

(주)동영미디어
• 주소 : 경기도 군포시 당정동 424번지
• http://www.dym.co.kr

사용중 불편한 점이 있을 땐 아래 전화번호로 연락해 주세요.

제품 모델명, 고장상태, 연락처를 정확히 알려주시면 언제나 친절함 상담과 빠른 서비스를 실시해 드립니다.



서비스센터 대표전화 (전국무료)

전국어디서나 : **080-011-1121**

DM-350AP, DM-450AP User Manual

dym (주)동영미디어

www.dym.co.kr

취급 설명서

DM-350AP / DM-450AP

가정용 무선 AP

인터넷부터 각종 네트워크까지
무선으로 손쉽게 - 무선 AP

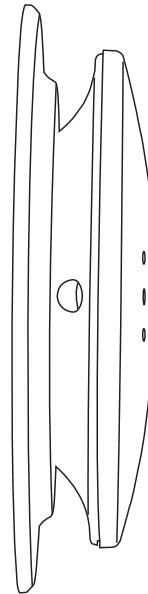
- 안전을 위한 주의사항은 사용자의 안전을 지키고, 재산상의 손해 등을 막기 위한 내용입니다. 반드시 읽고 올바르게 사용해 주십시오.
- 본 제품은 국내(대한민국)용입니다.



DM-450AP

목차

■ 안전을 위한 주의사항	· 04
■ 무선 네트워크 사용하기(Windows XP 기준)	· 05
■ AP의 WEB UI(웹 사용자인터페이스)에 접속하기	· 06
1.1. AP의 디폴트 설정값	· 06
1.2. 컴퓨터 랜카드 설정하기	· 08
1.3. 웹 브라우저를 통해 접속하기	· 10
1.4. WEB UI(웹 사용자 인터페이스) 화면 구성	· 11
1.4.1. 주요화면 구성요소	· 12
■ WEB UI 상세설명	· 16
2.1. HOME	· 16
2.2. 상태조회	· 17
2.2.1. 무선랜 접속정보	· 17
2.2.2. 무선 인터페이스 상태	· 22



2.2.3. 브리지 테이블	· 24
2.3. 장치설정	· 25
2.3.1. 시스템 설정	· 26
2.3.2. 무선랜 설정	· 27
2.3.3. MULTI-SSID	· 34
2.3.4. NAT/DHCP	· 36
2.4. 시스템 관리도구	· 39
2.4.1. 관리자 암호	· 39
2.4.2. 설정초기화	· 40
2.4.3. 업그레이드	· 40
2.4.4. 재시작	· 41
■ 이상이 생기면	· 42
■ 제품 규격	· 43

안전을 위한 주의사항

무선랜 제품을 설치 및 사용하실 때, 사용자의 안전과 재산상의 손해를 방지하기 위한 내용입니다. 아래의 내용을 읽어 보신 후 올바르게 사용하기 바랍니다.

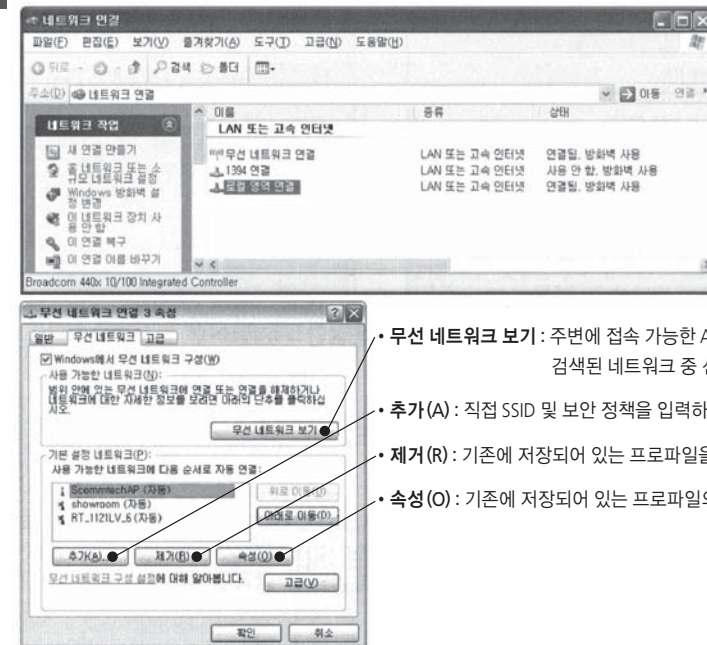
올바른 사용 방법	유형별 주의 내용
정격 전압을 사용하세요.	제품의 손상 및 화재의 위험이 있습니다.
제공되는 전원케이블과 어댑터를 사용하세요.	감전 및 화재의 위험이 있습니다.
안전한 장소에 설치하세요. (물리적 충격을 주지 마세요.)	떨어지거나 넘어지면 제품이 파손될 수 있습니다.
천둥, 번개가 칠 때에는 노출된 단자나 케이블을 만지지 마세요.	감전 및 화재의 위험이 있습니다.
절대로 분해하거나 개조하지 마세요.	제품에 손상이 될 수 있습니다.
처음 설치 및 사용 시에는 전원을 끄신 상태에서 시작하세요.	감전의 위험이 있습니다.
AC 어댑터를 연결한 상태에서 AP를 뒤집지 마세요.	플러그의 손상이 있을 수 있습니다.

본 제품은 무선랜을 이용하는 제품입니다. 무선랜 기능의 특성상 가전기기 및 주변 전자제품, 특히 타사 AP에 의해 통신에 지장을 받을 수 있습니다.

주의

- 당해 무선설비가 전파통신 가능성이 있으므로 인명안전과 관련된 서비스는 할 수 없음.
- AP와의 거리가 멀거나 중간에 장애물이 있는 경우 통신이 불안해 질 수 있음.

무선 네트워크 사용하기(Windows XP 기준)



AP의 WEB UI(웹 사용자 인터페이스)에 접속하기

1.1. AP의 디폴트 설정값

- 공장 출하 시 초기 설정 값들은 다음과 같습니다.

■ IP설정						
IP주소	192.168.0.254					
서브넷 마스크	255.255.255.0					
게이트웨이 주소	192.168.0.1					
■ 무선랜 기본설정						
Service	AP					
SSID	default					
채널	자동선택(1~13)					
모드	11g(11b 호환)					
전송속도	Best					
■ 무선랜 고급설정						
Short Preamble	Burst	WMM	Protection Mode	RTS Threshold	Fragmentation Threshold	TX Power
V	V	V		2345	2330	20
■ 무선랜 보안옵션						
SSID 숨김	사용안함					
보안정책	사용안함					
ACL 정책	Open (ACL 체크하지 않음)					

