables MAC address filtering	1 : disabled 2 : enabled
.1.3.6.1.4.1.28097.1.1.3.4.2.0	Read Write	apClientFilteringMode	Select the filter mode	1 : allow 2 : deny
.1.3.6.1.4.1.28097.1.1.3.4.3.0	Read Write	apClientWirelessFiltering	Filter clients from WLAN interface	1 : disabled 2 : enabled
.1.3.6.1.4.1.28097.1.1.3.4.4.0	Read Write	apClientWiredFiltering	Filter clients from LAN interface	1 : disabled 2 : enabled
.1.3.6.1.4.1.28097.1.1.3.4.5.0	Read Write	apClientFilteringMACAddress	Client MAC address	MAC address
.1.3.6.1.4.1.28097.1.1.3.4.6.0	Read Write	apClientFilteringName	Rule name	Character string (between 1 and 63 characters)
.1.3.6.1.4.1.28097.1.1.3.4.7.0	Write	apClientFilteringSave	Write 1 at this OID will create a new rule with <b>apClientFilteringMACAddress</b> and <b>apClientAPFilteringComputerName</b> parameters	1
.1.3.6.1.4.1.28097.1.1.3.4.8.0	Write	apClientFilteringDelete	Removes the selected rule	Index of the rule to delete
.1.3.6.1.4.1.28097.1.1.3.4.9.0	Write	apClientFilteringEnableRule	Enables the selected rule	Index of the rule to

OID	Access	Name	Description	Values
				enable
.1.3.6.1.4.1.28097.1.1.3.4.10.0	Write	apClientFilteringDisableRule	Disables the selected rule	Index of the rule to disable
.1.3.6.1.4.1.28097.1.1.3.4.11		apClientFilteringList	Client filtering rules list	
.1.3.6.1.4.1.28097.1.1.3.4.11.1		apClientFilteringListEntry	Single rule description	
.1.3.6.1.4.1.28097.1.1.3.4.11.1.1	Read Restricted	apClientFilteringListId	Rule index	
.1.3.6.1.4.1.28097.1.1.3.4.11.1.2	Read Restricted	apClientFilteringListName	Rule name	
.1.3.6.1.4.1.28097.1.1.3.4.11.1.3	Read Restricted	apClientFilteringListMAC	Client MAC address	
.1.3.6.1.4.1.28097.1.1.3.4.11.1.4	Read Restricted	apClientFilteringListEnable	Shows if the rule is selected or not	1 : disabled 2 : enabled
<b>.1.3.6.1.4.1.28097.1.1.3.4</b> 		<b>WDSConfiguration</b>	<b>WDS configuration</b>	

OID	Access	Name	Description	Values
.1.3.6.1.4.1.28097.1.1.3.4.1.0	Read Write	apWDSEnable	Enables or disables WDS	1 : Disabled 2 : Enabled
.1.3.6.1.4.1.28097.1.1.3.4.2.0	Read Write	apWDSEnableSTP	Enables or disables STP	1 : Disabled 2 : Enabled
.1.3.6.1.4.1.28097.1.1.3.4.3.0	Read Write	ApWDSMAC1	MAC address number 1	IP address
.1.3.6.1.4.1.28097.1.1.3.4.4.0	Read Write	ApWDSMAC2	MAC address number 2	IP address
.1.3.6.1.4.1.28097.1.1.3.4.5.0	Read Write	ApWDSMAC3	MAC address number 3	IP address
.1.3.6.1.4.1.28097.1.1.3.4.6.0	Read Write	ApWDSMAC4	MAC address number 4	IP address
.1.3.6.1.4.1.28097.1.1.3.4.7.0	Read Write	ApWDSMAC5	MAC address number 5	IP address
.1.3.6.1.4.1.28097.1.1.3.4.8.0	Read Write	ApWDSMAC6	MAC address number 6	IP address
<b>.1.3.6.1.4.1.28097.1.2</b> 		<b>administration</b>	<b>Device management</b>	
.1.3.6.1.4.1.28097.1.2.1.0	Read Write	adminReset	Device reboot	1 to reboot the product
.1.3.6.1.4.1.28097.1.2.2.0	Read Write	adminResetFactory	Restores factory settings	1 to restore factory settings
.1.3.6.1.4.1.28097.1.2.3.0	Read Write	adminEnableWebServer	Enables internal web server	1 : disabled 2 : enabled
<b>.1.3.6.1.4.1.28097.1.4</b>		<b>ProductSpecific</b>	<b>Product specific configuration</b>	
<b>.1.3.6.1.4.1.28097.1.4.1</b>		<b>Wlg-aboard</b>	<b>WLg-ABOARD/N[P] specific settings</b>	

