설계 가이드 CX - 대규모 공용 네트워크용 무선

목차

소개

이 문서에서는 대규모 공용 Wi-Fi 네트워크의 설계 및 구성 지침에 대해 설명합니다.

CX 설계 가이드

CX 설계 가이드는 Cisco TAC(Technical Assistance Center) 및 Cisco PS(Professional Services)의 전문가가 작성하고 Cisco의 전문가가 동료와 함께 검토하며, Cisco의 선도적인 사례, 수년 동안 수많은 고객이 구현하여 얻은 지식과 경험을 바탕으로 합니다. 이 문서의 권장 사항에 따라 설계 및 구성된 네트워크는 일반적인 위험을 방지하고 네트워크 운영을 개선하는 데 도움이 됩니다.

범위 및 정의

이 문서에서는 대규모 공용 무선 네트워크의 설계 및 구성 지침을 제공합니다.

정의: 대규모 공용 네트워크 - 고밀도의 무선 구축으로 수천 개의 알 수 없는 클라이언트 장치 및/또는 관리되지 않는 클라이언트 장치에 대한 네트워크 연결을 제공합니다.

이 문서에서는 종종 대상 네트워크가 대규모 및/또는 임시 이벤트에 서비스를 제공한다고 가정합니다. 또한 많은 방문객을 맞이하는 장소의 고정 영구 네트워크에도 적합합니다. 예를 들어, 쇼핑몰이나 공항은 경기장 또는 콘서트 장의 Wi-Fi 네트워크와 유사성이 있습니다. 최종 사용자에 대한 통제가 없다는 점에서 이러한 네트워크는 일반적으로 네트워크에 몇 시간 또는 하루 동안만 존재합니다.

대규모 행사나 장소의 무선 지원 범위에는 자체 요구 사항 집합이 있습니다. 이러한 요구 사항은 엔

터프라이즈, 제조 또는 대규모 교육 네트워크와는 다른 경향이 있습니다. 대규모 공용 네트워크에는 수천 명의 사용자가 있을 수 있으며 한 개 또는 몇 개의 건물에만 집중되어 있습니다. 클라이언트 로밍이 매우 빈번할 수 있으며, 끊임없이 또는 피크 시간 동안 발생할 수 있으며, 또한 네트워크는 클라이언트 장치 구성이나 보안에 대한 제어 없이 무선 클라이언트 장치에서 가능한 모든 것과 호환되어야 합니다.

이 가이드에서는 고집적도에 대한 일반적인 RF 개념과 구현 세부 사항을 소개합니다. 이 가이드의 대부분의 라디오 개념은 Cisco Meraki를 비롯한 모든 고밀도 네트워크에 적용됩니다. 그러나 구현 세부 사항 및 컨피그레이션은 Catalyst 9800 Wireless Controller를 사용하는 Catalyst Wireless에 중점을 두며, 이는 현재 대규모 공용 네트워크에 구축되어 있는 가장 일반적인 솔루션입니다.

이 문서에서는 무선 컨트롤러와 WLC(Wireless LAN Controller)라는 용어를 서로 바꿔 사용합니다.

대규모 공용 네트워크

대규모 공용 및 이벤트 네트워크는 여러 측면에서 고유한 특성을 갖고 있습니다. 이 문서에서는 이러한 주요 영역에 대해 살펴보고 지침을 제공합니다.

- 대규모 공용 네트워크는 매우 복잡합니다. 줄어든 RF(Radio Frequency) 공간에 수천 개의 디바이스가 있고 사람들이 걸어 다니면서 상당한 로밍이 이루어집니다. 일부 이벤트와 장소는 매우 특정 시간에 대역폭 피크가 발생하면서 더 정적일 수 있습니다. 인프라는 해당 지역으로 들어오고 이동하는 클라이언트에 대해 가능한 한 모든 상태 변경을 적절하게 처리해야 합니다.
- 핵심 우선 순위는 온보딩의 용이성입니다. 연결된 클라이언트는 행복한 클라이언트입니다. 즉, 클라이언트를 최대한 빨리 네트워크에 연결해야 합니다. Wi-Fi에 연결되지 않은 클라이언트는 사용 가능한 액세스 포인트를 스캔하여 원치 않는 RF 에너지를 발생시키며, 이는 추가적인 정체 및 대기 중 용량 손실로 이어집니다.
- RF 구축은 최대한 신중하게 설계해야 합니다. 매우 높은 밀도가 요구되거나 베뉴에 넓은 개방 공간 및/또는 높은 천장이 있는 경우 지향성 안테나를 사용하는 적절한 RF 설계가 필수적입니다.
- 또 다른 주요 설계 드라이브는 호환성입니다. 일부 기능은 802.11 사양의 표준이며, 다른 기능은 독점적이며, 클라이언트에 문제가 되지 않습니다. 그러나 현실은 다르며 복잡한 신호나 이해하지 못하는 기능/설정을 볼 때 제대로 프로그래밍되지 않은 클라이언트 드라이버가 많이 있습니다.
- 확장 및 시간 제한으로 인해 트러블슈팅이 어렵습니다. 특정 클라이언트에서 문제가 해결되지 않으면 해당 최종 사용자와 협력하여 문제를 파악할 수 없습니다. 이용자는 찾기가 어려울 수 있지만, 행사장 방문이라는 일시적인 특성상 비협조적일 수도 있다.
- 보안은 중요한 요소입니다. 게스트 방문자의 수가 매우 많고 공격 표면이 훨씬 넓기 때문에 제어력이 떨어집니다.

외부 참조

문서 이름	소스	위치
Cisco Catalyst 9800 Series 구성 모범 사례	Cisco	링크

문서 이름	소스	위치
무선 LAN 컨트롤러 CPU 문제 해결	Cisco	링크
Wi-Fi 처리량 검증: 테스트 및 모니터링 가이드	Cisco	링크
Cisco Catalyst CW9166D1 Access Point 구축 설명서	Cisco	링크
Catalyst 9104 Stadium Antenna(C-ANT9104) 구축 설명서	Cisco	링크
Catalyst 9800 KPI 모니터링(핵심 성과 지표)	Cisco	링크
Catalyst 9800 클라이언트 연결 문제 해결 흐름	Cisco	링크
Cisco Catalyst 9800 Series Wireless Controller 소프트웨어 컨피그레이션 가이드(17.12)	Cisco	링크
Wi-Fi 6E: Wi-Fi 백서의 다음 장	Cisco	링크

면책조항

이 문서에서는 다양한 구축에서 얻은 특정 시나리오, 가정 및 지식을 기반으로 한 권장 사항을 제공합니다. 그러나 사용자는 네트워크 설계, 비즈니스, 규정 준수, 보안, 개인 정보 및 기타 요구 사항(이 가이드에 제공된 지침 또는 권장 사항의 준수 여부 포함)을 결정할 책임이 있습니다.

네트워크 설계

RF 고려 사항

장소 유형

이 설명서는 일반적으로 공개되며 최종 사용자 및 클라이언트 디바이스 유형에 대한 제한적 제어와 함께 대규모 게스트 네트워크에 초점을 맞춥니다. 이러한 유형의 네트워크는 다양한 위치에 구축할 수 있으며, 임시적일 수도 있고 영구적일 수도 있습니다. 주요 활용 사례는 대개 방문자에게 인터넷 액세스를 제공하는 것이지만, 이는 거의 유일한 활용 사례는 아닙니다.

일반적인 위치:

- 경기장 및 경기장
- 회의 장소

- 대강당

RF 관점에서, 이러한 위치 유형들 각각은 고유의 뉘앙스 세트를 갖는다. 이러한 사례는 대개 회의 장소를 제외하고 영구 설치입니다. 이는 영구 설치이거나 임시로 특정 무역 박람회에 설치할 수 있기 때문입니다.

기타 위치:

- 유람선
- 공항
- 쇼핑 센터 / 몰

공항과 크루즈 선박도 대형 공용 네트워크의 범주에 맞는 구축 사례입니다. 그러나 각 사례에 대해 추가적인 고려 사항이 있으며 내부 전방위 AP를 사용하는 경우가 많습니다.

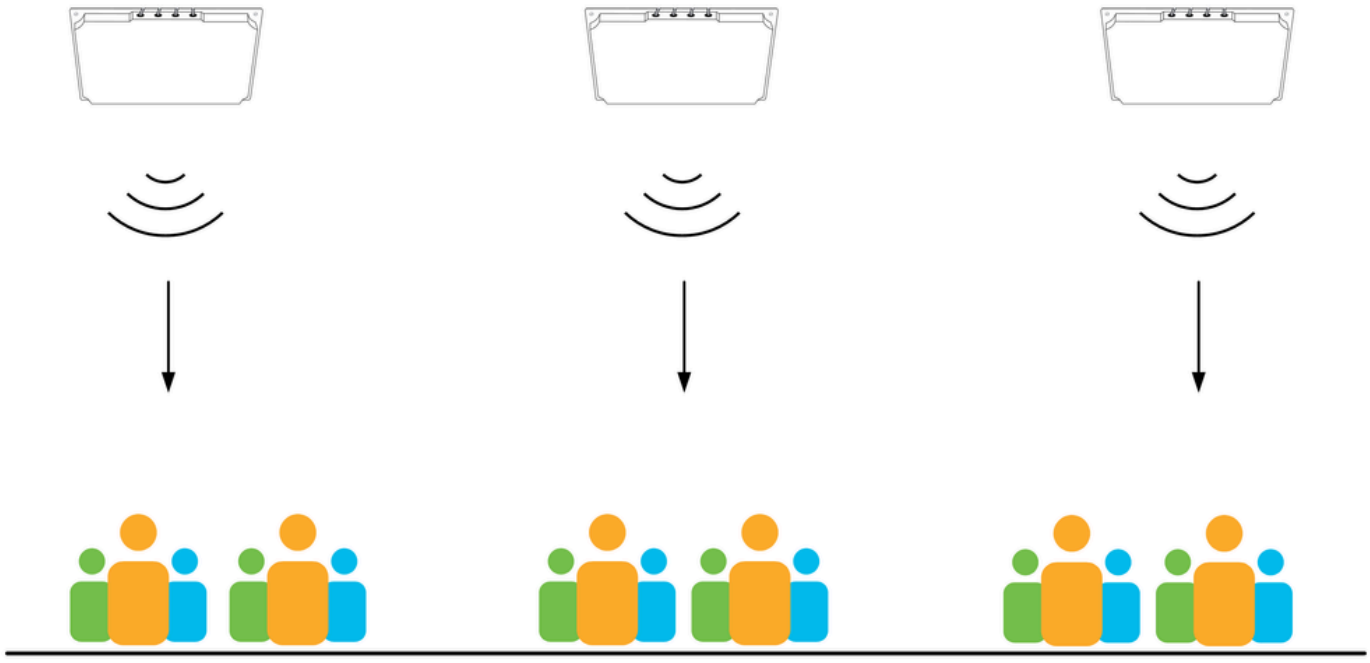
커버리지 전략

커버리지 전략은 주로 베뉴 유형, 사용되는 안테나 및 사용 가능한 안테나 장착 위치에 따라 달라집니다.

오버헤드

오버헤드 범위는 가능한 경우 항상 선호됩니다.

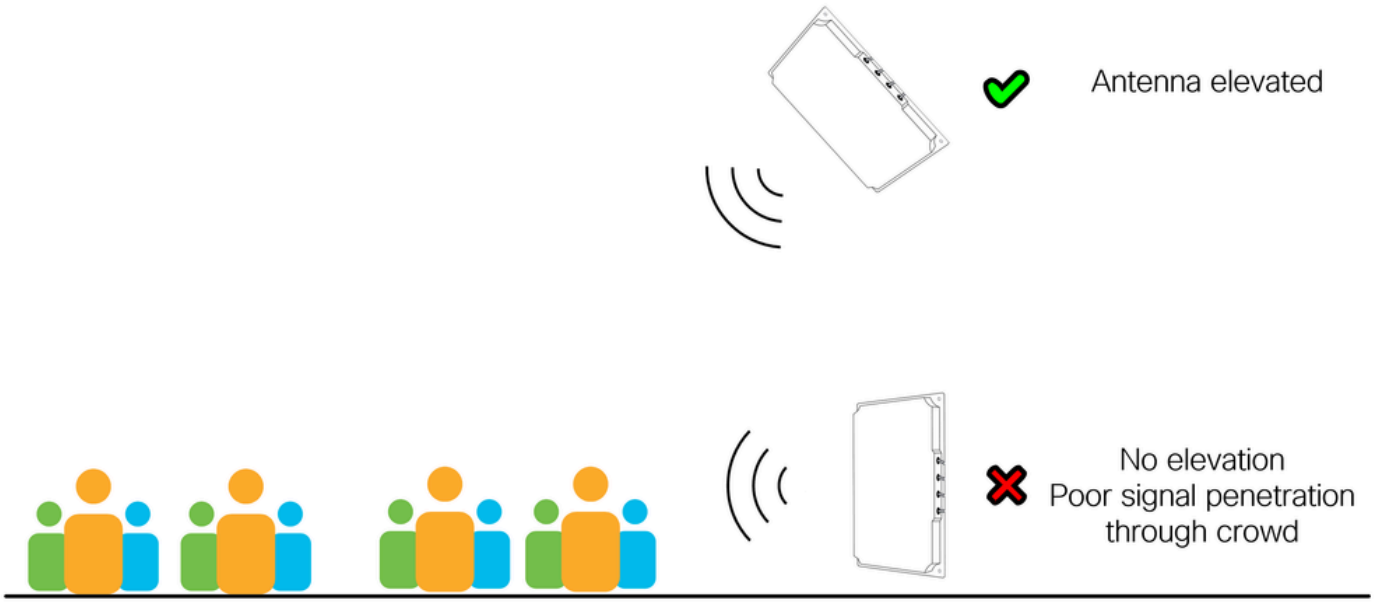
오버헤드 솔루션은 복잡한 시나리오에서도 일반적으로 모든 클라이언트 장치가 안테나 오버헤드에 대해 직접적인 가시선을 갖는다는 뚜렷한 장점을 가지고 있습니다. 지향성 안테나를 사용하는 오버헤드 솔루션은 무선 조정 관점에서 복잡성을 줄이는 동시에 뛰어난 로드 밸런싱 및 클라이언트 로밍 특성을 제공하기 위해 보다 잘 제어되고 잘 정의된 커버리지 영역을 제공합니다. 자세한 내용은 Power Balance 섹션을 참조하십시오.



클라이언트 위의 AP

측면

측면 장착형 지향성 안테나는 널리 사용되는 선택이며 다양한 시나리오, 특히 높이 또는 장착 제한으로 인해 오버헤드 장착이 불가능한 경우에 적합합니다. 측면 장착을 사용할 때 안테나가 커버하는 영역의 유형을 이해하는 것이 중요합니다. 예를 들어 개방형 실외 영역인지 아니면 밀집된 실내 영역인지 등을 파악해야 합니다. 커버리지 영역이 사람이 많은 고밀도 영역이라면 인간 군중을 통한 신호 전파가 항상 빈약한 만큼 안테나를 최대한 높여야 한다. 대부분의 모바일 장치는 사용자의 머리 위쪽이 아닌 허리 아래쪽에서 사용된다는 점을 기억하십시오! 안테나의 높이는 커버리지 영역이 더 낮은 밀도 영역이면 덜 중대하다.



안테나 고도가 항상 더 우수함

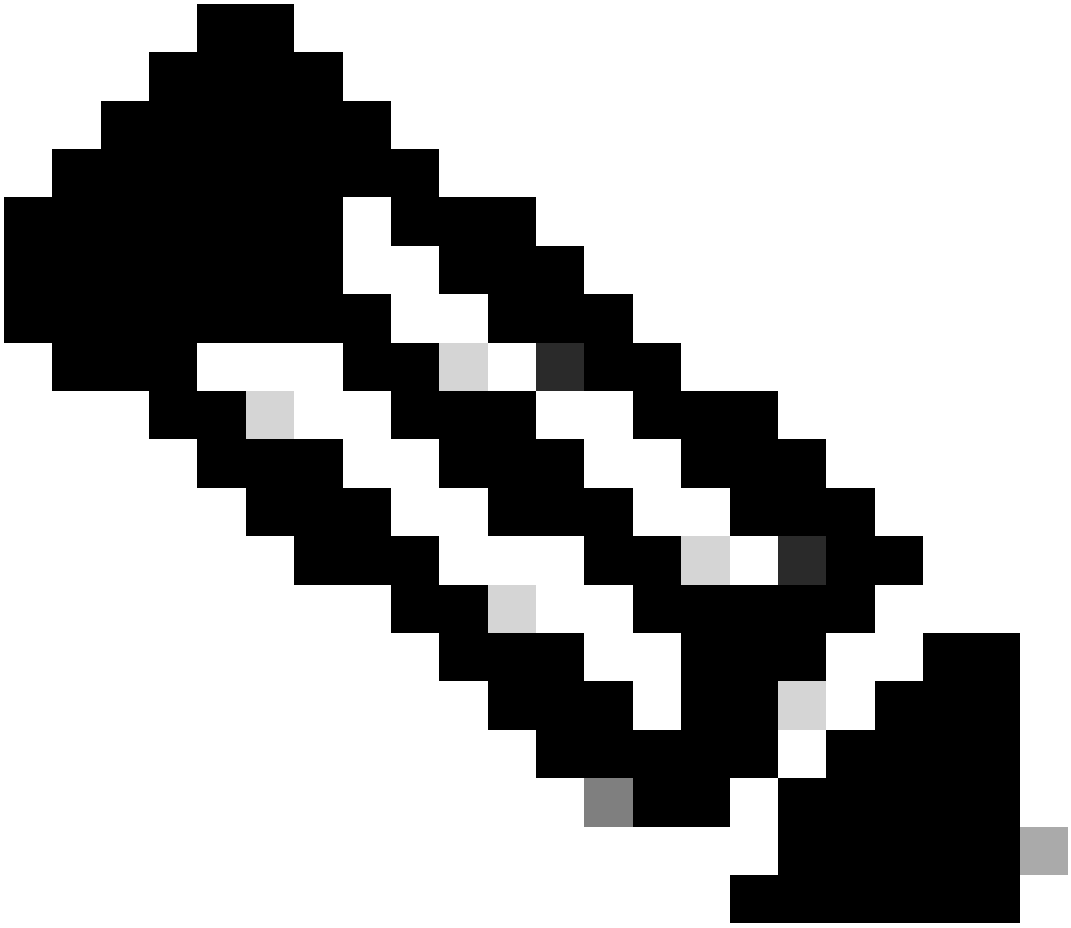
전방향

옴니 안테나(내부 또는 외부)는 매우 고밀도 시나리오에서 일반적으로 사용하지 않아야 하며, 이는 공동 채널 간섭에 대한 영향이 잠재적으로 크기 때문입니다. 옴니 안테나는 6m 이상의 높이에서 사용하지 않아야 합니다(고이득 실외기에서는 적용되지 않음).

하부 좌석

일부 경기장 또는 경기장에는 적절한 안테나 장착 위치가 없는 상황이 있을 수 있습니다. 마지막으로 남은 대안은 사용자가 앉아 있는 좌석 아래에 AP를 위치시켜 아래에서 커버리지를 제공하는 것입니다. 이러한 유형의 솔루션은 올바르게 구축하기가 더 어려우며 일반적으로 AP와 특정 설치 절차를 상당히 더 많이 수행해야 하므로 비용이 더 많이 듭니다.

좌석 미달 배치의 주요 과제는 전체 장소와 빈 장소의 커버리지에 큰 차이가 있습니다. 인체는 무선 신호를 감쇠하는 데 매우 효율적입니다. 즉, AP를 둘러싸고 있는 사람이 많을 경우 그에 따른 커버리지는 해당 사람이 없을 때보다 훨씬 작습니다. 이 인간 군중 감소 인자를 통해 더 많은 AP를 구축할 수 있으므로 전체 용량이 증가할 수 있습니다. 그러나 장소가 비어 있으면 인체의 감쇄가 없고 상당한 간섭이 일어나며, 이는 장소가 일부 가득 찰 때 합병증을 초래한다.



참고: 사용자 수에 따른 구축은 타당하지만 일반적이지 않은 해결책이므로 사례별로 평가해야 합니다. 이 문서에서는 언더시트(under-seat) 구축에 대해 자세히 설명하지 않습니다.

미학

일부 구축에서는 미학에 대한 질문이 등장합니다. 이러한 영역은 특정 아키텍처 설계, 역사적 가치가 있는 영역이거나 장비를 장착할 수 있는(또는 장착할 수 없는) 광고 및/또는 브랜딩이 필요한 공간일 수 있습니다. 특정 솔루션을 사용하여 배치 제한을 해결할 수 있습니다. 이러한 해결 방법 중 일부에는 AP/안테나 숨기기, AP/안테나 페인팅, 장비 인클로저 장착 또는 다른 위치 사용이 포함됩니다. 안테나를 페인트하려면 항상 비금속 페인트를 사용하십시오. Cisco는 일반적으로 안테나용 인클로저를 판매하지 않지만, 여러 공급업체를 통해 쉽게 사용할 수 있는 것이 많습니다.

이러한 모든 해결 방법은 네트워크의 성능에 영향을 미칩니다. 무선 설계자는 항상 최적의 무선 커버리지를 위해 최적의 마운팅 위치를 제안하는 것으로 시작하며, 이러한 초기 위치는 일반적으로 최상의 성능을 제공합니다. 이러한 위치를 변경하면 안테나를 최적의 위치에서 멀리 옮기는 경우가 많습니다.

안테나가 장착된 위치는 종종 상승되어 있으며, 천장, 보도, 지붕 구조, 보, 보도 및 의도한 적용 영역 위에 약간의 상승을 제공하는 모든 위치가 될 수 있습니다. 이러한 위치는 일반적으로 오디오 장비, 에어컨, 조명 및 다양한 탐지기 / 센서와 같은 다른 설치와 공유됩니다. 예를 들어, 오디오 및 조명 장비는 매우 특정 위치에 장착되어야 하는데, 왜 이런 것일까요? 단순히 오디오나 조명 기기가 박스 안이나 벽 뒤에 숨겨져 있으면 제대로 작동하지 않고, 모두가 이를 인정하기 때문이다.

무선 안테나도 마찬가지입니다. 무선 클라이언트 장치에 LOM(Line of Sight)이 있을 때 가장 잘 작동합니다. 심미성의 우선 순위는 무선 성능에 부정적인 영향을 미칠 수 있으며(또한 매우 자주 그러하므로) 인프라 투자의 가치가 줄어듭니다.

비인가 네트워크

비인가 Wi-Fi 네트워크는 공통 RF 공간을 공유하지만 동일한 운영자가 관리하지 않는 무선 네트워크입니다. 임시 또는 영구적일 수 있으며 인프라 장치(AP) 및 개인 장치(예: Wi-Fi 핫스팟을 공유하는 휴대폰)를 포함할 수 있습니다. 비인가 Wi-Fi 네트워크는 간섭의 원인이며 경우에 따라 보안 위험도 있습니다. 무선 성능에 대한 악의적인 영향은 과소평가되어서는 안 됩니다. Wi-Fi 전송은 모든 Wi-Fi 장치 간에 공유되는 비교적 작은 범위의 무선 스펙트럼으로 제한되며, 근접한 모든 잘못된 장치는 많은 사용자의 네트워크 성능을 방해할 수 있습니다.

대규모 공용 네트워크의 경우, 이러한 네트워크는 대개 전문 안테나를 사용하여 신중하게 설계되고 조정됩니다. RF 설계가 좋으면 필요한 영역만 지원하며, 주로 지향성 안테나를 사용하고, 전송 및 수신 특성을 조정하여 효율성을 극대화합니다.

