경량형 AP 및 WLC(Wireless LAN Controller)를 사용한 REAP(Remote-Edge AP) 컨피그레이션 예

목차

소개

Cisco Unified Wireless Network에 도입된 원격 에지 액세스 포인트(REAP) 기능을 사용하면 WLC(무선 LAN) 컨트롤러(WLAN)에서 Cisco LAP(Lightweight Access Point)를 원격으로 구축할 수 있습니다. 따라서 지사와 소규모 소매점에 이상적입니다.이 문서에서는 Cisco 1030 Series LAP 및 4400 WLC를 사용하여 REAP 기반 WLAN 네트워크를 구축하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- WLC에 대한 지식 및 WLC 기본 매개변수를 구성하는 방법
- Cisco 1030 LAP의 REAP 운영 모드 지식
- 외부 DHCP 서버 및/또는 DNS(Domain Name System) 서버 컨피그레이션에 대한 지식
- WPA(Wi-Fi Protected Access) 개념에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 릴리스 4.2를 실행하는 Cisco 4400 Series WLC
- Cisco 1030 LAP
- Cisco IOS® Software 릴리스 12.2(13)T13을 실행하는 Cisco 2800 Series 라우터 2개
- 펌웨어 릴리스 3.0을 실행하는 Cisco Aironet 802.11a/b/g Client Adapter
- Cisco Aironet Desktop Utility 버전 3.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

REAP 모드를 사용하면 LAP가 WAN 링크를 통해 상주할 수 있으며, WLC와 계속 통신하고 일반 LAP의 기능을 제공할 수 있습니다.REAP 모드는 현재 1030 LAP에서만 지원됩니다.

이 기능을 제공하기 위해 1030 REAP는 LWAPP(Lightweight Access Point Protocol) 컨트롤 플레인과 무선 데이터 플레인을 분리합니다.Cisco WLC는 일반 LWAPP 기반 액세스 포인트(AP)를 사용하는 것과 동일한 방식으로 중앙 집중식 제어 및 관리에 사용되고 모든 사용자 데이터는 AP에서 로컬로 브리지됩니다.로컬 네트워크 리소스에 대한 액세스는 WAN 중단 시 유지됩니다.

REAP AP는 두 가지 운영 모드를 지원합니다.

- 일반 REAP 모드
- 독립형 모드

LAP는 REAP AP와 WLC 간의 WAN 링크가 작동 중일 때 일반 REAP 모드로 설정됩니다.LAP는 일반 REAP 모드에서 작동할 때 최대 16개의 WLAN을 지원할 수 있습니다.

WLC와 LAP 간의 WAN 링크가 다운되면 REAP 지원 LAP는 독립형 모드로 전환됩니다.독립형 모드에서 WLAN이 WEP(Wired Equivalent Privacy) 또는 로컬 인증 방법으로 구성된 경우 REAP LAP는 WLC 없이 하나의 WLAN만 독립적으로 지원할 수 있습니다.이 경우 REAP AP가 지원하는 WLAN은 AP, WLAN 1에 구성된 첫 번째 WLAN입니다. 이는 다른 대부분의 인증 방법이 컨트롤러에 정보를 전달해야 하고 WAN 링크가 다운되면 이 작업이 가능하지 않기 때문입니다.독립형 모드에서는 LAP가 최소 기능 집합을 지원합니다.이 표에서는 REAP LAP가 독립형 모드에 있을 때 REAP LAP가 지원하는 기능(WAN 링크가 작동되고 WLC에 대한 통신이 작동 중인 경우)과 비교하여 지원하는 기능 집합을 보여 줍니다.

REAP LAP가 일반 REAP 모드 및 독립형 모드에서 지원하는 기능

		REAP (normal mode)	REAP (standalone mode)
Protocols	IPv4	Yes	Yes
	IPv6	Yes	Yes
	All other protocols	Yes (only if client is also IP enabled)	Yes (only if client is also IP enabled)
	IP Proxy ARP	No	No
WLAN	Number of SSIDs	16	1 (the first one)
	Dynamic channel assignment	Yes	No
	Dynamic power control	Yes	No
	Dynamic load balancing	Yes	No
VLAN	Multiple interfaces	No	No
	802.1Q Support	No	No
WLAN Security	Rogue AP detection	Yes	No
	Exclusion list	Yes	Yes (existing members only)
	Peer-to-Peer blocking	No	No
	Intrusion Detection System	Yes	No
Layer 2 Security	MAC authentication	Yes	No
	802.1X	Yes	No
	WEP (64/128/152bits)	Yes	Yes
	WPA-PSK	Yes	Yes
	WPA2-PSK	No	No
	WPA-EAP	Yes	No
	WPA2-EAP	Yes	No
Layer 3 Security	Web Authentication	No	No
	IPsec	No	No
	L2TP	No	No
	VPN Pass-through	No	No
	Access Control Lists	No	No
QoS	QoS Profiles	Yes	Yes
	Downlink QoS (weighted round-robin queues)	Yes	Yes
	802.1p support	No	No
	Per-user bandwidth contracts	No	No
	WMM	No	No
	802.11e (future)	No	No
	AAA QoS Profile override	Yes	No
Mobility	Intra-subnet	Yes	Yes
	Inter-subnet	No	No
DHCP	Internal DHCP Server	No	No
	External DHCP Server	Yes	Yes
Topology	Direct connect (2006)	No	No

이 표에서는 두 모드의 REAP LAP에서 여러 VLAN이 지원되지 않음을 보여줍니다.여러 VLAN은 지원되지 않습니다. REAP LAP는 IEEE 802.1Q VLAN 태깅을 수행할 수 없으므로 단일 서브넷에만 상주할 수 있기 때문입니다.따라서 각 SSID(서비스 집합 식별자)의 트래픽은 유선 네트워크와 동일한 서브넷에서 종료됩니다.그 결과 무선 트래픽이 SSID 간 공기 중에 분할될 수 있지만 유선 측에서 데이터 트래픽이 분리되지 않습니다.

REAP 구축 및 REAP의 관리 방법 및 제한 사항에 대한 자세한 내용은 지사의 REAP 구축 가이드를 참조하십시오.

구성

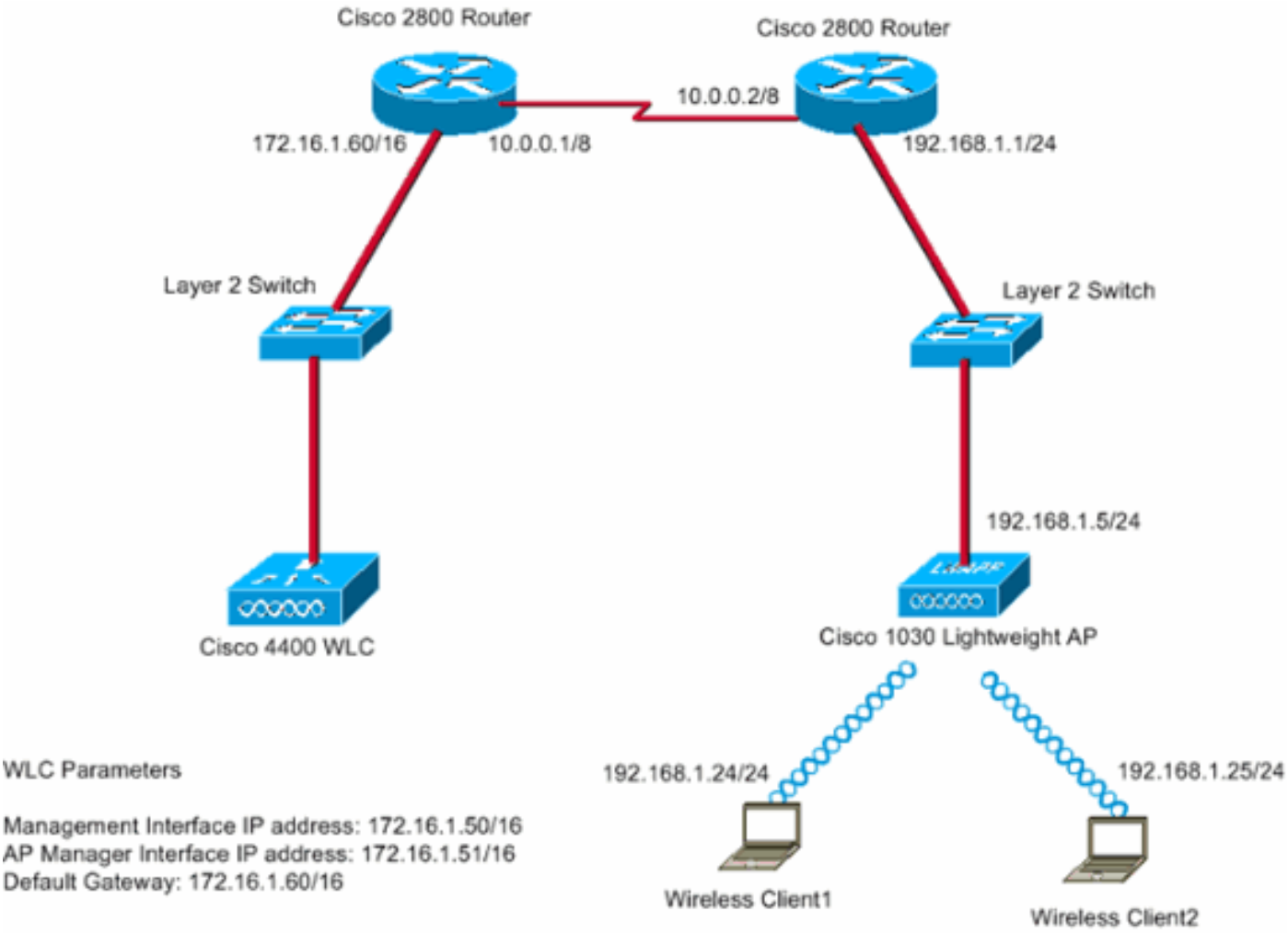
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

네트워크 설정을 구현하도록 디바이스를 구성하려면 다음 단계를 완료합니다.

