

WLC(Wireless LAN Controller) 설계 및 기능에 대한 FAQ 검토

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[구성 요소 사용](#)

[표기 규칙](#)

[WLC 설계 FAQ](#)

[Q. WLC와 연결되도록 스위치를 설정하려면 어떻게 해야 하나요?](#)

[Q. AP\(액세스 포인트\)가 컨트롤러에 등록되면 WLAN 클라이언트와 주고받는 모든 네트워크 트래픽이 WLC\(Wireless LAN Controller\)를 통해 터널링됩니까?](#)

[Q. 원격 사무실에 LAP\(경량형 액세스 포인트\)를 설치하고 본사에 Cisco WLC\(Wireless LAN Controller\)를 설치할 수 있습니까? LWAPP/CAPWAP는 WAN을 통해 작동합니까?](#)

[Q. REAP 및 H-REAP 모드는 어떻게 작동합니까?](#)

[Q. REAP\(Remote-Edge AP\)와 H-REAP\(Hybrid-REAP\)의 차이점은 무엇입니까?](#)

[Q. WLC에서 지원되는 WLAN은 몇 개입니까?](#)

[Q. WLC\(Wireless LAN Controller\)에서 VLAN을 설정하려면 어떻게 해야 하나요?](#)

[Q. 서로 다른 두 개의 동적 인터페이스를 사용하여 두 개의 WLAN을 프로비저닝했습니다. 각 인터페이스에는 관리 인터페이스 VLAN과 다른 자체 VLAN이 있습니다. 작동하는 것 같지만, WLAN에서 사용하는 VLAN을 허용하도록 트렁크 포트를 프로비저닝하지 않았습니다. AP\(액세스 포인트\)가 관리 인터페이스 VLAN을 사용하여 패킷에 태그를 지정합니까?](#)

[Q. AAA 서버와의 인증에는 어떤 WLC의 IP 주소가 사용됩니까?](#)

[Q. 동일한 VLAN에 10개의 Cisco 1000 시리즈 LAP\(경량형 액세스 포인트\)와 2개의 WLC\(Wireless LAN Controller\)가 있습니다. WLC1에 연결할 6개의 LAP를 등록하고 WLC2에 연결할 다른 4개의 LAP를 등록하려면 어떻게 해야 하나요?](#)

[Q. 2100 시리즈 WLC\(Wireless LAN Controller\)에서 지원되지 않는 기능은 무엇입니까?](#)

[Q. 5500 시리즈 컨트롤러에서 지원되지 않는 기능은 무엇입니까?](#)

[Q. 메시 네트워크에서 지원되지 않는 기능은 무엇입니까?](#)

[Q. Wireless LAN Controller에 있는 MIC\(제조업체 설치 인증서\) 및 경량형 AP 인증서의 유효 기간은 어떻게 됩니까?](#)

[Q. 페일오버를 위해 동일한 모빌리티 그룹 내에 WLC1 및 WLC2라는 두 개의 WLC\(Wireless LAN Controller\)가 설정되어 있습니다. 내 LAP\(경량형 액세스 포인트\)가 현재 WLC1에 등록되어 있습니다. WLC1이 실패하면 WLC1에 등록된 AP가 남아 있는 WLC\(WLC2\)로 전환되는 동안 재부팅됩니까? 또한 이 페일오버 중에 WLAN 클라이언트와 LAP의 WLAN 연결성을 잃게 됩니까?](#)

[Q. 로밍은 WLC\(Wireless LAN Controller\)가 사용하도록 설정된 LWAPP\(Lightweight Access Point Protocol\) 모드에 따라 달라집니까? 레이어 2 LWAPP 모드에서 작동하는 WLC가 레이어 3 로밍을 수행할 수 있습니까?](#)

[Q. 클라이언트가 새 AP\(액세스 포인트\) 또는 컨트롤러로 로밍하기로 결정하면 어떤 로밍 프로세스가 발생합니까?](#)

[Q. 네트워크에 방화벽이 있는 경우 LWAPP/CAPWAP 통신에 대해 어떤 포트를 허용해야 하나요?](#)

[Q. Wireless LAN Controller가 SSHv1 및 SSHv2를 모두 지원합니까?](#)

[Q. RARP\(Reverse ARP\)는 WLC\(Wireless LAN Controller\)를 통해 지원됩니까?](#)

[Q. WLC\(Wireless LAN Controller\)의 내부 DHCP 서버를 사용하여 LAP\(경량형 액세스 포인트\)에 IP 주소를 할당할 수 있습니까?](#)

[Q. WLAN 아래의 DHCP 필수 필드는 무엇을 의미합니까?](#)

[Q. CCKM\(Cisco 중앙 집중식 키 관리\)은 LWAPP/CAPWAP 환경에서 어떻게 작동합니까?](#)

[Q. WLC\(Wireless LAN Controller\) 및 LAP\(경량형 액세스 포인트\)에서 듀플렉스 설정을 지정하려면 어떻게 해야 합니까?](#)

[Q. 컨트롤러에 등록되지 않은 LAP\(경량형 액세스 포인트\)의 이름을 추적할 수 있는 방법이 있습니까?](#)

[Q. 컨트롤러에서 512명의 사용자를 설정했습니다. WLC\(Wireless LAN Controller\)의 사용자 수를 늘릴 수 있는 방법이 있습니까?](#)

[Q. WLC에 강력한 비밀번호 정책을 시행하려면 어떻게 해야 합니까?](#)

[Q. Wireless LAN Controller에서 패시브 클라이언트 기능은 어떻게 사용됩니까?](#)

[Q. 3분마다 또는 지정된 기간에 RADIUS 서버에 재인증하도록 클라이언트를 설정하려면 어떻게 해야 합니까?](#)

[Q. 앵커 WLC 역할을 하는 4400 WLC\(Wireless LAN Controller\)와 여러 원격 WLC 사이에 게스트 터널링인 EoIP\(Ethernet over IP\) 터널이 설정되어 있습니다. 이 앵커 WLC는 EoIP 터널을 통해 서브넷 브로드캐스트를 유선 네트워크에서 원격 컨트롤러와 연결된 무선 클라이언트로 전달할 수 있습니까?](#)

[Q. WLC\(Wireless LAN Controller\) 및 LWAPP\(Lightweight Access Point Protocol\) 설정에서 음성 트래픽에 대해 전달되는 DSCP\(Differentiated Services Code Point\) 값은 무엇입니까? QoS는 WLC에서 어떻게 구현됩니까?](#)

[Q. Cisco Wireless Unified 솔루션에서 Linksys 이더넷 브리지가 지원됩니까?](#)

[Q. WLC\(Wireless LAN Controller\)에 설정 파일을 저장하려면 어떻게 해야 합니까?](#)

WLC 기능 FAQ

[Q. WLC\(Wireless LAN Controller\)에서 EAP\(Extensible Authentication Protocol\) 유형을 설정하려면 어떻게 해야 합니까? ACS\(Access Control Server\) 어플라이언스에 대해 인증하려고 하는데, 로그에 "지원되지 않는 EAP" 유형이라고 표시됩니다.](#)

[Q. 고속 SSID 변경이란 무엇입니까?](#)

[Q. 무선 LAN에 연결할 수 있는 클라이언트 수에 제한을 설정할 수 있습니까?](#)

[Q. PKC란 무엇이며 WLC\(Wireless LAN Controller\)에서 어떻게 작동합니까?](#)

[Q. 컨트롤러의 시간 초과 설정, 즉 ARP\(Address Resolution Protocol\) 시간 초과, 사용자 유휴 시간 제한, 세션 시간 초과 설정에 대한 설명은 무엇입니까?](#)

[Q. RFID 시스템이란 무엇입니까? 현재 시스코에서 지원하는 RFID 태그는 무엇입니까?](#)

[Q. WLC에서 로컬로 EAP 인증을 수행할 수 있습니까? 이 로컬 EAP 기능을 설명하는 문서가 있습니까?](#)

[Q. WLAN 재정의 기능이란 무엇입니까? 이 기능을 어떻게 설정합니까? LAP는 백업 WLC로 페일 오버할 때 WLAN 재정의 값을 유지합니까?](#)

[Q. Cisco WLC\(Wireless LAN Controller\) 및 LAP\(경량형 액세스 포인트\)에서 IPv6가 지원됩니까?](#)

[Q. Cisco 2000 시리즈 WLC\(Wireless LAN Controller\)는 게스트 사용자에 대해 웹 인증을 지원합니까?](#)

[Q. 무선 모드에서 WLC를 관리할 수 있습니까?](#)

[Q. LAG\(Link Aggregation\)란 무엇입니까? WLC\(Wireless LAN Controller\)에서 LAG를 활성화하려면 어떻게 해야 합니까?](#)

[Q. LAG\(Link Aggregation\)를 지원하는 WLC\(Wireless LAN Controller\) 모델은 무엇입니까?](#)

[Q. Unified Wireless Network의 자동 앵커 모빌리티 기능이란 무엇입니까?](#)

[Q. Cisco 2006 WLC\(Wireless LAN Controller\)를 WLAN의 앵커로 설정할 수 있습니까?](#)

[Q. Wireless LAN Controller는 어떤 유형의 모빌리티 터널링을 사용합니까?](#)

[Q. 네트워크가 다운된 경우 WLC에 액세스하려면 어떻게 해야 합니까?](#)

[Q. Cisco WLC\(Wireless LAN Controller\)는 페일오버\(또는 리더던시\) 기능을 지원합니까?](#)

[Q. WLC\(Wireless LAN Controller\)에서 사전 인증 ACL\(액세스 제어 목록\)의 용도는 무엇입니까?](#)

[Q. 네트워크에 MAC 필터링된 WLAN 및 완전 개방형 WLAN이 있습니다. 클라이언트가 기본적으로 개방형 WLAN을 선택합니까? 아니면 클라이언트가 MAC 필터에 설정된 WLAN ID와 자동으로 연결합니까? 또한 MAC 필터에 "인터페이스" 옵션이 있는 이유는 무엇입니까?](#)

[Q. WLC\(Wireless LAN Controller\)에서 관리 사용자에 대한 TACACS 인증을 설정하려면 어떻게 해야 합니까?](#)

[Q. WLC\(Wireless LAN Controller\)에서 과도한 인증 실패 설정의 용도는 무엇입니까?](#)

[Q. 자동 AP\(액세스 포인트\)를 경량형 모드로 변환했습니다. 클라이언트 계정 관리를 위해 AAA RADIUS 서버를 사용하는 LWAPP\(Lightweight AP Protocol\) 모드에서 일반적으로 클라이언트는 WLC의 IP 주소를 기반으로 RADIUS 계정 관리를 사용하여 추적됩니다. WLC의 IP 주소가 아니라 해당 WLC와 연결된 AP의 MAC 주소를 기반으로 RADIUS 계정 관리를 설정할 수 있습니까?](#)

[Q. CLI를 통해 WLC\(Wireless LAN Controller\)에서 WPA\(Wi-Fi Protected Access\) 핸드셰이크 시간 초과 값을 변경하려면 어떻게 해야 합니까? dot11 wpa handshake timeoutvalue 명령을 사용하여 Cisco IOS AP\(액세스 포인트\)에서 이 작업을 수행할 수 있지만, WLC에서는 이 작업을 어떻게 수행합니까?](#)

[Q. WLAN > Edit > Advanced 페이지에서 진단 채널 기능의 용도는 무엇입니까?](#)

[Q. WLC에서 설정할 수 있는 AP 그룹의 수는 최대 몇 개입니까?](#)

[관련 정보](#)

소개

SSHv1

이 문서에서는 Wireless LAN Controller 설계 및 기능에 대한 최신 정보를 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

구성 요소 사용

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

표기 규칙

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

WLC 설계 FAQ

Q. WLC와 연결되도록 스위치를 설정하려면 어떻게 해야 합니까?

A. WLC가 연결된 스위치 포트를 IEEE 802.1Q 트렁크 포트로 설정합니다. 필요한 VLAN만 스위치에서 허용되는지 확인합니다. 일반적으로 WLC의 관리 및 AP-Manager 인터페이스는 태그가 지정되지 않은 상태로 유지됩니다. 즉, 연결된 스위치의 기본 VLAN을 가정합니다. 이 작업은 필요하지 않습니다. 이러한 인터페이스에 별도의 VLAN을 할당할 수 있습니다. 자세한 내용은 [WLC의 스위치 설정](#)을 참조하십시오.

Q. 액세스 포인트(AP)가 컨트롤러에 등록되면 WLC(Wireless LAN Controller)를 통

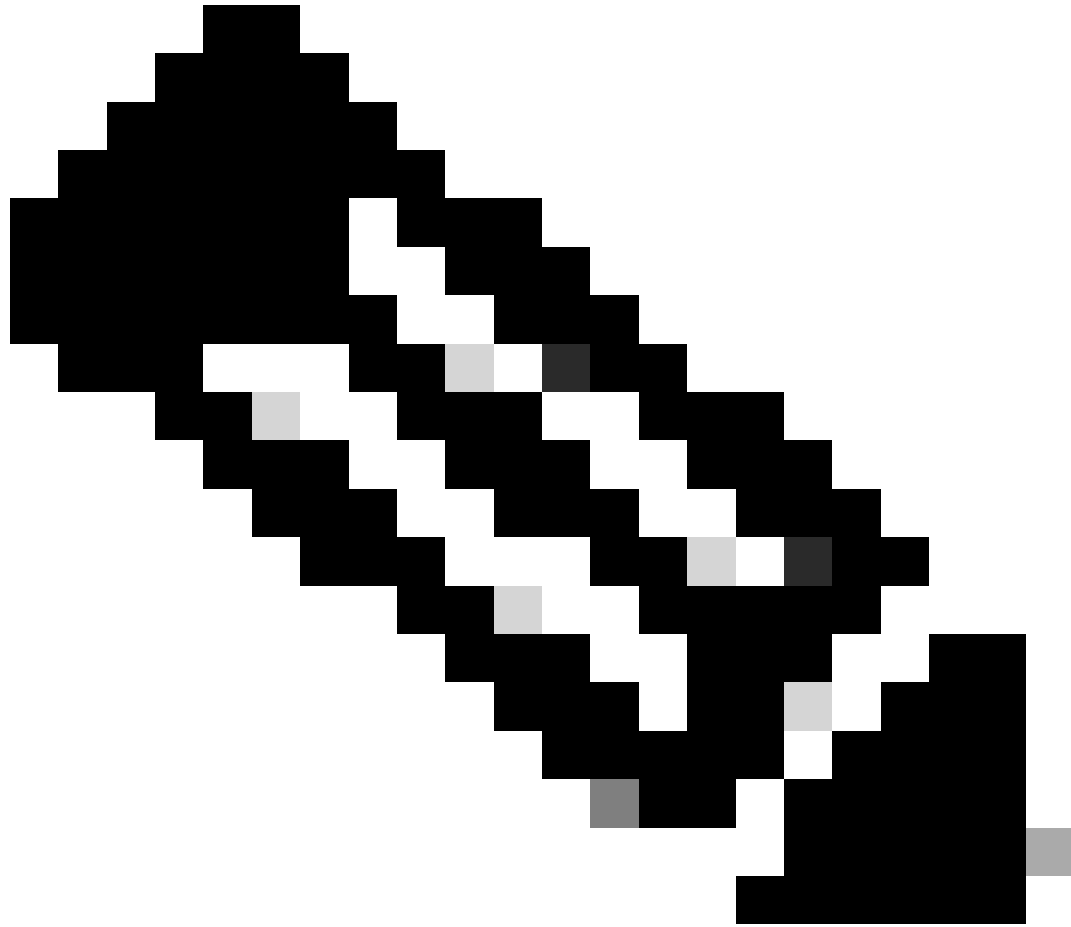
해 WLAN 클라이언트에서 나가고 들어오는 모든 네트워크 트래픽이 터널링됩니까?

A. AP가 WLC에 조인하면 두 디바이스 간에 CAPWAP(Control and Provisioning of Wireless Access Points) 프로토콜 터널이 형성됩니다. 모든 클라이언트 트래픽을 포함해 모든 트래픽은 CAPWAP 터널을 통해 전송됩니다.

유일한 예외는 AP가 Hybrid-REAP 모드인 경우입니다. Hybrid-REAP 액세스 포인트는 클라이언트 데이터 트래픽을 로컬로 전환하고, 컨트롤러에 대한 연결이 끊겼을 때 클라이언트 인증을 로컬로 수행할 수 있습니다. 컨트롤러에 연결되면 컨트롤러로 트래픽을 다시 전송할 수도 있습니다.

Q. 원격 사무실에 LAP(Lightweight Access Point)를 설치하고 본사에 Cisco WLC(Wireless LAN Controller)를 설치할 수 있습니까? LWAPP/CAPWAP는 WAN을 통해 작동합니까?

A. 예, AP에서 WAN을 통해 WLC를 사용할 수 있습니다. LWAPP/CAPWAP는 LAP가 REAP(Remote Edge AP) 또는 H-REAP(Hybrid Remote Edge AP) 모드에서 설정된 경우 WAN을 통해 작동합니다. 이러한 모드에서는 WAN 링크를 통해 연결된 원격 컨트롤러로 AP를 제어할 수 있습니다. 트래픽은 LAN 링크에 로컬로 브리지되므로 WAN 링크를 통해 불필요하게 로컬 트래픽을 전송할 필요가 없습니다. 이는 무선 네트워크에서 WLC를 사용할 때의 가장 큰 이점 중 하나입니다.