스펙트럼의 다른 쪽 끝에는 소비자 등급 디바이스, 또는 인터넷 서비스 제공자에 의해 공급되는 디바이스가 있습니다. 이러한 디바이스는 미세 RF 조정을 위한 제한된 옵션을 가지고 있거나, 종종 높은 전력, 낮은 데이터 속도 및 넓은 채널을 통해 최대 범위와 인식 성능을 제공하도록 구성되어 있습니다. 이러한 장치를 대규모 이벤트 네트워크에 도입하는 것은 대혼란을 일으킬 가능성이 있다.

어떻게 할 수 있을까요?

개인 핫스팟의 경우 수 만 명의 사람들이 한 행사장에 들어가는 것을 감시하는 것은 거의 불가능하기 때문에 할 수 있는 일이 거의 없다. 인프라 또는 반영구 장치의 경우 몇 가지 옵션이 있습니다. 가능한 교정은 단순한 인식용 신호 표시를 포함한 단순한 교육에서 시작하여 서명된 무선 정책 문서를 통해 적극적인 시행 및 스펙트럼 분석으로 마무리됩니다. 모든 경우, 해당 사업장의 무선 스펙트럼 보호에 대한 사업적 결정을 내려야 하며, 이러한 사업적 결정을 이행하기 위한 구체적인 조치도 함께 내려져야 합니다.

비인가 네트워크의 보안 측면은 서드파티에 의해 제어되는 디바이스가 관리 네트워크와 동일한 SSID를 광고할 때 활성화됩니다. 이는 허니팟 공격과 동일하며 사용자 자격 증명을 훔치는 방법으로 사용될 수 있습니다. 관리되지 않는 디바이스에서 광고하는 인프라 SSID의 탐지에 대해 경고하기 위해 비인가 규칙을 생성하는 것이 좋습니다. 보안 섹션에서는 비인가를 더 자세히 설명합니다.

단일 5GHz 대 이중 5GHz

이중 5GHz는 지원되는 AP에서 5GHz 무선 장치 모두를 사용하는 것을 의미합니다. 외부 안테나를 사용하는 듀얼 5GHz와 내부 안테나(전방향성 AP의 마이크로/매크로 셀)를 사용하는 듀얼 5GHz 간에는 중요한 차이가 있습니다. 외부 안테나의 경우 듀얼 5GHz가 유용한 메커니즘인 경우가 많으므로 총 AP 수를 줄이면서 추가 커버리지와 용량을 제공합니다.

마이크로/매크로/메소

내부 AP에는 두 안테나가 모두 가까이 있으며(AP 내부) 이중 5GHz 사용 시 최대 Tx 전력과 관련된 제한이 있습니다. 제2 라디오는 낮은 Tx 전력(이는 무선 컨트롤러에 의해 시행됨)으로 제한되어, 라디오들 사이의 Tx 전력의 큰 불균형을 초래한다. 이로 인해 기본(고전력) 무선 장치는 많은 클라이언트를 유치하고 보조(저전력) 무선 장치는 제대로 활용되지 않을 수 있습니다. 이 경우 두 번째 라디오는 고객에게 혜택을 제공하지 않고 환경에 에너지를 추가합니다. 이 시나리오가 관찰되면 추가 용량이 필요한 경우 두 번째 라디오를 비활성화하고 단순히 다른(5GHz 단일) AP를 추가하는 것이 좋습니다.

서로 다른 AP 모델에는 서로 다른 구성 옵션이 있습니다. 두 번째 5GHz 무선 장치는 9130 및 9136과 같은 최신 매크로/메소 AP에서 더 높은 전원 수준에서 작동할 수 있으며, 9160 시리즈와 같은 일부 내부 Wi-Fi 6E AP는 경우에 따라 매크로/매크로에서 작동할 수도 있습니다. 항상 정확한 AP 모델의 기능을 확인합니다. 두 번째 5GHz 슬롯은 채널 사용량도 제한됩니다. 한 슬롯이 하나의 UNII 대역에서 작동하고 다른 슬롯이 다른 UNII 대역으로 제한되어 채널 계획에 영향을 미치며, 그 이후에는 가용 전송 전력도 증가합니다. 항상 듀얼 5GHz 무선 장치 간의 Tx 전력 차이를 고려하십시오. 이는 내부 AP를 포함한 모든 경우에 적용됩니다.

FRA

FRA(Flexible Radio Assignment)는 추가 2.4GHz 무선 장치를 5GHz 모드로 전환하거나 사용하지 않을 가능성이 있는 5GHz 무선 장치를 모니터 모드로 전환하여 5GHz 커버리지를 향상시키는 기술로 도입되었습니다(이를 지원하는 AP의 경우). 이 문서에서는 대규모 공용 네트워크에 대해 설명하므로, 무선 설계뿐만 아니라 커버리지 영역이 지향성 안테나를 사용하여 잘 정의된다고 가정하므로, 동적 컨피그레이션보다 결정적 컨피그레이션이 선호됩니다. 대규모 공용 네트워크에서는 FRA를 사용하지 않는 것이 좋습니다.

선택적으로, 5GHz로 변환할 무선 장치를 결정하는 데 도움이 되도록 네트워크를 설정할 때 FRA를 사용할 수 있지만, 그 결과에 만족하면 FRA를 중지하는 것이 좋습니다.

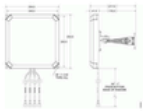
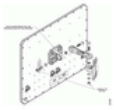
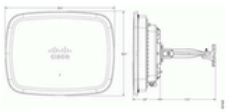
규정

각 규정 영역은 사용 가능한 채널 및 최대 전력 수준을 정의하고, 실내와 실외에서 사용할 수 있는 채널에 대한 제한도 있습니다. 규제 영역에 따라 듀얼 5GHz 솔루션을 효과적으로 활용하지 못하는 경우가 간혹 발생할 수 있습니다. 예를 들어 UNII-2e 채널에서는 30dBm이 허용되지만 UNII1/2에서는 23dBm만 허용되는 ETSI 도메인이 있습니다. 이 예에서 설계에 30dBm의 사용이 필요한 경우(일반적으로 안테나와의 거리가 더 멀기 때문) 단일 5GHz 무선 장치를 사용하는 것이 유일한 실현 가능한 해결책일 수 있습니다.

안테나

대형 공용 네트워크는 모든 유형의 안테나를 사용할 수 있으며 일반적으로 작업에 가장 적합한 안테나를 선택합니다. 동일한 커버리지 영역 내에서 안테나를 혼용하면 무선 설계 프로세스가 더욱 까다로워지며 가능하면 피해야 합니다. 그러나 대형 공용 네트워크에는 동일한 영역 내에서도 서로 다른 마운팅 옵션으로 커버리지 영역이 큰 경우가 많아 경우에 따라 안테나를 혼합해야 합니다. 옴니 안테나는 잘 이해되며 다른 모든 안테나와 동일하게 작동합니다. 이 가이드에서는 외부 지향성 안테나를 설명합니다.

이 표에는 가장 많이 사용되는 외부 안테나가 나열되어 있습니다.

	C-ANT9103 Patch antenna (8x8) 6 dBi	5GHz Beamwidth 70°x70° ~33ft (10m)
	ANT2566P4W-R/S Patch antenna (4x4) 6 dBi	5GHz Beamwidth 110°x55° (120°x60°) ~33ft (10m)
	ANT2566D4M-R/S Patch antenna (4x4) 6 dBi	5GHz Beamwidth 55°x60° (60°x60°) ~33ft (10m)
	ANT2513P4M-N/S HD “Stadium” antenna 13 dBi	5GHz Beamwidth 31°x27° (30°x30°) ~66ft (20m)
	C-ANT9104 HD “Stadium” antenna Narrow 10dBi / Wide 7dBi	5GHz Beamwidth Narrow 25°x25° Wide 80°x25°

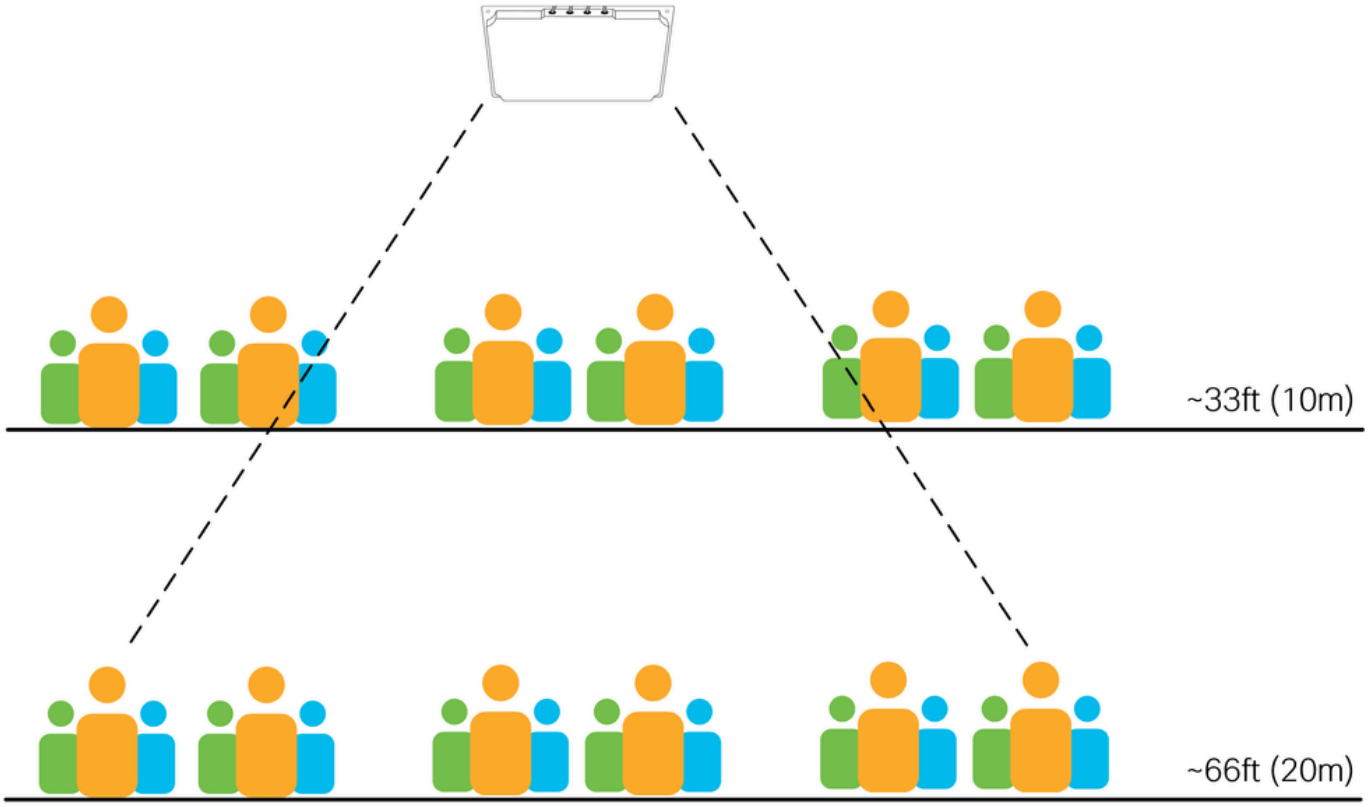
안테나 목록

안테나를 선택할 때 고려해야 할 주요 요소는 안테나가 실장되는 안테나 빔 폭과 거리/높이이다. 이 표에서는 각 안테나의 5GHz 빔 폭을 보여 줍니다. 대괄호 안의 숫자는 반올림된(그리고 기억하기 쉬운) 값을 보여 줍니다.

표에서 제시된 거리는 하드 규칙이 아니라 경험에 기초한 지침입니다. 전파는 빛의 속도로 이동하며 임의의 거리에 도달한 후 단순히 멈추지 않는다. 안테나는 모두 제안된 거리 이상으로 작동하지만 거리가 증가함에 따라 성능이 저하됩니다. 계획 시 설치 높이는 핵심 요소입니다.

아래 다이어그램은 고밀도 영역에서 ~33피트(10m) 및 ~66피트(20m)의 동일한 안테나에 대한 두 가지 가능한 장착 높이를 보여줍니다. 안테나가 볼 수 있고 연결을 수락할 수 있는 클라이언트 수가 거리에 따라 증가합니다. 더 작은 셀 크기를 유지하는 것은 더 큰 거리에서 더욱 어려워진다.

사용자의 밀도가 높을수록 해당 거리에 맞는 안테나를 사용하는 것이 중요하다는 것이 일반적인 규칙이다.



경기장 안테나

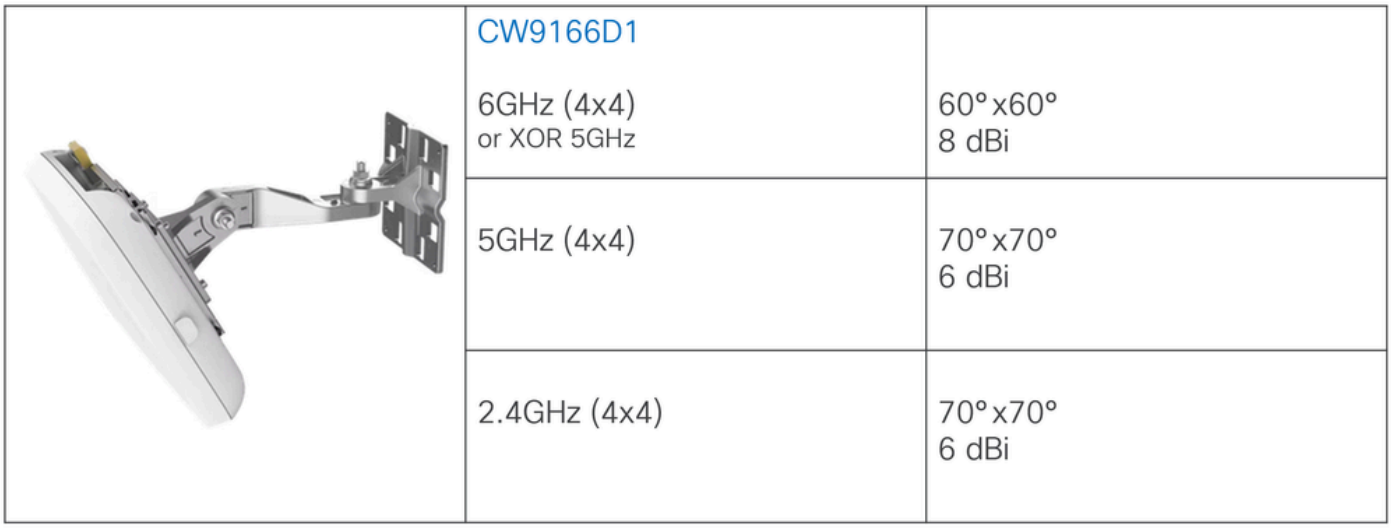
C9104 경기장 안테나는 고거리에서 고밀도 영역을 다루는 데 적합합니다. 자세한 내용은 Catalyst 9104 경기장 안테나(C-ANT9104) 배포 가이드를 참조하십시오.

시간의 경과에 따른 변화

시간이 지남에 따라 물리적 환경이 변경되는 것은 거의 모든 무선 설치(예: 내부 벽 이동)에서 흔히 발생합니다. 정기적인 사이트 방문과 육안 검사는 항상 권장되는 방식이었습니다. 이벤트 네트워크의 경우 오디오 및 조명 시스템, 그리고 많은 경우 다른 통신 시스템(예: 5G)을 다루는 데 있어서 복잡성이 더 커집니다. 이러한 모든 시스템은 종종 사용자 위의 높은 위치에 설치되며, 때로는 동일한 공간에 대한 경합을 초래하기도 한다. 무선 경기장 안테나의 좋은 위치는 종종 5G 안테나의 좋은 위치입니다! 게다가 이러한 시스템은 시간이 지남에 따라 업그레이드되므로 무선 시스템을 방해하거나 능동적으로 방해하는 위치로 재배치할 수 있습니다. 모든 시스템이 서로 간섭하지 않고(물리적 또는 전자기적으로) 적절한 위치에 설치되었는지 확인하기 위해 다른 설치를 추적하고 설치 팀과 통신하는 것이 중요합니다.

고밀도 및 6GHz

이 문서를 작성할 때 6GHz 지원 외부 안테나를 제한적으로 선택할 수 있습니다. CW9166D1 통합 AP/안테나만 6GHz에서 작동합니다. 자세한 안테나 사양은 Cisco Catalyst CW9166D1 Access Point Deployment Guide에서 확인할 수 있습니다. CW9166D1은 60°x60°의 빔 폭으로 6GHz 커버리지를 제공하며 이 유형의 안테나 조건을 충족하는 모든 구축에 효과적으로 사용할 수 있습니다. 예를 들어, CW9166D1은 실내에서 사용할 수 있는 지향성 안테나 기능을 제공하기 때문에 강당 및 창고가 적합합니다.

	CW9166D1 6GHz (4x4) or XOR 5GHz	60° x60° 8 dBi
	5GHz (4x4)	70° x70° 6 dBi
	2.4GHz (4x4)	70° x70° 6 dBi

9166D1

대형 공용 네트워크의 맥락에서, 이러한 네트워크는 종종 다양한 넓은 영역을 가지며 다양한 높이의 안테나 조합을 사용해야 합니다. 거리 제한으로 인해 60°x60° 안테나만 사용하여 대규모 공용 네트워크를 엔드 투 엔드로 구축하는 것이 어려울 수 있습니다. 따라서 대규모 공용 네트워크에서는 CW9166D1만 사용하여 6GHz에서 엔드 투 엔드 커버리지를 제공하는 것도 어려울 수 있습니다.

한 가지 가능한 접근 방식은 5GHz를 기본 커버리지 대역으로 사용하는 반면, 특정 영역에서만 6GHz를 사용하여 더 깨끗한 6GHz 대역으로 지원 가능한 클라이언트 디바이스를 오프로드하는 것입니다. 이 유형의 접근 방식은 더 넓은 영역에서 5GHz 전용 안테나를 사용하는 동시에, 가능한 경우 추가 용량이 필요한 경우 6GHz 안테나를 사용합니다.

예를 들어 무역상담회의 대형 이벤트 홀을 고려할 때 메인 홀은 경기장 안테나를 사용하여 5GHz에서 기본 커버리지를 제공하며, 설치 높이는 경기장 안테나 사용을 의무화합니다. CW9166D1은 거리 제한으로 인해 이 예에서 메인 홀에서 사용할 수 없습니다 - 그러나 더 높은 밀도가 필요한 인접 VIP 홀 또는 프레스 영역에서 효과적으로 사용할 수 있습니다. 5GHz와 6GHz 대역 간의 클라이언트 로밍에 대해서는 이 문서의 뒷부분에서 설명합니다.

규정

5GHz와 마찬가지로, 6GHz에 사용 가능한 전력 및 채널은 규정 도메인 간에 크게 다릅니다. 특히, FCC와 ETSI 도메인 간의 가용 스펙트럼에는 큰 차이가 있으며, 실내 및 실외 사용 가능한 Tx 전력, LPI(Low Power Indoor) 및 SP(Standard Power)에 대한 엄격한 지침도 있습니다. 6GHz를 사용하는 경우 클라이언트 전력 제한, 외부 안테나 사용 및 안테나 다운 틸트(down tilt), SP 구축을 위한 AFC(Automated Frequency Coordination) 요구 사항(현재는 미국만 해당)이 추가로 제한됩니다.

Wi-Fi 6E에 대한 자세한 내용은 Wi-Fi 6E: The Next Great Chapter in Wi-Fi 백서를 참조하십시오.

무선 리소스 관리

RRM(Radio Resource Management)은 무선 작동 제어를 담당하는 알고리즘 집합입니다. 이 가이드에서는 DCA(Dynamic Channel Assignment)와 TPC(Transmit Power Control)라는 두 가지 주요 RRM 알고리즘을 참조합니다. RRM은 고정 채널 및 전원 구성에 대한 대안입니다.

- DCA는 구성 가능한 일정에 따라 실행됩니다(기본값 10분).

- TPC는 자동 일정에 따라 실행됩니다(기본값 10분).

Cisco ED-RRM(Event Driven RRM)은 DCA 옵션으로서, 보통 심각한 RF 조건에 대응하여 표준 DCA 일정보다 채널 변경 결정을 내릴 수 있습니다. ED-RRM은 과도한 수준의 간섭이 감지되면 즉시 채널을 변경할 수 있습니다. ED-RRM을 활성화하는 소음이 많거나 불안정한 환경에서는 과도한 채널 변경이 발생할 수 있으며, 이는 클라이언트 디바이스에 부정적인 영향을 미칠 수 있습니다.

RRM을 사용하는 것이 좋으며 일반적으로 정적 컨피그레이션보다 선호되지만, 특정 주의 사항 및 예외 사항이 있습니다.

- TPC는 필요에 따라 TPC min/max 설정을 사용하는 좁은 범위의 값으로 제한해야 하며 항상 RF 설계에 맞춰야 합니다.
    - 고밀도 환경에서 TPC 채널 인식을 활성화합니다.

- DCA 주기는 기본 설정인 10분에서 변경해야 합니다.
    - HD 환경에서는 ED-RRM을 사용하지 마십시오.
    - Cisco AP 로드 방지를 비활성화합니다.
    - 비인가 AP 회피 옵션(예: 외부 AP 간섭 회피)은 비인가가 많은 경우 불안정한 환경을 초래할 수 있습니다. 비인가 공격을 제거하는 것이 그 공격에 대응하려는 시도보다 더 낫다.
- RRM 결정은 서로 멀리 떨어져 있는 지향성 안테나의 경우처럼 서로 제대로 들리지 않는 AP/안테나의 영향을 받을 수 있습니다.
- 일부 안테나(예: C9104)는 RRM을 지원하지 않으며 항상 고정 컨피그레이션이 필요합니다.
- RRM은 잘못된 RF 설계를 수정하지 않습니다.

모든 경우에 RRM은 예상되는 결과를 이해하고 구축해야 하며, 지정된 RF 환경에 적합한 경계 내에서 작동하도록 조정되어야 합니다. 이 문서의 후속 섹션에서는 이러한 점을 더 자세히 살펴봅니다.

RF 컨피그레이션

채널

일반적으로 채널이 많을수록 좋습니다. 고밀도 구축에서는 가용 채널보다 훨씬 많은 수의 AP 및 무선 장치가 구축될 수 있으므로 채널 재사용 비율이 클 뿐만 아니라 동일 채널 간섭 수준도 높습니다. 모든 가용 채널을 사용해야 하며, 일반적으로 가용 채널 목록을 제한하는 것은 권장되지 않습니다.

특정(및 별도의) 무선 시스템이 동일한 물리적 공간에 공존해야 하는 경우 및 전용 채널을 할당해야 하는 동시에 할당된 채널을 기본 시스템의 DCA 목록에서 제거해야 하는 경우가 있을 수 있습니다. 이러한 유형의 채널 제외는 매우 신중하게 평가되어야 하며 필요한 경우에만 사용됩니다. 이 예는 1차 네트워크에 인접한 열린 영역 또는 경기장 내부의 프레스 영역에서 작동하는 점대점 링크일 수 있습니다. 하나 또는 두 개 이상의 채널이 DCA 목록에서 제외되는 경우, 이는 제안된 솔루션의 재평가 원인이 된다. 매우 고밀도 경기장과 같이 경우에 따라서는 단 하나의 채널도 제외하는 것이 실현 가능한 선택이 되지 못하는 경우도 있다.

DCA(Dynamic Channel Assignment)는 WLC 기반 RRM 또는 AI 강화 RRM과 함께 사용할 수 있습니다.