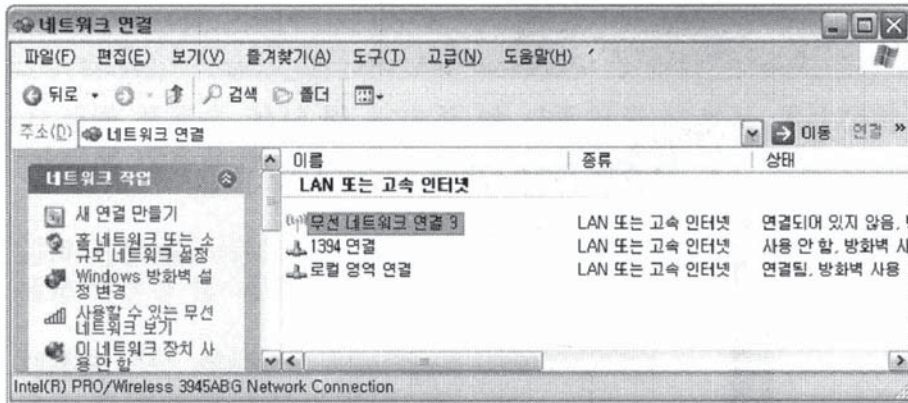
■ SNMP	
Public Community String	public
Private Community String	private
System Location	location
System Contact	23-1234, aa@aa.com
■ VLAN	
VLAN IP주소	192.168.1.254
VLAN 서브넷마스크	255.255.255.0
VLAN 게이트웨이	192.168.1.1
■ DHCP	
IP 설정 범위	192.168.250.11 ~ 192.168.250.254
서브넷마스크	255.255.255.0
DNS 주소	61.97.112.155, 61.97.113.250
WINS	192.168.250.1
도메인	
LEASE(초)	864000
DHCP 서버	192.168.0.1
게이트웨이	192.168.250.10
■ 관리자접근정보	
관리자 로그인	ID root
관리자 암호	admin

※ 설정 초기화를 하게 되면 모든 설정이 위의 디폴트 설정값으로 초기화됩니다.

AP의 WEB UI(웹 사용자 인터페이스)에 접속하기

1.2. 컴퓨터 랜카드 설정하기

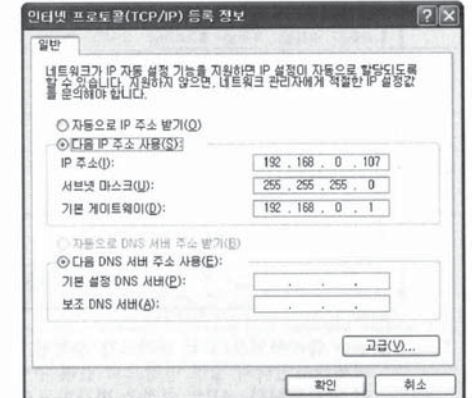
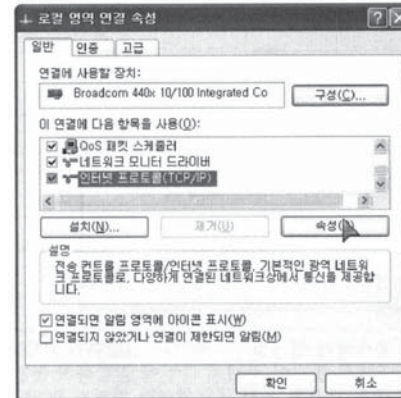
- 먼저 접속에 사용할 컴퓨터의 랜카드 설정을 AP와 일치시켜 줍니다.
- ※ 접속시 사용할 랜카드가 AP와 같은 네트워크 상에 연결되어 있어야 합니다.



- ※ 무선 클라이언트 (무선 랜타드가 장착된 PC)에서 접속하여 설정할 수 있으나 권장하지 않습니다.
- 액세스포인트의 설정 변경으로 인해 무선 클라이언트의 접속이 끊어져 작업이 원활하지 못할 수 있기 때문입니다.
- AP의 설정을 변경하고자 할 경우에는 가급적 유선 네트워크로 연결된 PC를 사용하실 것을 권장합니다.

1.2. 컴퓨터 랜카드 설정하기

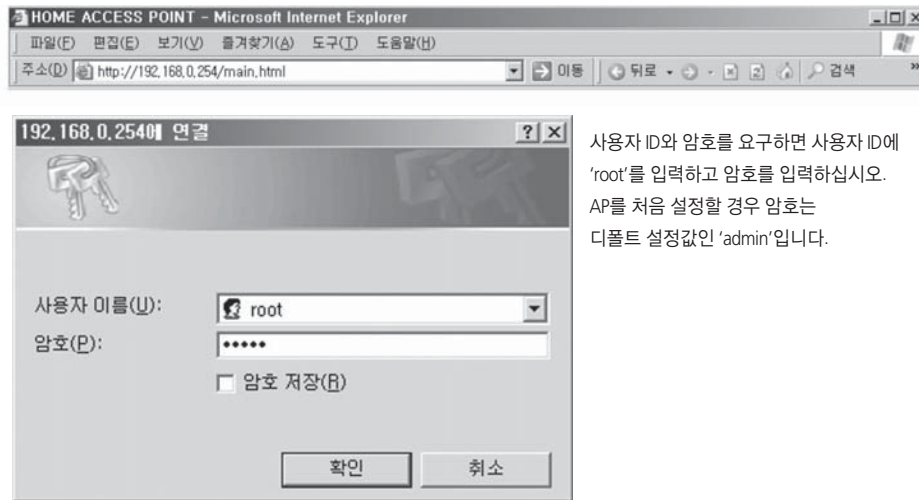
- AP의 IP 설정을 변경하지 않았을 시 아래와 같이 변경합니다.
- (192.168.0.1 또는 254를 제외한 IP)



AP의 WEB UI(웹 사용자 인터페이스)에 접속하기

1.3. 웹 브라우저를 통해 접속하기

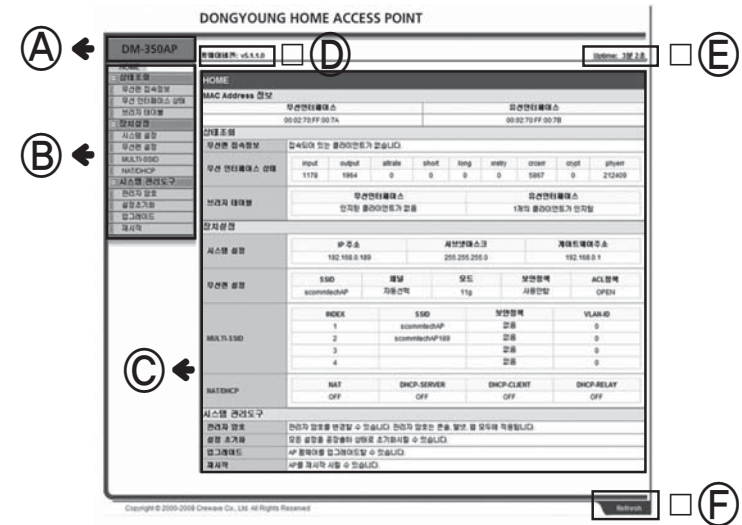
- 웹 브라우저(인터넷익스플로러6.0 이상 권장)의 주소입력란에 액세스포인트의 IP주소를 "http://192.168.0.254"와 같은 형식으로 입력하신 후 엔터를 치면 접속할 수 있습니다.



사용자 ID와 암호를 요구하면 사용자 ID에 'root'를 입력하고 암호를 입력하십시오.
AP를 처음 설정할 경우 암호는 디폴트 설정값인 'admin'입니다.

