H-REAP 운영 모드 구성 예

목차

소개

이 문서에서는 H-REAP(Hybrid Remote Edge Access Point)의 개념을 소개하고, 구성의 예를 들어 다른 작동 모드를 설명합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- WLC(Wireless LAN Controller)에 대한 지식 및 WLC 기본 매개변수를 구성하는 방법
- REAP 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 릴리스 7.0.116.0을 실행하는 Cisco 4400 Series WLC
- Cisco 1131AG LAP(Lightweight Access Point)
- 버전 12.4(11)T를 실행하는 Cisco 2800 Series 라우터
- 펌웨어 릴리스 4.0을 실행하는 Cisco Aironet 802.11a/b/g Client Adapter
- Cisco Aironet Desktop Utility 버전 4.0
- 버전 4.0을 실행하는 Cisco Secure ACS

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

H-REAP은 지사 및 원격 사무실 구축을 위한 무선 솔루션입니다.H-REAP을 사용하면 각 사무실에 컨트롤러를 구축하지 않고도 WAN 링크를 통해 기업 지사나 원격 사무실의 AP(액세스 포인트)를 구성하고 제어할 수 있습니다.

H-REAP은 클라이언트 데이터 트래픽을 로컬로 전환하고 컨트롤러와의 연결이 끊길 때 클라이언트 인증을 로컬로 수행할 수 있습니다.컨트롤러에 연결되면 H-REAP는 트래픽을 컨트롤러에 다시 터널링할 수도 있습니다.연결된 모드에서 하이브리드 REAP AP는 로컬 인증도 수행할 수 있습니다.

H-REAP은 다음에서만 지원됩니다.

- 1130AG, 1140, 1240, 1250, 1260, AP801, AP 802, 1040 및 AP3550 AP
- Cisco 5500, 4400, 2100, 2500 및 Flex 7500 Series 컨트롤러
- Catalyst 3750G Integrated Controller Switch
- Catalyst 6500 Series Wireless Services Module(WiSM)
- ISR(Integrated Services Router)용 WLCM(Wireless LAN Controller Module)

H-REAP의 클라이언트 트래픽은 AP에서 로컬로 전환하거나 컨트롤러에 다시 터널링될 수 있습니다.이는 WLAN별 컨피그레이션에 따라 달라집니다.또한 H-REAP의 로컬로 스위칭된 클라이언트 트래픽은 802.1Q 태그가 지정되어 유선 측 분리를 제공할 수 있습니다.WAN 중단 동안 로컬에서 스위칭되고 로컬로 인증된 모든 WLAN에 대한 서비스가 지속됩니다.

참고: AP가 H-REAP 모드에 있고 원격 사이트에서 로컬로 스위칭되는 경우 RADIUS 서버 컨피그레이션을 기반으로 특정 VLAN에 사용자를 동적으로 할당하는 것은 지원되지 않습니다.그러나 AP에서 로컬로 수행된 SSID(Service Set Identifier) 매핑에 고정 VLAN을 기반으로 특정 VLAN에 사용자를 할당할 수 있어야 합니다.따라서 특정 SSID에 속한 사용자는 AP에서 SSID가 로컬로 매핑되는 특정 VLAN에 할당할 수 있습니다.

참고: Voice over WLAN이 중요한 경우 AP가 로컬 모드에서 실행되어야 H-REAP 모드에서 지원되지 않는 CCKM 및 CAC(Connection Admission Control) 지원이 제공됩니다.

REAP보다 H-REAP

REAP에 대한 자세한 내용은 Remote-Edge AP (REAP) with Lightweight APs and Wireless LAN Controller (WLCs) Configuration Example을 참조하십시오.

H-REAP은 다음과 같은 REAP의 단점으로 도입되었습니다.

- REAP은 유선 측 분리가 없습니다.이는 802.1Q 지원이 부족하기 때문입니다.WLAN의 데이터가 동일한 유선 서브넷에 있습니다.
- WAN 장애 시 REAP AP는 컨트롤러에 처음 지정된 것을 제외하고 모든 WLAN에서 제공되는 서비스를 중지합니다.

H-REAP은 다음과 같은 두 가지 단점을 극복합니다.

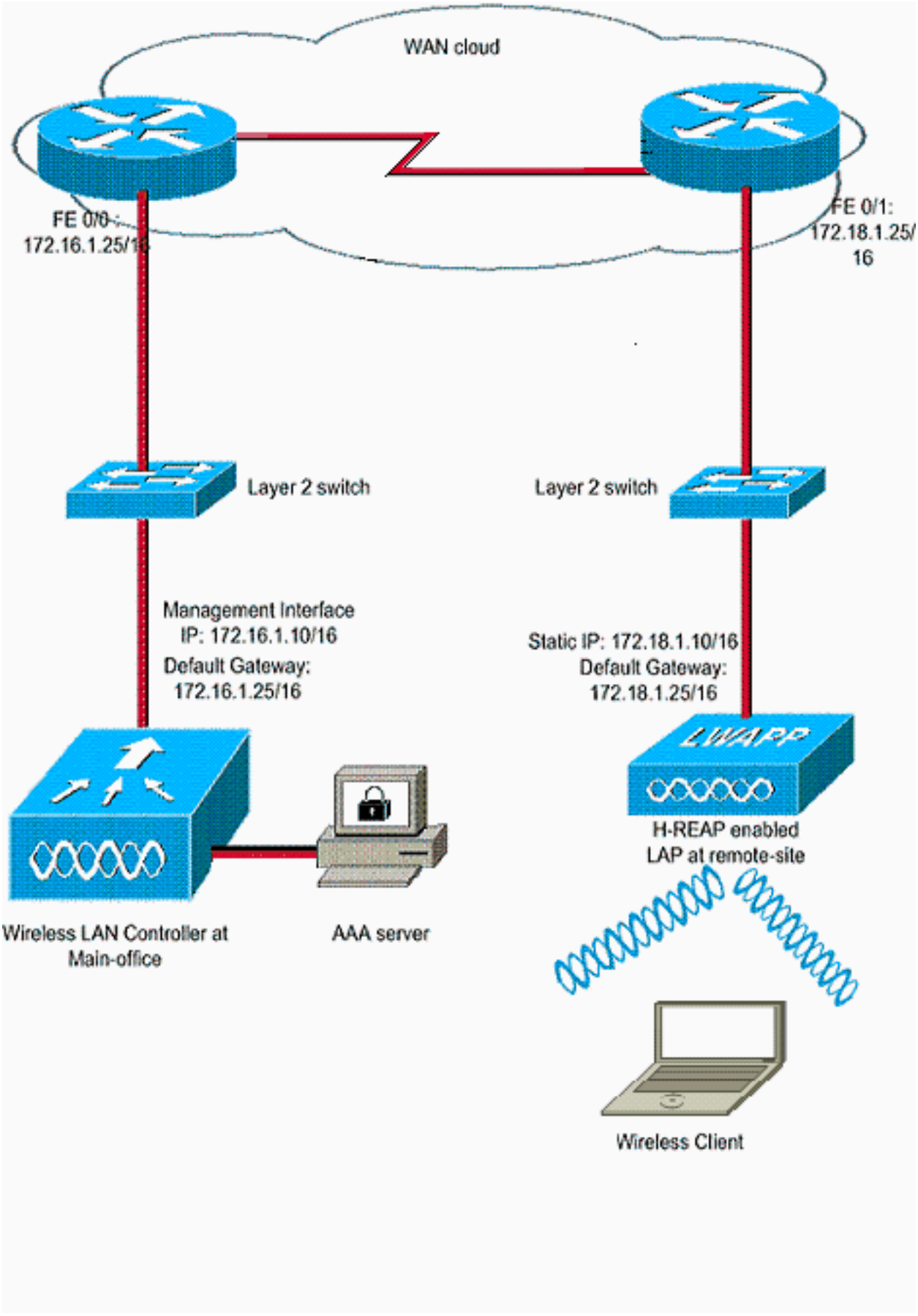
- dot1Q 지원 및 VLAN과 SSID 매핑을 제공합니다.이 VLAN과 SSID 매핑은 H-REAP에서 수행해야 합니다.이 작업을 수행하는 동안 구성된 VLAN이 중간 스위치 및 라우터의 포트를 통해 올바르게 허용되는지 확인합니다.
- 로컬 스위칭을 위해 구성된 모든 WLAN에 지속적인 서비스를 제공합니다.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 예에서는 컨트롤러가 기본 컨피그레이션으로 이미 구성되어 있다고 가정합니다.컨트롤러는 다음 컨피그레이션을 사용합니다.

- 관리 인터페이스 IP 주소—172.16.1.10/16
- AP-Manager 인터페이스 IP 주소—172.16.1.11/16
- 기본 게이트웨이 라우터 IP 주소—172.16.1.25/16
- 가상 게이트웨이 IP 주소 - 1.1.1.1

참고: 이 문서에서는 H-REAP와 컨트롤러 간에 사용할 수 있는 라우터 및 스위치의 WAN 컨피그레이션 및 컨피그레이션을 표시하지 않습니다.이는 WAN 캡슐화 및 사용되는 라우팅 프로토콜을 알고 있다고 가정합니다.또한 이 문서에서는 WAN 링크를 통해 H-REAP와 컨트롤러 간의 연결을 유지하기 위해 구성 방법을 이해하는 것으로 가정합니다.이 예에서 HDLC 캡슐화는 WAN 링크에서 사용됩니다.