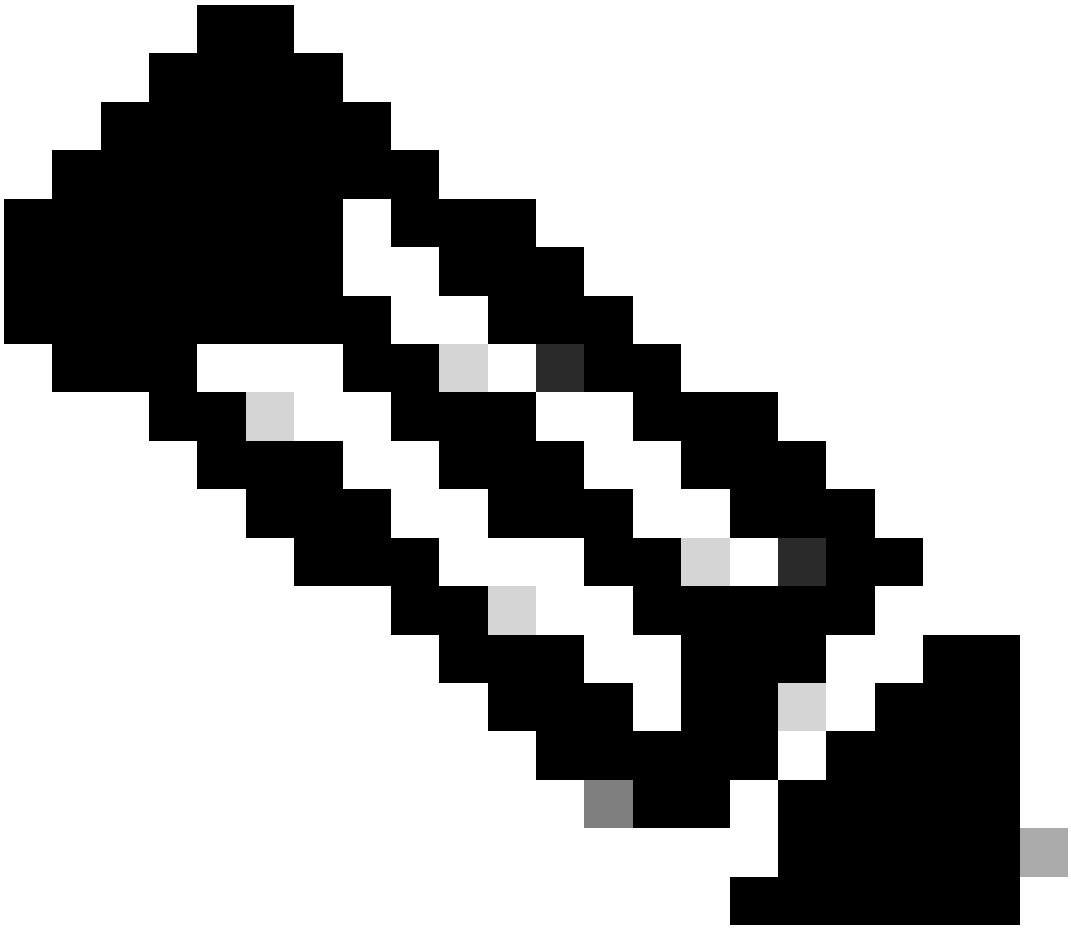
기본 DCA 간격은 10분이며, 이는 불안정한 RF 환경에서 빈번한 채널 변경을 초래할 수 있다. 기본

DCA 타이머를 기본 10분에서 늘려야 합니다(모든 경우). 특정 DCA 간격은 문제의 네트워크에 대한 운영 요구 사항에 맞게 조정해야 합니다. 컨피그레이션의 예는 DCA 간격 4시간, 앵커 시간 8입니다. 이렇게 하면 채널 변경은 오전 8시부터 4시간마다 1회로 제한됩니다.

간섭이 발생할 수밖에 없으므로 모든 DCA 주기에 적응하는 것이 많은 간섭이 일시적이므로 반드시 가치를 창출하는 것은 아닙니다. 좋은 기술은 처음 몇 시간 동안 자동 DCA를 사용하고, 당신이 만족스러운 어떤 안정적인 것이 있을 때 알고리즘과 채널 계획을 동결하는 것입니다.

WLC가 리부팅되면 DCA는 100분 동안 어그레시브 모드로 실행되어 적합한 채널 계획을 찾습니다. RF 설계를 크게 변경할 경우(예: 여러 AP 추가 또는 제거, 채널 폭 변경) 프로세스를 수동으로 다시 시작하는 것이 좋습니다. 이 프로세스를 수동으로 시작하려면 이 명령을 사용합니다.

```
ap dot11 [24ghz | 5ghz | 6ghz] rrm dca restart
```



참고: 채널 변경으로 인해 클라이언트 디바이스가 중단될 수 있습니다.

2.4기가헤르츠

2.4GHz 대역은 종종 비판을 받아왔습니다. 3개의 비중첩 채널만 있으며 Wi-Fi를 제외한 다른 여러 기술에서 사용하기 때문에 원치 않는 간섭이 발생합니다. 일부 단체에서 이에 대한 서비스 제공을 주장하는데 타당한 결론은 무엇인가? 2.4GHz 대역은 엔드 유저에게 만족스러운 경험을 제공하지 못한다는 것이 사실입니다. 2.4GHz에서 서비스를 제공하려고 하면 Bluetooth와 같은 다른 2.4GHz 기술에도 영향을 줍니다. 대규모 행사장이나 행사장에서는 여전히 많은 사람들이 전화를 걸거나 스마트 웨어러블이 평소와 같이 작동하기를 기대합니다. 고집적도 Wi-Fi가 2.4GHz에서 작동하면 2.4GHz Wi-Fi를 사용하지 않는 장치에 영향을 미치게 됩니다.

한 가지 확실한 것은 2.4GHz Wi-Fi 서비스를 제공해야 하는 경우 별도의 SSID(IoT 디바이스 전용 또는 "레거시")에서 제공하는 것이 가장 좋습니다. 즉, 이중 대역 디바이스는 비자발적으로 2.4GHz에 연결되지 않으며 단일 대역 2.4GHz 디바이스만 연결됩니다.

Cisco는 2.4GHz에서 40MHz 채널 사용을 권장하거나 지원하지 않습니다.

5GHz

고집적도 무선 환경을 위한 일반적인 구축. 가능한 경우 사용 가능한 모든 채널을 사용합니다.

채널 수는 규정 도메인에 따라 다릅니다. 특정 위치에서 레이더의 영향을 고려하여 가능한 경우 DFS 채널(TDWR 채널 포함)을 사용합니다.

20MHz 채널 폭은 모든 고밀도 구축에 매우 권장됩니다.

2.4GHz와 동일한 기준으로 40MHz를 사용할 수 있습니다. 즉, 절대적으로 필요한 경우에만 사용할 수 있습니다.

특정 환경에서 40MHz 채널의 필요성 및 실제 이점을 평가하십시오. 40MHz 채널은 더 높은 SNR(signal-to-noise ratio)을 요구하여 처리량을 개선할 수 있습니다. 더 높은 SNR이 불가능한 경우, 40MHz 채널은 유용하지 않습니다. 고밀도 네트워크는 모든 사용자의 처리량이 잠재적으로 더 높은 것보다 모든 사용자의 평균에 우선 순위를 둡니다. 보조 채널이 데이터 프레임에만 사용되므로 20MHz에서 작동하는 두 개의 서로 다른 무선 셀을 사용하는 것보다 40MHz를 사용하는 AP를 사용하는 것보다 20MHz 채널에 더 많은 AP를 배치하는 것이 훨씬 더 효율적입니다(단일 클라이언트 처리량이 아니라 총 용량 측면에서).

6GHz

6GHz 밴드는 아직 모든 국가에서 사용할 수 없습니다. 또한 일부 디바이스에는 6GHz 지원 Wi-Fi 어댑터가 있지만 디바이스를 작동 중인 특정 국가에서 활성화하려면 BIOS 업데이트가 필요합니다. 고객이 현재 6GHz 무선 장치를 검색하는 가장 일반적인 방법은 5GHz 무선 장치의 RNR 광고를 통한 것입니다. 이는 6GHz가 동일한 AP에서 5GHz 무선 장치 없이 단독으로 동작해서는 안 된다는 것을 의미합니다. 6GHz는 5GHz 무선 장치에서 클라이언트 및 트래픽을 오프로드하기 위한 것이며 일반적으로 지원 가능한 클라이언트에 더 나은 환경을 제공하기 위한 것입니다. 6GHz 채널은 더 큰 채널 대역폭을 사용할 수 있지만 규정 도메인에서 사용 가능한 채널 수에 크게 좌우됩니다. 유럽에서 24개의 6GHz 채널을 사용할 수 있기 때문에, 5GHz에서 사용 중인 20MHz에 비해 더 나은 최대 처리량을 제공하기 위해 40MHz 채널을 사용하는 것도 무리가 없습니다. 채널 수가 거의 두 배에 달하는 미국에서는 40MHz를 사용하는 것이 쉬운 일이 아니며 80MHz로 전환하더라도 대규모 집적도 이벤트에는 무리가 없습니다. 고밀도 이벤트 또는 장소에서는 더 큰 대역폭을 사용하지 않아야 합

니다.

데이터 전송률

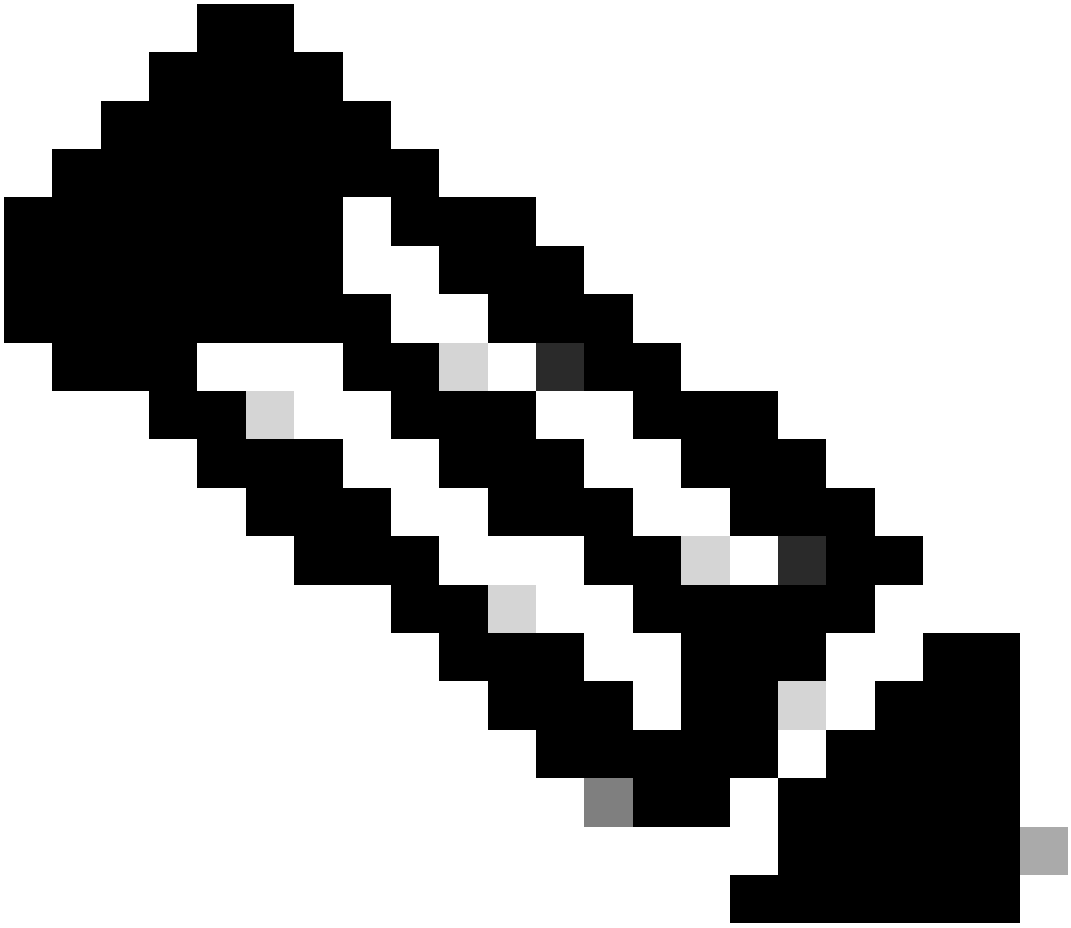
클라이언트가 AP와 협상하는 데이터 속도는 대부분 해당 연결의 SNR(Signal-to-Noise Ratio)의 함수이며, 그 반대도 마찬가지입니다. 즉, 데이터 속도가 높을수록 SNR이 높아져야 합니다. 실제로 가능한 최대 링크 속도를 결정하는 것은 대부분 SNR입니다. 그러나 데이터 속도를 구성할 때 왜 이것이 중요합니까? 어떤 데이터 속도는 특별한 의미를 갖기 때문입니다.

기존 OFDM(802.11a) 데이터 속도는 Disabled(비활성화됨), Supported(지원됨) 또는 Mandatory(필수)의 세 가지 설정 중 하나로 구성할 수 있습니다. OFDM 속도(Mbps 단위)는 6, 9, 12, 18, 24, 36, 48, 54이며 클라이언트와 AP 모두 속도를 지원해야 사용할 수 있습니다.

지원됨 - AP가 속도를 사용합니다.

필수 - AP가 속도를 사용하고 이 속도를 사용하여 관리 트래픽을 전송합니다.

Disabled(비활성화됨) - AP가 속도를 사용하지 않으므로 클라이언트가 다른 속도를 사용해야 합니다



참고: 필수 요율은 기본 요율이라고도 합니다.

필수 속도는 모든 관리 프레임이 브로드캐스트 및 멀티캐스트 프레임뿐만 아니라 이 속도를 사용하여 전송된다는 점에서 중요합니다. 여러 필수 레이트가 구성된 경우 관리 프레임에서는 가장 낮은 필수 레이트를 사용하고 브로드캐스트 및 멀티캐스트에서는 가장 높은 필수 레이트를 사용합니다.

관리 프레임에는 AP에 연결할 수 있도록 클라이언트가 들어야 하는 신호가 포함됩니다. 필수 속도를 높이면 해당 전송에 대한 SNR 요구 사항도 증가하므로, 데이터 속도가 높을수록 SNR이 높아야 하며, 이는 일반적으로 클라이언트가 비컨을 디코딩하고 연결할 수 있도록 AP에 더 가까이 있어야 한다는 것을 의미합니다. 따라서 필수 데이터 전송률을 조작하면 AP의 유효 연결 범위도 조작되므로 클라이언트가 AP에 가까워지거나 잠정적 로밍 결정을 내릴 수 있습니다. AP에 가까운 클라이언트는 더 높은 데이터 속도를 사용하고, 높은 데이터 속도는 더 적은 통신 시간을 사용합니다. 즉, 의도한 효과가 더 효율적인 셀입니다. 데이터 속도를 높이는 것은 특정 프레임의 전송 속도에만 영향을 미치며, 안테나의 RF 전파 또는 간섭 범위에는 영향을 미치지 않는다는 것을 기억해야 합니다. 동일 채널 간섭 및 노이즈를 최소화하기 위해서는 여전히 우수한 RF 설계 방식이 필요합니다.

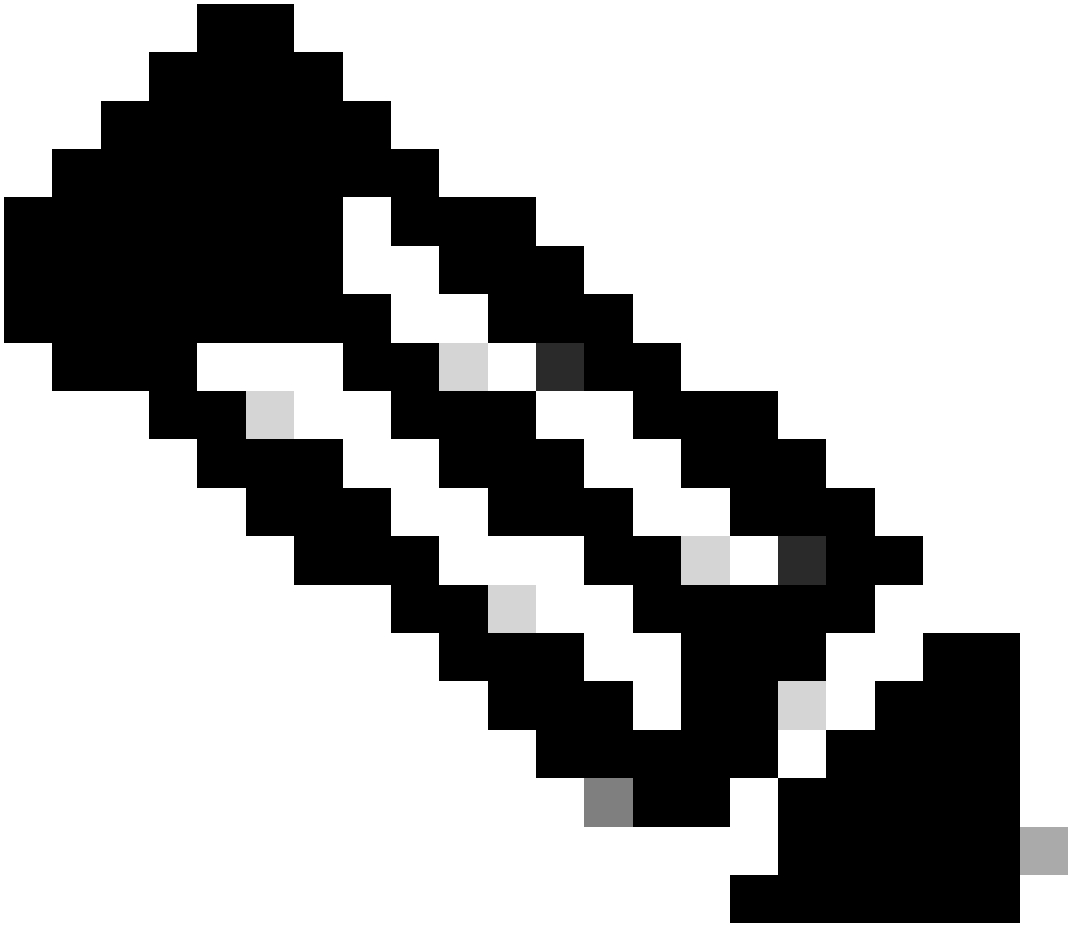
반대로, 일반적으로 요금이 낮다는 것은 클라이언트가 훨씬 더 먼 거리에서 연결할 수 있다는 것을

의미합니다. 이는 AP 밀도 감소 시나리오에서는 유용하지만 고밀도 시나리오에서 로밍의 대혼란을 일으킬 수 있는 잠재력과 관련이 있습니다. 6Mbps를 브로드캐스트하는 비인가 AP를 찾으려고 시도한 모든 사용자는 물리적 위치에서 매우 멀리 떨어진 AP를 탐지할 수 있다는 것을 알 수 있습니다!

브로드캐스트 및 멀티캐스트를 주제로 할 때, 경우에 따라 두 번째(더 높은) 필수 속도는 멀티캐스트 트래픽의 전송 속도를 높이도록 구성됩니다. 멀티캐스트는 승인되지 않으며 프레임이 손실될 경우 재전송되지 않으므로 성공하는 경우가 거의 없습니다. 일부 손실은 모든 무선 시스템에 내재되어 있으므로 구성된 속도에 관계없이 일부 멀티캐스트 프레임이 손실되는 것이 불가피합니다. 신뢰할 수 있는 멀티캐스트 전달에 대한 더 나은 접근 방식은 멀티캐스트를 유니캐스트 스트림으로 전송하는 멀티캐스트-유니캐스트 변환 기술이며, 이는 더 높은 데이터 전송률과 신뢰할 수 있는(확인된) 전달의 이점을 모두 가집니다.

단일 필수 비율만 사용하는 것이 좋습니다. 모든 비율이 필수 비율보다 낮으면 비활성화하고, 모든 비율이 필수 비율보다 높으면 지원되는 것으로 둡니다. 사용할 특정 속도는 사용 사례에 따라 다릅니다. 앞서 언급한 낮은 속도는 밀도가 낮고 AP 간 거리가 더 큰 실외 시나리오에서 유용합니다. 고밀도 및 이벤트 네트워크의 경우 낮은 속도를 비활성화해야 합니다.

어디서부터 시작해야 할지 잘 모르는 경우, 저밀도 구축에는 12Mbps의 필수 속도를 사용하고, 고밀도 구축에는 24Mbps를 사용하십시오. 많은 대규모 이벤트, 경기장 및 고집적도 엔터프라이즈 사무실 구축에서도 24Mbps의 필수 속도 설정으로 안정적으로 작동하는 것이 입증되었습니다. 12Mbps 미만이나 24Mbps 이상의 속도가 필요한 특정 사용 사례에 대해서는 적절한 테스트가 권장됩니다.

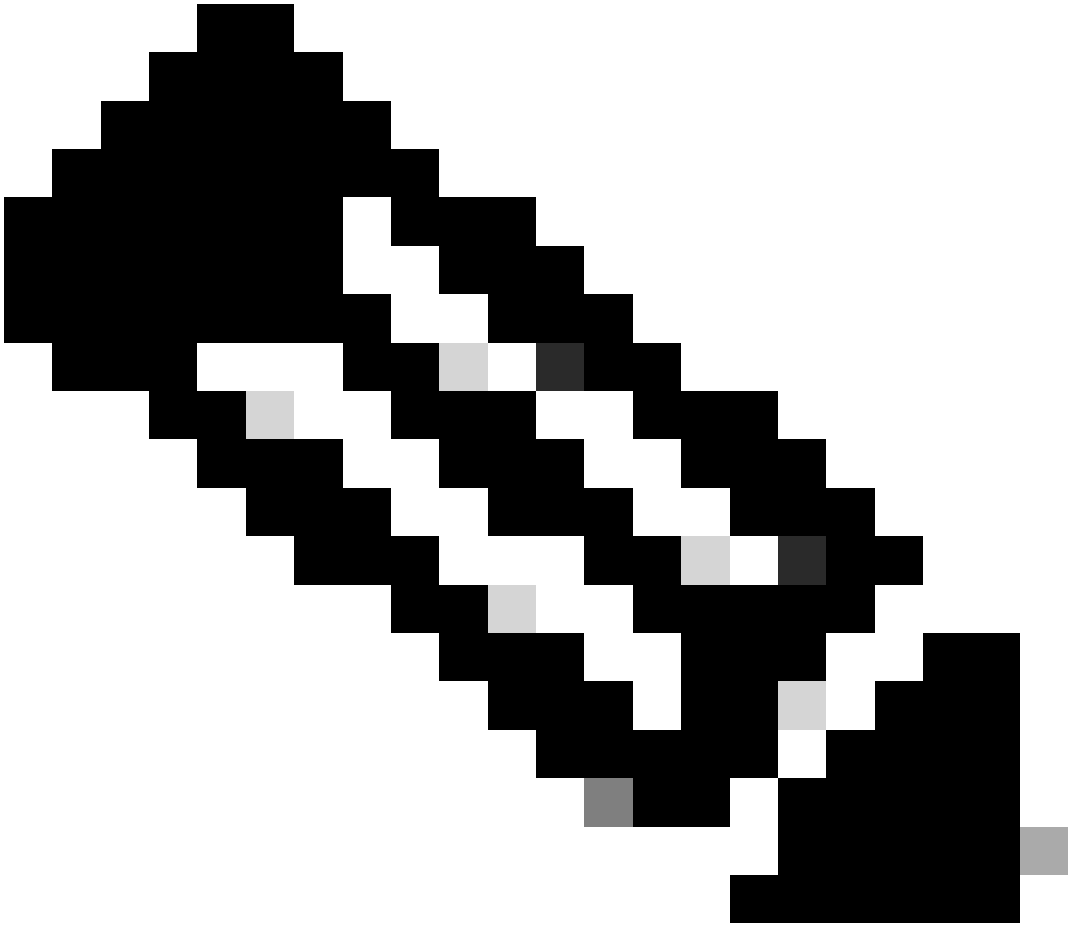


참고: 모든 802.11n/ac/ax 속도를 활성화된 상태로 두는 것이 가장 좋습니다(WLC GUI의 High Throughput 섹션에 있는 모든 속도). 이러한 속도를 비활성화할 필요는 거의 없습니다 .