1.4. WEB UI(웹 사용자 인터페이스) 화면 구성

- AP의 WEB UI에 성공적으로 접속하였다면 다음 그림과 같은 화면이 표시될 것입니다.



AP의 WEB UI(웹 사용자 인터페이스)에 접속하기

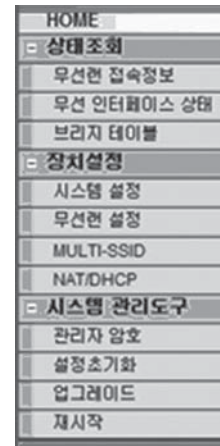
1.4.1. 주요화면 구성요소



■ A. 제품의 모델명을 표시합니다.

■ B. 선택할 수 있는 메뉴입니다.
 각 항목을 클릭하면 해당 페이지가 'E'영역에 표시됩니다.

- HOME : 위에 보이는 초기화면을 표시합니다. AP의 전반적인 상태와 주요 설정정보를 'E'영역에 표시합니다.
- 상태조회 : AP상태의 요약정보를 표시합니다. 상세한 AP상태를 확인하려면 상태조회 아래의 하위메뉴를 클릭하십시오.
 상태조회의 하위메뉴는 다음과 같습니다.
 - 무선랜 접속정보 : AP에 현재 접속되어 있는 무선랜 클라이언트들의 정보를 표시합니다.
 - 무선 인터페이스 상태 : AP의 무선 인터페이스를 통해 전송 및 수신된 데이터 프레임의 통계를 볼 수 있습니다.
 - 브리지 테이블 : AP는 무선 인터페이스와 유선 인터페이스를 브리지로 묶어 무선랜과 유선랜이 상호 통신할 수 있도록 하는 장치라고 할 수 있습니다. AP를 지나간 데이터 패킷을 통해 유선과 무선에 존재하는 클라이언트의 MAC Address를 수집하여 브리지 테이블에 일정시간 보관하게 됩니다.
 이 브리지 테이블의 내용을 확인할 수 있습니다.



- 장치설정 : AP의 현재 설정정보의 요약을 볼 수 있습니다. 하위메뉴를 통해 AP의 설정을 변경할 수 있습니다. 하위 메뉴는 다음과 같습니다.
 - 시스템 설정 : IP주소, 서브넷마스크, 게이트웨이 주소를 설정할 수 있습니다.
 - 무선랜 설정 : 무선랜을 설정합니다.
- 시스템관리도구 : 각 시스템 관리도구의 용도가 간략히 설명되어 있습니다. 시스템관리도구 하위메뉴에서 각 시스템 관리도구를 사용할 수 있습니다.
 하위 메뉴는 다음과 같습니다.
 - 관리자 암호 : 관리자 암호를 변경할 수 있습니다.
 - 설정 초기화 : 모든 설정을 공장 출하 상태로 초기화 시킬 수 있습니다.
 - 업그레이드 : AP펌웨어를 업그레이드할 수 있습니다.
 - 재시작 : AP를 재시작(Reboot)시킬 수 있습니다.
- NAT/DHCP 설정 : NAT/DHCP 설정, 변경 할 수 있습니다.
 - NAT : Network Address Translation
 - DHCP : Dynamic Host Configuration Protocol

AP의 WEB UI(웹 사용자 인터페이스)에 접속하기

C. 메뉴항목에서 선택한 해당 페이지를 표시합니다..

HOME				
MAC Address 정보				
무선랜 인터페이스		유선랜 인터페이스		
00:02:70:FF:00:7A		00:02:70:FF:00:7B		
상태조회				
무선랜 접속정보: 접속되어 있는 클라이언트가 없습니다.				
무선랜 인터페이스 상태				
input	output	airrate	short	long
1178	1964	0	0	0
xretry	creirr	crypt	phyerr	
0	5867	0	212409	
브리지 테이블				
무선랜 인터페이스		유선랜 인터페이스		
인자된 클라이언트가 없음		1개의 클라이언트가 인자됨		
장치설정				
시스템 설정				
IP 주소		서브넷 마스크		게이트웨이 주소
192.168.0.189		255.255.255.0		192.168.0.1
무선랜 설정				
SSID	채널	모드	보안정책	ACL정책
scommtechAP	자동선택	11g	사용안함	OPEN
MULTI-SSID				
INDEX	SSID	보안정책	VLAN-ID	
1	scommtechAP	없음	0	
2	scommtechAP189	없음	0	
3		없음	0	
4		없음	0	
NAT/DHCP				
NAT	DHCP-SERVER	DHCP-CLIENT	DHCP-RELAY	
OFF	OFF	OFF	OFF	
시스템 관리도구				
관리자 암호	관리자 암호를 변경할 수 있습니다. 관리자 암호는 콘솔, 텔넷, 웹 모두에 적용됩니다.			
설정 초기화	모든 설정을 공장출하 상태로 초기화시킬 수 있습니다.			
업그레이드	AP 펌웨어를 업그레이드할 수 있습니다.			
재시작	AP를 재시작시킬 수 있습니다.			

D. 펌웨어버전: AP의 현재 펌웨어 버전을 표시합니다.

E. Uptime: AP가 기동된 후 경과된 시간을 표시합니다.

DM-350AP	
HOME	Uptime: 3분 2초
상태조회	펌웨어버전: v5.1.1.0
무선랜 접속정보	HOME
무선랜 인터페이스 상태	MAC Address 정보
	업그레이드
	재시작
	Refresh

F. C에 표시된 페이지에 따른 조작버튼입니다. 대부분의 조회페이지에서는 'Refresh'가 표시되고, 설정페이지에서는 'Apply'와 'Cancel'이 표시됩니다.

- Refresh: E영역에 표시된 페이지를 갱신합니다.
- Apply: 변경된 설정을 AP로 전송하여 실시간으로 AP에 적용시킵니다.
- Cancel: 변경중인 설정 내용을 취소하고 현재 AP의 설정내용을 다시 읽어 옵니다.

WEB UI 상세설명

2.1. HOME

- AP의 전반적인 상태와 주요 설정정보를 표시합니다.

HOME									
MAC Address 정보									
무선랜 인터페이스		유선랜 인터페이스							
00:02:70:94:00:37		00:02:70:94:00:38							
상태조회									
무선랜 접속정보	접속되어 있는 클라이언트가 없습니다.								
무선 인터페이스 상태	input	output	altrate	short	long	xretry	crcerr	crypt	phyerr
	2	2951	0	0	0	0	21034	0	2084
브리지 테이블	무선랜 인터페이스		유선랜 인터페이스						
	인지된 클라이언트가 없음		16개의 클라이언트가 인지됨						
장치설정									
시스템 설정	IP 주소	서브넷마스크	게이트웨이주소						
	192.168.0.254	255.255.255.0	192.168.0.1						
무선랜 설정	SSID	채널	모드	보안정책	ACL정책				
	default	자동선택	11g	사용안함	OPEN				
MULTI-SSID	INDEX	SSID	보안정책	VLAN-ID					
	1	default	없음	0					
	2		없음	0					
	3		없음	0					
	4		없음	0					
NAT/DHCP	NAT	DHCP-SERVER	DHCP-CLIENT	DHCP-RELAY					
	OFF	ON	OFF	OFF					
시스템 관리도구									
관리자 암호	관리자 암호를 변경할 수 있습니다. 관리자 암호는 콘솔, 텔넷, 웹 모두에 적용됩니다.								
설정 초기화	모든 설정을 공장출하 상태로 초기화시킬 수 있습니다.								
업그레이드	AP 펌웨어를 업그레이드할 수 있습니다.								
재시작	AP를 재시작시킬 수 있습니다.								