컨트롤러로 AP 초기화 및 H-REAP 구성

CAPWAP 검색 메커니즘을 사용할 수 없는 원격 네트워크에서 AP가 컨트롤러를 검색하도록 하려면 priming을 사용할 수 있습니다.이 방법을 사용하면 AP가 연결할 컨트롤러를 지정할 수 있습니다.

H-REAP 지원 AP를 초기화하려면 AP를 본사의 유선 네트워크에 연결합니다.부팅 중에 H-REAP 지원 AP는 먼저 IP 주소를 찾습니다.DHCP 서버를 통해 IP 주소를 얻으면 부팅되고 등록 프로세스를 수행할 컨트롤러를 찾습니다.

H-REAP AP는 WLC(Wireless LAN Controller)에 LAP(Lightweight AP) 등록에 설명된 방법으로 컨트롤러 IP 주소를 학습할 수 있습니다.

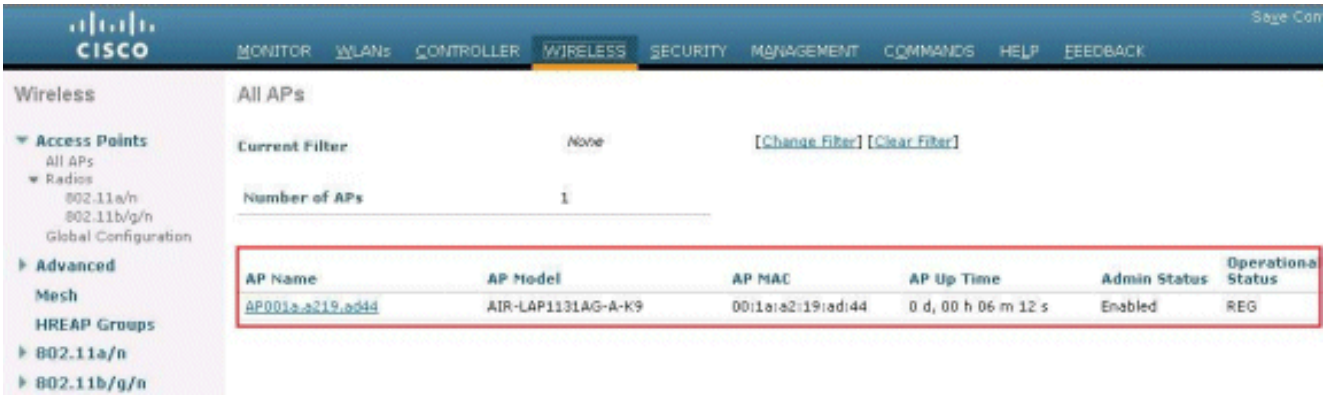
참고: AP에서 CLI 명령을 통해 컨트롤러를 검색하도록 LAP를 구성할 수도 있습니다.자세한 내용은 CLI 명령을 사용하여 H-REAP 컨트롤러 검색을 참조하십시오.

이 문서의 예에서는 컨트롤러 IP 주소를 학습하기 위해 H-REAP에 DHCP 옵션 43 절차를 사용합니다.그런 다음 컨트롤러에 연결하고 컨트롤러에서 최신 소프트웨어 이미지 및 컨피그레이션을 다운로드하고 무선 링크를 초기화합니다.독립형 모드에서 사용할 수 있도록 다운로드된 컨피그레이션을 비휘발성 메모리에 저장합니다.

LAP가 컨트롤러에 등록되면 다음 단계를 완료합니다.

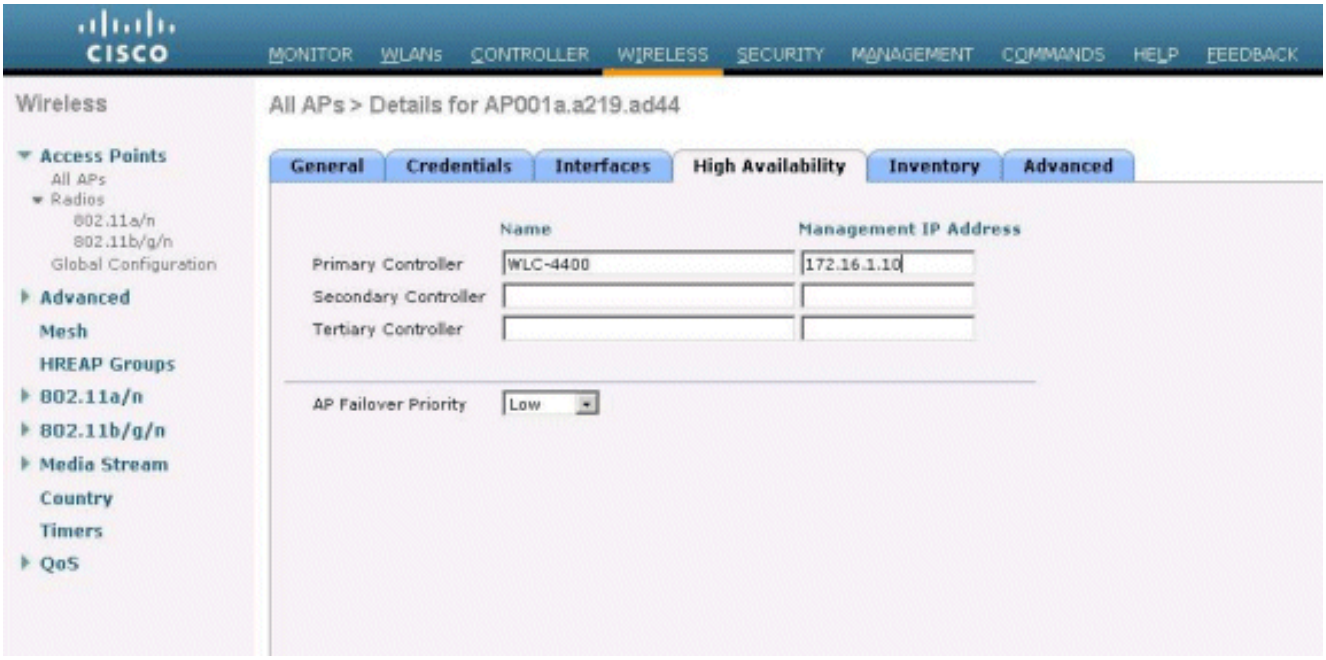
1. 컨트롤러 GUI에서 Wireless(무선) **>Access Points(액세스 포인트)를** 선택합니다.이 컨트롤러에 등록된 LAP가 표시됩니다.
2. 구성할 AP를 클릭합니다

.



3. APs>Details(APs>세부사항) 창에서 High Availability(고가용성) 탭을 클릭하고 AP가 등록하는 데 사용할 컨트롤러 이름을 정의한 다음 **Apply(적용)**를 클릭합니다

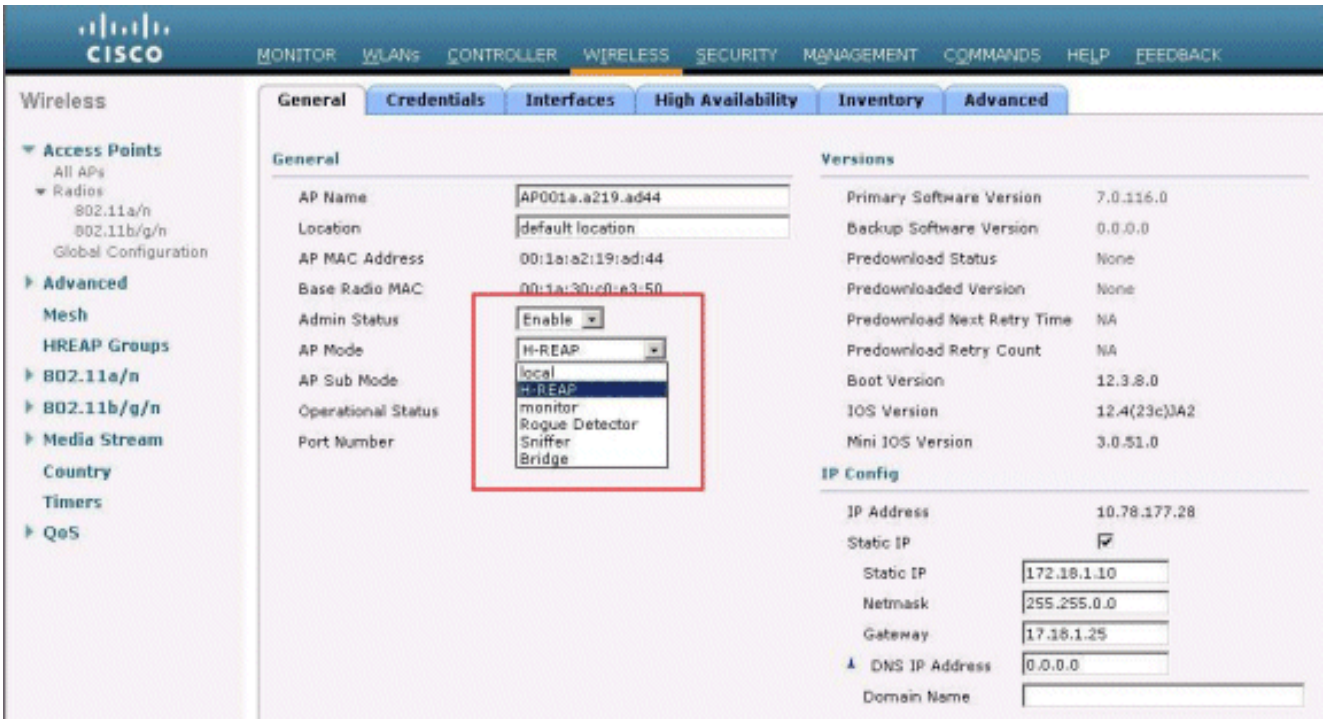
.