1. 기본 작동을 위해 WLC를 구성하고 WLAN을 구성합니다.
2. 원격 사이트에서 설치할 AP를 초기화합니다.
3. WAN 링크를 설정하도록 2800 라우터를 구성합니다.
4. 원격 사이트에 REAP LAP를 구축합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



본사는 임대회선을 이용하여 지사에 연결된다.임대 회선은 각 끝에 있는 2800 시리즈 라우터에서 종료됩니다.이 예에서는 OSPF(Open Shortest Path First) 프로토콜을 사용하여 PPP 캡슐화를 사용하여 WAN 링크의 데이터를 라우팅합니다.4400 WLC는 본사에 있으며 1030 LAP는 원격 사무소에 구축되어야 합니다.1030 LAP는 2개의 WLAN을 지원해야 합니다.WLAN에 대한 매개변수는 다음과 같습니다.

- **WLAN 1**SSID - **SSID1**인증 - **열기**암호화 - **TKIP(Temporal Key Integrity Protocol)(WPA-PSK[Pre-Shared Key])**
- **WLAN 2**SSID - **SSID2**인증 - **EAP(Extensible Authentication Protocol)**암호화 - **TKIP참고:** WLAN 2의 경우 이 문서의 컨피그레이션에서는 WPA(802.1x 인증 및 암호화에 TKIP)를 사용합니다.

이 설정에 대한 디바이스를 구성해야 합니다.

기본 작업을 위한 WLC 구성 및 WLAN 구성

기본 작업을 위해 WLC를 구성하려면 CLI(Command Line Interface)에서 시작 컨피그레이션 마법사를 사용할 수 있습니다.또는 GUI를 사용하여 WLC를 구성할 수도 있습니다.이 문서에서는 CLI에서 시작 컨피그레이션 마법사를 사용하여 WLC의 컨피그레이션에 대해 설명합니다.

WLC가 처음 부팅되면 시작 컨피그레이션 마법사로 직접 들어갑니다.구성 마법사를 사용하여 기본 설정을 구성합니다.CLI 또는 GUI에서 마법사를 실행할 수 있습니다.다음은 시작 구성 마법사의 예입니다.

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC_MainOffice
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 172.16.1.50
Management Interface Netmask: 255.255.0.0
Management Interface Default Router: 172.16.1.60
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 172.16.1.1
AP Manager Interface IP Address: 172.16.1.51
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Main
Network Name (SSID): SSID1
Allow Static IP Addresses [YES][no]: Yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: Yes
Enable 802.11a Network [YES][no]: Yes
Enable 802.11g Network [YES][no]: Yes
Enable Auto-RF [YES][no]: Yes

