

# ACCESS POINT/BRIDGE/REPEATER USER GUIDE

## 지원 모델

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



# 목차

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Device Installation on the Network</b>	<b>3</b>
<b>3</b>	<b>New IP Configuration</b>	<b>3</b>
<b>4</b>	<b>WEB Administration</b>	<b>4</b>
4.1	WEB Configuration Structure	5
4.2	Help	6
4.3	LAN Settings	6
4.4	Wireless Settings	6
4.4.1	Bridge or Access Point mode	8
4.4.1.1	Infrastructure mode	8
4.4.1.2	Ad-hoc mode	9
4.4.2	WDS mode	10
4.4.3	SSID	11
4.4.3.1	Broadcasting the SSID	11
4.4.4	802.11 mode	11
4.4.5	Super G and Super AG	12
4.4.6	Channels and International Compatibility	12
4.4.7	802.11b/g (2.4GHz)	12
4.4.8	802.11a/h (5GHz)	13
4.5	Wireless Security	14
4.5.1	MAC ID Filtering	14
4.5.1.1	MAC Address Filter	14
4.5.1.2	WEP & WPA & WPA2 Encryption	16
4.5.1.3	WEP Encryption	16
4.5.1.4	WPA/WPA2 Encryption	17
4.5.1.4.1	Security in Pre-Shared Key mode (PSK)	18
4.5.1.4.2	EAP Extensions under WPA and WPA2 Enterprise	18
<b>5</b>	<b>SNMP Monitoring and Management</b>	<b>20</b>
5.1	MIB (Management Information Bases)	20
5.2	SNMP Community	20
5.3	SNMP Trap	20
5.4	SNMP Menu	21
5.5	Traps Management	21
5.6	Enterprise MIB ACKSYS	22
<b>6</b>	<b>Factory Default Settings</b>	<b>26</b>
<b>7</b>	<b>Device Upgrade</b>	<b>27</b>
7.1	By the WEB Interface	27
7.2	By Locator	27
7.3	Recovering a Product after an Upgrade problem	28
7.4	전원 연결	29

# 1 INTRODUCTION

본 매뉴얼은 아래의 무선 제품군에 적용이 가능합니다.

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

제품 설치 및 설정 시 아래의 문서를 참고하시고 기타 문의 사항은 [tech@witree.co.kr](mailto:tech@witree.co.kr)로 연락 주시기 바랍니다.

- User Guide (본문서, 당사 홈페이지 [www.witree.co.kr](http://www.witree.co.kr)에서 다운로드 가능)
- Quick 매뉴얼 (제품 패키지에 포함)
- Help 도움말 (제품 내부의 WEB 설정 페이지에 구현)

전원공급, 안테나 및 케이블 연결과 관련된 사항은 모델 별로 제공되는 Quick 매뉴얼을 참고하시기 바랍니다.

# 2 DEVICE INSTALLATION ON THE NETWORK

제품을 Ethernet HUB 혹은 PC의 LAN 포트에 연결한 후 전원을 인가합니다.  
Quick 매뉴얼에서 각 제품마다 간단하게 설치할 수 있는 정보들을 참고하시기 바랍니다.

**※ 주의**

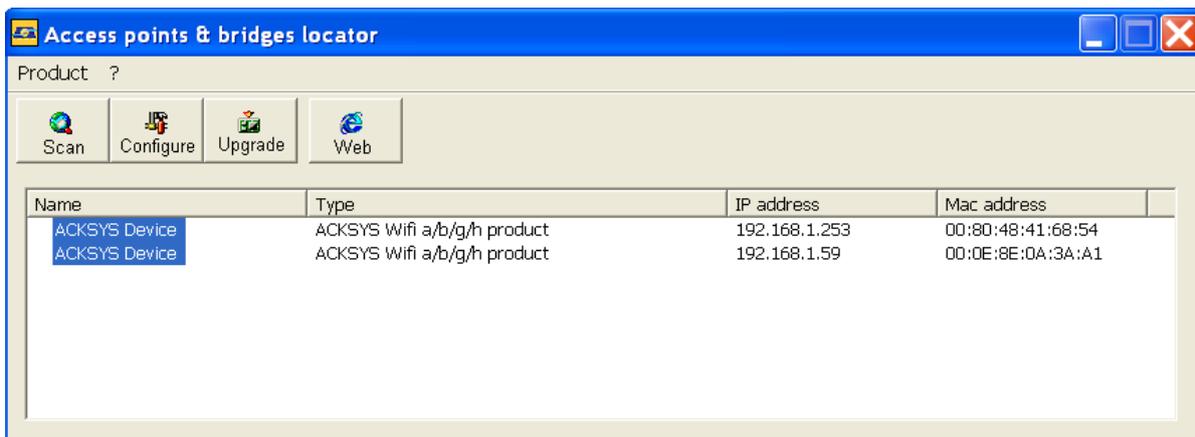
PoE 기능을 지원하는 HUB에 제품을 연결할 경우 제품의 LAN 포트가 PoE 기능을 지원하는지 확인하시기 바랍니다.

WLg-ABOARD/NP 모델은 PoE 기능을 지원하고 두 개의 LAN 포트 중 우측 한 개의 포트만 PoE 기능을 지원합니다.

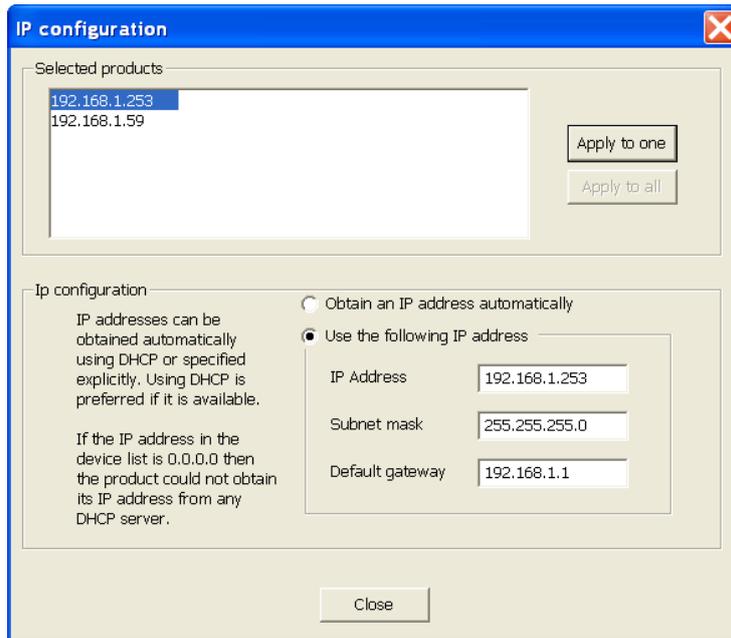
# 3 NEW IP CONFIGURATION

제품의 LAN 케이블을 네트워크에 연결한 후 올바르게 동작하기 위해서는 먼저 연결된 네트워크에서 사용할 수 있는 유효한 IP 주소를 설정해 주어야 합니다. **공장 출하시 제품은 기본 IP 주소(192.168.1.253)로 설정** 되어 있습니다.

CD-ROM에 포함되어 있는 Windows 기반의 “Locator” 응용 프로그램을 이용하여 쉽게 제품의 IP 정보를 변경하실 수 있습니다. 제품과 동일한 네트워크에 연결된 PC에서 “Locator” 응용 프로그램을 실행시킨 뒤 “Scan” 버튼을 클릭하시면 현재 네트워크에 연결되어 있는 장비들의 리스트가 화면에 표시됩니다.



“Locator” 응용 프로그램은 로컬 네트워크에 연결된 모든 Acksys 제품(AP, Bridge)을 화면에 표시합니다. 설정하려는 제품을 마우스로 선택하고 **“Configure”** 버튼을 클릭하여 제품의 IP 주소를 변경할 수 있습니다.



여러 개의 제품을 선택하고 **“configure”** 버튼을 클릭하면 **“Selected products”** 창에 선택된 여러 개의 제품 리스트가 표시됩니다.

각각의 제품을 한 개씩 따로 설정할 경우

**STEP1** “Selected products” 창에 표시된 제품 중에 IP 주소를 변경하려는 제품을 선택

**STEP2** 새로운 네트워크 정보(IP Address, Subnet mask, Default gateway 정보)를 입력

DHCP 서버로부터 IP 주소를 자동으로 받을 경우 **“Obtain an IP address automatically”** 를 선택

**STEP3** **“Apply to one”** 버튼을 클릭

“Selected products” 창에 표시된 모든 제품에 자동으로 IP 정보를 설정할 경우

**STEP1** “Selected products” 창에 표시된 제품 중에 한 개의 제품을 선택

**STEP2** **“Obtain an IP address automatically”** 버튼 클릭

**STEP3** **“Apply to all”** 버튼을 클릭

현재 네트워크에 적합한 IP 정보를 설정한 후 웹 브라우저를 통해서 세부적인 설정을 할 수 있습니다.

## 4 WEB ADMINISTRATION

“Locator” 프로그램에서 **“web”** 버튼을 클릭하거나, PC에서 웹 브라우저를 실행한 후 주소 창에 제품의 IP 주소를 입력하면 제품의 웹 설정화면에 접속할 수 있습니다. 제품에 연결되면 로그인 화면이 나타납니다. **공장 출하시 기본 값으로 설정된 User Name 은 “Admin” 이고 Password 는 없습니다.**



장비 설정을 위해서 아래의 정보들을 미리 알고 있어야 합니다.

- √ 무선 모드:
  - Infrastructure
  - Ad-hoc
- √ 무선 표준: 802.11a, 802.11b, 802.11g, 802.11b/g
- √ 무선 네트워크 SSID
- √ 무선 네트워크 채널 정보
- √ 보안 설정 (WEP, WPA, WPA2, 802.1x, MAC ID filtering)
- √ 제품 사용 모드:
  - Infrastructure 모드에서의 bridge 또는 access point
  - Ad-hoc 모드에서의 bridge

## 4.1 Web Configuration Structure

웹 설정 항목은 다음과 같이 구성되어 있습니다.

