지사에서 REAP 구축 설명서

목차

소개

이 문서에서는 REAP(Remote-Edge Access Point)를 구축할 때 고려해야 하는 정보를 제공합니다. 기본 REAP 구성 정보는 Lightweight AP 및 WLCs(Wireless LAN Controller) 컨피그레이션이 포함된 REAP(Remote-Edge AP)를 참조하십시오.

참고: REAP 기능은 WLC 릴리스 3.2.215까지 지원됩니다. WLC 릴리스 4.0.155.5에서 이 기능은 7.0.x.x.x까지 몇 가지 개선 사항이 포함된 Hybrid REAP(H-REAP)이라고 합니다.7.2.103 릴리스에서는 이 기능을 FlexConnect라고 합니다.

Cisco IOS® Software Release 12.3(7)JX 이상을 실행하는 1010, 1020, 1100 및 1200 Series AP와 같은 기존 Cisco LWAPP(Lightweight Access Point Protocol) 기반 액세스 포인트(LAP라고도 함) 기반 액세스 포인트(Cisco IOS)를 통해 중앙 집중식 관리 및 제어 가능 WLC(LAN 컨트롤러). 또한 이러한 LAP를 통해 관리자는 컨트롤러를 무선 데이터 집선의 단일 지점으로 활용할 수 있습니다.

이러한 LAP를 통해 컨트롤러는 QoS 및 ACL(Access Control List) 시행과 같은 고급 기능을 수행할 수 있지만, 모든 무선 클라이언트 트래픽에 대한 단일 인그레스 및 이그레스(egress)가 되어야 하는 컨트롤러 요구 사항은 사용자 요구 사항을 적절히 충족하는 기능을 활성화하지 않고 방해할 수 있습니다.원격 사무실과 같은 일부 환경에서는 컨트롤러에서 모든 사용자 데이터를 종료하면 대역폭이 너무 많이 소모될 수 있습니다. 특히 WAN 링크를 통해 제한된 처리량을 사용할 수 있는 경우 더욱 그렇습니다.또한 LAP와 WLC 간의 링크가 중단될 가능성이 높으며 원격 사무실에 대한 WAN 링크에서도 마찬가지로 일반적입니다. 사용자 데이터 종료에 WLC를 사용하는 LAP를 사용하면 WAN 중단 시 무선 연결이 끊깁니다.

대신 기존 LWAPP 컨트롤 플레인을 활용하여 동적 컨피그레이션 관리, AP 소프트웨어 업그레이드, 무선 침입 탐지 등의 작업을 수행할 수 있는 AP 아키텍처를 활용할 수 있습니다.이를 통해 무선 데이터는 로컬에서 유지되며, 무선 인프라는 WAN 중단에 대한 중앙 집중식 관리 및 복원력을 유지할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

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

1030 REAP 아키텍처 소개

Cisco 1030 REAP는 원격 기능을 제공하기 위해 LWAPP 컨트롤 플레인과 무선 데이터 플레인을 분리합니다.Cisco WLC는 여전히 일반 LAP와 같은 방식으로 중앙 집중식 제어 및 관리에 사용됩니다.차이점은 모든 사용자 데이터가 AP에서 로컬로 브리지된다는 것입니다.로컬 네트워크 리소스에 대한 액세스는 WAN 중단 시 유지됩니다.그림 1은 기본 REAP 아키텍처를 보여줍니다.

그림 1:기본 REAP 아키텍처 다이어그램

참고: 기존 LAP와 비교하여 REAP 기능의 기본 차이점 목록은 부록 A를 참조하십시오.

REAP AP는 언제 사용해야 합니까?

Cisco 1030 REAP AP는 주로 다음 두 가지 조건에서 사용해야 합니다.

- LAP와 WLC 간의 링크가 중단되기 쉬운 경우 1030 REAP를 사용하여 링크 장애 시 무선 사용

자가 무중단 데이터 액세스를 허용할 수 있습니다.

- 모든 사용자 데이터를 로컬에서 종료해야 하는 경우(다른 모든 LAP에 대한 데이터이므로 컨트롤러에서 종료되는 대신), 1030 REAP를 사용하여 컨트롤러 인터페이스 및/또는 WCS(Wireless Control System)를 통해 중앙 제어를 수행할 수 있습니다. 이렇게 하면 데이터가 로컬 상태로 유지됩니다.