전송 전력

전송 전력 권장 사항은 구축 유형에 따라 다릅니다. 여기서는 무지향성 안테나를 사용하는 실내 배치와 지향성 안테나를 사용하는 실내 배치를 구분합니다. 두 가지 유형의 안테나 모두 대규모 공용 네트워크에 존재할 수 있지만 일반적으로 서로 다른 유형의 영역을 포함합니다.

전방위 구축의 경우 고정으로 구성된 최소 임계값과 고정으로 구성된 최대 임계값이 포함된 자동 TPC(Transmit Power Control)를 사용하는 것이 일반적입니다.



참고: TPC 임계값은 무선 송신 전력을 참조하며 안테나 이득을 제외합니다. 항상 안테나 이득이 사용된 안테나 모델에 맞게 구성되었는지 확인합니다. 이 작업은 내부 안테나 및 자체 식별 안테나의 경우 자동으로 수행됩니다.

예 1

TPC 최소: 5dBm, TPC 최대: 최대(30dBm)

그러면 TPC 알고리즘에서 전송 전력을 자동으로 결정하지만, 구성된 최소 임계값인 5dBm 아래로 내려가지 않습니다.

예 2

TPC 최소: 2dBm, TPC 최대: 11dBm

그러면 TPC 알고리즘이 자동으로 전송 전력을 결정하지만 항상 2dBm에서 11dBm 사이에 머물게 됩니다.

좋은 방법은 서로 다른 임계값으로 여러 RF 프로파일을 생성하는 것입니다(예: 저전력(2-5dBm), 중간 전력(5-11dbM), 고전력(11-17dBM)). 그런 다음 필요에 따라 각 RF 프로파일에 전방향 AP를 할당하는 것입니다. 각 RF 프로파일의 값을 사용 용도 및 적용 범위 영역으로 조정할 수 있습니다. 이를 통해 RRM 알고리즘은 사전 정의된 경계 내에 머물면서 동적으로 작동할 수 있습니다.

지향성 안테나들에 대한 접근법은 매우 유사하며, 유일한 차이는 요구되는 정밀도의 레벨이다. 지향성 안테나 배치는 구축 전 RF 설문조사 과정에서 설계 및 검증되어야 하며, 특정 무선 컨피그레이션 값은 일반적으로 이 프로세스의 결과입니다.

예를 들어, 천장에 장착된 패치 안테나가 ~26피트(8m) 높이에서 특정 영역을 커버해야 하는 경우, RF 설문조사는 이 의도된 커버리지를 달성하기 위해 필요한 최소 Tx 전력을 결정해야 합니다(이는 RF 프로파일에 대한 최소 TPC 값을 결정함). 마찬가지로, 동일한 RF 설문조사를 통해 이 RF 프로파일과 다음 안테나, 또는 커버리지가 종료되기를 원하는 지점 간에 중복이 발생할 수 있음을 파악합니다. 이는 RF 프로파일에 대한 최대 TPC 값을 제공합니다.

지향성 안테나의 RF 프로파일은 일반적으로 최소 및 최대 TPC 값이 같거나 가능한 값의 범위가 좁습니다(일반적으로 3dBm 미만).

구성 일관성을 보장하기 위해 RF 프로파일을 선호하며, 개별 AP의 정적 구성은 권장되지 않습니다. 적용 범위, 안테나 유형 및 활용 사례(예: RF-Auditorium-Patch-Ceiling)에 따라 RF 프로파일의 이름을 지정하는 것이 좋습니다.

Tx 전력의 정확한 양은 의도된 커버리지 영역에서 가장 약한 클라이언트에 의해 요구되는 SNR 값이 달성되는 경우이며, 그 이하여야 한다. 30dBm은 실제 상황(즉 사람이 많은 장소에서)에서 뛰어난 클라이언트 SNR 목표 값입니다.

CHD

CHD(Coverage Hole Detection)는 커버리지 구멍을 식별하고 교정하는 별도의 알고리즘입니다. CHD는 전역적으로 구성되며 WLAN별로 구성됩니다. CHD의 가능한 영향은 커버리지 홀(클라이언트가 지속적으로 불량 신호로 감지되는 영역)을 보상하기 위한 Tx 전력의 증가이며, 이 영향은 무선 수준이며 CHD에 구성된 단일 WLAN에 의해 트리거되는 경우에도 모든 WLAN에 영향을 미칩니다.

대형 공용 네트워크는 일반적으로 RF 프로필을 사용하여 특정 전력 수준으로 구성되며, 일부 클라이언트는 개방된 지역에 있을 수 있으며, 클라이언트가 해당 지역을 오가며 로밍할 수 있습니다. 이러한 클라이언트 이벤트에 응답하여 AP Tx 전력을 동적으로 조정하는 알고리즘이 필요하지 않습니다.

대규모 공용 네트워크에서는 CHD를 전역적으로 비활성화해야 합니다.

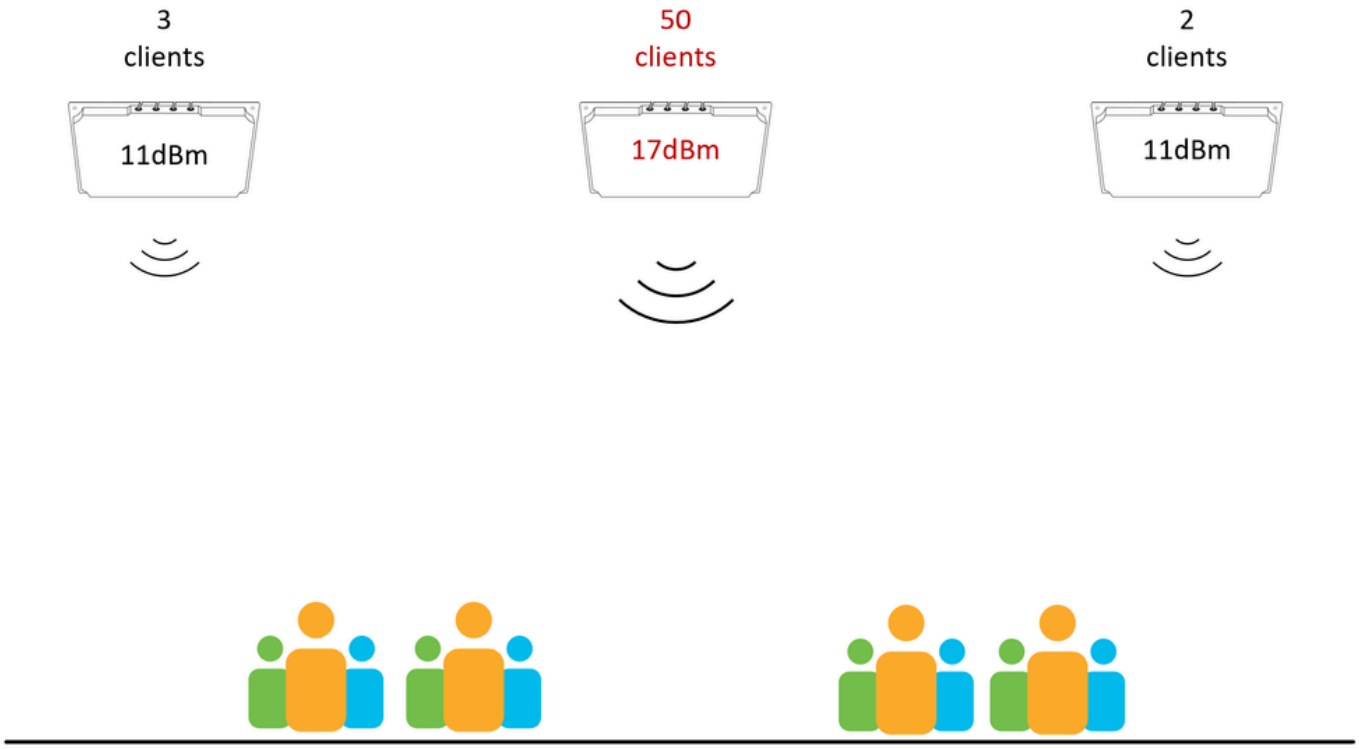
전원 균형

대부분의 클라이언트 디바이스는 연결할 AP를 선택할 때 더 높은 수신 신호를 선호합니다. AP가 주변 다른 AP에 비해 Tx 전력이 상당히 높게 구성된 상황은 피해야 합니다. Tx가 높은 상태에서 작동하는 AP는 더 많은 클라이언트를 유치하므로 AP 간에 클라이언트 분배가 불규칙합니다(예: 단일 AP/무선 장치가 클라이언트에 과부하되고 주변 AP의 활용도가 낮음). 이러한 상황은 다중 안테나에서 커버리지가 큰 구축 및 하나의 AP에 다중 안테나가 연결된 경우 일반적입니다.

C9104와 같은 경기장 안테나는 안테나 빔이 설계에 따라 중첩되므로 Tx 전력을 선택할 때 각별히

주의해야 합니다. 이에 대한 자세한 내용은 Catalyst 9104 Stadium Antenna (C-ANT9104) Deployment Guide를 참조하십시오.

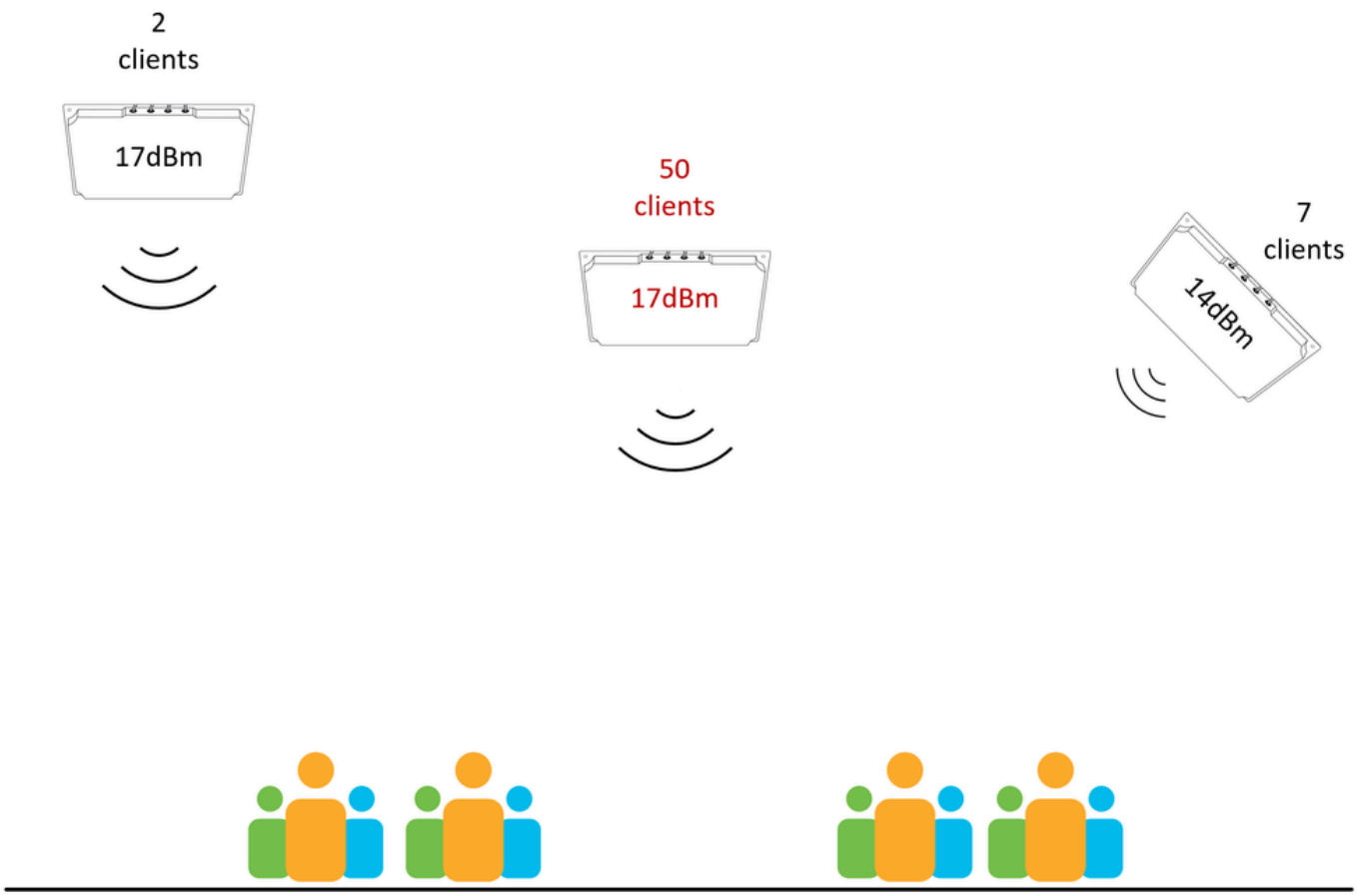
아래 다이어그램에서 중간 안테나는 주변 안테나보다 높은 Tx 전력으로 구성된다. 이러한 컨피그레이션으로 인해 클라이언트가 중간 안테나에 '고착'될 수 있습니다.



인접 AP보다 전력이 높은 AP는 주변의 모든 클라이언트를 끌어들입니다

다음 다이어그램은 더 복잡한 상황을 보여줍니다. 모든 안테나가 동일한 높이에 있는 것은 아니며 모든 안테나가 동일한 기울기/방향을 사용하는 것도 아닙니다. 균형 잡힌 전력을 달성하는 것은 단순히 동일한 Tx 전력으로 모든 무선 장치를 구성하는 것보다 더 복잡합니다. 이와 같은 시나리오에서는 구축 후 사이트 설문조사가 필요할 수 있습니다. 이 설문조사를 통해 클라이언트 디바이스의 관점에서 현장 지원 범위를 확인할 수 있습니다. 그런 다음 설문조사 데이터를 사용하여 최상의 커버리지와 클라이언트 배포를 위한 컨피그레이션의 균형을 맞출 수 있습니다.

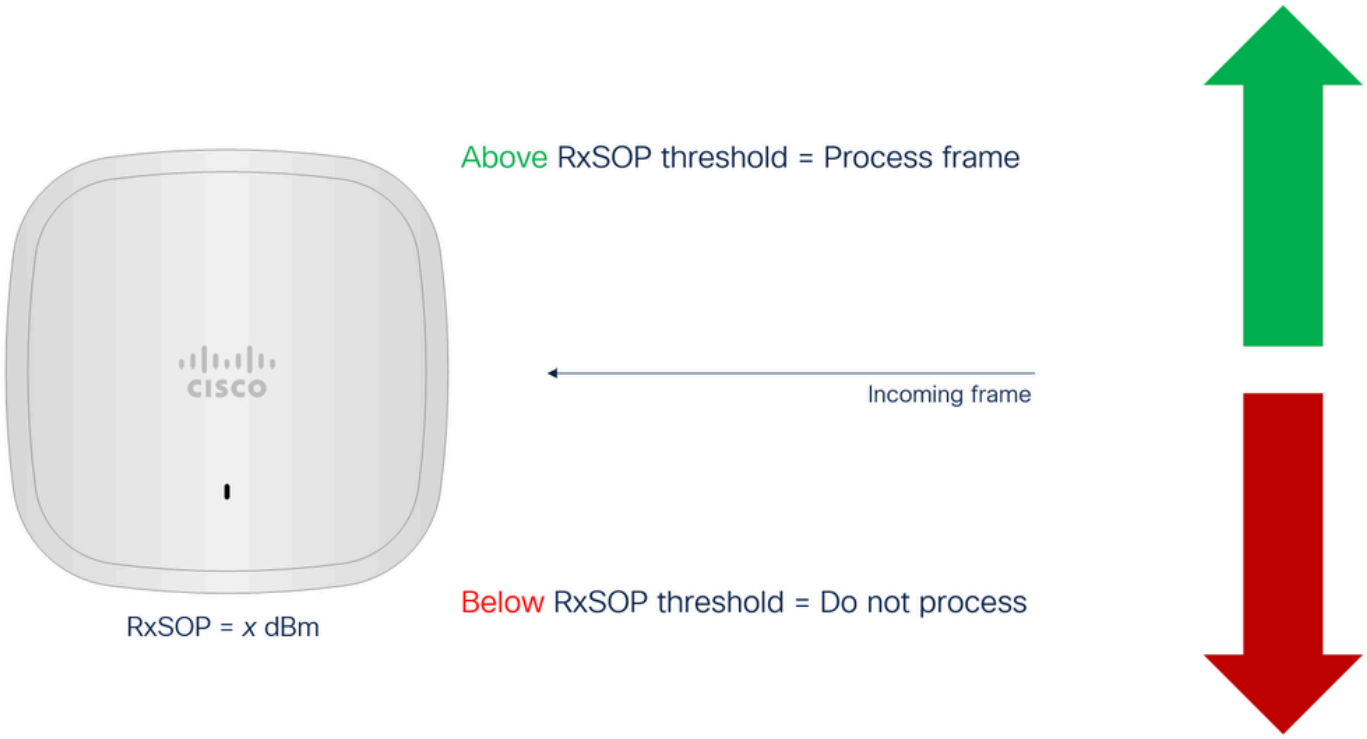
이와 같은 복잡한 상황을 피하는 균일한 AP 배치 위치를 설계하는 것이 어려운 RF 튜닝 시나리오를 방지하는 가장 좋은 방법입니다(때로는 다른 선택의 여지가 없습니다!).



Tx 전력이 비슷하지만 하나의 AP가 모든 클라이언트를 끌어들이고 있지만 높이와 각도가 그 역할을 합니다

RxSOP

전송 셀의 특성에 영향을 주는 Tx 전력이나 데이터 전송률과 같은 메커니즘과 달리, RxSOP(Receiver Start of Packet Detection)는 수신 셀의 크기에 영향을 주는 것을 목표로 합니다. 본질적으로, RxSOP는 AP가 전송을 디코딩하려고 시도하지 않는 수신 신호 레벨을 정의한다는 점에서 노이즈 임계값으로 간주할 수 있습니다. 구성된 RxSOP 임계값보다 약한 신호 레벨로 도착하는 모든 전송은 AP에서 처리되지 않으며 노이즈로 효과적으로 처리됩니다.



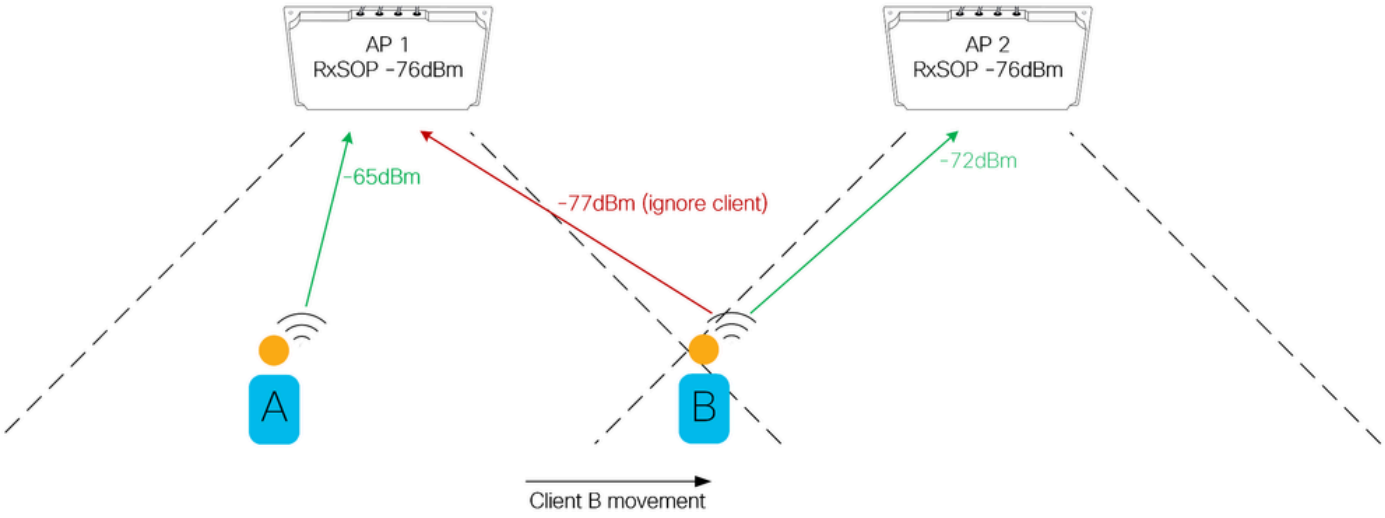
RxSOP 개념 설명

RxSOP의 중요성

RxSOP에는 여러 가지 용도가 있습니다. 노이즈가 많은 환경에서 AP를 전송할 수 있는 기능을 개선하고, 안테나 간 클라이언트 분배를 제어하며, 더 약하고 끈적한 클라이언트에 최적화하는 데 사용할 수 있습니다.

잡음 환경의 경우, 802.11 프레임을 전송하기 전에 전송 스테이션(이 경우에는 AP)에서 먼저 미디어의 가용성을 평가해야 하며, 이 프로세스의 일부는 이미 수행된 전송을 먼저 수신해야 합니다. 밀집된 Wi-Fi 환경에서는 많은 AP가 비교적 제한된 공간에 공존하는 것이 일반적이며 동일한 채널을 사용하는 경우가 많습니다. 이러한 바쁜 환경에서 AP는 주변 AP(반사 포함)로부터의 채널 활용을 보고하고 자체 전송을 지연시킬 수 있습니다. 적절한 RxSOP 임계값을 설정하면 AP가 이러한 약한 전송을 무시할 수 있습니다(감지된 채널 사용률 감소). 이는 더 빈번한 전송 기회와 향상된 성능으로 이어집니다. AP가 클라이언트 로드 없이 상당한 채널 사용률(예: 10% 이상)을 보고하는 환경(예: 빈 장소)은 RxSOP 튜닝에 적합합니다.

RxSOP를 사용한 클라이언트 최적화를 위해 이 다이어그램을 고려해 보십시오.



rxsop의 영향을 받는 클라이언트 로밍

이 예에는 커버리지 영역이 잘 정의된 2개의 AP/안테나가 있습니다. 클라이언트 B가 AP1의 커버리지 영역에서 AP2의 커버리지 영역으로 이동하고 있습니다. AP2가 AP1보다 클라이언트를 더 잘 수신하지만 클라이언트가 아직 AP2로 로밍하지 않는 크로스오버 지점이 있습니다. 이는 RxSOP 임계값을 설정하여 커버리지 영역의 경계를 적용하는 방법을 잘 보여 주는 예입니다. 클라이언트가 항상 가장 가까운 AP에 연결되어 있도록 보장하면 더 낮은 데이터 속도로 제공되는 원거리 및/또는 약한 클라이언트 연결이 제거되어 성능이 향상됩니다. 이와 같이 RxSOP 임계값을 구성하려면 각 AP의 예상 커버리지 영역이 어디에서 시작되고 종료되는지 철저히 파악해야 합니다.

RxSOP의 위험.