Configuration saved!
Resetting system with new configuration...
```

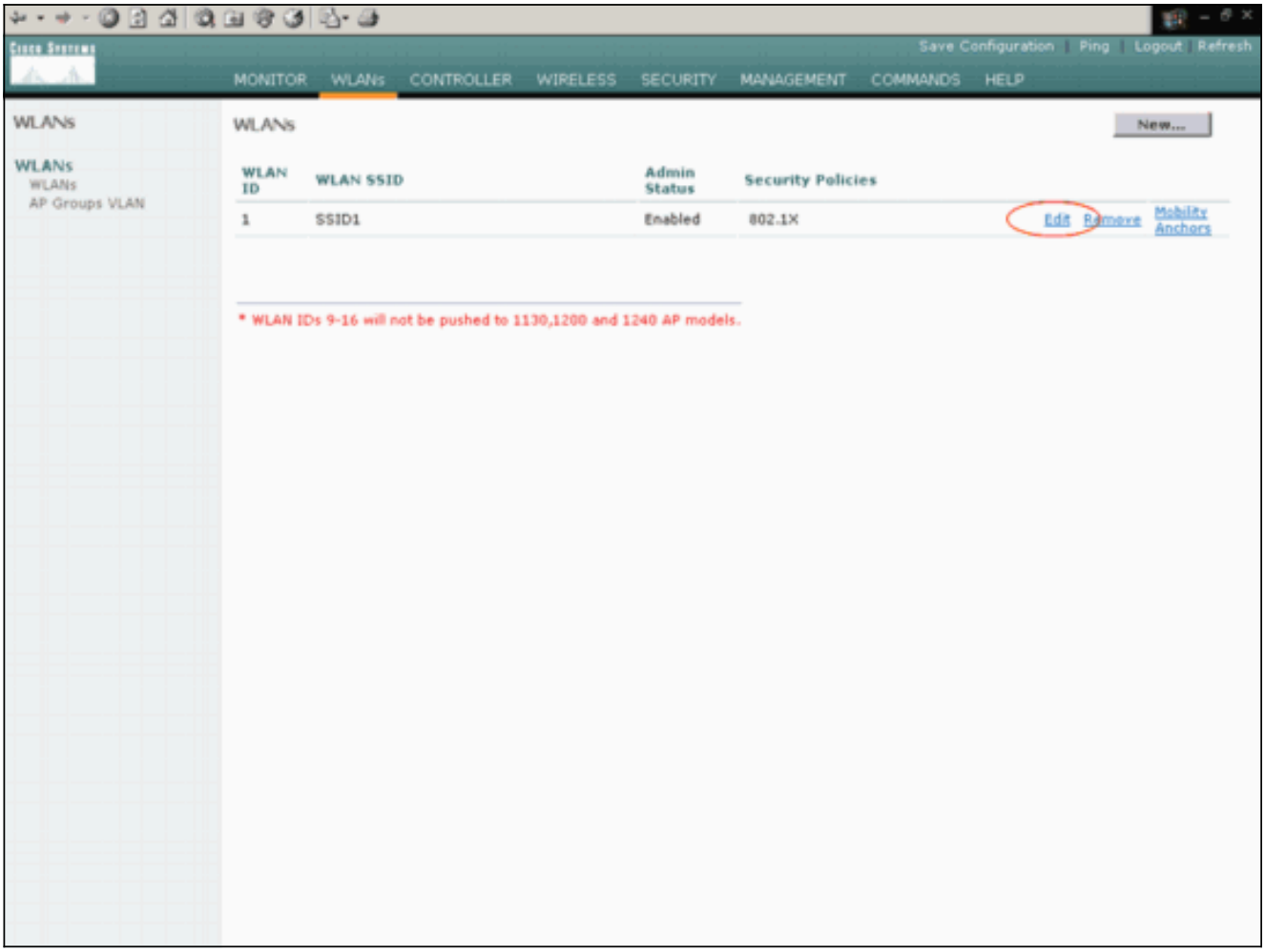
다음 예에서는 WLC에서 다음 매개변수를 구성합니다.

- 시스템 이름
- 관리 인터페이스 IP 주소
- AP-manager 인터페이스 IP 주소
- 관리 인터페이스 포트 번호
- 관리 인터페이스 VLAN 식별자
- 모빌리티 그룹 이름
- SSID
- 기타 여러 매개변수

이러한 매개변수는 기본 작업을 위해 WLC를 설정하는 데 사용됩니다.이 섹션의 WLC 출력에 표시된 것처럼 WLC는 관리 인터페이스 IP 주소로 172.16.1.50을, AP-manager 인터페이스 IP 주소로 172.16.1.51을 사용합니다.네트워크에 대해 2개의 WLAN을 구성하려면 WLC에서 다음 단계를 완료하십시오.

1. WLC GUI에서 창 상단의 메뉴에서 WLANs를 클릭합니다.WLANs 창이 나타납니다.이 창에는 WLC에 구성된 WLAN이 나열됩니다.시작 컨피그레이션 마법사를 사용하여 WLAN 하나를 구성했으므로 이 WLAN에 대한 다른 매개변수를 구성해야 합니다.
2. WLAN **SSID**1에 대해 Edit를 클릭합니다.예를 들면 다음과 같습니다

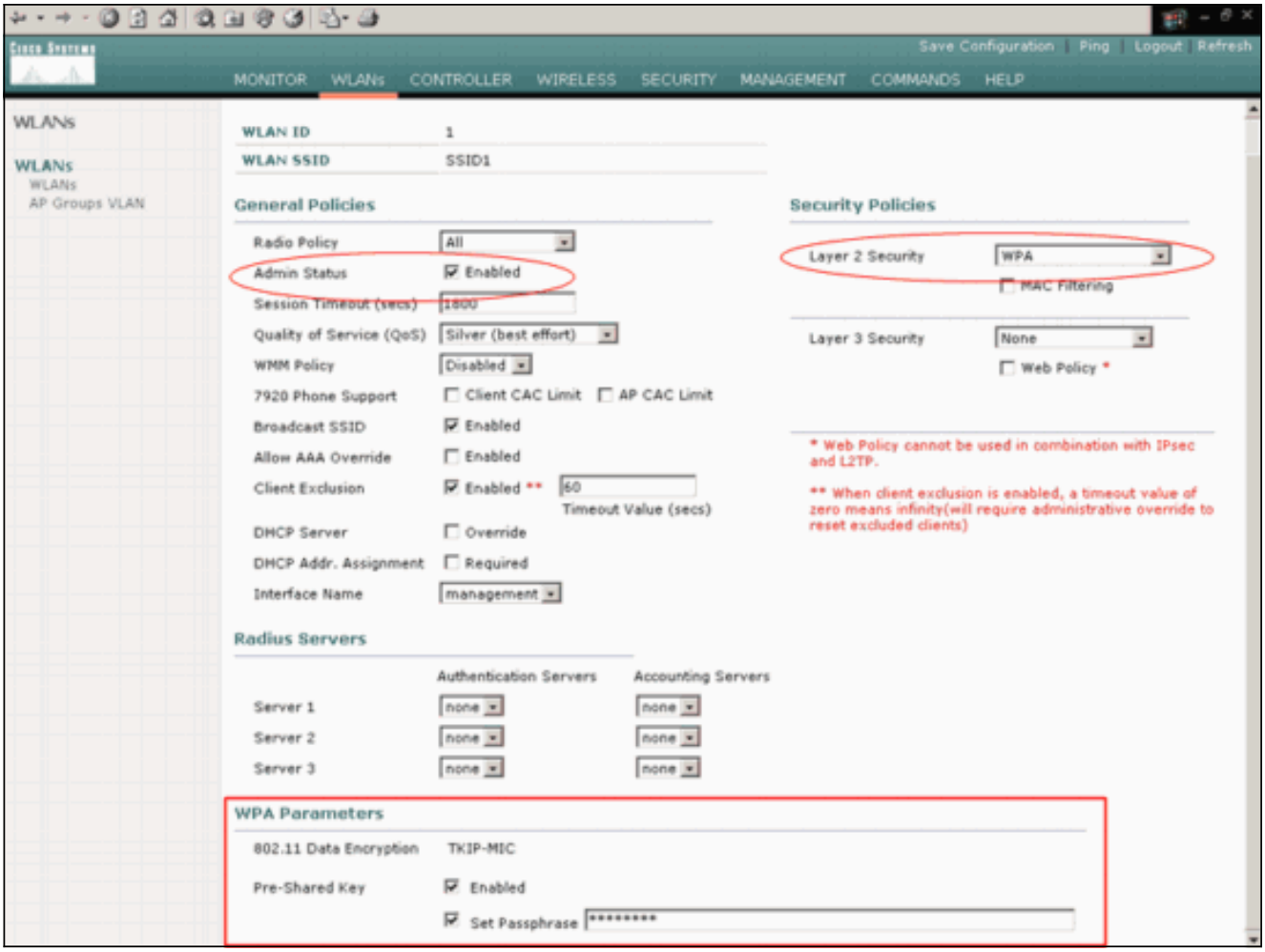
.



WLANs > Edit(수정) 창이 나타납니다.이 창에서 일반 정책, 보안 정책, RADIUS 서버 등을 포함하는 WLAN에 특정한 매개변수를 구성할 수 있습니다.

3. WLANs(WLAN) > Edit(편집) 창에서 다음 항목을 선택합니다.General Policies(일반 정책) 영역에서 Admin Status(관리 상태) 옆의 Enabled(**활성화**) 확인란을 선택하여 이 WLAN을 활성화합니다.WLAN 1에 WPA를 사용하려면 Layer 2 Security(레이어 2 보안) 드롭다운 메뉴에서 WPA를 선택합니다.창 아래쪽에 WPA 매개변수를 정의합니다.WLAN 1에서 WPA-PSK를 사용하려면 WPA Parameters(WPA 매개변수) 영역에서 Pre-Shared Key(사전 공유 키) 옆에 있는 **Enabled(활성화됨)** 확인란을 선택하고 WPA-PSK의 암호를 입력합니다.WPA-PSK는 암호화에 TKIP를 사용합니다.**참고:** WPA-PSK 패스프레이즈는 WPA-PSK가 작동하려면 클라이언트 어댑터에 구성된 패스프레이즈와 일치해야 합니다.Apply를 **클릭합니다**.예를 들면 다음과 같습니다

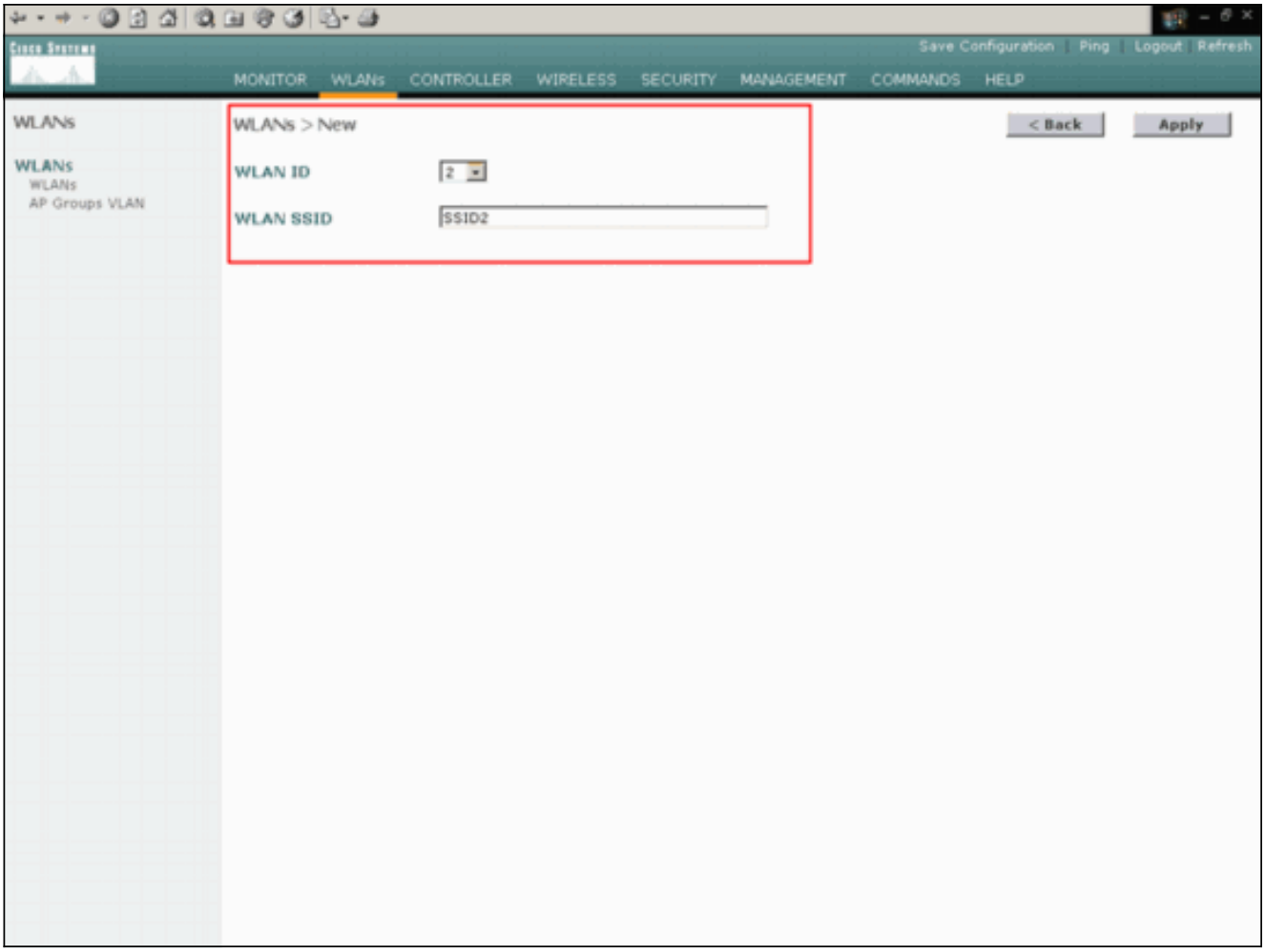
.



WPA-PSK 암호화를 위해 WLAN 1을 구성했습니다.

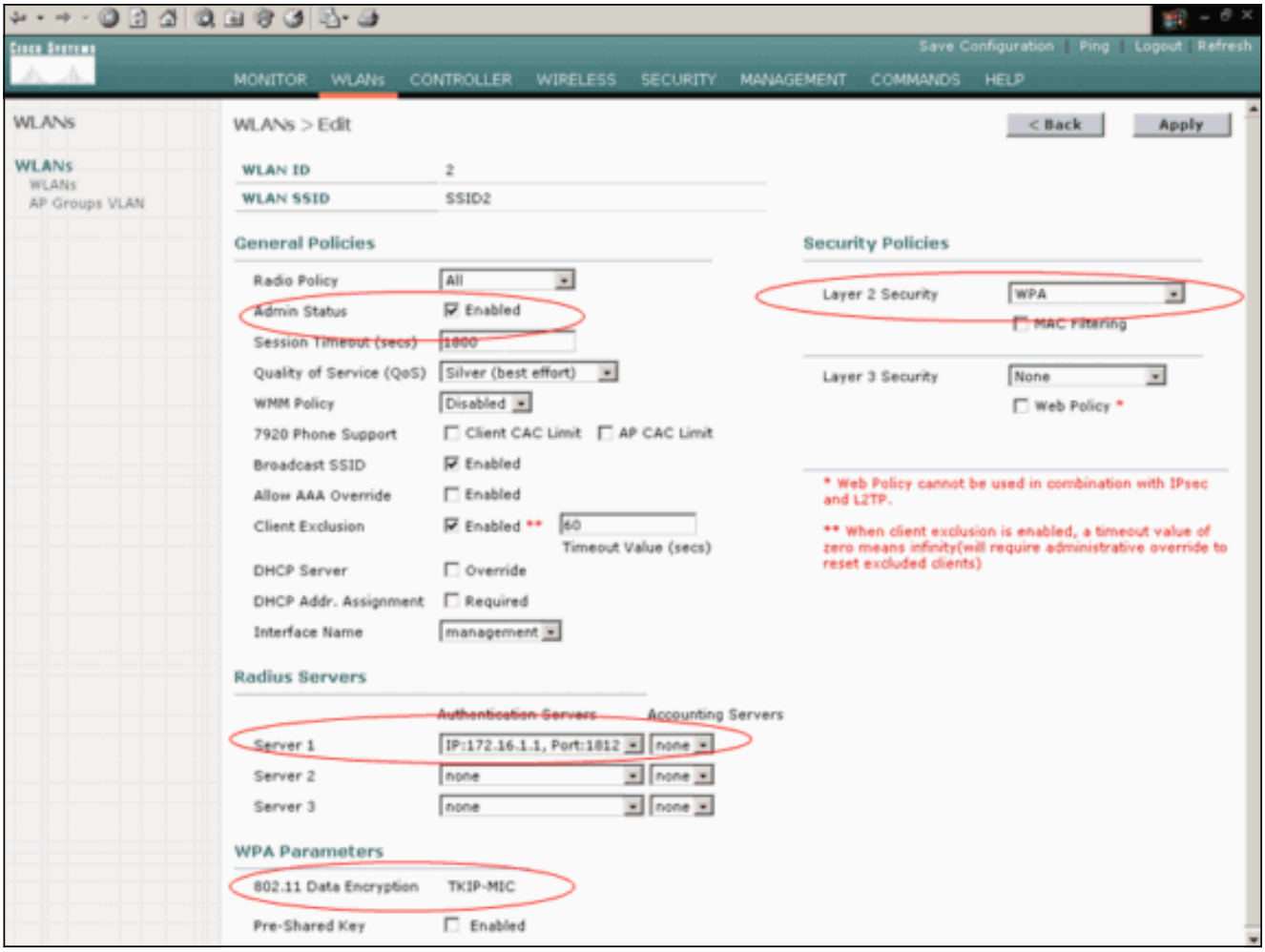