커버리지 또는 사용자 밀도가 단일 사이트에서 2~3개 이상의 1030 REAP AP를 필요로 하는 경우 2006 또는 2106 WLC의 구축을 고려해 보십시오.이러한 컨트롤러는 모든 유형의 LAP를 최대 6개까지 지원할 수 있습니다.이는 재정적으로 더 효과적일 수 있으며, REAP 전용 구축과 비교할 때 뛰어난 기능 및 기능을 제공합니다.

모든 1000 Series AP와 마찬가지로 하나의 1030 AP는 약 5,000제곱피트입니다.이는 각 사이트의 RF(Radio Frequency) 전파 특성, 필요한 무선 사용자 수 및 처리량 요구 사항에 따라 달라집니다.대부분의 일반적인 구축에서 단일 1000 Series AP는 802.11b에서 512kbps의 사용자 12명을 지원하고 802.11a에서는 2mbps의 사용자 12명을 동시에 지원할 수 있습니다.모든 802.11 기반 기술과 마찬가지로 미디어 액세스가 공유됩니다.따라서 더 많은 사용자가 무선 AP에 가입하면 그에 따라 처리량이 공유됩니다.사용자 밀도가 증가하고 처리량 요구 사항이 증가함에 따라 사용자당 비용을 절감하고 기능을 향상하기 위해 로컬 WLC를 추가하는 것을 고려해 보십시오.

참고: 1030 REAP을 다른 LAP와 동일하게 작동하도록 구성할 수 있습니다.따라서 원격 사이트의 WLAN 인프라 크기를 확장하기 위해 WLC를 추가하면 기존 REAP 투자를 계속 활용할 수 있습니다.

REAP 구축

1030 REAP는 WLC 인프라에서 멀리 떨어진 원격 사이트에 배치되도록 설계되었으므로 컨트롤러를 검색하고 조인하는 데 사용되는 기존의 제로 터치 방식(zero-touch method) LAP(예: DHCP 옵션 43)는 일반적으로 사용되지 않습니다.대신, 1030이 중앙 사이트에서 WLC에 다시 연결할 수 있도록 하려면 먼저 LAP를 준비해야 합니다.

Priming(초기화)은 LAP에 연결할 수 있는 WLC 목록이 제공되는 프로세스입니다.단일 WLC에 가입하면 LAP는 모빌리티 그룹의 모든 컨트롤러에 대해 알려지며 그룹의 모든 컨트롤러에 조인하는 데 필요한 모든 정보를 제공합니다.모빌리티 그룹, 로드 밸런싱 및 컨트롤러 이중화에 대한 자세한 내용은 Cisco 440X Series Wireless LAN Controller 구축을 참조하십시오.

NOC(Network Operations Center) 또는 데이터 센터와 같은 중앙 사이트에서 이 작업을 수행하려면 REAP이 유선 네트워크에 연결되어야 합니다.이를 통해 단일 WLC를 검색할 수 있습니다.컨트롤러에 연결되면 LAP는 WLAN 인프라에 해당하는 LAP OS 버전을 다운로드합니다.그런 다음 모빌리티 그룹에 있는 모든 WLC의 IP 주소가 AP로 전송됩니다.이렇게 하면 AP가 원격 사이트에서 전원을 켜면 IP 연결을 사용할 수 있는 경우, AP가 목록에서 가장 활용도가 낮은 컨트롤러를 검색하고 조인할 수 있습니다.

참고: DHCP 옵션 43 및 DNS(Domain Name System) 조회는 REAP에서도 작동합니다.AP에서 중앙 컨트롤러를 찾을 수 있도록 원격 사이트에서 DHCP 또는 DNS를 구성하는 방법에 대한 자세한 내용은 Cisco 440X Series Wireless LAN Controller 구축을 참조하십시오.