AP가 유효한 클라이언트 디바이스에서 유효한 전송을 디코딩하지 않으므로 RxSOP 임계값을 너무 적극적으로 설정하면 커버리지 구멍이 발생합니다. 이는 AP가 응답하지 않기 때문에 클라이언트에 불리한 결과를 초래할 수 있습니다. 결국, 클라이언트 전송이 들리지 않은 경우 응답할 이유가 없습니다. RxSOP 임계값 조정은 신중하게 수행해야 하며, 항상 구성된 값이 커버리지 영역 내의 유효한 클라이언트를 제외하지 않도록 해야 합니다. 일부 클라이언트는 이러한 방식으로 무시되는 것에 잘 대응할 수 없습니다. 너무 적극적인 RxSOP 설정은 클라이언트가 자연스럽게 로밍할 수 있는 기회를 제공하지 않으므로 클라이언트가 다른 AP를 찾도록 효과적으로 강제합니다. AP로부터 비컨을 디코딩할 수 있는 클라이언트는 해당 AP로 전송할 수 있다고 가정하므로 RxSOP 튜닝의 목적은 수신 셀의 크기를 AP의 비콘 범위와 일치시키는 것입니다. (유효한) 클라이언트 디바이스가 항상 AP에 직접적인 가시선을 갖는 것은 아니며, 안테나를 외면하고 있거나 디바이스를 가방이나 주머니에 넣고 다니는 사용자에 의해 신호가 약화되는 경우가 많습니다.

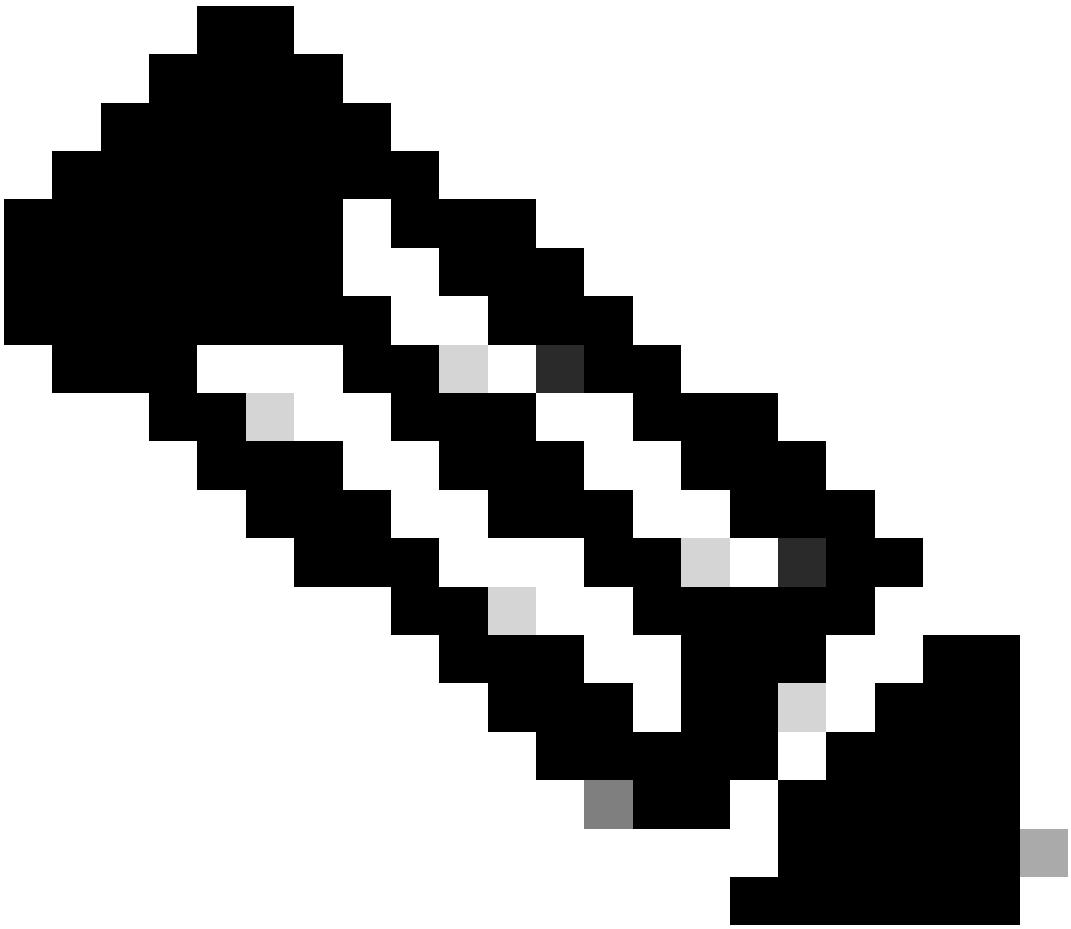
RxSOP 구성

RxSOP는 RF 프로필에 따라 구성됩니다.

대역별로 미리 설정된 임계값(Low/Medium/High)이 미리 정의된 dBm 값을 설정합니다. 여기서는 원하는 값이 사용 가능한 사전 설정인 경우에도 항상 사용자 지정 값을 사용하는 것이 좋습니다. 이렇게 하면 컨피그레이션을 더 쉽게 읽을 수 있습니다.

Setting	Value
Auto	Not configured
Low	-80dBm
Medium	-78dBm
High	-76dBm
Custom	-60dBm to -85dBm

RxSop 설정 테이블



참고: RxSOP를 변경할 경우 무선 재설정이 필요하지 않으며 즉석에서 변경할 수 있습니다.

네트워크 확장

일반적으로, 장치를 문서화된 기능의 최대치에 사용하는 것은 좋지 않은 생각입니다. 데이터 시트는 진실을 보고하지만, 언급된 수치는 활동의 특정 조건에 있을 수 있습니다. 무선 컨트롤러는 특정 수의 클라이언트와 AP 및 특정 처리량을 지원하도록 테스트 및 인증되었지만, 이는 클라이언트가 매초마다 로밍한다고 가정하지 않습니다. 즉, 각 클라이언트에 대해 매우 긴 고유한 ACL을 구성하거나 사용 가능한 모든 스누핑 기능을 활성화할 수 있습니다. 따라서 피크 시간대에 네트워크를 확장하고 향후 성장에 대비한 안전 여유를 유지하기 위해서는 모든 측면을 신중하게 고려하는 것이 중요합니다.

AP 수

모든 네트워크를 구축하는 첫 번째 작업 중 하나는 적절한 양의 장비를 예산 책정하고 주문하는 작업이며, 가장 큰 변수 요인은 액세스 포인트 및 안테나의 수와 유형입니다. 무선 솔루션은 항상 무선 주파수 설계를 기반으로 해야 하지만(안타깝게도) 이는 프로젝트 라이프사이클의 두 번째 단계입니다. 간단한 실내 엔터프라이즈 구축의 경우, 무선 설계자가 평면도를 살펴보기 전에 필요한 AP의 수를 합리적인 수준으로 예측할 수 있는 다양한 추정 기술이 있습니다. 예측 모델은 또한 이러한 경우에 매우 유용할 수 있다.

산업용, 실외, 대형 공용 네트워크 또는 외부 안테나가 필요한 장소와 같이 까다로운 설치 환경에서는 간단한 추정 기술이 적합하지 않은 경우가 많습니다. 필요한 장비의 종류와 양을 적절하게 추정하기 위해서는 이전 유사한 설치에 대해 어느 정도의 경험이 필요합니다. 무선 설계자의 사이트 방문은 복잡한 장소나 시설의 레이아웃을 이해하는 최소한의 방법입니다.

이 섹션에서는 지정된 구축의 최소 AP 및 안테나 수를 결정하는 방법에 대한 지침을 제공합니다. 최종 수량 및 특정 장착 위치는 항상 요구 사항 분석 및 무선 설계 프로세스를 통해 결정됩니다.

초기 BOM은 안테나 유형과 안테나 수량의 두 가지 요소를 기반으로 해야 합니다.

안테나 유형

지름길은 없습니다 안테나 유형은 커버해야 하는 영역과 해당 영역의 사용 가능한 마운팅 옵션에 따라 결정됩니다. 물리적 공간을 파악하지 못하면 이를 확인할 수 없습니다. 즉 안테나와 해당 커버리지 패턴을 파악한 사용자가 현장을 방문해야 합니다.

안테나 수량

필요한 장비 수량은 예상되는 클라이언트 연결 양을 파악하여 도출할 수 있습니다.

사람당 장치 수

사람 사용자 수는 장소의 좌석 용량, 판매 티켓 수, 또는 역사 통계에 따라 예상 방문자 수에 의해 결정 할 수 있습니다. 각 사람 사용자는 여러 개의 장치를 휴대할 수 있으며 사용자당 하나 이상의 장치를 가정하는 것이 일반적입니다. 그러나 한 사람이 동시에 여러 장치를 적극적으로 사용할 수 있는 능력은 의심스럽습니다. 네트워크에 능동적으로 연결하는 방문자의 수도 이벤트 및/또는 구축의 유형에 따라 달라집니다.

예 1: 80,000석 경기장에는 연결된 장치가 80,000개가 없는 것이 정상이며, 이 비율은 일반적으로

상당히 낮습니다. 스포츠 경기 중 연결 사용자 비율이 20%인 경우가 드물지 않습니다. 즉, 80,000석 경기장의 경우 예상 연결 장치 수가 16,000개(80,000 x 20% = 16,000)가 될 수 있습니다. 이 번호는 또한 사용되는 온보딩 메커니즘에 따라 다릅니다. 사용자가 웹 포털 클릭 등의 일부 작업을 수행해야 하는 경우 디바이스 온보딩이 자동인 경우보다 숫자가 더 낮습니다. 자동 온보딩은 이전 이벤트에서 기억된 PSK처럼 간단할 수도 있고, 사용자 상호 작용 없이 장치에 온보딩하는 OpenRoaming을 사용하는 것과 같이 더 발전된 것일 수도 있습니다. OpenRoaming 네트워크는 사용자 수용 비율을 50%를 훨씬 상회할 수 있으며, 이는 용량 계획에 큰 영향을 미칠 수 있습니다.

예 2: 기술 컨퍼런스의 사용자 연결 비율이 높을 것으로 예상하는 것이 합리적입니다. 회의 참석자는 네트워크에 더 오래 연결되었고, 하루 종일 이메일에 액세스하고 일상적인 작업을 수행할 수 있기를 기대합니다. 또한 이러한 유형의 사용자가 둘 이상의 디바이스를 네트워크에 연결하는 경우가 더 많지만, 여러 디바이스를 동시에 사용할 수 있는지는 여전히 미심쩍습니다. 기술 컨퍼런스의 경우 방문자의 100%가 네트워크에 연결된다는 가정 하에 컨퍼런스 유형에 따라 이 수치가 더 낮을 수 있습니다.

두 예에서 모두, 핵심은 예상되는 연결된 디바이스 수를 파악하는 것이며 모든 대규모 공용 네트워크에 대한 단일 솔루션이 없습니다. 어느 경우든 안테나는 라디오에 연결되며, 해당 라디오에 연결하는 것은 클라이언트 장치(사람 사용자가 아님)입니다. 따라서 라디오당 클라이언트 디바이스는 사용 가능한 메트릭입니다.

라디오당 디바이스 수

Cisco AP의 최대 클라이언트 수는 Wi-Fi 6 AP의 경우 라디오당 연결된 장치 수가 200개이고 Wi-Fi 6E AP의 경우 라디오당 장치가 400개입니다. 그러나 클라이언트 수를 최대화하기 위해 설계하는 것은 바람직하지 않습니다. 계획 목적상 라디오당 클라이언트 수를 최대 AP 용량의 50% 미만으로 유지하는 것이 좋습니다. 또한 무선 장치 수는 사용되는 AP 및 안테나 유형에 따라 다르며, 단일 및 이중 5GHz의 섹션에서 이를 더 자세히 살펴봅니다.

이 단계에서는 영역당 예상 디바이스 수를 사용하여 네트워크를 개별 영역으로 분할하는 것이 좋습니다. 이 섹션에서는 최소 AP 및 안테나 수를 추정합니다.

세 가지 커버리지의 예를 들어 보겠습니다. 각 영역에 대해 예상되는 클라이언트 수가 제공되며 필요한 무선 장치 수를 예상하는 데 무선 장치당 75개 클라이언트의 (정상) 값이 사용됩니다.

Area	Expected Devices	Devices / Radio	Radios
Area 1	1000	75	14
Area 2	2000	75	27
Area 3	2500	75	34
Total			75

영역당 예상 무선 장치/클라이언트 수

이러한 초기 번호는 각 영역에 어떤 유형의 AP 및 안테나가 구축되었는지, 그리고 단일 또는 이중 5GHz가 사용되는지 이해하는 것과 결합해야 합니다. 6GHz 계산은 5GHz와 동일한 논리를 따릅니다. 이 예에서는 2.4GHz를 고려하지 않습니다.

세 영역에서 각각 2566P 패치 안테나와 9104 스타디움 안테나의 조합을 사용하며 단일 및 이중 5GHz의 조합을 사용한다고 가정해 보겠습니다. 이 시나리오는 설명을 위해 사용됩니다.

Area	Total Radios	2566P (Dual 5GHz)	2566P (Single 5GHz)	9104 (Dual 5GHz)
Area 1	14	0	6	4
Area 2	27	6	3	6
Area 3	34	7	0	10
Total Antennas		26	9	20
Total APs		13	9	0 (integrated)

면적당 안테나 수

각 영역에는 필요한 안테나 및 AP의 유형이 나열됩니다. 듀얼 5GHz의 경우 안테나 2개와 AP 1개의 비가 있습니다.

이 섹션에서는 구축에 필요한 안테나 및 AP의 초기 수를 추정하는 방법을 설명합니다. 이 추정에는 물리적 영역, 각 영역의 가능한 장착 옵션, 각 영역에서 사용할 안테나 유형, 예상되는 클라이언트 장치 수에 대한 이해가 필요합니다.

각 구축은 서로 다르며 특정 또는 까다로운 영역을 지원하기 위해 추가 장비가 필요한 경우가 많습니다. 이러한 유형의 예측은 클라이언트 용량(지원 범위가 아님)만 고려하고 필요한 투자 규모를 개략적으로 설명하는 역할을 합니다. 최종 AP/안테나 배치 위치 및 장비 층계는 항상 숙련된 무선 전문가가 활용 사례와 현장 검증을 철저히 해야 합니다.

예상 처리량

각 무선 채널은 일반적으로 처리량으로 변환되는 가용 용량을 제공할 수 있습니다. 이 용량은 무선에 연결된 모든 장치 간에 공유되므로, 더 많은 사용자 연결이 무선에 추가될수록 각 사용자의 성능이 저하됩니다. 이러한 성능 감소는 선형적이지 않으며 연결된 클라이언트의 정확한 조합에 따라 달라집니다.

클라이언트 기능은 클라이언트 칩셋 및 클라이언트가 지원하는 공간 스트림 수에 따라 장치마다 다릅니다. 지원되는 각 공간 스트림 수에 대한 최대 클라이언트 데이터 속도는 아래 표에 나와 있습니다.

Client Capability	20MHz channel Wi-Fi 5 (802.11ac)	20MHz channel Wi-Fi 6 (802.11ax)
1 Spatial Stream(s)	86.7Mbps	121.9Mbps
2 Spatial Stream(s)	173.3Mbps	243.8Mbps
3 Spatial Stream(s)	288.9Mbps	365.6Mbps
4 Spatial Stream(s)	346.7Mbps	487.5Mbps

각 클라이언트 유형에 대해 예상되는 최대 실제 처리량

나열된 속도는 802.11 표준에서 파생된 이론적인 최대 MCS(Modulation and Coding Scheme) 속도이며 SNR(Signal-to-Noise Ratio) >30dBm을 가정합니다. 성능이 우수한 무선 네트워크의 주요 설계 목표는 모든 위치의 모든 클라이언트에 대해 이 수준의 SNR을 달성하는 것이지만, 이는 거의 그렇지 않습니다. 무선 네트워크는 기본적으로 동적이며 라이센스가 없는 주파수를 사용합니다. 클라이언트 기능 외에도 제어되지 않은 다양한 간섭이 클라이언트 SNR에 영향을 미칩니다.

필요한 수준의 SNR이 달성되는 경우에도, 앞서 나열한 속도는 프로토콜 오버헤드를 고려하지 않으므로, (다양한 속도 테스트 툴에 의해 측정된) 실제 처리량에 직접 매핑하지 않습니다. 전반적인 실제 환경은 항상 MCS 속도보다 낮습니다.

모든 무선 네트워크(대형 공용 네트워크 포함)에서 클라이언트 처리량은 항상 다음에 따라 달라집니다.

- 클라이언트의 기능.
- 해당 특정 시점의 클라이언트 신호 대 잡음 비율
- 해당 특정 시점에 연결된 다른 클라이언트 수입니다.
- 해당 특정 시점의 다른 클라이언트 기능
- 해당 특정 시점의 다른 클라이언트 활동
- 특정 시점에서의 간섭.

이러한 요인의 가변성에 따라 장비 공급업체에 관계없이 무선 네트워크 전반에 걸쳐 클라이언트당 최소 수를 보장할 수 없습니다.

자세한 내용은 Wi-Fi 처리량 검증: 테스트 및 모니터링 가이드를 참조하십시오.

WLC 플랫폼

WLC 플랫폼을 선택하는 것은 쉬워 보일 수 있습니다. 가장 먼저 생각나는 것은 관리하고자 하는 예상 AP 수와 클라이언트 수를 살펴보는 것입니다. 각 WLC 플랫폼의 데이터 시트에는 플랫폼에서 지원되는 모든 최대 객체(ACL, 클라이언트 수, 사이트 태그 등)가 포함되어 있습니다. 그것들은 문자 그대로 최대 숫자이고 종종 엄격한 적용이 있다. 예를 들어 6000 AP만 지원하는 9800-80에는 6001 AP를 조인할 수 없습니다. 하지만 어디에서나 최대를 목표로 하는 것이 현명할까?

Cisco 무선 컨트롤러는 이러한 최대값에 도달할 수 있는 것으로 테스트되지만, 모든 조건에서 모든 문서화된 최대값에 동시에 도달할 필요는 없습니다. 처리량의 예를 들어, 9800-80은 최대 80Gbps의 클라이언트 데이터 포워딩에 도달할 수 있지만, 이는 각 클라이언트 패킷이 1500바이트의 최대 및 최적 크기인 경우입니다. 패킷 크기를 혼합하면 최대 유효 처리량이 더 적습니다. DTLS 암호화를 활성화하면 처리량이 더욱 감소하며 Application Visibility(애플리케이션 가시성)도 마찬가지입니다. 9800-80의 경우 많은 기능이 활성화된 대규모 네트워크의 현실적인 조건에서 40Gbps 이상을 기대할 수 있을 것으로 낙관적입니다. 이는 사용 중인 기능과 네트워크 활동 유형에 따라 크게 다르므로 이 명령을 사용하여 데이터 경로 활용률을 측정하는 방법만이 용량에 대한 실제 개념을 얻을 수 있습니다. 컨트롤러에서 전달할 수 있는 최대 처리량의 백분율인 로드 메트릭에 초점을 맞춥니다.

```
WLC#show platform hardware chassis active qfp datapath utilization summary

  CPP 0:                      5 secs        1 min        5 min       60 min

Input:     Total (pps)            9            5            5            8

                  (bps)        17776         7632         9024        10568

Output:    Total (pps)            5            3            3            6

                  (bps)        11136        11640        11440        41448

Processing: Load (pct)            0            0            0            0


WLC#
```

마찬가지로, 9800-80은 정기적인 활동을 통해 6000개의 AP를 완벽하게 처리할 수 있습니다. 그러나 경기장이나 공항 같은 공공장소의 AP 6000개는 정규 활동에 포함되지 않습니다. 클라이언트 로밍 및 주변 프로빙의 양을 고려하면 최대 규모의 대형 공용 네트워크는 단일 WLC에서 CPU 사용률을 높일 수 있습니다. 클라이언트가 이동할 때마다 전송할 모니터링 및 SNMP 트랩을 추가하면 로드가 너무 커집니다. 대규모 공용 행사장이나 대규모 이벤트의 주요 특징 중 하나는 사람들이 이동하며 항상 연결/연결 해제됨에 따라 클라이언트 온보딩 이벤트가 상당히 많아진다는 것입니다. 따라서 CPU 및 컨트롤 플레인에 부담이 가중됩니다.

여러 구축 사례를 통해 9800-80 무선 컨트롤러 한 쌍으로 1,000개 이상의 AP가 있는 대규모 스타디움 구축을 처리할 수 있음을 알 수 있습니다. 또한 가동 시간과 가용성이 가장 큰 문제가 되는 중요한 이벤트를 위해 둘 이상의 컨트롤러 쌍에 AP를 배포하는 것이 일반적입니다. 대형 네트워크가 여러 WLC를 통해 분산되는 경우 컨트롤러 간 로밍이 복잡해지기 때문에 스타디움 볼과 같은 제한된 공간에서는 클라이언트 로밍을 신중하게 고려해야 합니다.

이 문서의 사이트 태그 섹션도 참조하십시오.

WLC 고가용성

HA SSO(High-Availability Stateful Switch Over) 쌍을 사용하는 것이 좋습니다. 이 쌍은 하드웨어 이

중화를 제공할 뿐 아니라 소프트웨어 오류도 방지합니다. HA SSO를 사용하면 보조 WLC가 원활하게 작동하므로 한 디바이스에서 소프트웨어 충돌이 최종 사용자에게 투명하게 발생합니다. HA SSO 쌍의 또 다른 장점은 ISSU(In-Service Software Upgrade) 기능이 제공하는 무중단 업그레이드입니다.

네트워크가 충분히 클 경우 추가 컨트롤러(N+1)를 사용하는 것도 좋습니다. HA SSO가 수행할 수 없는 여러 가지 용도로 사용할 수 있습니다. 프로덕션 쌍을 업그레이드하기 전에 이 WLC에서 새 소프트웨어 버전을 테스트할 수 있습니다(그리고 네트워크의 특정 섹션을 테스트하기 위해 몇 개의 테스트 AP만 마이그레이션할 수 있음). 몇 가지 드문 상황은 HA 쌍의 두 WLC에 영향을 미칠 수 있습니다(문제가 스탠바이에 복제되는 경우). 여기서 N+1은 AP를 점진적으로 마이그레이션할 수 있는 액티브-액티브 시나리오에서 안전한 WLC를 가질 수 있습니다. 또한 새 AP를 구성하기 위한 프로비저닝 컨트롤러 역할을 할 수도 있습니다.

9800-CL은 확장성이 뛰어나고 강력합니다. SR-IOV 이미지의 경우 2Gbps에서 4Gbps까지 데이터 포워딩 용량이 훨씬 작기 때문에 FlexConnect 로컬 스위칭 시나리오(그리고 중앙 스위칭의 AP 수가 적을 수 있음)로 제한될 수 있습니다. 그러나 유지 보수 기간 중에 또는 문제를 해결할 때 추가 컨트롤러가 필요한 경우 N+1 장치로 유용할 수 있습니다.

외부 시스템

이 문서에서는 주로 대형 이벤트 네트워크의 무선 구성 요소에 초점을 맞추고 있지만, 확장 및 설계 단계에서 고려해야 하는 지원 시스템도 무수히 많습니다. 이러한 지원 시스템 중 일부는 여기에서 설명합니다.

코어 네트워크

대형 무선 네트워크는 일반적으로 중앙 스위칭 모드에서 대형 서브넷과 함께 구축됩니다. 이는 매우 많은 수의 클라이언트 MAC 주소 및 ARP 항목이 인접한 유선 인프라로 푸시됨을 의미합니다. 다양한 L2 및 L3 기능을 전담하는 인접 시스템이 이 부하를 처리할 수 있는 적절한 리소스를 보유하는 것이 중요합니다. L2 스위치의 경우 공통 컨피그레이션은 시스템 리소스 할당을 담당하는 SDM(Switch Device Manager) 템플릿 조정이며, 네트워크 내 디바이스의 기능에 따라 L2와 L3 기능 간의 균형을 조정합니다. 코어 L2 장치가 예상되는 MAC 주소 항목 수를 지원할 수 있는지 확인하는 것이 중요합니다.