참고: 일부 경량형 AP는 이러한 모드를 지원하지 않습니다. 예를 들어 H-REAP 모드는 1131, 1140, 1242, 1250 및 AP801 LAP에서만 지원됩니다. REAP 모드는 1030 AP에서만 지원되며 1010 및 1020 AP는 REAP를 지원하지 않습니다. 이러한 모드를 구현하기 전에 LAP에서 이를 지원하는지 확인하십시오. LWAPP로 변환된 Cisco IOS® 소프트웨어 AP(자동 AP)는 REAP를 지원하지 않습니다.

Q. REAP 및 H-REAP 모드는 어떻게 작동합니까?

A. REAP 모드에서는 인증 트래픽을 포함하는 모든 제어 및 관리 트래픽이 WLC로 다시 터널링됩니다. 그러나 모든 데이터 트래픽은 원격 사무실 LAN 내에서 로컬로 전환됩니다. WLC에 대한 연결이 끊어지면 첫 번째 WLAN(WLAN1)을 제외한 모든 WLAN이 종료됩니다. 현재 이 WLAN에 연결된 모든 클라이언트가 유지됩니다. 새 클라이언트가 다운타임 내에 이 WLAN에서 서비스를 성공적으로 인증하고 수신할 수 있도록 하려면 인증이 REAP에서 로컬로 수행되도록 이 WLAN에 대한 인증 방법을 WEP 또는 WPA-PSK로 설정합니다. REAP 구축에 대한 자세한 내용은 [브랜치 오피스에서의 REAP 구축 가이드](#)를 참조하십시오.

H-REAP 모드에서 액세스 포인트는 인증 트래픽을 포함하는 제어 및 관리 트래픽을 다시 WLC로

터널링합니다. WLAN의 데이터 트래픽은 WLAN이 H-REAP 로컬 스위칭으로 설정되거나 데이터 트래픽이 WLC로 다시 전송되는 경우 원격 사무실에서 로컬로 브리지됩니다. WLC에 대한 연결이 끊어지면 H-REAP 로컬 스위칭으로 설정된 처음 8개의 WLAN을 제외하고 모든 WLAN이 종료됩니다. 현재 이 WLAN에 연결된 모든 클라이언트가 유지됩니다. 새 클라이언트가 다운타임 내에 이러한 WLAN에서 성공적으로 인증하고 서비스를 받을 수 있도록 하려면 H-REAP에서 인증이 로컬로 수행되도록 이 WLAN에 대한 인증 방법을 WEP, WPA PSK 또는 WPA2 PSK로 설정합니다.

H-REAP에 대한 자세한 내용은 [FlexConnect 무선 브랜치 컨트롤러 구축 가이드](#)를 참조하십시오.

Q. REAP(Remote-Edge AP)와 H-REAP(Hybrid-REAP)의 차이점은 무엇입니까?

A. REAP는 IEEE 802.1Q VLAN 태깅을 지원하지 않습니다. 따라서 여러 VLAN을 지원하지 않습니다. 모든 SSID(Service Set Identifier)의 트래픽은 동일한 서브넷에서 종료되지만 H-REAP는 IEEE 802.1Q VLAN 태깅을 지원합니다. 각 SSID의 트래픽은 고유한 VLAN으로 세분화될 수 있습니다.

독립형 모드에서 WLC에 대한 연결성이 끊어지면 REAP는 하나의 WLAN, 즉 첫 번째 WLAN만 제공합니다. 다른 모든 WLAN은 비활성화됩니다. H-REAP에서는 다운타임 내에 최대 8개의 WLAN이 지원됩니다.

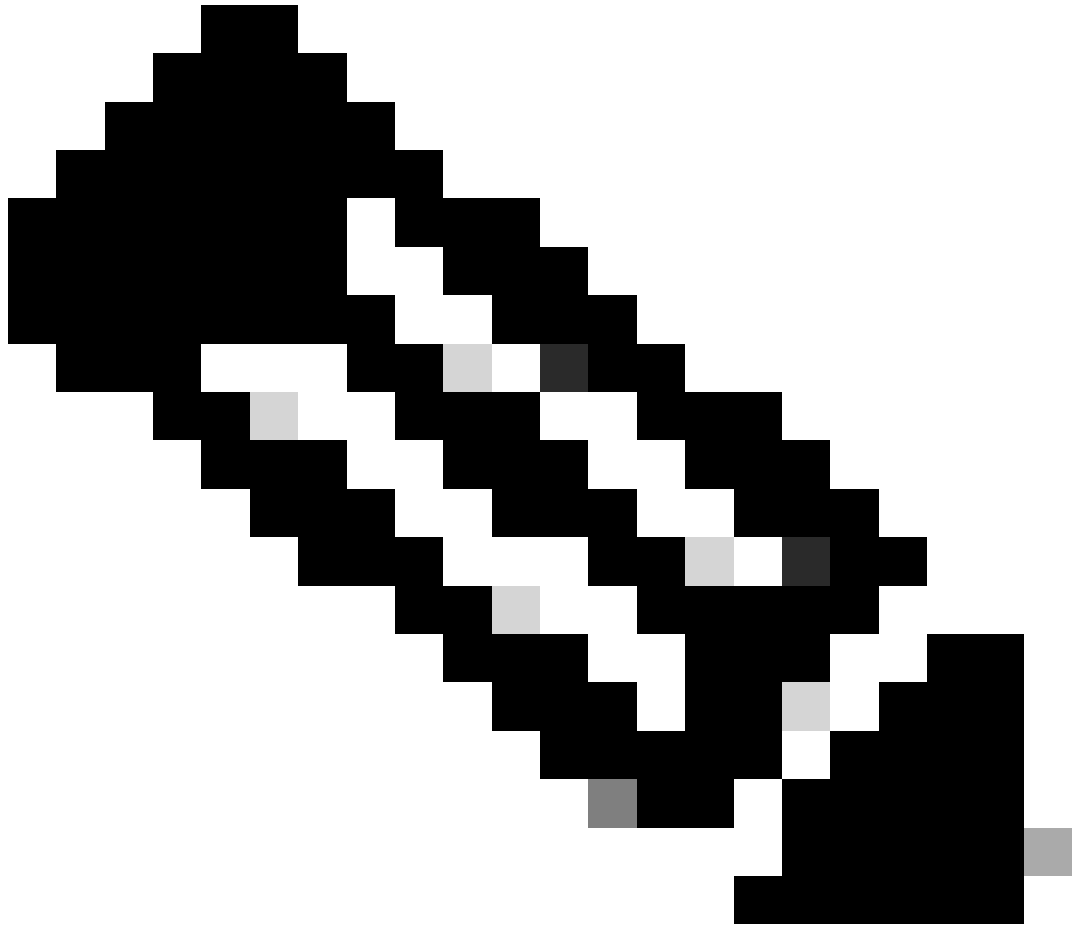
또 다른 주요 차이점은 REAP 모드에서 데이터 트래픽은 로컬로만 브리지될 수 있다는 것입니다. 이는 중앙 사무실로 다시 전환할 수 없지만 H-REAP 모드에서는 트래픽을 다시 중앙 사무실로 전환할 수 있는 옵션이 있습니다. H-REAP 로컬 스위칭으로 설정된 WLAN의 트래픽은 로컬로 전환됩니다. 다른 WLAN의 데이터 트래픽은 중앙 사무실로 다시 전환됩니다.

REAP에 관한 자세한 내용은 [경량형 AP 및 WLC\(Wireless LAN Controller\)를 사용하는 REAP\(Remote-Edge AP\) 설정 예시](#)를 참조하십시오.

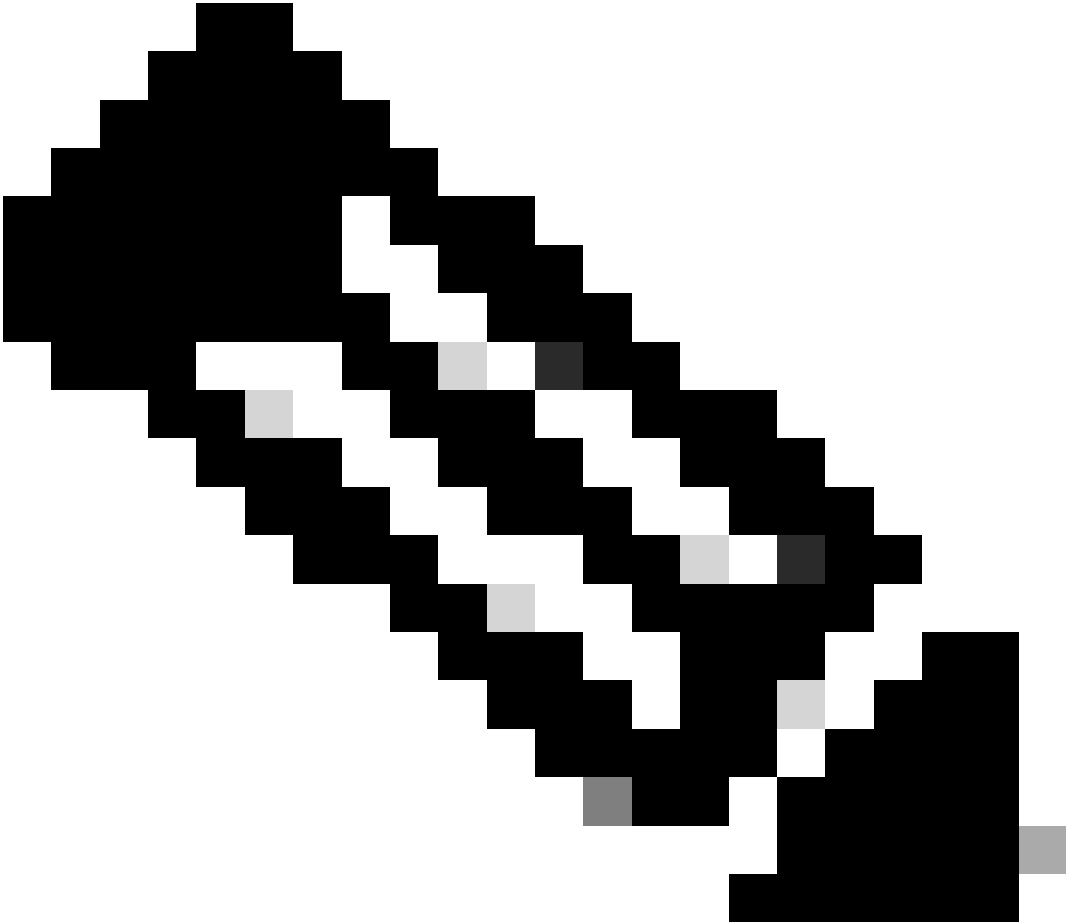
H-REAP에 관한 자세한 내용은 Hybrid REAP 설정을 참조하십시오.

Q. WLC에서 지원되는 WLAN은 몇 개입니까?

A. 소프트웨어 버전 5.2.157.0부터 WLC는 이제 경량형 액세스 포인트에 대해 최대 512개의 WLAN을 제어할 수 있습니다. 각 WLAN에는 별도의 WLAN ID(1~512), 별도의 프로파일 이름 및 WLAN SSID가 있으며 고유한 보안 정책을 할당할 수 있습니다. 컨트롤러는 연결된 각 액세스 포인트에 최대 16개의 WLAN을 게시하지만, 사용자는 컨트롤러에서 최대 512개의 WLAN을 생성한 다음 이러한 WLAN을 (액세스 포인트 그룹을 사용하여) 선택적으로 다른 액세스 포인트에 게시하여 무선 네트워크를 보다 효율적으로 관리할 수 있습니다.



참고: Cisco 2106, 2112 및 2125 컨트롤러는 최대 16개의 WLAN만 지원합니다.



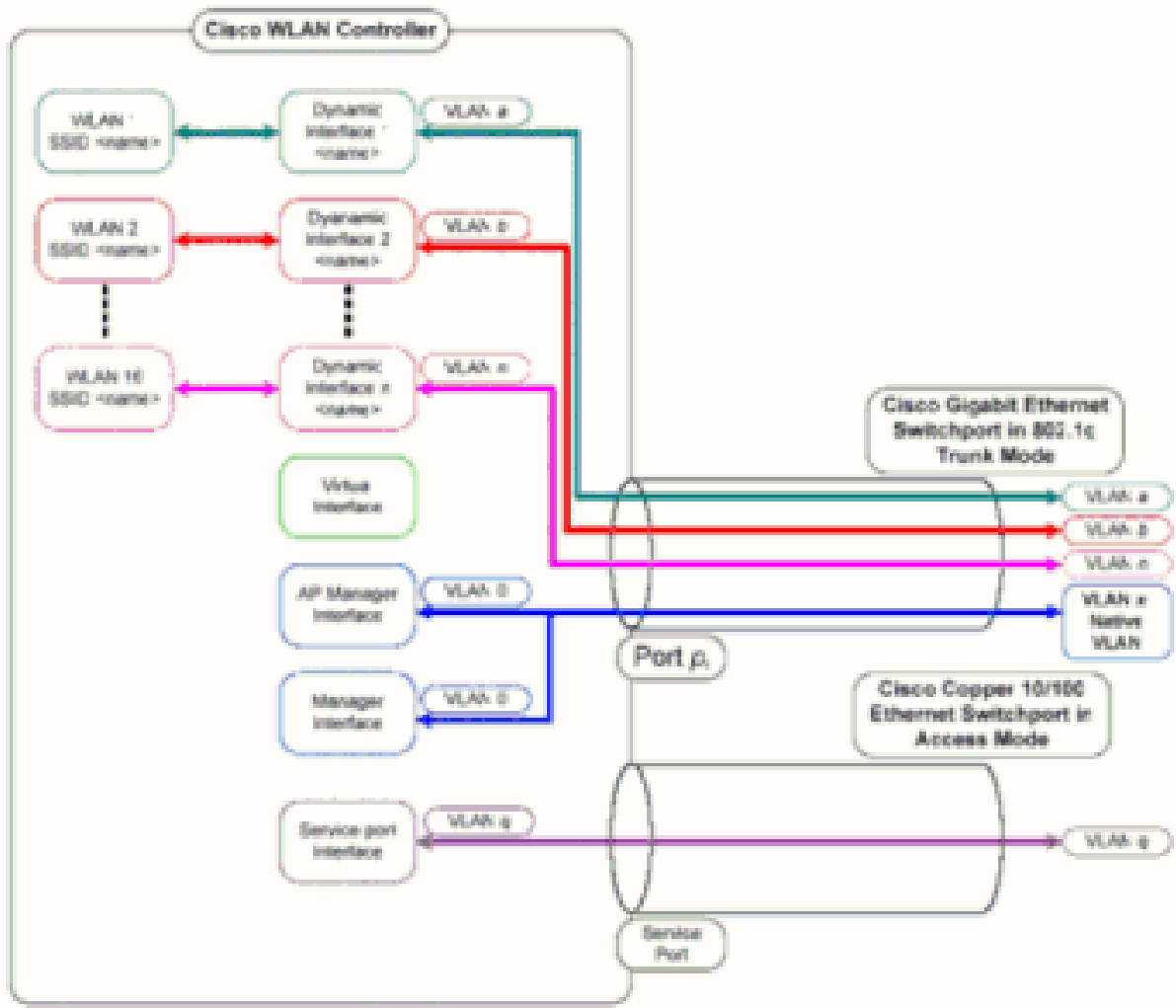
참고: WLC에서 WLAN을 설정하기 위한 지침에 대한 자세한 내용은 Cisco Wireless LAN Controller 설정 가이드, 릴리스 7.0.116.0의 WLAN 생성 섹션을 참조하십시오.

Q. WLC(Wireless LAN Controller)에서 VLAN을 구성하려면 어떻게 해야 합니까?

A.WLC에서 VLAN은 고유한 IP 서브넷에 설정된 인터페이스에 연결됩니다. 이 인터페이스는 WLAN에 매핑됩니다. 그러면 이 WLAN에 연결된 클라이언트는 인터페이스의 VLAN에 속하며 인터페이스가 속한 서브넷의 IP 주소를 할당받습니다. WLC에서 VLAN을 설정하려면 [Wireless LAN Controller의 VLAN 설정 예시](#)의 절차를 완료합니다.

Q. 두 개의 서로 다른 동적 인터페이스로 두 개의 WLAN을 프로비저닝했습니다. 각 인터페이스에는 관리 인터페이스 VLAN과 다른 자체 VLAN이 있습니다. 작동하는 것 같지만, WLAN에서 사용하는 VLAN을 허용하도록 트렁크 포트를 프로비저닝하지 않았습니다. AP(액세스 포인트)가 관리 인터페이스 VLAN을 사용하여 패킷에 태그를 지정합니까?

A.AP는 관리 인터페이스 VLAN을 사용하여 패킷에 태그를 지정하지 않습니다. AP는 클라이언트의 패킷을 LWAPP(Lightweight AP Protocol)/CAPWAP로 캡슐화한 다음 WLC로 전달합니다. 그런 다음 WLC는 LWAPP/CAPWAP 헤더를 제거하고 적절한 VLAN 태그를 사용하여 게이트웨이에 패킷을 전달합니다. VLAN 태그는 클라이언트가 속한 WLAN에 따라 달라집니다. WLC는 패킷을 대상으로 라우팅하는 게이트웨이에 따라 달라집니다. 여러 VLAN에 대한 트래픽을 전달할 수 있으려면 업 링크 스위치를 트렁크 포트로 설정해야 합니다. 이 다이어그램은 VLAN이 컨트롤러에서 작동하는 방식을 설명합니다.