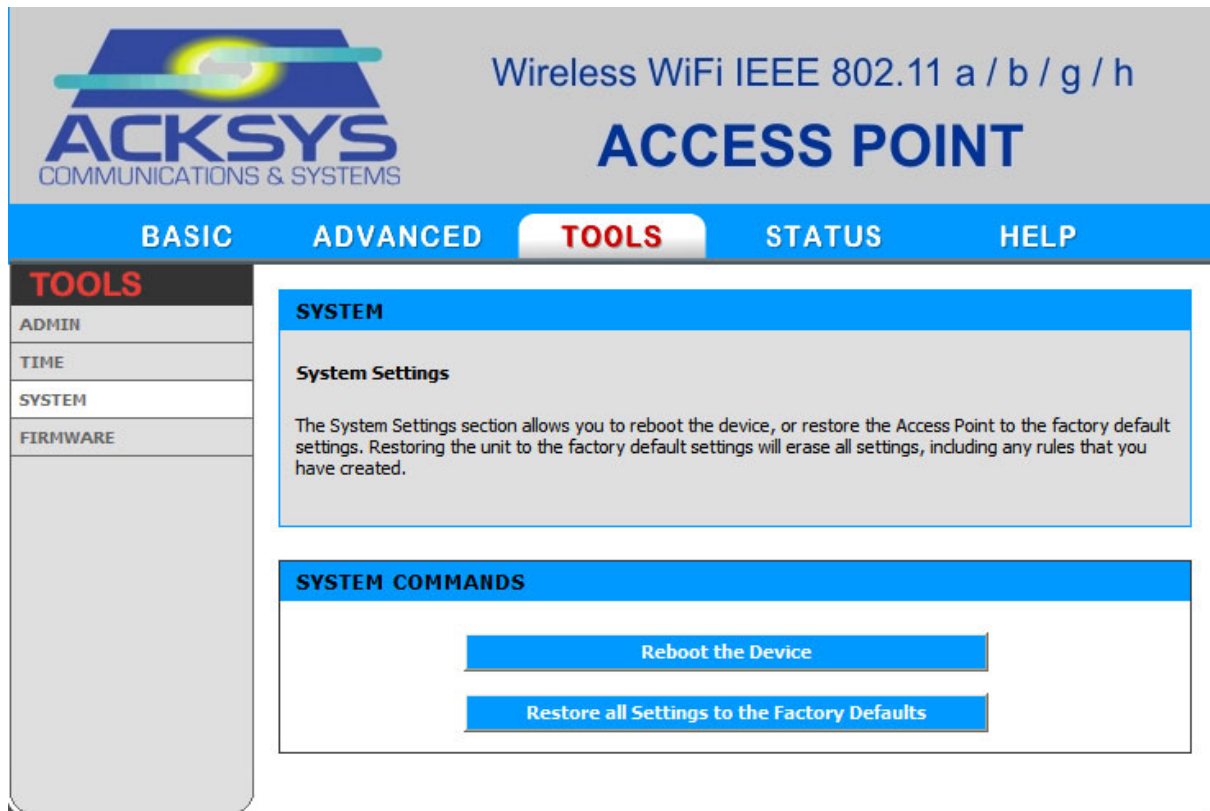
OID	Access	Name	Description	Values
				
.1.3.6.1.4.1.28097.1.4.1.1.0	Read	wlg-aboard-PW1-state	Power 1 status	1 : Power on 2 : Power off
.1.3.6.1.4.1.28097.1.4.1.2.0	Read	wlg-aboard-PW2-state	Power 2 status	1 : Power on 2 : Power off
<b>.1.3.6.1.4.1.28097.1.5</b> 		<b>lanInterface</b>	<b>LAN interface configuration</b>	
.1.3.6.1.4.1.28097.1.5.1.0	Read Restricted Write	lanInterfaceIpAddrMode	IP address configuration mode	1 : static 2 : DHCP
.1.3.6.1.4.1.28097.1.5.2.0	Read Restricted Write	lanInterfaceIpAddr	LAN IP address	IP address
.1.3.6.1.4.1.28097.1.5.3.0	Read Restricted Write	lanInterfaceSubNetMask	LAN subnet mask.	Subnet mask
.1.3.6.1.4.1.28097.1.5.4.0	Read Restricted Write	lanInterfaceGatewayIP	LAN gateway IP address	IP address
.1.3.6.1.4.1.28097.1.5.5.0	Read Restricted Write	lanInterfaceHostName	LAN host name	Character string (between 1 and 63 characters)
.1.3.6.1.4.1.28097.1.5.6.0	Read Restricted Write	lanInterfaceLocalDomainName	LAN local domain name	Character string (between 1 and 63 characters)



## VI FACTORY DEFAULT SETTINGS

This option restores all settings back to the settings that were in place at the time the Access Point was shipped from the factory.

Any settings that have not been backed up will be lost. If you wish to backup your Access Point configuration settings, this can be done from **Tools→Admin**.



Login: « admin »

Password: none

Mode « ACCESS POINT »

IP address: 192.168.1.253, subnet mask: 255.255.255.0

Wireless channel: automatic

Mode b/g

SSID « acksys »

SSID is broadcasted

No Wi-Fi security (no WEP, WPA, WPA2, and no MAC ADDRESS filtering)

SNMP management : disabled

DHCP server : disabled

## VII DEVICE UPGRADE

### VII.1 By the WEB interface

The Firmware Upgrade section can be used to update to the latest firmware code therefore improving functionality and performance.