게이트웨이 NAT

공용 네트워크의 가장 일반적인 활용 사례는 방문자에게 인터넷 액세스를 제공하는 것입니다. 데이터 경로를 따라 어딘가에 NAT/PAT 변환을 담당하는 디바이스가 있어야 합니다. 인터넷 게이트웨이는 로드를 처리하는 데 필요한 하드웨어 리소스 및 IP 풀 컨피그레이션을 보유해야 합니다. 단일 무선 클라이언트 디바이스가 수많은 NAT/PAT 변환을 담당할 수 있다는 점을 기억하십시오.

DNS/DHCP

이 두 시스템은 우수한 고객 경험을 보장하는 데 핵심적인 역할을 합니다. DNS 및 DHCP 서비스 모두 로드를 처리하기 위해 적절한 확장이 필요할 뿐 아니라 네트워크 내 배치에 대해서도 고려해야 합니다. WLC와 동일한 위치에 빠르고 대응성이 뛰어난 시스템을 배치하여 최상의 환경을 보장하고 긴 클라이언트 온보딩 시간을 피할 수 있습니다.

AAA/웹 포털

느린 웹 페이지를 좋아하는 사람은 없습니다. 외부 웹 인증에 적합하고 확장 가능한 시스템을 선택하는 것은 좋은 클라이언트 온보딩 경험에 중요합니다. AAA의 경우에도 마찬가지로 RADIUS 인증 서버는 무선 시스템의 요구 사항을 처리할 수 있어야 합니다. 경우에 따라 로드가 중요 순간 동안, 예를 들어 축구 경기 중 30분 동안 급증할 수 있으며, 이로 인해 적은 시간에 높은 인증 로드가 발생할 수 있습니다. 적절한 동시 로드를 위해 시스템을 확장하는 것이 중요합니다. AAA 어카운팅과 같은 기능을 사용할 때는 특별히 주의해야 한다. 모든 비용에서 시간 기반 회계를 피하고 회계를 사용하는 경우 중간 회계를 비활성화합니다. 고려해야 할 또 다른 중요한 사항은 로드 밸런서의 사용이며, 여기서 세션 파이닝 메커니즘은 완전한 인증 흐름을 보장하기 위해 사용되어야 합니다. RADIUS 시간 초과를 5초 이상으로 유지해야 합니다.

클라이언트 수가 많은 802.1X SSID를 사용하는 경우(예: OpenRoaming) 802.11r FT(Fast Transition)를 활성화해야 합니다. 그렇지 않으면 클라이언트가 로밍할 때마다 인증 폭풍이 발생할 수 있습니다.

DNS/DHCP

DHCP에 대한 몇 가지 권장 사항:

- DHCP 풀이 예상되는 클라이언트 수의 3배 이상인지 확인합니다. IP는 클라이언트의 연결이 끊긴 후에도 일정 시간 동안 할당된 상태로 유지되므로 게스트의 체류 시간에 따라 더 많은 IP 주소를 사용할 수 있습니다. 임대 시간을 사용자가 현장을 방문하는 예상 기간과 일치시키십시오. 일반적인 방문 기간이 2시간이면 1주일 동안 IP 주소를 할당해도 소용이 없으므로 오래된 임대가 만료됩니다.
- 클라이언트에 단일 대형 서브넷을 사용하는 것이 좋습니다. WLC는 프록시 ARP 기능을 갖추고 있으며 기본적으로 브로드캐스트(DHCP 제외)를 전달하지 않습니다. 클라이언트에 대해 큰(예: /16) 클라이언트 서브넷을 사용하는 것은 문제가 되지 않습니다. 하나의 큰 VLAN은 많은 VLAN을 가진 VLAN 그룹에 비해 더 간단합니다. 더 작은 서브넷(예: /24) 및 VLAN 그룹을 많이 구성하면 브로드캐스트 도메인에 영향을 주지 않으며 컨피그레이션이 더 복잡해지기 때문에 더티(dirty) VLAN과 같은 문제가 발생하고 균등하게 사용할 수 없는 다양한 DHCP 풀을 추적해야 합니다.
- 서브넷의 레이어 3 게이트웨이에서 처리하는 DHCP 릴레이 기능을 사용하여 무선 컨트롤러에서 DHCP를 브리징 모드로 유지합니다. 이를 통해 효율성과 단순성을 극대화할 수 있습니다. DHCP 프로세스에 무선 컨트롤러를 전혀 사용하지 않는 것이 좋습니다.
- 인증 방법과 상관없이 모든 공용 WLAN에서 DHCP Required(DHCP 필수)를 사용합니다. 이 경우 클라이언트 연결 실패의 작은 비율을 트리거할 수 있지만, 클라이언트가 고정 IP 주소를 할당하려고 시도하거나 클라이언트가 잘못된 동작을 시도하고 허가 없이 이전 IP 주소를 재사용하려고 시도하여 심각한 보안 문제를 방지할 수 있습니다.

네트워크 운영

올바른 구성

현대적인 Wi-Fi의 모든 최신 기능을 활용할 수 있는 다양한 옵션을 선택해 보십시오. 그러나 일부 기능은 소규모 환경에서 효과적이지만 크고 밀도가 높은 환경에서는 큰 영향을 미칩니다. 마찬가지로

, 특정 기능은 호환성 문제를 일으킬 수 있습니다. Cisco 장비는 모든 표준을 준수하며 테스트된 다양한 클라이언트와 호환되지만, 세상은 종종 버그가 있거나 특정 기능과 호환되지 않는 드라이버 소프트웨어 버전을 가진 고유한 클라이언트 장치로 가득 차 있습니다.

클라이언트에 대한 제어의 수준에 따라 보수적이어야 합니다. 예를 들어, 회사의 대규모 연례 모임에 Wi-Fi를 구축하는 경우 대부분의 클라이언트가 회사 장치이며 그에 따라 활성화할 기능 집합을 계획할 수 있습니다. 반면, 공항 Wi-Fi를 운영하는 경우, 게스트 만족도는 네트워크에 연결할 수 있는 기능과 직접적으로 관련이 있으며, 사용자가 사용할 수 있는 클라이언트 장치에 대한 제어권이 없습니다.

SSID

SSID는 몇 개입니까?

항상 가능한 한 적은 수의 SSID를 사용하는 것이 좋습니다. 이는 동일한 채널에 여러 AP가 있을 가능성이 거의 보장되므로 고밀도 네트워크에서 악화됩니다. 일반적으로 많은 구축에서 SSID를 너무 많이 사용하고, SSID가 너무 많다는 것을 인정하지만 더 적게 사용할 수는 없다고 선언합니다. SSID와 여러 SSID를 하나로 축소하는 옵션 간의 유사성을 파악하려면 각 SSID에 대해 비즈니스 및 기술 연구를 수행해야 합니다.

몇 가지 보안/SSID 유형과 그 용도를 살펴보겠습니다.

WPA2/3 개인

사전 공유 키 SSID는 단순성으로 인해 매우 널리 사용됩니다. 열쇠는 배지나 종이나 표지판에 인쇄하거나 방문객에게 어떻게든 전달할 수 있습니다. 게스트 SSID에 대해서도 사전 공유 키 SSID가 선호되는 경우가 있습니다(모든 참석자가 해당 키를 잘 알고 있는 경우). 고의적인 연결 특성으로 인해 DHCP 풀이 고갈되는 것을 방지할 수 있습니다. 통과하는 디바이스는 네트워크에 자동으로 연결되지 않으므로 DHCP 풀의 IP 주소를 사용할 수 없습니다.

WPA2 PSK는 모든 사용자가 동일한 키를 사용하므로 트래픽의 암호를 쉽게 해독할 수 있으므로 개인 정보를 제공하지 않습니다. 반대로, WPA3 SAE는 개인 정보를 제공합니다. 모든 사용자가 마스터 키를 가지고 있더라도 다른 클라이언트에서 사용하는 암호화 키를 파생할 수 없습니다.

WPA3 SAE는 보안을 위해 더 나은 선택이며 많은 스마트폰, 노트북 및 운영 체제가 이를 지원합니다. 일부 IoT 장치나 스마트 웨어러블은 여전히 제한된 지원을 받을 수 있으며, 일반적으로 오래된 클라이언트는 최신 드라이버나 펌웨어 업데이트를 받지 못할 경우 문제에 취약합니다.

상황을 단순화하기 위해 전환 모드 WPA2 PSK-WPA3 SAE SSID를 고려하는 것이 좋을 수 있지만, 일부 호환성 문제를 일으키기 위해 이 방법이 필드에 표시되어 있습니다. 제대로 프로그래밍되지 않은 클라이언트는 동일한 SSID에 두 가지 유형의 공유 키 방법을 사용할 수 없습니다. WPA2 및 WPA3 옵션을 모두 제공하려면 별도의 SSID를 구성하는 것이 좋습니다.

WPA2/3 엔터프라이즈

WPA3 Enterprise(AES 128비트 암호화 사용)는 WPA2 Enterprise와 기술적으로 동일한 보안 방법(최소한 SSID 신호에서 알려진 방법)으로, 최대 호환성을 제공합니다.

802.1X의 경우, 전환 모드 SSID는 최신 디바이스에서 호환성 문제가 나타나지 않으므로 권장됩니다(Android 8 또는 이전 Apple IOS 버전에서 문제가 보고됨). IOS XE 17.12 이상 릴리스에서는 단일 Transition Enterprise SSID를 사용할 수 있습니다. 여기서 6GHz에서는 WPA3만 사용되고 광고되며 5GHz 대역에서는 WPA2가 옵션으로 제공됩니다. 가능한 한 빨리 엔터프라이즈 SSID에서 WPA3를 활성화하는 것이 좋습니다.

WPA 엔터프라이즈 SSID는 사용자 ID에 따라 AAA 매개 변수(예: VLAN 또는 ACL)를 반환할 수 있는 ID 공급자 데이터베이스가 있는 키 사용자에게 사용할 수 있습니다. 이러한 유형의 SSID에는 게스트 SSID(방문자가 자격 증명을 입력하지 않고도 쉽게 연결할 수 있음)의 이점을 기업 SSID의 보안과 결합하는 Eduroam 또는 OpenRoaming이 포함될 수 있습니다. 클라이언트가 자신의 전화기에 프로파일이 있는 경우(이벤트 앱을 통해 쉽게 제공될 수 있음), euroam 또는 OpenRoaming SSID에 가입하기 위해 아무것도 할 필요가 없기 때문에 일반적으로 802.1X와 관련된 온보딩의 복잡성을 크게 줄여줍니다

게스트 SSID

게스트 SSID는 종종 개방형 인증과 동의어입니다. 외부, 로컬 또는 중앙 웹 인증과 같은 다양한 형식으로 웹 포털 뒤에(원하는 친절 또는 로컬 요구 사항에 따라) 웹 포털을 추가할 수 있지만 개념은 동일합니다. 게스트 포털을 사용할 경우 대규모 환경에서 확장성이 신속하게 문제가 될 수 있습니다. 이에 대한 자세한 내용은 Configuring for Scalability 섹션을 참조하십시오.

6GHz 운영에서 게스트 SSID를 사용하려면 Open이 아닌 Enhanced Open을 사용해야 합니다. 이렇게 하면 누구나 연결할 수 있지만 SSID에서 연결할 때 키나 자격 증명을 제공하지 않고도 프라이버시(WPA2-PSK보다 나은 프라이버시!)와 암호화를 제공할 수 있습니다. 주요 스마트폰 공급업체와 운영 체제는 이제 Enhanced Open을 지원하지만, 무선 클라이언트 기반에서는 아직 지원이 널리 보급되지 않았습니다. Enhanced Open 전환 모드는 (Enhanced Open을 사용하여) 지원되는 디바이스가 암호화된 게스트 SSID에 연결되고, 지원되지 않는 디바이스는 SSID를 이전처럼 단순히 열린 상태로 사용하는 양호한 호환성 옵션을 제공합니다. 최종 사용자는 단일 SSID만 인식하지만, 이 전환 모드는 비콘에서 두 개의 SSID를 브로드캐스트합니다(하나만 표시됨).

대규모 이벤트 및 장소에서는 게스트 SSID를 완전히 열어 두지 말고 게스트 SSID에 PSK를 구성하는 것이 좋습니다(Enhanced Open Transition(개방형 전환 강화) 모드가 더 낫지만 두 개의 SSID를 생성하고 클라이언트 호환성은 계속 광범위하게 검증되어야 함). 따라서 온보딩이 좀 더 복잡해지지만(PSK를 사람들의 배지나 티켓에 인쇄하거나 어떻게든 광고해야 함), 일반 클라이언트가 네트워크를 사용할 의향이 없어도 네트워크에 자동으로 연결되는 것을 방지합니다. 점점 더 많은 모바일 운영 체제 공급업체에서도 개방형 네트워크의 우선 순위를 내리고 보안 경고를 표시합니다. 다른 상황에서는 최대 수의 행인이 연결되기를 원할 수 있으므로 열려 있는 것이 더 좋습니다.

SSID 수에 대한 결론

몇 개의 SSID를 고수해야 하는 지에 대한 질문에 만족스러운 답변이 있을 수 없습니다. 효과는 최소 구성된 데이터 속도, SSID 수 및 동일한 채널에서 브로드캐스트하는 AP 수에 따라 달라집니다. 하나의 대형 Cisco 이벤트에서 무선 인프라는 5개의 SSID를 사용했습니다. 기본 WPA2 PSK, 보안을 위한 WPA 3 SAE SSID 및 6GHz 범위, 교육 참석자의 용이한 액세스를 위한 엔터프라이즈 Eduroam SSID, 이벤트 앱에서 Wi-Fi를 구성한 사용자를 안전하게 환영하는 OpenRoaming SSID 및 직원 및 관리 네트워크 액세스를 위한 별도의 802.1X SSID. 이는 이미 거의 과도했지만 사용 가능한 채널 수가 많고 채널 중복을 최대한 줄이는 데 사용되는 지향성 안테나 덕분에 효과가 합리적

으로 유지되었습니다.

레거시 SSID 대 기본 SSID 개념

특정 기간에는 2.4GHz 서비스를 2.4GHz에서만 광고되는 "레거시" 개별 SSID로 제한하는 것이 좋습니다. 이는 사람들이 2.4GHz 서비스를 완전히 중단함에 따라 점점 더 인기가 떨어지고 있습니다. 그러나, 그 아이디어는 다른 개념들과 함께 지속될 수 있고 지속되어야만 한다. WPA3 SAE를 롤아웃하려고 하지만 전환 모드에서 클라이언트와 호환성 문제가 발생합니까? WPA2 "Legacy" SSID 및 기본 WPA3 SAE SSID가 있습니다. 가장 성능이 낮은 SSID의 이름을 "레거시"로 지정하면 클라이언트가 관심을 끌지 않으며, 주 SSID와 호환성 문제가 지속되고 이 레거시 SSID를 필요로 하는 클라이언트의 수를 쉽게 확인할 수 있습니다.

그런데 왜 거기서 멈췄지? 802.11v로 인해 일부 이전 클라이언트에 문제가 발생했거나 일부 클라이언트 드라이버에서 SSID에 Device Analytics가 활성화되어 있지 않다는 소문을 들었습니다. 고급 기본 SSID에서 이러한 모든 핸디 기능을 활성화하고 레거시/호환성 SSID에서 이를 해제합니다. 이렇게 하면 주 SSID에서 새로운 기능의 롤아웃을 테스트하는 동시에, 클라이언트가 폴백할 수 있는 최대 호환성 SSID를 계속 제공할 수 있습니다. 이 시스템은 오직 이런 식으로만 작동합니다. 다른 이름으로 호환성 기반 SSID를 기본 이름으로 사용하고 고급 SSID를 "<name>-WPA3"과 같은 이름으로 지정하는 경우, 기존 SSID를 고수하는 사용자가 있음을 알 수 있으며, "new" SSID에 대한 채택 기간은 수년입니다. 새 설정 또는 기능을 롤아웃하면 연결되는 클라이언트 수가 적기 때문에 최종 결과가 없습니다.

SSID 기능

- Aironet Extensions를 비활성화하는 것이 가장 좋습니다. 이는 사이트 설문조사 및 WGB 운영에 특히 유용하지만 일부 레거시 클라이언트에 문제가 발생할 수 있습니다. Aironet IE는 또한 보안 중심 구축에서 원치 않는 AP 호스트 이름을 광고합니다.
- CCKM은 더 이상 사용되지 않는 프로토콜(FT 사용)이며 비활성화되어야 합니다.
- 이때 WPA3에서도 AES-128 암호화를 사용하는 것이 가장 좋습니다. 더 높은 암호화에 대한 클라이언트 지원이 낮기 때문입니다(특정 더 안전하고 제한적인 SSID를 구입할 수 있는 경우가 아니면)
- Coverage Hole Detection(커버리지 홀 탐지)은 모든 SSID에 대해 가장 많이 비활성화됩니다. 대규모 구축에서는 일반적으로 지향성 안테나를 사용하므로 철저한 사이트 조사가 필요합니다. 각 안테나의 전력 레벨은 RF 설계 프로세스의 결과일 것이며, 일반적으로 특정 레벨로 구성된다.
- FT가 완전히 보급되지 않았지만 일부 특성에 있는 경우 일부 클라이언트에 문제가 발생할 수 있으므로 적응형 FT를 비활성화해야 합니다. FT를 완전히 비활성화하거나(최대 호환성을 위해) 대부분의 클라이언트가 지원하는 FT+802.1X를 사용합니다(이전 버전이거나 IoT 지향적이지 않은 경우). FT+802.1X를 구성할 때 FT가 아닌 클라이언트도 SSID에 참가할 수 있습니다. 가능한 유일한 문제는 동일한 SSID에서 두 가지 보안 옵션이 표시되는 것을 허용하지 않는 일부 클라이언트에 있습니다.
- 802.11ac MU-MIMO를 비활성화합니다. 802.11ac에서는 복잡성이 가중되고 혜택도 매우 적습니다.
- BSS Target Wake Time을 비활성화합니다. 현재 클라이언트 측 도입률이 낮은 편입니다.
- 적극적인 로드 밸런싱 및 대역 선택을 비활성화합니다. 2.4GHz로 SSID를 알리지 않는 경우(또는 전용 SSID에 있는 경우) Band Select가 필요하지 않으며, 적극적인 로드 밸런싱은 로드

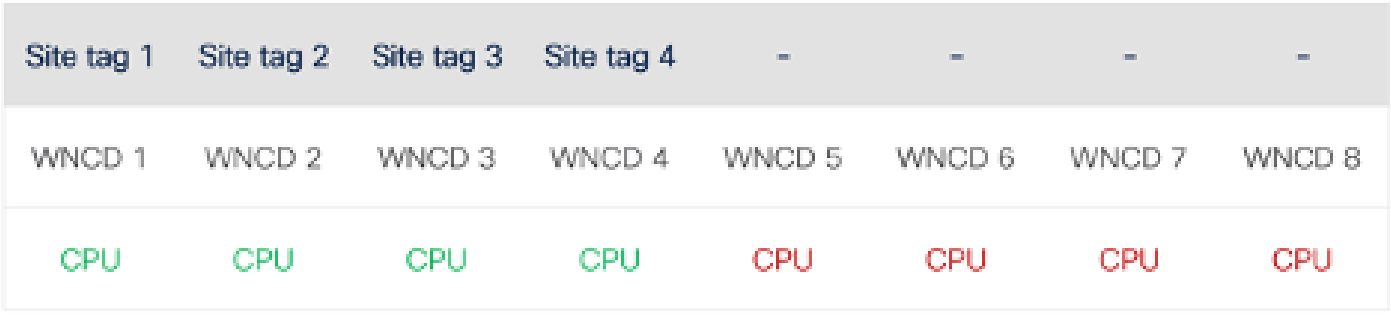
된 AP에 연결을 고집하는 경우 마지막으로 수락하기 전에 클라이언트를 몇 번 거부하여 클라이언트 연결을 지연시킵니다. 바쁜 환경에서 AP를 로드했으며 이는 클라이언트 환경에 부정적인 영향을 미칩니다.

- Fastlane+를 비활성화합니다.
- Universal Admin을 비활성화합니다. 이 기능은 3700 AP에 대한 것이며 -UX 도메인에서만 사용됩니다. 그대로 두면 불필요한 공격 벡터가 열립니다.
- OKC(Opportunistic Key Caching)를 사용하도록 설정합니다. FT를 지원하지 않는 클라이언트의 빠른 로밍 메커니즘 역할을 합니다.
- WMM을 계속 허용합니다. 이를 비활성화하면 네트워크가 802.11g 시대로 돌아가게 되며 9800 플랫폼에서는 이러한 요구 사항이 도움이 되지 않습니다.
- IP Source Guard를 활성화합니다.
- RADIUS 프로파일링 비활성화 매우 바쁜 환경에서는 클라이언트가 DHCP 또는 HTTP 패킷을 보낼 때마다 과도한 RADIUS 계정 관리 메시지를 보낼 수 있으며 RADIUS 서버를 과부하 시킬 가능성이 매우 높습니다.
- 숨겨진 SSID를 사용하지 마십시오. 이는 어떤 보안 목적도 제공하지 않습니다. SSID 이름은 간단한 애플리케이션이나 스니퍼 캡처를 통해 쉽게 검색할 수 있습니다. SSID를 숨기면 모든 클라이언트 로밍이 느려집니다. 패시브 비컨 스캐닝의 이점을 더 이상 누릴 수 없으며, 인접 AP 정보를 얻기 위해 액티브 스캐닝에 의존해야 하기 때문입니다.
- RF 사용률에 큰 영향을 미치므로 라디오당 4개 이상의 WLAN을 사용하지 마십시오. 5개의 WLAN을 사용하는 것이 효과적일 뿐 아니라 점점 더 많은 WLAN을 사용하므로 통신 시간이 낭비된다는 점을 잘 알고 있습니다.
- 802.11v 및 802.11k는 널리 사용되는 클라이언트 유형에서 점점 더 많이 지원하는 표준입니다. 일반적으로 클라이언트 연결과 관련해서는 문제가 발생하지 않습니다. 이러한 프로토콜의 장점은 클라이언트가 이러한 프로토콜을 어떻게 활용하는지에 따라 크게 달라지는데, 때때로 (802.11k의 경우) CPU 사용량이 약간 증가할 수 있습니다. IoT 또는 레거시 SSID에서 이들을 보호할 수 있지만 프로덕션 SSID에서 가능한 경우 이들을 활성화해야 합니다.

사이트 태그

사이트 태그는 동일한 FlexConnect 설정은 물론 AP 가입 프로필 설정(예: 자격 증명, SSH 세부사항 및 국가 코드)을 공유하는 액세스 포인트를 그룹화할 수 있는 구성 항목입니다. 사이트 태그가 중요한 이유 사이트 태그는 또한 Catalyst 9800 내부의 WNCD 프로세스에서 AP를 처리하는 방법을 정의합니다. 몇 가지 예를 들어 보겠습니다.

- 8개의 WNCD 프로세스가 있는 9800-80에서 4개의 사이트 태그를 구성하는 경우, 각 사이트 태그가 다른 WNCD 프로세스(각각 별도의 CPU 코어에서 실행)에 할당되고 4개의 WNCD 프로세스는 아무 작업도 하지 않습니다. 즉, 9800-80의 모든 CPU를 사용하고 있지 않으며 최대 6000개의 지원되는 AP로 로드하는 것이 권장되지 않습니다.