### BASIC :

#### WIZARD

LAN : TCP/IP 주소 설정

DHCP : DHCP 서버 설정 (브리지 모드에서는 사용할 수 없습니다.)

WIRELESS : Wi-Fi 설정

SNMP : SNMP agent 설정

### ADVANCED :

MAC ADDRESS FILTER : Access Point 모드에서 MAC 주소 필터링 설정

ADVANCED WIRELESS : Advanced wireless 설정

### TOOLS :

ADMIN : admin 또는 다른 유저 계정에 대한 패스워드 설정

파일을 이용하여 모든 설정 정보를 백업하고 재저장 가능

TIME : 시간 설정

SYSTEM : 공장 초기화 상태로 제품을 되돌리거나 제품을 재부팅

FIRMWARE : 현재 펌웨어 버전 표시, 새로운 펌웨어 업로드

### STATUS :

DEVICE INFO : 제품 기본 정보를 표시 (IP 정보, 무선 정보)

WIRELESS : 제품 주위에서 감지된 AP 정보들을 표시

LOGS : 제품에서 발생하는 이벤트에 대한 로그 정보 표시

STATISTICS : 제품을 경유하는 송수신 패킷에 대한 정보 표시

### HELP :

MENU : 각 메뉴에 대한 설명

BASIC : BASIC 메뉴에 대한 설명

ADVANCED : ADVANCED 메뉴에 대한 설명

TOOLS : TOOLS 메뉴에 대한 설명

STATUS : STATUS 메뉴에 대한 설명

GLOSSARY : 기술적 용어 대한 설명

각 메뉴 사이의 전환은 메인 메뉴를 클릭한 후 해당하는 서브 메뉴를 클릭하여 이동합니다.

몇몇 항목은 제품을 access point 혹은 bridge 모드로 선택하는 것에 따라 표시되지 않습니다. 예를 들어 **BASIC** → **DHCP** 메뉴와 **ADVANCED** → **MAC ADDRESS FILTER** 메뉴는 제품을 bridge 모드로 설정할 경우 사용할 수 없습니다.

## 4.2 Help

각 메뉴들에 대한 설명이나 기술적 용어들을 설명합니다.

## 4.3 LAN Settings

LAN 설정에서는 제품의 IP Address 모드(고정 IP 주소, 자동 IP 주소 받기), IP Address, Subnet Mask, Gateway 정보를 설정합니다. [BASIC](#) → [LAN](#) 페이지에서 설정할 수 있습니다.

**LAN SETTINGS**

IP Address Mode :  Static  DHCP

IP Address :

Subnet Mask :

Gateway :

Local Domain Name :  (optional)

### IP Address Mode

**Static (Manual)** : DHCP 서버를 사용하지 않고 네트워크 정보를 수동으로 설정  
IP Address, Subnet Mask, Gateway 설정 필수

**DHCP (Dynamic)** : 현재 네트워크의 DHCP 서버로부터 IP 주소를 자동으로 설정

### ※ 주의

만약 [BASIC](#) → [DHCP](#) 페이지에서 **DHCP Server** 를 **Enable**로 설정 하였다면 이 항목에서 **DHCP**를 선택할 수 없습니다. 제품에서 **DHCP** 서버와 클라이언트를 동시에 실행 할 수는 없습니다.

**IP Address** : 현재 네트워크에서 다른 장비에 사용되지 않는 유효한 IP 주소 입력

**Subnet Mask** : 현재 네트워크의 서브넷 마스크 입력

**Gateway** : 현재 네트워크의 게이트웨이 IP 주소 입력

**Local Domain Name (옵션)** : 현재 네트워크의 도메인 이름 입력

제품 내부에 구현된 DHCP 서버는 이곳에 입력한 도메인 이름을 제품에 연결되는 유무선 클라이언트 시스템에 부여합니다. 즉, 사용자가 mynetwork.net 이란 도메인을 이름을 이 항목에 설정한 후, alan 이란 이름의 무선 클라이언트 시스템을 제품에 연결하면 그 클라이언트 시스템은 alan.mynetwork.net 이란 이름으로 식별됩니다. 하지만 제품이 전체 네트워크의 DHCP 서버로부터 자동으로 IP 주소를 할당 받는 것으로 설정되어 있으면 제품에 설정된 도메인 이름에 상관없이 전체 네트워크가 할당하는 도메인 이름이 클라이언트에 부여됩니다.

## 4.4 Wireless Settings

이 장에서는 무선과 관련된 정보를 설정합니다. 이 항목에서 무선 관련 정보를 수정할 경우 수정된 정보를 무선 클라이언트 제품에도 적용시켜야 합니다.

무선 네트워크 보안이 필요할 경우 “wireless security mode” 를 설정합니다. WLg 시리즈 제품은 WEP, WPA-Personal, WPA-Enterprise 등 세가지 보안 모드를 지원합니다. WEP 은 가장 기본적인 무선 보안을 제공하고 WPA 는 더 높은 수준의 보안을 위해서 사용됩니다. WPA-Personal 은 별도의 보안 서버가 필요하지 않지만, WPA-Enterprise 를 사용할 때에는 RADIUS 라고 불리는 보안 서버가 따로 필요합니다.

### Enable Wireless Radio

이 항목은 제품의 무선 기능을 활성화 하거나 비활성화 합니다. disable 로 설정하면 제품의 무선 기능은 모두 사라지게 됩니다.

**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 A G H™ Mode :

Region / Country :

Auto Channel Select :

Channel :

Antenna :

Transmission Rate :  (Mbit/s)

### Wireless Network Name

사용자가 무선 네트워크를 검색했을 때 표시되는 무선 네트워크 이름을 SSID 라고도 합니다. AP 와 클라이언트는 같은 SSID 정보를 공유합니다. 제품 출하시 기본값은 “acksys”로 설정 되어 있으며 보안을 위해서 네트워크 이름을 변경할 것을 권장합니다.

### Visibility Status

이 항목을 이용하여 제품에 설정된 무선 네트워크(SSID)를 외부에 검색되지 않도록 할 수 있습니다. Visible 로 설정되어 있을 경우 무선 시그널 범위 내의 모든 무선단말기에 SSID 를 브로드캐스트 하기 때문에 암호화를 사용하지 않는 네트워크는 보안에 매우 취약하게 됩니다. Invisible 로 설정하면 제품은 SSID 를 브로드캐스트 하지 않으며 외부의 무선 클라이언트에서 무선 네트워크를 검색해도 제품의 SSID 가 보이지 않습니다. 하지만 SSID 를 알고 있는 클라이언트 장비에서 동일한 SSID 정보를 직접 입력하면 제품과 연결이 가능해 집니다.

### Auto Channel Select

이 항목을 설정하면 AP 는 무선 간섭이 가장 적은 채널을 자동으로 검색하여 사용합니다. 해제할 경우 AP 는 Channel 항목에 지정된 채널을 사용합니다.

### Channel

클라이언트들과 통신하기 위한 무선 채널을 설정합니다. 일반적으로 무선 채널은 주변 환경 및 인접한 무선 장치들에 의하여 간섭을 받게 됩니다. 효율적인 무선 네트워크를 구성하기 위하여 간섭이 적은 채널을 설정 하시기 바랍니다.

### Transmission Rate

기본값인 Best(automatic)는 현재 무선 상태에서 최적의 전송속도를 자동으로 설정합니다. 또한 통신에 필요한 전송 속도를 수동으로 설정할 수도 있습니다.

### 802.11 Mode

802.11a/b/g 무선 표준 모드를 설정합니다. 모든 클라이언트 장비가 802.11g 모드를 사용할 경우 802.11g only 로 설정이 가능하며 802.11b 와 802.11g 모드의 장비가 혼용될 경우 Mixed 802.11g and 802.11b 를 선택합니다.

### Super AG™ Mode

Super AG 모드를 설정하면 Atheros 칩을 사용하는 무선 장비간에 최대 108Mbps 의 속도로 통신할 수 있습니다.

### WEP

WEP 은 무선 데이터를 암호화하는 방법중의 하나로서 유선 네트워크 레벨의 보안수준을 제공합니다. WEP 보안을 사용하는 네트워크에 접근하기 위해서는 보안 key 값을 미리 알고 있어야 합니다.

### 4.4.1 Bridge or Access Point mode

제품의 기본 모드는 “ACCESS POINT” 입니다. 브리지 모드로 변경하기 위해서는 “BRIDGE” 버튼을 클릭합니다.

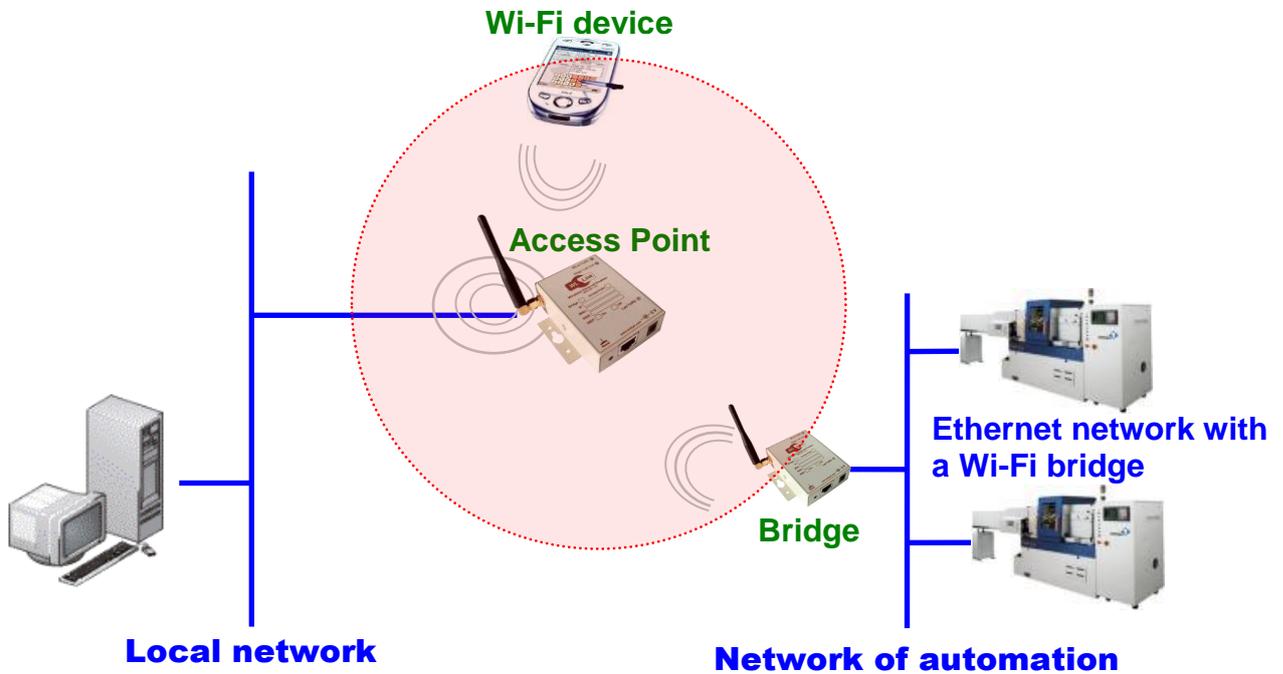
Bridge 모드를 선택할 경우 제품은 Bridge 모드로 자동 재부팅 합니다. 제품이 Access Point 로 설정되어 있을 경우 웹 접속 시 Access Point 배너가 표시되며 Bridge 모드로 설정되면 Bridge 모드 배너가 표시됩니다. Bridge 모드로 재부팅 후 “Wireless Mode” 항목이 아래와 같이 설정할 수 있도록 활성화 됩니다.



