



Aruba Instant AP 설정 가이드

[Version 6.1.3.4]

(주)애플씨

OCT, 2012

Contents

1. Quick Start

2. 신규 네트워크 설정

3. IAP 인터페이스

4. IAP 세부설정





1. Quick Start

1.1 Instant AP 연결 및 접속

❖ 최초 IAP 설정을 위해서는 다음의 절차를 거쳐야 한다.

1. 전원 인가

- IAP에 전원을 인가하는 방법은 다음 두 가지가 있다.
 - 1) IEEE 802.3af PoE source
 - 2) 외부 AC-DC adapter (별도 구매 필요)

2. IAP의 Ethernet Port 연결

- IAP가 동작하기 위해서는 IAP의 Ethernet Port의 Link가 반드시 Up 상태여야 한다.

3. IP address 설정

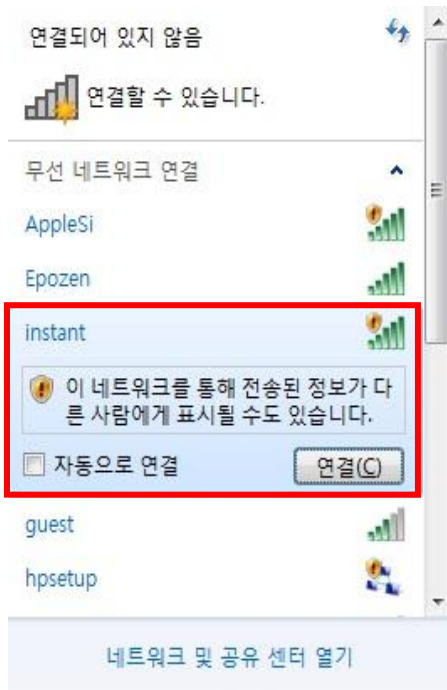
- 네트워크 상에 DHCP서버가 있을 때: DHCP로부터 IP address 자동 부여
- 네트워크 상에 DHCP서버가 없을 때:
 - 1) Console을 통해 수동으로 IP address 부여
 - 2) 자동 IP부여 실패 시 설정되는 기본 IP address (169.x.x.x) 사용
(단, 이 방법은 DHCP를 통한 자동 IP부여가 실패할 때까지 기다려야 하므로 시간이 걸림)

```
Model: AP-10x
CPU: AR7161 revision: A2
Clock: 680 MHz, DDR clock: 340 MHz, Bus clock: 170 MHz
DRAM: 128 MB
POST1: passed
Copy: done
Flash: 16 MB
PCI: scanning bus 0 ...
      dev fn verID devID class rev  MBAR0  MBAR1  MBAR2  MBAR3
      00 00 168c 0029 00002 01 10000000 00000000 00000000 00000000
      01 00 168c 0029 00002 01 10010000 00000000 00000000 00000000
Net: eth0
Radio: ar922x#0, ar922x#1

Hit <Enter> to stop autoboot: 0
apboot> setenv ipaddr 192.168.0.100
apboot> setenv netmask 255.255.255.0
apboot> setenv gatewayip 192.168.0.1
apboot> save
```

[Console을 이용한 수동 IP 설정]

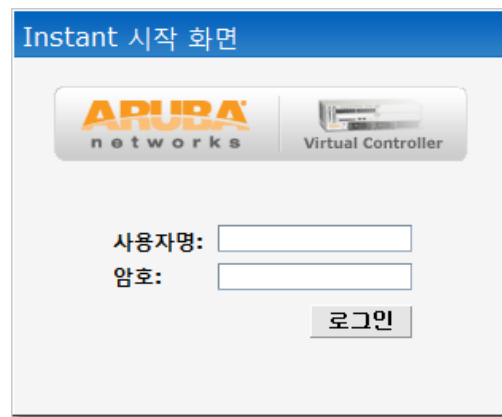
1.1 Instant AP 연결 및 접속(계속)



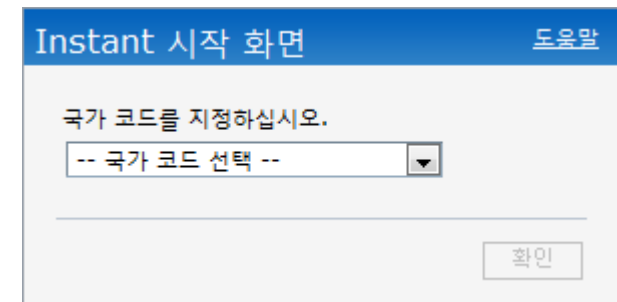
[무선 접속]

1개의 네트워크						
이름	클라이언트	유형	Radio 밴드	인증 방법	키 관리	IP 할당
instant	0	직렬	2.4	없음	없음	NAT Mode
신규						

[초기 SSID(instant) 정보]



[WebUI login 창]



[국가코드 설정 창]

4. IAP 설정을 위한 provisioning용 무선 네트워크 접속

- 전원인가, Ethernet 연결 및 IP address 부여가 끝나면 그림 1-2와 같이 'instant'라는 provisioning용 무선 네트워크(SSID)가 방사되며 노트북 등 무선단말에서 확인 및 접속이 가능하다.
- 'instant'는 IAP provisioning을 위해 2.4GHz 밴드에 대해서 인증 없이 접속할 수 있도록 미리 설정되어 있는 무선 네트워크(SSID)이며 이를 통한 인터넷접속은 불가능하다.(그림 1-3 참조)

5. IAP login 및 국가코드 설정

- 'instant'에 접속 후 웹 브라우저를 이용하여 'instant.arubanetworks.com'으로 접속한 후 login 한다. (그림 1-4 참조)
- 초기 login ID 및 Password는 'admin/admin'이다.
- Login이 완료되면 국가코드 설정창이 나타나는데 'KR - Republic of Korea(South Korea)'로 설정 후 'OK'를 선택하면 설정 준비가 끝나게 된다. (그림 1-5 참조)

1.2 초기 화면



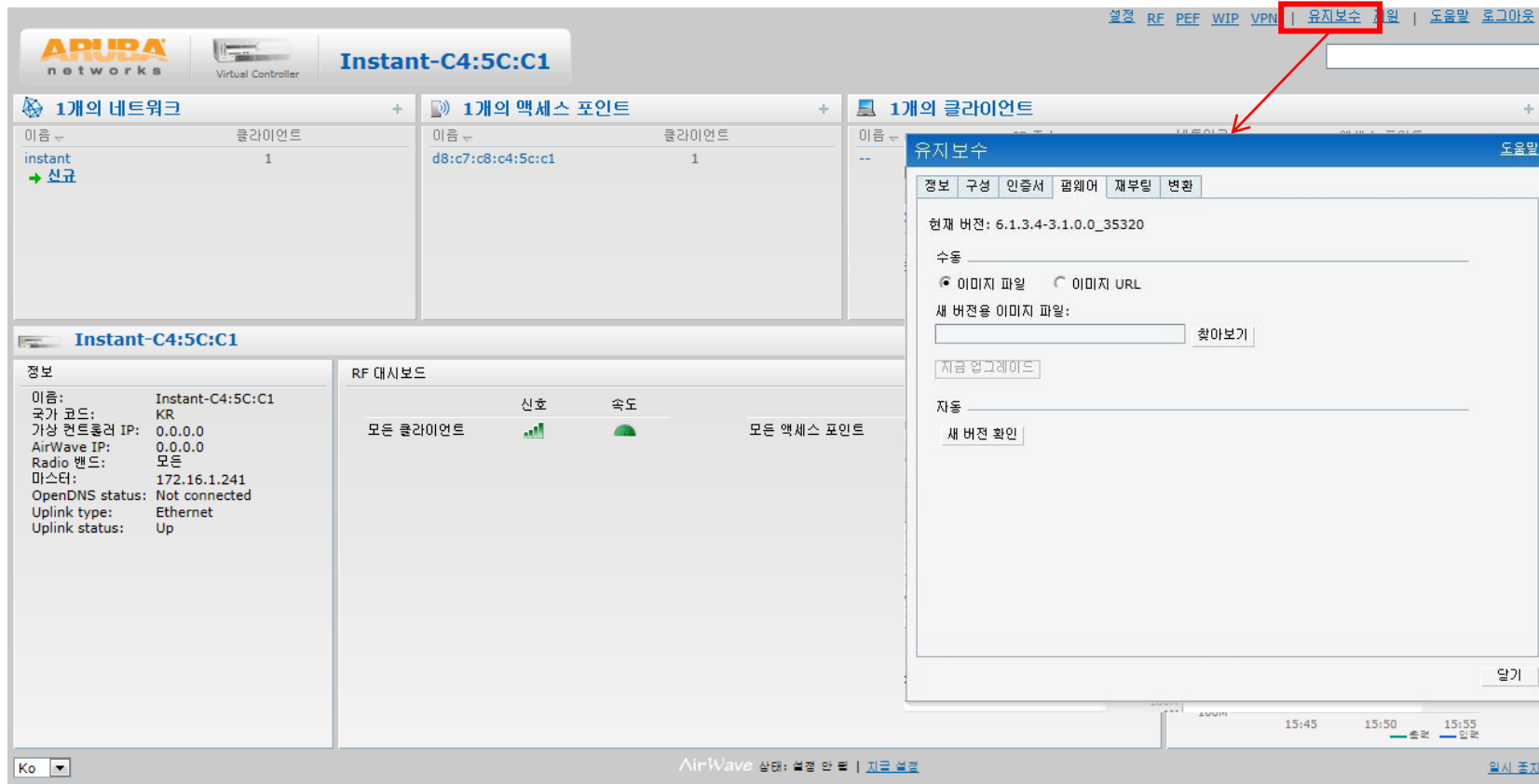
[초기 화면]

❖ 접속이 완료된 후 보이는 초기 화면은 그림 1-6과 같다.

- 네트워크: SSID 설정 창이며 초기 SSID인 instant가 보임
- 액세스 포인트: 현재 동작중인 AP(Virtual Controller 및 연동중인 다른 AP)들이 보임
- 클라이언트: 현재 접속중인 client가 보임
- 모니터링: 각 항목별 세부정보 확인 가능(기본적으로 Virtual Controller에 대한 정보 표시)

❖ 화면의 오른쪽 상단에 있는 도움말 메뉴 선택 시 녹색, 기울임 꼴로 변하는 항목에 대해 간략한 설명을 볼 수 있다.

1.3 새 버전 체크 및 업그레이드



[초기 화면 > 버전 체크 및 업그레이드]

- ❖ IAP를 설정하기에 앞서 우선 현재 IAP의 펌웨어가 최신이 아니라면 업그레이드를 할 필요가 있다.
- ❖ 펌웨어 업그레이드는 다음과 같이 두 가지 방법으로 할 수 있다.
 - 자동: 화면 상단 메뉴에 보이는 '새 버전 사용가능' (신규버전이 있을 때만 보임)을 실행하거나 '유지보수' → '펌웨어' 메뉴에서 '새버전 확인' 후 '지금 업그레이드' 실행
 - 수동: '유지보수' → '펌웨어' 메뉴에서 PC 등에 미리 다운로드 받아 둔 펌웨어를 '찾아보기'로 선택한 후 '지금 업그레이드' 실행



2. 신규 네트워크 설정



2.1 네트워크 추가

The screenshot shows the Aruba Instant-CC:90:7C web interface. At the top, there's a navigation bar with links like '설정', 'RF', 'PEF', 'WIP', 'VPN', '요선', '유지보수', '지원', '도움말', and '로그아웃'. Below this, the main content area is divided into three sections: '1개의 네트워크' (1 Network), '1개의 액세스 포인트' (1 Access Point), and '1개의 클라이언트' (1 Client). The '1개의 네트워크' section has a table with columns '이름' (Name) and '클라이언트' (Client). The first row shows 'instant' with '1' client. A red box highlights a '+ 신규' (New) button next to the 'instant' entry. The '1개의 액세스 포인트' section shows a table with '이름' (Name) and '클라이언트' (Client), with one entry 'd8:c7:c8:cc:90:7c' and '1' client. The '1개의 클라이언트' section shows a table with '이름' (Name), 'IP 주소' (IP Address), '네트워크' (Network), and '액세스 포인트' (Access Point), with one entry '192.168.11.25' connected to 'instant' and 'd8:c7:c8:cc:90:7c'. Below these sections, there's a '정보' (Info) section on the left with details about the controller, an 'RF 대시보드' (RF Dashboard) in the middle showing a table of clients and their status, and '사용 추이' (Usage History) on the right with two line graphs showing client usage and throughput over time.