2.2. 상태조회

- AP상태의 요약정보를 표시합니다.

상태조회									
무선랜 접속정보									
접속되어 있는 클라이언트가 없습니다.									
무선 인터페이스 상태									
input	output	altrate	short	long	xretry	crcerr	crypt	phyerr	
5	18322	0	0	0	0	251456	0	34337	
브리지 테이블									
무선랜 인터페이스					유선랜 인터페이스				
인지된 클라이언트가 없음					16개의 클라이언트가 인지됨				

2.2.1. 무선랜 접속정보

- AP에 현재 접속되어 있는 무선랜 클라이언트들의 정보를 표시합니다.

무선랜 접속정보															
ADDR	AID	CHAN	RATE	RSSI	IDLE	TXSEQ	RXSEQ	CAPS	ACAPS	ERP	STATE	TYPE	CIPHER	MODE	A_TIME
00:00:b4:20:04:8c	1	4	36M	18	180	3	16944	ESS		0	25	open	none	Normal	01:04:40
00:40:96:a8:d7:18	2	4	54M	39	120	11	3024	ESS		0	27	open	none	Normal	01:12:42
2 개의 클라이언트가 접속되어 있습니다.															

WEB UI 상세설명

- ADDR : 접속된 무선랜 클라이언트의 MAC Address
- AID : 접속ID(Association ID)
- CHAN : 현재 접속채널
- RATE : 현재 AP와 클라이언트간 마지막으로 통신했을 때의 통신속도.
- RSSI : 클라이언트로부터 마지막으로 수신된 신호의 품질.
- IDLE : 데이터통신 없이 경과한 시간.
- TXSEQ : 다음에 전송될 프레임의 Sequence Number
- RXSEQ : 최근에 수신된 프레임의 Sequence Number
- CAPS : Capabilities. 아래 표시문자들의 조합으로 Capability를 표시함.

E	ESS	station이 ESS(Infrastructure network)에 속함
I	IBSS	tation이 IBSS(Ad-hoc network)에 속함
S	SHORT PREAMBLE	통신을 위해 WEP, TKIP, AES-CCMP등의 방식으로 데이터를 암호화하는 지의 여부.
B	PBCC	PREAMBLE short preamble의 사용 여부. * long preamble이 128-bit sync field를 사용하는 데에 반해 short preamble은 64-bit sync field를 사용함.

B	PBCC	PBCC modulation 지원 여부 * 11g OFDM이 채택되기 전 TI에서 제안한 변조방식으로 11b+로 출시된 제품에서 사용된 기술임. 802.11g에서는 선택적으로 22, 23 Mbps모드를 지원할 수 있도록 하고 있으나 본 AP에서는 지원하지 않음.
s	SHORT SLOTTIME	Short slot time 사용 여부
R	RSN	RSN(Robust Secure Network, IEEE 802.11i) 지원 여부
D	DSSS-OFDM	DSSS-OFDM modulation 지원여부 * preamble과 header는 DSSS방식으로 payload는 OFDM방식을 사용함. Data rates은 ERP-OFDM과 동일함.

- ACAPS : Atheros Proprietary Capabilities. 아래 표시문자들의 조합으로, Atheros 고유의 SuperG기술관련 Capability를 표시함.

D	TURBO	채널 대역폭을 2배로 점유하여 data rate을 2배(108Mbps)로 늘리는기술. (* 본 AP는 Turbo를 지원하지 않음)
C	COMPRESSON	리얼타임 하드웨어 데이터 압축기술 (* 본 AP는 Compression을 지원하지 않음.)
F	FF	Fast Frame. 여러 개의 frame을 묶어서(aggregation) 한번에 보내는기술. (* 본 AP는 FF를 지원하지 않음)
X	XR	eXtended Range. throughput을 희생시키고 거리(range)를 늘리는 기술.

WEB UI 상세설명

A	AR	Super G Adaptive Radio. Turbo 기술처럼 채널 대역폭을 미리 2배로 할당해 놓는 것이 아니라, 채널을 모니터링 하고 있다가 대역폭을 2배로 늘려도 괜찮을 때 자동적으로 대역폭을 늘려서 성능을 높이는 기술 (Dynamic Turbo기술. *본 AP는 AR을 지원하지 않음.)
T	Burst	802.11e의 일부분. 동일 시간동안 보다 많은 frame을 전송할 수 있도록 하여 성능을 높이는 기술.

- ERP: ERP(Extended Rate PHY) information element flags. 비트맵 정보로써 비트 별 의미는 다음과 같음.

비트번호	16진수 환산값		
bit 0	0x01	NON_ERP_RESENT	non ERP 모드가 존재함
bit 1	0x02	USE_PROTECTION	protection mode 사용
bit 2	0x04	LONG_PREAMBLE	long preamble mode 사용

- STATE: 비트맵 정보로써 비트 별 의미는 다음과 같음.

비트번호	16진수 환산값	
bit 0	0x0001	Authorized for data
bit 1	0x0002	QoS enabled
bit 2	0x0004	ERP(Extended Rate PHY) enabled

bit 3	-	- RESERVED bit4
bit 4	0x0010	power save mode enabled
bit 5	0x0020	Authentication ref held
bit 6	0x0040	U-APSD power save enabled
bit 7	0x0080	U-APSD triggerable state
bit 8	0x0100	U-APSD SP in progress

- TYPE : Authentication Type.(open, shared, wpa, ...)
- CIPHER : 데이터 암호화방식(wep, tkip, aes, ...)
- MODE : 현재 통신모드가 XR모드인지 Normal 모드인지 표시.
- A_TIME : 해당 클라이언트가 접속된 시간(Uptime기준)

WEB UI 상세설명

2.2.2. 무선 인터페이스 상태

- 무선 인터페이스를 통해 주고받은 데이터 프레임의 통계치를 표시합니다.