Q. AAA 서버와의 인증에 어떤 WLC의 IP 주소를 사용합니까?

A.WLC는 AAA 서버와 관련된 모든 인증 메커니즘(레이어 2 또는 레이어 3)에 관리 인터페이스의 IP 주소를 사용합니다. WLC의 포트 및 인터페이스에 대한 자세한 내용은 Cisco Wireless LAN Controller 설정 가이드, 릴리스 7.0.116.0의 포트 및 인터페이스 설정 섹션을 참조하십시오.

Q. 동일한 VLAN에 Cisco 1000 Series LAP(Lightweight Access Point) 10개와 WLC(Wireless LAN Controller) 2개가 있습니다. WLC1에 연결할 6개의 LAP를 등록하고 WLC2에 연결할 다른 4개의 LAP를 등록하려면 어떻게 해야 합니까?

A. LWAPP/CAPWAP는 유동 리던던시 및 로드 밸런싱을 허용합니다. 예를 들어 옵션 43에 대해 들

이상의 IP 주소를 지정하는 경우, LAP는 AP가 수신하는 각 IP 주소로 LWAPP/CAPWAP 검색 요청을 전송합니다. WLC LWAPP/CAPWAP 검색 응답에서 WLC는 다음 정보를 포함합니다.

- 해당 시점에 WLC에 조인된 LAP 수로 정의되는 현재 LAP 로드 관련 정보
- LAP 용량
- WLC에 연결된 무선 클라이언트의 수

이후 LAP는 로드가 가장 적은 WLC, 즉 사용 가능한 LAP 용량이 가장 많은 WLC에 조인하려고 시도합니다. 또한 LAP가 WLC에 조인한 후 LAP는 조인된 WLC에서 모빌리티 그룹에 있는 다른 WLC의 IP 주소를 파악합니다.

LAP가 WLC에 조인하면 다음 재부팅 시 LAP가 특정 WLC에 조인하도록 할 수 있습니다. 이렇게 하려면 LAP에 대해 기본, 보조 및 3차 WLC를 할당합니다. LAP가 재부팅되면 기본 WLC를 찾아 해당 WLC의 로드와 무관하게 해당 WLC에 조인합니다. 기본 WLC가 응답하지 않으면 보조 WLC를 찾고, 응답이 없으면 3차 WLC를 찾습니다. LAP에 대해 기본 WLC를 설정하는 방법에 대한 자세한 내용은

섹션을 참조하십시오.

Q. 2100 Series WLC(Wireless LAN Controller)에서 지원되지 않는 기능은 무엇입니까?

A. 이러한 하드웨어 기능은 2100 시리즈 컨트롤러에서 지원되지 않습니다.

- 서비스 포트(별도의 대역 외 관리 10/100Mb/s 이더넷 인터페이스)

이러한 소프트웨어 기능은 2100 시리즈 컨트롤러에서 지원되지 않습니다.

- VPN 종단(예: IPsec 및 L2TP)
- 게스트 컨트롤러 터널 종단(게스트 컨트롤러 터널의 시작은 지원됨)
- 외부 웹 인증 웹 서버 목록
- 레이어 2 LWAPP
- 스페닝 트리
- 포트 미러링
- Cranite
- Fortress
- AppleTalk
- QoS 사용자별 대역폭 계약
- IPv6 패스스루

- LAG(Link Aggregation)
- 멀티캐스트 유니캐스트 모드
- 유선 게스트 액세스

Q. 5500 Series 컨트롤러에서 지원되지 않는 기능은 무엇입니까?

A. 이러한 소프트웨어 기능은 5500 시리즈 컨트롤러에서 지원되지 않습니다.

- 정적 AP-manager 인터페이스

참고: 5500 시리즈 컨트롤러의 경우 AP-manager 인터페이스를 설정할 필요가 없습니다. 관리 인터페이스는 기본적으로 AP-manager 인터페이스 역할을 하며 액세스 포인트가 이 인터페이스에 조인할 수 있습니다.

- 비대칭 모빌리티 터널링
- STP(Spanning Tree Protocol)
- 포트 미러링
- 레이어 2 ACL(액세스 제어 목록) 지원
- VPN 종단(예: IPSec 및 L2TP)
- VPN 패스스루 옵션
- 802.3 브리징, AppleTalk 및 PPPoE(Point-to-Point Protocol over Ethernet)의 설정

Q. 메시 네트워크에서 지원되지 않는 기능은 무엇입니까?

A. 다음 컨트롤러 기능은 메시 네트워크에서 지원되지 않습니다.

- 다국가 지원
- 로드 기반 CAC(메시 네트워크는 대역폭 기반 또는 정적 CAC만 지원).
- 고가용성(빠른 하트비트 및 기본 검색 조인 타이머)
- EAP-FASTv1 및 802.1X 인증
- 액세스 포인트 조인 우선순위(메시 액세스 포인트는 우선순위가 고정되어 있음)
- LSC(Locally Significant Certificate)
- 위치 기반 서비스

Q. 무선 LAN 컨트롤러에 설치된 제조업체 MIC(Installed Certificates)와 경량 AP 인증서의 유효 기간은 어떻게 됩니까?

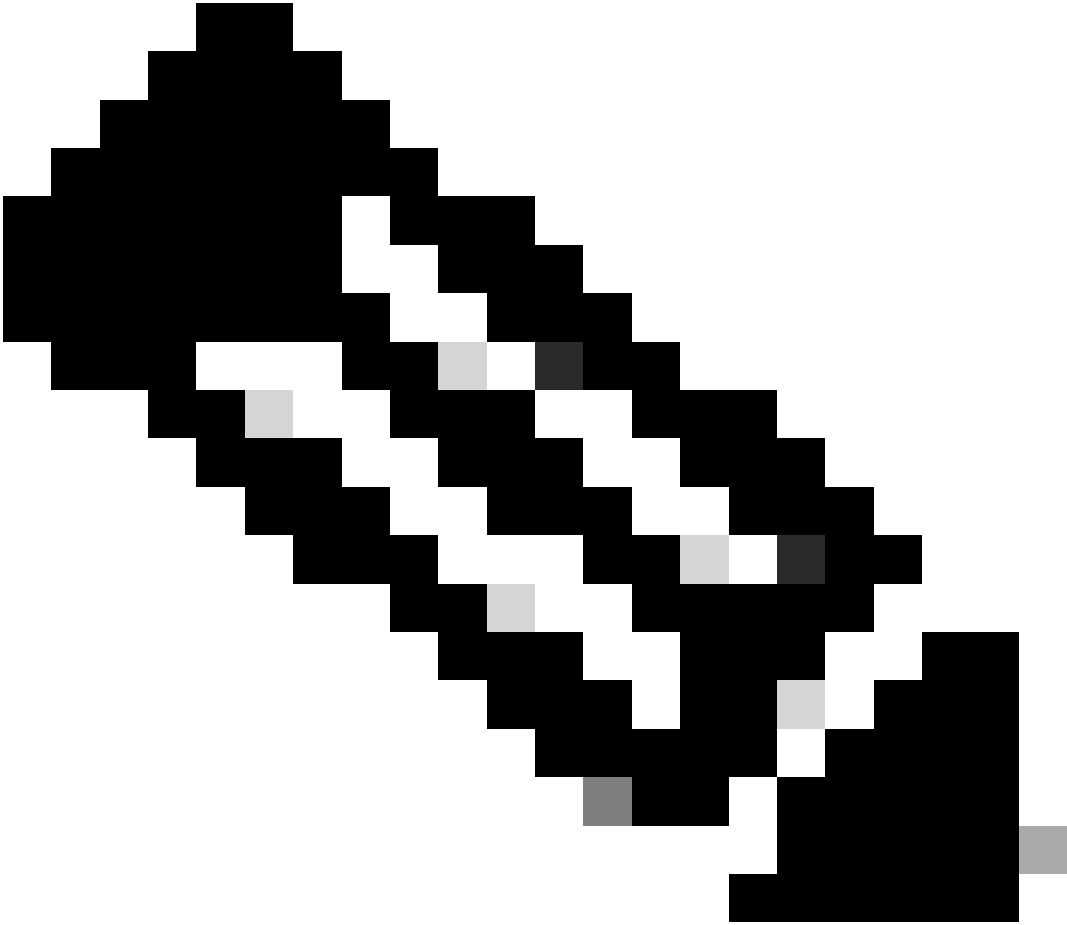
A.WLC에서 MIC의 유효 기간은 10년입니다. 생성 시점부터 경량형 AP의 인증서에는 10년의 동일한 유효 기간이 적용됩니다(MIC인지 또는 SSC(자체 서명 인증서)인지에 상관없음).

Q. 장애 조치를 위해 동일한 모빌리티 그룹 내에 WLC1 및 WLC2라는 두 개의 WLC(Wireless LAN Controller)가 구성되어 있습니다. 내 LAP(경량형 액세스 포인트)가 현재 WLC1에 등록되어 있습니다. WLC1이 실패하면 WLC1에 등록된 AP가 남아 있는 WLC(WLC2)로 전환되는 동안 재부팅됩니까? 또한 이 페일오버 중에 WLAN 클라이언트와 LAP의 WLAN 연결성을 잃게 됩니까?

A. 예. WLC1이 실패하면 LAP가 WLC1에서 등록 취소되고 재부팅된 다음 WLC2에 다시 등록됩니다. LAP가 재부팅되므로 연결된 WLAN 클라이언트와 재부팅 중인 LAP과의 연결성을 잃게 됩니다. 관련 정보는 [Unified Wireless Network의 AP 로드 밸런싱 및 AP 대체 시스템](#)을 참조하십시오.

Q. 로밍은 WLC(Wireless LAN Controller)에서 사용하도록 구성된 LWAPP(Lightweight Access Point Protocol) 모드에 종속됩니까? 레이어 2 LWAPP 모드에서 작동하는 WLC가 레이어 3 로밍을 수행할 수 있습니까?

A. 컨트롤러의 모빌리티 그룹이 올바르게 설정되어 있으면 클라이언트 로밍이 정상적으로 작동합니다. 로밍은 LWAPP 모드(레이어 2 또는 레이어 3)의 영향을 받지 않습니다. 그러나 가능한 경우 레이어 3 LWAPP를 사용하는 것이 좋습니다.



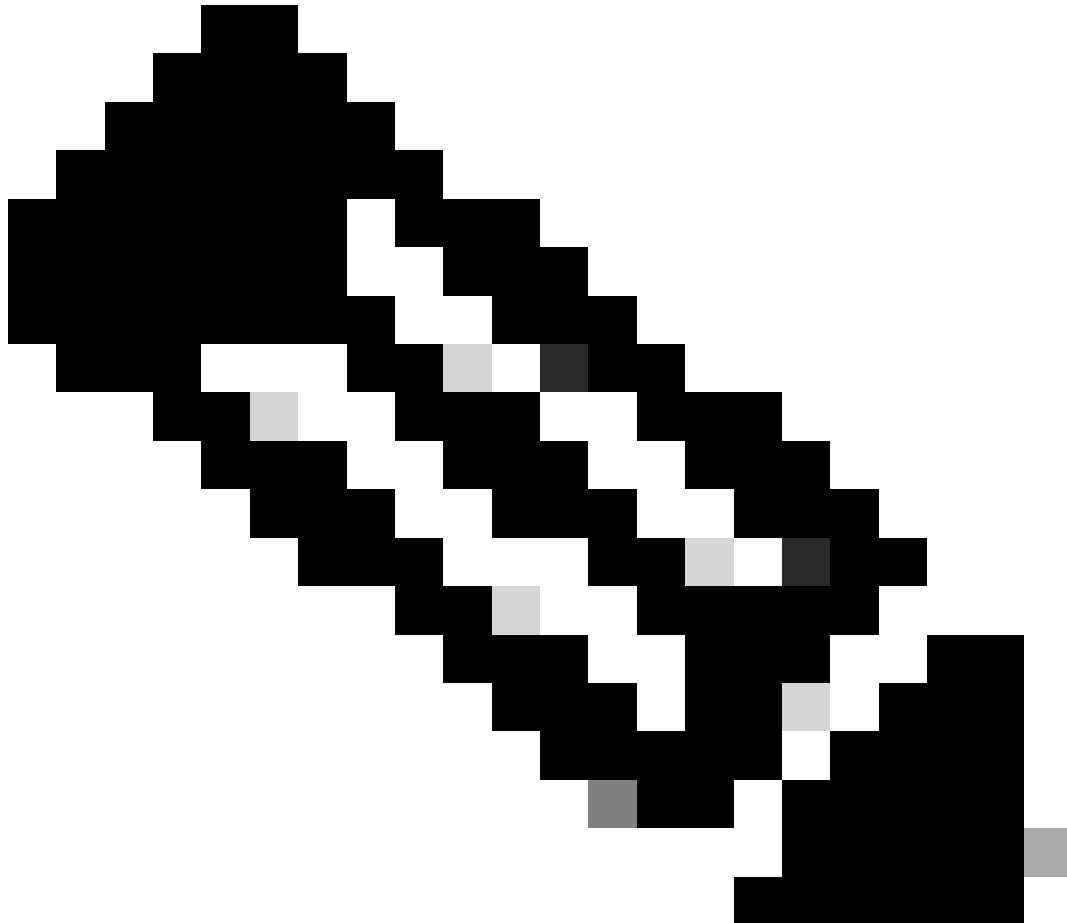
참고: 레이어 2 모드는 WLC의 Cisco 410x 및 440x 시리즈와 Cisco 1000 시리즈 액세스 포인트에서만 지원됩니다. 레이어 2 LWAPP는 기타 Wireless LAN Controller 및 경량형 액세스 포인트 플랫폼에서 지원되지 않습니다.

Q. 클라이언트가 새 액세스 포인트(AP) 또는 컨트롤러로 로밍하기로 결정할 때 발생하는 로밍 프로세스는 무엇입니까?

A. 다음은 클라이언트가 새 AP로 로밍할 때 발생하는 이벤트 순서입니다.

1. 클라이언트는 LAP를 통해 WLC에 재연결 요청을 보냅니다.
2. WLC는 클라이언트가 이전에 연결되었던 WLC를 확인하기 위해 모빌리티 그룹의 다른 WLC에 모빌리티 메시지를 전송합니다.
3. 기존 WLC는 모빌리티 메시지를 통해 클라이언트에 대한 MAC 주소, IP 주소, QoS, 보안 컨텍스트 등의 정보를 사용하여 응답합니다.

4. WLC는 제공된 클라이언트 세부 정보로 데이터베이스를 업데이트합니다. 그런 다음 필요한 경우 클라이언트는 재인증 프로세스를 거칩니다. 클라이언트가 현재 연결되어 있는 새 LAP도 WLC 데이터베이스의 다른 세부 정보와 함께 업데이트됩니다. 이렇게 하면 클라이언트 IP 주소가 WLC 사이의 로밍 간에 유지되므로 원활한 로밍을 제공하는 데 도움이 됩니다.
-



참고: 무선 클라이언트는 재연결 중에 (802.11) 인증 요청을 전송하지 않습니다. 무선 클라이언트는 재연결을 즉시 전송합니다. 그런 다음 802.1x 인증을 거칠 수 있습니다.

Q. 네트워크에 방화벽이 있을 때 LWAPP/CAPWAP 통신을 위해 어떤 포트를 허용해야 합니까?

A. 다음 포트를 활성화해야 합니다.

- LWAPP 트래픽에 대해 다음 UDP 포트를 활성화합니다.
 - 데이터 - 12222

- 제어 - 12223
- CAPWAP 트래픽에 대해 다음 UDP 포트를 활성화합니다.
 - 데이터 - 5247
 - 제어 - 5246
- 모빌리티 트래픽에 대해 다음 UDP 포트를 활성화합니다.
 - 16666 - 보안 모드
 - 16667 - 비보안 모드

모빌리티 및 데이터 메시지는 일반적으로 EtherIP 패킷을 통해 교환됩니다. EtherIP 패킷을 허용하려면 방화벽에서 IP 프로토콜 97을 허용해야 합니다. ESP를 사용하여 모빌리티 패킷을 캡슐화하는 경우 UDP 포트 500을 열 때 방화벽을 통해 ISAKMP를 허용해야 합니다. 또한 암호화된 데이터가 방화벽을 통과하도록 허용하려면 IP 프로토콜 50을 열어야 합니다.

이러한 포트는 선택 사항입니다(요구 사항에 따라 다름).