[초기 화면 > 네트워크 > 신규]

- ❖ 네트워크 탭에서 '신규'를 클릭하면 '새 네트워크' 창이 뜨는데 이 창을 이용하여 서비스하고자 하는 새로운 무선 네트워크 (SSID)를 추가할 수 있다.

2.2 WLAN Setting

New WLAN

1 WLAN Settings 2 VLAN 3 보안 4 액세스

WLAN Settings

Name & Usage

이름(SSID): demo

주 사용: ☒ 직원 ☐ 음성 ☐ 게스트

브로드캐스트/멀티캐스트

브로드캐스트 필터링: 사용 안 함

DTIM 간격: 1 신호

멀티캐스트 최적화: 사용 안 함

Dynamic multicast optimization: 사용 안 함

DMO channel utilization threshold: %

대역폭 제한

☐ Airtime ☐ 각 사용자 ☐ 각 무선

전송율

2.4GHz: 최소: 1 최대: 54

5GHz: 최소: 6 최대: 54

Miscellaneous

콘텐츠 필터링: 사용 안 함

Radio 밴드: 모든

비활성 시간 제한: 1000 초

SSID 숨기기: ☐

[고급 옵션 숨기기](#)

다음 취소

[New WLAN > WLAN Setting]

- ❖ 첫 번째 단계에서 생성할 네트워크의 기본 정보를 설정한다. '고급옵션표기'를 선택하면 상세설정이 가능하다.
 - 이름(SSID) : 사용할 무선네트워크 이름(SSID) 지정
 - 주 사용: 사용할 네트워크의 타입 지정
 - 직원: 내부사용자 용, Key 방식 혹은 802.1x 방식의 인증 지원
 - 음성: voice 용 handset이나 voice 수준의 QoS가 필요한 어플리케이션 용
 - 게스트: 손님 용, Virtual controller가 사설 IP를 할당하도록 기본 설정 됨. Captive portal 혹은 Key 방식의 인증 지원
 - 대역폭제한: 3가지 형태의 대역폭 제한 설정 가능
 - 방송시간(% of Airtime): 해당 네트워크(SSID)에 있는 모든 단말들이 사용할 수 있는 Airtime의 총합 (% 단위)
 - 각 사용자(Each user): 해당 네트워크(SSID)에 있는 사용자(단말)당 Throughput (kbps 단위)
 - 각 무선(Each radio): Radio별로 접속된 사용자(단말)에 허용되는 Throughput(kbps)의 총합 (kbps 단위)

2.2 WLAN Setting(계속)

New WLAN

1 WLAN Settings 2 VLAN 3 보안 4 액세스

WLAN Settings

Name & Usage

이름(SSID): demo

주 사용: ☒ 작업 ☐ 음성 ☐ 게스트

대역폭 제한

☐ Airtime ☐ 각 사용자 ☐ 각 무선

전송률

2.4GHz: 최소: 1 최대: 54
5GHz: 최소: 6 최대: 54

Miscellaneous

콘텐츠 필터링: 사용 안 함
Radio 밴드: 모든
비활성 시간 제한: 1000 초
SSID 숨기기: ☐

브로드캐스트/멀티캐스트

브로드캐스트 필터링: 사용 안 함
DTIM 간격: 1 신호
멀티캐스트 최적화: 사용 안 함
Dynamic multicast optimization: 사용 안 함
DMO channel utilization threshold: 0 %

고급 옵션 숨기기

다음 취소

[New WLAN > WLAN Setting]

- Miscellaneous

- 콘텐츠 필터링: 모든 non-corporate domain에 대한 모든 DNS 요청을 OpenDNS로 보내는 기능 콘텐츠 필터링 설정
- 대역(Band): 무선 네트워크(SSID)에서 사용할 대역 지정 - 모든, 2.4GHz, 5GHz
- 비활성 시간 제한: Idle 단말이 IAP에서 없어지는 시간(초)으로 최소 60초, 기본 값은 1,000초
- SSID 숨기기: 무선 네트워크(SSID) 이름을 사용자들이 볼 수 없도록 설정

- 브로드캐스트/멀티캐스트

- 멀티캐스트 최적화: 브로드캐스트 및 멀티캐스트 프레임 송신에 필요한 최적의 속도 보장. 활성화 시 기본 1Mbps(2.4GHz 대역) 및 6Mbps(5GHz 대역) 대비 최대 24Mbps까지 성능개선 가능
- 브로드캐스트 필터링:
 - ✓ '모든'으로 설정 시 DHCP와 ARP를 제외한 모든 브로드캐스트와 멀티캐스트는 프레임을 drop
 - ✓ 'ARP'로 설정 시 '모든' 설정 값이 적용됨과 동시에 ARP request를 unicast로 변환해서 해당 단말에게 직접 전달
- DTIM 간격: 무선단말이 수신할 데이터가 IAP에 있는지 확인하는 주기로 단위는 Beacon을 사용. 보이스 통신 등에서 단말의 power saving을 목적으로 더 큰값을 설정할 수 있음

- 전송률: SSID별 기본 및 지원 전송률 설정. 각 밴드 별 최소 및 최대 legacy(non-802.11n) 전송률 지정

2.3 VLAN

New WLAN

1 WLAN Settings 2 VLAN 3 보안 4 액세스

클라이언트 IP 및 VLAN 할당

클라이언트 IP 할당: ☐ 가상 컨트롤러 할당됨 ☒ 네트워크 할당됨

클라이언트 VLAN 할당: ☒ 기본값 ☐ 정적 ☐ 동적

VLAN ID: 1

VLAN Assignment Rules
Default VLAN: 1

새 VLAN 할당 규칙

속성: AP-Group 운영자: 포함 문자열: VLAN:

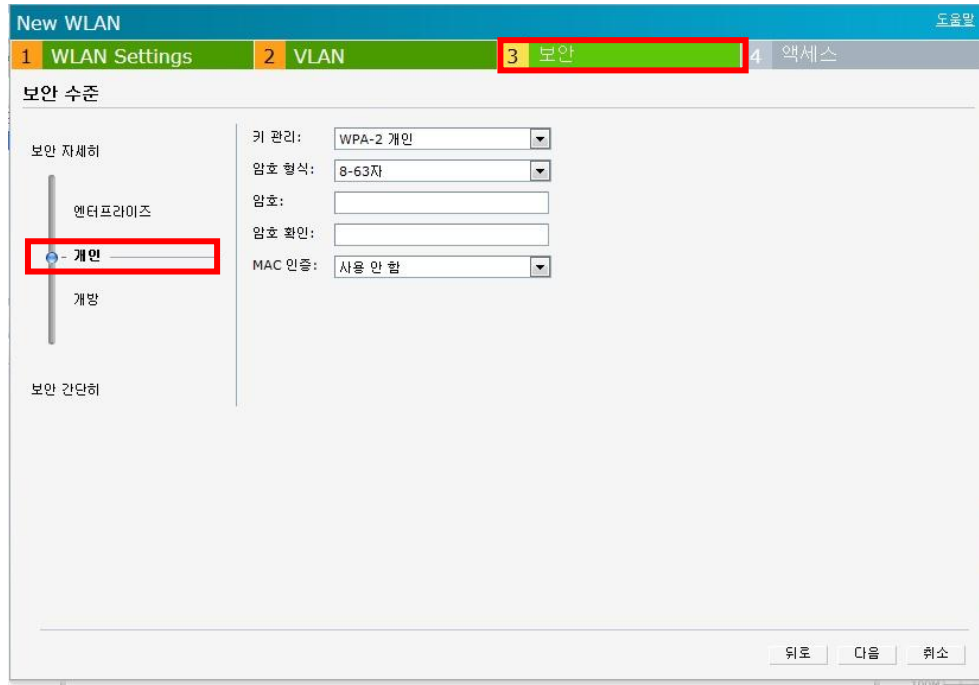
확인 취소

뒤로 다음 취소

[New WLAN > VLAN]

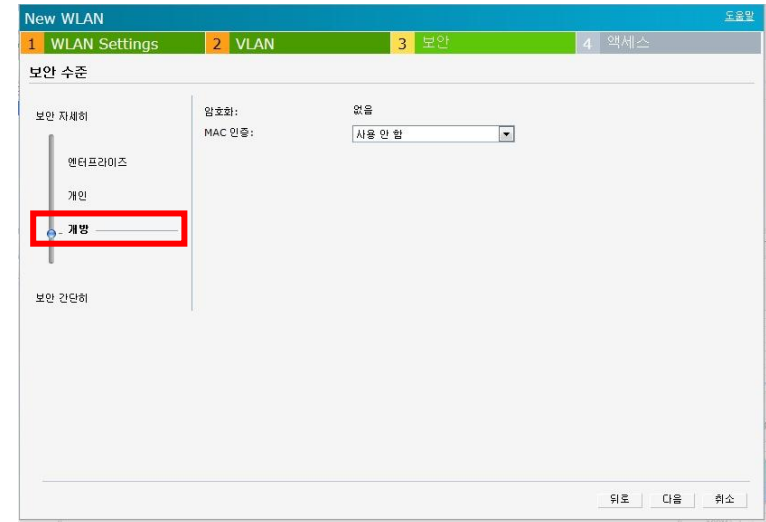
- 클라이언트 IP 할당 : 무선 단말의 IP 할당 방법 지정
 - 가상 컨트롤러 할당됨: 가상 컨트롤러가 DHCP서버가 되어 단말에 대해 사설 IP 할당
 - 네트워크 할당됨: AP가 연결된 네트워크에 있는 DHCP 서버로부터 IP를 자동으로 받도록 설정(기본값)하거나 AP가 802.1Q trunk로 연결되어 있는 경우 특정 VLAN ID를 지정해서 해당 VLAN에 있는 DHCP 서버로부터 IP를 자동으로 받도록 설정
- 클라이언트 VLAN 할당 : VLAN 할당 방법 지정
 - 기본값 : Native VLAN 할당
 - 정적 : 내부 네트워크 구성에 따라 정적 VLAN Tag 가능
 - 동적 : 외부 인증서버와 연동할 경우 속성값(역할:Role)에 따른 개별 VLAN을 할당

2.4 보안 - 직원용



The screenshot shows the 'New WLAN' configuration window with the '보안' (Security) tab selected. The '보안 수준' (Security Level) is set to '개인' (Personal), which is highlighted with a red box. The '키 관리' (Key Management) is set to 'WPA-2 개인' (WPA-2 Personal), '암호 형식' (Encryption Type) is '8-63자' (8-63 characters), and 'MAC 인증' (MAC Authentication) is '사용 안 함' (Not used).