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.

4. H-REAP용 LAP를 구성합니다.H-REAP 모드에서 작동하도록 LAP를 구성하려면 APs>Details 창의 General(일반) 탭 아래에서 해당 드롭다운 메뉴에서 **AP 모드**를 H-REAP로 선택합니다 .이렇게 하면 LAP가 H-REAP 모드에서 작동하도록 구성됩니다

.



참고: 이 예에서는 AP의 IP 주소가 고정 모드로 변경되고 고정 IP 주소 172.18.1.10이 할당되었음을 확인할 수 있습니다.이 할당은 원격 사무실에서 사용할 서브넷이기 때문에 발생합니다 .따라서 DHCP 서버의 IP 주소를 사용하지만 등록 단계에서 처음 사용하는 경우에만 사용합니다.AP가 컨트롤러에 등록되면 주소를 고정 IP 주소로 변경합니다.

이제 LAP가 컨트롤러와 함께 준비되고 H-REAP 모드로 구성되었으므로, 다음 단계는 컨트롤러 측에서 H-REAP를 구성하고 H-REAP 스위칭 상태에 대해 논의하는 것입니다.

H-REAP 운영 이론

H-REAP 지원 LAP는 다음과 같은 두 가지 모드에서 작동합니다.

- **연결된** 모드:WLC에 대한 CAPWAP 컨트롤 플레인 링크가 작동 및 작동 중일 때 H-REAP가 연결 모드에 있다고 합니다.즉, LAP와 WLC 간의 WAN 링크가 다운되지 않습니다.
- **독립형** 모드:WLC에 대한 WAN 링크가 다운된 경우 H-REAP가 독립형 모드로 전환된다고 합니다.예를 들어, 이 H-REAP가 더 이상 WAN 링크를 통해 연결된 WLC에 연결되지 않을 경우.

클라이언트를 인증하는 데 사용되는 인증 메커니즘은 **Central** 또는 **Local**로 정의할 수 있습니다.

- **Central Authentication(중앙 인증)** - 원격 사이트에서 WLC의 프로세스를 포함하는 인증 유형을 참조합니다.
- **Local Authentication(로컬 인증)** - 인증을 위해 WLC에서 어떤 프로세스도 수행하지 않는 인증 유형을 참조합니다.

참고: 모든 802.11 인증 및 연결 처리는 LAP의 어떤 모드에 있든지 H-REAP에서 발생합니다.연결된 모드에서 H-REAP는 이러한 연결 및 인증을 WLC에 프록시합니다.독립형 모드에서는 LAP가 WLC에 이러한 이벤트를 알릴 수 없습니다.

클라이언트가 H-REAP AP에 연결되면 AP는 모든 인증 메시지를 컨트롤러에 전달합니다.인증에 성공하면 데이터 패킷이 로컬로 전환되거나 컨트롤러로 다시 터널링됩니다.이는 연결된 WLAN의 컨피그레이션에 따라 결정됩니다.

H-REAP을 사용하면 컨트롤러에 구성된 WLAN은 두 가지 다른 모드로 작동할 수 있습니다.

- **중앙 스위칭:**H-REAP의 WLAN은 해당 WLAN의 데이터 트래픽이 WLC로 터널링되도록 구성된 경우 중앙 스위칭 모드에서 작동하는 것으로 알려져 있습니다.
- **로컬 스위칭:**H-REAP의 WLAN은 WLC로 터널링되지 않고 해당 WLAN의 데이터 트래픽이 LAP 자체의 유선 인터페이스에서 로컬로 종료될 경우 로컬 스위칭 모드에서 작동한다고 합니다.**참고:** H-REAP 기능을 지원하는 1130, 1240 및 1250 Series AP에는 이러한 WLAN만 적용할 수 있으므로 WLAN 1~8만 H-REAP 로컬 스위칭에 대해 구성할 수 있습니다.

H-REAP 스위칭 상태

이전 섹션에서 언급한 인증 및 스위칭 모드와 결합되어 H-REAP는 다음 중 어느 한 상태에서 작동할 수 있습니다.

- 중앙 인증, 중앙 스위칭
- 인증 중단, 전환 중단
- 중앙 인증, 로컬 스위칭
- 인증 중단, 로컬 스위칭
- 로컬 인증, 로컬 스위칭

중앙 인증, 중앙 스위칭

이 상태에서 지정된 WLAN에 대해 AP는 모든 클라이언트 인증 요청을 컨트롤러에 전달하고 모든 클라이언트 데이터를 WLC에 터널링합니다.이 상태는 H-REAP이 연결된 모드에 있는 경우에만 유효합니다.이 모드에서 작동하도록 구성된 WLAN은 인증 방법이 무엇이든지 WAN 중단 중에 손실됩니다.

이 예에서는 다음 컨피그레이션 설정을 사용합니다.

- WLAN/SSID 이름:**중앙**
- 레이어 2 보안:**WPA2**
- H-REAP 로컬 스위칭:**비활성화됨**

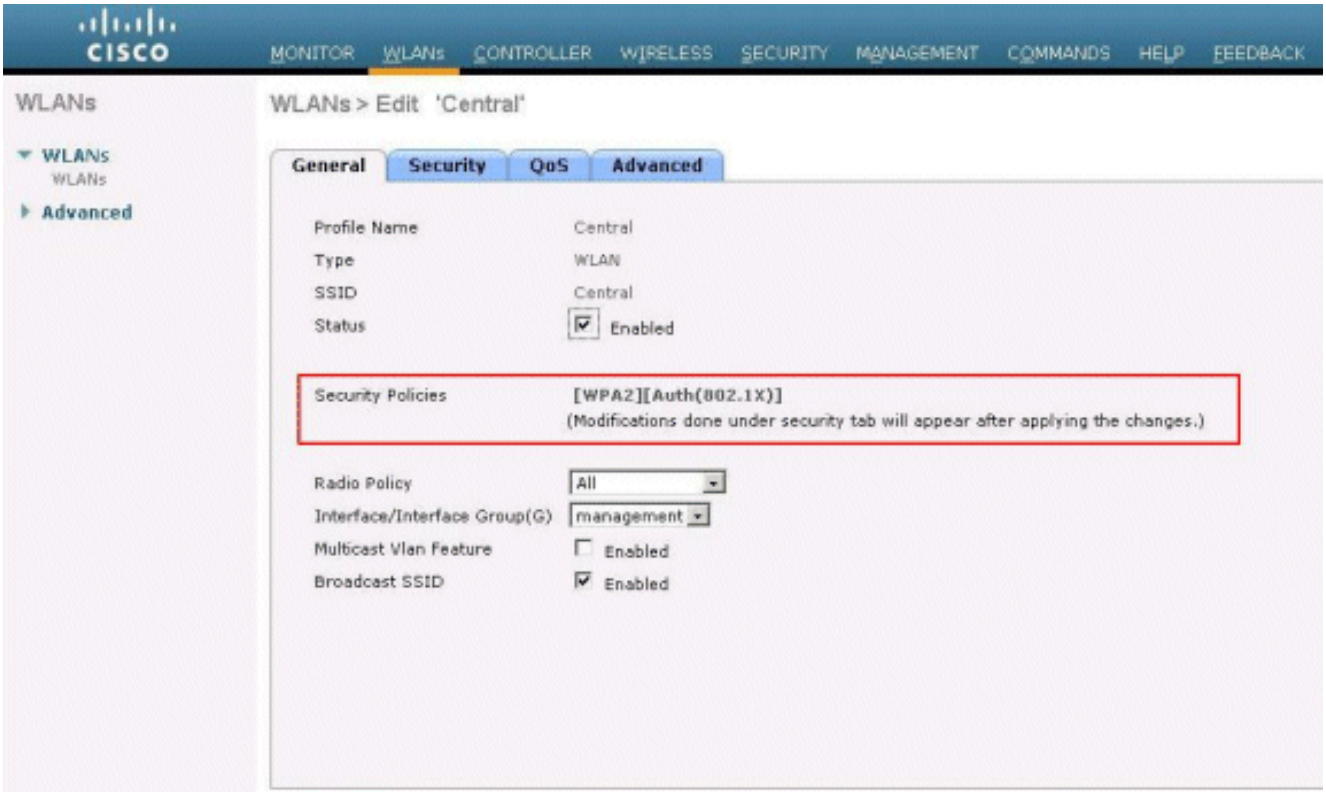
GUI를 사용하여 중앙 인증, 중앙 스위칭을 위한 WLC를 구성하려면 다음 단계를 완료합니다.

1. WLANs(**WLANs)**를 클릭하여 Central이라는 새 WLAN을 생성한 다음 Apply(적용)를 **클릭합니다**

.