이 시점에 필요한 경우 1030에 고정 주소를 지정할 수 있습니다.이렇게 하면 IP 주소 지정 체계가 대상 원격 사이트와 일치하게 됩니다.또한 각 LAP에서 연결을 시도할 3개의 컨트롤러를 자세히 설명하기 위해 WLC 이름을 입력할 수 있습니다.이 세 가지 장애가 발생하면 LWAPP의 자동 로드 밸런싱 기능을 통해 LAP는 클러스터에 있는 나머지 컨트롤러 목록에서 로드가 가장 적은 AP를 선택할 수 있습니다.LAP 컨피그레이션의 편집은 WLC CLI(Command-Line Interface) 또는 GUI를 통해 또는 WCS를 통해 보다 쉽게 수행할 수 있습니다.

참고: 1030 REAP은 연결되는 WLC가 레이어 3 LWAPP 모드에서 작동해야 합니다.즉, 컨트롤러에 IP 주소를 지정해야 합니다.또한 WLC를 사용하려면 각 원격 사이트에서 DHCP 서버를 사용할 수 있어야 합니다. 그렇지 않으면 고정 주소를 할당해야 합니다.컨트롤러에 내장된 DHCP 기능은 1030s LAP 또는 해당 사용자에게 주소를 제공하는 데 사용할 수 없습니다.

1030 LAP의 전원을 끄고 원격 사이트로 배송하기 전에 각 1030이 REAP 모드로 설정되어 있는지 확인합니다.모든 LAP의 기본값은 일반 로컬 기능을 수행하는 것이고 1030은 REAP 기능을 수행하도록 설정해야 하기 때문에 이는 매우 중요합니다.이 작업은 컨트롤러 CLI 또는 GUI를 통해 LAP 레벨에서 수행하거나 WCS 템플릿을 통해 더욱 쉽게 수행할 수 있습니다.

기본 REAP Priming 기능

1030개의 REAP가 원격 사이트에 배치될 때 REAP가 연결되는 모빌리티 그룹 내의 WLC에 연결되면 다음 정보를 제공할 수 있습니다.

필수 REAP 설정

- 모빌리티 그룹의 WLC에 대한 IP 주소 목록(컨트롤러/AP 연결 시 자동으로 제공)
- REAP AP 모드(REAP 기능을 수행하려면 REAP 모드에서 작동하도록 AP를 구성해야 함)

선택적 REAP 설정

- 정적으로 할당된 IP 주소(AP별로 선택적 설정 입력)
- 기본, 보조 및 3차 WLC 이름(AP별로 또는 WCS 템플릿을 통해 선택적으로 설정 입력)
- AP 이름(AP별로 선택적으로 정보 설정 입력)
- AP 위치 정보(AP별 또는 WCS 템플릿을 통한 선택적 정보 설정 입력)

REAP-to-Controller 링크 요구 사항

REAP을 구축할 계획이라면 몇 가지 기본 요구 사항을 기억해야 합니다.이러한 요구 사항은 REAP LWAPP 제어 트래픽이 통과할 WAN 링크의 속도와 레이턴시에 대해 우려합니다.1030 LAP는 IP 보안 터널, 프레임 릴레이, DSL(비 PPPoE) 및 임대 회선 등 WAN 링크 전체에서 사용됩니다.

참고: 1030 REAP LWAPP 구현에서는 AP와 WLC 간의 1500바이트 MTU 경로를 가정합니다.하위 1500바이트 MTU로 인해 전송 중에 발생하는 프래그먼트화는 예측할 수 없는 결과를 초래합니다.따라서 1030 LAP는 라우터가 사전 대응적으로 패킷을 1500바이트 미만으로 프래그먼트화하는 PPPoE와 같은 환경에 적합하지 않습니다.

WAN 링크 레이턴시는 특히 중요합니다. 1030 LAP마다 기본적으로 하트비트 메시지를 컨트롤러에 30초마다 다시 보내기 때문입니다.하트비트 메시지가 손실되면 LAP는 초당 한 번씩 5개의 연속적인 하트비트를 전송합니다.아무 것도 성공하지 못하면 LAP는 컨트롤러 연결이 끊어진 것으로 확인하고 1030은 독립형 REAP 모드로 돌아갑니다.1030 LAP는 자체와 WLC 사이의 레이턴시를 허용할 수 있지만 레이턴시가 LAP와 컨트롤러 사이의 100ms를 초과하지 않도록 해야 합니다.이는 타이머가 인증에 실패했음을 확인하기 전에 클라이언트가 대기하는 시간을 제한하는 클라이언트측 타이머 때문입니다.