[New WLAN > 보안(개인)]



The screenshot shows the 'New WLAN' configuration window with the '보안' (Security) tab selected. The '보안 수준' (Security Level) is set to '개방' (Open), which is highlighted with a red box. The '암호화' (Encryption) is set to '없음' (None) and 'MAC 인증' (MAC Authentication) is '사용 안 함' (Not used).

[New WLAN > 보안(개방)]

❖ 보안: 무선 네트워크(SSID)에 대한 보안수준을 설정한다.

- 개방: 사용자인증 및 데이터 암호화를 사용하지 않는 경우 설정, 필요 시 MAC 인증 사용 가능
- 개인: 보안 수준 설정의 기본 값이며 PSK방식의 사용자인증 및 데이터 암호화 설정. 필요 시 MAC 인증 병행 사용 가능
 - 키 관리: WPA Personal, WPA-2 Personal, Both(WPA-2 & WPA), Static WEP 지원
 - 암호형식: WPA 혹은 WPA-2의 경우 8-63 chars 혹은 64 hexadecimal chars 선택 가능하며 Static WEP의 경우 64-bit 혹은 128-bit WEP Key 선택이 가능

2.4 보안 - 직원용(계속)

New WLAN

1 WLAN Settings 2 VLAN 3 보안 4 액세스

보안 수준

보안 자체화

엔터프라이즈

개인

개방

보안 간단히

키 관리: WPA-2 엔터프라이즈

종단: 사용 안 함

인증 서버 1: InternalServer

재인증 간격: 0 분

불랙리스트: 사용 안 함

내부 서버: No users 사용자

내부 서버: No certificate 인증서 업로드

뒤로 다음 취소

[New WLAN > 보안(엔터프라이즈)]

- 엔터프라이즈: 인증서 기반의 802.1x 사용자인증 및 암호화 설정이 가능
 - Key 관리: WPA 엔터프라이즈, WPA-2 엔터프라이즈, Both(WPA-2 & WPA), Dynamic WEP with 802.1x 지원
 - Termination: EAP termination을 IAP에서 처리할지 여부 설정. 내부 인증서 서버 사용 시에는 반드시 사용해야 함
 - 인증서 서버 1: 내부 인증서 서버 혹은 외부 인증서 서버 설정 가능
 - 인증서 서버 2: 인증서 서버 1에서 외부 인증서 서버 설정 시 나타나는 메뉴이며 인증서 서버 이중화 설정 시 필요
 - 재인증 간격: 0보다 큰 값 입력 시 IAP는 접속 및 인증된 모든 단말들은 주기적으로 재인증 함
 - 내부 서버용: 내부 서버 인증 시 필요한 계정(사용자) 및 인증서(별도의 인증서 필요) 관리
 - 계정(Accounting): 외부 인증서 서버 연동 시 IAP는 RADIUS START 및 RADIUS STOP과 같은 accounting 레코드를 전달
 - 계정 간격(Accounting interval): 0보다 큰 값 입력 시 IAP는 RADIUS INTERIM과 같은 accounting 레코드를 주기적으로 전달

2.4 보안 - 게스트용

The screenshot shows the 'New WLAN' configuration interface with the '보안' (Security) tab selected. The 'Splash page type' is set to '내부 - 확인됨' (Internal - Verified). The 'Splash Page Visuals' section displays a preview of the guest network splash page. The '암호화' (Encryption) dropdown is set to '사용 안 함' (Not used). The 'Redirect URL' field is empty. Navigation buttons at the bottom are '뒤로' (Back), '다음' (Next), and '취소' (Cancel).

New WLAN

1 WLAN Settings 2 VLAN 3 보안 4 액세스 도움말

보안 수준

Splash page type: 내부 - 확인됨

Splash Page Visuals

Welcome to Guest Network

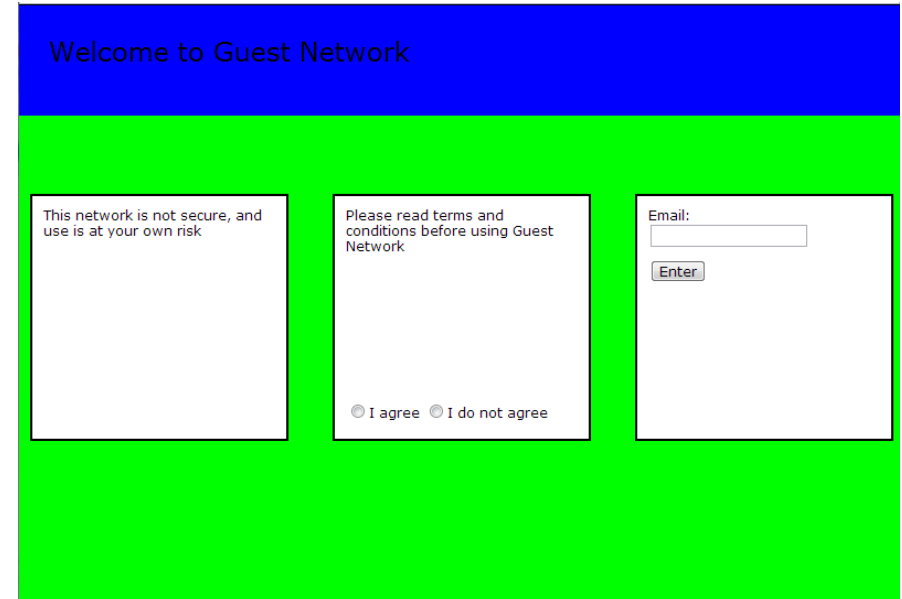
Click thumbnail above to edit [미리 보기](#)

암호화: 사용 안 함

Redirect URL: (Optional)

뒤로 다음 취소

[New WLAN > 보안(내부-확인됨)]



[무선 접속자 첫 페이지 화면]

❖ 보안: 무선 네트워크(SSID)에 대한 보안수준을 설정한다.

- Splash page type = 내부 - 확인됨 : E-mail 계정을 입력, 접속시 AP상 클라이언트 이름이 입력한 E-mail 값으로 보여짐.
암호화(PSK) 동시 사용 가능
- Splash page Visuals : 게스트 페이지 수정 가능 (배경색, TEXT)

2.4 보안 - 게스트용(계속)

New WLAN 도움말

1 WLAN Settings 2 VLAN 3 보안 4 액세스

보안 수준

Splash page type: 내부 - 인증됨

인증 서버 1: InternalServer

재인증 간격: 0 분

블랙리스트: 사용 안 함

내부 서버: 1 User

내부 서버: No certificate [인증서 업로드](#)

암호화: 사용 안 함

Splash Page Visuals

Welcome to Guest Network

Click thumbnail above to edit [미리 보기](#)

Redirect URL: (Optional)

뒤로 다음 취소

[New WLAN > 보안(내부-인증됨)]

- Splash page type = 내부 - 인증됨 : 인증서버와 연동하여 계정 정보를 입력
- Splash page Visuals : 게스트 페이지 수정 가능 (배경색, TEXT)

Welcome to Guest Network

This network is not secure, and use is at your own risk

Please read terms and conditions before using Guest Network

User Name:

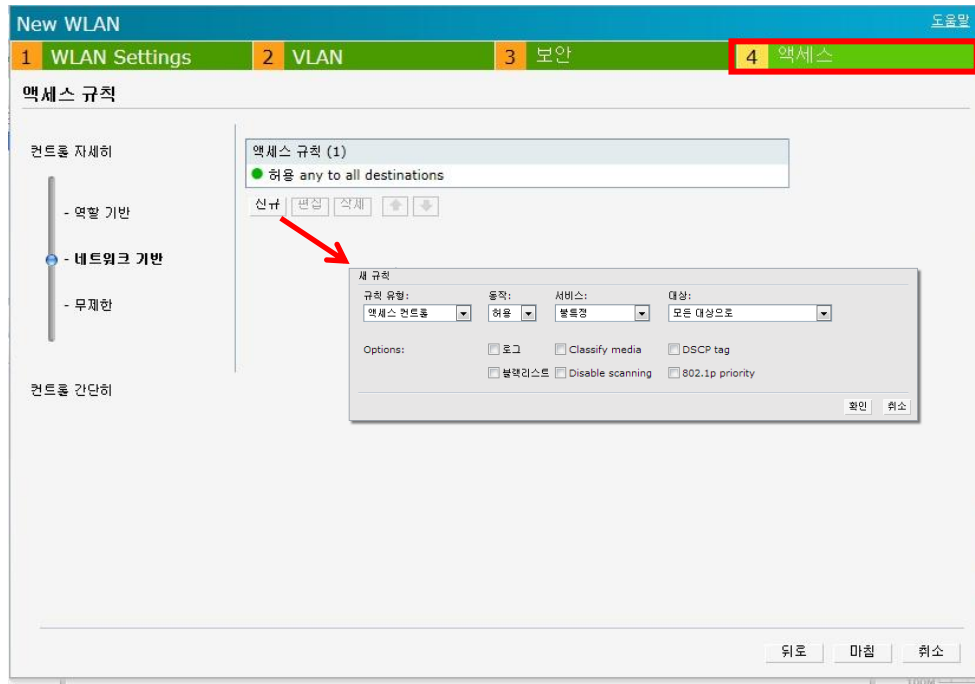
Password:

Login

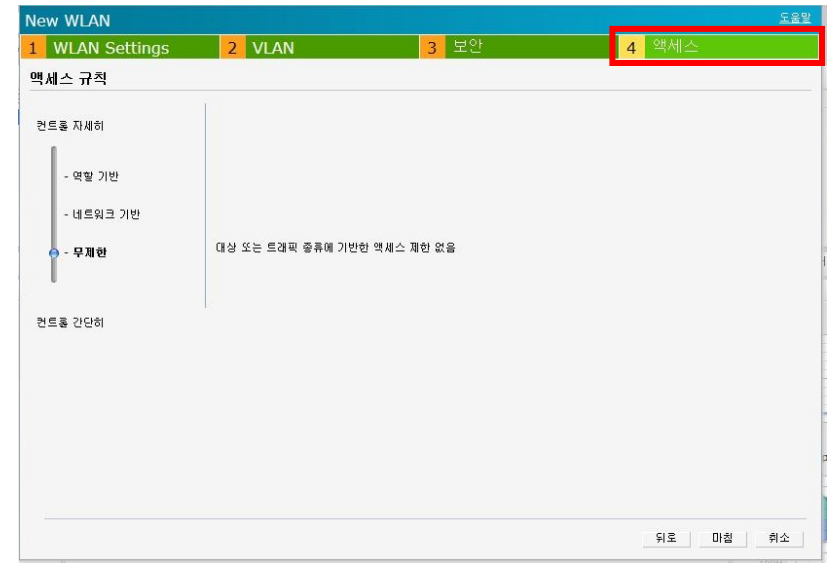
☐ I agree ☐ I do not agree

[무선 접속자 첫 페이지 화면]