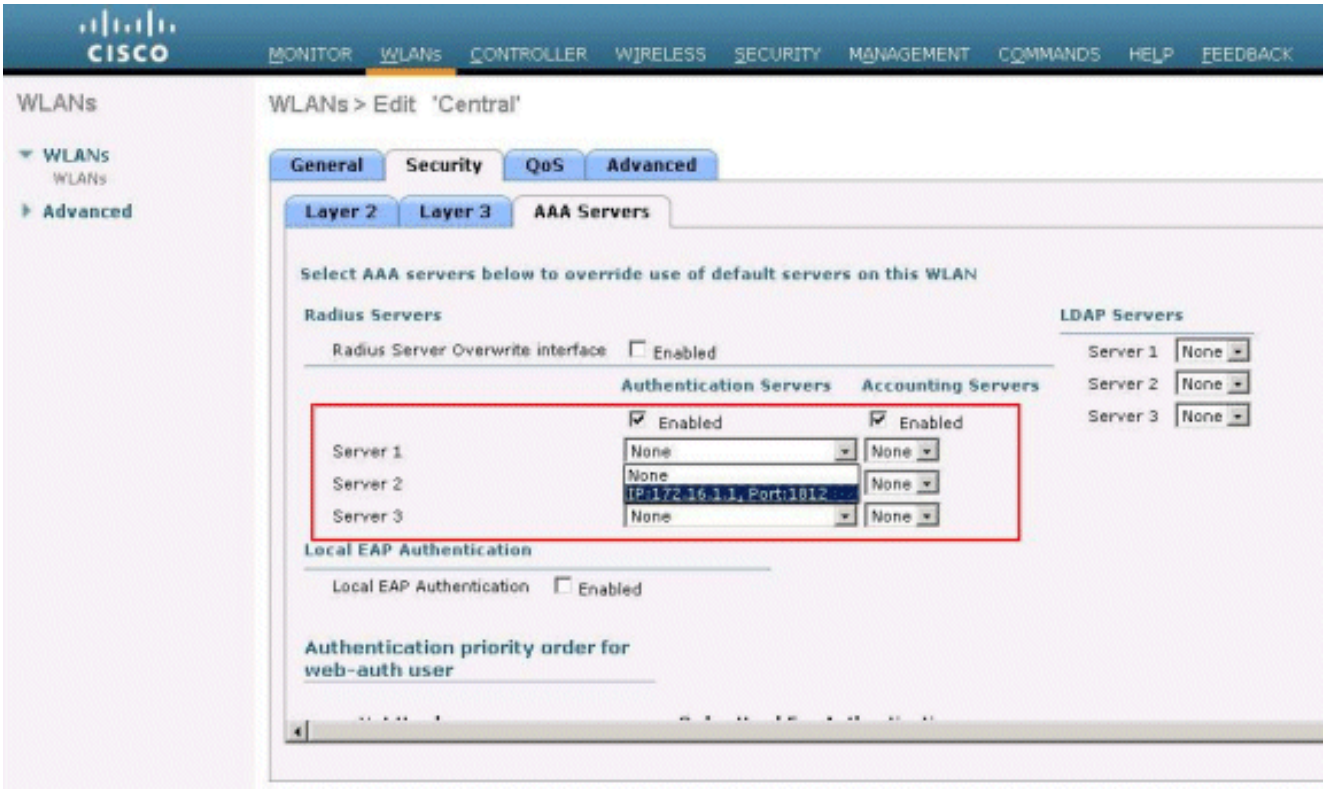
2. 이 WLAN은 중앙 인증을 사용하므로 Layer 2 Security(레이어 2 보안) 필드에서 WPA2 인증을 사용합니다.WPA2는 WLAN의 기본 레이어 2 보안입니다

.



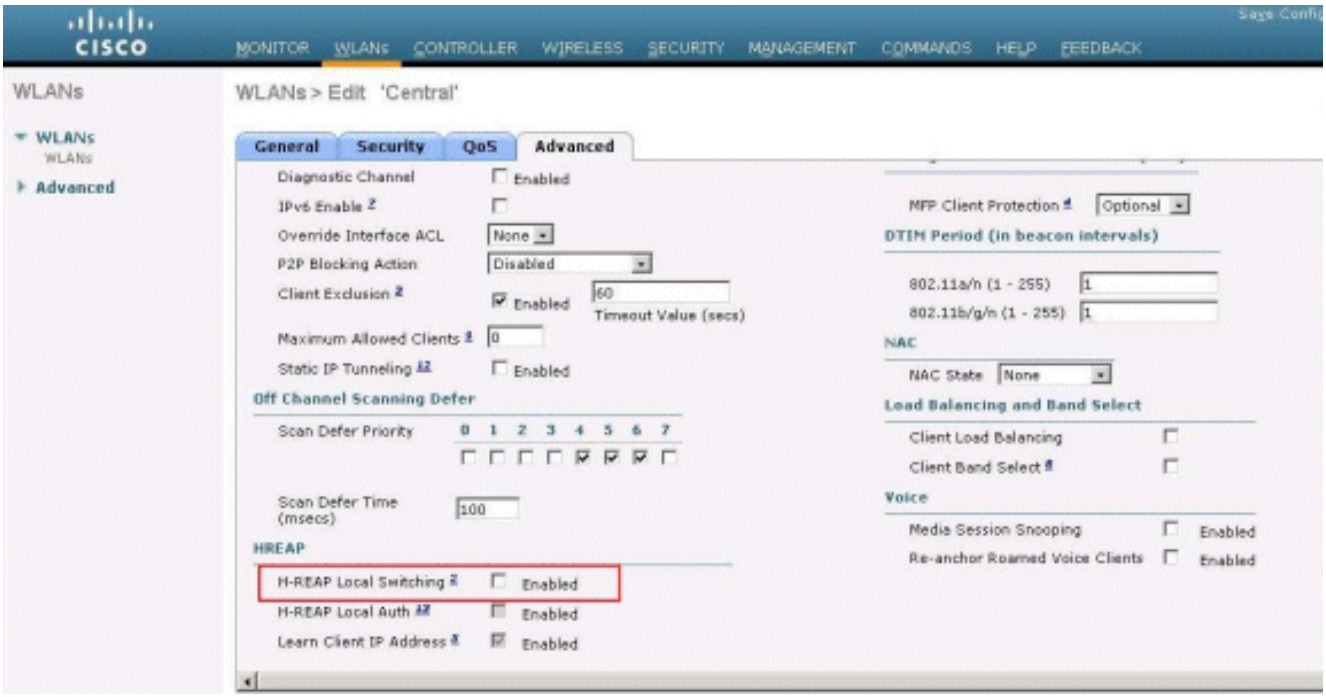
3. AAA Servers(AAA 서버) 탭을 선택한 다음 인증에 대해 구성된 적절한 서버를 선택합니다

.



4. 이 WLAN은 중앙 스위칭을 사용하므로 H-REAP Local Switching(H-REAP 로컬 스위칭) 확인란이 비활성화되었는지 확인해야 합니다(예: 로컬 스위칭 확인란이 선택되지 않음). 그런 다음 **적용**을 클릭합니다

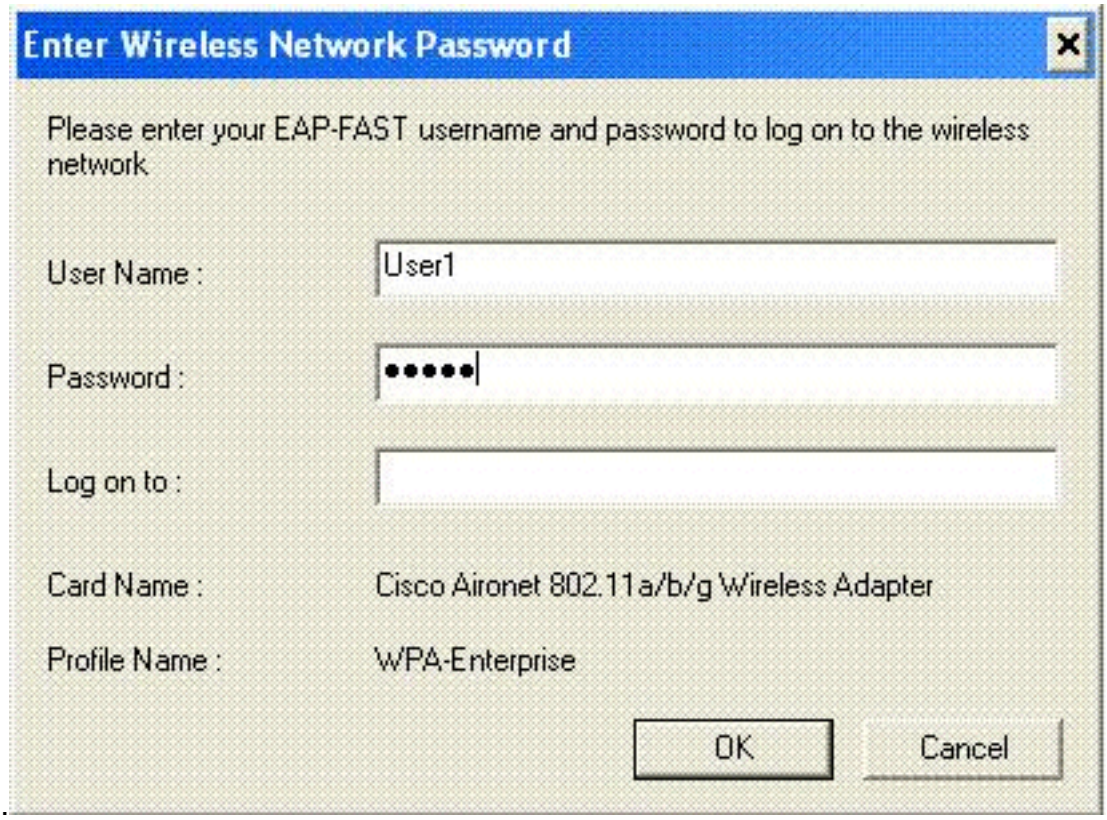
.



