Designleitfaden CX - Wireless für große öffentliche Netzwerke

Inhalt

Einleitung

Dieses Dokument beschreibt Design- und Konfigurationsrichtlinien für große öffentliche Wi-Fi-Netzwerke.

CX-Designleitfaden

Die CX-Designleitfäden wurden von Spezialisten des Cisco Technical Assistance Center (TAC) und des Cisco Professional Services (PS) verfasst und von Experten bei Cisco begutachtet. Sie basieren auf den bewährten Praktiken von Cisco sowie auf dem Wissen und der Erfahrung, die im Laufe vieler Jahre durch zahllose Kundenimplementierungen gewonnen wurden. Netzwerke, die entsprechend den Empfehlungen in diesem Dokument entwickelt und konfiguriert wurden, helfen dabei, gängige Probleme zu vermeiden und den Netzwerkbetrieb zu verbessern.

Geltungsbereich und Definitionen

Dieses Dokument enthält Design- und Konfigurationsrichtlinien für große öffentliche Wireless-Netzwerke.

Definition: Große öffentliche Netzwerke - häufig mit hoher Dichte ausgestattete Wireless-Bereitstellungen, die für Tausende von unbekannten und/oder nicht verwalteten Client-Geräten Netzwerkverbindungen bereitstellen.

In diesem Dokument wird häufig davon ausgegangen, dass das Zielnetzwerk Dienste für große und/oder temporäre Ereignisse bereitstellt. Es eignet sich auch für statische permanente Netzwerke für Sportstätten, die viele Gäste empfangen. Ein Einkaufszentrum oder ein Flughafen haben zum Beispiel Ähnlichkeiten mit dem Wi-Fi-Netzwerk eines Stadions oder Konzerthauses - in dem Sinne, dass es keine Kontrolle über die Endbenutzer gibt und diese im Netzwerk in der Regel nur für ein paar Stunden oder höchstens für einen Tag existieren.

Die Wireless-Abdeckung für große Veranstaltungen oder Sportstätten hat eigene Anforderungen, die sich in der Regel von den Anforderungen des Unternehmens, der Fertigung oder selbst von großen Bildungsnetzwerken unterscheiden. Große öffentliche Netzwerke können Tausende von Menschen haben, die sich in nur einem oder wenigen Gebäuden konzentrieren. Sie können über sehr häufiges Client-Roaming verfügen, ständig oder in Spitzenzeiten, und das Netzwerk muss hinsichtlich drahtloser Client-Geräte mit allem kompatibel sein, ohne Kontrolle über die Konfiguration oder Sicherheit der Client-Geräte.

Dieser Leitfaden stellt allgemeine RF-Konzepte für High-Density- sowie Implementierungsdetails vor. Viele der Funkkonzepte in diesem Leitfaden gelten für alle Netzwerke mit hoher Dichte, einschließlich Cisco Meraki. Die Implementierungsdetails und Konfigurationen konzentrieren sich jedoch auf Catalyst Wireless mit dem Catalyst 9800 Wireless Controller, da dies die häufigste Lösung ist, die heutzutage für große öffentliche Netzwerke bereitgestellt wird.

In diesem Dokument werden die Begriffe Wireless Controller und Wireless LAN Controller (WLC) synonym verwendet.

Große öffentliche Netzwerke

Große Netzwerke für die Öffentlichkeit und Veranstaltungen sind in vielerlei Hinsicht einzigartig. In diesem Dokument werden diese Schlüsselbereiche untersucht und erläutert.

- Große öffentliche Netzwerke sind sehr intensiv. Es gibt Tausende von Geräten in einem reduzierten Funkfrequenzbereich und es kann zu bestimmten Zeiten zu Spitzenzeiten der Bandbreite kommen, wenn die Menschen herumlaufen. Manche Veranstaltungen und Veranstaltungsorte sind statischer. Die Infrastruktur muss alle diese Statusänderungen für Clients, die in das Gebiet eintreten und sich dort bewegen, so problemlos wie möglich handhaben können.
- Die wichtigste Priorität ist die einfache Integration. Ein verbundener Kunde ist ein zufriedener Kunde. Das bedeutet, dass Sie die Client-Verknüpfung mit dem Netzwerk so schnell wie möglich herstellen möchten. Ein Client, der nicht mit dem Wi-Fi-Netzwerk verbunden ist, sucht nach verfügbaren Access Points, die unerwünschte HF-Energie erzeugen, was zu zusätzlichen Überlastungen und Kapazitätsverlusten auf dem Funkweg führt.
- Die Bereitstellung der Funkumgebung muss so sorgfältig wie möglich erfolgen. Wenn eine sehr hohe Dichte erforderlich ist oder der Veranstaltungsort über große Freiflächen und/oder hohe Decken verfügt, ist ein geeignetes Design für die Funkumgebung mit Richtantennen unerlässlich.
- Ein weiterer wichtiger Aspekt ist die Kompatibilität. Einige Funktionen sind Standard in der 802.11-Spezifikation, während andere Funktionen proprietär sind, stellen keine Probleme für Clients dar. Die Realität sieht jedoch anders aus, und es gibt viele schlecht programmierte

Client-Treiber, die sich falsch verhalten, wenn sie komplizierte Beacons oder Funktionen/Einstellungen sehen, die sie nicht verstehen.
- Die Fehlerbehebung gestaltet sich aufgrund von Skalierungs- und Zeitbeschränkungen schwierig. Wenn etwas nicht mit einem bestimmten Client funktioniert, können Sie das Problem nicht mit diesem Endbenutzer verstehen. Benutzer können schwierig zu finden sein, können aber auch nicht kooperativ sein, da ihr Besuch am Veranstaltungsort nur vorübergehend ist.
- Sicherheit ist ein wichtiger Faktor. Weniger Kontrolle durch die große Anzahl an Besuchern und eine viel größere Angriffsfläche.

Externe Referenzen

Dokumentname	Quelle	Location (Standort)
Cisco Catalyst Serie 9800 - Best Practices für die Konfiguration	Cisco	Link
Fehlerbehebung bei der Wireless LAN Controller-CPU	Cisco	Link
Validierung des Wi-Fi-Durchsatzes: Leitfaden für Tests und Überwachung	Cisco	Link
Bereitstellungsleitfaden für Cisco Catalyst Access Points der Serie CW9166D1	Cisco	Link
Catalyst 9104 Stadium Antenna (C-ANT9104) - Bereitstellungsleitfaden	Cisco	Link
Catalyst 9800-Leistungskennzahlen überwachen (wichtige Leistungsindikatoren)	Cisco	Link
Fehlerbehebung: Catalyst 9800 Client-Konnektivitätsprobleme	Cisco	Link
Software-Konfigurationsleitfaden für Cisco Catalyst Wireless Controller der Serie 9800 (17.12)	Cisco	Link
Wi-Fi 6E: Das nächste große Kapitel im Wi-Fi-Whitepaper	Cisco	Link

Haftungsausschluss

Dieses Dokument enthält Empfehlungen, die auf bestimmten Szenarien, Annahmen und Kenntnissen basieren, die im Rahmen zahlreicher Bereitstellungen gewonnen wurden. Sie als Leser sind jedoch dafür verantwortlich, das Netzwerkdesign, den Geschäftsbetrieb, die Einhaltung gesetzlicher Vorschriften, die Sicherheit, den Datenschutz und andere Anforderungen zu bestimmen, einschließlich der Frage, ob Sie die in diesem Leitfaden bereitgestellten Anleitungen oder Empfehlungen befolgen sollten.