2.5 액세스



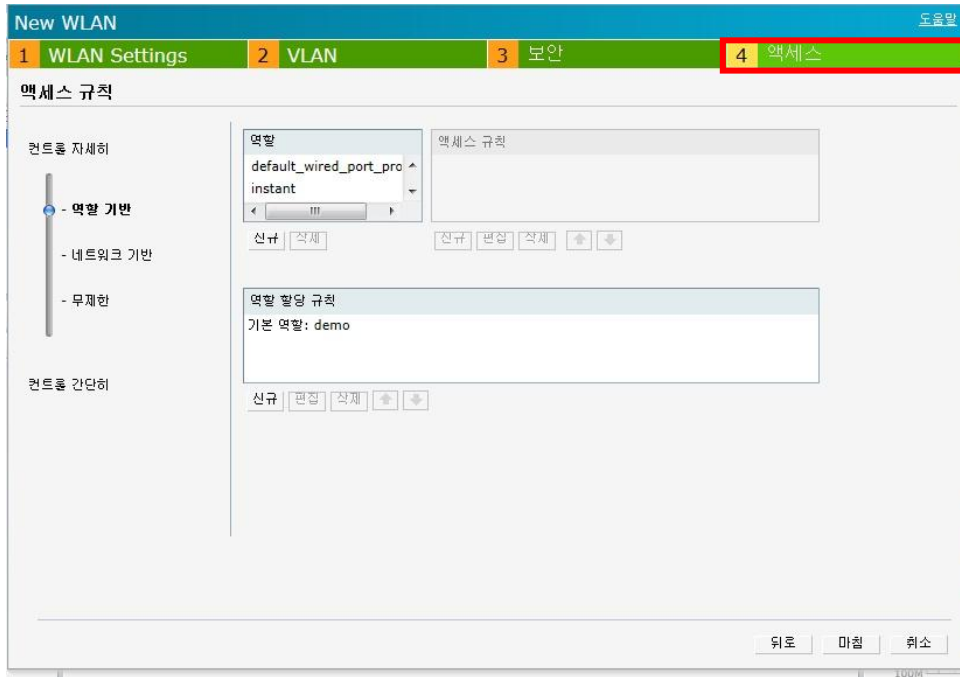
[New WLAN > 액세스(네트워크 기반)]



[New WLAN > 액세스(무제한)]

- ❖ 액세스: 마지막 단계에서 무선 네트워크(SSID)에 대한 접근권한(액세스 규칙)을 설정한다.
 - 무제한: 액세스 규칙의 기본 설정 값이며 무선 네트워크에 접근 시 별도의 액세스 제한 없음
 - 네트워크 기반: 네트워크 기반의 접근권한 설정이 가능하며 기본값은 '모두 허용' 임
 - 신규: 네트워크(SSID) 단위의 접근권한 설정을 위해 액세스 규칙 설정
 - 편집/삭제/↑/↓: 기 설정 액세스 규칙의 편집, 삭제 혹은 순서변경 가능

2.5 액세스(계속)



[New WLAN → 액세스(역할 기반)]

- ❖ 액세스: 마지막 단계에서 무선 네트워크(SSID)에 대한 접근권한(액세스 규칙)을 설정한다.
 - 역할 기반: 역할(Role) 기반의 접근권한 설정이 가능하며 기본값은 '모두 허용' 임
 - 역할: 역할(Role) 별 접근권한(액세스 규칙)을 부여하거나 '추가/편집/삭제/순서조정'이 가능하며 이런 역할(Role)을 신규로 만들거나 삭제 가능
 - 역할 할당 규칙: 외부 RADIUS 인증서버를 통해 사용자 인증 시 return 되는 속성값(VSA, vendor-specific attribute)에 따라 서로 다른 역할(role)을 부여할 수

2.6 네트워크 추가 확인

The screenshot displays the Aruba Instant-CC:90:7C web interface. At the top, there are navigation links: 설정, RF, PEF, WIP, VPN, 유선, 유지보수, 지원, 도움말, and 로그아웃. Below the header, the interface is divided into three main sections: '1개의 네트워크' (1 Network), '1개의 액세스 포인트' (1 Access Point), and '1개의 클라이언트' (1 Client). The '1개의 네트워크' section is highlighted with a red box, showing a table with one entry: 'demo' with a status of '신규' (New). The '1개의 액세스 포인트' section shows a table with one entry: 'd8:c7:c8:cc:90:7c' with a status of '1'. The '1개의 클라이언트' section shows a table with one entry: '172.16.1.247' with a status of 'demo'. Below these sections, there is a '정보' (Info) section on the left, an 'RF 대시보드' (RF Dashboard) in the middle, and a '사용 수미' (Usage Summary) section on the right. The '정보' section displays details about the Instant-CC:90:7C, including its name, country code, IP address, radio band, master IP, OpenDNS status, MAS integration, uplink type, and uplink status. The 'RF 대시보드' section shows a table with columns for '클라이언트' (Client), '신호' (Signal), '속도' (Speed), '사용률' (Usage), '노이즈' (Noise), and '오류' (Error). The '사용 수미' section contains two line graphs: '클라이언트' (Client) and '처리량 (bps)' (Throughput (bps)).

[네트워크 추가 확인]

- ❖ 세 단계를 거쳐 새 네트워크 추가가 완료되면 초기 화면의 네트워크 항목에서 추가된 네트워크 이름을 확인할 수 있다. Provisioning용 네트워크(instant)에 대한 접속을 끊고 신규 네트워크로 재 접속을 하면 기존 SSID 'instant'는 자동으로 삭제된다.



3. IAP 인터페이스



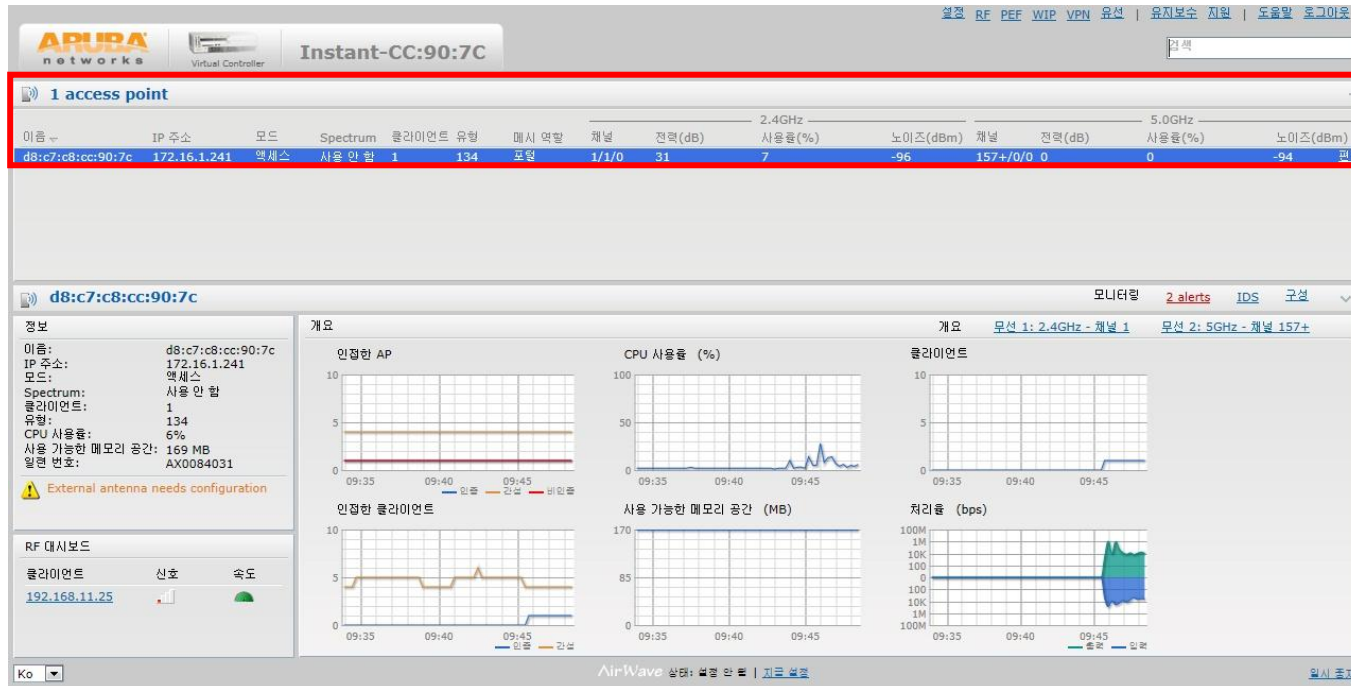
3.1 네트워크



❖ 네트워크 탭을 클릭하면 해당 네트워크에 대한 세부 정보를 확인할 수 있다.

- 이름 : 무선 네트워크 이름(SSID)
- 클라이언트 : 접속 단말 수
- 유형 : 네트워크 타입(직원, 음성, 게스트)
- 대역 : 사용 주파수 대역(2.4GHz, 5GHz or 모두)
- 인증방법 : 네트워크 접속에 적용된 인증방법
- 키 관리 : 인증 key 타입
- IP 할당 : 단말에 대한 IP 주소 할당 방법
- 편집, x : 네트워크 설정내용 수정 혹은 삭제

3.2 액세스 포인트



❖ 액세스 포인트 탭을 클릭하면 각 IAP별 세부 정보를 확인할 수 있다.

- 이름 : IAP의 이름, 기본 값은 IAP의 MAC address
- IP 주소, 모드, 클라이언트, 유형, 메시 역할 : IAP의 IP 주소, mode, 접속중인 단말 수, 기종 및 메시구성 시 역할
- 채널, 전력(dB), 사용률(%), 잡음(dBm) : IAP의 현재 서비스 채널, radio 별 전송 EIRP 값 및 사용률, 주변 잡음(noise floor) 등의 정보 확인
- 편집 : IAP 설정 편집(IAP-92의 경우 안테나 Gain 설정 필수)

3.2.1 액세스 포인트 설정

액세스 포인트 편집 d8:c7:c8:cc:90:7c 도움말

General Radio 외부 안테나 Uplink

이름: d8:c7:c8:cc:90:7c

액세스 포인트용 IP 주소:

☐ DHCP 서버에서 IP 주소를 가져옵니다

☒ 정적 지정

IP 주소: 172.16.1.241

네트워크 마스크: 255.255.255.0

기본 게이트웨이: 172.16.1.1

DNS 서버: 168.126.63.1

도메인 이름: arubanetworks.com

확인 취소

액세스 포인트 편집 d8:c7:c8:cc:90:7c 도움말

General **Radio** 외부 안테나 Uplink

모드: 액세스

2.4GHz 대역

☐ 적응식 무선 관리 할당됨

☒ 관리자 할당됨

채널: 1

송신 출력: 0 dBm

5GHz 대역

☒ 적응식 무선 관리 할당됨

☐ 관리자 할당됨

채널: 36

송신 출력: dBm

확인 취소

❖ 액세스 포인트 '편집' 메뉴를 통해 세부 설정을 할 수 있다.