- SNMP용 TCP 161 및 162(WCS(Wireless Control System)용)
- TFTP용 UDP 69
- HTTP용 TCP 80 및/또는 443 또는 GUI 액세스용 HTTPS
- Telnet용 TCP 23 및/또는 22 또는 CLI 액세스용 SSH(Secure Shell)

Q. Wireless LAN Controller는 SSHv1 및 SSHv2를 모두 지원합니까?

A. Wireless LAN Controller는 SSHv2만 지원합니다.

Q. RARP(Reverse ARP)는 WLC(Wireless LAN Controller)를 통해 지원됩니까?

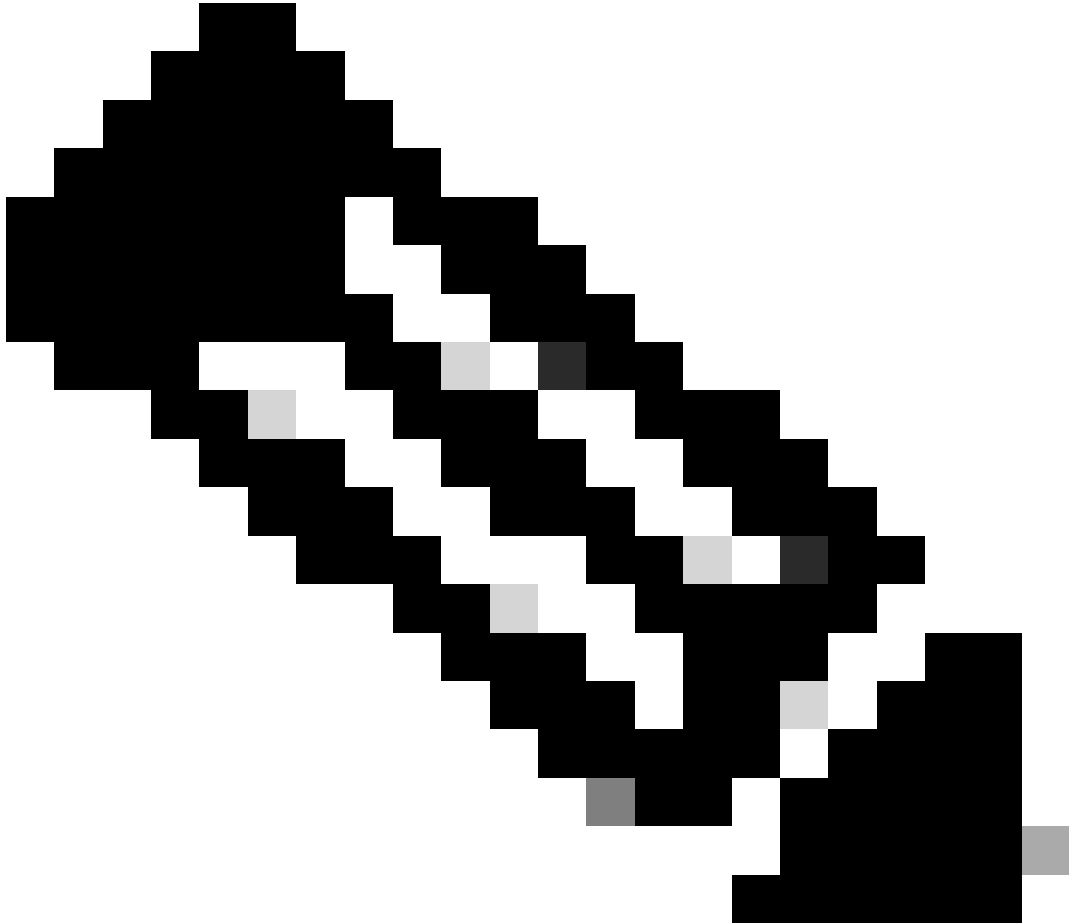
A. RARP(Reverse Address Resolution Protocol)는 이더넷 주소와 같은 지정된 링크 레이어 주소에 대한 IP 주소를 가져오는 데 사용되는 링크 레이어 프로토콜입니다. RARP는 펌웨어 버전이 4.0.217.0 이상인 WLC에서 지원됩니다. 그 이전 버전에서는 지원되지 않습니다.

Q. WLC(Wireless LAN Controller)에서 내부 DHCP 서버를 사용하여 LAP(Lightweight Access Point)에 IP 주소를 할당할 수 있습니까?

A. 컨트롤러에는 내부 DHCP 서버가 포함되어 있습니다. 이 서버는 일반적으로 아직 DHCP 서버가 없는 브랜치 오피스에서 사용됩니다. DHCP 서비스에 액세스하려면 WLC GUI에서 컨트롤러 메뉴를 클릭합니다. 그런 다음 페이지 왼쪽에서 내부 DHCP 서버 옵션을 클릭합니다. WLC에서 DHCP 범위를 설정하는 방법에 대한 자세한 내용은 Cisco Wireless LAN Controller 설정 가이드, 릴리스 7.0.116.0의 DHCP 설정 섹션을 참조하십시오.

내부 서버는 무선 클라이언트, LAP, 관리 인터페이스의 어플라이언스 모드 AP 및 LAP에서 릴레이

되는 DHCP 요청에 DHCP 주소를 제공합니다. WLC는 유선 네트워크의 디바이스 업스트림에 주소를 제공하지 않습니다. DHCP 옵션 43은 내부 서버에서 지원되지 않으므로 AP는 로컬 서브넷 브로드캐스트, DNS, 초기화 또는 OTA(Over-the-Air) 검색과 같은 대체 방법을 사용하여 컨트롤러의 관리 인터페이스 IP 주소를 찾아야 합니다.



참고: WLC 펌웨어 4.0 이전 버전은 LAP가 WLC에 직접 연결되어 있지 않은 경우 LAP에 대한 DHCP 서비스를 지원하지 않습니다. 내부 DHCP 서버 기능은 무선 LAN 네트워크에 연결하는 클라이언트에 IP 주소를 제공하는 데만 사용되었습니다.

Q. WLAN 아래의 DHCP Required(DHCP 필수) 필드는 무엇을 의미합니까?

A.DHCP 필수는 WLAN에 대해 활성화할 수 있는 옵션입니다. 이를 위해서는 특정 WLAN에 연결된 모든 클라이언트가 DHCP를 통해 IP 주소를 가져와야 합니다. 정적 IP 주소를 사용하는 클라이언트는 WLAN에 연결할 수 없습니다. 이 옵션은 WLAN의 고급 탭에 있습니다. WLC는 해당 IP 주소가 WLC의 MSCB 테이블에 있는 경우에만 클라이언트와 주고받는 트래픽을 허용합니다. WLC는 DHCP 요청 또는 DHCP 갱신 중에 클라이언트의 IP 주소를 기록합니다. 이렇게 하려면 클라이언트가 WLC에 다시 연결할 때마다 IP 주소를 갱신해야 합니다. 클라이언트가 로밍 프로세스 또는 세션

시간 초과로 일부로 연결을 해제할 때마다 MSCB 테이블에서 해당 항목이 지워지기 때문입니다. 클라이언트는 다시 인증하고 WLC에 다시 연결해야 합니다. 그러면 테이블에 클라이언트 항목이 다시 생성됩니다.

Q. CCKM(Cisco Centralized Key Management)은 LWAPP/CAPWAP 환경에서 어떻게 작동합니까?

A. 초기 클라이언트 연결 중에 AP 또는 WLC는 무선 클라이언트가 802.1x 인증을 통과한 후 PMK(Pair-wise Primary Key)를 협상합니다. WLC 또는 WDS AP는 각 클라이언트에 대해 PMK를 캐시합니다. 무선 클라이언트는 다시 연결하거나 로밍할 때 802.1x 인증을 건너뛰고 PMK를 즉시 검증합니다.

CCKM에서 WLC의 유일한 특수 구현은 WLC가 UDP 16666과 같은 모빌리티 패킷을 통해 클라이언트 PMK를 교환하는 것입니다.

Q. WLC(Wireless LAN Controller) 및 LAP(Lightweight Access Point)에서 듀플렉스 설정을 어떻게 설정합니까?

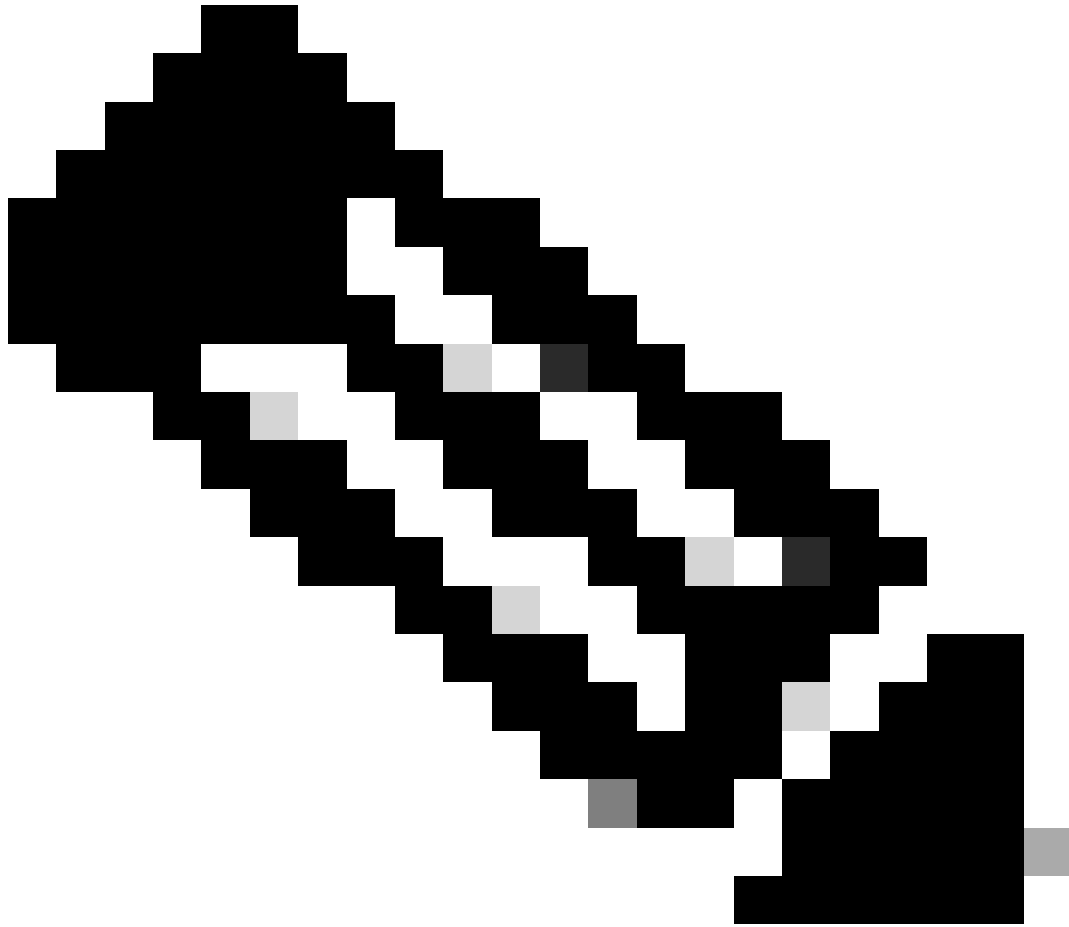
A. Cisco Wireless 제품은 속도 및 듀플렉스 모두 자동 협상될 때 가장 잘 작동하지만 WLC 및 LAP에서 듀플렉스 설정을 지정할 수 있는 옵션이 있습니다. AP 속도/듀플렉스 설정을 설정하려면 컨트롤러에서 LAP의 듀플렉스 설정을 설정한 다음 LAP에 푸시할 수 있습니다.

```
configure ap ethernet duplex <auto/half/full> speed <auto/10/100/1000> <all/Cisco AP Name>
```

이 명령은 CLI를 통해 듀플렉스 설정을 지정하는 명령으로 4.1 이상 버전에서만 지원됩니다.

WLC 물리적 인터페이스에 대한 듀플렉스 설정을 설정하려면 명령을 `config port physicalmode {all | port} {100h | 100f | 10h | 10f}` 사용합니다.

이 명령은 전용 10Mbps 또는 100Mbps, 하프 듀플렉스(half-duplex) 또는 풀 듀플렉스(full-duplex) 작업을 위해 지정된 또는 모든 전면 패널 10/100BASE-T 이더넷 포트를 설정합니다. 포트에서 물리적 모드를 수동으로 설정하기 전에 `config port autoneg disable` 명령을 사용하여 자동 협상을 비활성화해야 합니다. 또한 `config port autoneg` 명령은 `config port physicalmode` 명령으로 지정한 설정을 재정의합니다. 기본적으로 모든 포트는 자동 협상으로 설정됩니다.



참고: 파이버 포트의 속도 설정을 변경할 수 있는 방법은 없습니다.

Q. LAP(Lightweight Access Point)가 컨트롤러에 등록되지 않은 경우 이름을 추적할 수 있는 방법이 있습니까?

A. AP가 완전히 중단되고 컨트롤러에 등록되지 않은 경우 컨트롤러를 통해 LAP를 추적할 수 있는 방법은 없습니다. 유일한 방법은 이러한 AP가 연결된 스위치에 액세스해서 다음 명령을 사용하여 연결된 스위치 포트를 찾는 것입니다.

<#root>

```
show mac-address-table address <mac address>
```

이 명령을 사용하면 이 AP가 연결된 스위치의 포트 번호가 제공됩니다. 이후 다음 명령을 실행합니다.

```
<#root>
```

```
show cdp nei <type/num> detail
```

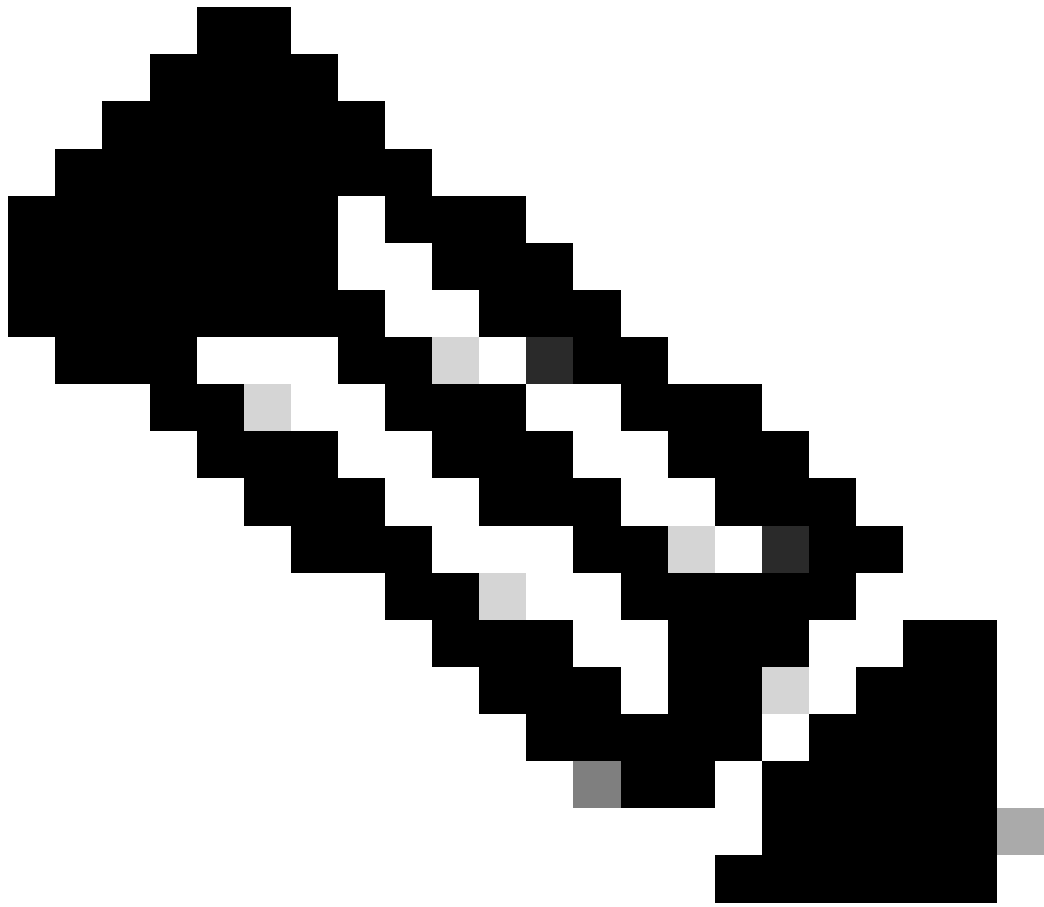
이 명령의 출력에서도 LAP 이름을 제공합니다. 그러나 이 방법은 AP의 전원이 켜져 있고 스위치에 연결된 경우에만 가능합니다.

Q. 컨트롤러에서 512명의 사용자를 구성했습니다. WLC(Wireless LAN Controller)의 사용자 수를 늘릴 수 있는 방법이 있습니까?

A. 로컬 사용자 데이터베이스는 [보안> 일반] 페이지에서 최대 2048개 항목으로 제한됩니다. 이 데이터베이스는 로컬 관리 사용자 (Lobby Ambassador 포함), 네트워크 사용자(게스트 사용자 포함), MAC 필터 항목, 액세스 포인트 권한 부여 목록 항목 및 제외 목록 항목이 공유합니다. 이러한 모든 유형의 사용자는 설정된 데이터베이스 크기를 초과할 수 없습니다.

로컬 데이터베이스를 늘리려면 CLI에서 다음 명령을 사용합니다.

```
<Cisco Controller>config database size ?  
<count> Enter the maximum number of entries (512-2048)
```



참고: 변경 사항을 적용하려면 설정을 저장하고 시스템을 재설정(reset system 명령 사용)해야 합니다.