REAP 제한 사항

1030 AP는 중앙 집중식으로 관리되도록 설계되었으며 WAN 링크 중단 시 WLAN 서비스를 제공하

도록 설계되었지만, LEAF가 WLC 연결을 통해 제공하는 서비스와 연결이 끊어질 때 제공할 수 있는 서비스 사이에는 몇 가지 차이점이 있습니다.

WLAN

1030 REAP는 최대 16개의 WLAN(모든 보안, QoS 및 기타 정책과 함께 각각 SSID(Service Set Identifier)가 포함된 무선 프로파일)을 지원할 수 있지만, 각각 MBSSID(Multiple Basic Service Set ID)가 있는 1030 REAP는 컨트롤러와의 연결이 중단된 경우에만 첫 번째 WLAN을 지원할 수 있습니다.WAN 링크 중단 시 첫 번째 WLAN을 제외한 모든 WLAN은 서비스 해제됩니다.따라서 WLAN 1은 기본 WLAN 및 보안 정책을 적절하게 계획해야 합니다.WAN 링크가 실패할 경우 백엔드 RADIUS 인증도 실패하므로 이 첫 번째 WLAN의 보안이 특히 중요합니다.이는 이러한 트래픽이 LWAPP 컨트롤러 플레인을 통과하기 때문입니다.따라서 어떤 사용자도 무선 액세스 권한을 부여받지 않습니다.

이 첫 번째 WLAN에서는 WPA-PSK(Wi-Fi Protected Access)의 사전 공유 키 부분과 같은 로컬 인증/암호화 방법을 사용하는 것이 좋습니다.WEP(Wired Equivalent Privacy)는 충분하지만 알려진 보안 취약성 때문에 권장되지 않습니다.WPA-PSK(또는 WEP)를 사용할 경우, WAN 링크가 다운되더라도 올바르게 구성된 사용자가 로컬 네트워크 리소스에 액세스할 수 있습니다.

참고: 모든 RADIUS 기반 보안 방법에서는 LWAPP 컨트롤 플레인을 통해 중앙 사이트로 다시 인증 메시지를 전송해야 합니다.따라서 WAN 중단 시 모든 RADIUS 기반 서비스를 사용할 수 없습니다.여기에는 RADIUS 기반 MAC 인증, 802.1X, WPA, WPA2 및 802.11i가 포함되지만 이에 국한되지 않습니다.

1030 REAP는 802.1q VLAN 태깅을 수행할 수 없으므로 단일 서브넷에만 상주할 수 있습니다.따라서 각 SSID의 트래픽은 유선 네트워크의 동일한 서브넷에서 종료됩니다.즉, 무선 트래픽이 SSID 간 공기 중에 분할될 수 있지만 사용자 트래픽은 유선 측에서 분리되지 않습니다.

보안

1030 REAP는 Cisco의 컨트롤러 기반 WAN 아키텍처에서 지원하는 모든 레이어 2 보안 정책을 제공할 수 있습니다.여기에는 WEP, 802.1X, WPA, WPA2 및 802.11i와 같은 모든 레이어 2 인증 및 암호화 유형이 포함됩니다.앞서 설명한 것처럼 이러한 보안 정책의 대부분은 백엔드 인증을 위해 WLC 연결이 필요합니다.WEP 및 WPA-PSK는 AP 수준에서 완전히 구현되며 백엔드 RADIUS 인증이 필요하지 않습니다.따라서 WAN 링크가 중단되더라도 사용자는 계속 연결할 수 있습니다.Cisco WLC에 제공된 클라이언트 제외 목록 기능은 1030 LAP에서 지원됩니다.컨트롤러에 다시 연결할 수 있는 경우 MAC 필터링 기능은 1030에서 작동합니다.

참고: AP가 독립형 모드인 경우 REAP는 WPA2-PSK를 지원하지 않습니다.