- General

- 이름 : IAP 이름 설정, 기본 값은 IAP의 MAC address
- 액세스 초인트용 IP 주소 : IAP의 IP 주소 부여 방법
 - 유선 네트워크에 있는 DHCP 서버에서 IP 주소를 할당 받음
 - 정적지정 : 고정 IP 주소 지정

- Radio

- 모드: 액세스(무선 단말 서비스 용) 또는 모니터(센서용) 지정
- 적응식 무선 관리(Adaptive Radio Management)를 통해 자동으로 조정되도록 설정하거나 관리자가 수동으로 할당하도록 설정 가능

3.2.1 액세스 포인트 설정(계속)

액세스 포인트 편집 d8:c7:c8:cc:90:7c 도움말

General Radio **외부 안테나** Uplink

2.4GHz 안테나 이득: 0 dBi

5GHz 안테나 이득: 0 dBi

확인 취소

액세스 포인트 편집 d8:c7:c8:cc:90:7c 도움말

General Radio 외부 안테나 **Uplink**

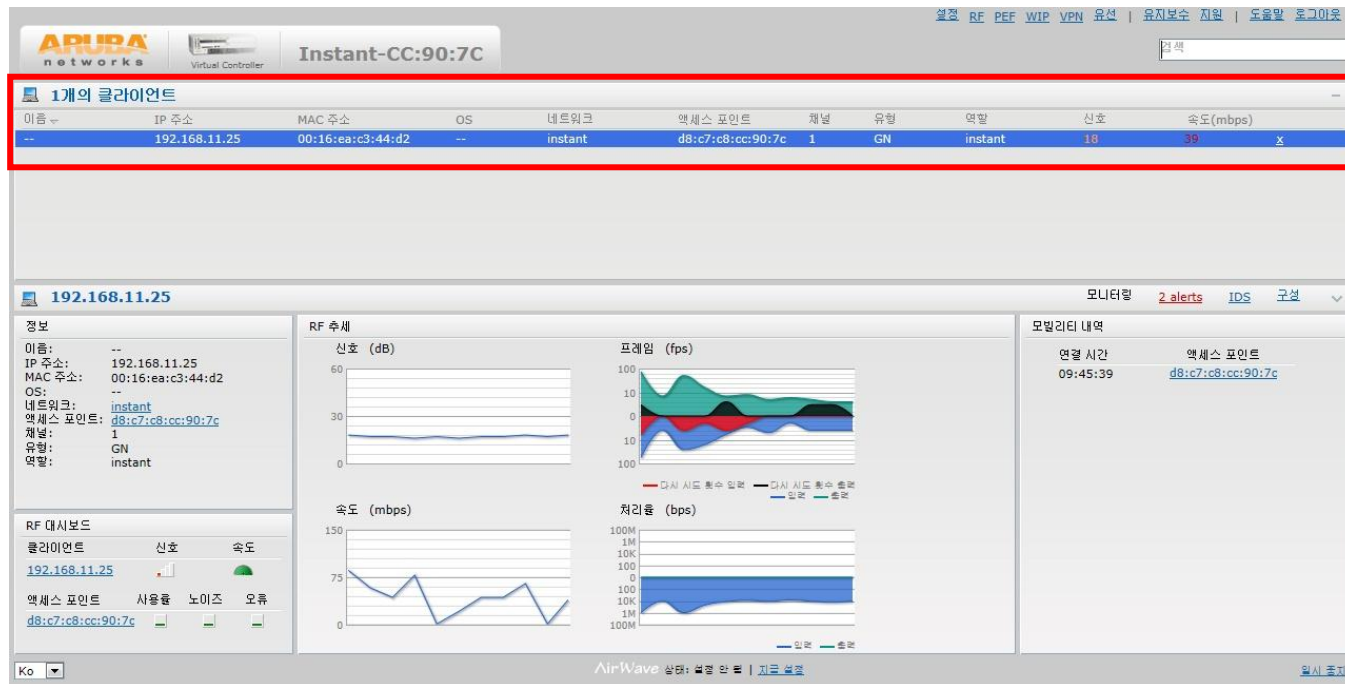
Uplink management VLAN: 0

Eth0 bridging: 사용 안 함 ▼

확인 취소

- 외부안테나 : IAP-92, IAP-124의 경우 외부안테나를 사용해야 하며 이때 반드시 밴드 별 안테나의 이득(Gain) 설정 필수
- Uplink : 관리 트래픽에 Tag를 추가할 수 있다. 매쉬 포인트 용도로 사용시 설정.

3.3 클라이언트



- ❖ 클라이언트 탭을 클릭하면 IAP에 접속된 사용자(무선 단말)의 세부 정보를 확인할 수 있다.
 - 이름 : 클라이언트 이름(802.1x 등 계정으로 접속 시 계정 이름)
 - IP 주소, MAC 주소, OS : 클라이언트의 IP 주소, MAC 주소, 사용중인 OS
 - 네트워크, 액세스포인트, 채널, 유형 : 클라이언트가 접속된 SSID, IAP, 채널 및 Wi-Fi 타입(G, GN, A, AN 등)
 - 역할, 신호, 속도(mbps) : 클라이언트에 부여된 역할(Role), 무선신호 세기 및 현재 연결속도
 - x : 클라이언트 강제 접속 종료 시 사용. 클라이언트가 접속 종료된 상태이면 IAP의 DB에서 삭제되거나 현재 접속중인 상태이면 바로 재접속 됨

3.4 IDS

The screenshot shows the Aruba Instant-CC:90:7C web interface. The 'IDS' tab is selected, displaying two tables of detected external devices.

감지된 외부 액세스 포인트						
MAC 주소	네트워크	분류	채널	유형	마지막 표...	장소
00:08:9f:ac:ea:0c	Epozen	간섭	11	GN 40MZ	10:00:13	
00:1a:1e:8e:4c:93	AppleSi-1x	간섭	36	AN 40MZ	10:00:13	
00:26:66:c4:e0:3c	procn	간섭	11	GN 40MZ	10:00:13	
00:25:a6:93:cb:65	Netween	간섭	6	GN 40MZ	10:00:13	
00:1a:1e:8e:4c:80	AppleSi-1x	비인증	1	GN 40MZ	10:00:13	
00:08:9f:52:d3:60	LOGEO	간섭	9	GN 40MZ	10:00:13	
00:1a:1e:cb:33:22	AppleSi-1x	간섭	36	A	10:00:13	

감지된 외부 클라이언트						
MAC 주소	네트워크	분류	채널	유형	마지막 표...	장소
40:25:c2:08:c3:f8	AppleSi-1x	간섭	1	GN 20MZ	10:00:13	
00:08:9f:f1:c3:bc	AppleSi-1x	간섭	1	GN 20MZ	10:00:13	
00:14:78:ed:a0:d7	AppleSi-1x	간섭	1	G	10:00:13	
68:09:27:2b:0f:3e	AppleSi-1x	간섭	1	GN 20MZ	09:57:13	

- ❖ 초기 화면에서 IDS 메뉴를 클릭하여 무선 IDS 정보를 확인 할 수 있다.
 - 감지된 외부 액세스 포인트 : IAP가 감지한 외래 AP들에 대한 정보를 분류하여(Rogue, Interfering) 보여줌
 - 감지된 외부 클라이언트 : IAP가 감지한 클라이언트에 대한 정보를 분류하여(Rogue, Interfering) 보여줌



4. IAP 세부설정



4.1 설정 - General

설정

General 관리자 RTLS SNMP OpenDNS Uplink 엔터프라이즈 도메인 할드가든 Syslog L3 Mobility

이름: Instant-CC:90:7C 자동 참가 모드: 사용

가상 컨트롤러 IP: 0.0.0.0 터미널 액세스: 사용 안 함

동작 RADIUS 프로시: 사용 안 함 LED 디스플레이: 사용

MAS integration: 사용 TFTP 덤프 서버: 0.0.0.0

NTP 서버: Extended SSID: 사용 안 함

시간대: International-Date-Line-1 Deny inter user bridging: 사용 안 함

기본 설정 대역: 모든 Deny local routing: 사용 안 함

DHCP 서버

도메인 이름:

DNS 서버:

임대 시간: 14400 분

네트워크:

Mask:

고급 옵션 숨기기

확인 취소

- 자동 참가 모드 : Virtual Controller에 해당 AP를 자동으로 그룹핑
- 터미널 액세스 : Telnet을 통한 CLI 접속 허용 여부 설정
- LED 디스플레이 : LED 사용 여부
- TFTP 덤프서버 : 덤프파일을 저장하기 위한 서버 설정
- Extended SSID : SSID 최대 생성 개수를 확장
- Deny inter user bridging : 무선 내부간 local 통신 제한
- Deny local routing : 무선 내부간 L3 통신 제한

❖ 설정 메뉴를 통해 IAP에 필요한 여러가지 값들을 설정할 수 있다.

- General : IAP의 기본 값 설정

→ 이름, 가상 컨트롤러 IP: Virtual Controller의 이름 및 IP 설정, IP 설정 시 Virtual Controller AP의 IP를 지정하는 것이 아닌 별도의 IP를 부여하여 관리 IP로 설정(외부 인증서버 연동 시 필수 조건)

→ 날짜 및 시간 : NTP 서버 및 Timezone 설정

→ DHCP 서버 : DHCP 서버 동작 시(클라이언트 IP할당을 컨트롤러 할당 시) 할당 네트워크 대역, Domain name, DNS Server 및 Lease time 설정(Gateway는 AP자신)

4.1 설정 – 관리자, RTLS

설정

General 관리자 RTLS SNMP OpenDNS Uplink 엔터프라이즈 도메인 월드가든 Syslog L3 Mobility

로컬

인증: 내부

사용자명: admin

암호:

암호 확인:

AirWave

조직:

AirWave IP:

AirWave backup IP:

공유 키:

암호 확인:

[고급 옵션 숨기기](#) 확인 취소

설정

General 관리자 RTLS SNMP OpenDNS Uplink 엔터프라이즈 도메인 월드가든 Syslog L3 Mobility

Aruba RTLS: ☒

Aeroscout: ☐

[고급 옵션 숨기기](#) 확인 취소

- 관리자 : IAP 관리를 위한 계정 설정
 - 로컬: WebUI를 통한 Virtual Controller 접속 시 필요한 관리자 계정, 인증 주체는 내부/Radius 서버/내부를 대체로 사용한 Radius 서버 지정 가능
 - AirWave: AirWave를 통해 관리를 하고자 할 때 필요한 정보 설정
- RTLS : RTLS 관련 설정
 - Aruba RTLS: Aruba RTLS 솔루션 연동 시 설정(IP address, Port, Passphrase 등)
 - Aeroscout: Aeroscout 솔루션 연동 시 설정(IP address, Port)

4.1 설정 - SNMP

The screenshot shows the '설정' (Settings) page for SNMP. The 'SNMP' tab is selected and highlighted with a red box. The interface includes several sections: 'SNMPV1 및 SNMPV2용 커뮤니티 문자열' (Community strings for SNMPv1 and v2) with a '신규' (New) button; 'SNMPV3용 사용자' (Users for SNMPv3) with columns for '이름' (Name), '인증 프로토콜' (Auth protocol), and '개인 정보 프로토콜' (Priv protocol), and buttons for '신규' (New), '편집' (Edit), and '삭제' (Delete); 'SNMP 트랩' (SNMP Traps) with an 'SNMP 엔진 ID' field; and 'SNMP 트랩 수신기' (SNMP Trap Receivers) with columns for 'IP 주소' (IP address), '버전' (Version), '커뮤니티/사용자 이름' (Community/user name), '포트' (Port), and '알림' (Notification), with '신규' (New) and '삭제' (Delete) buttons. At the bottom, there are links for '고급 옵션 숨기기' (Hide advanced options) and buttons for '확인' (OK) and '취소' (Cancel).

- SNMP : NMS 연동 시 필요한 SNMP 설정
 - SNMPv1 & SNMPv2용 커뮤니티 문자열: SNMPv1 & SNMPv2용 Community String 추가/삭제
 - SNMPv3용 사용자: SNMPv3 user 추가/수정/삭제

4.1 설정 – 엔터프라이즈 도메인, 월드가든

The screenshot shows the '설정' (Settings) window with the '엔터프라이즈 도메인' (Enterprise Domain) tab selected. The main area contains a text input field labeled '엔터프라이즈 도메인 이름' (Enterprise Domain Name). Below the field are buttons for '신규' (New) and '삭제' (Delete). At the bottom, there are links for '고급 옵션 숨기기' (Hide Advanced Options) and buttons for '확인' (OK) and '취소' (Cancel).

The screenshot shows the '설정' (Settings) window with the '월드가든' (Walled Garden) tab selected. The main area contains two sections: '블랙리스트' (Blacklist) and '화이트리스트' (Whitelist), each with a text input field. Below each field are buttons for '신규' (New), '편집' (Edit), and '삭제' (Delete). At the bottom, there are links for '고급 옵션 숨기기' (Hide Advanced Options) and buttons for '확인' (OK) and '취소' (Cancel).