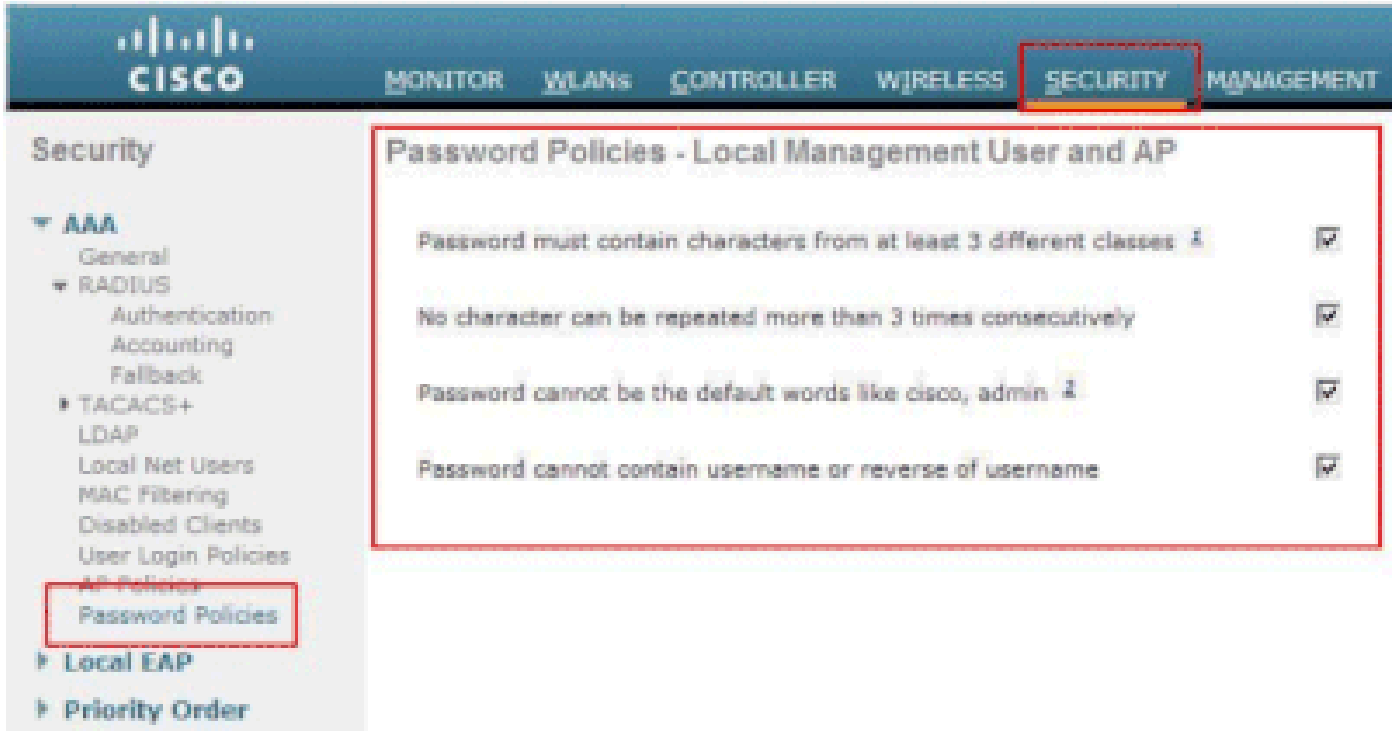
General

Maximum Local Database entries (on next reboot).	<input type="text" value="512"/>	(Current Maximum is 2048)
Number of entries, already used	1	

Q. WLC에 강력한 비밀번호 정책을 시행하려면 어떻게 해야 하나요?

A. WLC를 사용하면 강력한 비밀번호 정책을 정의할 수 있습니다. 이 작업은 CLI 또는 GUI를 사용하여 수행할 수 있습니다.

GUI에서 **Security > AAA > Password Policies**로 이동합니다. 이 페이지에는 강력한 비밀번호를 적용하기 위해 선택할 수 있는 일련의 옵션이 있습니다. 예를 들면 다음과 같습니다.



Q. Wireless LAN Controller에서 패시브 클라이언트 기능은 어떻게 사용됩니까?

A. 패시브 클라이언트는 정적 IP 주소로 설정된 스케일 및 프린터 같은 무선 디바이스입니다. 이러한 클라이언트는 액세스 포인트와 연결될 때 IP 주소, 서브넷 마스크, 게이트웨이 정보 등의 IP 정보를 전송하지 않습니다. 따라서 패시브 클라이언트가 사용된 경우 DHCP를 사용하지 않는 한 컨트롤러가 IP 주소를 인식하지 못합니다.

WLC는 현재 ARP 요청에 대한 프록시 역할을 합니다. 컨트롤러는 ARP 요청을 수신하면 요청을 클라이언트에 직접 전달하는 대신 ARP 응답으로 응답합니다. 이 시나리오에는 두 가지 이점이 있습니다.

• 클라이언트에 ARP 요청을 전송하는 업스트림 디바이스는 클라이언트의 위치를 알 수 없습니다.

휴대폰 및 프린터와 같이 배터리로 작동하는 디바이스는 모든 ARP 요청에 응답할 필요가 없으므로 전력이 유지됩니다.

무선 컨트롤러에는 패시브 클라이언트에 대한 IP 관련 정보가 없으므로 ARP 요청에 응답할 수 없습니다. 현재 동작에서는 패시브 클라이언트에 ARP 요청을 전송할 수 없습니다. 패시브 클라이언트에 액세스를 시도하는 모든 애플리케이션은 실패합니다.

패시브 클라이언트 기능을 사용하면 유선 및 무선 클라이언트 간에 ARP 요청 및 응답을 교환할 수 있습니다. 이 기능을 활성화하면 원하는 무선 클라이언트가 RUN 상태가 될 때까지 컨트롤러가 유선에서 무선 클라이언트로 ARP 요청을 전달할 수 있습니다.

패시브 클라이언트 기능을 설정하는 방법에 대한 자세한 내용은 Cisco Wireless LAN Controller 설정 가이드, 릴리스 7.0.116.0의 GUI를 사용한 패시브 클라이언트 설정 섹션을 참조하십시오.

Q. 3분마다 또는 지정된 기간에 RADIUS 서버에 재인증하도록 클라이언트를 설정하려면 어떻게 해야 합니까?

A. WLC의 세션 시간 초과 매개변수를 사용하여 이를 수행할 수 있습니다. 기본적으로 세션 시간 초과 매개변수는 재인증이 발생하기 전 1,800초로 설정됩니다.

3분 후에 클라이언트를 재인증하려면 이 값을 180초로 변경합니다.

세션 시간 초과 매개변수에 액세스하려면 GUI에서 WLAN 메뉴를 클릭합니다. WLC에 설정된 WLAN 목록이 표시됩니다. 클라이언트가 속한 WLAN을 클릭합니다. **Advanced** 탭으로 이동하여 *Enable Session Timeout* 매개변수를 찾습니다. 기본값을 180으로 변경하고 **Apply**를 클릭하여 변경 사항을 적용합니다.

RADIUS-Request의 Termination-Action 값과 함께 Access-Accept에서 전송되는 경우, Session-Timeout 속성은 재인증 전에 제공되는 서비스의 최대 시간(초)을 지정합니다. 이 경우 Session-Timeout 속성은 802.1X의 재인증 타이머 상태 시스템 내에서 ReAuthPeriod 상수를 로드하는 데 사용됩니다.

Q. 앵커 WLC 역할을 하는 4400 WLC(Wireless LAN Controller)와 여러 원격 WLC 사이에 게스트 터널링 EoIP(Ethernet over IP) 터널이 구성되어 있습니다. 이 앵커 WLC는 EoIP 터널을 통해 서브넷 브로드캐스트를 유선 네트워크에서 원격 컨트롤러와 연결된 무선 클라이언트로 전달할 수 있습니까?

A. 아니요, WLC 4400은 EoIP 터널을 통해 유선 측에서 무선 클라이언트로 IP 서브넷 브로드캐스트를 전달하지 않습니다. 지원되는 기능이 아닙니다. 시스코에서는 게스트 액세스 토폴로지서 서브넷 브로드캐스트 또는 멀티캐스트의 터널링을 지원하지 않습니다. 게스트 WLAN은 네트워크의 특정 위치(대부분 방화벽 외부)에 클라이언트 POP(Point of Presence)를 강제 적용하므로 서브넷 브로드

캐스트의 터널링은 보안 문제를 일으킬 수 있습니다.

Q. WLC(Wireless LAN Controller) 및 LWAPP(Lightweight Access Point Protocol) 설정에서 음성 트래픽에 대해 어떤 DSCP(Differentiated Services Code Point) 값이 전달되니까? QoS는 WLC에서 어떻게 구현되니까?

A.Cisco UWN(Unified Wireless Network) 솔루션 WLAN은 4가지 QoS 레벨을 지원합니다.

- 플래티넘/보이스

- 골드/비디오

- 실버/최선(기본)

- 브론즈/백그라운드

플래티넘 QoS를 사용하도록 음성 트래픽 WLAN을 설정하고, 브론즈 QoS를 사용하도록 저대역폭 WLAN을 할당하며, 다른 QoS 레벨 사이에 모든 기타 트래픽을 할당할 수 있습니다. 자세한 내용은 WLAN에 QoS 프로파일 할당을 참조하십시오.

Q. Cisco Wireless Unified 솔루션에서 Linksys 이더넷 브리지가 지원되니까?

A.아니요, WLC는 Cisco WGB 제품만 지원합니다. Linksys WGB는 지원되지 않습니다. Cisco Wireless Unified 솔루션은 Linksys WET54G 및 WET11B 이더넷 브리지를 지원하지 않지만, 다음 지침을 사용하는 경우 Wireless Unified 솔루션 설정에서 이러한 디바이스를 사용할 수 있습니다.

-

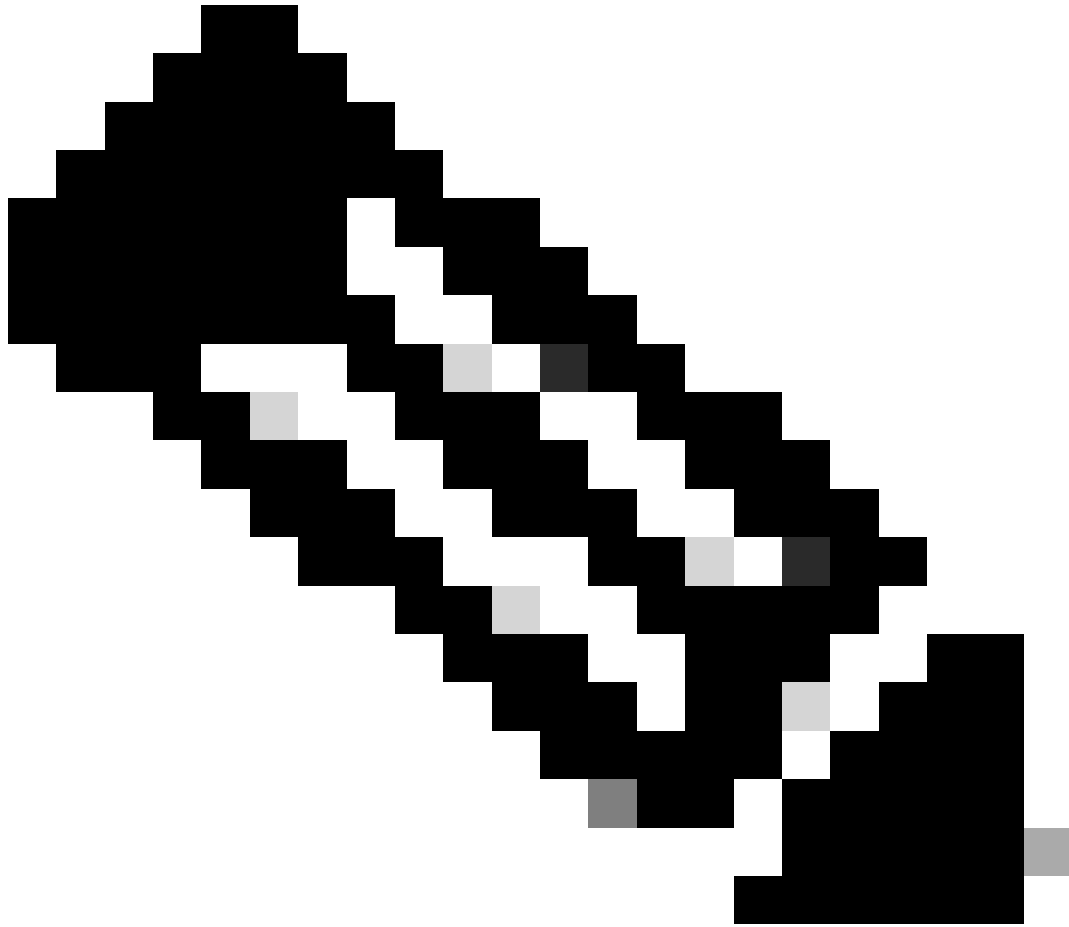
WET54G 또는 WET11B에 하나의 디바이스만 연결합니다.

-

WET54G 또는 WET11B에서 MAC 복제 기능을 활성화하여 연결된 디바이스를 복제합니다.

-

WET54G 또는 WET11B에 연결된 디바이스에 최신 드라이버 및 펌웨어를 설치합니다. 이전 펌웨어 버전에서는 DHCP에 문제가 발생하므로 이 지침은 특히 JetDirect 프린터에 중요합니다.



참고: 다른 서드파티 브리지는 지원되지 않습니다. 언급된 단계는 다른 서드파티 브리지에 대해서도 시도할 수 있습니다.

Q. WLC(Wireless LAN Controller)에 컨피그레이션 파일을 저장하려면 어떻게 해야 합니까?

A. WLC에는 두 종류의 메모리가 포함되어 있습니다.

-

휘발성 RAM - 현재, 활성 컨트롤러 설정 유지

-

NVRAM(비휘발성 RAM) - 재부팅 설정 유지

WLC에서 운영 체제를 설정하면 휘발성 RAM이 수정됩니다. WLC가 현재 설정에서 재부팅되도록 하려면 휘발성 RAM의 설정을 NVRAM에 저장해야 합니다.

다음 작업을 수행할 때는 어떤 메모리를 수정하고 있는지를 알아야 합니다.

-

설정 마법사를 사용합니다.

-

컨트롤러 설정을 지웁니다.

-

설정을 저장합니다.

-

컨트롤러를 재설정합니다.

-

CLI에서 로그아웃합니다.

WLC 기능 FAQ

Q. WLC(Wireless LAN Controller)에서 EAP(Extensible Authentication Protocol) 유형을 설정하려면 어떻게 해야 하나요? ACS(Access Control Server) 어플라이언스에 대해 인증하려고 하는데, 로그에 "지원되지 않는 EAP" 유형이라고 표시됩니다.

A. WLC에는 별도의 EAP 유형 설정이 없습니다. LEAP(Light EAP), EAP-FAST(EAP Flexible Authentication via Secure Tunneling) 또는 MS-PEAP(Microsoft Protected EAP)의 경우 IEEE 802.1x 또는 WPA(Wi-Fi Protected Access)를 설정하십시오(WPA 포함 802.1x를 사용하는 경우). RADIUS 백엔드 및 클라이언트에서 지원되는 모든 EAP 유형은 802.1x 태그를 통해 지원됩니다. 클라이언트와 RADIUS 서버의 EAP 설정이 일치해야 합니다.

WLC의 GUI를 통해 EAP를 활성화하려면 다음 단계를 완료합니다.

1. WLC GUI에서 **WLAN**을 클릭합니다.
2. WLC에 설정된 WLAN 목록이 나타납니다. WLAN을 클릭합니다.
3. **WLANs > Edit**에서 **Security** 탭을 클릭합니다.
4. **Layer 2**를 클릭하고 레이어 2 보안을 802.1x 또는 WPA+WPA2로 선택합니다. 동일한 창에서 사용 가능한 802.1x 매개변수를 설정할 수도 있습니다. 그런 다음 WLC는 무선 클라이언트와 인증 서버 간에 EAP 인증 패킷을 전달합니다.
5. **AAA** 서버를 클릭하고 이 WLAN의 드롭다운 메뉴에서 인증 서버를 선택합니다. 인증 서버가 이미 전역으로 설정되어 있다고 가정합니다.

Q. 빠른 SSID 변경이란 무엇입니까?

A. 고속 SSID 변경을 통해 클라이언트는 서로 다른 SSID 간에 이동할 수 있습니다. 클라이언트가 다른 SSID에 대한 새 연결을 전송하는 경우, 컨트롤러 연결 테이블의 클라이언트 항목은 클라이언트가 새 SSID에 추가되기 전에 지워집니다. 고속 SSID 변경이 비활성화된 경우 컨트롤러는 클라이언트가 새 SSID로 이동하는 것이 허용되기 전에 지연을 적용합니다. 고속 SSID 변경을 활성화하는 방법에 대한 자세한 내용은 Cisco Wireless LAN Controller 설정 가이드, 릴리스 7.0.116.0의 고속 SSID 변경 설정 섹션을 참조하십시오.

Q. 무선 LAN에 연결할 수 있는 클라이언트 수를 제한할 수 있습니까?

A.WLAN에 연결할 수 있는 클라이언트 수에 제한을 설정할 수 있습니다. 이는 컨트롤러에 연결할 수 있는 클라이언트 수가 제한된 시나리오에서 유용합니다. WLAN당 설정할 수 있는 클라이언트 수는 사용 중인 플랫폼에 따라 달라집니다.