4. WLAN 2를 정의하려면 WLANs 창에서 New를 클릭합니다.WLAN > New 창이 나타납니다.
5. WLAN(WLAN) > New(새로 만들기) 창에서 WLAN ID 및 WLAN SSID를 정의하고 Apply(적용)를 **클릭합니다**.예를 들면 다음과 같습니다

.



두 번째 WLAN에 대한 WLAN > Edit 창이 나타납니다.

6. WLANs(WLAN) > Edit(편집) 창에서 다음 항목을 선택합니다.General Policies(일반 정책) 영역에서 Admin Status(관리 상태) 옆의 Enabled(**활성화**) 확인란을 선택하여 이 WLAN을 활성화합니다.이 **WLAN에** 대한 WPA를 구성하려면 Layer 2 Security 드롭다운 메뉴에서 WPA를 선택합니다.Radius Servers(RADIUS 서버) 영역에서 클라이언트 인증에 사용할 적절한 RADIUS 서버를 선택합니다.Apply를 **클릭합니다**.예를 들면 다음과 같습니다
.



참고: 이 문서에서는 RADIUS 서버 및 EAP 인증을 구성하는 방법에 대해 설명하지 않습니다 .WLC를 사용하여 EAP 인증을 구성하는 방법에 대한 자세한 내용은 WLAN 컨트롤러(WLC)를 사용한 EAP 인증 구성 예를 참조하십시오.

원격 사이트에서 설치할 AP 프라임

Priming은 LAP가 연결할 수 있는 컨트롤러 목록을 가져오는 프로세스입니다.LAP는 단일 컨트롤러에 연결되자마자 모빌리티 그룹의 모든 컨트롤러에 대해 알림을 받습니다.이렇게 하면 LAP는 그룹의 모든 컨트롤러에 연결하기 위해 필요한 모든 정보를 학습합니다.

REAP 지원 AP를 초기화하려면 AP를 본사의 유선 네트워크에 연결합니다.이 연결을 통해 AP는 단일 컨트롤러를 검색할 수 있습니다.LAP가 본사의 컨트롤러에 조인하면 AP는 WLAN 인프라 및 컨피그레이션에 해당하는 AP OS(운영 체제) 버전을 다운로드합니다.모빌리티 그룹에 있는 모든 컨트롤러의 IP 주소가 AP로 전송됩니다.AP에 필요한 모든 정보가 있으면 원격 위치에서 AP를 연결할 수 있습니다.그런 다음 IP 연결을 사용할 수 있는 경우 AP가 목록에서 가장 활용도가 낮은 컨트롤러를 검색하고 조인할 수 있습니다.

참고: AP를 원격 사이트로 배송하려면 AP를 끄기 전에 "REAP" 모드로 설정해야 합니다.컨트롤러 CLI 또는 GUI를 통해 또는 WCS(Wireless Control System) 템플릿을 사용하여 AP 레벨에서 모드를 설정할 수 있습니다.AP는 기본적으로 일반 "로컬" 기능을 수행하도록 설정됩니다.

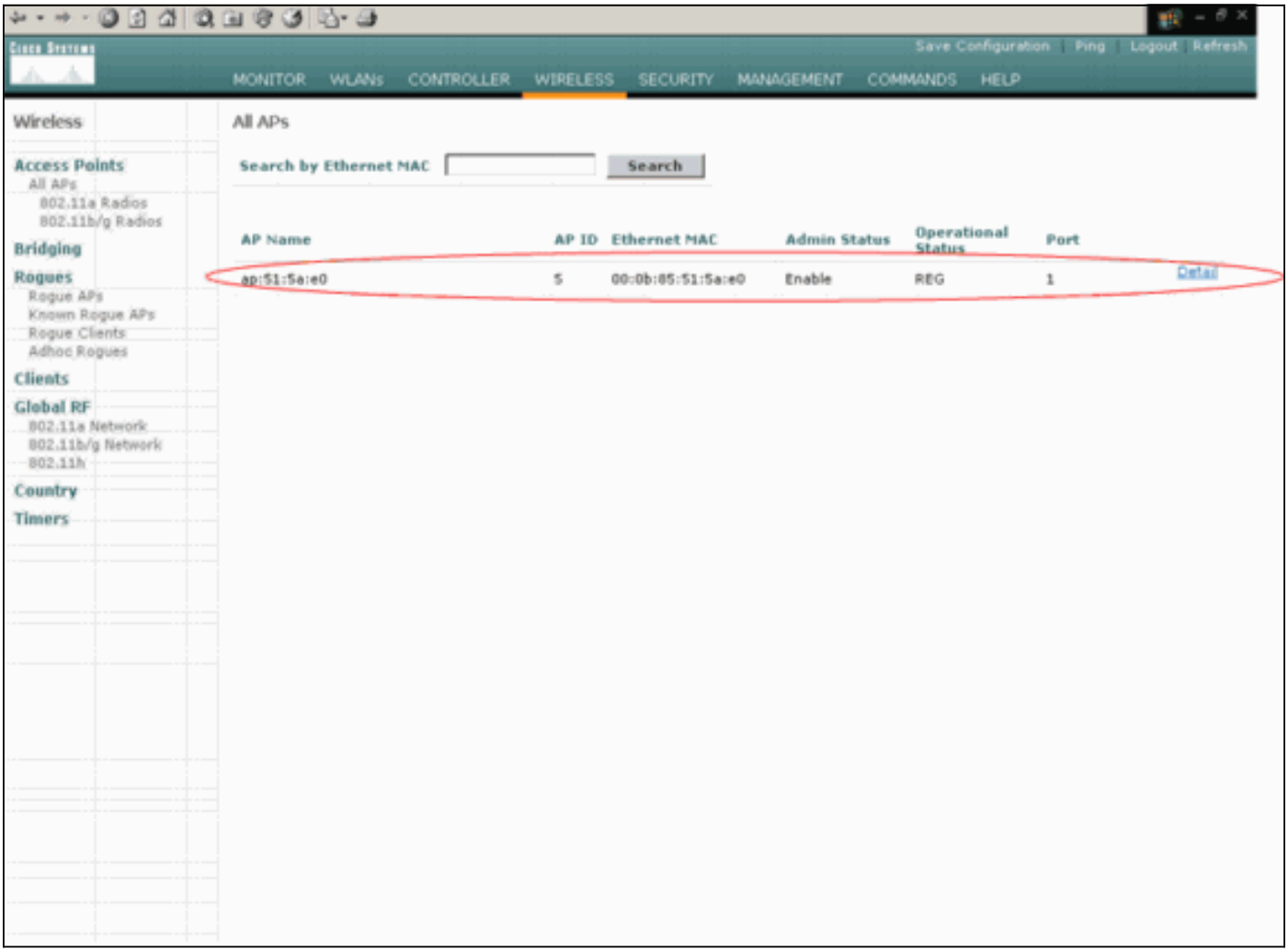
LAP는 다음 방법 중 하나를 사용하여 컨트롤러를 검색할 수 있습니다.

- **레이어 2 검색**