It can be done from the “tools → firmware” menu.

The screenshot shows the ACKSYS web interface. On the left is a sidebar menu with the following items: **TOOLS** (highlighted), ADMIN, TIME, SYSTEM, and FIRMWARE. The main content area is titled **FIRMWARE** and contains three sections:

- Firmware Upgrade**: A section with a description: "The Firmware Upgrade section can be used to update to the latest firmware code to improve functionality and performance." Below this are two buttons: "Save Settings" and "Don't Save Settings".
- FIRMWARE INFORMATION**: A section displaying the current firmware details:  
**Current Firmware Version :** 3.2.1  
**Current Firmware Date :** 27-jul-2007
- FIRMWARE UPGRADE**: A section with instructions: "To upgrade the firmware, your PC must have a wired connection to the Access Point. Enter the name of the firmware upgrade file, and click on the Upload button." Below this is an "Upload:" label, a text input field, a "Parcourir..." button, and an "Upload" button.

All configuration parameters are kept.

### VII.2 By ACKSYS NDM

3.6.0 firmware release is at least required.

The screenshot shows the ACKSYS Networking Devices Manager (NDM) software interface. It features a menu bar (File, Edit, Help), a toolbar with buttons for Refresh, Configure IP, Upgrade, and Web, and a "Hide selection" checkbox. On the left is a tree view showing the device hierarchy: All products (2), Access points (2), Infrastructure clients (0), Ad-hoc clients (0), and Unmanageable products (0). The main area displays a table of two devices:

Product	Model	Function	Name	MAC address	IP address	Association	Firmware	Security	SSID	Channel
	WLg-LINK	Access Point	ACKSYS Device	00:0E:8E:08:6B...	192.168.1.201	0 Clients	4.3.0	none	acksys	6 mixed-b-g
	WLg-LINK	Access Point	ACKSYS Device	00:0E:8E:08:6B...	192.168.1.205	0 Clients	4.3.0	none	acksys	6 mixed-b-g

At the bottom left, it indicates "2 product(s)".