사이트 태그 밸런싱의 첫 번째 예

- 8개의 WNCD 프로세스가 있는 9800-80에서 10개의 측면 태그를 구성하는 경우, 2개의 WNCD 프로세스는 각각 2개의 사이트 태그를 처리하고 나머지 6개는 각각 1개의 사이트 태그를 처리합니다.

Site tag 1 Site tag 9	Site tag 2 Site tag 10	Site tag 3	Site tag 4	Site tag 5	Site tag 6	Site tag 7	Site tag 8
WNCD 1	WNCD 2	WNCD 3	WNCD 4	WNCD 5	WNCD 6	WNCD 7	WNCD 8
CPU	CPU	CPU	CPU	CPU	CPU	CPU	CPU

사이트 태그 밸런싱의 두 번째 예

많은 사이트와 많은 사이트 태그가 있는 지리적으로 대규모 구축의 경우 사이트 태그 수는 사용 중인 플랫폼에서 WNCD 프로세스 수의 배수인 것이 좋습니다.

그러나 일반적으로 한 지붕 아래 있거나 동일한 장소에 있는 여러 건물인 이벤트 네트워크의 경우 사이트 태그 수를 지정된 플랫폼의 정확한 WNCD 수와 일치시키는 것이 좋습니다. 최종 목표는 각 WNCD 프로세스(및 이에 따라 무선 작업에 할당된 각 CPU 코어)에서 대략 비슷한 수의 클라이언트 로밍 이벤트를 처리하여 모든 CPU 코어에서 로드 밸런싱을 수행하는 것입니다.

Platform type	Number of WNCD processes
9800-CL small OVA	1
9800-CL medium OVA	3
9800-CL large OVA	7
9800-L	1
9800-40/CW9800-M	5
9800-80/CW9800-H	8

각 플랫폼 유형에 대한 WNCD 프로세스 수

핵심은 동일한 물리적 환경에 있는 AP를 동일한 사이트 태그로 그룹화하여 이러한 AP 간의 빈번한 클라이언트 로밍 이벤트가 동일한 CPU 프로세스에서 유지되도록 하는 것입니다. 즉, 하나의 큰 장소를 가지고 있더라도 장소를 여러 개의 사이트 태그(장소를 처리하는 WNCD 프로세스가 있는 만큼)로 나누고 가능한 한 논리적으로 AP를 이러한 태그로 그룹화하여 사이트 태그 간에 고르게 분포된 논리적 RF 인접 그룹을 형성하는 것이 좋습니다.

IOS XE 17.12부터 WLC가 RF 근접성을 기준으로 AP를 그룹화하도록 로드 밸런싱 알고리즘을 활성화할 수 있습니다. 이렇게 하면 사용자의 부담이 사라지고 WNCD 프로세스 전반에 걸쳐 AP가 균형 있게 분산됩니다. 이 방법은 사이트 태그의 정확한 양에 배치할 인접 AP 그룹을 쉽게 그릴 수 없

는 경우에 유용합니다. 이 알고리즘의 한 가지 특이점은 AP가 사이트 태그 할당과 상관없이 WNCD 프로세스에 AP를 할당한다는 것입니다. 즉, AP의 사이트 태그 할당을 변경하지 않습니다. 그런 다음 구성 로직에서 순전히 기본적인 사이트 태그를 할당하고 알고리즘이 CPU 간에 가장 최적의 방식으로 AP의 균형을 조정하도록 할 수 있습니다.

RF 기반 자동 AP 로드 밸런싱 기능은 Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Dublin 17.12.x에 설명되어 있습니다.

대규모 이벤트 중에 WNCD 프로세스의 CPU 사용량을 모니터링해야 합니다. 하나 이상의 WNCD 프로세스가 높은 활용률을 보일 경우, WNCD가 너무 많은 AP 또는 클라이언트를 처리하고 있거나, 처리하는 AP 또는 클라이언트가 평균보다 더 많을 수 있습니다(예: 모든 AP 또는 클라이언트가 공항에서처럼 지속적으로 로밍하는 경우).

정책 프로파일

- ARP 및 DAD(Duplicate Address Detection) 프록시를 활성화하면 디바이스가 무선 디바이스의 MAC 주소를 학습하려고 할 때 WLC가 무선 클라이언트 대신 회신할 수 있습니다. 또한 무선 클라이언트 배터리도 절약됩니다.
- 필요한 경우가 아니면 WGB 기능을 활성화하지 마십시오.
- 고정 IP 주소를 사용하는 클라이언트를 방지하려면 DHCP를 활성화해야 합니다.
- 유휴 시간 제한을 짧게 유지합니다(300초). 일부 관리자는 클라이언트를 다시 인증하지 않도록 오래 걸리지만, 유휴 시간 초과가 길면 클라이언트 수가 실시간으로 지연되어 고스트 클라이언트 항목이 발생하고 보고에 영향을 미칩니다. 클라이언트가 삭제될 때 어카운팅 플러드를 방지하려면 유휴 시간 -timeout을 그룹 키 순환 타이머보다 낮게 유지하는 것이 좋습니다. 웹 UI의 Configuration(컨피그레이션) > Security(보안) > Advanced EAP(고급 EAP) 아래에서 그룹 키 순환 간격을 "EAP-Broadcast Key Interval(EAP 브로드캐스트 키 간격)"으로 구성할 수 있습니다.
- 불필요한 연결 끊기 및 재인증을 방지하려면 세션 시간 제한을 86400초로 설정합니다.

AP 조인 프로파일

- TCP adjust MSS(TCP 조정 MSS)가 활성화되었는지 확인합니다.
- Trust DSCP 업스트림을 활성화합니다. 많은 무선 클라이언트가 802.11e WMM UP 태깅을 수행하지 않습니다. DSCP 필드를 신뢰하는 것이 음성 애플리케이션에 올바른 우선 순위를 제공하는 확실한 방법입니다.
- 액세스 포인트에 대해 Syslog를 활성화합니다. Syslog 서버 IP를 구성하면 AP가 콘솔 로그를 유니캐스트합니다. AP 트러블슈팅에 유용할 뿐만 아니라 AP가 로컬 VLAN에서 Syslog를 브로드캐스트하도록 하는 기본 설정보다 네트워크에 더 적합합니다. AP 로깅은 AP Syslog가 모니터링되지 않는 경우에도 상당한 메시지 로드를 생성할 수 있습니다. 적절한 메시지 심각도를 설정하거나 메시지 브로드캐스트를 방지하기 위해 더미 Syslog IP 주소(예: 0.0.0.0)를 구성하여 이벤트 수를 제한하는 것이 좋습니다.
- CAPWAP 재시도 및 시간 제한을 최대화합니다. 문제는 더 빨리 감지되지만 네트워크는 사소한 일시적 패킷 삭제에 더 잘 견뎌냅니다.
- SSH를 활성화하고 자격 증명을 구성합니다. AP 콘솔을 비활성화합니다.
- 필요한 경우 AP 모니터를 활성화하되 라디오 모니터는 활성화하지 않습니다.
- 비인가 탐지를 활성화하고 RSSI 임계값을 -70dBm으로 구성합니다.

네트워크 모니터링

네트워크가 가동되고 실행되면 문제를 면밀히 모니터링해야 합니다. 표준 사무실 환경에서는 사용자가 네트워크를 알고 있으며 문제가 발생할 경우 서로 도움을 주거나 내부 헬프데스크 티켓을 열 수 있습니다. 많은 방문자가 오는 더 큰 장소에서 당신은 단지 잘못된 구성을 가질 수 있는 특정 개인보다 가장 큰 문제에 초점을 맞추고 싶어, 그래서 당신은 올바른 모니터링 전략을 가져야 합니다.

Catalyst 9800 CLI 또는 GUI에서 네트워크를 모니터링할 수는 있지만 매일 모니터링하는 데 가장 적합한 툴은 아닙니다. 문제에 대한 의심이나 데이터가 이미 있고 특정 명령을 실시간으로 실행하고자 할 때 가장 직접적인 방법입니다. 주요 모니터링 옵션은 Cisco Catalyst Center 또는 잠재적으로 맞춤형 텔레메트리 대시보드입니다. 서드파티 모니터링 툴을 사용할 수도 있지만 SNMP를 프로토콜로 사용하는 경우 데이터가 실시간 모니터링 툴과 거리가 멀며 일반적인 서드파티 모니터링 툴은 모든 무선 공급업체의 특성에 비해 세분화되지 않습니다. SNMP 프로토콜을 선택하는 경우 SNMPv2에 오래된 보안이 있으므로 SNMPv3을 사용해야 합니다.

Cisco Catalyst Center는 모니터링뿐만 아니라 네트워크를 관리할 수 있는 최상의 옵션입니다. 모니터링 이상의 기능을 통해 실시간 문제 해결 및 여러 상황 해결 가능

사용자 지정 텔레메트리 대시보드는 NOC 또는 SOC에 대해 매우 특정한 메트릭 및 위젯을 상시 방식으로 화면에 표시하려는 경우에 유용할 수 있습니다. 네트워크의 특정 영역을 주시하고 싶은 경우 전용 위젯을 만들어 해당 영역의 네트워크 메트릭을 원하는 방식으로 표시할 수 있습니다.

이벤트 네트워크의 경우 시스템 전체의 RF 통계, 특히 채널 사용률 및 AP당 클라이언트 수를 모니터링하는 것이 좋습니다. 이는 CLI에서 수행할 수 있지만 특정 시점의 스냅샷만 제공합니다. 채널 활용도는 동적인 경향이 있으며 시간이 지남에 따라 모니터링하는 데 더 적합합니다. 이러한 모니터링 유형에서는 일반적으로 사용자 지정 대시보드를 사용하는 것이 좋습니다. 시간이 지남에 따라 모니터링할 때 더 유용한 기타 메트릭으로는 WNCD 사용률, 클라이언트 및 해당 상태 수, 장소별 메트릭이 있습니다. 장소 특정 메트릭의 예로는 특정 지역 또는 위치(예: 컨퍼런스 센터의 경우 홀 X, 이벤트 장소의 경우 좌석 공간 Y)에 대한 사용량 및/또는 부하를 모니터링하는 것이 있습니다.

맞춤형 모니터링의 경우 NETCONF RPC(풀) 및 NETCONF 스트리밍 텔레메트리(푸시) 모두 유효한 접근 방식이지만, Catalyst Center와 함께 맞춤형 스트리밍 텔레메트리를 사용하려면 약간의 부지런함이 필요합니다. WLC에 구성할 수 있는 텔레메트리 서브스크립션의 수에는 제한이 있으며 Catalyst Center는 이러한 서브스크립션 중 상당수를 미리 채웁니다(및 활용).

NETCONF RPC를 사용하는 경우 WLC가 NETCONF 요청으로 오버로드되지 않도록 일부 테스트가 필요합니다. 특히 일부 데이터 포인트의 새로 고침 비율과 데이터가 반환되는 데 걸리는 시간을 염두에 두어야 합니다. 예를 들어, AP 채널 사용률이 60초마다 새로 고쳐지고(AP에서 WLC로) 1000개 AP에 대한 RF 메트릭을 수집하는 데 몇 초가 걸릴 수 있습니다. 이 예에서는 5초마다 WLC를 폴링하는 것이 유용하지 않으며, 3분마다 시스템 전반의 RF 메트릭을 수집하는 것이 더 나은 방법입니다.

NETCONF는 항상 SNMP보다 우선합니다.

마지막으로, DHCP 풀 사용률, 코어 라우터의 NAT 항목 수 등을 비롯한 코어 네트워크 구성 요소의 모니터링을 간과할 수 없습니다. 이 중 하나에 장애가 발생할 경우 무선 중단의 원인이 될 수 있습니다.

대규모 네트워크별 문제

웹 인증을 사용하는 SSID가 있는 경우 한 가지 문제는 해당 SSID에 연결하고 IP 주소를 얻지만 엔드 유저가 연결을 적극적으로 시도하지 않기 때문에 인증되지 않는 클라이언트일 수 있습니다(장치가 자동으로 연결됨). 컨트롤러는 웹 인증 보류 상태라고 하는 클라이언트에 의해 전송된 모든 HTTP 패킷을 가로채야 하며, 이는 WLC 리소스를 사용합니다. 네트워크가 실행되면 지정된 시간에 웹 인증 보류 상태에 있는 클라이언트의 수를 주기적으로 확인하여 기준 번호와 비교되는 방식을 확인합니다. IP Learn 상태의 클라이언트에도 마찬가지입니다. 클라이언트가 DHCP 프로세스를 수행할 때 항상 해당 상태에 있지만 네트워크에 적합한 작동 번호를 알면 기준을 설정하고 이 번호가 너무 높고 더 큰 문제를 나타낼 수 있는 순간을 식별하는 데 도움이 됩니다.

대규모 장소의 경우 웹 인증 보류 중 상태의 클라이언트를 10% 이상 확인하는 경우가 드물지 않습니다.

Day 2 모니터링: 사용자 만족도 모니터링

네트워크가 가동되고 실행되면 일반적인 두 가지 유형의 최종 사용자 불만 사항이 발생합니다. 연결이 안 되거나 연결이 끊기는 문제(연결 끊기) 또는 Wi-Fi가 예상보다 느리게 작동하고 있습니다. 후자는 주어진 영역의 실시간 밀도뿐만 아니라 속도라는 기대에 먼저 의존하기 때문에 식별하기가 매우 까다롭다. 대규모 공공 장소 네트워크를 매일 모니터링하는 데 도움이 될 수 있는 몇 가지 리소스를 살펴보겠습니다.

Wi-Fi 처리량 검증: 테스트 및 모니터링 가이드. 이 cisco.com 문서에서는 네트워크를 모니터링하여 처리량 문제를 찾아내는 방법을 다룹니다. 이 방법은 사물이 조용할 때 클라이언트가 네트워크에서 합리적으로 기대할 수 있는 처리량을 파악하고 클라이언트 수 및 로드가 증가하면 이러한 예상치가 얼마나 저하되는지 예상하는 과정을 거칩니다. 이는 최종 사용자가 처리량에 대해 불만을 제기하는 것이 기술적인 측면에서 타당한지, 타당하지 않은지, 그리고 해당 영역이 잠재적으로 직면하는 로드에 대해 다시 설계해야 하는지를 평가하는 데 매우 중요합니다.

클라이언트가 연결 문제를 보고하면 Catalyst Center에서 이를 격리하고 확인한 후 Catalyst 9800 클라이언트 연결 문제 해결 흐름을 살펴보십시오.

마지막으로, 일반적인 모범 사례로서, Monitor Catalyst 9800 KPI(Key Performance Indicators: 핵심 성과 지표)의 도움을 받아 WLC의 전반적인 주요 메트릭을 주시하십시오.

확장성을 위한 구성

9800의 SVI 및 인터페이스

WLC에서 클라이언트 VLAN에 대한 SVI를 생성하지 마십시오. 이전 AireOS WLC에 사용되던 관리자는 각 클라이언트 VLAN에 대해 레이어 3 인터페이스를 만드는 반사 기능을 가지고 있지만, 이는 거의 필요하지 않습니다. 인터페이스는 컨트롤 플레인 공격 벡터를 증가시키며, 더 복잡한 엔트리와 함께 더 많은 ACL이 필요할 수 있습니다. WLC는 기본적으로 모든 인터페이스에서 액세스할 수 있으며, 더 많은 인터페이스로 WLC를 보호하기 위해 더 많은 작업이 필요합니다. 또한 라우팅이 복잡하므로 피하는 것이 좋습니다.

IOS XE 17.9부터 mDNS 스누핑 또는 DHCP 릴레이 시나리오에 SVI 인터페이스가 더 이상 필요하

지 않습니다. 따라서 클라이언트 VLAN에서 SVI 인터페이스를 구성하는 데에는 몇 가지 이유가 있습니다.

집계된 프로브 응답

대규모 공용 네트워크의 경우 액세스 포인트에서 보낸 기본 집계 프로브 간격을 수정하는 것이 좋습니다. 기본적으로 AP는 클라이언트가 전송한 프로브에 대해 500ms마다 WLC를 업데이트합니다. 이 정보는 로드 밸런싱, 대역 선택, 위치 및 802.11k 기능에 사용됩니다. 클라이언트와 액세스 포인트가 많은 경우 WLC에서 제어 평면 성능 문제를 방지하기 위해 업데이트 간격을 수정하는 것이 좋습니다. 권장 설정은 64초마다 50개의 집계된 프로브 응답입니다. 또한 AP가 로컬로 관리되는 MAC 주소에서 프로브를 보고하지 않는지 확인하십시오. 단일 클라이언트가 의도적으로 추적을 피하는 동안 스캔하는 동안 로컬로 관리되는 여러 MAC을 사용할 수 있는 것으로 간주하는 항목을 추적하는 지점이 없기 때문입니다.

```
wireless probe limit 50 64000

no wireless probe localy-administered-mac
```

IPv6

많은 네트워크 관리자가 여전히 IPv6를 거부하고 있습니다. IPv6에는 두 가지 옵션만 사용할 수 있습니다. 즉, IPv6를 지원하고 어디에서나 적절한 구성을 구축해야 하거나 구축하지 않고 차단해야 합니다. IPV6에 대해 신경 쓰지 않고 적절한 컨피그레이션 없이 일부 장소에서 IPV6를 활성화한 상태로 두는 것은 허용되지 않습니다. 그러면 네트워크 보안이 외면할 수 있는 IP 환경이 모두 사라집니다.

IPv6을 활성화하는 경우 2001:DB8::/32 범위에서 가상 IPv6 주소를 구성해야 합니다(이 단계는 종종 잊혀집니다).

IPv6는 기본 작업에서 멀티캐스트에 많이 의존하지만, WLC에서 멀티캐스트 전달을 비활성화할 경우 여전히 작동할 수 있습니다. 멀티캐스트 전달은 클라이언트 멀티캐스트 데이터 전달을 의미하며, IPv6를 작동하기 위해 Neighbor Discovery, Router Solicitations 및 기타 필요한 프로토콜에는 해당되지 않습니다.

인터넷 연결 또는 인터넷 서비스 공급자가 IPv6 주소를 제공하는 경우 클라이언트에 대해 IPv6를 허용하도록 결정할 수 있습니다. 이는 인프라에서 IPv6를 활성화하는 것과는 다른 결정입니다. AP는 IPv4에서만 작동할 수 있지만 CAPWAP 패킷 내에서 IPv6 클라이언트 데이터 트래픽을 전달합니다. 인프라에서 IPv6를 활성화하려면 AP, WLC 및 관리 서브넷에 대한 클라이언트 액세스를 보호해야 합니다.

클라이언트 게이트웨이의 RA 빈도를 확인합니다. WLC는 클라이언트에 전달되는 RA의 수를 제한하는 RA 제한 정책을 제공하며, 이는 RA가 가끔 채팅할 수 있기 때문입니다.

mDNS

일반적으로 대규모 장소 구축에서는 mDNS를 완전히 비활성화하는 것이 가장 좋습니다.

mDNS 브리징은 mDNS 패킷을 레이어 2 멀티캐스트(따라서 전체 클라이언트 서브넷)로 전송하도록 허용하는 개념을 의미합니다. mDNS는 홈 및 소규모 사무실에서 널리 사용되는 시나리오로, 서브넷에서 서비스를 검색하는 것이 매우 실용적입니다. 그러나 대규모 네트워크에서 이는 대규모 공용 네트워크의 트래픽 관점에서 문제가 되는 서브넷의 모든 클라이언트에 패킷을 전송함을 의미합니다. 반면 브리징은 일반 데이터 트래픽으로 간주되므로 AP 또는 WLC CPU에 오버헤드를 발생시키지 않습니다. mDNS 프록시 또는 mDNS 게이트웨이는 WLC를 네트워크의 모든 서비스에 대한 디렉터리로 사용하는 개념을 의미합니다. 이를 통해 레이어 2 경계를 넘어 효율적인 방식으로 mDNS 서비스를 제공하고 전체 트래픽을 줄일 수 있습니다. 예를 들어 mDNS 게이트웨이를 사용하는 프린터는 동일한 서브넷 레이어 2 멀티캐스트를 사용하여 mDNS를 통해 정기 서비스 알림을 전송하지만 WLC는 이를 다른 모든 무선 클라이언트에 전달하지 않습니다. 대신 제공된 서비스를 메모하여 서비스 디렉토리에 등록합니다. 클라이언트가 사용 가능한 특정 유형의 서비스를 요청할 때마다 WLC가 프린터를 대신하여 알림으로 회신합니다. 그러면 다른 모든 무선 클라이언트가 불필요한 요청 및 서비스 제공에 대해 듣지 않고, 어떤 서비스가 있는지 문의할 때마다 회신만 받습니다. 트래픽 효율성을 크게 향상시키지만, mDNS 트래픽의 스누핑으로 인해 WLC(또는 FlexConnect 시나리오에서 AP mDNS에 의존하는 경우 AP)에 오버헤드가 발생하지 않습니다. mDNS 게이트웨이를 사용하는 경우 CPU 사용량을 감시하는 것이 중요합니다.

이를 브리징하면 대규모 서브넷에서 멀티캐스트 스톰이 발생하고 이를 스누핑하면(mDNS 게이트웨이 기능 사용) CPU 사용률이 높아집니다. 전역적으로 비활성화하고 각 WLAN에서도 비활성화합니다.

일부 관리자는 특정 위치에서 몇 가지 서비스에 mDNS가 필요하기 때문에 mDNS를 활성화하지만, 이를 통해 원치 않는 트래픽이 얼마나 증가하는지 파악하는 것이 중요합니다. Apple 장치는 종종 자신을 광고할 뿐만 아니라 끊임없이 서비스를 사냥하고 있습니다. 아무도 어떤 서비스를 특별히 사용하지 않는 경우에도 mDNS 쿼리의 배경 노이즈를 유발합니다. 특정 비즈니스 요구 사항으로 인해 mDNS를 허용해야 하는 경우 전역적으로 활성화한 다음 필요한 WLAN에서만 활성화하고 mDNS가 허용되는 범위를 제한합니다.

네트워크 강화

보안

대규모 공용 네트워크에서는 관리자가 모르는 사이에 많은 일이 발생할 수 있습니다. 사람들은 무작위 장소에 케이블 드롭을 요청하거나, 또는 더 많은 스위치 포트를 가진 위치에 가정용 스위치를 꽂습니다. ... 일반적으로 그들은 먼저 허가를 요청하지 않고 이러한 것들을 시도합니다. 즉, 악의적인 배우가 등장하지 않더라도 선의의 고객 및/또는 직원에 의해 이미 보안이 침해될 수 있습니다. 그러면 나쁜 배우들이 그냥 돌아다니면서 플러그를 꽂을 케이블을 찾아 거기서 어떤 네트워크 액세스를 얻는지 확인하는 것이 아주 쉬워집니다. 모든 스위치포트에서 802.1X 인증을 구성하는 것은 대규모 네트워크에서 적절한 보안을 유지하기 위한 거의 필수적인 작업입니다. Catalyst Center는 이러한 롤아웃을 자동화하는 데 도움이 될 수 있으며, 802.1X 인증을 지원하지 않는 특정 디바이스에는 예외를 둘 수 있지만 실제 보안이 아닌 MAC 기반 인증에는 최대한 적게 의존하려고 합니다.