Design des Netzwerks

RF-Überlegungen

Veranstaltungstypen

Der Schwerpunkt dieses Leitfadens liegt auf großen Gastnetzwerken, die in der Regel für die Öffentlichkeit zugänglich sind und nur eine begrenzte Kontrolle über Endbenutzer und Client-Gerätetypen haben. Diese Netzwerktypen können an verschiedenen Standorten bereitgestellt werden und temporär oder permanent sein. Der Hauptnutzungsfall ist in der Regel die Bereitstellung des Internetzugangs für Besucher, obwohl dies selten der einzige Anwendungsfall ist.

Typische Standorte:

- Stadien und Stadien
- Veranstaltungsorte
- Große Hörsäle

Jede dieser Standortarten hat aus RF-Sicht ihre eigenen Nuancen. Bei den meisten dieser Beispiele handelt es sich um permanente Installationen, mit Ausnahme von Konferenzräumen, da diese permanent sein oder vorübergehend für eine bestimmte Messe eingerichtet werden können.

Weitere Standorte:

- Kreuzfahrtschiff
- Flughafen
- Einkaufszentrum/Einkaufszentrum

Flughäfen und Kreuzfahrtschiffe sind auch Beispiele für Bereitstellungen, die in die Kategorie der großen öffentlichen Netze passen; diese haben jedoch jeweils spezifische zusätzliche Überlegungen und nutzen häufig interne omnidirektionale APs.

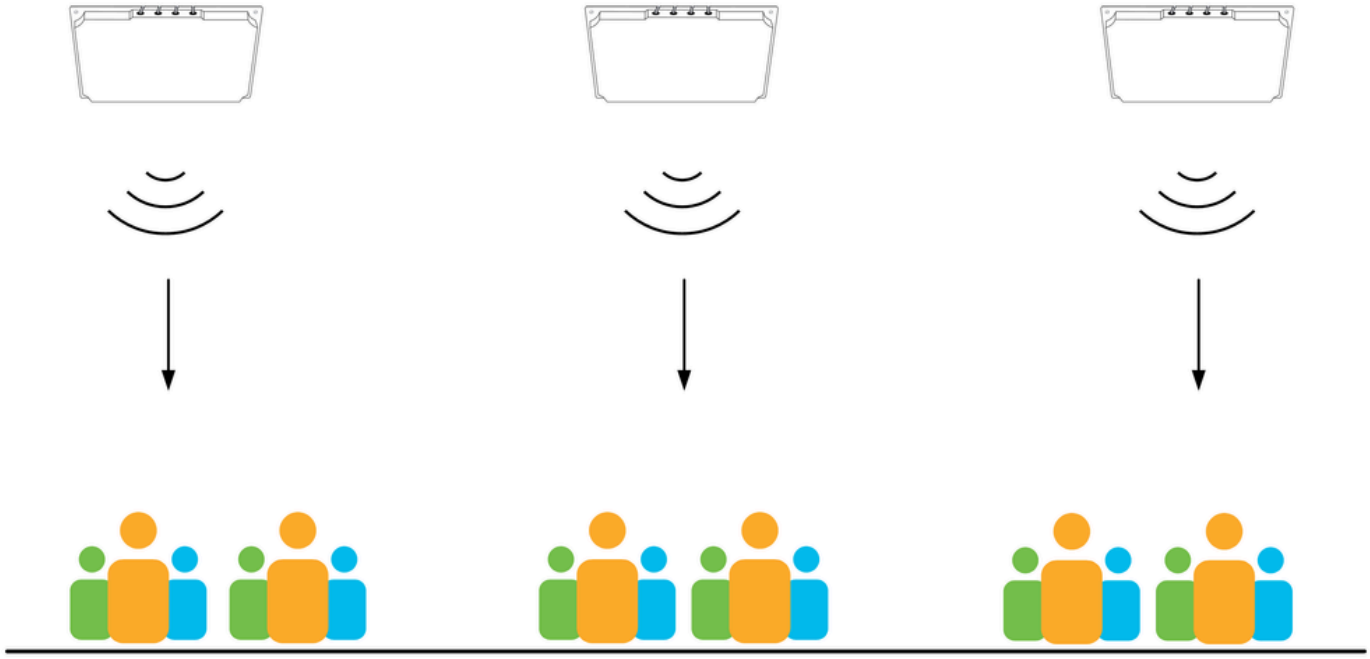
Abdeckungsstrategien

Die Abdeckungsstrategien hängen weitgehend vom Veranstaltungsort, den verwendeten Antennen und den verfügbaren Antennenmontageorten ab.

Gemeinkosten

Eine Overhead-Abdeckung ist immer dann vorzuziehen, wenn dies möglich ist.

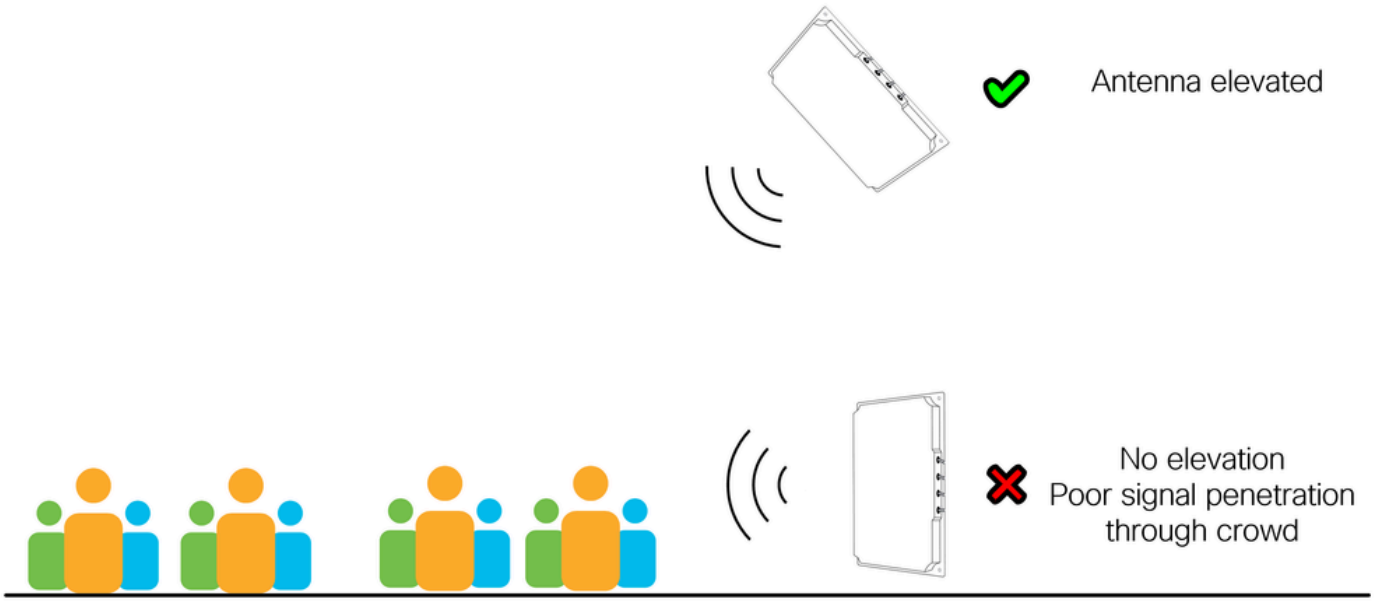
Overhead-Lösungen haben den entscheidenden Vorteil, dass alle Client-Geräte in der Regel über eine direkte Sichtverbindung zum Antennenoverhead verfügen, selbst bei stark ausgelasteten Szenarien. Overhead-Lösungen, die Richtantennen verwenden, bieten einen kontrollierteren und klar definierten Abdeckungsbereich, der sie hinsichtlich der Funkabstimmung weniger kompliziert macht, während sie gleichzeitig einen besseren Lastenausgleich und bessere Client-Roaming-Eigenschaften bieten. Weitere Informationen finden Sie im Abschnitt Leistungsbilanz.