- 엔터프라이즈 도메인 이름: 엔터프라이즈 네트워크 환경에서 valid한 모든 DNS 등록
- 월드가든(Walled Garden) : 무선유저의 일부 웹사이트의 웹컨텐츠와 서비스 접근을 제어하기 위한 설정

4.1 설정 – Syslog, L3 Mobility

The screenshot shows the '설정' (Settings) window with the 'Syslog' tab selected. The 'Syslog' section includes a 'Syslog 서버' (Syslog server) field set to '0.0.0.0' and a 'Syslog 수준' (Syslog level) dropdown set to '경고' (Warning). Below this, the 'Syslog 시설 수준' (Syslog facility level) section contains several dropdown menus for different log categories, all set to '경고' (Warning): Ap-Debug, 네트워크 (Network), 보안 (Security), 시스템 (System), 사용자 (User), User-Debug, and 무선 (Wireless). At the bottom, there are buttons for '고급 옵션 숨기기' (Hide advanced options), '확인' (OK), and '취소' (Cancel).

The screenshot shows the '설정' (Settings) window with the 'L3 Mobility' tab selected. The 'Home agent load balancing' dropdown is set to '사용 안 함' (Not used). Below this is a 'Virtual Controller IP Addresses' section with a text area and buttons for '신규' (New), '편집' (Edit), and '삭제' (Delete). Further down is a 'Subnets' section with a table header: 'IP address', 'Subnet mask', 'VLAN ID', and 'Virtual controller IP'. Below the table are buttons for '신규' (New), '편집' (Edit), and '삭제' (Delete). At the bottom, there are buttons for '고급 옵션 숨기기' (Hide advanced options), '확인' (OK), and '취소' (Cancel).

- Syslog : logging 설정
 - Syslog 서버: Syslog server의 IP address
 - Syslog 수준: Syslog로 보낼 메시지의 level(Debug, Information, Notice, Warning, Error, Critical, Alert, Emergency)
 - Syslog 시설 수준 : logging 상세 분류
- L3 Mobility : L3 Roaming(Controller간 Mobility 정보 교환을 통한 3계층기반의 로밍) 구성
 - Virtual Controller IP Address : 각 Mobility의 Virtual Controller
 - Subnet : L3 로밍 기능을 적용할 해당 Mobility 정보 (Network, Mask, VLAN ID, VC IP)

4.2 RF - ARM

RF

도움말

ARM Radio

클라이언트 제어

밴드 조정 모드: 5Ghz 기본 설정

Airtime 공정 모드: 공정 액세스

액세스 포인트 제어

올바른 채널 사용자 지정: ☐

최소 송신 출력: 18

최대 송신 출력: 최대

클라이언트 인식: 사용

스캐닝: 사용

광대역 채널: 5GHz

고급 옵션 숨기기

확인 취소

- ARM : 무선신호 관련 Client & Access Point 제어 설정

- 클라이언트 제어: 대역조정 모드(사용안 함/5GHz 기본설정/5GHz 강제 적용/균형대역) 설정 가능, band steering 기능 구현
- 방송시간 공정 모드: 기본 액세스 - 이 액세스 모드로 설정시 SSID에서 설정하는 대역폭제한 설정적용 X
- 공정 액세스 - 기본 설정 값으로 무선 클라이언트의 무선 사용을 균등 분할
- 선점 액세스 - 고속 사용자가 많을 때 적용

→ 액세스포인트 제어: 올바른 채널 사용자 지정은 위의 그림과 같이 기본으로 채널이 설정되어 있음. 편집으로 가용 채널 수정 가능하고, AP의 자동 출력 조절 및 스캐닝, 광대역 채널 설정으로 AP의 자동 ARM 설정을 할 수 있다.

4.2 RF - Radio

❖ 설정 메뉴를 통해 IAP에 필요한 여러가지 값들을 설정할 수 있다.

- 무선 : 무선 주파수 대역의 세부 설정 (2.4GHz, 5GHz)

→ 레거시만: 802.11a/b/g(non-802.11n)로 사용시 사용설정, 기본값은 사용안 함

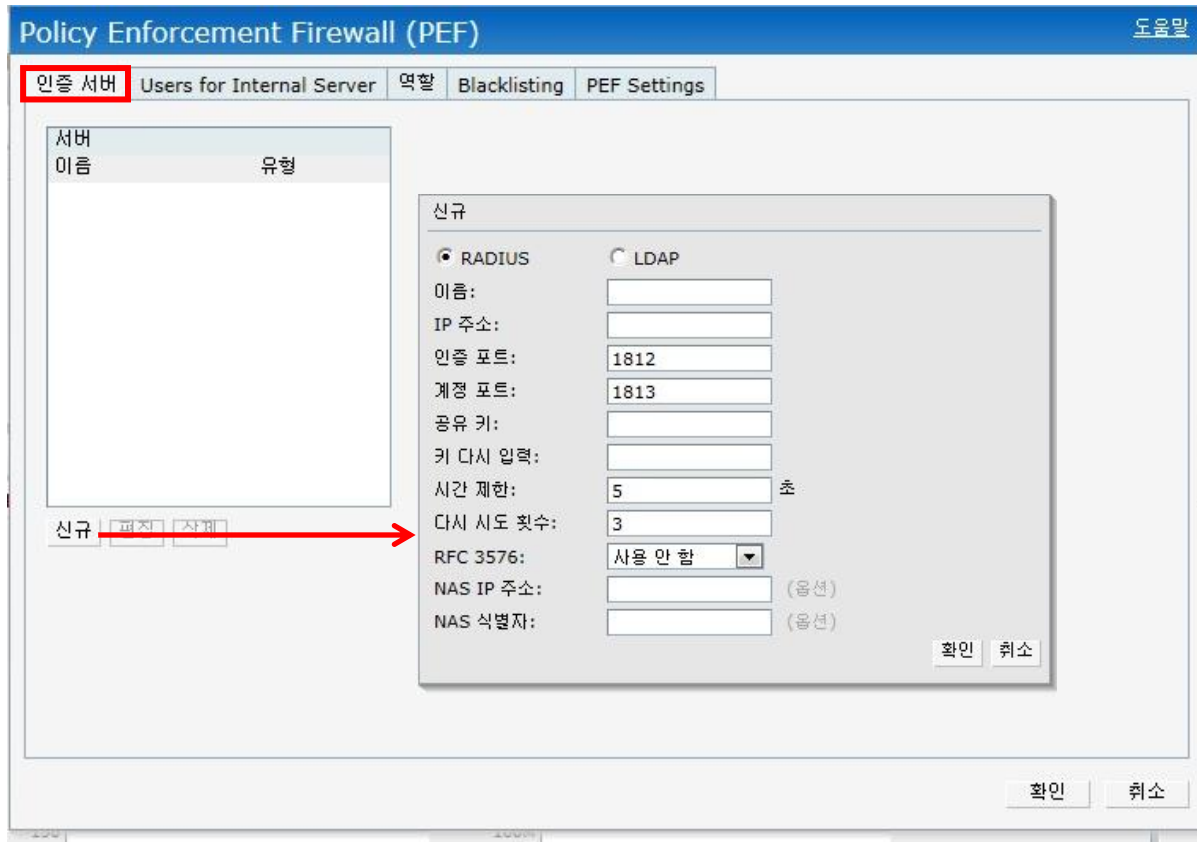
→ 802.11d/802.11h: 국가 별 채널 규약(802.11d)및 전송전력관리(802.11h)의 사용여부 설정, 기본값은 사용안 함

→ 신호간격 : 무선 신호의 간격 조절

→ 간섭면역수준: 1~5로 분류, 기본값은 2로 설정 됨, 숫자가 높을수록 간섭에 대한 면역력을 높여 어느 정도의 간섭에는 간섭이 없는 환경과 같은 수준의 서비스를 제공할 수 있게 함

→ Background spectrum monitoring : 스펙트럼 모드(RF 간섭 모니터링)로 사용하고자 할 시 적용

4.3 PEF – 인증 서버



❖ 서버 메뉴를 통해 외부 인증서버를 설정할 수 있다.

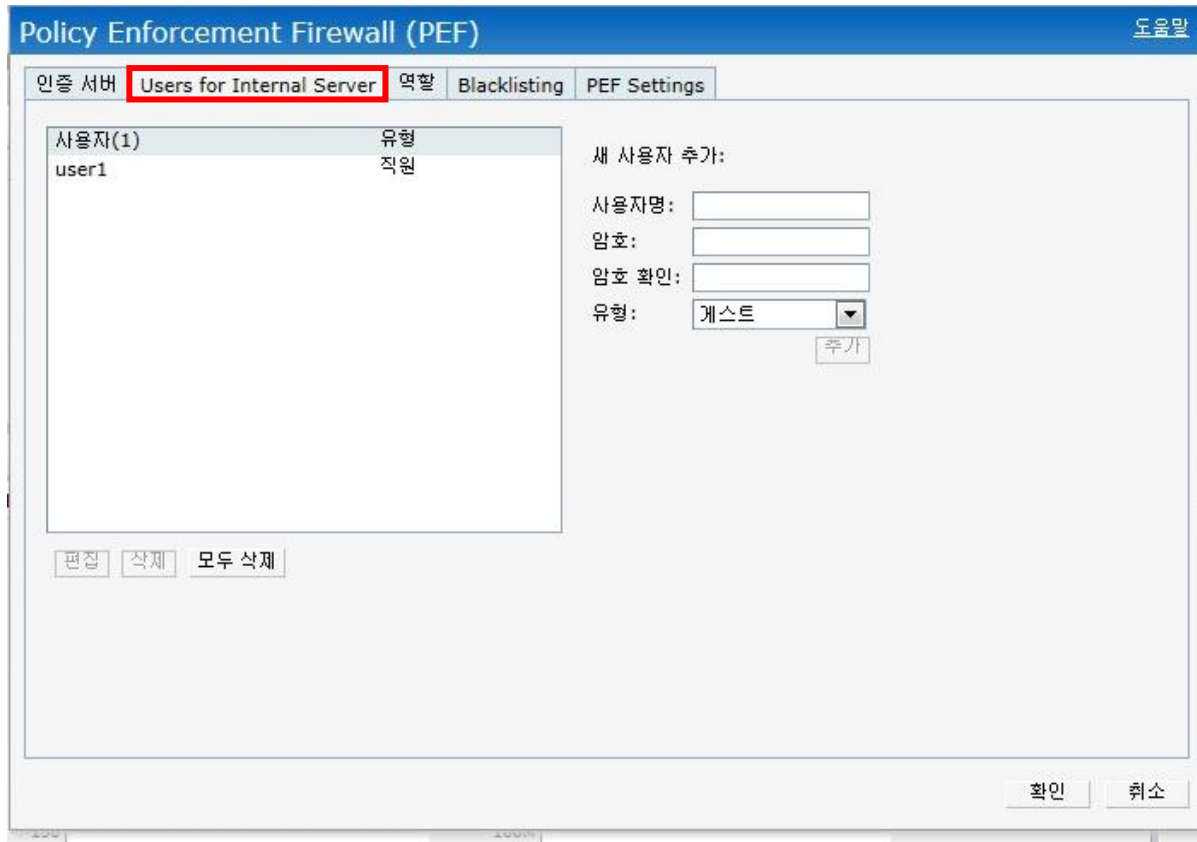
- 신규 : 외부 인증서버 추가

 - 이름, IP 주소 및 인증 시 사용할 Port 번호(기본 1812,1813)

 - 공유 키 : 외부 인증서버 연동 시 필요한 key (인증서버와 Virtual controller가 동일한 Key 설정해야 함)