무선 인터페이스 상태									
요약정보									
input	output	altrate	short	long	xretry	rcerr	crypt	phyerr	
1655	21861	0	0	2178	535	10481148	0	56658837	
상세정보									
General Statistics									
634 tx management frames									
535 tx failed because too many retries									
2178 long on-chip tx retries									
21249 tx frames with no ack marked									
16 tx frames with short preamble									
10481148 rx failed because of bad CRC									
582 periodic calibrations									
56658837 <u>PHY errors</u>									
55188897 OFDM timing									
5 OFDM restart									
1469894 CCK timing									
41 CCK restart									
Antenna Statistics									
1 switched default/tx antenna									
76 tx used alternate antenna									
Antenna Profile									
Ant-1 tx: 10642 rx: 2									
Ant-2 tx: 10661 rx: 1653									

필드명	설 명
input	수신된 frame의 수
output	전송된 frame의 수
altrate	지원되지 않는 data rate으로 수신된 frame의 수
short	short retries. RTS packet이 재전송된 횟수
long	long retries. Data packet이 재전송된 횟수
xretry	과도한 재전송 시도로 인해 전송되지 못한 packet의 수
rcerr	수신된 frame중 CRC 오류로 인해 버려진 개수
crypt	수신된 frame중 보안옵션(WEP Key, WPA등)이 잘못되어 버려진 개수
phyerr	수신된 frame중 physical layer의 error로 판단되어 버려진 개수

※ xretry값이 매우 높고 실제 통신품질(throughput)이 낮다면 Fragmentation Threshold와 RTS Threshold의 값을 낮춰 보시길 권합니다. 단, Station에서 수신되는 AP의 신호세기(RSSI)나 현저히 낮거나, 접속된 Station(클라이언트)가 많을 경우에는 AP를 증설해야 문제가 해결될 수 있습니다.

※ rcerr와 phyerr가 상대적으로 매우 높고 실제 통신품질(throughput)이 낮다면 채널을 변경하는 것을 고려할 필요가 있습니다. 주변의 다른 무선네트워크와 너무 인접한 채널을 사용하고 있어 주변의 다른 무선네트워크의 패킷이 수신되면 이러한 패킷들이 대부분 phyerr나 rcerr로 카운트될 수 있습니다.

이 때는 주변의 다른 무선네트워크 사용자와 협의하여 서로의 채널을 조절하여 고정채널로 설정할 것을 권장합니다. 통상 무선랜에서 상호간섭을 최소화 하려면 인접 무선네트워크와의 채널을 4개 이상 이격시켜야 하는 것으로 알려져 있습니다. 하여, 정통부에서는 가급적 1, 5, 9, 13 채널만 사용할 것을 권고하고 있습니다.

WEB UI 상세설명

2.2.3. 브리지 테이블

- 유선과 무선 인터페이스 각각에 접속되어 있는 클라이언트의 수와 그 클라이언트들의 MAC Address를 확인할 수 있습니다.

브리지 테이블 목록			
로컬 MAC Address 정보			
무선인터페이스		유선인터페이스	
00:02:70:09:62:64		00:02:70:09:62:65	
인터페이스별 브리지 테이블 목록			
무선인터페이스		유선인터페이스	
MAC Address	Ageing Timer	MAC Address	Ageing Timer
00:00:b4:20:04:8c	70.34	00:02:3f:23:63:73	0.73
00:40:96:a8:d7:18	0.96	00:02:70:ff:00:00	0.36
-2개의 클라이언트가 인지됨-		00:0e:0c:4c:0f:33	0.27
		00:0e:0c:4c:14:7f	1.7
		00:13:20:c0:d5:36	2.27
		00:19:21:52:c4:73	173.16
		00:50:ce:18:12:59	174.44
		00:50:da:8c:74:4e	67.01
		00:50:da:8c:75:19	24.9
		00:50:da:8d:76:ad	205.32
		00:a0:b0:14:df:ba	43.03
		-11개의 클라이언트가 인지됨-	

※ 브리지 테이블 목록에서 표시되는 무선 인터페이스에 인식된 클라이언트들과 무선랜접속정보에서 표시되는 무선 랜클라이언트의 목록이 항상 일치하는 것은 아닙니다. 예를 들어 무선랜 클라이언트가 접속했다가 정상적인 절차로 접속을 끊을 경우 무선랜 접속정보에서는 거의 실시간으로 반영되지만 여기 브리지 테이블 목록에서는 해당 클라이언트로부터 수신되는 데이터없이 일정 시간(Ageing Timer)이 지나야 삭제됩니다.

2.3. 장치설정

- AP의 현재 설정정보의 요약을 볼 수 있습니다.

장치설정				
시스템 설정				
무선인터페이스 MAC Address		유선인터페이스 MAC Address		
00:02:70:94:00:37		00:02:70:94:00:38		
IP 주소	서브넷마스크	게이트웨이주소		
192.168.0.254	255.255.255.0	192.168.0.1		
무선랜 설정				
SSID	채널	모드	보안정책	ACL 정책
default	자동선택	11g	사용안함	OPEN
MULTI-SSID				
INDEX	SSID	보안정책	VLAN-ID	
1	default	없음	0	
2		없음	0	
3		없음	0	
4		없음	0	
NAT/DHCP				
NAT	DHCP-SERVER	DHCP-CLIENT	DHCP-RELAY	
OFF	OFF	OFF	OFF	

WEB UI 상세설명

2.3.1. 시스템 설정

- SNMP 사용여부 및 AP의 IP주소, 서브넷마스크, 게이트웨이주소를 설정할 수 있습니다.

시스템설정	
MAC Address 정보	
무선엔터페이스	유선엔터페이스
00:02:70:94:00:37	00:02:70:94:00:38
SNMP 설정	
SNMP 사용:	<input type="checkbox"/>
Public Community String:	public
Private Community String:	private
System Location:	location
System Contact:	123-1234_aa@aa.com
IP 설정	
IP 주소:	192.168.0.254
서브넷마스크:	255.255.255.0
게이트웨이주소:	192.168.0.1

• SNMP 설정

- Community string : 서버와 클라이언트 간의 관계를 정의합니다. 클라이언트가 서버로 접근할 경우 패스워드와 같은 역할을 하며 접근을 제어합니다.
- System Location, System Contact : 클라이언트에 대한 정보를 입력합니다. 서버에서는 해당 정보를 통하여 클라이언트에 대한 정보를 얻습니다.

2.3.2. 무선랜 설정

무선랜 설정						
Repeater 설정						
Service:	AP	Remote_SSID:				
기본설정						
SSID:	default	채널:	자동선택			
모드:	11g 모드(11b호환)	전송속도:	Best			
고급설정						
Short Preamble	Burst	WMM	Protection Mode	RTS Threshold	Fragmentation Threshold	TX Power
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2345 Bytes	2300 Bytes	20 dBm
보안설정						
<input type="checkbox"/> SSID 숨김						
보안정책: 사용안함						
ACL (Access Control List, MAC Address Filtering)						
ACL 정책: Open (ACL 체크하지 않음)						
ACL Database						
-등록된 MAC Address가 없습니다.-						
선택된 항목 삭제		00:00:00:00:00:00	추가			

• Repeater 설정

- Service : AP의 기능(AP/Repeater)을 선택합니다. 기본값으로 AP가 선택되어 있습니다.
- Remote_SSID : AP가 Repeater로 동작 할 경우 접속하고자 하는 AP의 SSID를 입력합니다.
 - * AP가 Repeater로 작동 될 경우 보안설정은 Remote-AP와 동일하게 설정해야 접속가능 합니다.
 - * AP가 NAT, VLAN, DHCP-SERVER, DHCP-RELAY 중 하나로 작동 될 경우 Repeater설정 항목은 화면에 보이지 않습니다.