#### 4.4.1.1 Infrastructure mode

Infrastructure 네트워크는 아래와 같이 두 종류의 요소로 구성할 수 있습니다.

- Access Point (ACKSYS Access Point 는 최대 20 개의 클라이언트까지 연결 가능)
- Access Point 에 연결된 Wi-Fi 클라이언트 (Bridge 에 유선 케이블로 연결된 랜장비는 무선랜 장비처럼 동작)



ACKSYS 제품은 :

- ACCESS POINT 모드 설정을 통해 access point 로 동작
- BRIDGE 모드와 Infrastructure 모드 설정을 통해 무선 Bridge 로 동작

Infrastructure 무선 네트워크 모드는 무선 네트워크를 유선 네트워크에 연결시켜줍니다. 또한 Infrastructure 무선 네트워크 모드는 무선랜 클라이언트 장비들을 AP 를 통하여 중앙 집중화 시켜줍니다.

Infrastructure 무선 네트워크를 구성하기 위해서는 Access Point 가 필요합니다. 무선랜에 접속하기 위해서 Access Point 와 Access Point 에 연결되는 무선 클라이언트 장비는 모두 동일한 SSID 를 설정해야 합니다. Access Point 의 랜포트를 유선 네트워크에 연결하여 무선 클라이언트 장비들도 유선 네트워크에 접속이 가능하게 됩니다. 무선랜에 Access Point 를 추가하면 Infrastructure 무선 네트워크의 서비스 영역을 확장할 수도 있으며 무선 클라이언트 수도 증가 시킬 수 있습니다.

Ad-hoc 무선 네트워크와 비교하여 Infrastructure 무선 네트워크는 Ad-hoc 무선 네트워크와 비교하여 확장성, 중앙관리, 보안, 서비스 영역 등에서 많은 장점을 가지고 있습니다.

### 4.4.1.2 Ad-hoc mode

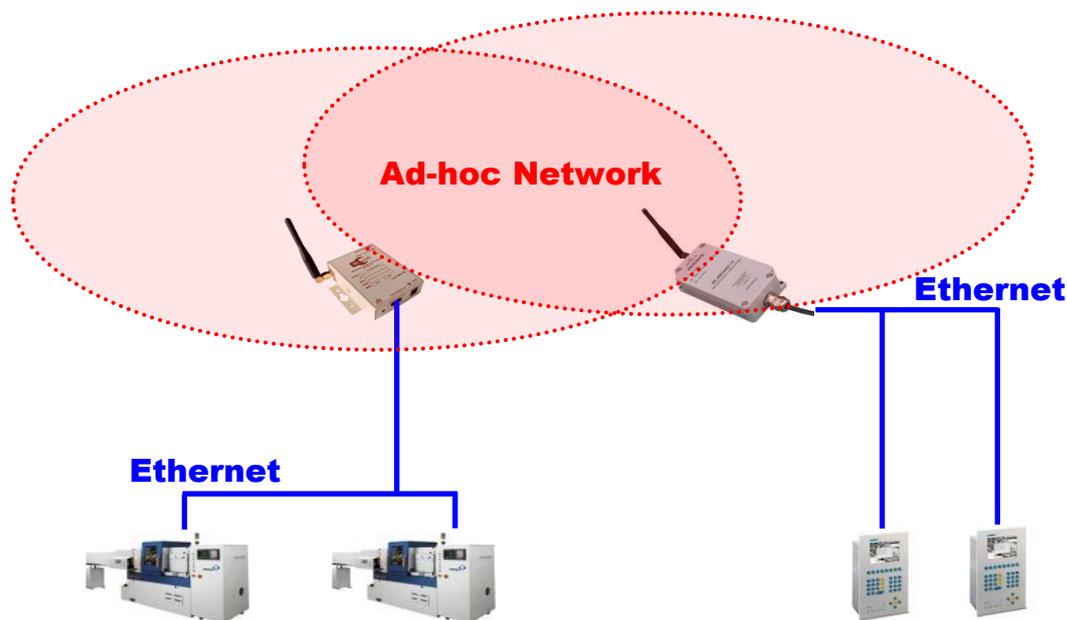
Ad-hoc 모드는 각각의 무선 장치가 1:1 로 직접 무선으로 통신하는 방식입니다. Ad-hoc 모드의 장치들은 별도의 Access Point 의 인증 없이도 일정 무선 통신 범위 내에서 자신과 통신할 Ad-hoc 장치를 검색하여 peer-to-peer 통신을 하게 됩니다.

Ad-hoc 무선 네트워크를 구축하기 위해서는 통신하려는 각각의 제품을 모두 Infrastructure 모드 대신 Ad-hoc 모드로 설정하셔야 합니다. Ad-hoc 모드는 제품을 Bridge 방식으로 사용할 경우에만 설정할 수 있습니다.

**※ 주의**

Ad-hoc 으로 연결하려는 두 대의 무선 장비는 동일한 SSID 와 채널 번호를 설정하여야 합니다. 한 개의 Ad-hoc 네트워크는 두 대의 무선 장치로 구성됩니다. 따라서 원활한 통신이 이루어지기 위해서는 한 개의 장치가 또 다른 상대방 장치의 신호전달 범위 내에 위치해야만 합니다. Ad-hoc 모드는 802.11b 무선 모드에서만 동작하며 WEP 방식 이외의 암호화를 사용하지 않습니다.

Ad-hoc 네트워크를 구성하는 두 대의 제품은 반드시 동일한 SSID 와 채널을 공유해야 합니다. 또한 하나의 제품에서 발생하는 무선 신호는 상대방 제품까지 반드시 도달해야 합니다. 만약 두 대의 제품이 신호가 도달할 수 없을 정도로 떨어진 경우 신호 경로 중간에 무선 신호를 릴레이 할 수 있는 장치를 설치하는 것도 Ad-hoc 모드에서는 사용이 불가능 합니다. 무선 신호를 릴레이 하는 기능이 필요할 때에는 Infrastructure 모드에서 WDS Repeater 기능을 활용하실 수 있습니다.(4.4.2 WDS mode 참조)



### 4.4.2 WDS mode

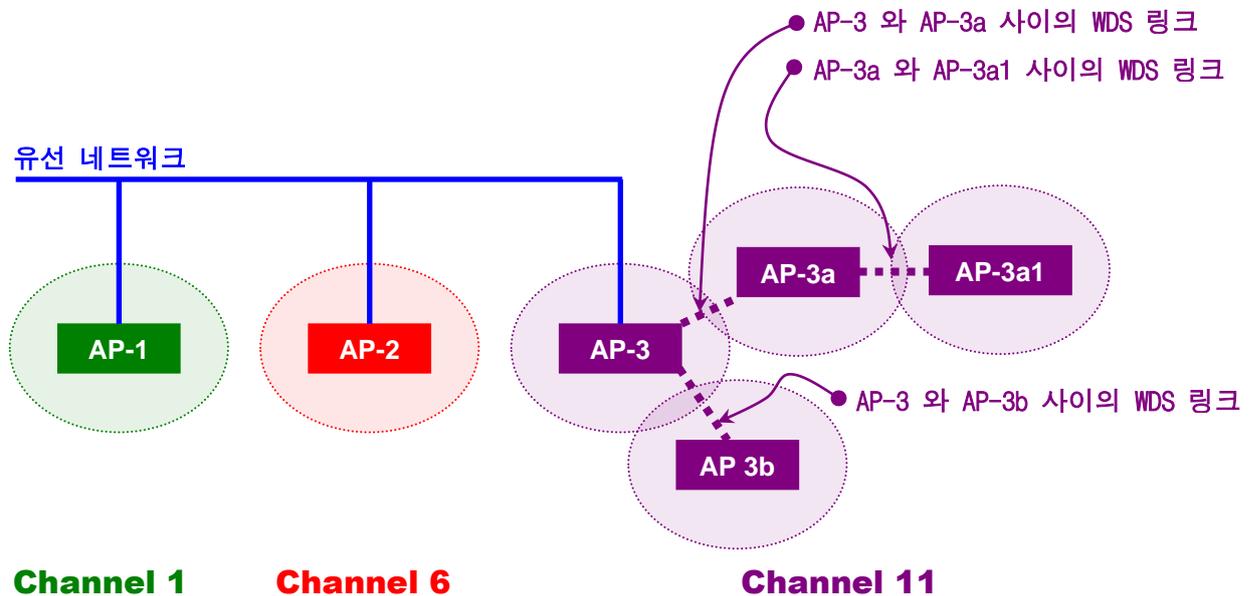
WDS(Wireless Distribution System)는 IEEE802.11 무선 네트워크에서 AP 들 간의 상호 무선 연결을 가능하게 해주는 시스템입니다. 기존에는 무선 네트워크를 확장하기 위해서 유선 네트워크에 AP 를 추가로 연결하여 무선 네트워크를 확장하였습니다. 하지만 WDS 기능을 이용하면 유선 네트워크에 AP 를 연결하지 않고 단순히 AP 를 추가시키는 것만으로도 무선 네트워크 영역을 확장 할 수 있습니다. WDS 기능의 특징은 클라이언트 장비의 MAC 주소를 AP와 AP를 옮기더라도 계속 유지 할 수 있다는 것입니다. 따라서 이동성이 많은 환경에 무선을 설치할 경우 매우 유용하게 활용할 수 있습니다.