Select the device to upgrade, and click on « Upgrade ».

The screenshot shows a window titled 'Upgrade' with a blue header bar. Inside, there is a table with three columns: 'MAC address', 'Name', and 'IP address'. Below the table is a section titled 'Upgrade parameters' containing a text box for 'Upgrade file name' (with a browse button) and a password field. Below that is an 'Upgrade status' section with a large empty text area. At the bottom are three buttons: 'Upgrade', 'Upgrade All', and 'Close'.

MAC address	Name	IP address
00:0E:8E:08:6B:D6	ACKSYS Device	192.168.1.201
00:80:48:47:8B:6F	ACKSYS Device	192.168.1.202

**Upgrade parameters**

Upgrade file name:  ...

Password:

**Upgrade status**

Select the correct file to be loaded, then click on « Upgrade ».

If you want to upgrade several devices, select all the devices to be upgraded and click on « Upgrade All ».

Comment: To update several devices at one time with the same file the same password is needed.

All configuration parameters will be kept after the update.

### VII.3 Recovering a product after an upgrade problem

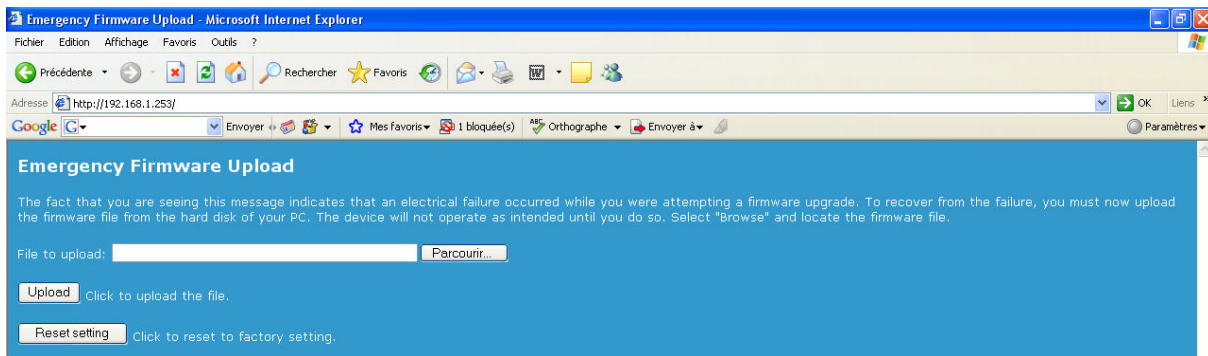
If the upgrade fails to correctly write the EPROM, which occurs most often when the power supply is switched off during the upgrade, an emergency upgrade mode is automatically enabled (as from the firmware update 3.2.0).

At first the reboot after the upgrade will fail and your device will detect that the EPROM is corrupted. It will launch the emergency upgrade mode; only allowing a firmware upgrade via an embedded web server.

The emergency upgrade mode is signaled by the DIAG led blinking fast (it is turned off in normal mode).

If you wish to access to this emergency mode please do the following:

In a web browser (internet explorer, Netscape, Firefox...), go to « 192.168.1.253 ». If you cannot reach this address check that your IP address is in this format: 192.168.1.xxx. If not, change it in your network settings.



Select the firmware file in the « file to upload » field and select 'upload'.

All the settings are kept unless they were in the EPROM corrupted area. In this case the default settings will be restored.

Once done, the release of the uploaded firmware can be verified in the TOOLS→firmware menu. Before accessing the product, make sure that you restore your computer IP configuration, in case it has been changed.

Since 4.4.0 release, you can restore the factory settings by selecting "Reset setting".