- **레이어 3 검색**로컬 서브넷 브로드캐스트 사용DHCP 옵션 43 사용DNS 서버 사용OTAP(Over-the-Air Provisioning) 사용내부 DHCP 서버를 사용하는 경우**참고:** 내부 DHCP 서버를 사용하려

면 LAP가 WLC에 직접 연결해야 합니다.

이 문서에서는 DHCP 옵션 43 검색 메커니즘을 사용하여 LAP가 WLC에 등록된다고 가정합니다 .DHCP 옵션 43을 사용하여 컨트롤러에 LAP를 등록하는 방법과 다른 검색 메커니즘에 대한 자세한 내용은 WLC(Wireless LAN Controller)에 LAP(Lightweight AP) 등록을 참조하십시오.

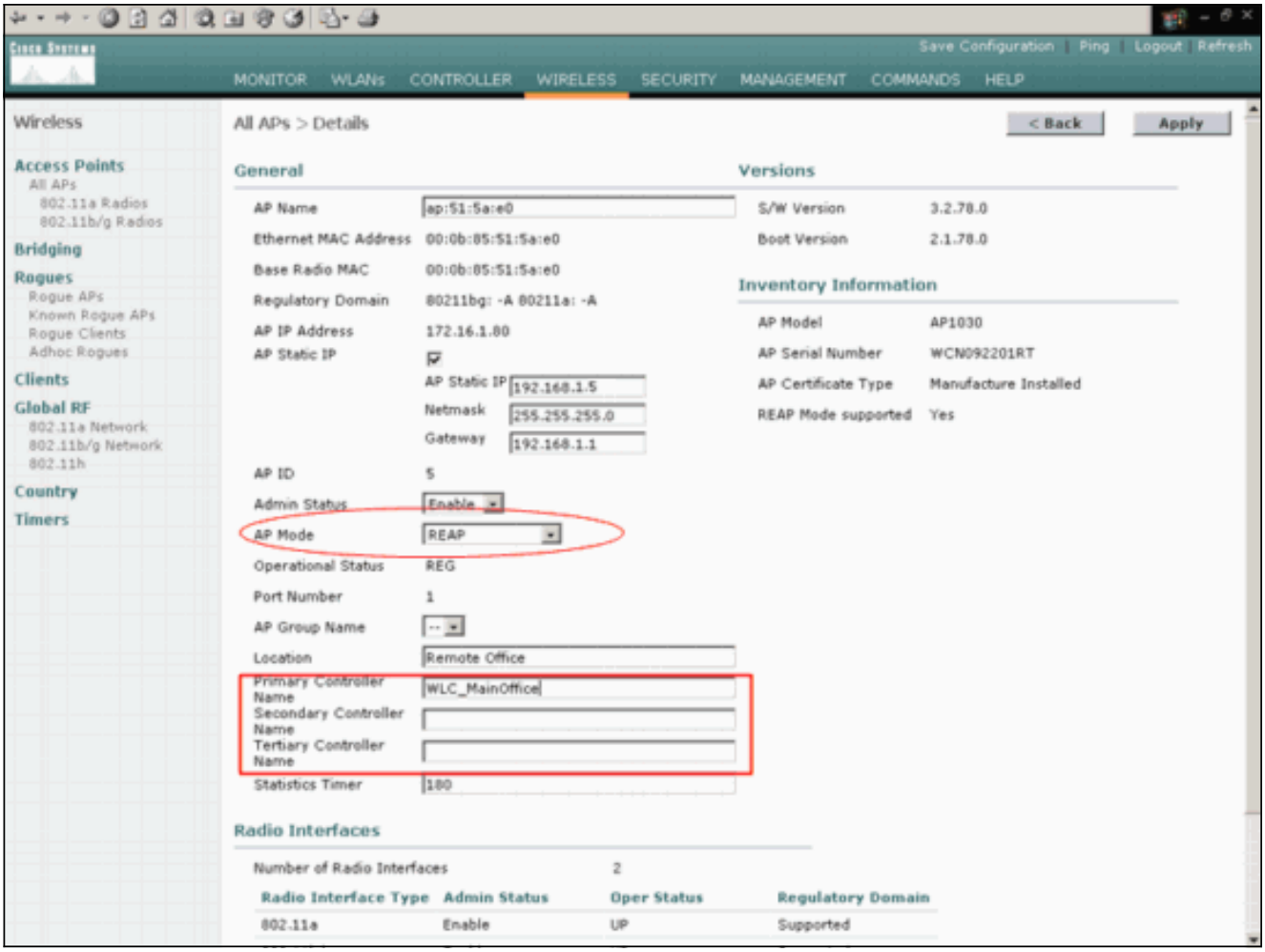
LAP에서 컨트롤러를 검색한 후 WLC의 Wireless(무선) 창에서 컨트롤러에 AP가 등록되었음을 확인할 수 있습니다.예를 들면 다음과 같습니다.



일반 REAP 모드에 대해 LAP를 구성하려면 다음 단계를 완료합니다.

1. WLC GUI에서 **Wireless**를 클릭합니다.All APs 창이 나타납니다.이 창에는 WLC에 등록된 AP가 나열됩니다.
2. REAP 모드에 대해 구성해야 하는 AP를 선택하고 Detail을 **클릭합니다**.특정 AP에 대한 All APs > Detail 창이 나타납니다.이 창에서 AP의 다양한 매개변수를 구성할 수 있습니다. 여기에는 다음이 포함됩니다.AP 이름IP 주소(정적으로 변경할 수 있음)관리 상태보안 매개변수AP 모드AP가 연결할 수 있는 WLC 목록기타 매개변수
3. AP Mode 드롭다운 메뉴에서 REAP을 선택합니다.이 모드는 REAP 지원 AP에서만 사용할 수 있습니다.
4. AP에서 등록하는 데 사용할 컨트롤러 이름을 정의하고 Apply(적용)를 **클릭합니다**.최대 3개의 컨트롤러 이름(기본, 보조 및 3차)을 정의할 수 있습니다. AP는 이 창에서 제공한 것과 동일한 순서로 컨트롤러를 검색합니다.이 예에서는 하나의 컨트롤러만 사용하므로 컨트롤러를 기본 컨트롤러로 정의합니다.예를 들면 다음과 같습니다

.



REAP 모드를 위한 AP를 설정했으며 원격 사이트에서 구축할 수 있습니다.

참고: 이 예제 창에서 AP의 IP 주소가 고정 IP 주소로 변경되고 고정 IP 주소 192.168.1.5이 할당되었음을 확인할 수 있습니다.이 할당은 원격 사무실에서 사용할 서브넷이기 때문에 발생합니다.따라서 DHCP 서버 172.16.1.80의 IP 주소는 초기화 단계 동안에만 사용합니다.AP가 컨트롤러에 등록되면 주소를 고정 IP 주소로 변경합니다.

WAN 링크를 설정하도록 2800 라우터 구성

WAN 링크를 설정하기 위해 이 예에서는 OSPF와 함께 2개의 2800 시리즈 라우터를 사용하여 네트워크 간에 정보를 라우팅합니다.다음은 이 문서의 예제 시나리오에 대한 두 라우터의 컨피그레이션입니다.

본사