AP 는 주 스테이션, 중계 스테이션, 원격 스테이션 등으로 동작할 수 있습니다. 주 스테이션은 보통 유선 네트워크에 연결되고, 중계 스테이션은 주 스테이션이나 다른 중계 스테이션으로부터 원격 스테이션이나 무선 클라이언트, 또 다른 중계 스테이션으로 데이터를 중계해주는 역할을 합니다. 원격 스테이션은 연결된 무선 클라이언트들의 데이터를 중계 스테이션이나 주 스테이션으로 전송합니다. 스테이션과 클라이언트들 간의 연결은 클라이언트의 IP 정보를 사용하지 않고 MAC 주소 값을 사용하게 됩니다.

WDS 시스템의 모든 스테이션은 동일한 무선 채널을 사용해야 하며, WEP 보안 설정이 되어 있다면 Key 값을 공유해야 합니다. 하지만 SSID 는 다르게 설정할 수 있습니다. 또한 WDS 시스템에서는 최소한 한 개의 스테이션이 다른 한 개의 스테이션과 유무선으로 링크될 수 있도록 설치하여 모든 스테이션이 유무선으로 링크될 수 있도록 구성해야 합니다(하단 그림 참조).

WDS 는 무선 클라이언트의 접속을 허용하면서도 AP 간을 상호 연결하는 기능을 제공하기 때문에 리피터로 불리기도 합니다. 하지만 주의할 것은, 시스템 내의 모든 스테이션은 동일한 채널을 사용하기 때문에 최대 데이터 전송률은 스테이션을 거칠 때마다 2 배 감소하게 됩니다. 예를 들어, 클라이언트가 중계 스테이션을 경유하여 주 스테이션으로 데이터를 전송하면 주 스테이션에 직접 연결된 것과 비교하여 거의 1/2 정도로 최대 데이터 전송률이 감소합니다. 만약 클라이언트가 2 개의 중계 스테이션을 경유하여 주 스테이션에 데이터를 전송하게 된다면 최대 전송률은 기존의 1/4 정도로 감소하게 됩니다.

아래의 그림은 3 개의 AP 영역으로 구성되어 있으며, 오른쪽 한 개의 영역은 WDS 로 서비스 영역을 확장하였습니다.



- 위 그림에서 AP-3 영역은 3 개의 WDS 링크로 구성되어 있습니다.
- √ AP-3 에는 AP-3a 와 AP-3b 의 MAC 주소 값을 설정해야 합니다.
- √ AP-3a 에는 AP-3 와 AP-3a1 의 MAC 주소 값을 설정해야 합니다.
- √ AP-3a1 에는 AP-3a 의 MAC 주소 값만 설정하면 됩니다.
- √ AP-3b 에는 AP-3 의 MAC 주소 값만 설정하면 됩니다.

한대의 ACKSYS AP 에는 최대 6 개의 MAC 주소 값을 저장할 수 있습니다.

### 4.4.3 SSID

SSID(service set identifier) 는 802.11 무선랜을 구분하는 이름으로서, 사용자는 SSID 를 이용하여 특정 네트워크에 접속할 수 있습니다. 클라이언트 장비에 미리 저장된 SSID 가 있다면 해당 SSID 를 가진 AP 로 접속을 시도합니다. 저장된 SSID 가 없다면 클라이언트 장비는 주변의 모든 AP 들이 브로드캐스팅 하는 메시지에서부터 SSID 정보를 받은 후 사용자가 선택한 AP 로 접속을 시도합니다.

#### 4.4.3.1 Broadcasting the SSID

기본적으로 SSID 는 무선 클라이언트가 네트워크에 원활하게 접속할 수 있도록 AP 의 beacon 프레임에 포함되어 브로드캐스팅 됩니다.

하지만 **Visibility Status** → **invisible** 를 선택하면 AP 가 SSID 를 브로드캐스팅 하지 않습니다. AP 가 자신의 SSID 를 브로드캐스팅 하지 않으면 클라이언트 장비에서 AP 를 검색하여도 해당 SSID 가 검색되지 않습니다. 따라서 이 기능을 사용할 경우 사용자는 미리 정확한 SSID 를 알고 있어야 하며, 클라이언트 장비에서는 연결하려는 SSID 를 수동으로 입력해야 합니다.

그러나 단순히 SSID 를 브로드캐스팅 하지 않는 기능만으로 무선 네트워크의 보안을 지키기는 어렵습니다. 허가 받지 않은 클라이언트가 정확한 SSID 를 이미 알고 있다면 수동으로 SSID 를 입력하는 것만으로도 쉽게 AP 에 접속할 수 있기 때문입니다. 따라서 WPA 와 같은 데이터 암호화 기능을 함께 사용하시는 것을 권장합니다.

### 4.4.4 802.11 mode

다음 3 가지 모드를 사용할 수 있습니다.

➤ 802.11b

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 의 최대 데이터 전송률은 11 Mbit/s 입니다.

802.11b 를 사용하는 장비는 2.4 GHz 대역을 사용하는 다른 장비들 (전자레인지, 블루투스 무선장치, 베이비 모니터, 구형 무선전화기) 들의 영향을 받을 수 있습니다.

➤ 802.11g

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

802.11g 는 802.11b 와 같은 2.4GHz 영역을 사용하지만 최대 무선 전송 속도는 54 Mbit/s 이며, 평균 Throughput 은 대략 19 Mbit/s 입니다. 그리고 802.11g 장비는 802.11b 장비와 완벽하게 호환합니다. 802.11g 는 802.11b 와 마찬가지로 2.4GHz 대역을 사용하는 다른 장비들의 영향을 받을 수 있습니다.

➤ 802.11a

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

802.11a 는 5 GHz 대역의 주파수를 사용하고 최대 전송 속도는 54 Mbit/s 이며, 평균 Throughput 은 25 Mbit/s 정도 입니다.

무선네트워크의 사용이 폭발적으로 증가하면서 2.4GHz 보다 상대적으로 사용이 적은 5GHz 대역을 사용하는 것이 중요한 장점이 되었습니다. 그러나 802.11a 대역의 신호는 벽이나 기타 지형지물에 더 쉽게 흡수되는 경향이 있어 802.11b 만큼 신호가 멀리 도달되지 않는 단점이 있습니다.

### 4.4.5 Super G and Super AG

Super G 기능은 Atheros 칩 제조사가 802.11g 무선 네트워크의 성능을 향상시키기 위해 개발한 frame-bursting, compression, channel bonding 기술입니다. Super G 모드를 사용하면 108Mbit/s 로 속도를 설정했을 때 40Mbit/s-60Mbit/s 정도의 성능이 보장됩니다.

Super G 기능을 지원하는 제품은 제조사가 다르더라도 같이 사용할 수가 있습니다. Atheros 사는 자사의 802.11a/g 칩셋에 이 기능을 적용하였고 Super AG 로 명칭하고 있습니다.

Super AG 모드를 사용 하려면 모든 Wi-Fi 장비가 Atheros 사의 칩이나 또는 호환하는 칩셋을 사용해야 합니다.

Super AG 는 다음 세가지 모드로 사용할 수 있습니다.

- Without turbo : 터보 모드 OFF
- Dynamic turbo : 터보 모드가 사용 가능한지 자동으로 검색하여 설정
- Static turbo : 터보 모드 ON

Super AG 모드에서 사용 가능한 데이터 전송률은 108 Mbps, 96 Mbps, 72 Mbps, 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps and 6 Mbps 입니다.

### 4.4.6 Channels and international compatibility

세계 각 국가들은 자국내의 다양한 무선 서비스를 위하여 주파수 대역을 스스로 제한하고 관리 하기 때문에 Wi-Fi 무선제품이 사용할 수 있는 무선 채널은 각 국가 별로 다르게 규정하고 있습니다.

그러나 아래와 같이 크게 세 지역으로 분류할 수 있습니다.

- Europe ( ETSI 에서 규정 )
- US (FCC 에서 규정)
- Asia (MKK/TELEC 에서 규정)

사용 가능한 채널은 [region/country](#) 메뉴에서 해당 국가나 지역을 선택하면 자동으로 표시 됩니다.