WEB UI 상세설명

• 기본설정

- SSID : 무선네트워크 이름입니다. 최대 32자까지 입력할 수 있습니다.
- 채널 : 채널을 지정하십시오. '자동선택'으로 설정하면 점유율이 가장 낮은 채널을 자동으로 선택합니다. 하지만 고정적으로 채널을 지정할 것을 권장합니다.
- 모드 : 무선랜 운용모드를 지정합니다.
 - 11g : IEEE 802.11g(54Mbps) 모드로 설정합니다. 기본적으로 IEEE 802.11b(11Mbps)와 호환됩니다.
 - 11b : IEEE 802.11b(11Mbps) 모드로 설정합니다.
- 전송속도 : 최대 전송속도를 지정합니다. 일반적으로 best를 지정하여 사용하십시오. 주파수환경이 나쁜 경우에는 오히려 최대전송속도를 낮추는 것이 보다 안정적이고 높은 성능을 보일 수도 있습니다.

• 고급설정

- Short Preamble : 짧은 Preamble을 사용하여 오버헤드를 줄여 성능을 높일 수 있습니다. 주파수 환경이 나쁠 경우에는 오히려 성능을 저하시킬 수도 있습니다만 대개의 경우 Short Preamble을 사용하는 것이 성능이 좋습니다.
- Burst : 데이터 프레임간의 간격을 줄여 오버헤드를 줄여서 성능을 높여 줍니다.
- WMM : Wi-Fi Multimedia. 멀티미디어 패킷에 대해 우선순위를 높이는 기능입니다. 멀티미디어 패킷의 경우 일반적인 데이터 패킷에 비해 실시간성을 요합니다. 따라서 멀티미디어 패킷에 우선순위를 높여 음성이나 영상의 끊김 현상을 줄일 수 있습니다.

- Protection Mode : 11b 무선랜과 11g무선랜이 공존할 때 11g 데이터신호를 수신할 수 없는 11b 무선랜의 통신을 보호하는 것이라고 간단히 설명할 수 있습니다. 11b무선랜을 사용하지 않는다면 Protection Mode를 사용하지 않는 것이 전반적인 성능을 향상시킵니다.
- RTS Threshold : 주파수 환경이 좋지 않을 때(일례로 인접한 무선네트워크가 많을 때) RTS Threshold를 낮춰 주면 통신이 보다 안정적으로 이뤄질 수 있습니다.
- Fragmentation Threshold : RTS Threshold와 마찬가지로 주파수환경이 좋지 않을 경우 값을 낮춰 주십시오.
- TX Power : 여러 개의 무선네트워크를 운용할 경우(여러 대의 AP를 사용할 경우) 무선네트워크 상호간의 간섭을 줄이기 위해 TX Power를 줄여서 AP의 서비스 범위를 줄일 수 있습니다. 일반적으로는 TX Power를 최대값인 20dBm으로 지정하여 사용하십시오.

• 보안설정

- SSID 숨김 : SSID 숨김을 활성화하면 클라이언트에서 AP 탐색(스캔, scan)했을 때 SSID를 알 수 없도록 합니다. 무선랜에서 AP와 클라이언트의 접속 시 가장 기본이 되는 것이 SSID인데 이렇게 SSID 숨김이 되어 있을 경우 AP의 SSID를 알지 못하면 접속할 수 없도록 하여 보안성을 높일 수 있습니다.
- 보안정책 : AP가 Client로 사용될 경우 접속하고자 하는 AP와 동일한 보안정책을 설정해야 합니다.
 - 사용안함 : WEP이나 WPA-PSK를 사용하지 않습니다. 부득이한 경우가 아니라면 보안정책을 활성화 시켜 사용할 것을 권장합니다. 보안정책을 사용하지 않을 경우 공기 중으로 전파되는 무선랜의 특성상 누구나 여러분의 네트워크에 접근할 수 있게 됩니다.
 - WEP Key : WEP Key를 이용하여 무선네트워크의 보안을 유지할 수 있습니다. WPA/PSK를 사용할 수 없는 클라이언트가 존재하는 경우에 사용할 수 있습니다만 WPA/PSK방식에 비해 보안성이 많이 낮습니다. 보안정책으로 'WEP Key'를 선택하면 아래와같이 WEP Key 설정 화면이 표시됩니다.

WEB UI 상세설명

WEP Key 설정	
인증모드:	개방모드 (Open System) ▼
WEP Key Size:	128 bits ▼
Default Key:	default wepkey를 선택하십시오. ▼
Key 입력 방식:	ASCII (문자) ▼
WEP Key 1:	128bitwepkey1
WEP Key 2:	wepkeytest22
WEP Key 3:	wepkey128bits
WEP Key 4:	asciiwepkeyqq

- 인증모드 : 개방모드, 공유모드, 자동모드 세 가지 인증모드가 있습니다. 보안성은 개방모드가 높은 것으로 알려져 있습니다. (공유모드는 WEP Key가 일치하지 않으면 클라이언트의 접속을 거부합니다. 하지만 WEP Key를 확인하는 절차상에서 WEP Key가 해킹되어 노출될 수 있다는 사실이 밝혀졌습니다. 이에 반해 개방모드는 WEP Key가 일치하지 않더라도 클라이언트는 일단 접속이 가능하지만 WEP Key가 일치하지 않아 통신을 할 수 없습니다.)
- WEP Key Size : 64bit와 128bit 를 지원합니다. 당연히 128bit가 보안성이 높습니다. 모든 클라이언트가 128bit WEP Key를 지원한다면 128bit WEP Key를 사용하십시오.
- Default Key : 데이터를 전송할 때 사용하는 기본적으로 사용하는 Key입니다. 4 개의 WEP Key중 어느 것이라도 상관없이 사용할 수 있습니다만, 무선랜 카드의 종류에 따라 WEP Key를 하나만 입력할 수 있는 것들이 있으며 이럴 경우에는 Default Key를 반드시 Key 1]]로 지정하십시오.
- Key 입력 방식: 16진수 또는 ASCII문자로 WEP Key를 입력할 수 있습니다.

WPA-PSK 설정	
인증모드:	AUTO (WPA version1 or version2 Preshared Key) ▼
암호화 방식:	AUTO (TKIP or AES) ▼
그룹키 갱신주기:	600 초
Passphrase:	ThisIsWpsPskPassphraseExample

- 인증모드 : WPAv1-PSK와 WPAv2-PSK가 있으며, WPAv2-PSK가 보안성이 높습니다. 아직은 WPAv2-PSK를 지원하지 않는 무선랜카드가 많이 존재하므로 사용하는 무선랜카드의 지원여부를 확인하고 설정하십시오. 알 수 없을 경우 AUTO로 지정하십시오.
- 암호화 방식 : TKIP과 AES(=CCMP)를 지원합니다. 이 또한 무선랜카드의 지원여부를 확인하고 설정하거나 AUTO로 설정하십시오.
- 그룹키 갱신주기 : 브로드캐스트 혹은 멀티캐스트 패킷을 보낼 때 사용되는 그룹키를 갱신하는 주기를 설정합니다. 그룹키는 Passphrase를 바탕으로 AP에서 자동으로 생성되면 주어진 주기에 따라 자동으로 갱신됩니다.
- Passphrase : 이 Passphrase에 의해 그룹키를 비롯한 데이터 암호와 인증에 사용되는 암호키들이 생성됩니다. AP와 AP에 접속을 원하는 클라이언트는 이 Passphrase를 동일하게 설정해야 합니다.