```
MainOffice#show run
Building configuration...

Current configuration : 728 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname MainOffice
!
!
ip subnet-zero
```

```
!
!
!
!
interface Ethernet0
 ip address 172.16.1.60 255.255.0.0
!--- This is the interface which acts as the default
gateway to the WLC. ! interface Virtual-Template1 no ip
address ! interface Serial0 no ip address ! interface
Serial1 !--- This is the interface for the WAN link. ip
address 10.0.0.1 255.0.0.0 encapsulation ppp !--- This
example uses PPP. Use the appropriate !--- encapsulation
for the WAN connection. ! router ospf 50 !--- Use OSPF
to route data between the different networks. log-
adjacency-changes network 10.0.0.0 0.255.255.255 area 0
network 172.16.0.0 0.0.255.255 area 0 ! ! ip classless
ip http server ! ! ! line con 0 line aux 0 line vty 0 4
! end
```

지사

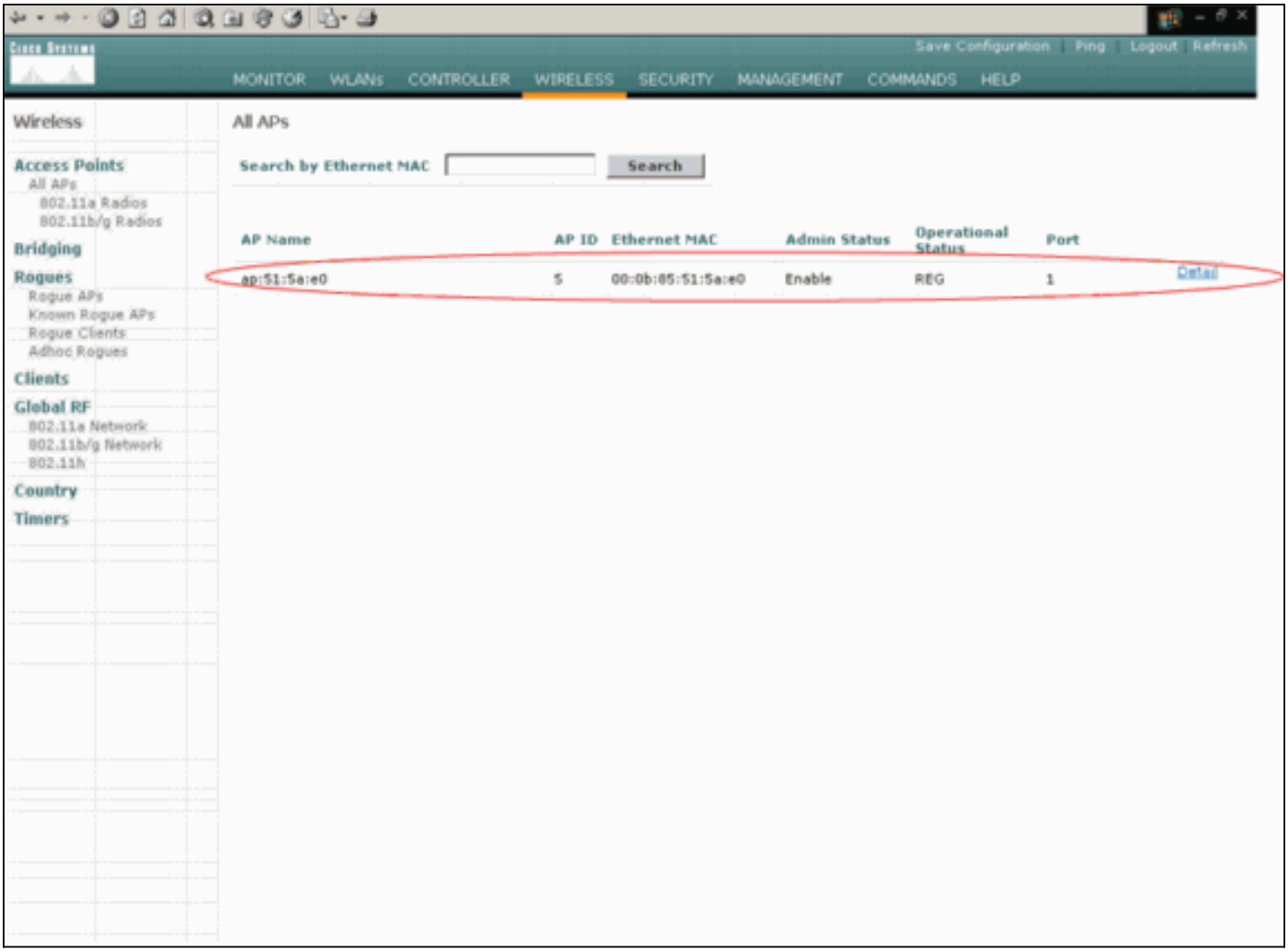
```
BranchOffice#show run
Building configuration...