APs über den Clients

Seite

Seitlich angebrachte Richtantennen sind eine beliebte Wahl und funktionieren in einer Vielzahl von Szenarien gut, insbesondere wenn eine Overhead-Montage aufgrund von Höhenbeschränkungen oder Montageeinschränkungen nicht möglich ist. Bei der seitlichen Montage ist es wichtig zu verstehen, welche Art von Bereich von der Antenne abgedeckt wird, z. B. ist es ein offener Außenbereich oder ein dichter Innenbereich? Wenn der Abdeckungsbereich ein Bereich mit hoher Personendichte ist, muss die Antenne so weit wie möglich erhöht werden, da die Signalausbreitung durch eine Menschenmenge immer schlecht ist. Denken Sie daran, dass die meisten Mobilgeräte in einer tieferen Taille und nicht über dem Kopf des Benutzers verwendet werden! Die Höhe der Antenne ist weniger wichtig, wenn der Abdeckungsbereich ein Bereich mit geringerer Dichte ist.



Antennenhöhe ist immer besser

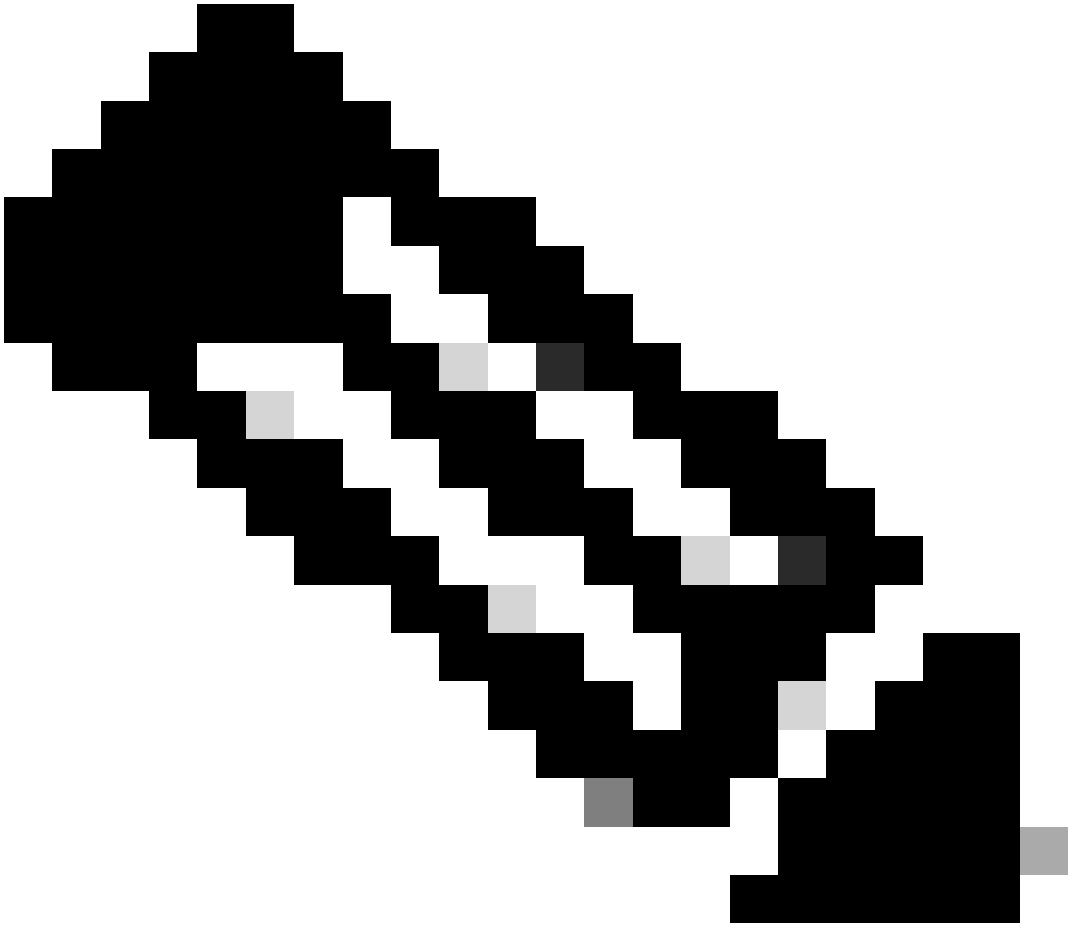
Omnidirektional

Die Verwendung von Rundstrahlantennen (intern oder extern) ist in der Regel bei sehr hochdichten Szenarien zu vermeiden, da bei Co-Channel-Interferenzen potenziell ein hoher Aufprallbereich vorliegt. Rundstrahlantennen dürfen nicht in einer Höhe über 6 m verwendet werden (gilt nicht für Außeneinheiten mit hoher Verstärkung).

Untersitz

In einigen Stadien oder Arenen kann es Situationen geben, in denen es keine geeigneten Antennenmontageplätze gibt. Die letzte verbleibende Alternative besteht darin, die Abdeckung von unten bereitzustellen, indem APs unter den Sitzen positioniert werden, an denen die Benutzer sitzen. Eine solche Lösung ist schwieriger richtig bereitzustellen und erfordert in der Regel wesentlich mehr Access Points und spezifische Installationsverfahren.

Die größte Herausforderung bei der Bereitstellung von weniger genutzten Sitzplätzen ist der große Abdeckungsunterschied zwischen einem vollen und einem leeren Veranstaltungsort. Ein menschlicher Körper ist sehr effizient bei der Dämpfung von Funksignalen, was bedeutet, dass, wenn es eine Menschenmenge um den AP ist die Abdeckung ist deutlich kleiner als wenn diese Menschen nicht da sind. Durch diesen Faktor der menschlichen Massen-Dämpfung können mehr APs bereitgestellt werden, was die Gesamtkapazität erhöhen kann. Wenn der Veranstaltungsort jedoch leer ist, gibt es keine Abschwächung durch den menschlichen Körper und keine nennenswerten Störungen, was zu Komplikationen führt, wenn der Veranstaltungsort teilweise voll ist.



Hinweis: Die Bereitstellung unter einem Arbeitsplatz ist eine gültige, aber ungewöhnliche Lösung. Sie muss von Fall zu Fall evaluiert werden. Die Bereitstellung unter einem Arbeitsplatz wird in diesem Dokument nicht weiter behandelt.

Ästhetik

Bei einigen Bereitstellungen kommt die Frage der Ästhetik ins Spiel. Hierbei kann es sich um Bereiche mit spezifischen Architekturdesigns, historischem Wert oder um Bereiche handeln, in denen Werbung und/oder Branding vorgeben, wo die Geräte angebracht werden können (oder nicht). Um Platzierungseinschränkungen zu umgehen, können spezielle Lösungen erforderlich sein. Zu diesen Problemumgehungen gehören das Verbergen des Access Points/der Antenne, das Anstreichen des Access Points/der Antenne, die Montage des Geräts in einem Gehäuse oder die Verwendung eines anderen Standorts. Die Antennenlackierung erlischt die Garantie, wenn Sie die Antenne lackieren möchten, verwenden Sie immer eine nichtmetallische Lackierung. Cisco verkauft in der Regel keine Antennengehäuse, aber viele sind über verschiedene Anbieter leicht erhältlich.

All diese Problemumgehungen wirken sich auf die Leistung des Netzwerks aus. Drahtlose Architekten schlagen zu Beginn immer optimale Montagepositionen für eine optimale Funkabdeckung vor. Diese Ausgangspositionen bieten in der Regel die beste Leistung. Alle Änderungen an diesen Positionen führen häufig dazu, dass Antennen von ihrem optimalen Standort entfernt werden.