중앙 인증, 중앙 스위칭 확인

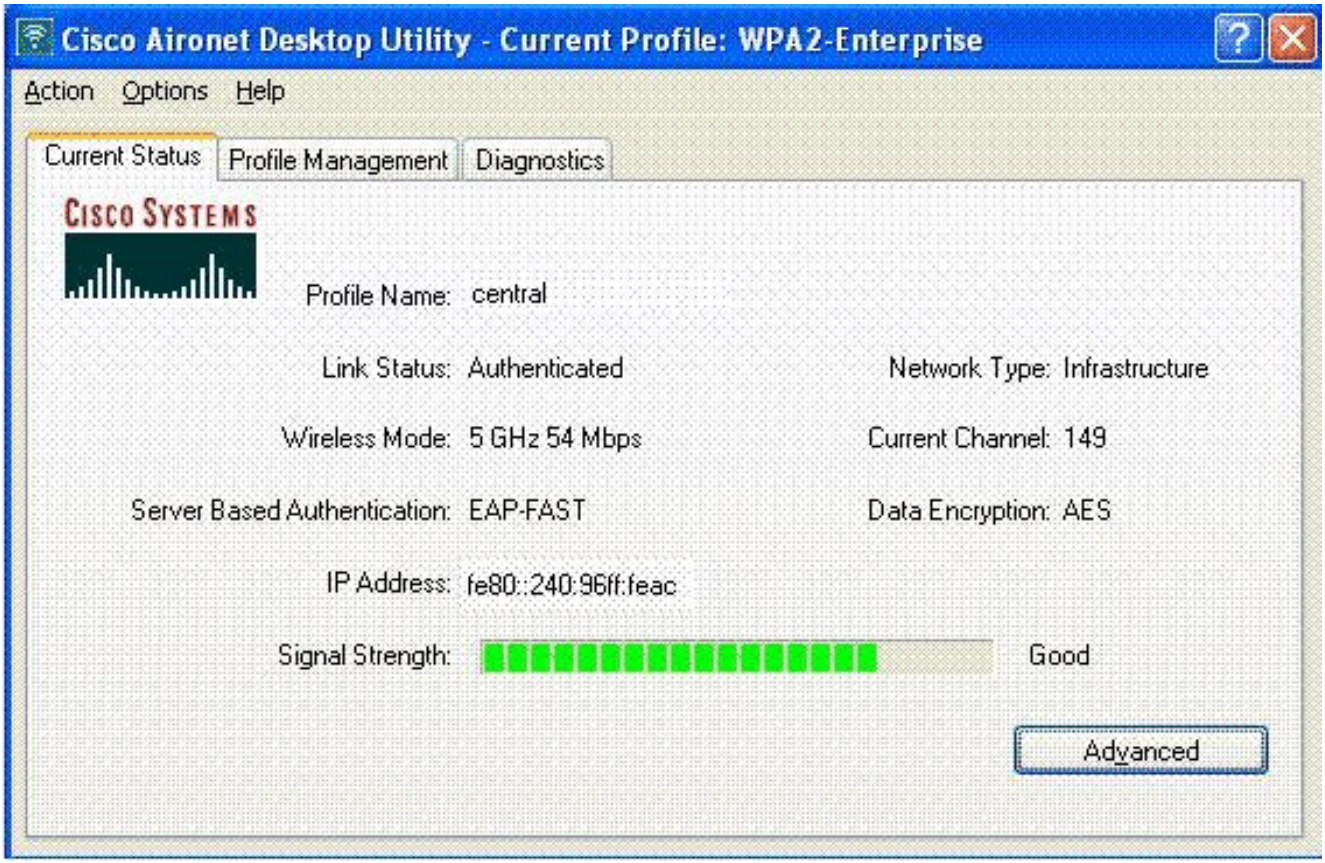
다음 단계를 완료하십시오.

1. 동일한 SSID 및 보안 컨피그레이션으로 무선 클라이언트를 구성합니다.이 예에서 SSID는 *Central*이고 보안 방법은 *WPA2입니다*.
2. 클라이언트에서 중앙 SSID를 활성화하려면 RADIUS 서버>사용자 설정에 구성된 대로 사용자 이름과 비밀번호를 입력합니다.이 예에서는 *User1*을 사용자 이름과 비밀번호로 사용합니다



. 클라이언트는 RADIUS 서버에 의해 중앙에서 인증되며 H-REAP AP에 연결됩니다.H-REAP은 이제 **중앙 인증, 중앙 스위칭**에 **포함됩니다**

.



인증 중단, 전환 중단

Central Authentication, Central Switching 섹션에 설명된 것과 동일한 컨피그레이션을 사용하여 컨트롤러를 연결하는 WAN 링크를 비활성화합니다.이제 컨트롤러는 AP에서 하트비트 응답을 기다립니다.하트비트 응답은 keepalive 메시지와 유사합니다.컨트롤러는 매 1초마다 5개의 연속 하트비트

를 시도합니다.

H-REAP의 하트비트 응답으로 수신되지 않으므로 WLC는 LAP를 등록 취소합니다.

WLC의 **CLI**에서 debug capwap events enable 명령을 실행하여 등록 취소 프로세스를 확인합니다 .다음은 이 **debug** 명령의 출력 예입니다.

```
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Did not receive heartbeat reply from
AP 00:15:c7:ab:55:90
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:
15:c7:ab:55:90 slot 0!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:
c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:
15:c7:ab:55:90 slot 1!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:
c7:ab:55:90 slot 1
```

H-REAP은 독립형 모드로 들어갑니다.

이 WLAN은 이전에 중앙에서 인증되고 중앙에서 전환되었으므로 제어 및 데이터 트래픽이 모두 컨트롤러에 다시 터널링되었습니다.따라서 컨트롤러가 없으면 클라이언트가 H-REAP와의 연결을 유지할 수 없으며 연결이 끊어집니다.클라이언트 연결 및 인증이 모두 중단된 H-REAP의 이 상태를 Authentication Down, Switching Down이라고 합니다.

중앙 인증, 로컬 스위칭

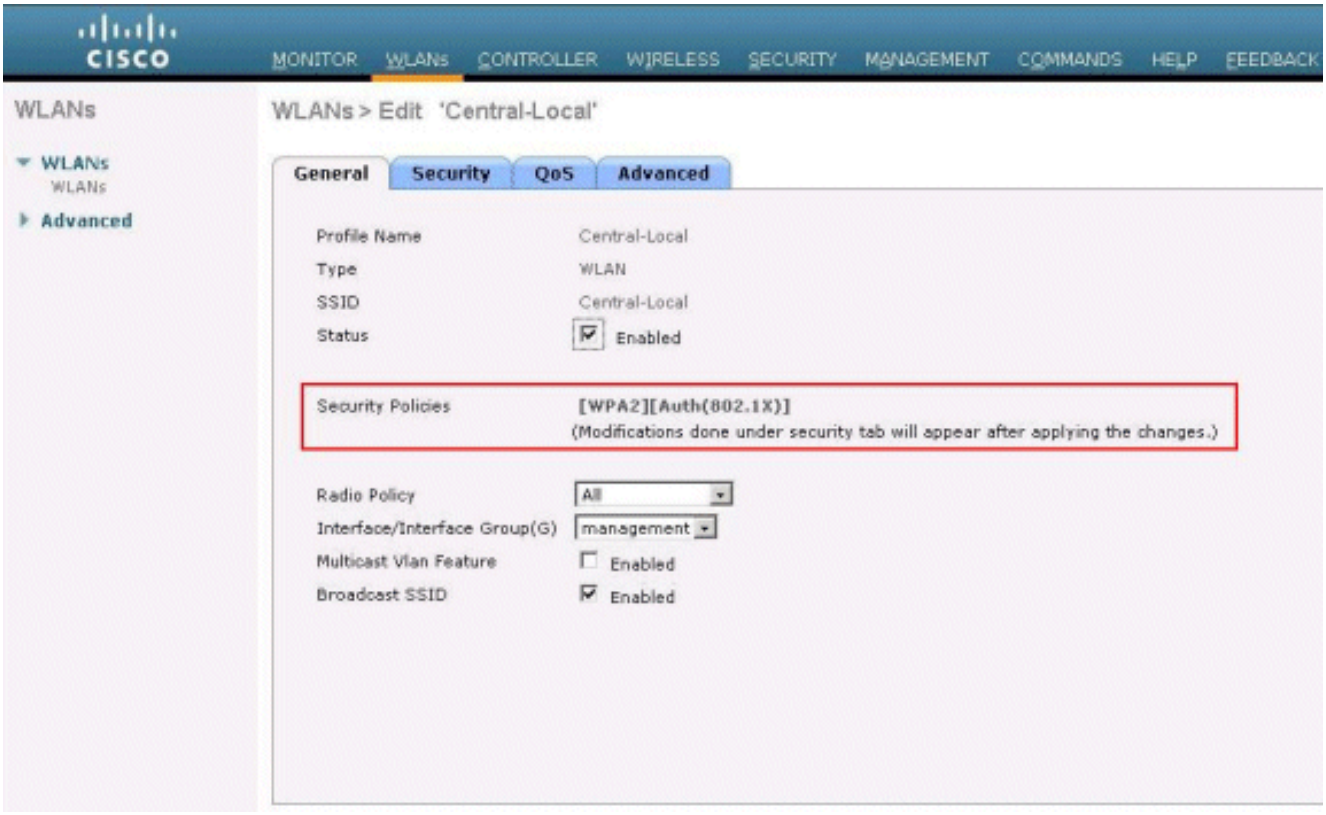
이 상태에서 지정된 WLAN의 경우 WLC는 모든 클라이언트 인증을 처리하고 H-REAP LAP는 데이터 패킷을 로컬로 전환합니다.클라이언트가 성공적으로 인증되면 컨트롤러는 capwap 제어 명령을 H-REAP에 전송하고 LAP에 해당 클라이언트의 데이터 패킷을 로컬로 전환하도록 지시합니다.이 메시지는 인증 성공 시 클라이언트당 전송됩니다.이 상태는 연결된 모드에서만 적용됩니다.