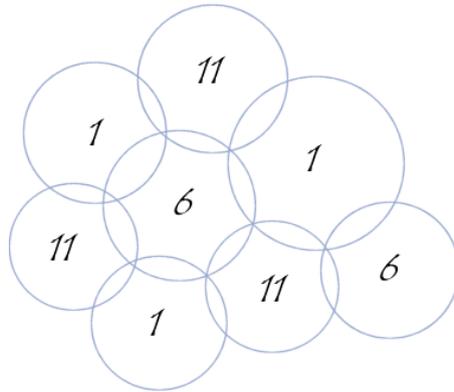
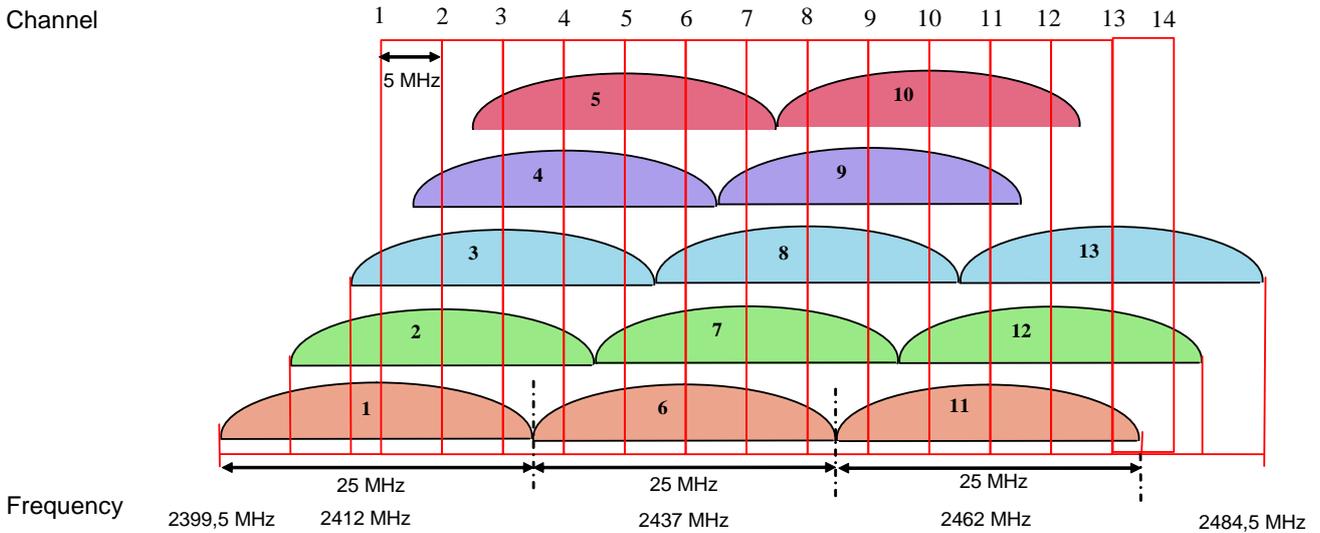
**제품의 설치장소(실내/실외)에 따라서도 사용 가능한 채널이 변경될 수 있습니다. 각 국가별 전파 관련 법규를 참고 하시기 바랍니다.**

### 4.4.7 802.11b/g (2.4GHz)

802.11 b/g 네트워크는 2.3995-2.4965 GHz 의 ISM(Industrial Scientific and Medical) 주파수 대역을 사용합니다.

Channel (25MHz)	Central Frequency (GHz)	Allow 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

채널 간의 간섭을 피하기 위해서는 주변 채널과 4~5 채널 떨어져 있는 것을 사용할 것을 권장하며, 일반적으로 채널간의 간섭이 발생하는 지역에서는 1, 6, 11 번과 같이 채널을 사용합니다.



### 4.4.8 802.11a/h (5 GHz)

802.11 a/h 네트워크는 5Ghz 의 UN-II(Unlicensed-National Information Infrastructure) 주파수 대역을 사용합니다.

Channel	Central Frequency (GHz)	Power	Allow 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)	Europe (ETSI)	Japan (TELEC)
13 channels	19 channels	4 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 GHz ] Called U-NII III	[ 5.150 to 5.350 GHz ] [ 5.500 to 5.725 GHz ]	[ 5.150 to 5.250 GHz ]

### 4.5 Wireless security

무선 네트워크의 보안을 위한 기술들은 많이 있습니다. 그러나 어떠한 방법도 절대적인 안전을 보장하지는 않습니다. 여러 보안 기술들을 적절히 조합해서 사용하는 방법이 현재로서는 가장 안전한 대책입니다.

무선 네트워크를 안전하게 사용하기 위한 지침:

- 모든 무선 장비에 보안을 설정합니다
- 모든 무선 장비 사용자는 무선 보안에 대한 교육을 받아야 합니다.
- 모든 무선 네트워크는 취약점과 허가 받지 않은 시스템의 접근을 모니터링 해야 합니다.

무선 보안을 위해 사용 가능한 대책들 :

- Not broadcasting the SSID ( 0 참조 )
- MAC ID filtering
- WEP encryption
- WPA with 802.1x authentication or PSK
- WPA2 with 802.1x authentication or PSK

#### 4.5.1 MAC ID filtering

ACKSYS AP 는 특정한 MAC 주소를 가진 장비만이 AP 에 접근이 가능하도록 하는 MAC address filter 기능을 포함하고 있습니다. 하지만 MAC 주소는 네트워크를 통해서 위조될 수도 있습니다.

MAC 주소를 통한 필터링은 AP 에 사전 등록된 MAC 주소 값과 AP 에 접근하려는 장비의 MAC 주소 값을 비교하여 등록된 장비만을 네트워크에 접근하거나 접근할 수 없도록 필터링 합니다. 이 기능은 허가되지 않은 무선 장비가 당신의 네트워크로 접속하는 것을 차단할 때 유용하게 사용할 수 있습니다. MAC 주소는 네트워크 장비의 제조사가 각 장비마다 부여한 고유의 ID 입니다.

##### 4.5.1.1 MAC ADDRESS FILTER

이 메뉴는 제품이 Access Point 모드로 설정되었을 때만 사용이 가능합니다.

**※ 주의**

이 기능을 잘못 사용할 경우 유무선의 모든 장비가 네트워크로의 접근이 차단될 수 있습니다. 접속이 불가능할 경우 Access Point 를 Factory Default 상태로 변경해야 합니다.  
AP 를 설정 및 관리하는 PC 가 접속할 수 있도록 필히 설정하시기 바랍니다.

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 : only allow listed machines

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	

### Enable MAC Address Filter

이 기능이 설정하면 filter 모드에 따라 유무선 네트워크 장비의 접근이 허용되거나 거부됩니다.

### Mode

only allow listed machines : 사용자가 등록한 MAC 주소를 가진 장비만 네트워크로의 접근을 허용합니다.

only deny listed machines : 사용자가 등록한 MAC 주소를 가진 장비만 네트워크로의 접근이 거부됩니다.

### Filter Wireless Clients

이 옵션이 선택되면, 무선 네트워크 클라이언트에 MAC Filter 기능이 적용됩니다.

### Filter Wired Clients

이 옵션이 선택되면, 유선 네트워크 클라이언트에 MAC Filter 기능이 적용됩니다.

### Enable

리스트에 저장된 MAC 주소에 필터링을 사용할지 여부를 선택합니다.

### MAC Address

등록할 MAC 주소 값을 입력합니다. 현재 연결된 PC의 MAC 주소 값을 입력하려면 **Copy Your PC's MAC Address** 버튼을 클릭합니다.

### Save

새로 입력하거나 수정한 내용을 리스트에 저장합니다. 새로 입력한 값을 적용 시키려면 반드시 페이지 상단의 **Save setting** 버튼을 클릭해야 합니다.

### MAC Address List

현재 등록된 MAC 주소 값의 리스트를 보여줍니다. 우측의 **Edit, Delete** 아이콘을 클릭하여 개별 항목을 수정하거나 삭제할 수 있습니다. **Edit** 아이콘을 클릭하면 현재 선택된 MAC 주소 값이 위쪽의 **MAC Address** 창에 표시되고 수정 할 수 있습니다.

### 4.5.1.2 WEP & WPA & WPA2 encryption

아래의 암호화 방식은 제품의 설정 모드에 따라 달라질 수 있습니다.

**Access point 모드:**

WIRELESS SECURITY MODE

**Security Mode :**  None  WEP  WPA/WPA2-PSK  WPA/WPA2

- **None** : 보안 기능을 사용하지 않음
- **WEP** : WEP encryption
- **WPA/WPA2-PSK** : WPA 또는 WPA2 encryption without 802.1x authentication
- **WPA/WPA2** : WPA 또는 WPA2 encryption with 802.1x authentication

**Bridge & Infrastructure 모드:**

WIRELESS SECURITY MODE

**Security Mode :**  None  WEP  WPA/WPA2-PSK

- **None** : 보안 기능을 사용하지 않음
- **WEP** : WEP encryption
- **WPA/WPA2-PSK** : WPA 또는 WPA2 encryption without 802.1x authentication
- **WPA/WPA2** : 사용할 수 없음

**Bridge & Ad-Hoc 모드:**

WIRELESS SECURITY MODE

**Security Mode :**  None  WEP  WPA/WPA2-PSK

- **None** : no security
- **WEP** : WEP encryption
- **WPA/WPA2-PSK** : 사용할 수 없음
- **WPA/WPA2** : 사용할 수 없음

### 4.5.1.3 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 은 무선통신에서 데이터를 암호화하는 방법 중의 하나이며 유선 네트워크 수준의 보안을 위해 고안 되었습니다. 그러나 WEP 은 WPA 방식만큼 안전하지는 않습니다. WEP 네트워크에 접속하기 위해서 AP 에 접속하려는 사용자는 WEP Key 값을 알고 있어야 하며 이 값은 AP 관리자가 생성한 문자열 입니다. WEP 을 사용할 때에는 암호화 레벨을 정해야 하고 이 암호화 레벨에 따라 Key 문자열의 길이가 달라집니다. 128-bit encryption 은 64-bit encryption 보다 긴 문자열을 필요로 합니다.

Key 값은 ASCII (American Standard Code for Information Interchange - alphanumeric characters) 형식의 문자열 또는 HEX (16 진수 : 0-9, A-F 사이의 문자) 값으로 입력할 수 있습니다. 사용자가 기억하기 쉽도록 ASCII 형식의 문자열을 지원하며 이 문자열은 네트워크에서 HEX 코드로 변경되어서 사용됩니다. 사용자가 WEP Key 값을 쉽게 변경할 수 있도록 4 개의 Key 값을 미리 입력해 놓을 수 있습니다. 입력된 여러 개의 Key 값 중에서 "Default WEP Key" 에 선택된 Key 값이 사용됩니다.

**Authentication** : WEP 방식에서는 Open System 과 Shared Key 인증 방법이 있습니다. :

**Open System authentication** 에서는 무선 클라이언트가 인증 과정 중에 자신의 인증 정보를 접속하려는 Access Point 로 전송하지 않아도 됩니다. 즉 클라이언트는 자신의 WEP Key 와 상관없이 자기 자신과 Access Point 를 인증하고 연결을 시도할 수 있기 때문에 사실상 진정한 의미의 인증 과정은 발생하지 않습니다. 인증과 연결 절차가 끝난뒤 실제 데이터 프레임을 암호화 할때 WEP Key 가 사용 됩니다. 이 시점에서 클라이언트는 유효한 WEP Key 를 가지고 있어야 합니다.