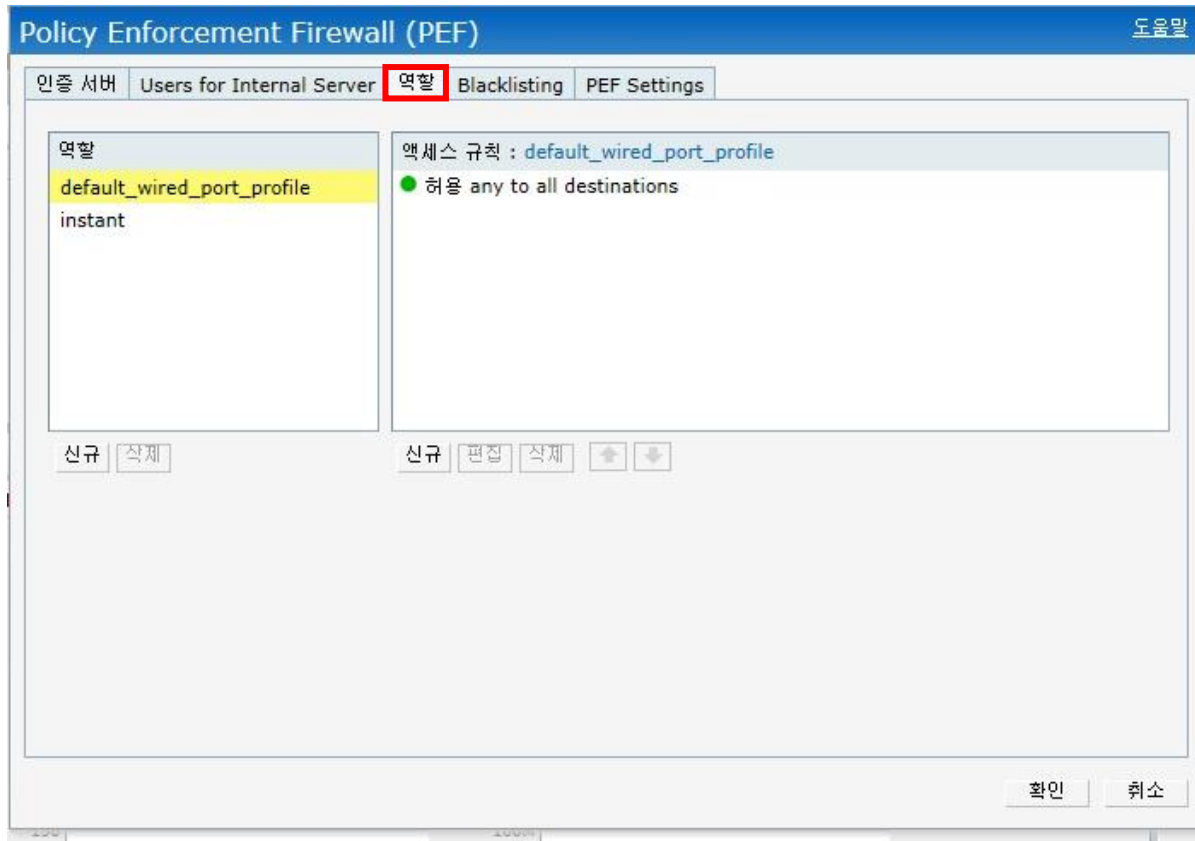
- 편집/삭제 : 등록된 인증서버 수정/삭제

4.3 PEF – User for Internal Server



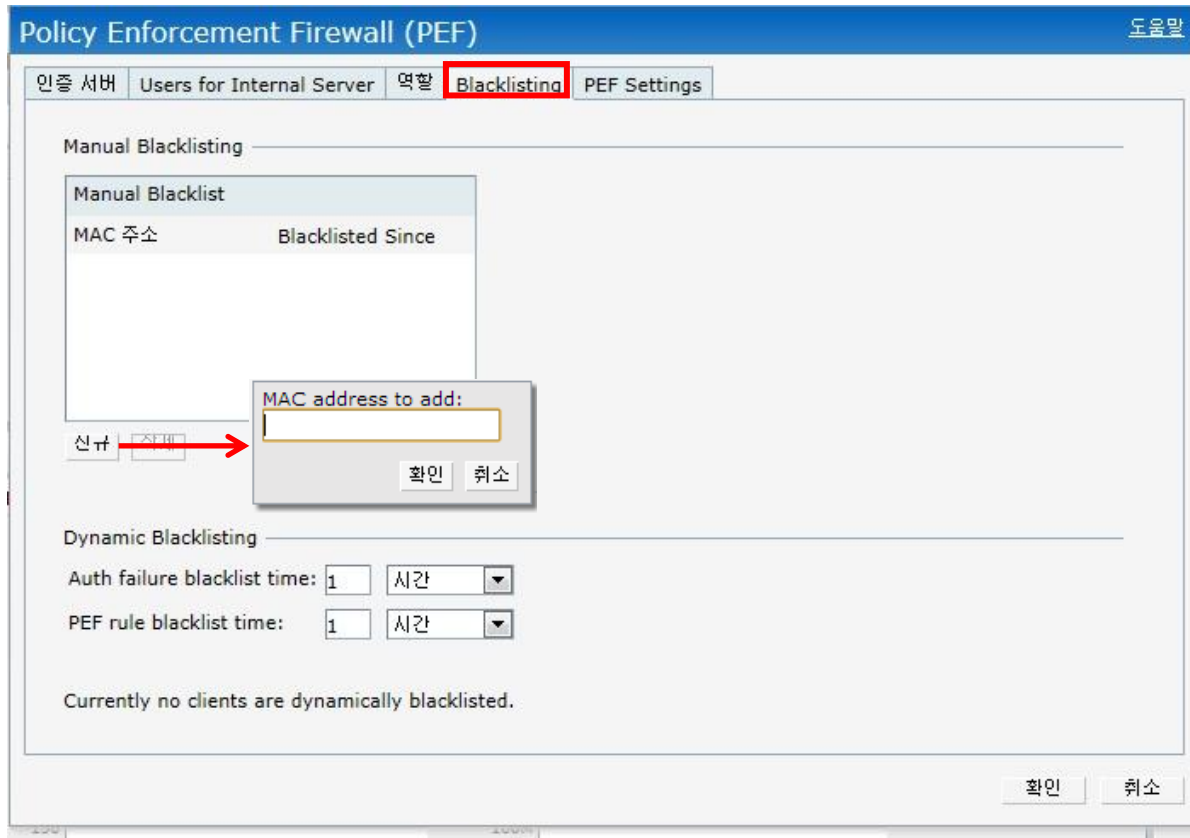
- ❖ 사용자 메뉴를 통해 내부 인증서버 사용 시 필요한 사용자 계정 관리가 가능하다.
 - 사용자 명 : 사용자 계정 이름 (Mac 인증 시에는 콜론을 뺀 소문자 형태로 등록)
 - 암호 : 사용자 계정 비밀번호 (Mac 인증 시에는 사용자명과 동일하게 입력)
 - 유형 : '게스트/임직원' 지정가능하며 Guest는 Captive portal 사용자 인증 시 지정

4.3 PEF – 역할



- ❖ 역할 메뉴를 통해 접근 권한 설정 시 필요한 역할을 추가/수정/삭제할 수 있다.
 - 역할 : Role의 세부 내역 확인, Role 신규/삭제 가능
 - 액세스 규칙 : Role에 대한 Rule의 신규/편집/삭제/우선순위 지정 가능

4.3 PEF – Blacklisting



- ❖ Blacklisting 메뉴를 통해 MAC Address에 의한 접속 제한 정책을 적용할 수 있다.
 - Manual Blacklisting : 사용자에게 의한 수동 설정
 - Dynamic Blacklisting : 인증 실패 임계값에 의해 자동적으로 리스팅 설정

4.4 WIP - 탐지

무선 침입 방지(WIP)

도움말

1 탐지

2 방지

감지할 위협 지정

인프라:

- 높음

- 중간

- 낮음

- **꺼짐**

[사용자 지정 설정](#)

detect-ap-spoofing

detect-windows-bridge

signature-deauth-broadcast

signature-deassociation-broadcast

detect-adhoc-using-valid-ssid

detect-malformed-large-duration

클라이언트:

- 높음

- 중간

- 낮음

- **꺼짐**

[사용자 지정 설정](#)

detect-valid-clientmisassociation

detect-disconnect-sta

detect-omerta-attack

detect-fatajack

detect-block-ack-attack

detect-hotspotter-attack

다음

취소

- ❖ WIP 메뉴를 통해 주변 위협 AP에 대한 탐색, 보호 기능을 적용 할 수 있다.
 - 탐지 : 주변 무선 기기에 대한 Detecting
 - 인프라 : 무선 Device (예, Access Point, 공유기, ad-hoc 등)
 - 클라이언트 : 무선 사용자 (예, PC, NoteBook, SmartPhone 등)

※ 각 항목에 대한 상세사항은 관련 기술문서 참조

39

CONFIDENTIAL © Copyright 2012. Apple Si Company. All rights reserved

Apple si

ARUBA
networks

4.4 WIP - 방지

무선 침입 방지(WIP)

도움말

1 탐지

2 방지

방지할 위협 지정

인프라:

- 높음

- 낮음

꺼짐

[사용자 지정 설정](#)

protect-ssid
rogue-containment
protect-adhoc-network
protect-ap-impersonation

클라이언트:

- 높음

- 낮음

꺼짐

[사용자 지정 설정](#)

protect-valid-sta
protect-windows-bridge

봉쇄 방법

유선 봉쇄:

꺼짐

무선 봉쇄:

없음

기본 봉쇄 설정을 사용하는 것이 좋습니다.

[기본값 복원](#)

[고급 옵션 숨기기](#)

뒤로

마침

취소

- 방지 : 주변 무선 기기에 대한 Protecting
 - 인프라 : 무선 Device (예, Access Point, 공유기, ad-hoc 등)
 - 클라이언트 : 무선 사용자 (예, PC, NoteBook, SmartPhone 등)
- 봉쇄방법
 - 유선봉쇄 : 유선 네트워크 망에 ARP 패킷을 생성
 - 무선봉쇄 : 인증해제만 - 비인가 AP로의 접속을 방해, 타피팅 - 비인가 AP의 통신속도를 고의적으로 지연