1030 LAP에서는 모든 레이어 3 보안 정책을 사용할 수 없습니다.이러한 보안 정책에는 웹 인증, 컨트롤러 기반 VPN 종료, ACL, 피어 투 피어 차단 등이 포함됩니다. 이는 컨트롤러에서 구현되기 때문입니다.VPN Pass-Through는 외부 VPN 집중장치에 연결하는 클라이언트에 대해 작동합니다.그러나 지정된 VPN Concentrator(VPN Pass-Through 전용)로 향하는 트래픽만 허용하는 컨트롤러 기능은 그렇지 않습니다.

NAT(Network Address Translation)

REAP이 연결되는 WLC는 NAT 경계 뒤에 상주할 수 없습니다.그러나 LWAPP에 사용되는 포트(UDP 포트 12222 및 12223)가 1030s로 포워딩되는 경우 원격 사이트의 REAP은 NAT 상자 뒤에 상주할 수 있습니다.즉, 포트 전달이 안정적으로 작동하려면 각 REAP에 고정 주소가 있어야 하며,

각 NAT 인스턴스 뒤에는 단일 AP만 있을 수 있습니다.이유는 NAT IP 주소당 단일 포트 전달 인스턴스만 존재할 수 있기 때문입니다. 즉, 원격 사이트의 각 NAT 서비스 뒤에서 하나의 LAP만 작동할 수 있습니다.각 외부 IP 주소에 대해 LWAPP 포트를 각 내부 IP 주소(고정 REAP IP 주소)로 전달할 수 있으므로 일대일 NAT는 여러 REAP에서 작동할 수 있습니다.

QoS(Quality of Service)

802.1p 우선순위 비트를 기반으로 한 패킷 우선 순위는 REAP에서 802.1q 태깅을 수행할 수 없으므로 사용할 수 없습니다.즉, WMM(Wi-Fi Multimedia) 및 802.11e는 지원되지 않습니다.SSID 및 ID 기반 네트워킹을 기반으로 하는 패킷 우선 순위가 지원됩니다.그러나 ID 기반 네트워킹을 통한 VLAN 할당은 802.1q 태깅을 수행할 수 없으므로 REAP에서 작동하지 않습니다.

로밍 및 클라이언트 로드 밸런싱

단일 REAP가 하나 이상 있고 AP 간 이동성이 예상되는 환경에서는 각 LAP가 동일한 서브넷에 있어야 합니다.레이어 3 모빌리티는 1030 LAP에서 지원되지 않습니다.일반적으로 원격 사무소는 이러한 유연성을 필요로 할 만큼 충분한 LAP를 사용하지 않기 때문에 이러한 제한이 없습니다.

업스트림 컨트롤러 연결을 사용할 수 있는 경우(호스트 컨트롤러에서만 로드 밸런싱이 활성화됨) 단일 AP를 초과하는 사이트의 모든 REAP에 적극적인 클라이언트 로드 밸런싱이 제공됩니다.

RRM(Radio Resource Management)

컨트롤러에 대한 연결이 있는 경우 1030 LAP는 WLC의 RRM 메커니즘에서 동적 채널 및 전원 출력을 받습니다.WAN 링크가 다운되면 RRM이 작동하지 않으며 채널 및 전원 설정이 변경되지 않습니다.

비인가 탐지 및 IDS 기능

REAP 아키텍처는 일반 LAP와 일치하는 모든 비인가 탐지 및 침입 탐지 시그니처(IDS)를 지원합니다.그러나 중앙 컨트롤러와의 연결이 끊기면 수집된 모든 정보가 공유되지 않습니다.따라서 원격 사이트의 RF 도메인에 대한 가시성이 손실됩니다.