Wireless LAN Controller의 다양한 플랫폼에서 WLAN당 클라이언트 제한에 대한 자세한 내용은 Cisco Wireless LAN Controller 설정 가이드, 릴리스 7.0.116.0의 WLAN당 최대 클라이언트 수 설정 섹션을 참조하십시오.

Q. PKC란 무엇이며 WLC(Wireless LAN Controller)에서는 어떻게 작동합니까?

A. PKC는 Proactive Key Caching의 약어입니다. 이는 802.11i IEEE 표준의 확장으로 설계되었습니다.

PKC는 Cisco 2006/410x/440x 시리즈 컨트롤러에서 활성화된 기능으로, 제대로 장착된 무선 클라이언트가 AAA 서버를 사용하여 전체 재인증 없이 로밍할 수 있습니다. PKC를 이해하려면 먼저 키 캐싱을 이해해야 합니다.

키 캐싱은 WPA2에 추가된 기능입니다. 이를 통해 모바일 스테이션은 AP(액세스 포인트)와의 성공적인 인증을 통해 얻은 기본 키(PMK(Pairwise Primary Key))를 캐시하고 동일한 AP와의 향후 연결에서 재사용할 수 있습니다. 즉, 지정된 모바일 디바이스는 특정 AP로 한 번 인증하고 나중에 사용할 수 있도록 키를 캐시해야 합니다. 키 캐싱은 PMK, 문자열, 스테이션 및 AP의 MAC 주소의 해시인 PMKID(PMK Identifier)라는 메커니즘을 통해 처리됩니다. PMKID는 PMK를 고유하게 식별합니다.

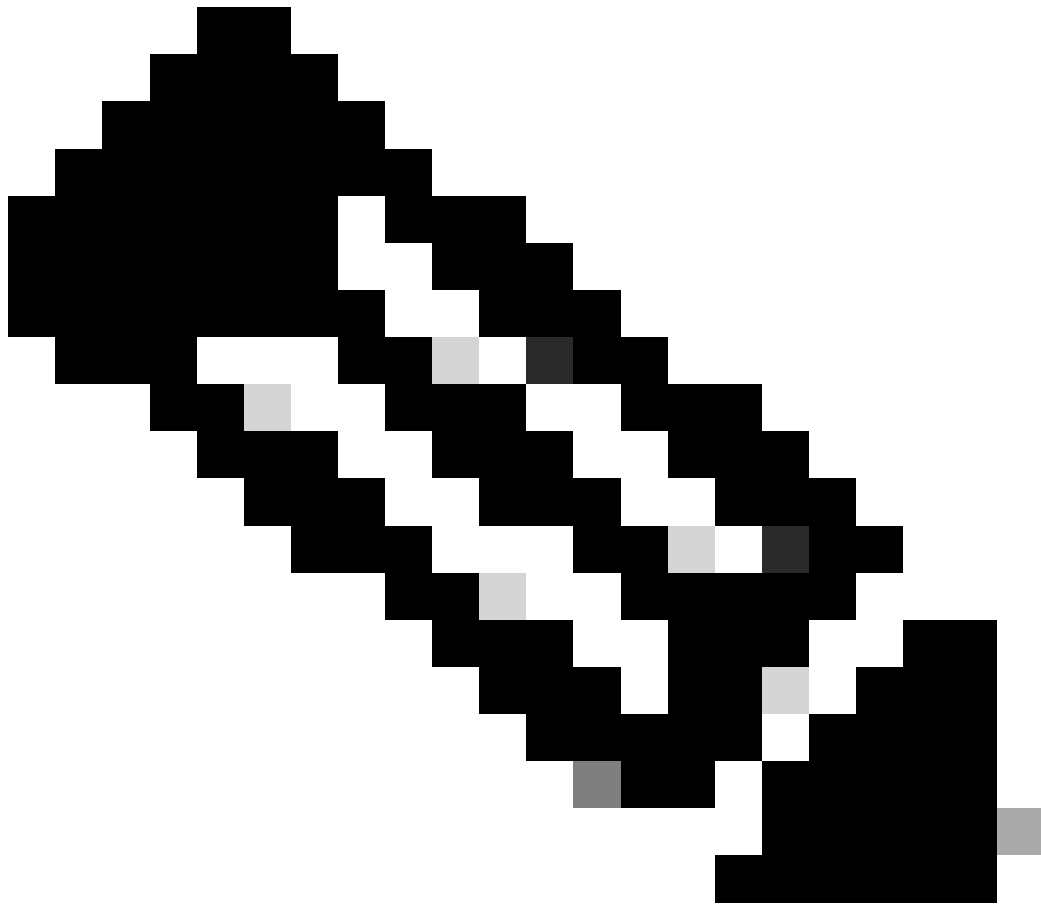
키 캐싱을 사용하는 경우에도 무선 스테이션은 서비스를 받으려는 각 AP를 인증해야 합니다. 이로 인해 상당한 레이턴시 및 오버헤드가 발생하며, 이는 핸드오프 프로세스를 지연시키고 실시간 애플리케이션을 지원하는 기능을 제한할 수 있습니다. 이 문제를 해결하기 위해 WPA2와 함께 PKC가 도입되었습니다.

PKC를 통해 스테이션은 성공적인 인증 프로세스를 통해 이전에 얻은 PMK를 다시 사용할 수 있습니다. 이렇게 하면 스테이션이 로밍할 때 새 AP에 대해 인증할 필요가 없습니다.

따라서 컨트롤러 내 로밍에서 모바일 디바이스가 동일한 컨트롤러의 한 AP에서 다른 AP로 이동하면 클라이언트는 이전에 사용한 PMK를 사용하여 PMKID를 다시 계산하고 연결 프로세스 중에 제시합니다. WLC는 PMK 캐시를 검색하여 해당 항목이 있는지 확인합니다. 있는 경우 802.1x 인증 프로세스를 우회하고 즉시 WPA2 키 교환을 시작합니다. 그렇지 않은 경우 표준 802.1X 인증 프로세스를 거칩니다.

PKC는 WPA2에서 기본적으로 활성화됩니다. 따라서 WLC의 WLAN 설정에서 WPA2를 레이어 2 보안으로 활성화하면 WLC에서 PKC가 활성화됩니다. 또한 적절한 EAP 인증을 위해 AAA 서버 및 무선 클라이언트를 설정합니다.

PKC가 작동하려면 클라이언트 측에서 사용되는 신청자가 WPA2도 지원해야 합니다. PKC는 컨트롤러 간 로밍 환경에서도 구현할 수 있습니다.



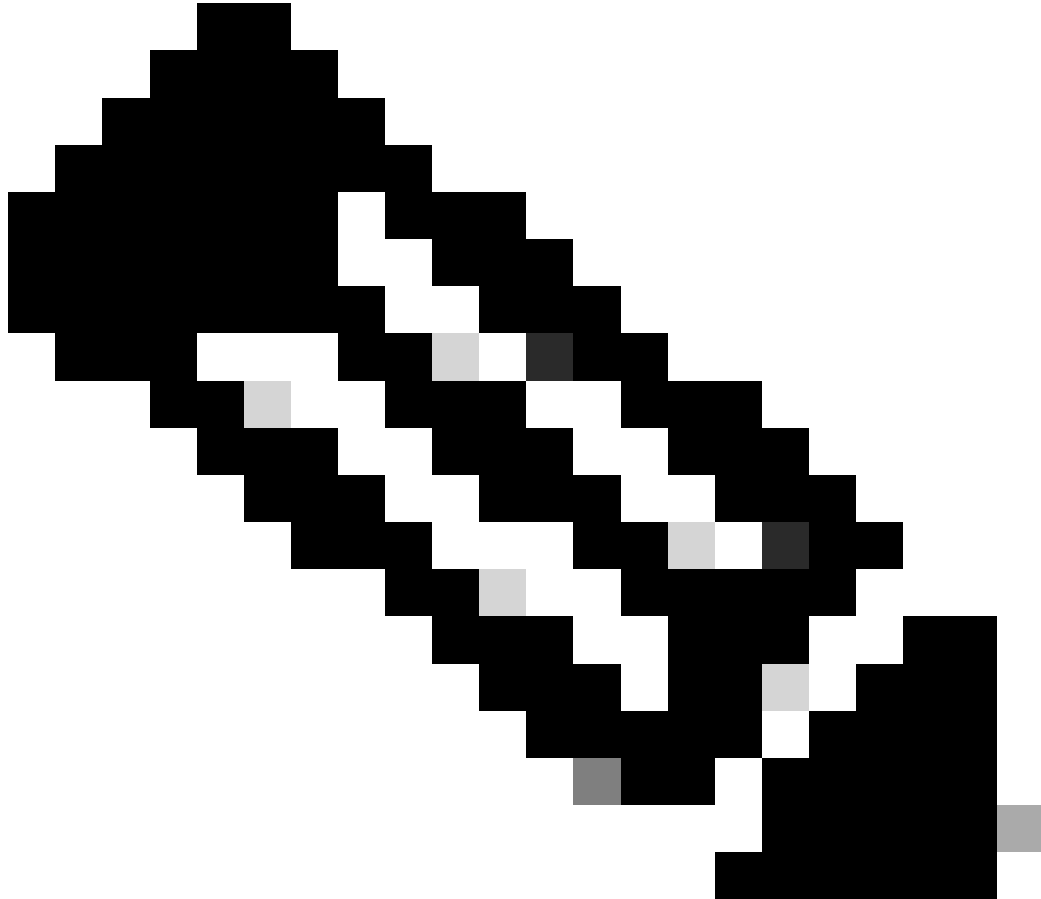
참고: PKC는 ADU(Aironet Desktop Utility)와 함께 클라이언트 신청자로 작동하지 않습니다.

Q. 컨트롤러에서 이러한 시간 초과 설정에 대한 설명: ARP(Address Resolution Protocol) 시간 초과, 사용자 유휴 시간 초과, 세션 시간 초과?

A.A. ARP 시간 초과는 네트워크에서 학습한 디바이스에 대한 WLC의 ARP 항목을 삭제하는 데 사용됩니다.

사용자 유휴 시간 제한: 사용자가 사용자 유휴 시간 제한으로 설정된 시간 동안 LAP와 통신하지 않고 유휴 상태인 경우 클라이언트

는 WLC에 의해 인증 취소됩니다. 클라이언트는 다시 인증하고 WLC에 다시 연결해야 합니다. 이는 클라이언트가 LAP에 알리지 않고 연결된 LAP에서 삭제될 수 있는 상황에서 사용됩니다. 이는 클라이언트에서 배터리가 완전히 소모되거나 클라이언트 연결이 다른 곳으로 이동하는 경우에 발생할 수 있습니다.



참고: WLC GUI에서 ARP 및 사용자 유휴 시간 제한에 액세스하려면 컨트롤러 메뉴로 이동하십시오. 왼쪽에서 General을 선택하여 ARP 및 User Idle Timeout 필드를 찾습니다.

Session Timeout은 WLC와의 클라이언트 세션에 대한 최대 시간입니다. 이 시간이 지나면 WLC는 클라이언트를 인증 취소하고 클라이언트는 전체 인증(재인증) 프로세스를 다시 거칩니다. 이는 암호화 키를 순환하기 위한 보안 예방 조치의 일부입니다. 키 관리와 함께 EAP(Extensible Authentication Protocol) 방법을 사용하는 경우, 새 암호화 키를 파생하기 위해 정기적인 간격으로 키 재입력이 발생

합니다. 키 관리를 사용하지 않는 경우 이 시간 초과 값은 무선 클라이언트가 전체 재인증을 수행하는 데 필요한 시간입니다. 세션 시간 초과는 WLAN에 따라 다릅니다. 이 매개변수는 **WLAN > Edit** 메뉴에서 액세스할 수 있습니다.

Q. RFID 시스템이란? 현재 시스코에서 지원하는 RFID 태그는 무엇입니까?

A. RFID(Radio Frequency Identification)는 매우 짧은 범위 통신에 대해 무선 주파수 통신을 사용하는 기술입니다. 기본 RFID 시스템은 RFID 태그, RFID 리더 및 프로세싱 소프트웨어로 구성됩니다.

현재 Cisco는 AeroScout 및 Pango의 RFID 태그를 지원합니다. AeroScout 태그를 설정하는 방법에 대한 자세한 내용은 [AeroScout RFID 태그에 대한 WLC 설정](#)을 참조하십시오.

Q. WLC에서 로컬로 EAP 인증을 수행할 수 있습니까? 이 로컬 EAP 기능을 설명하는 문서가 있습니까?

A. 예, EAP 인증은 WLC에서 로컬로 수행할 수 있습니다. 로컬 EAP는 사용자 및 무선 클라이언트를 WLC에서 로컬로 인증할 수 있는 인증 방법입니다. 이는 백엔드 시스템이 중단되거나 외부 인증 서버가 다운될 때 무선 클라이언트에 대한 연결성을 유지하려는 원격 사무실에서 사용하도록 설계되었습니다. 로컬 EAP를 활성화하면 WLC가 인증 서버 역할을 합니다. 로컬 EAP-Fast 인증을 위해 WLC를 설정하는 방법에 대한 자세한 내용은 [EAP-FAST 및 LDAP 서버 설정을 사용하는 Wireless LAN Controller의 로컬 EAP 인증](#) 예시를 참조하십시오.

Q. WLAN 재정의 기능이란 무엇입니까? 이 기능을 어떻게 설정합니까? LAP는 백업 WLC로 페일오버할 때 WLAN 재정의 값을 유지합니까?

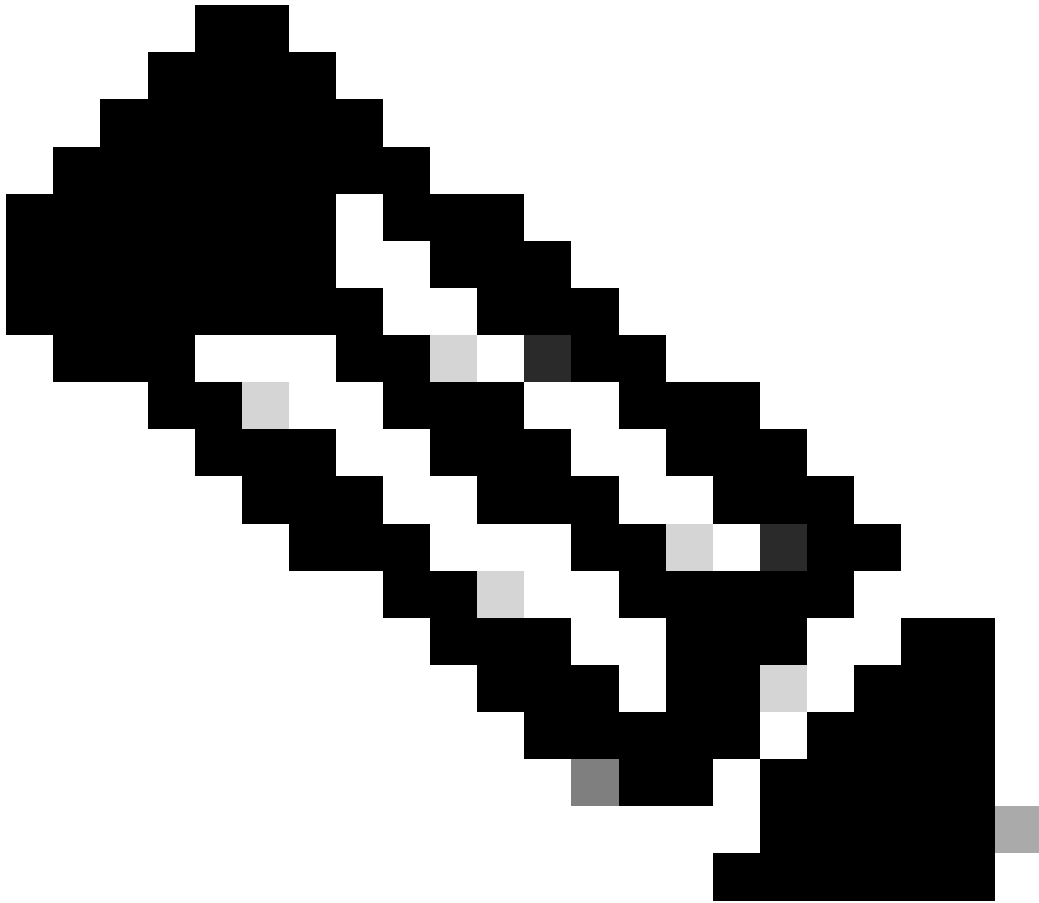
A. WLAN 재정의 기능을 사용하면 개별 LAP 단위로 적극적으로 사용할 수 있는 WLC에 설정된 WLAN 중에서 WLAN을 선택할 수 있습니다. WLAN 재정의의 완료하려면 다음 단계를 완료하십시오.

1. WLC GUI에서 **Wireless** 메뉴를 클릭합니다.
2. 왼쪽에서 **Radios** 옵션을 클릭하고 **802.11 a/n** 또는 **802.11 b/g/n**을 선택합니다.
3. 오른쪽에 있는 드롭다운 메뉴에서 WLAN 재정의의 설정하려는 AP의 이름에 해당하는 **Configure** 링크를 클릭합니다.
4. WLAN 재정의의 드롭다운 메뉴에서 **Enable**을 선택합니다. WLAN 재정의의 메뉴는 창 왼쪽의 마지막 항목입니다.
5. WLC에 설정된 모든 WLAN의 목록이 나타납니다.