An Standorten, an denen Antennen angebracht sind, sind häufig erhöhte Werte zu erkennen. Dies können Decken, Laufstege, Dachstrukturen, Balken, Gehwege und alle Standorte sein, die eine gewisse Höhe über dem vorgesehenen Abdeckungsbereich bieten. Diese Standorte werden in der Regel gemeinsam mit anderen Installationen genutzt, z. B. Audiogeräte, Klimaanlagen, Beleuchtung und verschiedenen Detektoren/Sensoren. Zum Beispiel müssen Audio- und Beleuchtungsgeräte an ganz bestimmten Orten montiert werden - aber warum ist das so? Es liegt einfach daran, dass Audio- und Beleuchtungsgeräte nicht richtig funktionieren, wenn sie in einer Kiste oder hinter einer Wand versteckt sind, und jeder erkennt dies.

Dasselbe gilt für Wireless-Antennen. Sie funktionieren am besten, wenn eine Sichtlinie zum Wireless-Client-Gerät besteht. Eine priorisierte Ästhetik kann sich (und wird es sehr oft) negativ auf die Wireless-Leistung auswirken und den Wert der Infrastrukturinvestitionen schmälern.

Nicht autorisierte Netzwerke

Nicht autorisierte Wi-Fi-Netzwerke sind Wireless-Netzwerke, die einen gemeinsamen Funkraum nutzen, aber nicht vom selben Betreiber verwaltet werden. Diese können temporär oder permanent sein und umfassen Infrastrukturgeräte (APs) und private Geräte (wie Mobiltelefone, die einen Wi-Fi-Hotspot gemeinsam nutzen). Nicht autorisierte Wi-Fi-Netzwerke stellen eine Störungsquelle und in einigen Fällen auch ein Sicherheitsrisiko dar. Die Auswirkungen unberechtigter Programme auf die Wireless-Leistung dürfen nicht unterschätzt werden. Wi-Fi-Übertragungen sind auf einen relativ kleinen Bereich von Funkfrequenzen beschränkt, die von allen Wi-Fi-Geräten genutzt werden. Fehlerhafte Geräte in der Nähe können die Netzwerkleistung für viele Benutzer beeinträchtigen.

Im Rahmen großer öffentlicher Netze werden diese üblicherweise mit speziellen Antennen sorgfältig konzipiert und abgestimmt. Eine gute Funkumgebung deckt nur die erforderlichen Bereiche ab und nutzt häufig Richtantennen. Durch Abstimmung der Sende- und Empfangscharakteristik wird eine maximale Effizienz erreicht.

Am anderen Ende des Spektrums befinden sich Geräte der Verbraucherklasse oder Geräte, die von Internetdienstanbietern bereitgestellt werden. Diese verfügen entweder über eingeschränkte Optionen zur Feineinstellung der Funkfrequenz oder sind für maximale Reichweite und wahrgenommene Leistung konfiguriert, häufig mit hoher Leistung, niedrigen Datenraten und breiten Kanälen. Die Einführung solcher Geräte in ein großes Veranstaltungsnetzwerk hat das Potenzial, Chaos zu verursachen.

Was kann getan werden?

Im Falle persönlicher Hotspots kann nur sehr wenig getan werden, da es fast unmöglich wäre, Zehntausende von Menschen zu überwachen, die einen Veranstaltungsort betreten. Bei

Infrastrukturen oder semi-permanenten Geräten gibt es einige Optionen. Mögliche Abhilfemaßnahmen beginnen mit einfacher Aufklärung, einschließlich einfacher Beschilderung zur Sensibilisierung, bis hin zu unterzeichneten Dokumenten zur Funkpolitik, die mit aktiver Durchsetzung und Spektrumanalyse enden. In allen Fällen muss eine geschäftliche Entscheidung über den Schutz des Funkfrequenzspektrums am jeweiligen Veranstaltungsort getroffen werden, zusammen mit konkreten Schritten, um diese Geschäftsentscheidung durchzusetzen.

Der Sicherheitsaspekt von nicht autorisierten Netzwerken kommt ins Spiel, wenn von einem Drittanbieter gesteuerte Geräte dieselbe SSID wie das verwaltete Netzwerk ankündigen. Dies entspricht einem Honeypot-Angriff und kann als Methode zum Diebstahl von Benutzerdaten verwendet werden. Es wird immer empfohlen, eine nicht autorisierte Regel zu erstellen, um vor der Erkennung von Infrastruktur-SSIDs zu warnen, die von nicht verwalteten Geräten gemeldet werden. Im Abschnitt "Sicherheit" werden unberechtigte Personen ausführlicher behandelt.

Single, 5 GHz oder Dual, 5 GHz

Dual 5 GHz bezieht sich auf die Verwendung beider 5 GHz-Funkmodule auf unterstützten APs. Es besteht ein wesentlicher Unterschied zwischen zwei 5-GHz-Netzwerken mit externen Antennen und zwei 5-GHz-Netzwerken mit internen Antennen (Mikro-/Makrozellen auf omnidirektionalen APs). Bei externen Antennen ist Dual 5 GHz häufig ein nützlicher Mechanismus, der für zusätzliche Abdeckung und Kapazität sorgt und gleichzeitig die Gesamtzahl der Access Points verringert.

Mikro/Makro/Meso

Interne APs haben beide Antennen in der Nähe (innerhalb des AP), und bei Verwendung von Dual-5-GHz-Verbindungen gibt es Einschränkungen hinsichtlich der maximalen Tx-Leistung. Das zweite Funkmodul ist auf eine niedrige Tx-Leistung beschränkt (wird vom Wireless Controller durchgesetzt), was zu einem großen Ungleichgewicht der Tx-Leistung zwischen den Funkmodulen führt. Dies kann dazu führen, dass das primäre Funkmodul (mit höherer Leistung) viele Clients anzieht, während das sekundäre Funkmodul (mit niedrigerer Leistung) nicht ausgelastet ist. In diesem Fall versorgt das zweite Funkmodul die Umwelt mit Energie, ohne dass die Kunden davon profitieren. Wenn dieses Szenario eintritt, kann es sinnvoller sein, die zweite Funkverbindung zu deaktivieren und einen weiteren AP (einzelner 5-GHz-Access Point) hinzuzufügen, wenn zusätzliche Kapazität erforderlich ist.

Verschiedene AP-Modelle haben verschiedene Konfigurationsoptionen, das zweite 5-GHz-Funkmodul kann mit höheren Leistungsniveaus in neueren Makro/Meso-APs wie dem 9130 und 9136 betrieben werden, und einige interne Wi-Fi 6E-APs wie die 9160-Serie können sogar in Makro/Makro in einigen Fällen betrieben werden. Überprüfen Sie stets die Funktion Ihres AP-Modells. Der zweite 5-GHz-Steckplatz ist auch in seiner Kanalnutzung eingeschränkt, wenn ein Steckplatz in einem UNII-Band betrieben wird, ist der andere Steckplatz auf ein anderes UNII-Band beschränkt, was sich auf die Kanalplanung und anschließend auch auf die verfügbare Sendeleistung auswirkt. Berücksichtigen Sie stets die Differenz zwischen der Übertragungsleistung von zwei 5-GHz-Funkmodulen. Dies gilt in allen Fällen, einschließlich der internen APs.

FRA

Flexible Radio Assignment (FRA) wurde als Technologie zur Verbesserung der 5-GHz-Abdeckung eingeführt, indem zusätzliche 2,4-GHz-Funkmodule in den 5-GHz-Modus oder potenziell nicht verwendete 5-GHz-Funkmodule in den Überwachungsmodus (für APs, die dies unterstützten) geschaltet wurden. Da dieses Dokument große öffentliche Netzwerke abdeckt, wird davon ausgegangen, dass die Abdeckungsbereiche sowie das Funkdesign mit Richtantennen gut definiert sind, weshalb eine deterministische Konfiguration gegenüber einer dynamischen bevorzugt wird. Die Verwendung von FRA wird für große öffentliche Netzwerke nicht empfohlen.