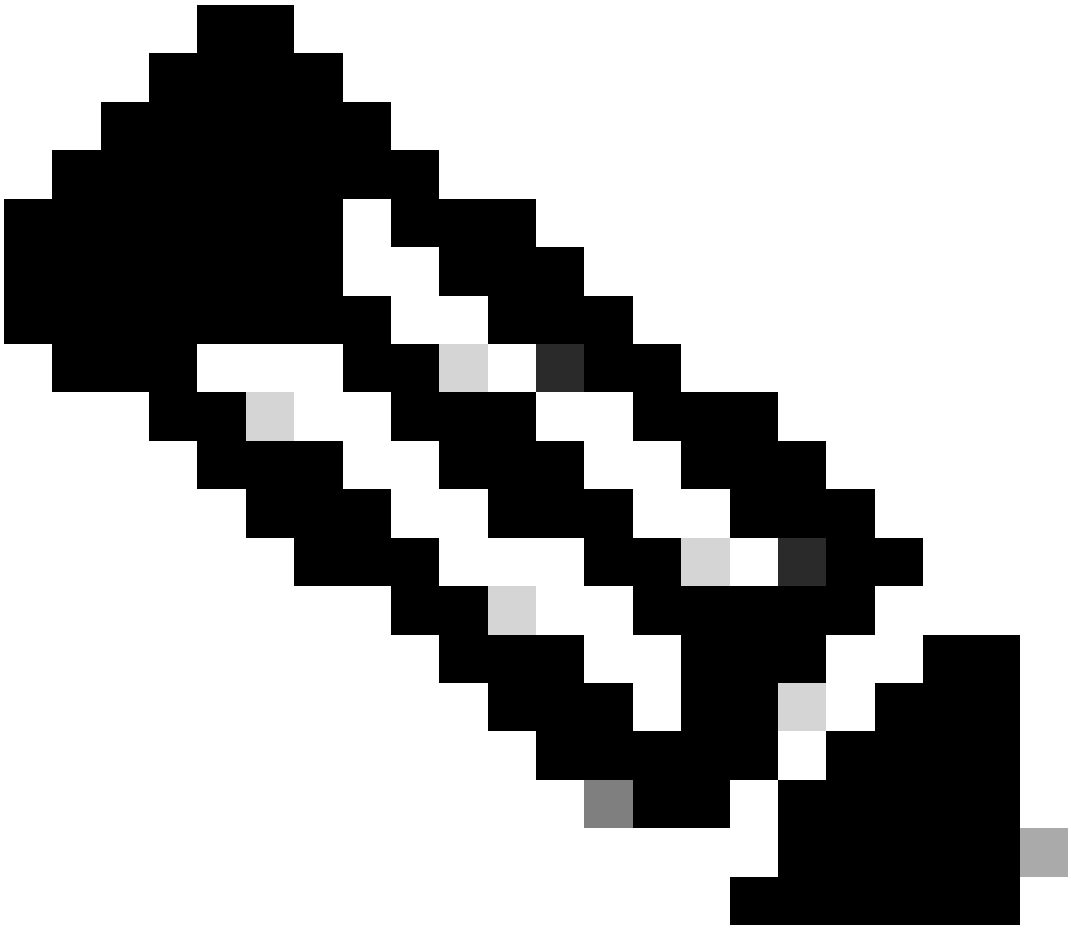
비인가 액세스 포인트

악당과 싸우는 당신의 전략은 몇 가지 요인에 달려 있다. 많은 관리자들은 본능적으로 매우 엄격한

규칙을 추구하지만, 주요 질문은 다음과 같습니다.

- 수백(수천 건 아님) 개의 비인가 알림을 받으면, 이를 모두 살펴보고 조치를 취할 수 있는 인력을 보유하고 있습니까?
- 안전한 RF 스펙트럼을 유지하기 위해 비인가를 물리적으로 제거하는 것이 목표입니까? 그렇다면 이 수술을 하려면 많은 사람이 필요합니다. 아니면 여러분의 목표는 단지 보안 요인을 주시하면서 비위가 어떤 위험도 나타내지 않도록 하는 것일 수도 있습니다. 이것은 훨씬 더 관리 가능한 인적 작업 비용이 있습니다.
- 비인가 탐지를 활성화하면 통신 시간에 영향을 미칠 수 있으며 비인가 차단은 일반적으로 더 큰 영향을 미칩니다. 이러한 영향을 분석하고 이를 고려했습니까?

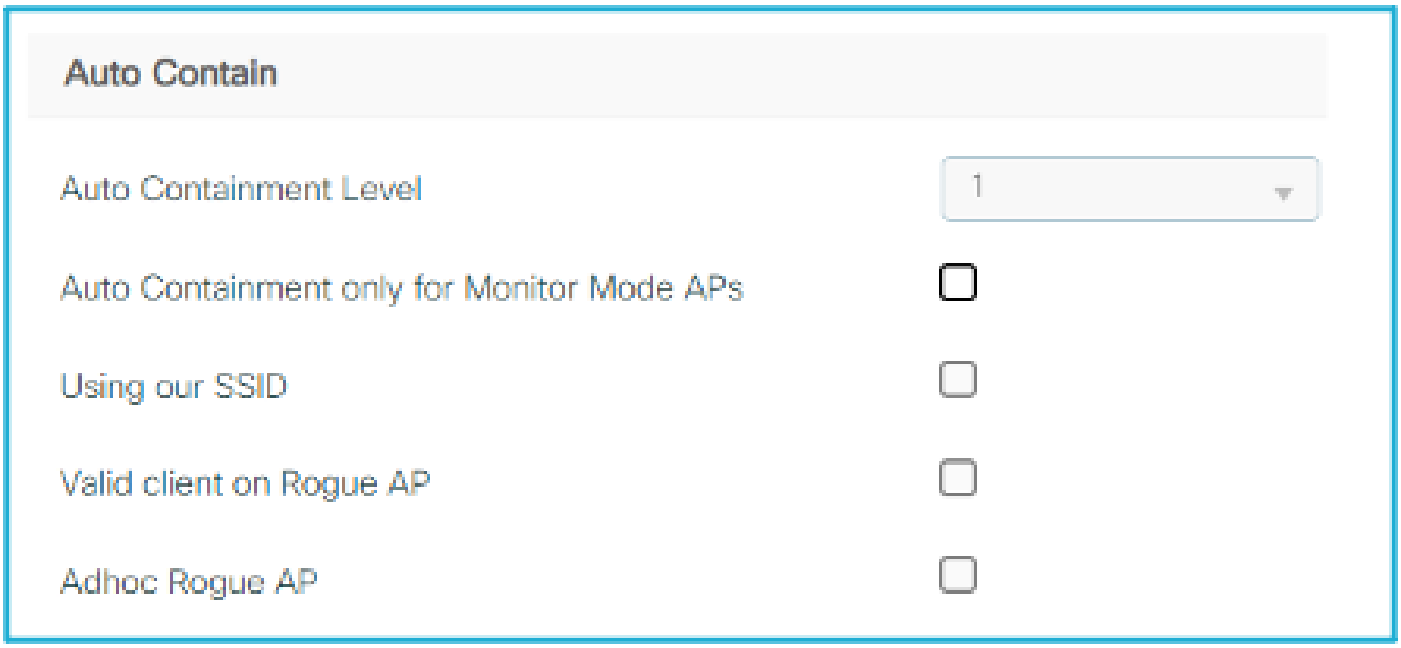
비인가 탐지의 영향과 관련하여, 9120 및 9130s에는 비인가 스캐닝을 처리하는 전용 CleanAir 칩이 있으므로 비인가 탐지가 클라이언트 제공 무선에 미치는 영향은 거의 null입니다. CleanAir Pro 칩을 탑재한 9160 Series AP는 유사한 무영향 검사 기능을 갖추고 있지만, CleanAir 칩을 탑재하지 않은 다른 AP는 비인가를 검사하거나 차단을 위해 클라이언트 제공 무선 채널을 오프채널로 전환해야 합니다. 따라서 사용 중인 AP 모델은 비인가 탐지 및 억제 여부에 전용 모니터 모드 AP를 사용하도록 결정하는 데 역할을 합니다.



참고: Wi-Fi 핫스팟을 공유하는 휴대폰은 기존 AP와 마찬가지로 '인프라' 모드에서 작동하며, '애드혹' 모드는 모바일 장치 간의 직접 연결을 의미하며 일반적이지 않습니다.

비인가 차단은 규정 규칙에 의해 금지되는 경우가 많으므로 이를 활성화하기 전에 반드시 현지 당국에 확인해야 합니다. 비인가 항목을 포함한다는 것은 비인가를 원격으로 종료하는 것이 아니라 비인가 액세스 포인트에 연결을 시도하는 클라이언트를 비인증 프레임으로 스팸하여 연결하지 못하게 하는 것입니다. 액세스 포인트가 인증 해제 프레임에 올바르게 서명할 수 없기 때문에 레거시 보안 SSID에서만 작동할 수 있습니다(WPA3에서 또는 WPA2에서 PMF가 활성화된 경우에는 작동하지 않음). 억제 기능은 AP가 인증 해제 프레임으로 통신 시간을 채우므로 대상 채널의 RF 성능에 부정적인 영향을 미칩니다. 따라서 자신의 합법적인 클라이언트가 실수로 불법 액세스 포인트에 연결하는 것을 방지하기 위한 보안 조치로만 간주해야 합니다. 언급된 모든 이유로 인해 비인가 문제가 완전히 해결되지 않고 더 많은 RF 문제를 야기하므로 어떤 억제도 하지 않는 것이 좋습니다. 컨테인먼트를 사용해야 하는 경우, 매니지드 SSID 중 하나를 스푸핑하는 악의적인 것에 대해 이를 활성화하는 것이 당연합니다. 이는 명백한 허니팟 공격이기 때문입니다.

"SSID 사용" 옵션으로 자동 억제를 구성할 수 있습니다.



자동 포함 설정

자신의 기준에 따라 악의적인 비인가 액세스 포인트로 분류하도록 비인가 규칙을 구성할 수도 있습니다. 경보 목록에서 제거하기 위해 인접 및 승인된 SSID의 이름을 친숙한 로그로 입력해야 합니다.

가장에서 AP를 보호하려면 AP 인증 또는 PMF를 활성화합니다.

유선 비인가(rogue)는 유선 네트워크에 연결된 비인가 액세스 포인트로, 보안 위협이 증가합니다. 비인가 장치의 이더넷 MAC 주소가 일반적으로 무선 MAC 주소와 다르므로 유선 비인가 장치의 탐지가 더 복잡합니다. Cisco Catalyst Center에는 비인가 유선을 탐지하고 무선 환경에서 들리고 유선 인프라에서 볼 수 있는 비인가 클라이언트 MAC을 검색하는 알고리즘이 있습니다. 유선 비인가를 모두 방지하는 최상의 솔루션은 802.1X 인증으로 모든 스위치 포트를 보호하는 것입니다.

비인가 액세스 포인트에서 물리적으로 활동하려면 Cisco Spaces를 활용하는 것이 비인가의 정확

한 위치를 파악하는 데 중요합니다. 사람들이 가끔 비인가 AP를 숨기는 경향이 있기 때문에 여전히 사이트에서 한 번 검색해야 할 가능성이 높지만 검색 영역을 몇 미터로 줄이면 매우 실현 가능한 노력이 됩니다. 스페이스가 없으면 AP 옆의 맵에 비인가 항목이 가장 크게 표시되어 검색 영역이 매우 넓습니다. 비인가 액세스 포인트의 신호를 실시간으로 보여주는 많은 무선 툴과 디바이스가 있으므로 비인가를 물리적으로 찾을 수 있습니다.

CleanAir는 비인가와 정확히 관련이 없지만, CleanAir를 지원했기 때문에 2.4GHz 성능에 영향을 미치므로 BLE 비컨 탐지를 제외한 성능에는 눈에 띄는 부정적인 영향을 미치지 않습니다. 오늘날의 세상에서는 Bluetooth 간섭 요인이 전무한 만큼 Bluetooth 간섭 요인을 모두 무시하도록 무선 환경을 구성할 수 있으며, 클라이언트가 Bluetooth를 활성화하는 것을 막을 수 없습니다.

WiPS

WiPS는 비승인 비인가 디바이스의 존재를 탐지하는 것보다 더 발전된 공격 벡터를 다룹니다. 이러한 공격 외에도, 포렌식 분석을 위해 이벤트의 PCAP를 제공하기도 합니다.

이 기능은 기업에 매우 유용한 보안 기능이지만, 공용 네트워크에서는 항상 다음과 같은 질문에 직면해야 합니다.

제어하지 않는 많은 클라이언트를 관리하기가 어렵기 때문에 경보를 두 가지 범주로 나눌 수 있습니다. Cisco Catalyst Center에서 다음과 같은 경보가 너무 많이 표시될 경우 무시하기로 결정할 수 있습니다.

- 10001: DoS: 인증 플러드 경보
- 10002: DoS: 연결 요청 경보
- 10003: DoS: 브로드캐스트 프로브 플러드 경보
- 10004: DoS: 연결 해제 플러드 경보
- 10005: DoS: 브로드캐스트 연결 해제 경보
- 10006: DoS: 인증 취소 플러드 경보
- 10007: DOS: 브로드캐스트 인증 취소 경보
- 10008: DOS: EAPOL-Logoff 공격 경보
- 10009: CTS 플러드 경보
- 10010: RTS 연결 요청 경보
- 10011: 쌍별 인증 해제 플러드
- 10021: Airdrop 세션(일반적으로 모든 네트워크에서 많이 발생하며 Apple 장치 간의 정기적인 피어 투 피어 활동을 간단하게 설명)
- 10022: 잘못된 형식의 연결 요청
- 10023: 서명에 의한 인증 실패 플러드
- 10024: 서명에 의한 잘못된 MAC OUI
- 10025: 형식이 잘못된 인증

이러한 경보는 클라이언트 오작동으로 인해 발생할 수 있습니다. 기본적으로 결함이 있는 클라이언트가 통화 중 상태로 유지되는 것을 방지할 수 없으므로 서비스 거부 공격을 자동으로 방지할 수 없습니다. 인프라에서 클라이언트를 무시하더라도 미디어와 통신 시간을 사용하여 전송할 수 있으므로 주변 클라이언트의 성능에 영향을 미칩니다.

다른 경보는 매우 구체적이어서 실제 악의적인 공격을 나타낼 가능성이 높으며 클라이언트 드라이

버가 잘못되어 거의 발생하지 않습니다. 다음 경보를 계속 모니터링하는 것이 좋습니다.

- 10012: Fuzzed 비컨
- 10013: Fuzzed 프로브 요청
- 10014: Fuzzed Probe 응답
- 10015: 서명에 의한 PS 폴링 플러드
- 10016: 서명에 의한 EAPOL 시작 V1 플러드
- 10017: 대상별 재연결 요청 플러드
- 10018: 시그니처별 비컨 플러드
- 10019: 대상별 프로브 응답 플러드
- 10020: 서명에 의한 Ack 플러드 차단
- 10026/10027: RTS 및 CTS Virtual Carrier Sense 공격

무선 인프라는 때때로 위반 디바이스를 나열하는 차단 조치와 같은 완화 조치를 취할 수 있지만, 그러한 공격을 제거하기 위한 유일한 실제 조치는 물리적으로 그 곳에 가서 위반 디바이스를 제거하는 것입니다.

잘못된 클라이언트와 상호 작용하여 낭비되는 통신 시간을 절약하려면 모든 형태의 클라이언트 제외를 활성화하는 것이 좋습니다.

클라이언트 액세스 제한

모든 WLAN에서 P2P(peer-to-peer) 차단을 활성화하는 것이 좋습니다(클라이언트-클라이언트 통신에 대한 까다로운 요구 사항이 있는 경우 제외). 그러나 이는 신중하게 고려해야 하며 제한될 수 있습니다. 이 기능은 동일한 WLAN의 클라이언트가 서로 연결하지 못하도록 합니다. 다른 WLAN에 있는 클라이언트는 여전히 서로 연락할 수 있고 모빌리티 그룹의 다른 WLC에 속하는 클라이언트도 이러한 제한을 우회할 수 있으므로 완벽한 솔루션은 아닙니다. 하지만 이는 보안과 최적화의 쉽고 효율적인 첫 번째 레이어로 작동합니다. P2P(peer-to-peer) 차단의 이 기능의 또 다른 이점은 애플리케이션이 로컬 네트워크에서 다른 디바이스를 검색하지 못하게 하는 클라이언트-클라이언트 ARP도 방지한다는 점입니다. P2P(peer-to-peer) 차단이 없으면 클라이언트에 간단한 애플리케이션을 설치하면 서브넷에 연결된 다른 모든 클라이언트가 해당 IP 주소 및 호스트 이름과 함께 표시될 수 있습니다.

또한 클라이언트 간 통신을 방지하기 위해 WLAN에 IPv4 및 IPv6(네트워크에서 IPv6를 사용하는 경우) ACL을 모두 적용하는 것이 좋습니다. WLAN 레벨에서 클라이언트 간 통신을 차단하는 ACL을 적용하면 클라이언트 SVI가 있는지 여부와 상관없이 작동합니다.

또 다른 필수 단계는 무선 클라이언트가 무선 컨트롤러의 모든 관리 형식에 액세스하지 못하도록 하는 것입니다.

예:

```
ip access-list extended ACL_DENY_CLIENT_VLANS

 10 deny ip any 10.131.0.0 0.0.255.255

 20 deny ip 10.131.0.0 0.0.255.255 any
```

```
 30 deny ip any 10.132.0.0 0.0.255.255
 40 deny ip 10.132.0.0 0.0.255.255 any
 50 deny ip any 10.133.0.0 0.0.255.255
 60 deny ip 10.133.0.0 0.0.255.255 any
 70 deny ip any 10.134.0.0 0.0.255.255
 80 deny ip 10.134.0.0 0.0.255.255 any
 90 deny ip any 10.135.0.0 0.0.255.255
 100 deny ip 10.135.0.0 0.0.255.255 any
 110 deny ip any 10.136.0.0 0.0.255.255
 120 deny ip 10.136.0.0 0.0.255.255 any
 130 deny ip any 10.137.0.0 0.0.255.255
 140 deny ip 10.137.0.0 0.0.255.255 any
 150 permit ip any any
```

이 ACL은 관리 인터페이스 SVI에 적용할 수 있습니다.

```
interface Vlan130
 ip access-group ACL_DENY_CLIENT_VLANS in
```

이는 클라이언트 VLAN 131~137이 레이어 2 VLAN 데이터베이스에 생성되었지만 해당 SVI가 없는 WLC에서 수행되며, WLC 관리 방식인 VLAN 130에 대해 SVI가 하나만 존재합니다. 이 ACL은 모든 무선 클라이언트가 WLC 관리 및 제어 플레인에 트래픽을 보낼 수 없게 합니다. 모든 AP에 대한 CAPWAP 연결도 허용해야 하므로 SSH 또는 웹 UI 관리만 허용해서는 안 됩니다. 이 ACL에 기본 허용이 있지만 허용되는 모든 AP 서브넷 범위 및 관리 범위를 지정하는 데 필요한 기본 거부 모든 작업에 의존하는 대신 무선 클라이언트 범위를 차단하는 이유가 여기에 있습니다.

마찬가지로, 가능한 모든 관리 서브넷을 지정하는 다른 ACL을 생성할 수 있습니다.

```
ip access-list standard ACL_MGMT
 10 permit 10.128.0.0 0.0.255.255
 20 permit 10.127.0.0 0.0.255.255
 30 permit 10.100.0.0 0.0.255.255
 40 permit 10.121.0.0 0.0.255.255
```

```
 50 permit 10.141.0.0 0.0.255.255
```

그런 다음 CLI 액세스에 이 ACL을 적용할 수 있습니다.

```
line vty 0 50
 access-class ACL_MGMT in
 exec-timeout 180 0
 ipv6 access-class ACL_IPV6_MGMT in
 logging synchronous
 length 0
 transport preferred none
 transport input ssh
 transport output ssh
```

동일한 ACL을 웹 관리자 액세스에도 적용할 수 있습니다.

교통 폭풍으로부터 보호

멀티캐스트 및 브로드캐스트는 다른 애플리케이션보다 일부 애플리케이션에서 더 많이 사용됩니다. 유선 전용 네트워크를 고려할 때, 브로드캐스트 스톰에 대한 보호가 유일한 예방 조치인 경우가 많습니다. 그러나 멀티캐스트는 방송을 통해 전송될 때 브로드캐스트만큼 고통스러우며 그 이유를 이해하는 것이 중요합니다. 먼저 모든 무선 클라이언트에 (브로드캐스트 또는 멀티캐스트를 통해) 전송된 패킷을 상상해 보십시오. 그러면 많은 대상이 빠르게 추가됩니다. 각 AP는 이 프레임을 가장 안정적인 방법으로 공중으로 전송해야 하며(신뢰성이 보장되지는 않지만) 필수 데이터 전송률(때로는 가장 낮지만 구성할 수 있는 경우도 있음)을 사용하여 이를 구현해야 합니다. Layman의 용어에서 이는 프레임이 OFDM(802.11a/g) 데이터 전송률을 사용하여 전송됨을 의미하며, 이는 분명 좋지 않습니다.

대규모 공용 네트워크에서는 멀티캐스트에 의존하여 통신 시간을 보존하는 것이 좋습니다. 그러나 대기업의 네트워크에서는 특정 애플리케이션에 대해 멀티캐스트를 활성화해야 하지만, 그 영향을 제한하려면 멀티캐스트를 최대한 제어해야 한다는 요구 사항이 있을 수 있습니다. 애플리케이션 세부사항, 멀티캐스트 IP를 문서화하고 다른 형태의 멀티캐스트를 차단하는 것이 좋습니다. 앞서 설명한 대로 Multicast 포워딩을 활성화하는 것은 IPv6를 활성화하는 데 필요하지 않습니다. 브로드캐스트 포워딩은 완전히 비활성화되는 것이 가장 좋습니다. 브로드캐스트는 애플리케이션에서 동일한 서브넷의 다른 디바이스를 검색하는 데 사용되기도 하는데, 이는 대규모 네트워크의 보안 문제임이 분명합니다.

전역 멀티캐스트 전달을 활성화하는 경우 멀티캐스트-멀티캐스트 AP CAPWAP 설정을 사용해야 합니다. 이 기능을 활성화하면 WLC가 유선 인프라에서 멀티캐스트 패킷을 수신하면 단일 멀티캐스

트 패킷으로 모든 관련 AP에 이를 전송하여 많은 패킷 중복을 줄입니다. 각 WLC에 대해 다른 CAPWAP 멀티캐스트 IP를 설정해야 합니다. 그렇지 않으면 AP가 원하지 않는 다른 WLC에서 멀티캐스트 트래픽을 수신합니다.

AP가 WLC의 무선 관리 인터페이스(대규모 네트워크일 수 있음)에서 다른 서브넷에 있는 경우 유선 인프라에서 멀티캐스트 라우팅을 활성화해야 합니다. 다음 명령을 사용하여 모든 AP가 멀티캐스트 트래픽을 올바르게 수신하는지 확인할 수 있습니다.

```
show ap multicast mom
```

멀티캐스트에 의존해야 하는 경우 IGMP(IPv4 멀티캐스트용) 및 MLD(IPv6) 멀티캐스트도 모든 경우에 활성화하는 것이 좋습니다. 이 스위치는 관련 무선 클라이언트(관련 클라이언트가 있는 AP만)만 멀티캐스트 트래픽을 수신하도록 허용합니다. WLC는 멀티캐스트 트래픽에 등록을 프록시하고 등록을 계속 유지함으로써 클라이언트를 오프로드합니다.

결론

대규모 공용 네트워크는 복잡하며 각각 특정 요구 사항 및 성과와 함께 고유합니다.

이 문서의 지침을 준수하는 것은 매우 중요한 출발점이며 가장 일반적인 문제를 피하면서 구축을 성공적으로 완료하는 데 도움이 됩니다. 다만 가이드라인은 가이드라인에 불과하여 특정 장소의 맥락 내에서 해석되거나 조정될 필요가 있다.

Cisco CX는 스포츠 이벤트, 컨퍼런스 등 다양한 대규모 이벤트 경험을 보유한 대규모 무선 구축을 전담하는 무선 전문가 팀을 보유하고 있습니다. 어카운트 팀에 문의하여 추가 지원을 받으십시오.

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.