REAP 제한 요약

부록 B의 표는 정상 작동 중에 REAP의 기능을 요약하며, WAN 링크를 통해 WLC에 연결할 수 없는 경우

REAP 및 중앙 WLAN 아키텍처 관리

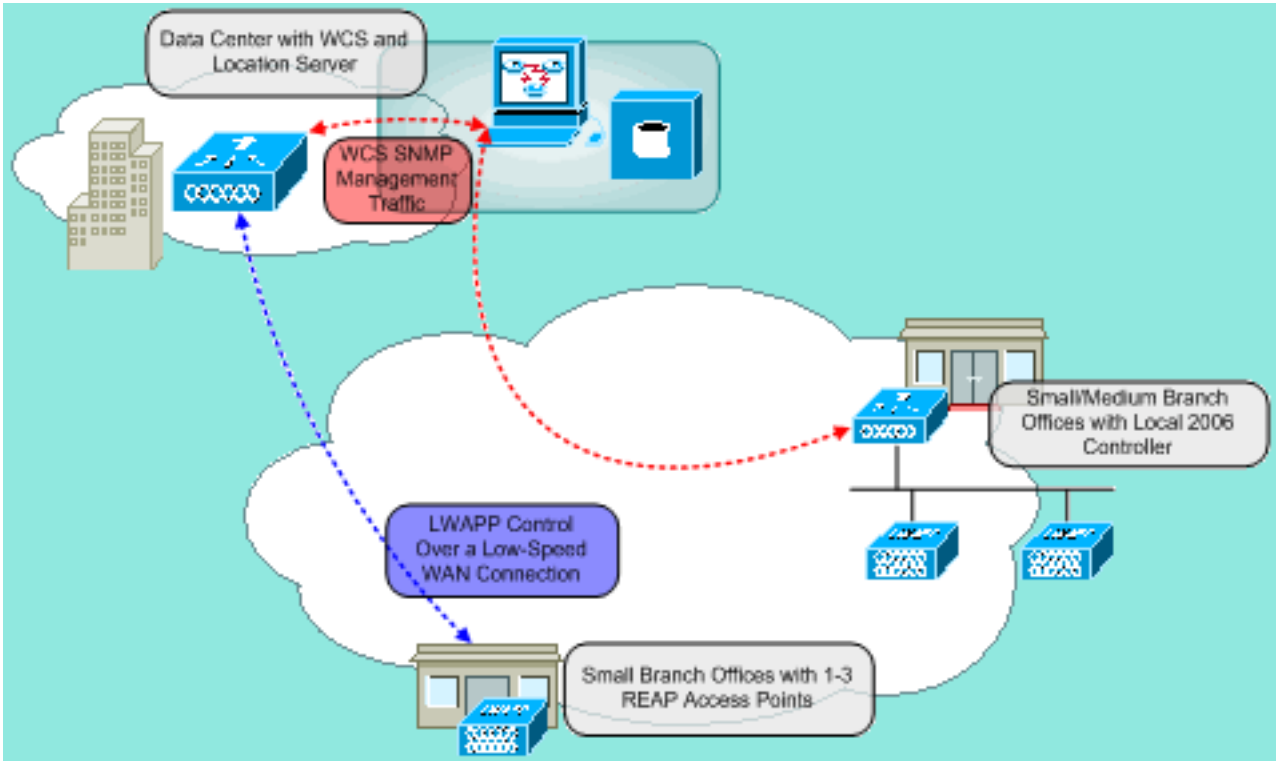
1030 REAP 관리는 일반 LAP 및 WLC의 관리 방식과 다르지 않습니다.관리 및 컨피그레이션은 각 컨트롤러 또는 웹 GUI의 CLI를 통해 컨트롤러 수준에서 모두 수행됩니다.시스템 차원의 컨피그레이션 및 네트워크 가시성은 WCS를 통해 제공되며, 여기서 모든 컨트롤러 및 AP(REAP 등)는 단일 시스템으로 관리할 수 있습니다.REAP 컨트롤러 연결이 중단되면 관리 기능도 중단됩니다.

REAP을 사용하는 중앙 집중식 WLAN 아키텍처

그림 2는 다양한 무선 네트워킹 요구 사항을 충족하기 위해 중앙 집중식 LWAPP 아키텍처의 각 부분이 어떻게 연동되는지 보여줍니다.관리 및 위치 서비스는 WCS 및 2700 Location Appliance를 통

해 중앙에서 제공됩니다.

그림 2:REAP을 사용하는 중앙 집중식 WLAN 아키텍처



부록 A

REAP 아키텍처와 일반 LAP의 주요 차이점은 무엇입니까?