Optional kann FRA verwendet werden, wenn das Netzwerk eingerichtet ist, um zu bestimmen, welche Funkmodule in 5 GHz umgewandelt werden sollen. Wenn Sie mit dem Ergebnis zufrieden sind, wird empfohlen, FRA einzufrieren.

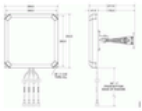
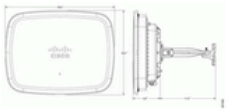
Gesetzliche

Jeder Zulassungsbereich legt fest, welche Kanäle für die Nutzung zur Verfügung stehen und wie hoch die maximale Leistung ist. Darüber hinaus gibt es Beschränkungen, welche Kanäle sowohl in Innenräumen als auch im Freien genutzt werden können. Je nach Zulassung ist es manchmal nicht möglich, eine duale 5-GHz-Lösung effektiv einzusetzen. Ein Beispiel hierfür ist die ETSI-Domäne, in der 30 dBm auf UNII-2e-Kanälen zulässig sind, jedoch nur 23 dBm auf UNII1/2. Wenn für dieses Beispiel 30 dBm erforderlich sind (normalerweise aufgrund der größeren Entfernung zur Antenne), kann die Verwendung eines einzelnen 5-GHz-Funkmoduls die einzig mögliche Lösung sein.

Antennen

Große öffentliche Netzwerke können jede Art von Antenne verwenden und wählen in der Regel die für diesen Auftrag am besten geeignete Antenne aus. Das Mischen von Antennen im gleichen Abdeckungsbereich erschwert das Funkdesign und muss nach Möglichkeit vermieden werden. Große öffentliche Netzwerke verfügen jedoch häufig über große Abdeckungsbereiche mit unterschiedlichen Montageoptionen, selbst innerhalb desselben Bereichs, sodass in einigen Fällen Antennen gemischt werden müssen. Rundstrahlantennen sind allgemein bekannt und funktionieren wie alle anderen Antennen. In diesem Leitfaden werden externe Rundstrahlantennen erläutert.

In dieser Tabelle sind die am häufigsten verwendeten externen Antennen aufgeführt.

	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°

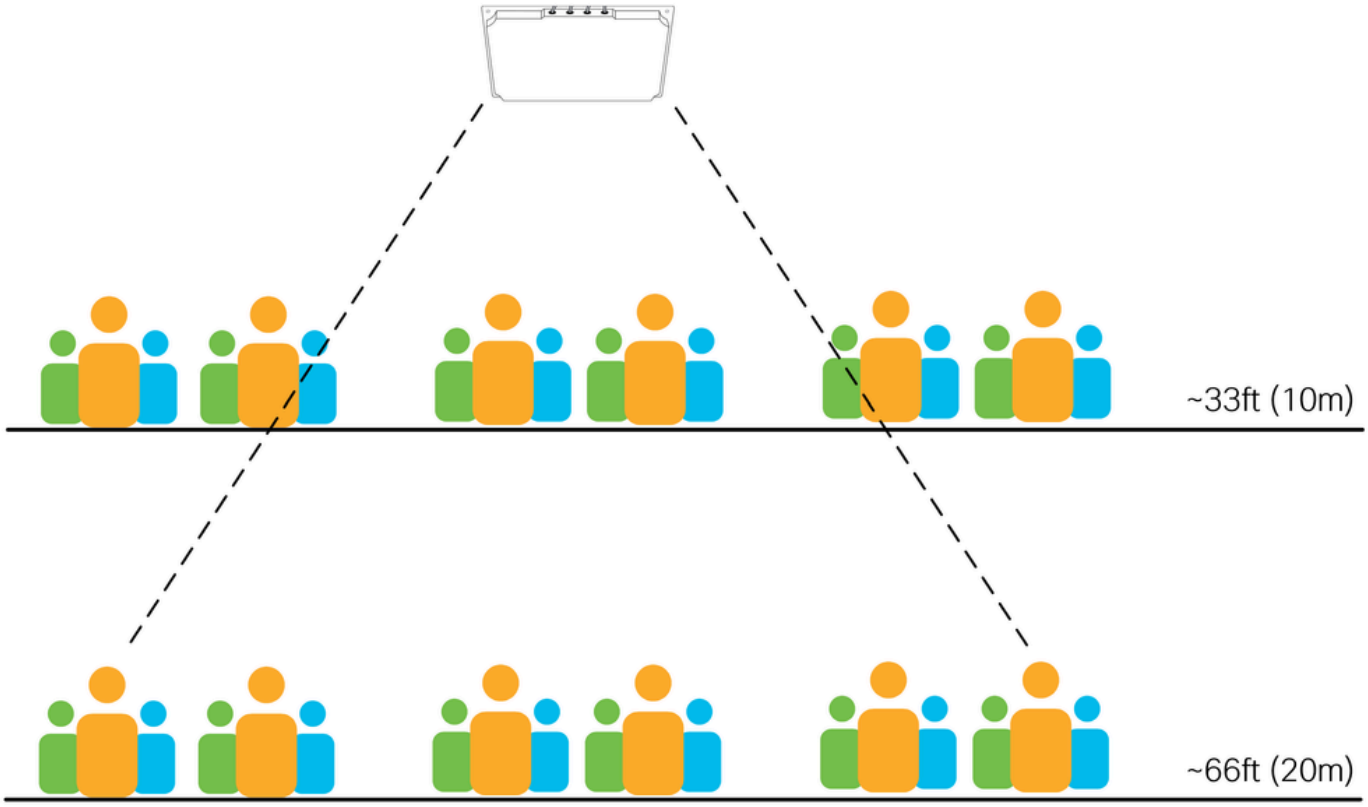
Antennenliste

Die wichtigsten Faktoren bei der Auswahl einer Antenne sind die Strahlbreite und der Abstand bzw. die Höhe der Antenne. Die Tabelle zeigt eine Strahlbreite von 5 GHz für jede der Antennen. Die Zahlen in Klammern sind gerundet (und lassen sich besser merken).

Die vorgeschlagenen Entfernungen in der Tabelle sind keine harten Regeln, sondern nur Richtlinien, die auf Erfahrungen basieren. Radiowellen wandern mit Lichtgeschwindigkeit und stoppen nicht einfach nach Erreichen einer beliebigen Entfernung. Die Antennen arbeiten alle über die empfohlene Entfernung, die Leistung sinkt jedoch mit zunehmender Entfernung. Die Installationshöhe ist ein Schlüsselfaktor bei der Planung.

Das folgende Diagramm zeigt zwei mögliche Montagehöhen für dieselbe Antenne bei ~10 m und ~20 m in einem Bereich mit hoher Dichte. Beachten Sie, dass die Anzahl der Clients, von denen die Antenne sehen kann (und von denen Verbindungen akzeptiert werden), mit der Entfernung zunimmt. Mit größeren Entfernungen wird es schwieriger, kleinere Zellgrößen zu erhalten.

Die allgemeine Regel ist, je höher die Benutzerdichte ist, desto wichtiger ist es, die richtige Antenne für die gegebene Entfernung zu verwenden.



Eine Stadionantenne

Die Stadionantenne C9104 eignet sich für die Abdeckung von Bereichen mit hoher Personendichte über große Entfernungen. Weitere Informationen finden Sie im Bereitstellungsleitfaden für die Catalyst Stadium Antenna 9104 (C-ANT9104).