6. 이 목록에서 LAP에 표시할 WLAN을 선택하고 **Apply**를 클릭하여 변경 사항을 적용합니다.

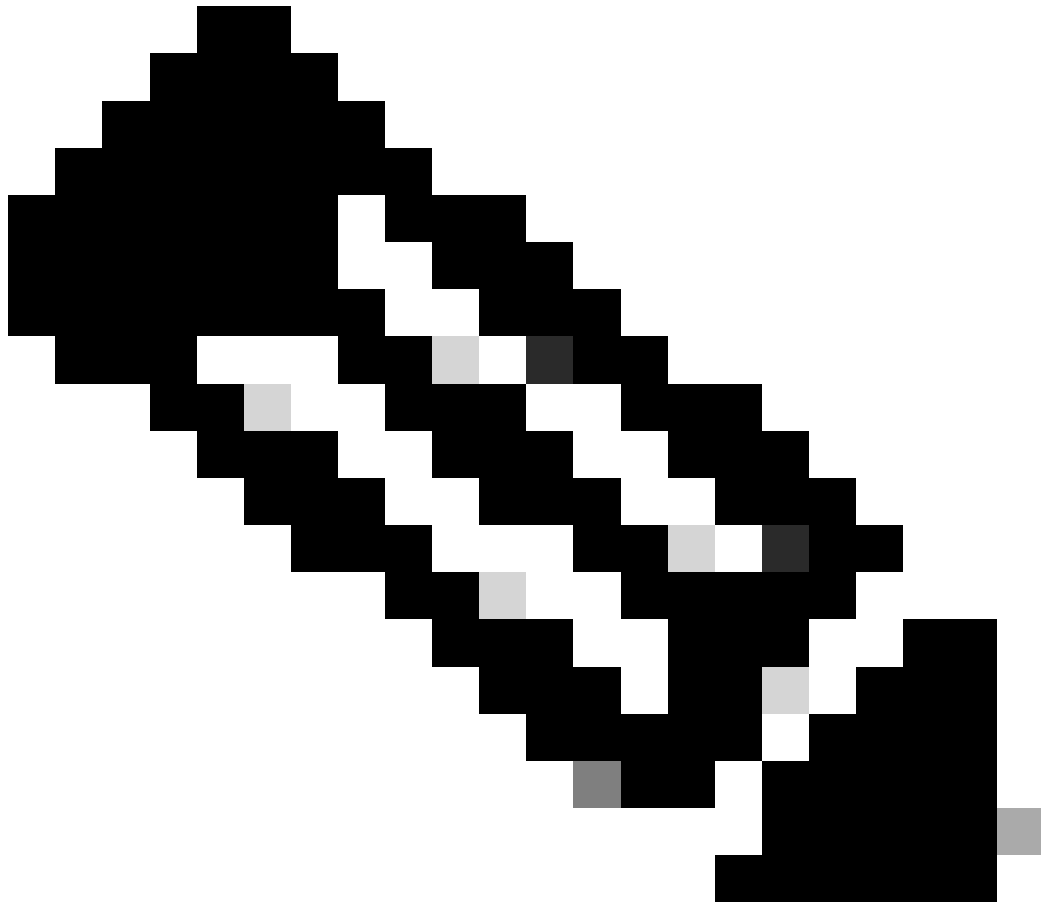
7. 이러한 변경을 수행한 후 설정을 저장합니다.

재정의하려는 WLAN 프로파일 및 SSID가 모든 WLC에 설정되어 있는 경우 AP는 다른 WLC에 등록될 때 WLAN 재정의 값을 유지합니다.



참고: 컨트롤러 소프트웨어 릴리스 5.2.157.0에서는 WLAN 재정의 기능이 컨트롤러 GUI 및 CLI에서 모두 제거되었습니다. 컨트롤러가 WLAN 재정의에 대해 설정되어 있고 컨트롤러 소프트웨어 릴리스 5.2.157.0으로 업그레이드하는 경우,

컨트롤러는 WLAN 설정을 삭제하고 모든 WLAN을 브로드캐스트합니다. 액세스 포인트 그룹을 설정하는 경우 특정 WLAN만 전송되도록 지정할 수 있습니다. 각 액세스 포인트는 해당 액세스 포인트 그룹에 속하는 활성화된 WLAN만 알립니다.



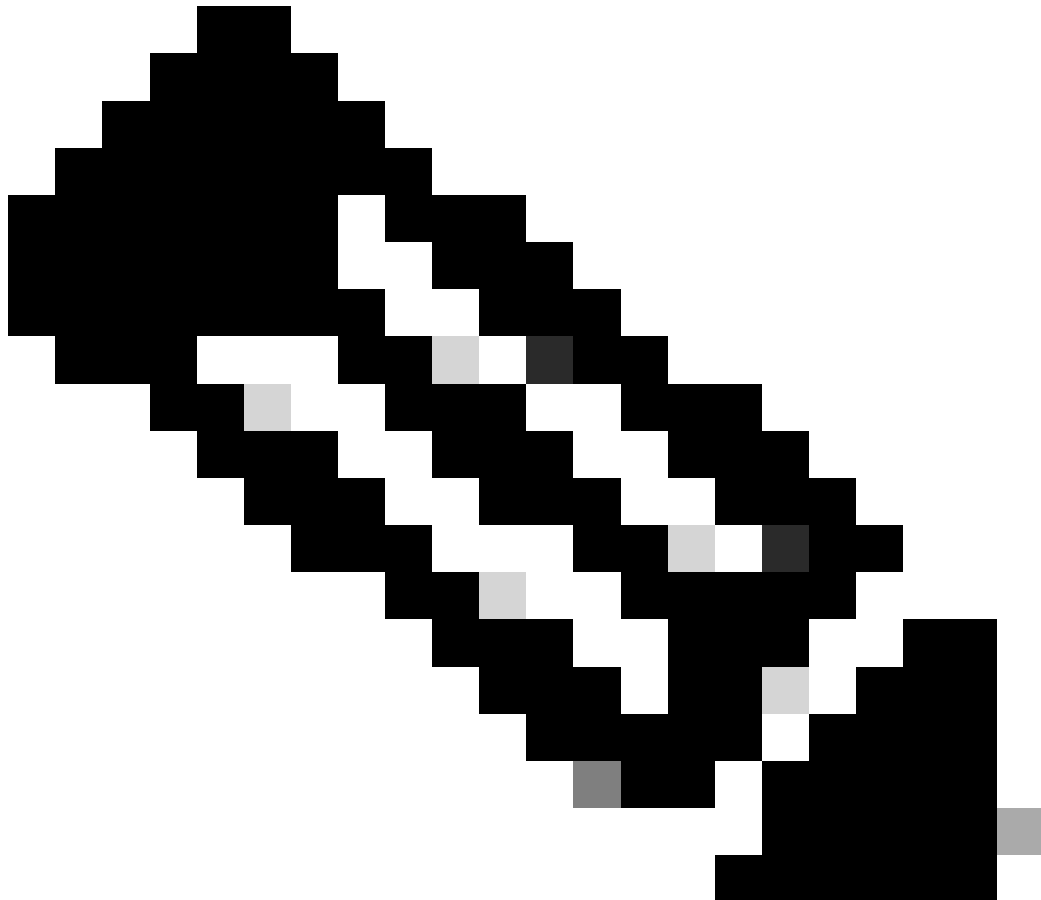
참고: 액세스 포인트 그룹은 WLAN이 AP의 무선 인터페이스별로 전송되도록 활성화하지 않습니다.

Q. IPv6는 Cisco WLC(Wireless LAN Controller) 및 LAP(Lightweight Access Point)에서 지원됩니까?

A. 현재 4400 및 4100 시리즈 컨트롤러는 IPv6 클라이언트 패스스루만 지원합니다. 네이티브 IPv6 지원은 지원되지 않습니다.

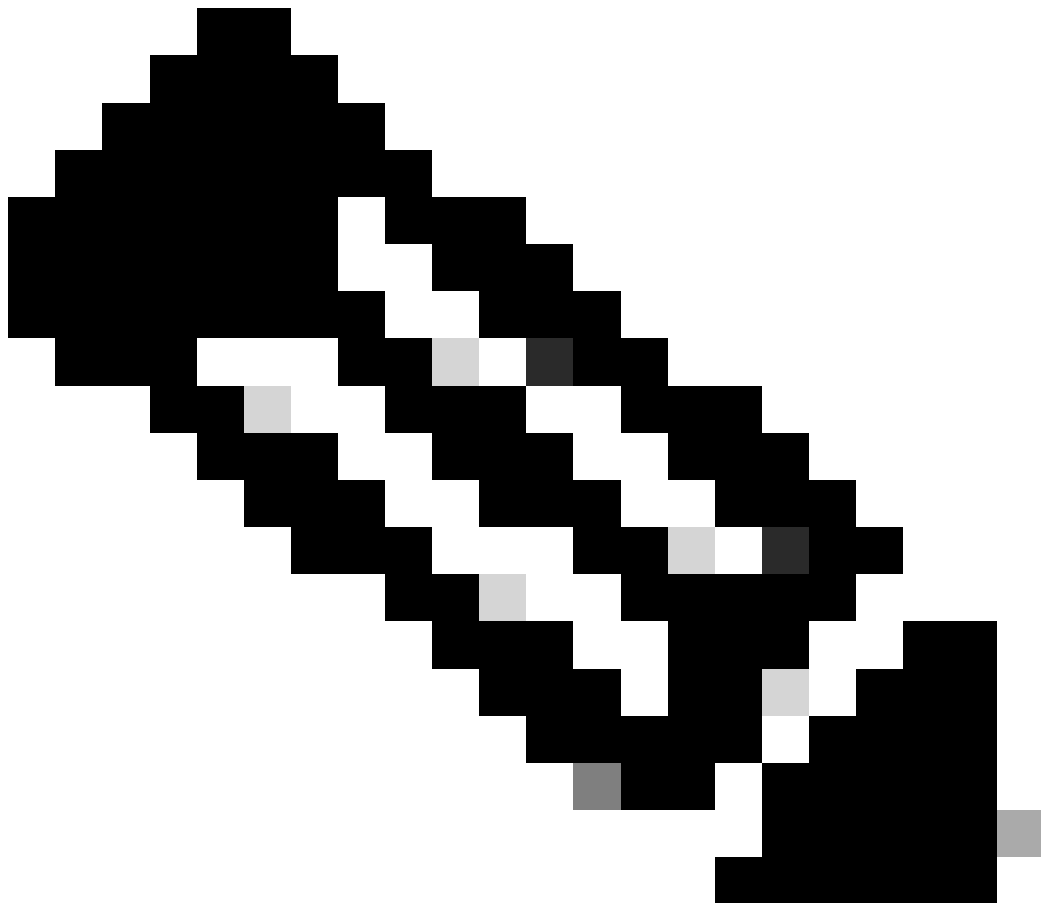
WLC에서 IPv6를 활성화하려면 WLAN > Edit 페이지의 WLAN SSID 설정에서 **IPv6 Enable** 체크 박스를 선택합니다.

또한 IPv6를 지원하려면 EMM(Ethernet Multicast Mode)이 필요합니다. EMM을 비활성화하면 IPv6를 사용하는 클라이언트 디바이스와의 연결성을 잃게 됩니다. EMM을 활성화하려면 Controller > General 페이지로 이동하여 Ethernet Multicast Mode 드롭다운 메뉴에서 **Unicast** 또는 **Multicast**를 선택합니다. 이렇게 하면 유니캐스트 모드 또는 멀티캐스트 모드에서 멀티캐스트가 활성화됩니다. 멀티캐스트가 멀티캐스트 유니캐스트로 활성화되면 각 AP에 대해 패킷이 복제됩니다. 이는 프로세서를 많이 사용하므로 주의해서 사용해야 합니다. 멀티캐스트로 활성화된 멀티캐스트는 사용자 할당 멀티캐스트 주소를 사용하여 AP(액세스 포인트)에 대한 보다 전통적인 멀티캐스트를 수행합니다.



참고: IPv6는 2006 컨트롤러에서 지원되지 않습니다.

또한 AAA 재정의 기능을 사용할 때 IPv6 통과 사용을 방지하는 Cisco 버그 ID [CSCsg78176](#)이 있습니다.

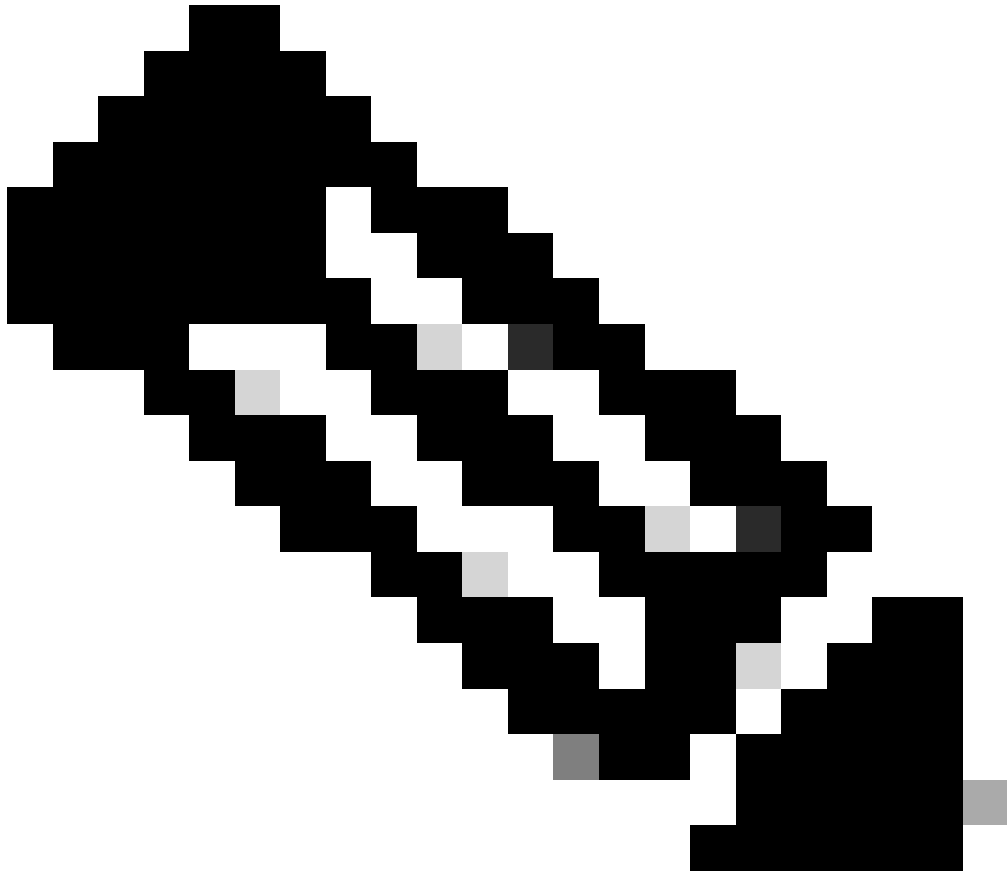


참고: 등록된 Cisco 사용자만 내부 Cisco 툴 및 정보에 액세스할 수 있습니다.

Q. Cisco 2000 Series WLC(Wireless LAN Controller)는 게스트 사용자를 위한 웹 인증을 지원합니까?

A. 웹 인증은 모든 Cisco WLC에서 지원됩니다. 웹 인증은 단순 인증 자격 증명으로 사용자를 인증하는 데 사용되는 레이어 3 인증 방법입니다. 암호화는 포함되지 않습니다. 이 기능을 활성화하려면 다음 단계를 완료하십시오.

1. GUI에서 **WLAN** 메뉴를 클릭합니다.
 2. **WLAN**을 클릭합니다.
 3. **Security** 탭으로 이동하여 **Layer 3**를 선택합니다.
 4. **Web Policy** 박스를 선택하고 **Authentication**을 선택합니다.
 5. **Apply**를 클릭하여 변경 사항을 저장합니다.
 6. WLC에서 사용자를 인증할 데이터베이스를 생성하려면 GUI의 **Security** 메뉴로 이동하여 **Local Net User**를 선택하고 다음 작업을 완료합니다.
 - a. 로그인하기 위해 사용할 게스트 사용자 이름 및 비밀번호를 정의합니다. 이 값은 대/소문자를 구별합니다.
 - b. 사용하는 WLAN ID를 선택합니다.
-
-



참고: 보다 자세한 설정에 관한 정보는 Wireless LAN Controller 웹 인증 설정 예시를 참조하십시오.

Q. WLC를 무선 모드로 관리할 수 있습니까?

A. WLC는 일단 활성화되면 무선 모드를 통해 관리할 수 있습니다. 무선 모드를 활성화하는 방법에 대한 자세한 내용은 Cisco Wireless LAN Controller 설정 가이드, 릴리스 7.0.116.0의 GUI 및 CLI에 대한 무선 연결 활성화 섹션을 참조하십시오.

Q. LAG(Link Aggregation)란? WLC(Wireless LAN Controller)에서 LAG를 활성화하려면 어떻게 해야 하나요?

A.LAG는 WLC의 모든 포트를 단일 EtherChannel 인터페이스로 번들합니다. 시스템은 LAG를 사용하여 트래픽 로드 밸런싱 및 포트 리던던시를 동적으로 관리합니다.