이 예에서는 다음 컨피그레이션 설정을 사용합니다.

- WLAN/SSID 이름:**중앙-로컬**
- 레이어 2 보안:**WPA2**.
- H-REAP 로컬 스위칭:**사용**

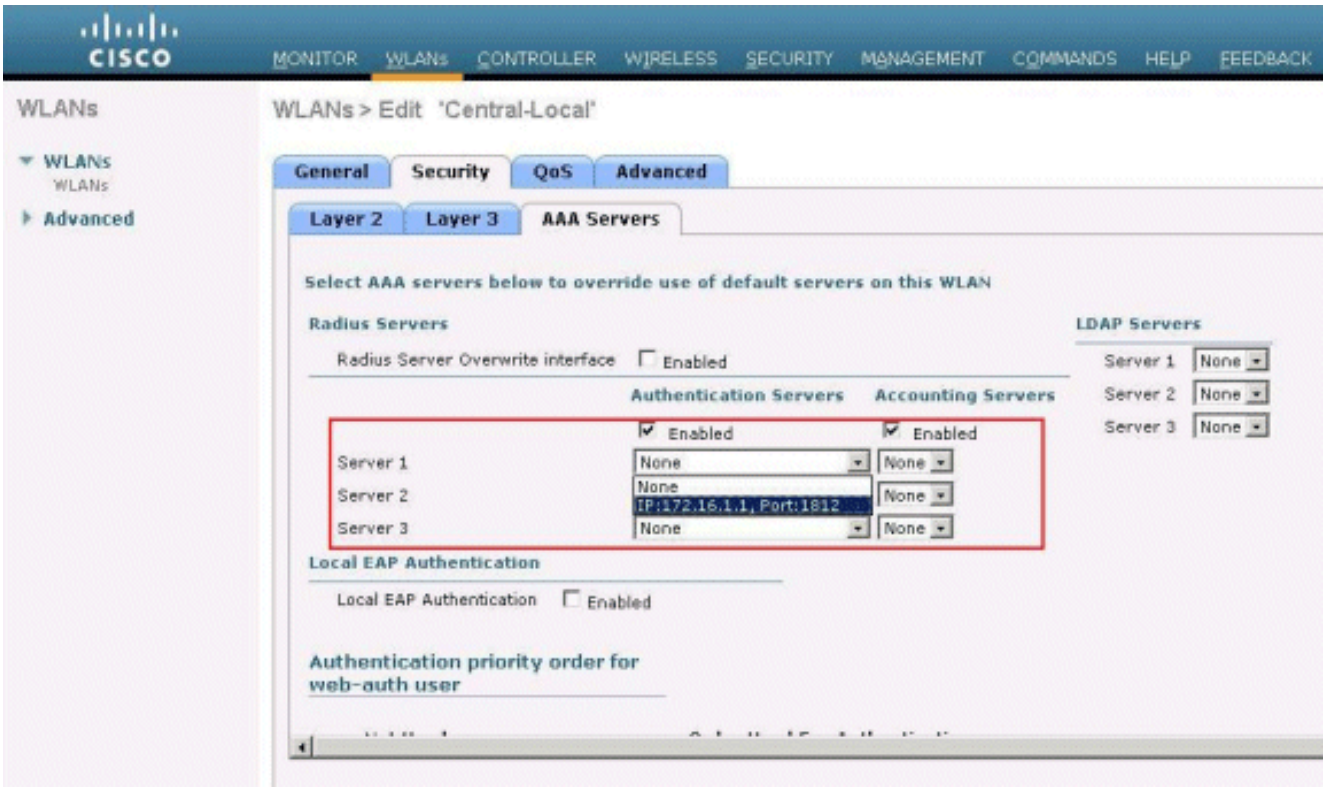
컨트롤러 GUI에서 다음 단계를 완료합니다.

1. Central-Local이라는 새 WLAN을 생성하려면 **WLANs**를 클릭한 다음 Apply(적용)를 **클릭합니다**.
2. 이 WLAN은 중앙 인증을 사용하므로 Layer 2 Security(레이어 2 보안) 필드에서 **WPA2** 인증을 선택합니다
   .



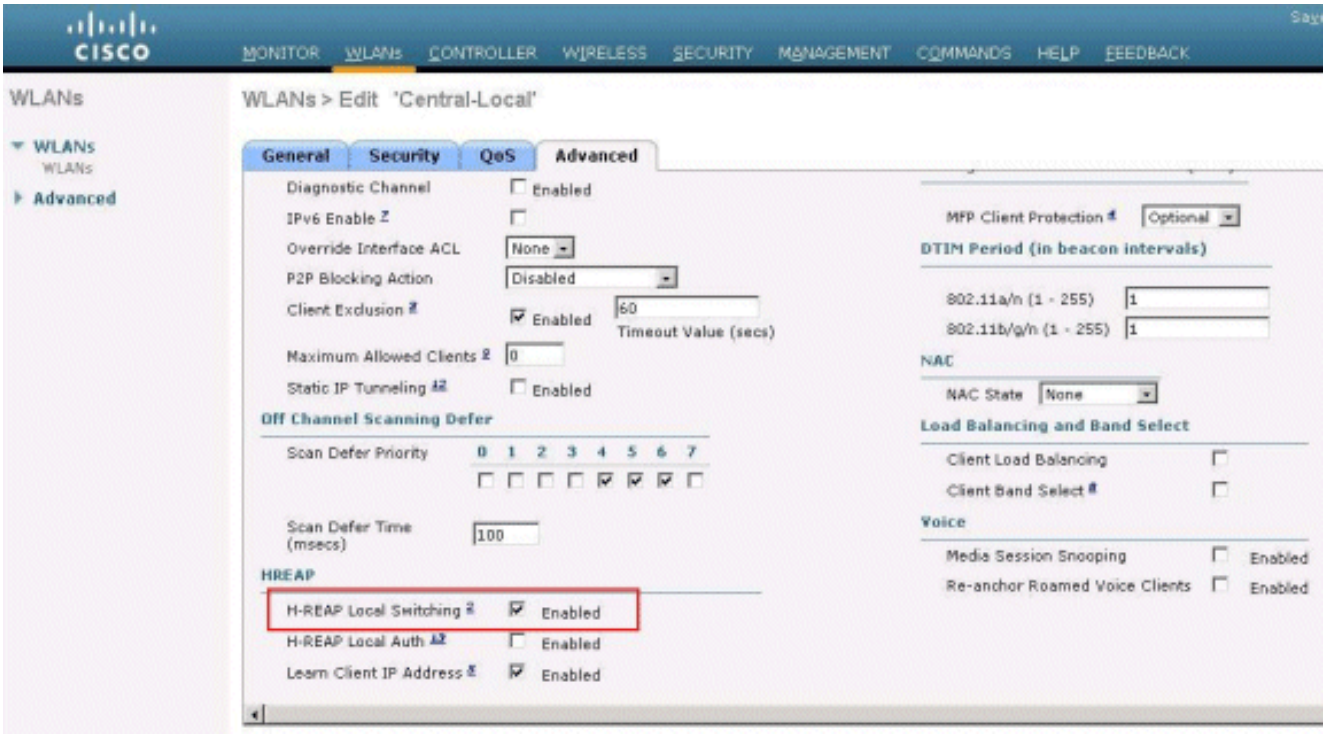
3. Radius Servers(RADIUS 서버) 섹션에서 인증에 대해 구성된 적절한 서버를 선택합니다

.



4. H-**REAP에서** 이 WLAN에 속한 클라이언트 트래픽을 로컬로 전환하려면 H-REAP Local Switching 확인란을 선택합니다

.