Änderungen im Laufe der Zeit

Veränderungen an der physischen Umgebung sind in fast allen drahtlosen Installationen (z. B. Bewegung von Innenwänden) üblich. Regelmäßige Ortsbesichtigungen und visuelle Inspektionen sind seit jeher eine empfohlene Praxis. Bei Event-Netzwerken ist der Umgang mit Audio- und Beleuchtungssystemen und in vielen Fällen auch mit anderen Kommunikationssystemen (z.B. 5G) noch komplexer. All diese Systeme werden oft an erhöhten Stellen über den Benutzern installiert, was manchmal zu Konflikten um den gleichen Platz führt. Ein guter Standort für eine drahtlose Stadionantenne ist oft auch ein guter Standort für eine 5G-Antenne! Wenn diese Systeme im Laufe der Zeit aktualisiert werden, können sie an Orte verlagert werden, an denen sie Ihr Wireless-System behindern und/oder aktiv stören. Es ist wichtig, die anderen Installationen zu verfolgen und mit den Teams zu kommunizieren, die sie installieren, um sicherzustellen, dass alle Systeme an geeigneten Orten installiert werden, ohne sich gegenseitig zu stören (physisch oder elektromagnetisch).

Hohe Dichte und 6 GHz

Zum Zeitpunkt der Erstellung dieses Dokuments gibt es eine begrenzte Auswahl an externen 6-GHz-fähigen Antennen. Nur der integrierte Zugangspunkt/die integrierte Antenne CW9166D1 arbeitet mit 6 GHz. Detaillierte Informationen zu den Antennenspezifikationen finden Sie im Cisco Catalyst CW9166D1 Access Point Deployment Guide. Der CW9166D1 bietet eine Abdeckung von

6 GHz mit einer Strahlbreite von 60° x 60° und kann effektiv für jede Bereitstellung verwendet werden, die die Bedingungen für diesen Antennentyp erfüllt. Zuschauerräume und Lagerhäuser sind beispielsweise gute Kandidaten für den Einsatz des CW9166D1, da das integrierte Gerät Richtantennenfunktionen für den Innenbereich bietet.

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

9166D1

Im Zusammenhang mit großen öffentlichen Netzen haben diese oft verschiedene große Flächen und erfordern den Einsatz einer Kombination von Antennen in verschiedenen Höhen. Die End-to-End-Bereitstellung eines großen öffentlichen Netzwerks mit nur einer 60°x60°-Antenne kann aufgrund von Entfernungsmitteilungen eine Herausforderung darstellen. Daher kann es auch eine Herausforderung sein, eine End-to-End-Abdeckung bei 6 GHz bereitzustellen, indem nur der CW9166D1 für ein großes öffentliches Netzwerk verwendet wird.

Ein möglicher Ansatz besteht darin, 5 GHz als primäres Abdeckungsband zu verwenden, während 6 GHz nur in bestimmten Bereichen verwendet wird, um fähige Client-Geräte auf das sauberere 6 GHz-Band auszulagern. Bei diesem Ansatz werden in größeren Bereichen nur 5-GHz-Antennen verwendet. Die 6-GHz-Antennen werden nach Möglichkeit verwendet, wenn zusätzliche Kapazität erforderlich ist.

Nehmen wir als Beispiel einen großen Veranstaltungssaal bei einer Fachkonferenz. Der Hauptraum nutzt Stadionantennen, um eine Primärabdeckung bei 5 GHz bereitzustellen. Die Höhe der Installation erfordert die Verwendung von Stadionantennen. Der CW9166D1 kann in diesem Beispiel aufgrund von Entfernungsbeschränkungen nicht in der Haupthalle eingesetzt werden, sondern kann effektiv in einem angrenzenden VIP-Saal oder Pressenbereich eingesetzt werden, in dem eine höhere Dichte erforderlich ist. Client-Roaming zwischen dem 5-GHz- und dem 6-GHz-Band wird später in diesem Dokument behandelt.

Gesetzliche

Wie bei 5 GHz unterscheiden sich die verfügbare Leistung und die Kanäle für 6 GHz erheblich zwischen den Zulassungsbereichen. Bemerkenswert ist, dass zwischen den FCC- und ETSI-Domänen ein großer Unterschied besteht. Außerdem gelten strenge Richtlinien bezüglich der verfügbaren Tx-Leistung für den Innen- und Außenbereich sowie für Low Power Indoor (LPI) und

Standard Power (SP). Mit 6 GHz umfassen zusätzliche Einschränkungen die Leistungsgrenzen für Clients, die Verwendung externer Antennen und die Neigung nach unten und (derzeit nur in den USA) die Anforderung nach Automated Frequency Coordination (AFC) für SP-Bereitstellungen.

Weitere Informationen zu Wi-Fi 6E finden Sie im Whitepaper Wi-Fi 6E: Das nächste große Kapitel.

Verwaltung von Funkressourcen

Radio Resource Management (RRM) ist eine Gruppe von Algorithmen, die für die Steuerung des Funkbetriebs verantwortlich sind. Dieses Handbuch bezieht sich auf zwei wichtige RRM-Algorithmen, nämlich Dynamic Channel Assignment (DCA) und Transmit Power Control (TPC). RRM ist eine Alternative zur statischen Kanal- und Stromversorgungskonfiguration.

- DCA wird nach einem konfigurierbaren Zeitplan ausgeführt (standardmäßig 10 Minuten).
- TPC wird nach einem automatischen Zeitplan ausgeführt (standardmäßig 10 Minuten).

Cisco Event Driven RRM (ED-RRM) ist eine DCA-Option, die es ermöglicht, eine Kanaländerungsentscheidung außerhalb des DCA-Standardplans zu treffen, in der Regel als Reaktion auf schwerwiegende HF-Bedingungen. ED-RRM kann einen Kanal sofort wechseln, wenn übermäßige Interferenzen erkannt werden. In lauten und/oder instabilen Umgebungen birgt die Aktivierung von ED-RRM das Risiko übermäßiger Kanaländerungen, was sich negativ auf die Client-Geräte auswirken kann.

Die Verwendung von RRM wird empfohlen und im Allgemeinen gegenüber statischen Konfigurationen bevorzugt - allerdings mit gewissen Einschränkungen und Ausnahmen.

- TPC muss je nach Bedarf auf einen engen Wertebereich unter Verwendung der TPC-Min./Max.-Einstellung beschränkt und stets auf das HF-Design ausgerichtet sein.
    - Aktivieren Sie TPC Channel Aware in Umgebungen mit hoher Dichte.

- Der DCA-Zyklus muss in der Standardeinstellung von 10 Minuten geändert werden.
    - Verwenden Sie ED-RRM nicht in HD-Umgebungen.
    - Deaktivieren Sie die Option zum Vermeiden der Auslastung des Cisco Access Points.
    - Optionen zur Vermeidung nicht autorisierter APs wie die Vermeidung von Fremdzugangsstörungen können zu einer instabilen Umgebung führen, wenn viele unberechtigte APs vorhanden sind. Es ist immer besser, die Schurken zu entfernen, als zu versuchen, darauf zu reagieren.
- RRM-Entscheidungen können durch APs/Antennen beeinflusst werden, die sich nicht richtig hören, wie z. B. bei Richtantennen, die voneinander weg zeigen.
- Einige Antennen (z. B. C9104) unterstützen kein RRM und erfordern immer eine statische Konfiguration.
- RRM behebt kein schlechtes RF-Design.

In allen Fällen muss das RRM unter Berücksichtigung der erwarteten Ergebnisse implementiert und so eingestellt werden, dass es innerhalb der für die jeweilige Funkumgebung geeigneten Grenzen funktioniert. In den folgenden Abschnitten dieses Dokuments werden diese Punkte ausführlicher behandelt.