- 원격 사이트에서 DHCP 옵션 43 또는 DNS 확인을 사용할 수 없는 경우 먼저 중앙 사무실에서 1030을 준비해야 합니다.그런 다음 목적지 사이트로 배송됩니다.
- WAN 링크 장애 시 첫 번째 WLAN만 활성 상태로 유지됩니다.RADIUS가 필요한 보안 정책이 실패합니다.WLAN 1에는 WPA-PSK를 사용하는 인증/암호화가 권장됩니다. WEP는 작동하지만 권장되지는 않습니다.
- 레이어 3 암호화 없음(레이어 2 암호화만 해당)
- REAP이 연결되는 WLC는 NAT 경계 뒤에 상주할 수 없습니다.그러나 각 내부 고정 REAP IP 주소에 LWAPP 포트(1222 및 12223)가 모두 전달되어 있는 경우 REAP은 LEAF를 수 있습니다.**참고:** LAP에서 시작되는 LWAPP 트래픽의 소스 포트는 시간이 지남에 따라 변경될 수 있으므로 오버로딩된 PAT(Port Address Translation)/NAT가 지원되지 않습니다.그러면 LWAPP 연결이 끊어집니다.PIX/ASA와 같은 포트 주소가 변경될 수 있는 REAP에 대한 NAT 구현에서도 동일한 문제가 발생할 수 있습니다. 이는 컨피그레이션에 따라 다릅니다.
- LWAPP 제어 메시지만 WAN 링크를 통과합니다.
- 데이터 트래픽은 1030의 이더넷 포트에서 브리지됩니다.
- 1030 LAP는 802.1Q 태깅(VLAN)을 수행하지 않습니다. 따라서 모든 SSID의 무선 트래픽은 동일한 유선 서브넷에서 종료됩니다.

부록 B

일반 REAP 모드와 독립형 REAP 모드 간의 기능에는 어떤 차이가 있습니까?

		REAP(일반 모드)	REAP(독립형 모드)
프로토콜	IPv4	예	예
	IPv6	예	예
	기타 모든 프로토콜	예(클라이언트가 IP도 활성화된 경우에만)	예(클라이언트가 IP도 활성화된 경우에만)
	IP 프록시 ARP	아니요	아니요
WLAN	SSID 수	16	1(첫 번째 항목)
	동적 채널 할당	예	아니요
	동적 전원 제어	예	아니요
	동적 로드 밸런싱	예	아니요
VLAN	다중 인터페이스	아니요	아니요
	802.1Q 지원	아니요	아니요
WLAN 보안	비인가 AP 탐지	예	아니요
	제외 목록	예	예(기존 구성원만 해당)
	P2P 차단	아니요	아니요
	침입 탐지 시스템	예	아니요
레이어 2 보안	MAC 인증	예	아니요
	802.1X	예	아니요
	WEP(64/128/152비트)	예	예
	WPA-PSK	예	예
	WPA2-PSK	예	아니요
	WPA-EAP	예	아니요
	WPA2-EAP	예	아니요
레이어 3 보안	웹 인증	아니요	아니요
	IPsec	아니요	아니요
	L2TP	아니요	아니요
	VPN 통과	아니요	아니요
	액세스 제어 목록	아니요	아니요
QoS	QoS 프로파일	예	예

	다운링크 QoS(가중 라운드 로빈 대기열)	예	예
	802.1p 지원	아니요	아니요
	사용자별 대역폭 계약	아니요	아니요
	WMM	아니요	아니요
	802.11e(미래)	아니요	아니요
	AAA QoS 프로파일 재정의	예	아니요
모빌리티	서브넷 내	예	예
	서브넷 간	아니요	아니요
DHCP	내부 DHCP 서버	아니요	아니요
	외부 DHCP 서버	예	예
토폴로지	직접 연결(2006)	아니요	아니요

관련 정보

- 경량형 AP 및 WLC(Wireless LAN Controller)를 사용한 REAP(Remote-Edge AP) 컨피그레이션 예
- 통합 무선 네트워크의 AP 로드 밸런싱 및 AP 대체
- Cisco 440X Series Wireless LAN Controller 구축
- 무선 LAN 컨트롤러 및 경량 액세스 포인트 기본 구성 예
- 기술 지원 및 문서 – Cisco Systems