Current configuration : 596 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BranchOffice
!
!
ip subnet-zero
!
!
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
!--- This is the interface which acts as the default
gateway to the LAP. ! interface Serial0 no ip address !
interface Serial1 !--- This is the interface for the WAN
link. ip address 10.0.0.2 255.0.0.0 encapsulation ppp
clockrate 56000 ! router ospf 50 !--- Use OSPF to route
data between the different networks. log-adjacency-
changes network 10.0.0.0 0.255.255.255 area 0 network
192.168.1.0 0.0.0.255 area 0 ! ip classless ip http
server ! ! ! ! line con 0 line aux 0 line vty 0 4 login
autocommand access enable-timeout 2 ! end
```

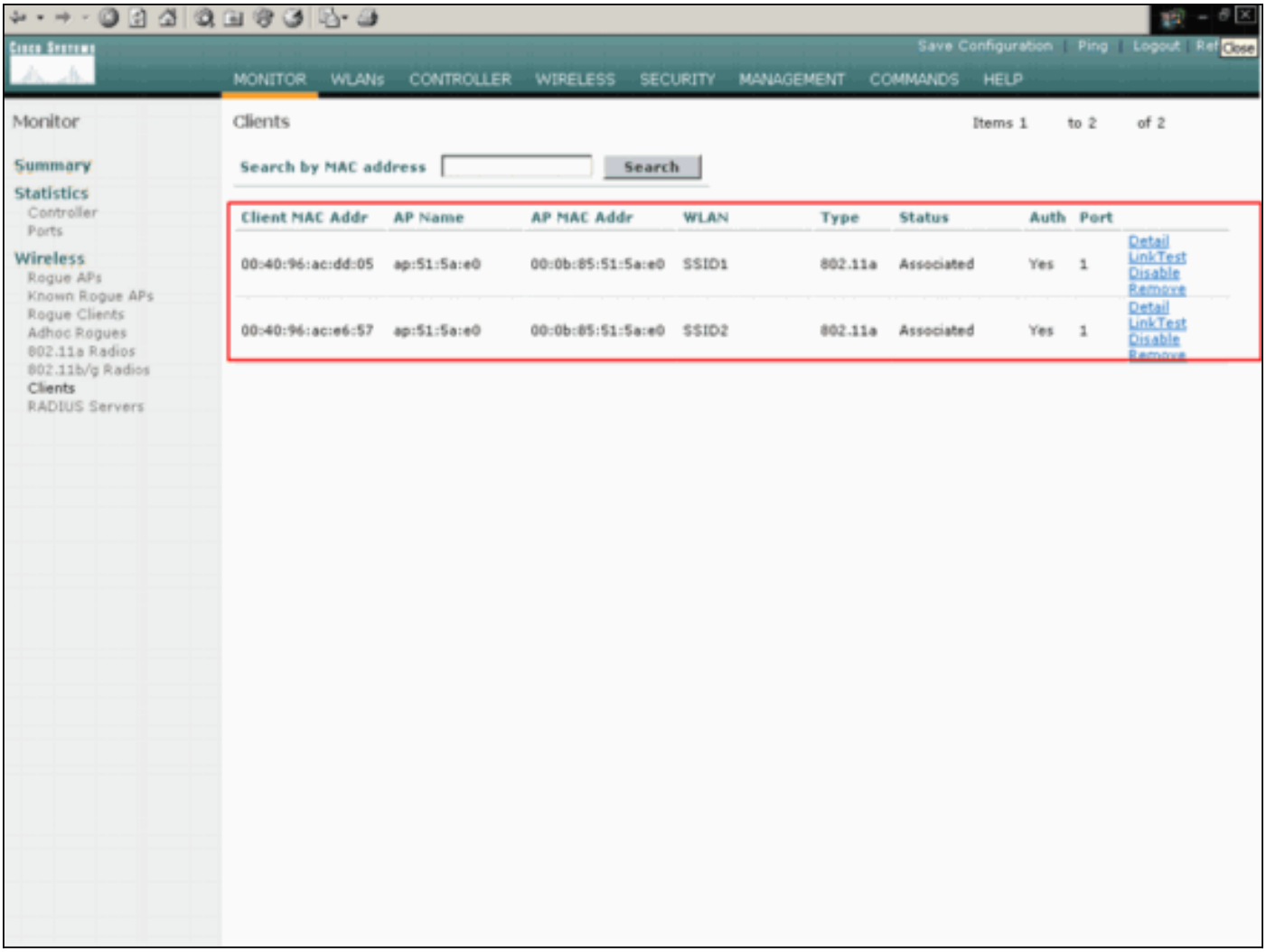
원격 사이트에 REAP AP 구축

이제 WLC에 WLAN을 구성하고 LAP를 준비했으며 본사와 원격 사무실 간에 WAN 링크를 설정했으므로 원격 사이트에 AP를 구축할 준비가 되었습니다.

원격 사이트에서 AP의 전원을 켜면 AP는 초기화 단계에서 구성한 순서대로 컨트롤러를 찾습니다.AP가 컨트롤러를 찾으면 AP가 컨트롤러에 등록됩니다.이제 DDoS 공격의 실제 사례를 살펴보겠습니다.WLC에서 AP가 포트 1의 컨트롤러에 연결되었음을 확인할 수 있습니다.



SSID **SSID1**을 가지고 있고 WPA-PSK가 활성화된 클라이언트는 WLAN 1의 AP에 연결합니다. SSID **SSID2**가 있고 802.1x 인증이 활성화된 클라이언트는 WLAN 2의 AP에 연결합니다. 다음은 두 개의 클라이언트를 보여주는 예입니다.클라이언트 하나가 WLAN 1에 연결되고 다른 클라이언트는 WLAN 2에 연결됩니다.



다음을 확인합니다.

이 섹션을 사용하여 REAP 구성이 제대로 작동하는지 확인합니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

WAN 링크를 축소합니다.WAN 링크가 다운되면 AP가 WLC와의 연결이 끊어집니다.그런 다음 WLC는 목록에서 AP를 등록 취소합니다.예를 들면 다음과 같습니다.

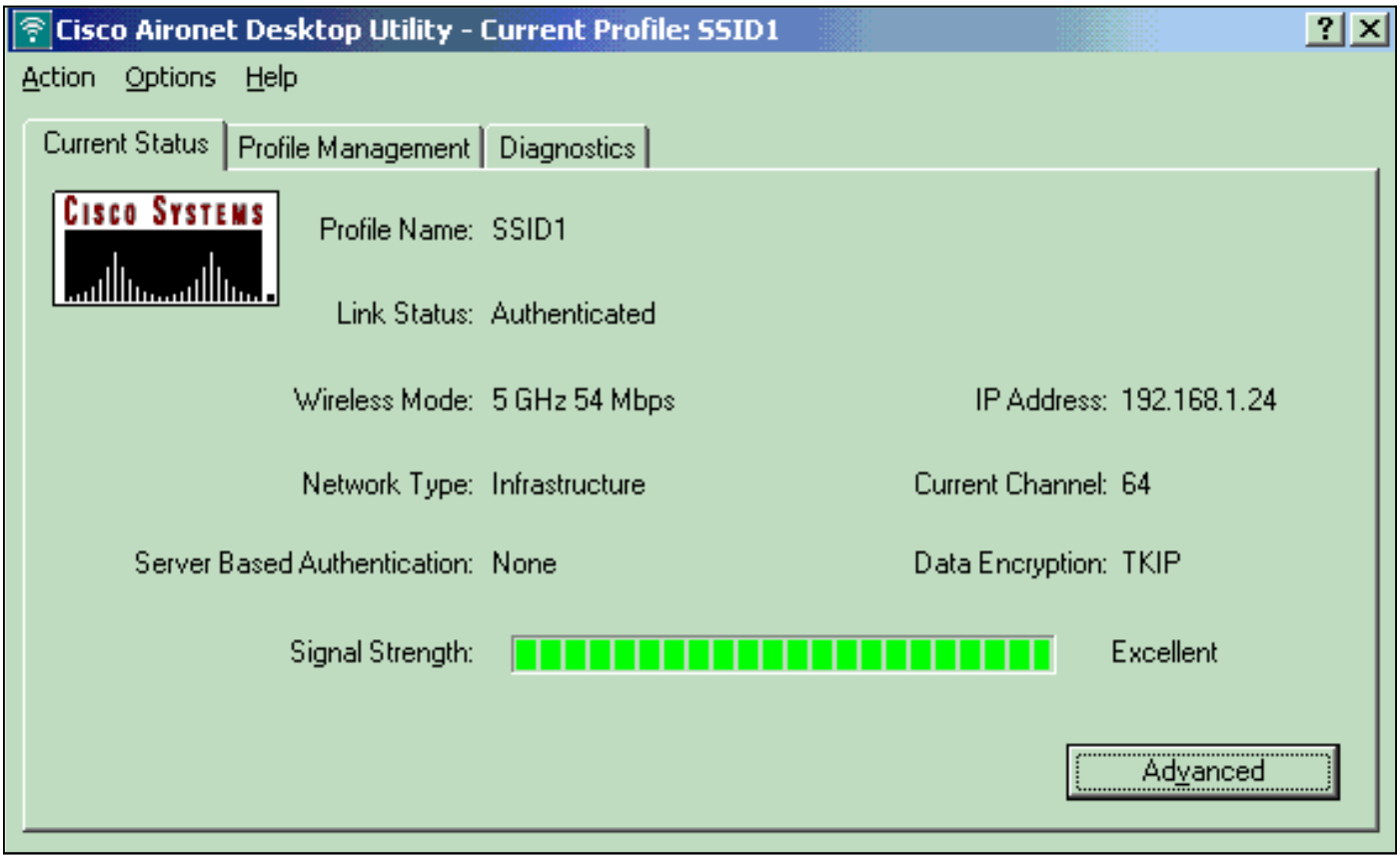
```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:04:22 2006: Did not receive heartbeat reply from AP 00:0B:85:51:5A:E0
Wed May 17 15:04:22 2006: Max retransmissions reached on AP 00:0B:85:51:5A:E0
(CONFIGURE_COMMAND, 1)
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Down LWAPP event for
AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event
for AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Down LWAPP event for
AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event
for AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:04:22 2006: spamDeleteLCB: stats timer not initialized for AP
00:0b:85:51:5a:e0
Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 0!
Wed May 17 15:04:22 2006: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 1!
```