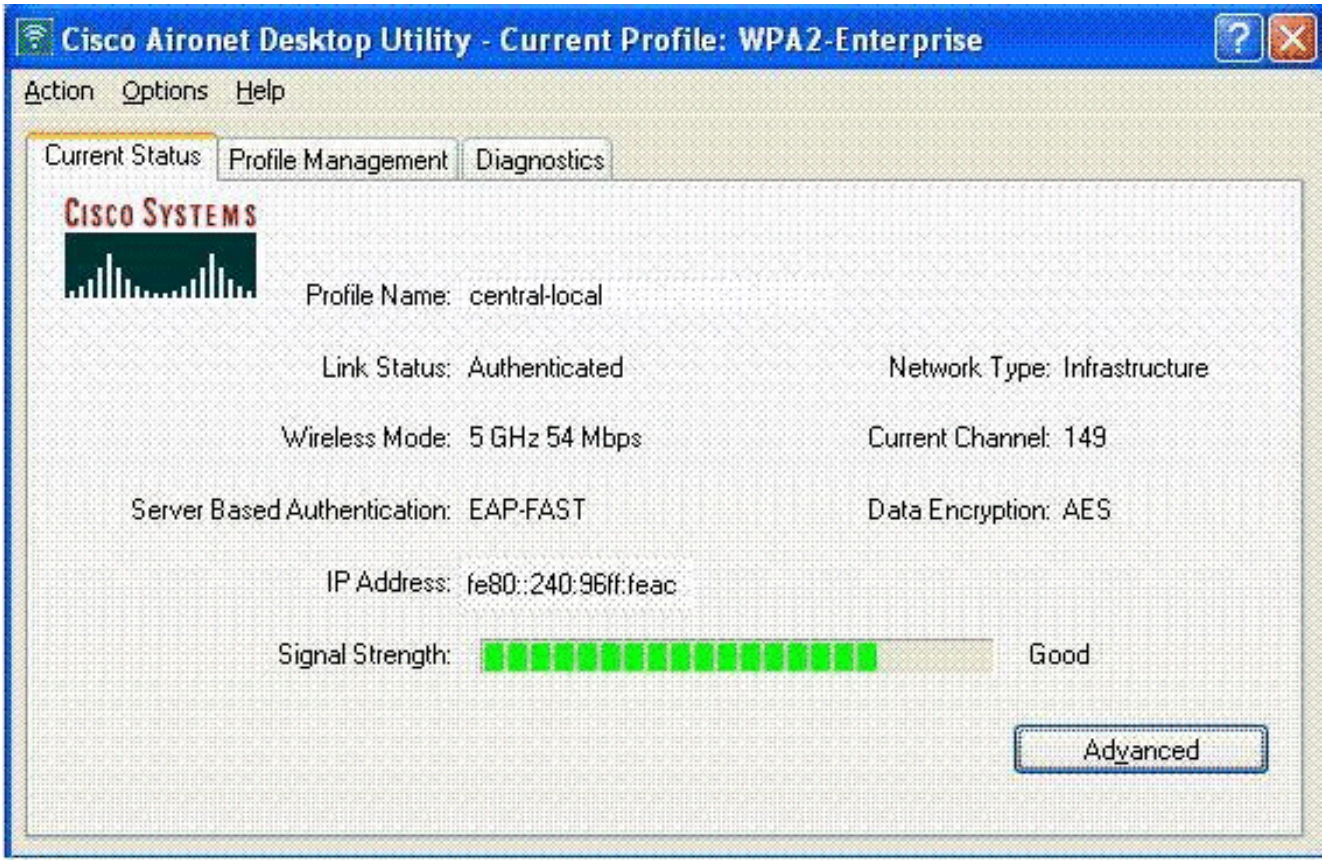
중앙 인증, 로컬 스위칭 확인

다음 단계를 완료하십시오.

1. 동일한 SSID 및 보안 컨피그레이션으로 무선 클라이언트를 구성합니다.이 예에서 SSID는 *Central-Local*이고 보안 방법은 *WPA2입니다*.
2. 클라이언트에서 중앙 로컬 SSID를 활성화하려면 RADIUS 서버>사용자 설정에 구성된 대로 사용자 이름과 비밀번호를 입력합니다.이 예에서는 *User1*을 사용자 이름과 비밀번호로 사용

합니다.
3. **확인**을 **클릭합니다**.클라이언트는 RADIUS 서버에 의해 중앙에서 인증되며 H-REAP AP와 연결됩니다.H-REAP은 이제 **중앙 인증, 로컬 스위칭에 있습니다**

.



인증 중단, 로컬 스위칭

WLC에서 처리해야 하는 인증 유형(예: EAP 인증[동적 WEP/WPA/WPA2/802.11i], WebAuth 또는 NAC)에 대해 로컬로 스위칭된 WLAN이 구성된 경우 WAN 장애 시 **인증 다운 로컬 스위칭** 상태를 입력합니다.이 상태에서 지정된 WLAN에 대해 H-REAP은 인증을 시도하는 새 클라이언트를 거부합니다.그러나 기존 클라이언트가 제대로 연결되도록 신호를 계속 보내고 응답을 검색합니다.이 상태는 독립형 모드에서만 유효합니다.

이 상태를 확인하려면 Central Authentication, Local Switching 섹션에 설명된 것과 동일한 컨피그레이션을 사용합니다.

WLC를 연결하는 WAN 링크가 다운되면 WLC는 H-REAP의 등록을 취소하는 프로세스를 거칩니다.

등록 취소가 완료되면 H-REAP는 독립형 모드로 전환됩니다.

이 WLAN을 통해 연결된 클라이언트는 여전히 연결을 유지합니다.그러나 컨트롤러는 사용할 수 없으므로 H-REAP에서는 이 WLAN에서 새 연결을 허용하지 않습니다.

이는 동일한 WLAN에서 다른 무선 클라이언트를 활성화하여 확인할 수 있습니다.이 클라이언트에 대한 인증이 실패하고 해당 클라이언트가 연결할 수 없음을 확인할 수 있습니다.

참고: WLAN 클라이언트 수가 0인 경우 H-REAP는 연결된 모든 802.11 기능을 중단하고 지정된 SSID에 대한 신호가 더 이상 표시되지 않습니다.이렇게 하면 WLAN이 다음 H-REAP 상태, **인증이 중단되고 스위치가 다운됩니다**.

로컬 인증, 로컬 스위칭

이 상태에서 H-REAP LAP는 클라이언트 인증을 처리하고 클라이언트 데이터 패킷을 로컬로 전환

합니다.이 상태는 독립형 모드에서만 유효하며 AP에서 로컬로 처리할 수 있으며 컨트롤러 프로세싱과 관련이 없는 인증 유형에만 유효합니다.

이전에 **중앙 인증, 로컬 스위칭** 상태에 있었던 H-REAP는 구성된 인증 유형을 AP에서 로컬로 처리할 수 있는 경우 이 상태로 전환됩니다.구성된 인증을 로컬로 처리할 수 없는 경우(예: 802.1x 인증, 독립형 모드) H-REAP은 **인증**을 **중지한 로컬 스위칭** 모드**로** 이동합니다.

다음은 독립형 모드의 AP에서 로컬로 처리할 수 있는 널리 사용되는 인증 메커니즘의 일부입니다.

- 열기
- 공유
- WPA-PSK
- WPA2-PSK

참고: AP가 연결 모드에 있을 때 WLC에서 모든 인증 프로세스를 처리합니다.H-REAP이 독립형 모드에 있는 동안 WPA/WPA2-PSK 인증이 모든 클라이언트 인증이 발생하는 LAP로 전송됩니다.

참고: WLAN에서 로컬 스위칭이 활성화된 하이브리드 REAP를 사용할 경우 외부 웹 인증이 지원되지 않습니다.

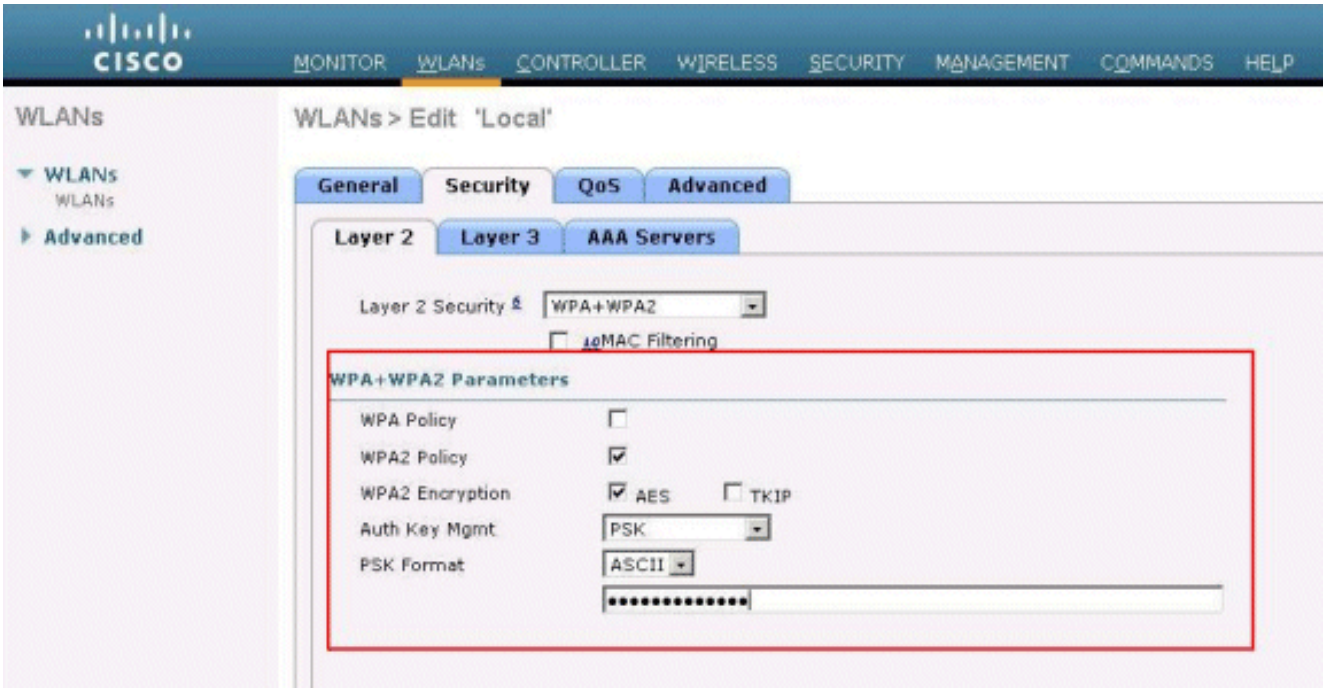
이 예에서는 다음 컨피그레이션 설정을 사용합니다.