※ 각 항목에 대한 상세사항은 관련 기술문서 참조

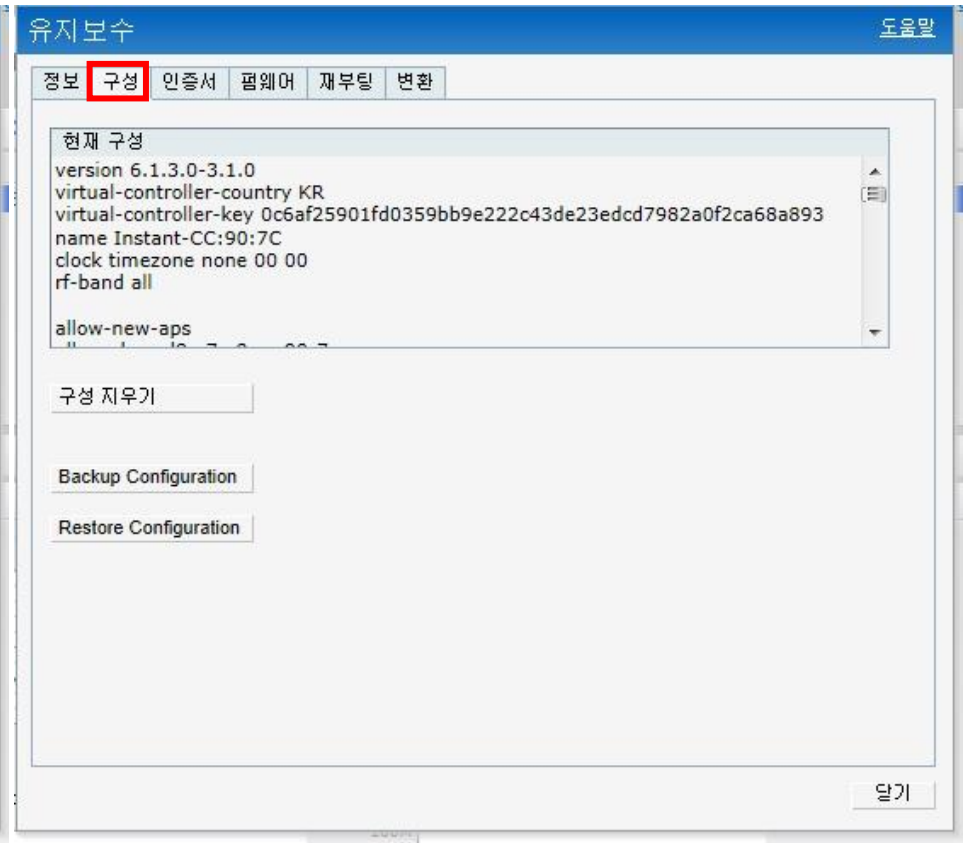
40

CONFIDENTIAL © Copyright 2012. Apple Si Company. All rights reserved

Apple si

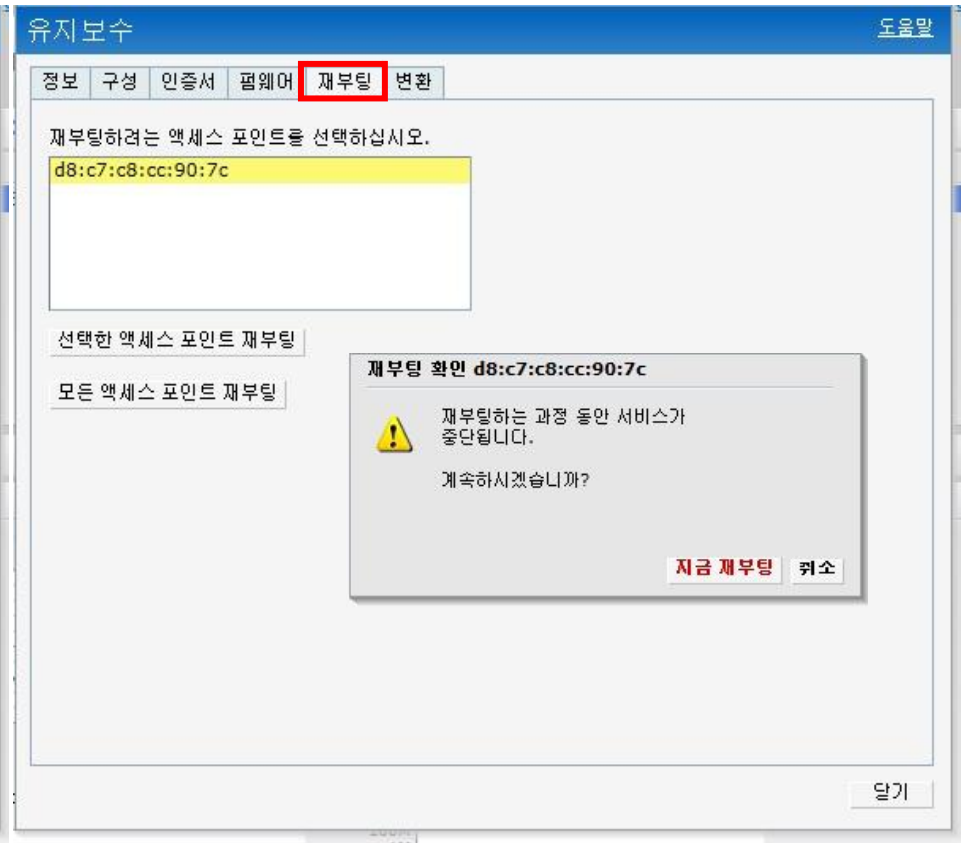
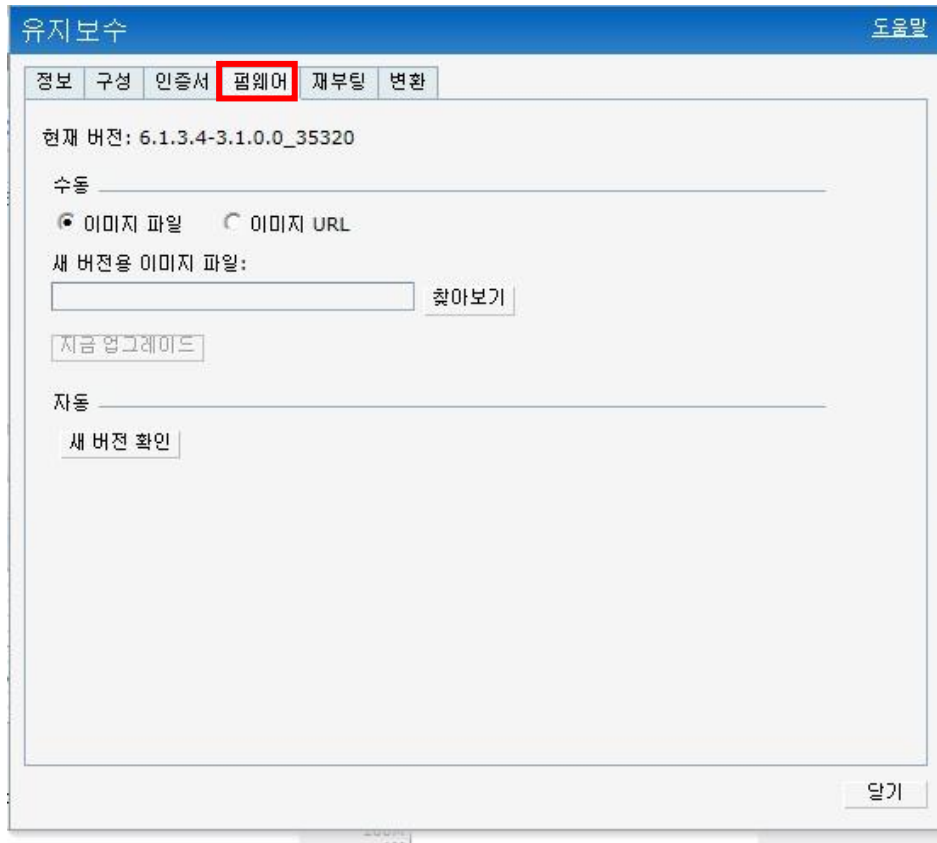
ARUBA
networks

4.5 유지보수 – 정보, 구성



- ❖ 유지관리 메뉴를 통해 IAP 관리를 위해 필요한 사항을 확인 및 설정할 수 있다.
 - 정보 : IAP의 타입, 버전 등 기본정보 확인
 - 구성 : IAP의 설정 값을 확인하거나 삭제, 백업, 재설정 기능

4.5 유지보수 – 펌웨어, 재부팅



- 펌웨어 : IAP의 현재 펌웨어 버전을 확인하고 수동/자동 업그레이드 가능
- 재부팅 : 특정 IAP를 지정하거나 전체 IAP를 다시부팅

4.5 유지보수 – 변환

유지보수

정보 구성 인증서 펌웨어 재부팅 **변환** 도움말

Convert one or more Access Points to:

Remote APs managed by a Mobility Controller

Hostname or IP Address of Mobility Controller:

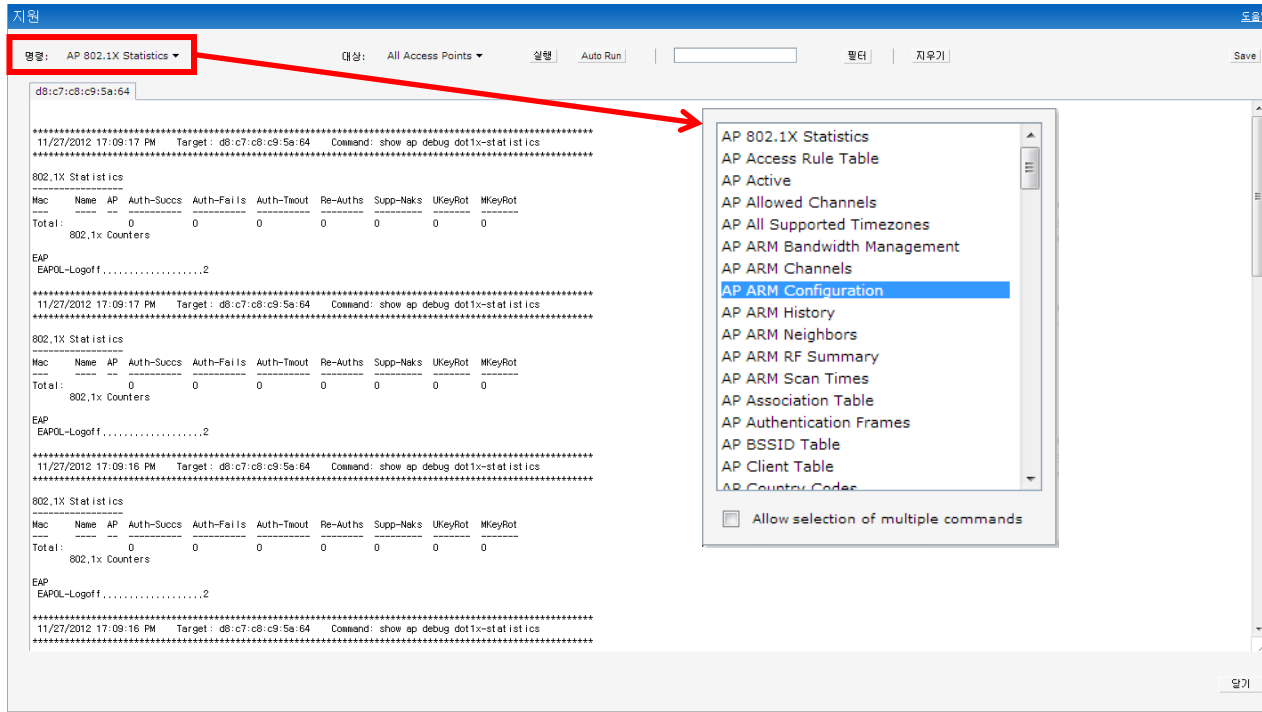
변환 후 모든 액세스 포인트가 위에서 지정한 컨트롤러에 의해 관리됩니다.

지금 변환

닫기

- 변환 : 특정 AP를 StandAlone Mode로 변환 가능
 - Campus Mode : IAP를 Controller 기반의 일반 AP로 전환시킬 때 사용. 단, 한번 AP로 전환되면 다시 IAP로의 전환 불가
 - Remote Mode : IAP를 Controller 기반의 Remote AP로 전환시킬때 사용
 - StandAlone Mode : Virtual Controller에 속하지 않은 단독형의 의미로 Virtual Controller(AP Group)와는 별도의 설정이 가능

4.6 지원



❖ Support 메뉴를 통해 CLI 기반의 명령어들을 특정 IAP 혹은 전체 IAP에 대해 WebUI 기반으로 실행할 수 있고, 그것에 대한 결과값을 저장할 수 있음

- 명령 : 약 80여 개의 명령어 지정
- 대상 : 모든 AP 혹은 개별 AP 지정

감사합니다.