RF-Konfiguration

Kanäle

Im Allgemeinen gilt: Je mehr Kanäle, desto besser. Bei Bereitstellungen mit hoher Dichte können um ein Vielfaches mehr APs und Funkmodule bereitgestellt werden als verfügbare Kanäle. Dies bedeutet eine hohe Wiederverwendungsrate der Kanäle und in Kombination damit eine stärkere Interferenz zwischen den Kanälen. Es müssen alle verfügbaren Kanäle verwendet werden. Eine Einschränkung der Liste der verfügbaren Kanäle wird generell abgeraten.

Es kann Fälle geben, in denen ein bestimmtes (und separates) Wireless-System im gleichen physischen Raum nebeneinander bestehen muss und dedizierte Kanäle zugewiesen werden müssen, während die zugewiesenen Kanäle aus der DCA-Liste des primären Systems entfernt werden. Solche Kanalausschlüsse müssen sehr sorgfältig geprüft und nur bei Bedarf verwendet werden. Ein Beispiel hierfür kann eine Point-to-Point-Verbindung sein, die in einem offenen Bereich neben dem Primärnetz arbeitet, oder ein Pressebereich innerhalb eines Stadions. Wenn mehr als ein oder zwei Kanäle von der DCA-Liste ausgeschlossen werden, ist dies ein Grund für eine Neubewertung der vorgeschlagenen Lösung. In manchen Fällen, z. B. in Stadien mit sehr hoher Dichte, ist auch ein einzelner Kanal nicht immer möglich.

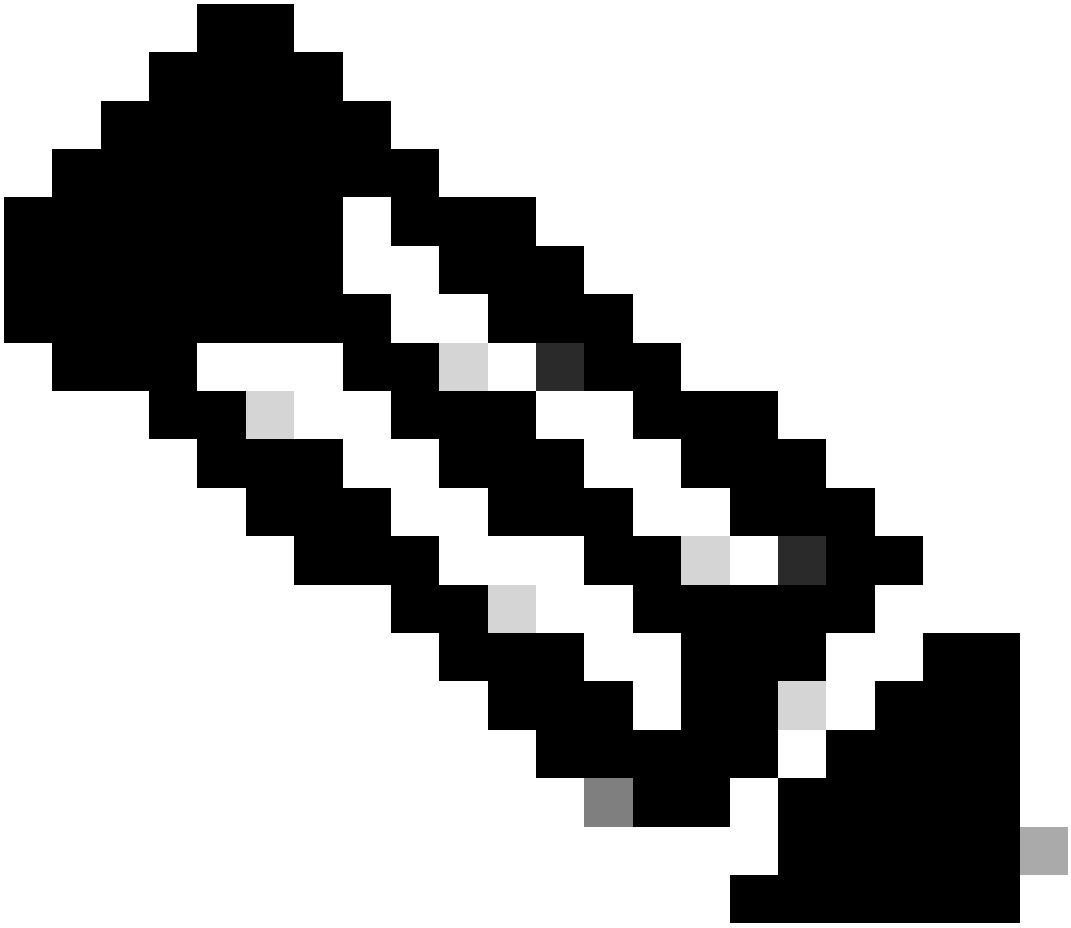
Dynamic Channel Assignment (DCA) kann mit WLC-basiertem RRM oder mit KI-optimiertem RRM verwendet werden.

Das Standard-DCA-Intervall beträgt 10 Minuten, was in instabilen Funkumgebungen zu häufigen Kanalwechseln führen kann. Der standardmäßige DCA-Timer muss in allen Fällen von den standardmäßigen 10 Minuten auf 10 Minuten erhöht und das spezifische DCA-Intervall an die Betriebsanforderungen des jeweiligen Netzwerks angepasst werden. Eine Beispielkonfiguration kann sein: DCA-Intervall 4 Stunden, Ankerzeit 8. Dadurch werden Kanaländerungen auf einmal alle 4 Stunden, beginnend um 8 Uhr, begrenzt.

Da Störungen unweigerlich auftreten können, bringt die Anpassung an jeden DCA-Zyklus nicht unbedingt einen Mehrwert, da viele dieser Störungen nur vorübergehend auftreten. Eine gute Technik ist es, automatische DCA für die ersten paar Stunden zu verwenden und den Algorithmus und den Channel-Plan einzufrieren, wenn Sie etwas Stabiles haben, mit dem Sie zufrieden sind.

Nach dem Neustart des WLC wird der DCA 100 Minuten lang im aggressiven Modus ausgeführt, um einen geeigneten Kanalplan zu finden. Es empfiehlt sich, den Prozess manuell neu zu starten, wenn wesentliche Änderungen am HF-Design vorgenommen werden (z. B. Hinzufügen oder Entfernen zahlreicher APs oder Ändern der Kanalbreite). Verwenden Sie diesen Befehl, um diesen Vorgang manuell zu starten.

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



Hinweis: Kanaländerungen können zu Unterbrechungen für Client-Geräte führen.

2.4 GHz)

Das 2,4-GHz-Band wurde oft kritisiert. Es verfügt nur über drei überlappungsfreie Kanäle, die von vielen anderen Technologien als Wi-Fi genutzt werden. Dies kann zu unerwünschten Interferenzen führen. Einige Organisationen bestehen darauf, einen Service zu bieten. Was ist also eine vernünftige Schlussfolgerung? Tatsache ist, dass das 2,4-GHz-Band keine zufriedenstellende Erfahrung für Endbenutzer bietet. Schlimmer noch: Wenn Sie versuchen, einen 2,4-GHz-Dienst bereitzustellen, wirkt sich dies auf andere 2,4-GHz-Technologien wie Bluetooth aus. In großen Veranstaltungsorten erwarten viele Menschen noch immer, dass ihr Wireless-Headset funktioniert, wenn sie einen Anruf tätigen oder ihre Smart Wearables nutzen, um den gewohnten Betrieb aufrechtzuerhalten. Wenn Ihr dichtes Wi-Fi mit 2,4 GHz betrieben wird, wirkt sich dies auf die Geräte aus, die Ihr 2,4 GHz-Wi-Fi nicht einmal verwenden.