- WLAN/SSID 이름:**로컬**
- 레이어 2 보안:**WPA-PSK**
- H-REAP 로컬 스위칭:**활성화됨**

컨트롤러 GUI에서 다음 단계를 완료합니다.

1. WLANs(**WLANs)**를 클릭하여 Local(로컬)이라는 새 WLAN을 생성한 다음 Apply(적용)를 **클릭합니다**.
2. 이 WLAN은 로컬 인증을 사용하므로 Layer 2 Security(레이어 2 보안) 필드에서 로컬로 처리할 수 있는 **WPA-PSK** 또는 언급된 보안 메커니즘을 선택합니다.이 예에서는 **WPA-PSK를 사용합니다**

   .

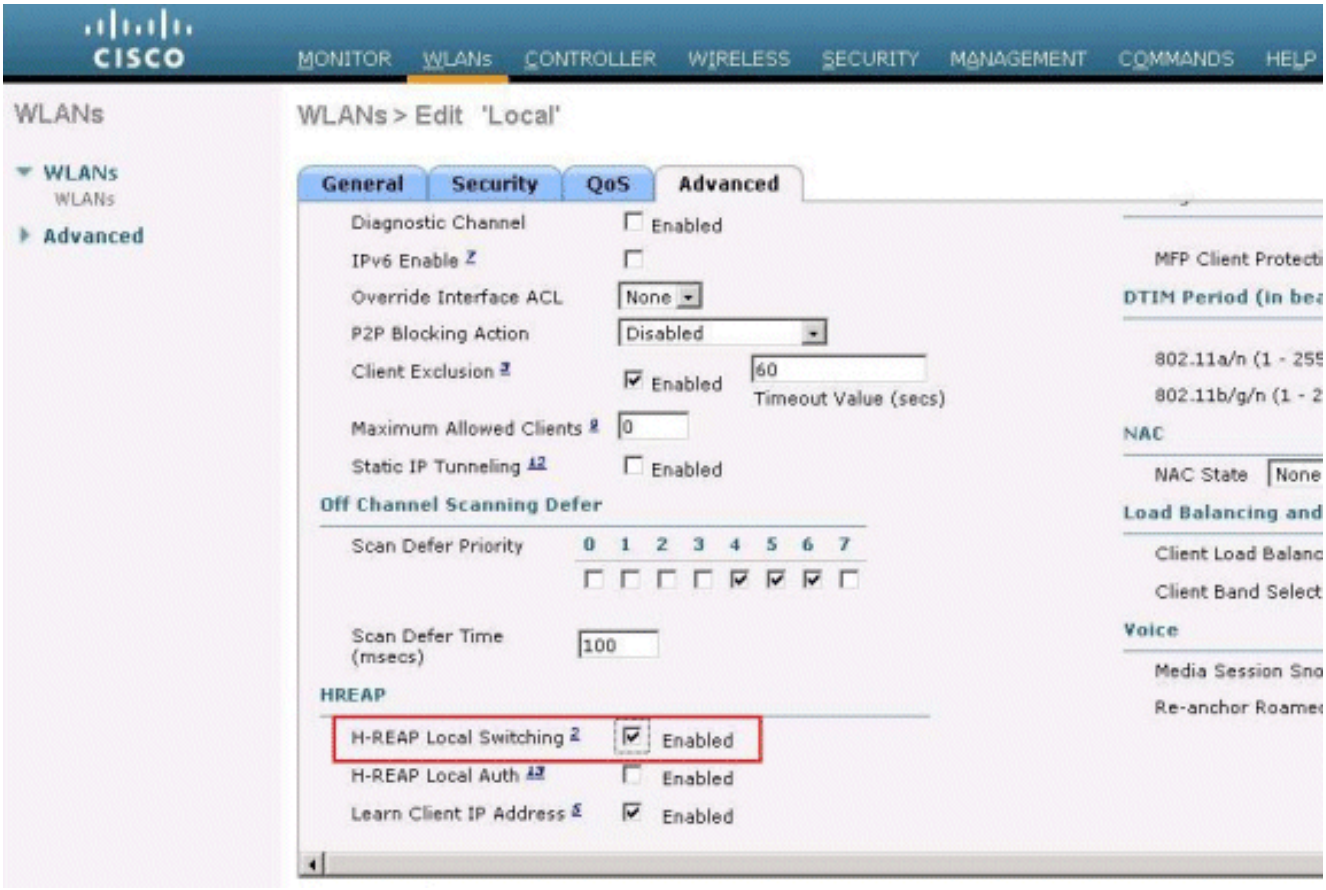


3. 선택한 후에는 사전 공유 키/암호 구문을 사용하도록 구성해야 합니다.인증이 성공하려면 클

라이언트 측에서 동일해야 합니다.

4. H-**REAP에서** 이 WLAN에 속한 클라이언트 트래픽을 로컬로 전환하려면 H-REAP Local Switching 확인란을 선택합니다

.



로컬 인증, 로컬 스위칭 확인

다음 단계를 완료하십시오.

1. 동일한 SSID 및 보안 컨피그레이션으로 클라이언트를 구성합니다.여기서 SSID는 *로컬이며* 보안 방법은 *WPA-PSK입니다*.
2. 클라이언트에서 로컬 SSID를 활성화합니다.클라이언트가 중앙에서 컨트롤러에서 인증되고 H-REAP와 연결됩니다.클라이언트 트래픽은 로컬로 전환하도록 구성됩니다.이제 H-REAP은 중앙 인증, 로컬 스위칭 상태에 있습니다.
3. 컨트롤러에 연결되는 WAN 링크를 비활성화합니다.컨트롤러는 평소처럼 등록 취소 프로세스를 거칩니다.H-REAP은 컨트롤러에서 등록 해제됩니다.등록 취소가 완료되면 H-REAP는 독립형 모드로 전환됩니다.그러나 이 WLAN에 속하는 클라이언트는 H-REAP과의 연결을 유지합니다.또한 여기서 인증 유형은 컨트롤러 없이 AP에서 로컬로 처리할 수 있으므로 H-REAP에서는 이 WLAN을 통해 새 무선 클라이언트의 연결을 허용합니다.
4. 이를 확인하려면 동일한 WLAN에서 다른 무선 클라이언트를 활성화합니다.클라이언트가 인증되고 성공적으로 연결되었음을 확인할 수 있습니다.

문제 해결

- H-REAP의 콘솔 포트에서 클라이언트 연결 문제를 추가로 해결하려면 다음 명령을 입력합니다

.

```
AP_CLI#show capwap reap association
```

- 컨트롤러에서 클라이언트 연결 문제를 추가로 해결하고 추가 디버깅 출력을 제한하려면 다음 명령을 사용합니다.
  AP_CLI#**debug mac addr**

- 클라이언트의 802.11 연결 문제를 디버깅하려면 다음 명령을 사용합니다.
  AP_CLI#**debug dot11 state enable**

- 다음 명령을 사용하여 클라이언트의 802.1X 인증 프로세스 및 오류를 디버깅합니다.
  AP_CLI#**debug dot1x events enable**

- 백엔드 컨트롤러/RADIUS 메시지는 다음 명령을 사용하여 디버깅될 수 있습니다.
  AP_CLI#**debug aaa events enable**

- 또는 클라이언트 **debug** 명령의 전체 작업을 활성화하려면 다음 명령을 사용합니다.
  AP_CLI#**debug client**

관련 정보

- 무선 LAN 컨트롤러 및 경량 액세스 포인트 기본 구성 예
- 무선 LAN 컨트롤러의 VLAN 컨피그레이션 예
- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 7.0
- Hybrid REAP 설계 및 구축 설명서
- H-REAP(Hybrid Remote Edge Access Point) 기본 문제 해결
- 경량 액세스 포인트에 대한 WLAN 컨트롤러 장애 조치 컨피그레이션 예
- 무선 제품 지원
- 기술 지원 및 문서 – Cisco Systems