**Shared Key authentication** 에서는 WEP Key 를 이용하여 아래의 4 단계 인증 절차가 진행됩니다.

STEP1 : 클라이언트는 인증 요청 메시지를 Access Point 로 전송

STEP2 : Access Point 는 Clear-Text Challenge 를 클라이언트로 전송

STEP3 : 클라이언트는 Clear-Text Challenge 를 WEP Key 를 이용하여 암호화 한 후 Access Point 로 전송

STEP4 : Access Point 는 수신한 데이터를 복호화(decoding) 하여 자신이 보낸 Clear-Text Challenge 와 비교 후 인증 성공 또는 실패 결과를 클라이언트에 전송

언뜻 보면 Open System authentication 은 실제 인증과정이 없기 때문에 Shared Key authentication 이 Open System authentication 보다 더 안전한 것처럼 보입니다. 하지만 실제로는 그 반대입니다. Shared Key authentication 에서는 악의적인 사용자가 위의 4 단계 메시지를 캡처하여 WEP Key 를 추출할 수도 있습니다. 그래서 WEP 암호화 방식을 사용할 때는 Open System authentication 을 사용하기를 추천합니다. 물론 위 두가지 방법 모두 WPA 방식에 비해 그다지 안전한 방법은 아닙니다.

#### 4.5.1.4 WPA/WPA2 encryption

WPA 는 무선 네트워크의 데이터 보호와 접근 제어를 상당 수준으로 높인 방법으로서 기존 WEP 방식의 모든 단점들을 보완하였습니다. WPA 방식은 WEP 방식의 취약점을 보완하기 위하여 강력한 데이터 암호화를 제공할 뿐만 아니라 사용자 인증을 보강하였습니다. WPA 는 802.11b, 802.11g, 802.11a, Multi-band, Multi-mode 를 포함하는 모든 802.11 장치의 보안을 위하여 디자인 되었습니다.

**WPA**

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

WPA Mode :

Cipher Type :

Group Key Update Interval :  (seconds)

WPA 는 구형 표준 방식으로서 Access Point 에 연결할 클라이언트가 구형 표준만을 지원할 경우 사용합니다.

**WPA2** 는 강력한 IEEE 802.11i 보안 표준을 적용한 새로운 인증방법입니다. WPA2 옵션을 선택하면 Access Point 는 먼저 WPA2 방식으로 인증을 진행합니다. 하지만 클라이언트가 WPA 방식만을 지원할 경우 WPA 방식으로 인증을 진행합니다. **WPA2 Only** 옵션을 선택하면 WPA2 보안을 지원할 수 없는 클라이언트의 인증은 거부됩니다.

**Cipher Type** 은 데이터 통신의 보안을 위해 사용되는 암호화 알고리즘 입니다. **TKIP** (Temporal Key Integrity Protocol) 은 WEP Key 를 각각의 패킷 단위로 빠르게 갱신하여 암호화 하는 방식입니다.

**AES** (Advanced Encryption Standard)은 128 bits 블록 단위로 암호화하는 매우 복잡하고 안전한 방법입니다. AES 방식은 구현이 쉽고 메모리를 적게 소모하는 장점을 가지고 있습니다. **TKIP and AES** 옵션을 선택하면 Access Point 는 클라이언트의 Cipher type 을 검사하고 AES 가 사용 가능하다면 AES 를 사용합니다.

다음 4 가지 보안 옵션이 사용 가능합니다.

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

Access point 모드에서, Group Key 변경 주기는 **Group Key Update Interval** 을 이용하여 조정이 가능합니다.

#### 4.5.1.4.1 Security in pre-shared key mode (PSK)

Pre-shared Key mode(PSK, also known as personal mode)는 802.1x 인증 서버를 필요로 하지 않은 가정이나 소규모 사무실에서 사용할 수 있도록 고안된 방법입니다. 사용자는 네트워크에 접속하기 위해서 반드시 8~63 개의 ASCII 문자나 64 개(256bits/4bits)의 HEX 코드로 구성된 비밀번호(Pre-Shared Key)를 입력해야 합니다. 무선 네트워크 안의 모든 Wi-Fi 장치는 동일한 Pre-Shared Key (PSK)를 가져야 합니다.

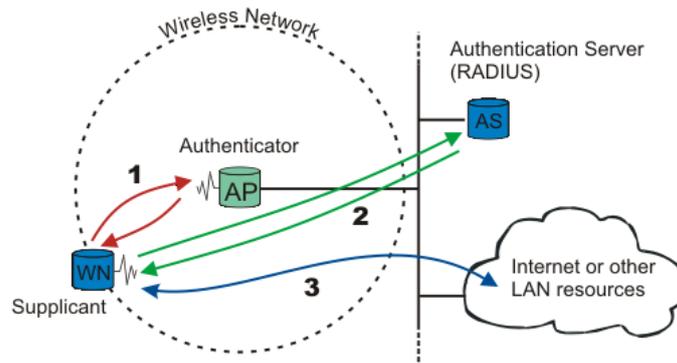


#### 4.5.1.4.2 EAP extensions under WPA- and WPA2- Enterprise

WPA/WPA2 또는 WPA/WPA2-Enterprise 는 802.1x 를 사용하여 LAN 포트에 연결된 장치를 Point-to-Point 방식으로 연결 하거나 인증이 실패할 경우 접근을 제한할 수 있습니다. 새로운 무선 노드(WN)가 LAN 에 접근을 요청하면 Access Point 는 새로운 무선 노드를 확인합니다. 무선 노드가 인증되기 전에는 EAP 인증 과정을 제외한 어떠한 트래픽도 발생하지 않습니다.

인증 프로세스는 다음의 몇 가지 요소들로 구성됩니다.

- User 또는 supplicant 또는 Wireless Node (WN)
- Wireless access point 또는 authenticator
- Authentication server, 대부분 RADIUS (Remote Authentication Dial-In User Service) 서버
- Authentication 처리 방식



**Supported authentication features**

- ACKSYS 제품은 Access Point 모드에서 authenticator 로 동작이 가능합니다.
- ACKSYS 제품은 Bridge 모드에서 supplicant 로 동작할 수 없습니다.

**Authentication 처리 방식**

EAP (Extensible Authentication Protocol) 방식 중에 한가지를 사용합니다. 보편적으로 사용되는 방식은

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

**EAP (802.1x)**

**EAP (802.1x) 메뉴는 제품이 Access Point 모드와 WPA/WPA2 로 설정되어 있을 때만 사용이 가능합니다.** 이 옵션은 무선 클라이언트를 인증하기 위한 RADIUS Server 를 대상으로 설정합니다. 무선 클라이언트들은 현재 설정 중인 Access Point(gateway)를 경유하여 서버로 인증을 요청하기 전에 Access Point 로부터 필요한 자격을 획득해야 합니다. 또한 이 Access Point(gateway)가 User 를 인증할 수 있는 권한을 가질 수 있도록 RADIUS Server 에서 Access Point 를 미리 설정해야 합니다.

**<< Advanced**

버튼을 클릭하여 Second RADIUS Server 를 설정할 수 있습니다.

### 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 :**

<< Advanced

**Optional backup RADIUS server:**

**Second RADIUS server IP Address :**

**Second RADIUS server Port :**

**Second RADIUS server Shared Secret :**

**Second MAC Address Authentication :**

- **Authentication Timeout** : 클라이언트가 인증을 요청한 후 응답을 대기하는 시간
- **RADIUS Server IP Address** : 인증 서버의 IP 주소
- **RADIUS Server Port** : 인증 서버의 접속 포트 번호
- **RADIUS Server Shared Secret** : 인증 서버 비밀번호
- **MAC Address Authentication** : 선택할 경우, 사용자는 무선 네트워크에 로그인할 때마다 현재 시스템과 동일한 MAC 주소를 가진 시스템을 이용해야 합니다.

## 5 SNMP MONITORING AND MANAGEMENT

일반적인 SNMP 의 구성은, 한 개 혹은 그 이상의 관리 시스템이 여러 개의 SNMP 클라이언트 시스템들을 관리 합니다. “agent” 라고 불리는 소프트웨어가 각 클라이언트 시스템에서 동작하고 SNMP 프로토콜을 이용하여 시스템 정보를 관리 시스템으로 전송합니다.

SNMP 를 이용하여 다음과 같은 작업을 수행할 수 있습니다.

- 디바이스의 상태 확인
- 디바이스의 설정
- 이벤트 관리

WLg 시리즈 제품은 SNMP agent 를 포함하고 있습니다.

### 5.1 MIB (Management Information Bases)

SNMP 자체만으로는 클라이언트 시스템이 어떠한 정보를 관리 시스템에 제공해야 할지를 알 수 없습니다. 그래서 SNMP 는 유효한 정보를 지정하기 위하여 MIBs(management information bases) 라고 불리우는 확장 가능한 구조를 사용합니다. MIBs 는 시스템의 관리 데이터 구조를 기술하며 OID(object identifiers) 를 포함하는 계층적 구조를 가지고 있습니다. 즉 OID 를 이용하면 SNMP 를 통해서 Read/Write 할 수 있는 정보를 확인할 수 있습니다.

당 제품은 MIB II 에 포함된 다음 그룹을 사용합니다.

- System, OID .1.3.6.1.2.1.1, 시스템 정보 포함
- IP, OID .1.3.6.1.2.1.4.20.1.4.2, 시스템 IP 정보 포함

또한 “Enterprise MIB” 로 불리우는 특정 MIB 도 있습니다.

Enterprise MIB 에서 ACKSYS 의 root OID 는 « .1.3.6.1.4.1.28097 » 입니다. 좀더 자세한 내용은 이 문서의 다음 부분에서 설명합니다. MIB 파일은 CDROM 에 포함되어 있으며 ACKSYS 홈페이지에서 다운로드 하실 수 있습니다.