일반적으로 WLC의 인터페이스에는 IP 주소, 기본 게이트웨이(IP 서브넷의 경우), 기본 물리적 포트, 보조 물리적 포트, VLAN 태그 및 DHCP 서버를 포함해 이와 연결된 여러 매개변수가 있습니다. LAG를 사용하지 않는 경우 각 인터페이스는 일반적으로 물리적 포트에 매핑되지만, 여러 인터페이스를 단일 WLC 포트에 매핑할 수도 있습니다. LAG를 사용하는 경우 시스템은 인터페이스를 집계된 포트 채널에 동적으로 매핑합니다. 이는 포트 리던던시 및 로드 밸런싱에 도움이 됩니다. 포트에 장애가 발생하면 인터페이스는 다음으로 사용 가능한 물리적 포트에 동적으로 매핑되며, LAG는 여러 포트에서 밸런싱됩니다.

WLC에서 LAG가 활성화된 경우 WLC는 데이터 프레임 수신한 것과 동일한 포트에서 데이터 프레임을 전달합니다. WLC는 인접한 스위치를 사용하여 EtherChannel 전체에서 트래픽을 로드 밸런싱합니다. WLC는 자체적으로 EtherChannel 로드 밸런싱을 수행하지 않습니다.

Q. WLC(Wireless LAN Controller)의 어떤 모델이 LAG(Link Aggregation)를 지원하나요?

A.Cisco 5500 시리즈 컨트롤러는 소프트웨어 릴리스 6.0 이상에서 LAG를 지원하고, Cisco 4400 시리즈 컨트롤러는 소프트웨어 릴리스 3.2 이상에서 LAG를 지원하며, LAG는 Cisco WiSM 및 Catalyst 3750G Integrated Wireless LAN Controller 스위치 내의 컨트롤러에서 자동으로 활성화됩니다. LAG가 없으면 Cisco 4400 시리즈 컨트롤러의 각 배포 시스템 포트는 최대 48개의 액세스 포인트를 지원합니다. LAG를 활성화하면 Cisco 4402 컨트롤러의 논리적 포트는 최대 50개의 액세스 포인트를 지원하고, Cisco 4404 컨트롤러의 논리적 포트는 최대 100개의 액세스 포인트를 지원하며, Catalyst 3750G Integrated Wireless LAN Controller 스위치 및 각 Cisco WiSM 컨트롤러의 논리적 포트는 최대 150개의 액세스 포인트를 지원합니다.

Cisco 2106 및 2006 WLC는 LAG를 지원하지 않습니다. Cisco 4000 시리즈 WLC와 같은 이전 모델은 LAG를 지원하지 않습니다.

Q. Unified Wireless Networks의 Auto-Anchor 모빌리티 기능은 무엇입니까?

A.자동 앵커 모빌리티(또는 게스트 WLAN 모빌리티)는 WLAN(무선 LAN)의 로밍 클라이언트에 대한 로드 밸런싱 및 보안을 개선하는 데 사용됩니다. 정상적인 로밍 조건에서 클라이언트 디바이스는 WLAN에 조인하고 클라이언트 디바이스가 연결하는 첫 번째 컨트롤러에 고정됩니다. 클라이언트가 다른 서브넷으로 로밍하는 경우 클라이언트가 로밍하는 컨트롤러는 앵커 컨트롤러를 사용하여 클라이언트에 대한 외부 세션을 설정합니다. 자동 앵커 모빌리티 기능을 사용하면 WLAN에서 클라이언트에 대한 앵커 포인트로 컨트롤러 또는 컨트롤러 세트를 지정할 수 있습니다.



참고: 레이어 3 모빌리티에 대해 모빌리티 앵커를 설정해서는 안 됩니다. 모빌리티 앵커는 게스트 터널링에만 사용됩니다.

Q. Cisco 2006 WLC(Wireless LAN Controller)를 WLAN에 대한 앵커로 구성할 수 있습니까?

A. Cisco 2000 시리즈 WLC는 WLAN의 앵커로 지정할 수 없습니다. 그러나 Cisco 2000 시리즈 WLC에서 생성된 WLAN은 Cisco 4100 시리즈 WLC 및 Cisco 4400 시리즈 WLC를 앵커로 사용할 수 있습니다.

Q. Wireless LAN Controller는 어떤 유형의 모빌리티 터널링을 사용합니까?

A. 컨트롤러 소프트웨어 릴리스 4.1~5.1은 비대칭 및 대칭 모빌리티 터널링을 모두 지원합니다. 컨트롤러 소프트웨어 릴리스 5.2 이상에서는 대칭 모빌리티 터널링만 지원하며, 기본적으로 항상 활성화되어 있습니다.

비대칭 터널링에서 유선 네트워크에 대한 클라이언트 트래픽은 외부 컨트롤러를 통해 직접 라우팅됩니다. 업스트림 라우터에서 RPF(Reverse Path Filtering)가 활성화된 경우 비대칭 터널링이 중단됩니다. 이 경우 RPF 확인에서 소스 주소로 돌아가는 경로가 패킷이 오는 경로와 일치하는지 확인하기 때문에 클라이언트 트래픽이 라우터에서 삭제됩니다.

대칭 모빌리티 터널링이 활성화된 경우 모든 클라이언트 트래픽이 앵커 컨트롤러로 전송된 다음 RPF 확인을 성공적으로 통과할 수 있습니다. 대칭 모빌리티 터널링은 다음과 같은 상황에서도 유용합니다.

- 소스 IP 주소가 패킷을 수신하는 서브넷과 일치하지 않아 클라이언트 패킷 경로의 방화벽 설치가 패킷을 삭제하는 경우 유용합니다.

- 앵커 컨트롤러의 액세스 포인트 그룹 VLAN이 외부 컨트롤러의 WLAN 인터페이스 VLAN과 다른 경우. 이 경우 모빌리티 이벤트 중에 클라이언트 트래픽이 잘못된 VLAN에서 전송될 수 있습니다.

Q. 네트워크가 중단되었을 때 WLC에 어떻게 액세스합니까?

A. 네트워크가 다운되면 서비스 포트에서 WLC에 액세스할 수 있습니다. 이 포트에는 WLC의 기타 포트와 완전히 다른 서브넷의 IP 주소가 할당되므로 대역 외 관리라고 합니다. 자세한 내용은 Cisco Wireless LAN Controller 설정 가이드, 릴리스 7.0.116.0의 포트 및 인터페이스 설정 섹션을 참조하십시오.

Q. Cisco WLC(Wireless LAN Controller)는 장애 조치(또는 이중화) 기능을 지원합니까?

A. 예, WLAN 네트워크에 두 개 이상의 WLC가 있는 경우 리던던시를 위해 설정할 수 있습니다. 일반적으로 LAP는 설정된 기본 WLC에 조인됩니다. 기본 WLC에 장애가 발생하면 LAP가 재부팅되고 모빌리티 그룹의 다른 WLC에 조인합니다. 페일오버는 LAP가 기본 WLC에 대해 폴링하고 기본 WLC가 작동하면 조인하는 기능입니다. 자세한 내용은 경량형 액세스 포인트에 대한 WLAN 컨트롤러 페일오버 설정 예시를 참조하십시오.

Q. WLC(Wireless LAN Controller)에서 사전 인증 ACL(Access Control List)은 어떻게 사용됩니까?

A. 사전 인증 ACL을 사용하면 이름에서 알 수 있듯이 클라이언트가 인증하기 전에도 특정 IP 주소를 오가는 클라이언트 트래픽을 허용할 수 있습니다. 웹 인증을 위해 외부 웹 서버를 사용하는 경우, 일부 WLC 플랫폼에는 외부 웹 서버(Cisco 5500 시리즈 컨트롤러, Cisco 2100 시리즈 컨트롤러, Cisco 2000 시리즈 및 컨트롤러 네트워크 모듈)에 대한 사전 인증 ACL이 필요합니다. 다른 WLC 플랫폼의 경우 사전 인증 ACL은 필수가 아닙니다. 하지만 외부 웹 인증을 사용할 때는 외부 웹 서버에 대해 사전 인증 ACL을 설정하는 것이 좋습니다.

Q. MAC에서 필터링한 WLAN과 완전히 열려 있는 WLAN이 네트워크에 있습니다. 클라이언트가 기본적으로 개방형 WLAN을 선택합니까? 아니면 클라이언트가 MAC 필터에 설정된 WLAN ID와 자동으로 연결합니까? 또한 MAC 필터에 "인터페이스" 옵션이 있는 이유는 무엇입니까?

A. 클라이언트는 연결하도록 설정된 모든 WLAN에 연결할 수 있습니다. MAC 필터의 인터페이스 옵션은 WLAN 또는 인터페이스에 필터를 적용할 수 있는 기능을 제공합니다. 여러 WLAN이 동일한 인터페이스에 연결된 경우 개별 WLAN에 대해 필터를 생성할 필요 없이 인터페이스에 MAC 필터를 적용할 수 있습니다.

Q. WLC(Wireless LAN Controller)에서 관리 사용자에게 대한 TACACS 인증을 구성하려면 어떻게 합니까?

A. WLC 버전 4.1부터 TACACS가 WLC에서 지원됩니다. WLC의 관리 사용자를 인증하도록 TACACS+를 설정하는 방법을 이해하려면 TACACS+ 설정을 참조하십시오.

Q. WLC(Wireless LAN Controller)에서 과도한 인증 실패 설정은 어떻게 사용됩니까?

A. 이 설정은 클라이언트 예외 정책 중 하나입니다. 클라이언트 예외는 컨트롤러의 보안 기능입니다. 이 정책은 네트워크에 대한 불법적인 액세스 또는 무선 네트워크에 대한 공격을 방지하기 위해 클라이언트를 제외하는 데 사용됩니다.

이 과도한 웹 인증 실패 정책을 활성화한 상태에서 클라이언트의 웹 인증 실패 횟수가 5회를 초과하면 컨트롤러는 클라이언트가 최대 웹 인증 시도 횟수를 초과한 것으로 간주하고 클라이언트를 제외합니다.

이 설정을 활성화 또는 비활성화하려면 다음 단계를 완료하십시오.

1. WLC GUI에서 **Security > Wireless Protection Policies > Client Exclusion Policies**로 이동합니다.

2. **Excessive Web AuthenticationFailures**를 선택하거나 선택 취소합니다.

Q. 자동 액세스 포인트(AP)를 경량 모드로 전환했습니다. 클라이언트 계정 관리를 위해 AAA RADIUS 서버를 사용하는 LWAPP(Lightweight AP Protocol) 모드에서 일반적으로 클라이언트는 WLC의 IP 주소를 기반으로 RADIUS 계정 관리를 사용하여 추적됩니다. WLC의 IP 주소가 아니라 해당 WLC와 연결된 AP의 MAC 주소를 기반으로 RADIUS 계정 관리를 설정할 수 있습니까?

A. 예, 이 작업은 WLC 측 설정으로 수행할 수 있습니다. 다음 단계를 완료하십시오.

1. 컨트롤러 GUI의 **Security > Radius Accounting** 아래에 호출 스테이션 ID 유형에 대한 드롭다운 박스가 있습니다. **AP MAC Address**를 선택합니다.

2. LWAPP AP 로그를 통해 이를 확인합니다. 여기에서 특정 클라이언트가 연결된 AP의 MAC 주소를 표시하는 called-station ID 필드를 확인할 수 있습니다.

Q. CLI를 통해 WLC(Wireless LAN Controller)에서 WPA(Wi-Fi Protected Access) 핸드셰이크 시간 초과 값을 어떻게 변경합니까? **dot11 wpa handshake timeout value** 명령을 사용하여 Cisco IOS AP(액세스 포인트)에서 이 작업을 수행할 수 있지만, WLC에서는 이 작업을 어떻게 수행합니까?

A. WLC를 통해 WPA 핸드셰이크 시간 초과를 설정하는 기능은 소프트웨어 릴리스 4.2 이상에서 통합되었습니다. 이전 WLC 소프트웨어 버전에서는 이 옵션이 필요하지 않습니다.

다음 명령을 사용하여 WPA 핸드셰이크 시간 초과를 변경할 수 있습니다.

<#root>

```
config advanced eap eapol-key-timeout
```

<value>

```
config advanced eap eapol-key-retries
```

<value>

기본값은 WLC의 현재 동작을 계속 반영합니다.

- the default value for eapol-key-timeout is 1 second.
 - the default value for eapol-key-retries is 2 retries
-
-

참고: IOS AP에서는 dot11 wpa handshake 명령을 사용하여 이 설정을 구성할 수 있습니다.

config advanced eap 명령의 옵션을 사용하여 다른 EAP 매개변수를 설정할 수도 있습니다.

(Cisco Controller) >config advanced eap ?

```
eapol-key-timeout
  Configures EAPOL-Key Timeout in seconds.
eapol-key-retries
  Configures EAPOL-Key Max Retries.
identity-request-timeout
  Configures EAP-Identity-Request Timeout in seconds.
```

identity-request-retries

Configures EAP-Identity-Request Max Retries.

key-index

Configure the key index used for dynamic WEP(802.1x) unicast key (PTK).

max-login-ignore-identity-response

Configure to ignore the same username count reaching max in the EAP identity response

request-timeout

Configures EAP-Request Timeout in seconds.

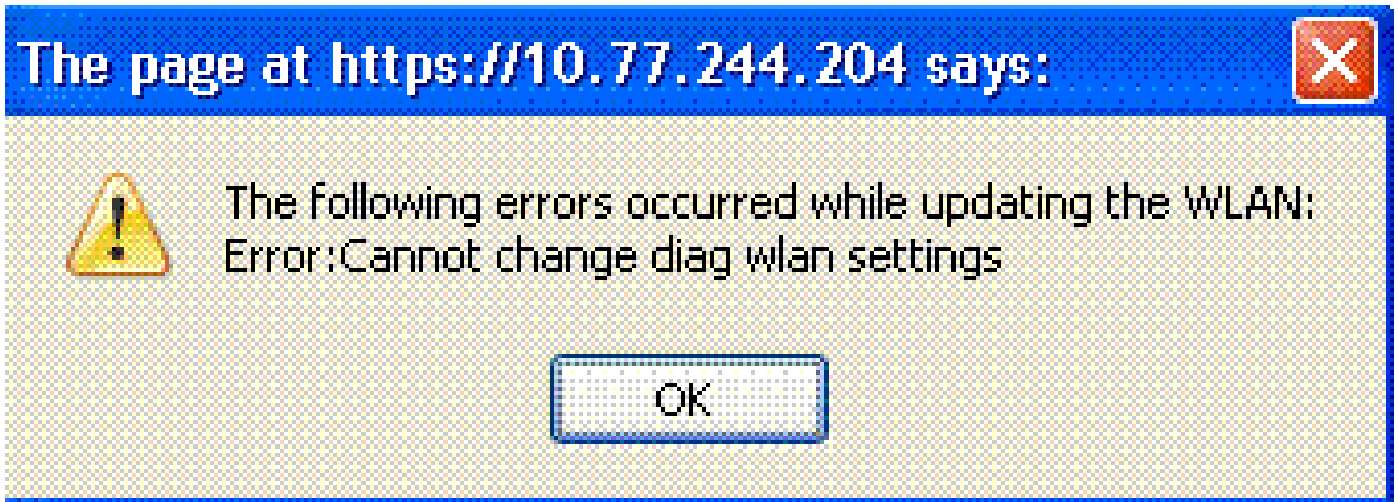
request-retries

Configures EAP-Request Max Retries.

Q. WLAN(WLAN) > Edit(편집) > Advanced(고급) 페이지에서 진단 채널 기능의 목적은 무엇입니까?

A. 진단 채널 기능을 사용하면 WLAN을 통한 클라이언트 통신과 관련된 문제를 해결할 수 있습니다. 클라이언트 및 액세스 포인트는 정의된 테스트 세트를 통해 클라이언트가 경험하는 통신 문제의 원인을 식별한 다음 클라이언트가 네트워크에서 작동하도록 수정 조치를 수행할 수 있습니다. 컨트롤러 GUI 또는 CLI를 사용하여 진단 채널을 활성화할 수 있으며, 컨트롤러 CLI 또는 WCS를 사용하여 진단 테스트를 실행할 수 있습니다.

진단 채널은 테스트에만 사용할 수 있습니다. 진단 채널이 활성화된 WLAN에 대한 인증 또는 암호화를 설정하려고 하면 다음 오류가 표시됩니다.



Q. WLC에서 구성할 수 있는 최대 AP 그룹 수는 몇 개입니까?

A. 이 목록에는 WLC에서 설정할 수 있는 최대 AP 그룹 수가 표시됩니다.

Cisco 2100 시리즈 컨트롤러 및 컨트롤러 네트워크 모듈의 경우 최대 50개의 액세스 포인트 그룹

•

Cisco 4400 시리즈 컨트롤러, Cisco WiSM, Cisco 3750G 무선 LAN 컨트롤러 스위치의 경우 최대 300개의 액세스 포인트 그룹

•

Cisco 5500 시리즈 컨트롤러의 경우 최대 500개의 액세스 포인트 그룹

관련 정보

- [WLC\(Wireless LAN Controller\) 오류 및 시스템 메시지 FAQ](#)
- [경량형 액세스 포인트 FAQ](#)
- [Wireless LAN Controller의 IPv6 지원](#)
- [무선 제품 지원](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.