```
Wed May 17 15:04:22 2006: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
```

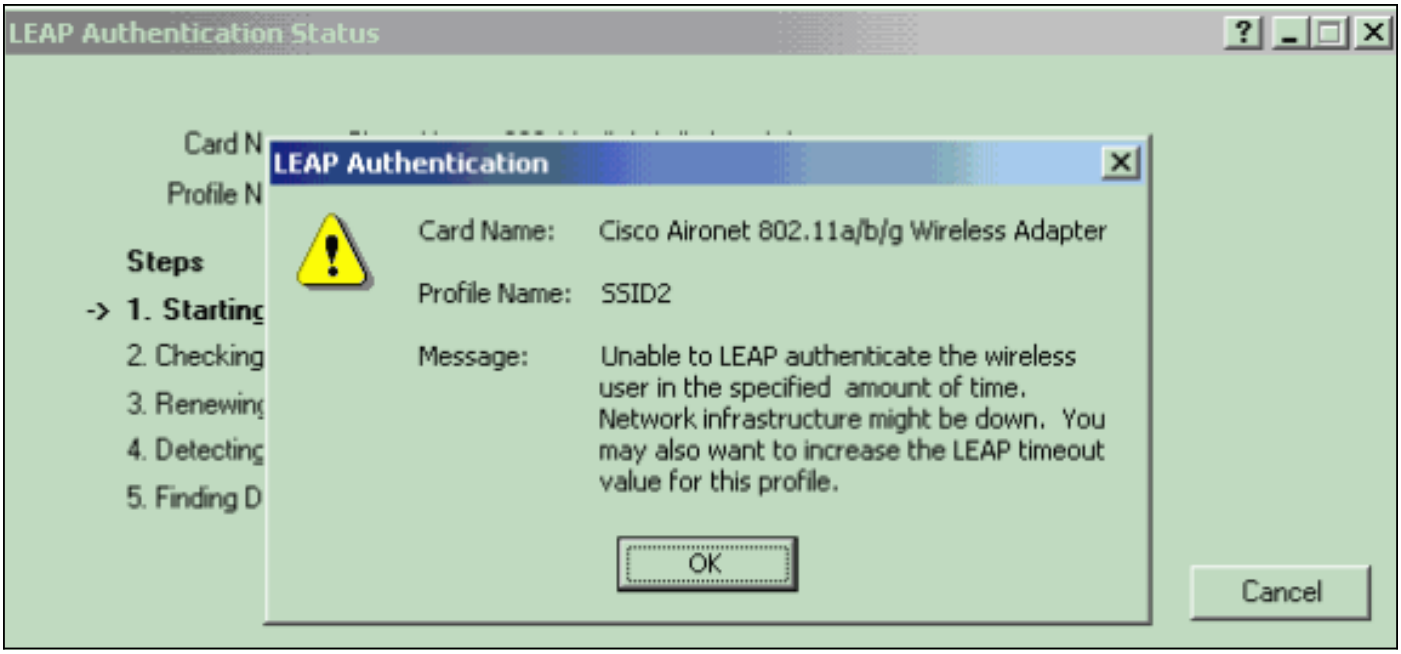
debug lwapp **events enable** 명령 출력에서 WLC가 AP에서 하트비트 응답을 받지 못했기 때문에 WLC가 AP를 등록 취소하는 것을 확인할 수 있습니다.하트비트 응답은 keepalive 메시지와 유사합니다.컨트롤러는 1초 간격으로 5회 연속 하트비트를 시도합니다.WLC가 회신을 받지 못하면 WLC는 AP를 등록 취소합니다.

AP가 독립형 모드에 있으면 AP 전원 LED가 깜박입니다.첫 번째 WLAN(WLAN 1)에 연결된 클라이언트는 첫 번째 WLAN의 클라이언트가 WPA-PSK 암호화에만 구성되어 있으므로 여전히 AP에 연결되어 있습니다.LAP는 독립형 모드에서 암호화 자체를 처리합니다.다음은 SSID1 및 WPA-PSK를 사용하여 WLAN 1에 연결된 클라이언트의 상태(WAN 링크가 다운된 경우)를 보여주는 예입니다.

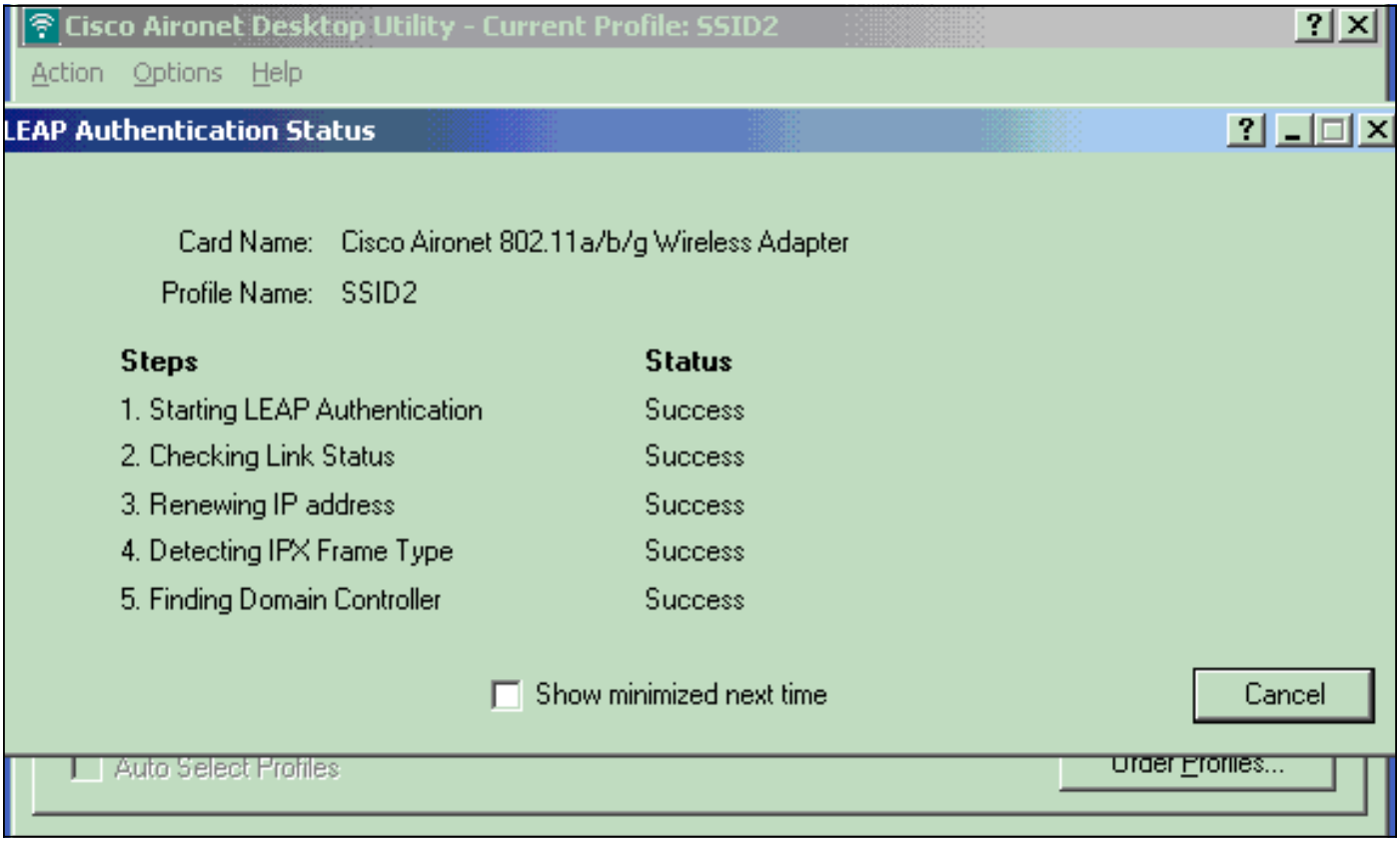
참고: TKIP는 WPA-PSK와 함께 사용되는 암호입니다.



WLAN 2는 EAP 인증을 사용하므로 WLAN 2에 연결된 클라이언트의 연결이 끊어집니다.이 연결 끊기는 EAP 인증을 사용하는 클라이언트가 WLC와 통신해야 하기 때문입니다.다음은 WAN 링크가 다운되었을 때 EAP 인증이 실패함을 보여주는 예제 창입니다.



WAN 링크가 작동하면 AP가 정상 REAP 모드로 다시 전환되고 컨트롤러에 등록합니다.EAP 인증을 사용하는 클라이언트도 나타납니다.예를 들면 다음과 같습니다.



컨트롤러에서 debug lwapp **events enable** 명령의 샘플 출력에는 다음 결과가 표시됩니다.

```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:06:40 2006: Successful transmission of LWAPP Discovery-Response
to AP 00:0b:85:51:5a:e0 on Port 1
Wed May 17 15:06:52 2006: Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0to
00:0b:85:33:84:a0 on port '1'
Wed May 17 15:06:52 2006: LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0is 1500,
remote debug mode is 0
Wed May 17 15:06:52 2006: Successfully added NPU Entry for AP 00:0b:85:51:5a:e0(index 51)
```

```
Switch IP: 172.16.1.51, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 192.168.1.5, AP
Port: 5550, next hop MAC: 00:d0:58:ad:ae:cb
Wed May 17 15:06:52 2006: Successfully transmission of LWAPP Join-Reply to AP
00:0b:85:51:5a:e0
Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:06:54 2006: Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:51:5a:e0 to
00:0b:85:33:84:a0
Wed May 17 15:06:54 2006: Updating IP info for AP 00:0b:85:51:5a:e0 -- static 1,
192.168.1.5/255.255.255.0, gtw 192.168.1.1
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

문제 해결 명령

이러한 **debug** 명령을 사용하여 컨피그레이션을 트러블슈팅할 수 있습니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug lwapp events enable** - LAP와 WLC 간에 발생하는 이벤트의 시퀀스를 표시합니다.
- **debug lwapp errors enable** - LWAPP 통신에서 발생하는 오류를 표시합니다.
- **debug lwapp packet enable** - LWAPP 패킷 추적의 디버그를 표시합니다.
- **debug mac addr** - 지정한 클라이언트에 대해 MAC 디버깅을 활성화합니다.

관련 정보

- 지사에서 REAP 구축 설명서
- WLAN 컨트롤러(WLC)를 사용한 EAP 인증 컨피그레이션 예
- 무선 LAN 컨트롤러 및 경량 액세스 포인트 기본 구성 예
- 경량 액세스 포인트에 대한 WLAN 컨트롤러 장애 조치 컨피그레이션 예
- 무선 지원 페이지
- 기술 지원 및 문서 – Cisco Systems