### 5.2 SNMP community

SNMP community 는 SNMP 를 운영하는 각 장비와 관리 서버가 속한 그룹을 말하며 이를 통해 관리자는 어떤 정보를 어디로 전송하는지 확인할 수 있습니다. Community 이름은 각각의 그룹을 구별하는데 사용됩니다. SNMP 장비나 agent 는 하나 이상의 SNMP community 에 속해 있습니다. 자신이 속해있지 않은 community 의 관리 시스템으로부터 수신한 정보 요청에는 응답하지 않습니다.

### 5.3 SNMP trap

Trap 은 agent 가 관리 시스템으로 보내는 경고성 메시지입니다.

ACKSYS 장비는 다음과 같은 Trap 을 전송할 수 있습니다.

- ColdStart : 장비가 기동되었음
- Linkdown : Access Point 와의 무선 연결이 끊어졌음(bridge infrastructure 모드 일 경우만)
- LinkUp : Access Point 와 무선 연결이 성립되었음 (bridge infrastructure 모드 일 경우만)
- Power1 On : 첫번째 전원 단자를 통해 전원이 켜졌음 (WLg-ABOARD/N 모델에만 해당)
- Power1 Off : 첫번째 전원 단자를 통해 전원이 꺼졌음 (WLg-ABOARD/N 모델에만 해당)
- Power2 On : 두번째 전원 단자를 통해 전원이 켜졌음 (WLg-ABOARD/N 모델에만 해당)
- Power2 Off : 두번째 전원 단자를 통해 전원이 꺼졌음 (WLg-ABOARD/N 모델에만 해당)

## 5.4 SNMP menu

SNMP 기능을 사용하기 위하여 SNMP agent 를 실행해야 합니다.

- STEP1 : **Basic** 메뉴에서 **SNMP** 선택
- STEP2 : **Enable SNMP agent** 설정
- STEP3 : agent community(**Read/write community**) 입력(기본값 : public)
- STEP4 : **save setting** 버튼을 클릭하여 설정 저장
- STEP5 : **reboot** 버튼을 클릭하여 시스템 재부팅  
시스템이 재부팅 한 후 SNMP agent 가 시작됩니다.

SNMP AGENT SETTING

Enable SNMP agent :

Read / write community :

설정을 저장한 후 다른 설정을 원할 경우 **continue** 버튼을 클릭하시기 바랍니다.

## 5.5 Traps management

**SNMP agent 가 enabled 로 설정되어 있는지 확인하시기 바랍니다.**

SNMP AGENT SETTING

Enable SNMP agent :

Read / write community :

SNMP TRAP SETTING

Enable trap :

Trap type :

Trap receiver IP :

Community :

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	

### Add a trap

SNMP TRAP SETTING 창에서 설정할 수 있습니다.

- **Enable trap** : 현재 Trap 의 사용 유무를 설정합니다.
- **Trap type** : 사용할 Trap 을 선택합니다. (ColdStart, Linkdown, LinkUp)
- **Trap receiver IP** : 해당 Trap 을 전송할 SNMP 관리 시스템의 IP 주소를 입력합니다.
- **Community** : Trap community 를 입력합니다.

**Save** 버튼을 클릭하면 새로운 Trap 이 **SNMP TRAP LIST** 창에 추가됩니다.

**참고:**

- 최대 5 개의 Trap 까지 설정할 수 있습니다.
- 같은 Trap 을 여러 번 설정할 수 있습니다.
- 각 Trap 은 특정 IP 정보를 포함할 수 있습니다.
- 각 Trap 은 특정 destination community 정보를 포함할 수 있습니다.
- agent 는 Destination community 를 각각 다르게 설정할 수 있습니다.

**Delete a trap**

각 Trap 을 삭제하려면 리스트에서 아이콘을 클릭하고 **confirm** 버튼을 클릭합니다.

**Modify a trap**

Trap 을 수정하려면 리스트에서 아이콘을 클릭하고 설정 창에서 수정합니다. 수정이 완료되면 **save** 버튼을 클릭하여 저장합니다.

SNMP TRAP SETTING

Enable trap :

Trap type : ColdStart ▼

Trap receiver IP :

Community :

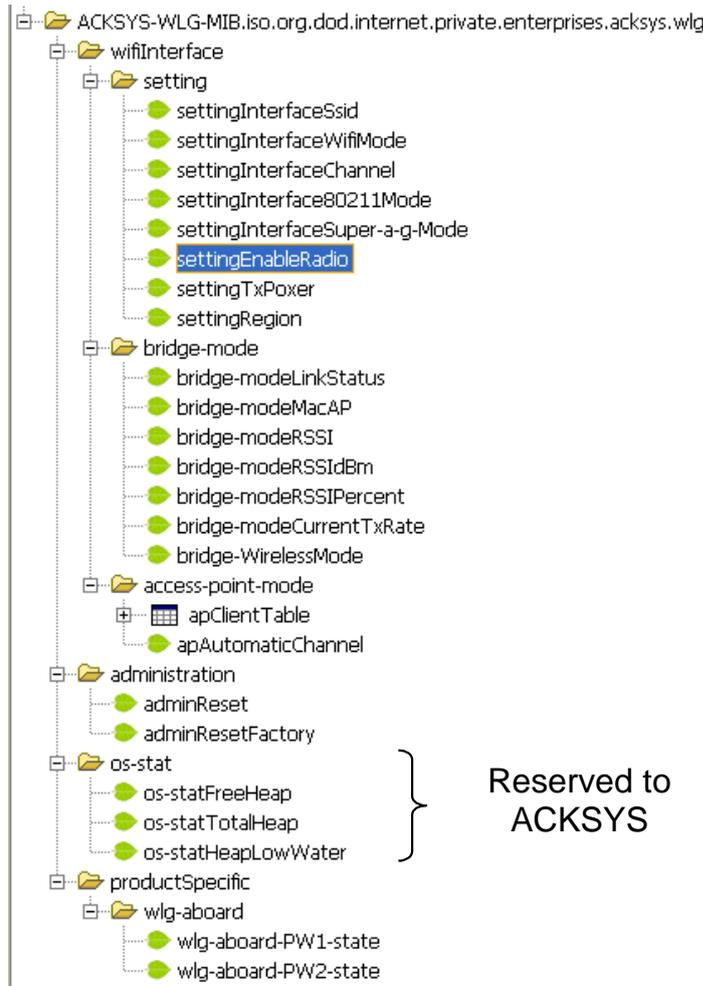
SNMP TRAP LIST

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	

**SNMP TRAP SETTING** 에서 Trap 을 수정할 수 있습니다.  
 수정 후 **Save** 버튼을 클릭하시면 TRAP LIST 가 업데이트 됩니다.

## 5.6 Enterprise MIB ACKSYS

- 제품의 사용 모드(Bridge mode 또는 Access Point mode)에 따라서 bridge-mode 혹은 access-point-mode 에 해당하는 정보만 확인이 가능합니다.
- 변경된 사항은 제품이 재부팅 후 적용됩니다.
- SNMP 를 이용하여 제품을 재부팅 시킬 수 있습니다.  
 OID .1.3.6.1.4.1.28097.1.2.1.0. 에 **1** 을 쓰면 장비는 재부팅 됩니다.



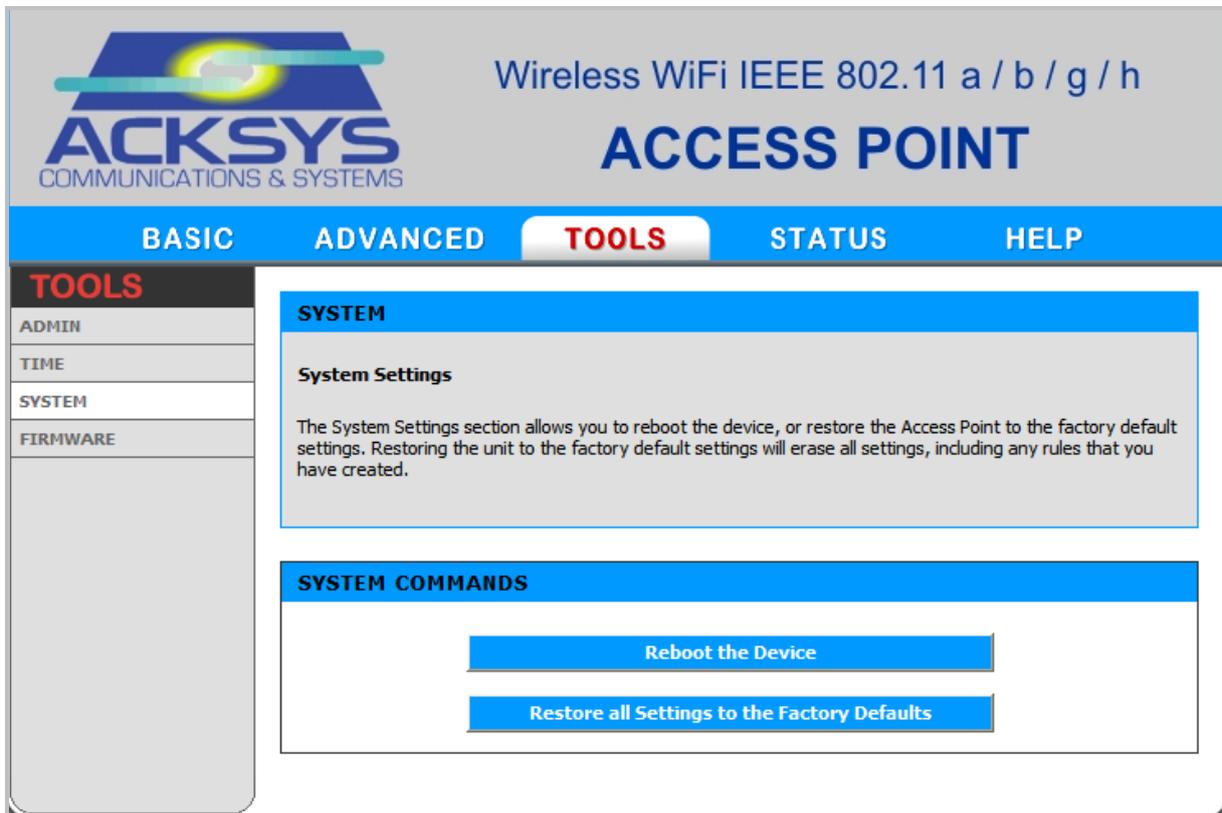
<p><b>.1.3.6.1.4.1.28097.1.1.1</b></p>	
<p><b>.1.3.6.1.4.1.28097.1.1.2</b></p>	
<p><b>.1.3.6.1.4.1.28097.1.1.3</b></p>	
<p><b>.1.3.6.1.4.1.28097.1.2</b></p>	
<p><b>.1.3.6.1.4.1.28097.1.4.1</b></p>	