WEB UI 상세설명

- WPA-EAP(Extensible Authentication Protocol) : Radius Server를 통한 인증이 필요할 경우 선택합니다.

WPA-EAP 설정	
인증모드:	WPA
암호화 방식:	AUTO (TKIP or AES) 그룹키 갱신주기: 600 초
Radius Server:	192.168.0.10
Radius Port:	1812
Radius Secret:	Atheros

- 인증모드 : WPA와 WPA2가 있으며, WPA2가 보안성이 높습니다. 사용하는 무선랜카드의 지원여부를 확인하고 설정하십시오. 알 수 없을 경우 AUTO로 지정하십시오.
- 암호화 방식 : TKIP과 AES(=CCMP)를 지원합니다. 이 또한 무선랜카드의 지원여부를 확인하고 설정하거나 AUTO로 설정하십시오.
- 그룹키 갱신주기 : 브로드캐스트 혹은 멀티캐스트 패킷을 보낼 때 사용되는 그룹키를 갱신하는 주기를 설정합니다. 그룹키는 Passphrase를 바탕으로 AP에서 자동으로 생성되면 주어진 주기에 따라 자동으로 갱신됩니다.
- Radius Server : Radius Server의 IP 주소를 입력합니다.
- Radius Port : AP와 서버가 통신에 사용할 포트 번호를 입력합니다. 기본적으로 RADIUS 서버는 포트 1812에서 통신합니다.
- Radius Secret : 공유 비밀번호를 입력합니다. 이것은 RADIUS 서버와 AP가 공유하는 암호입니다. RADIUS 서버에서도 같은 암호를 구성해야 합니다.

• ACL

- ACL : Access Control List. 모든 네트워크장비는 고유의 MAC Address를 가지게 됩니다. 이 MAC Address를 이용해서 접속을 허용하거나 막을 수 있습니다. (※ 하지만, ACL은 접속 자체를 통제할 수 있지만 접속된 클라이언트들이 송수신하는 데이터를 보호할 수는 없습니다. 데이터 보호를 위해서는 보안정책을 반드시 사용해야 합니다.). ACL 정책에는 다음 세 가지가 있습니다.
 - Open : ACL을 사용하지 않습니다.
 - Allow : ACL Database에 등록된 MAC Address의 무선랜 클라이언트만 접속을 허용합니다.
 - Deny : ACL Database에 등록된 MAC Address의 무선랜 클라이언트의 접속을 거부합니다.

WEB UI 상세설명

2.3.3. MULTI-SSID

Multi-SSID 설정

기본설정

Multi-SSID	VLAN	BSS INDEX	SSID	VLAN ID
<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	default	0

VLAN_IP 설정

VLAN_IP 설정

VLAN_IP 주소:

VLAN_서브넷마스크:

VLAN_게이트웨이주소:

보안정책: 사용안함

Multi-SSID

삭제	INDEX	SSID	보안정책	VLAN ID
<input type="checkbox"/>	1	default	없음	0
<input type="checkbox"/>	2		없음	0
<input type="checkbox"/>	3		없음	0
<input type="checkbox"/>	4		없음	0

* 본 화면은 Repeater, NAT, DHCP 중 하나가 설정되었을 경우 접속되지 않습니다.

* 복수개의 BSS INDEX 설정을 위해서는 각 BSS 별로 설정/저장을 반복 해야 합니다.

• 기본설정

- Multi-SSID : Multi-SSID 사용여부를 나타내며, 항상 Enable 상태입니다.

- VLAN : VLAN 사용 여부를 선택합니다.

- BSS INDEX : 4개의 BSS 설정이 가능하며, BSS 변경시 해당 BSS의 정보를 보여줍니다.

- SSID : BSS INDEX에 지정된 BSS의 SSID를 입력합니다.

- VLAN ID : VLAN이 DISABLE 상태일 경우 "0"값을 가지며, VLAN이 ENABLE 되었을 경우 ID(1 ~ 4094)를 입력합니다.

• VLAN_IP 설정 : BSS INDEX와 상관없이 동일하게 설정됩니다. 현재 사용되지 않는 IP대역일 경우 디폴트 값을 사용하도록 권장합니다.

- VLAN_IP 주소 : VLAN IP를 입력합니다. 입력하지 않을 경우 "192.168.1.254"가 설정됩니다.

- VLAN_서브넷마스크 : VLAN 서브넷마스크를 입력합니다. 입력하지 않을 경우 "255.255.255.0"가 설정됩니다.

- VLAN_게이트웨이주소 : VLAN 게이트웨이를 입력합니다. 입력하지 않을 경우 "192.168.1.1"가 설정됩니다.

• 보안정책

- 각 BSS INDEX별로 보안정책이 설정되며, WEP Key의 경우 하나의 BSS에만 설정 가능하다.

이하 설정은 "무선랜 설정" 메뉴의 보안설정과 동일합니다.

• Multi-SSID

- 현재 설정된 Multi-SSID/VLAN 상태를 보여줍니다. INDEX 2 이상의 BSS가 설정 될 경우 삭제메뉴 박스가 활성화 됩니다. INDEX 1 BSS 는 삭제 불가능합니다.

WEB UI 상세설명

2.3.4. NAT/DHCP

NAT/DHCP 설정		
NAT 설정		
NAT <input type="checkbox"/> 인터페이스별 IP 설정		
<input type="checkbox"/>	무선인터페이스 무선 IP를 설정할 수 없습니다.	유선인터페이스 유선 IP를 설정할 수 없습니다.
DHCP 설정		
DHCP SERVER <input type="checkbox"/>	DHCP CLIENT <input type="checkbox"/>	DHCP RELAY <input type="checkbox"/>
DHCP-SERVER, RELAY 설정		

* NAT는 외부 네트워크에 알려진 것과 다른 IP 주소를 사용하는 내부 네트워크에서, IP 주소를 변환해 주는 기능을 합니다.

* Repeater, VLAN 중 일부가 설정되어 있을 경우 DHCP CLIENT기능만 사용 가능합니다.

- NAT설정 : NAT(Network Address Translation) 사용 여부를 선택합니다.
NAT를 사용하고자할 경우 다음과 같은 창이 추가로 보여집니다.

무선인터페이스	유선인터페이스
게이트웨이 : 192.168.250.10	IP 주소 : 192.168.0.254
	서브넷마스크 : 255.255.255.0
	게이트웨이주소 : 192.168.0.1

- 무선인터페이스 : 무선 클라이언트가 접속할 수 있는 환경을 설정합니다.

- 게이트웨이 : 게이트웨이를 설정합니다.(Default : 192.168.250.10)

- 유선인터페이스 : AP가 접속 할 환경을 설정합니다. 현재 설정된 유선 환경을 보여줍니다.