OID	Access	Name	Description	Value
.1.3.6.1.4.1.28097.1		ACKSYS-WLG-MIB	MIB for the Access point and Bridge Wi-Fi 802.11 a/b/g/h devices.	
.1.3.6.1.4.1.28097.1.1		wifiInterface	Part of the MIB allowing access to data related to the Wi-Fi interface.	
<b>.1.3.6.1.4.1.28097.1.1.1</b>		<b>setting</b>	<b>WLAN settings</b>	
.1.3.6.1.4.1.28097.1.1.1.1.0	Read/Write	settingInterfaceSsid	WLAN name (SSID).	Character string, (up to 33 characters).
.1.3.6.1.4.1.28097.1.1.1.2.0	Read/Write	settingInterfaceWifiMode	Wi-Fi mode.	1: Bridge 2: Access Point
.1.3.6.1.4.1.28097.1.1.1.3.0	Read/Write	settingInterfaceChannel	Wireless channel.	Wireless channel number. Depends on the selected 802.11x mode: A, H or B/G (use only for Access Point and Bridge ad-hoc)
.1.3.6.1.4.1.28097.1.1.1.4.0	Read/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/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/Write	SettingEnableRadio	Enable/disable wireless radio	1: Disable wireless radio 2: Enable wireless radio
.1.3.6.1.4.1.28097.1.1.1.7.0	Read/Write	SettingTxPower	Wireless radio power	1: Strong (100 %) 2: Medium (50 %) 3: Low (25%)
.1.3.6.1.4.1.28097.1.1.1.8.0	Read/Write	SettingRegion	Select your country	2 = Israel 4 = USA 5 = Hong Kong 6 = Canada 7 = Australia 14 = Europe 17 = Japan 18 = Singapore 20 = Korea
<b>.1.3.6.1.4.1.28097.1.1.2</b>		<b>Bridge-mode</b>	<b>Bridge infrastructure settings</b>	
.1.3.6.1.4.1.28097.1.1.2.1.0	Read	bridge-modeLinkStatus	Access point link status	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.	

OID	Access	Name	Description	Value
.1.3.6.1.4.1.28097.1.1.2.3.0	Read	bridge-modeRSSI	RSSI connection (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 in %.	
.1.3.6.1.4.1.28097.1.1.2.6.0	Read	bridge-modeCurrentTxRate	Transmission rate in bits/s.	
<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 users list.	
.1.3.6.1.4.1.28097.1.1.3.1.1		apClientEntry	Connected user description.	
.1.3.6.1.4.1.28097.1.1.3.1.1.1	Read	clientMacAddr	User's MAC address.	
.1.3.6.1.4.1.28097.1.1.3.1.1.2	Read	client80211Mode	802.11 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	User's transmission rate in bits/s.	
.1.3.6.1.4.1.28097.1.1.3.1.1.4	Read	clientRssiPercent	User RSSI value, in %.	
.1.3.6.1.4.1.28097.1.1.3.2.0	Read/Write	apAutomaticChannel	Enable/disable automatic channels selection	1: disable 2: enable
<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 by SNMP.	Write 1 to reboot the device
.1.3.6.1.4.1.28097.1.2.2.0	Read/Write	adminResetFactory	This option restores all configuration settings back to the settings that were in effect at the time the Access Point was shipped from the factory. Reboot the device. The SNMP agent will be disabled.	Write 1 restores factory settings
<b>.1.3.6.1.4.1.28097.1.4</b>		<b>ProductSpecific</b>	<b>Product specific settings</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>	
.1.3.6.1.4.1.28097.1.4.1.1.0	Read	wlg-aboard-PW1-state	Power1 status.	1: Power on 2: Power off
.1.3.6.1.4.1.28097.1.4.1.2.0	Read	wlg-aboard-PW2-state	Power2 status.	1: Power on 2: Power off

## 6 FACTORY DEFAULT SETTINGS

이 옵션은 모든 설정 상태를 공장 초기화 상태로 돌려놓는 기능입니다. 기존에 설정된 모든 정보는 초기값으로 변경 됩니다. 현재 설정 상태의 저장은 **TOOLS** → **ADMIN** 페이지에서 할 수 있습니다.



### Factory Default 값 :

**Login** : admin

**Password** : none(없음)

**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 broadcast**

**No security** (no wep, WPA, WPA2, and no MAC id filtering)

**SNMP management** : disabled

**DHCP server** : disabled

## 7 DEVICE UPGRADE

### 7.1 By the WEB interface

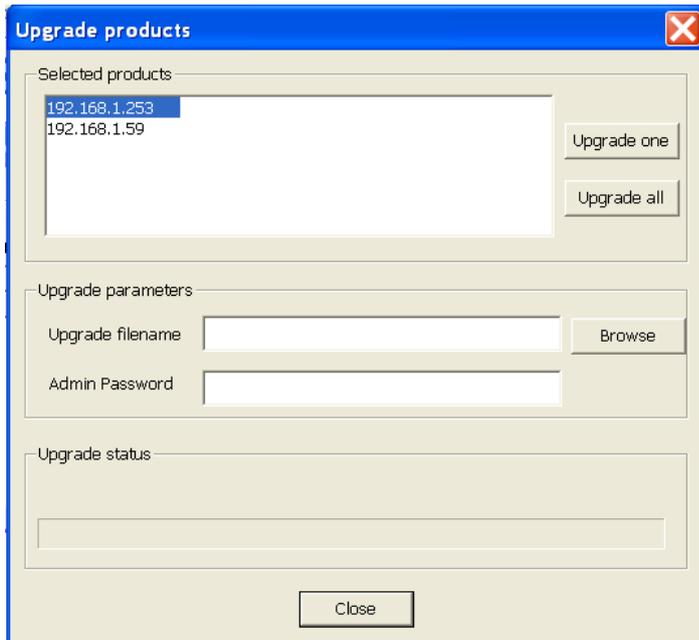
펌웨어 업그레이드는 새로운 기능이 추가되거나 성능이 향상된 최신 펌웨어로 시스템을 업데이트 할 때 확인합니다. ACKSYS 홈페이지( [www.acksys.com](http://www.acksys.com) ) 에서 최신 버전을 확인하시기 바랍니다. 이 옵션은 **TOOLS** → **FIRMWARE** 메뉴에서 사용 가능합니다. 펌웨어를 업그레이드 하여도 기존 설정 정보는 유지됩니다.

### 7.2 By Locator

이 기능은 **Locator ver 7.0.0** 이상, 제품은 **ver 3.6.0** 이상의 펌웨어에서 사용이 가능합니다.

Name	Type	IP address	Mac address
ACKSYS Device	ACKSYS Wifi a/b/g/h product	192.168.1.253	00:80:48:41:68:54
ACKSYS Device	ACKSYS Wifi a/b/g/h product	192.168.1.59	00:0E:8E:0A:3A:A1

- STEP1 : **Scan** 버튼을 클릭하여 네트워크에 설치된 제품을 검색합니다.
- STEP2 : 업데이트 하려는 제품을 마우스로 선택합니다.
- STEP3 : **Upgrade** 버튼을 클릭합니다.



STEP4 : **Browse** 버튼을 클릭하여 업데이트 할 펌웨어 파일을 선택합니다.

STEP5 : **Upgrade one** 버튼을 클릭하면 업그레이드가 시작됩니다. Selected products 리스트에 표시된 모든 제품을 업그레이드 하려면 **Upgrade all** 버튼을 클릭하시기 바랍니다.

참고 : 동일한 펌웨어 파일로 동시에 여러 장비를 업그레이드 하려면 각각의 장비가 모두 똑같은 패스워드 정보를 가지고 있어야 가능합니다.

### 7.3 Recovering a product after an upgrade problem

Ver 3.2.0 이상의 펌웨어가 적용된 제품에서는, 업데이트가 실패할 경우 응급 복구 펌웨어가 자동으로 실행됩니다. 이러한 상황은 거의 대부분 업데이트 중에 전원이 꺼졌을 때 발생합니다. 응급 복구 펌웨어는 펌웨어 업데이트 외의 어떠한 기능도 지원하지 않습니다.

업데이트가 실패할 경우 제품이 재부팅 하면 **DIAG LED** 가 빠르게 깜빡거립니다.

응급 복구 펌웨어를 이용하여 새로운 펌웨어를 업데이트 하려면 웹브라우저를 이용해 “192.168.1.253”으로 접속합니다. 이때 PC의 IP 주소는 192.168.1.xxx 대역으로 설정되어 있어야 합니다.



Browse 버튼을 이용하여 업데이트 할 펌웨어를 선택하고 Upload 버튼을 클릭하면 됩니다.

EPROM에 특별한 문제가 없으면 기존 설정은 모두 유지됩니다. 하지만 EPROM에 새로운 펌웨어를 쓰는 과정에서 문제가 발생할 경우 Factory default 설정 상태로 자동 설정됩니다.

펌웨어 업데이트 완료 후, 새로운 펌웨어 버전은 **TOOLS** → **FIRMWARE** 메뉴에서 확인하실 수 있습니다. 제품에 접속하기 전에 PC의 IP 주소를 확인하시기 바랍니다.

## 7.4 전원 연결

### WLg-ABOARD/N:

- 9~72V DC 전원 입력, 2 개의 전원 입력 인터페이스 제공
- 2 개의 입력 인터페이스 중 1 개를 선택하여 전원 연결, M12 Power Cable 사용(검은색 피복 케이블)
- Power 1 입력 단자 > Brown(+), White(-)
- Power 2 입력 단자 > Blue(+), Black(-)

아래의 그림 중 1 가지 방법으로 연결