- IP 주소 : IP 주소를 설정합니다.
- 서브넷마스크 : 서브넷마스크를 설정합니다.
- 게이트웨이주소 : 게이트웨이주소를 설정합니다.

- DHCP 설정 : NAT를 사용하지 않을경우 DHCP는 SERVER/CLIENT 중 1개 또는 SERVER/RELAY 중 1개만 사용 가능하며, CLIENT/RELAY는 동시 사용 가능합니다. 또한 NAT가 사용중일 경우 SERVER/RELAY 중 1개만 사용 가능하며, CLIENT는 어느 경우에도 사용 가능합니다.

- DHCP SERVER : AP가 DHCP SERVER 기능을 하도록 설정합니다. DHCP SERVER 기능을 사용하려면 무선인터페이스의 게이트웨이를 지정해야 하며, 지정된 게이트웨이는 DHCP SERVER의 IP가 됩니다. 따라서 할당 해 주는 IP범위에 포함되지 않도록 주의 바랍니다.

DHCP-SERVER, RELAY 설정	
IP 설정 범위:	192.168.250.11 ~ 192.168.250.254
서브넷마스크:	255.255.255.0
DNS 주소:	61.97.112.155 61.97.113.250
WINS:	192.168.250.1
도메인:	
LEASE(초):	864000

WEB UI 상세설명

- IP 설정범위 : AP의 DHCP 서버가 할당할 수 있는 IP 범위를 지정합니다.
 - 서브넷마스크 : 서브넷마스크를 지정합니다.
 - DNS 주소 : DNS 주소를 지정합니다.
 - WINS : WINS를 지정합니다.
 - 도메인 : 도메인을 지정합니다.
 - LEASE(초) : 서버가 할당한 IP의 사용기간을 초 단위로 지정합니다. DEFAULT 값은 864,000초(10일) 입니다.
- DHCP CLIENT : AP의 유선인터페이스가 CLIENT로 동작하도록 설정됩니다. CLIENT 기능을 사용 할 경우 NAT의 유선 인터페이스 설정항목이 제한됩니다.
- DHCP RELAY : AP가 DHCP RELAY 기능을 하도록 설정합니다.

DHCP-SERVER, RELAY 설정

DHCP 서버:

- DHCP 서버 : AP가 RELAY로 동작 할 경우 CLIENT가 IP 주소를 받을 수 있는 DHCP서버의 IP를 입력 합니다.

2.4. 시스템 관리도구

시스템 관리도구	
관리자 암호	관리자 암호를 변경할 수 있습니다. 관리자 암호는 콘솔, 텔넷, 웹 모두에 적용됩니다.
설정 초기화	모든 설정을 공장출하 상태로 초기화시킬 수 있습니다.
업그레이드	AP 펌웨어를 업그레이드할 수 있습니다.
재시작	AP를 재시작 시킬 수 있습니다.

- 관리자 메뉴는 AP설치자(관리자)를 위한 메뉴입니다.
임의로 변경시 문제 발생의 소지가 있으니 가급적 변경을 자제해 주세요.

2.4.1. 관리자 암호

- 관리자 암호를 변경합니다. WEB UI뿐만 아니라 텔넷과 콘솔 로그인 암호도 함께 변경됩니다.
변경된 암호를 잘 기억하십시오.

관리자 암호	
관리자 암호를 변경할 수 있습니다. 콘솔과 텔넷으로 접속할 때의 암호도 변경됩니다. 변경된 암호를 잘 기억하십시오.	
새 관리자 암호:	<input type="text"/>
관리자 암호 확인:	<input type="text"/>

WEB UI 상세설명

2.4.2. 설정초기화

- AP의 모든 설정을 '1.1 AP이 디폴트 설정값' 에 명시된 공장출하 상태로 초기화 시킵니다.



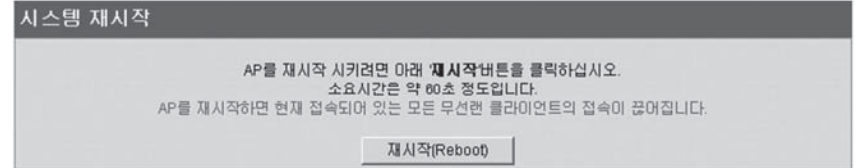
2.4.3. 업그레이드

- AP의 펌웨어를 업그레이드 합니다.

※ 설치 기사 이외에는 절대 사용하지 마십시오. AP를 사용할 수 없게 될 수도 있습니다.

2.4.4. 재시작

- AP를 재시작(Reboot)시킬 수 있습니다.



이상이 생기면

■ 고장이라고 생각하기 전에...

- 제품 사용중 이상이 있으면 아래 내용을 먼저 점검한 후 구입처나 서비스 센터로 연락합니다.
지정된 곳을 통하여 설치하지 않았거나 임의로 분해·조립하여 문제가 발생한 경우 무상수리를 받을 수 없습니다.

증 상	확 인 사 항
네트워크 연결이 되지 않아요.	<ul style="list-style-type: none"> - 전원 및 무선랜 램프가 정상적으로 동작되어 있는지 확인해 보세요. - 현재 사용중인 컴퓨터의 무선 네트워크 설정 정보를 확인해 보세요. - 보안 정책 등 설정값이 AP의 설정값과 일치하지 않으면 접속이 되지 않습니다.
인터넷이 되지 않아요.	<ul style="list-style-type: none"> - 인터넷 서비스에 가입이 되어 있는지 확인해 보세요. - 본 AP는 외부 인터넷망 서비스는 제공하지 않습니다. 꼭 인터넷 서비스에 가입하신 후 사용하세요. - 현재 사용중인 컴퓨터의 무선 네트워크 설정 정보를 확인해 보세요. - 보안 정책 등 설정값이 AP의 설정값과 일치하지 않으면 통신이 되지 않습니다.
속도가 느려요.	<ul style="list-style-type: none"> - 무선랜 기능의 특성상 가전기기 및 주변 전자제품 특히, 타사 AP에 의해 통신에 지장을 받을 수 있습니다. - AP와의 거리가 멀거나 중간에 장애물이 있는 경우 통신이 불안해 질 수 있습니다. AP와의 거리를 가깝게 하거나 장애물을 제거한 후 다시 시도해 보세요. - 보안 정책을 사용하게 되면 사용하지 않을 경우보다 속도가 느려집니다. - 사용중인 컴퓨터의 무선랜카드 사양을 확인해 보세요. 랜카드가 802.11b만 지원할 경우 11Mbps 이하의 속도만 가능합니다. 무선랜카드 드라이버가 구버전일 경우 속도에 영향을 미칠 수 있습니다.

제품 규격

- 제품의 규격

구 분	DM-350AP / DM-450AP
사용전원	DC 12V, 300mA
소비전력	Max 10W 이하
무선랜	IEEE 802.11b/g, 13채널 지원
중 량	84g
제 원	직경 : 110mm. 두께 : 40mm

MEMO

dongyoung media

Lined writing area on the left page, consisting of 15 horizontal dotted lines.

Lined writing area on the right page, consisting of 15 horizontal dotted lines.