Eines ist sicher: Wenn Sie wirklich einen 2,4-GHz-Wi-Fi-Service bereitstellen müssen, ist es am besten, dies auf einer separaten SSID zu tun (diese dedizieren Sie für IoT-Geräte oder nennen

Sie sie "Legacy"). Das bedeutet, dass Dual-Band-Geräte nicht unfreiwillig mit 2,4 GHz verbunden werden und nur Single-Band-Geräte mit 2,4 GHz verbunden werden.

Cisco empfiehlt und unterstützt die Verwendung von 40-MHz-Kanälen im 2,4-GHz-Band nicht.

5 GHz)

Typische Bereitstellung für Wireless-Netzwerke mit hoher Dichte Verwenden Sie nach Möglichkeit alle verfügbaren Kanäle.

Die Anzahl der Kanäle variiert je nach Zulassung. Berücksichtigen Sie die Auswirkungen von Radar an einem bestimmten Standort, und verwenden Sie DFS-Kanäle (einschließlich TDWR-Kanäle), wo dies möglich ist.

Die Kanalbreite von 20 MHz wird dringend für alle Bereitstellungen mit hoher Dichte empfohlen.

40 MHz können auf der gleichen Basis wie 2,4 GHz verwendet werden, das ist nur, wenn (und wo) absolut erforderlich.

Ermitteln Sie den tatsächlichen Bedarf und Nutzen von 40-MHz-Kanälen in der jeweiligen Umgebung. 40-MHz-Kanäle erfordern ein höheres Signal-Rausch-Verhältnis (Signal-to-Noise Ratio, SNR), um eine mögliche Verbesserung des Durchsatzes zu realisieren. Wenn eine höhere SNR-Rate nicht möglich ist, erfüllen 40-MHz-Kanäle keinen sinnvollen Zweck. Netzwerke mit hoher Dichte priorisieren den Durchschnitt für alle Benutzer gegenüber einem potenziell höheren Durchsatz für einzelne Benutzer. Es ist besser, mehr APs auf 20-MHz-Kanälen zu platzieren, als APs mit 40 MHz als sekundärem Kanal nur für Datenframes zu verwenden und daher viel weniger effizient zu nutzen, als mit zwei verschiedenen Funkzellen, die jeweils mit 20 MHz betrieben werden (hinsichtlich der Gesamtkapazität, nicht hinsichtlich des Durchsatzes eines einzelnen Clients).

6 GHz

Das 6GHz-Band ist noch nicht in allen Ländern verfügbar. Darüber hinaus verfügen einige Geräte über einen 6-GHz-fähigen Wi-Fi-Adapter, der jedoch ein BIOS-Update erfordert, damit er für das Land aktiviert wird, in dem das Gerät betrieben wird. Die beliebteste Art und Weise, wie Clients 6GHz-Funkmodule entdecken, ist über RNR-Werbung auf dem 5GHz-Funkmodul. Das bedeutet, dass 6 GHz nicht allein ohne ein 5 GHz-Funkmodul auf demselben AP betrieben werden darf. 6 GHz dient dazu, Clients und Datenverkehr vom 5 GHz-Funkmodul auszulagern und den fähigen Clients typischerweise ein besseres Erlebnis zu bieten. 6-GHz-Kanäle ermöglichen die Verwendung größerer Kanalbandbreiten, dies hängt jedoch stark von der Anzahl der Kanäle ab, die im Zulassungsbereich verfügbar sind. Bei 24 6-GHz-Kanälen in Europa ist es nicht unvernünftig, für 40-MHz-Kanäle einen besseren maximalen Durchsatz im Vergleich zu den 20 MHz bereitzustellen, die Sie wahrscheinlich in 5 GHz verwenden. In den USA, wo fast doppelt so viele Kanäle zur Verfügung stehen, ist die Nutzung von 40 MHz ein Selbstgänger, und selbst 80 MHz sind für ein Ereignis mit hoher Dichte nicht unangemessen. Größere Bandbreiten dürfen nicht bei Veranstaltungen mit hoher Personendichte oder an Veranstaltungsorten verwendet werden.

Datenraten

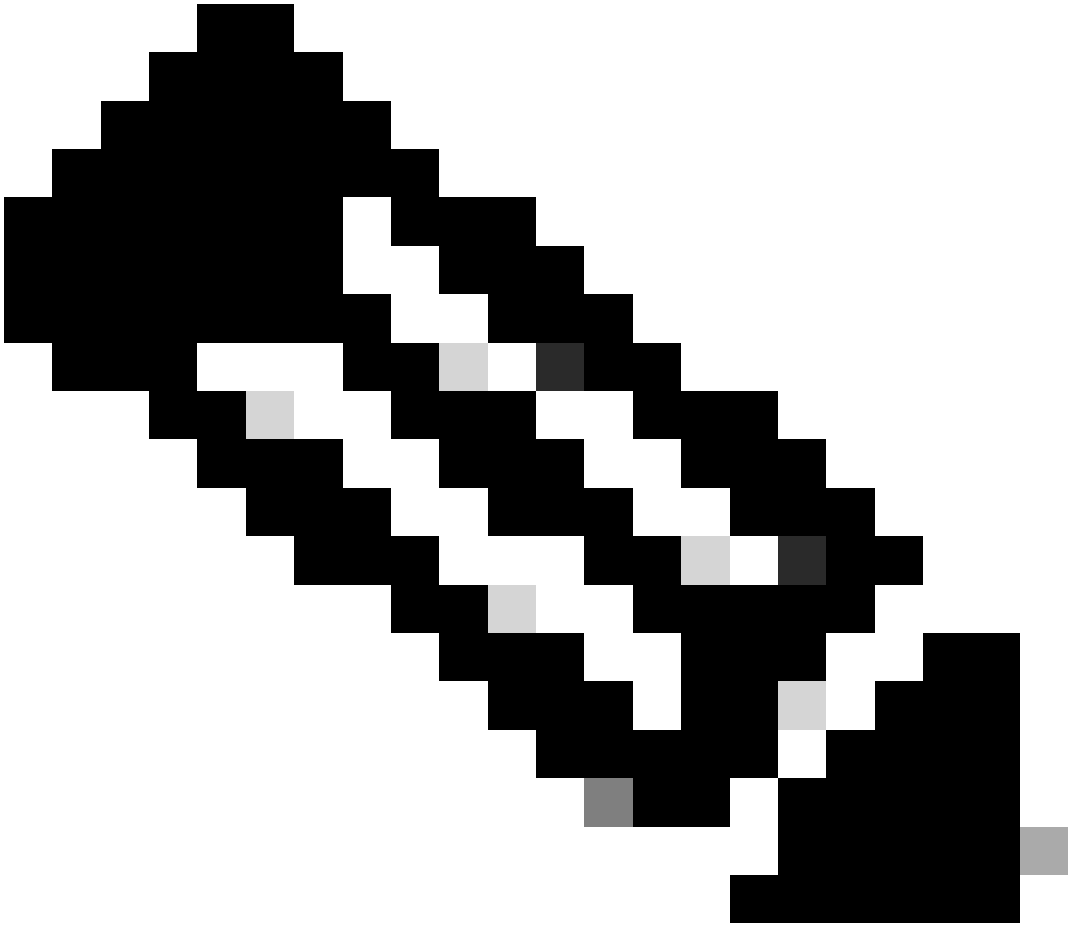
Die Datenrate, die ein Client mit einem Access Point aushandelt, ist weitgehend eine Funktion des Signal-Rausch-Verhältnisses (Signal-to-Noise Ratio, SNR) dieser Verbindung, und das Gegenteil ist auch wahr, d.h. höhere Datenraten erfordern eine höhere SNR. Tatsächlich bestimmt vor allem die SNR-Funktion die maximal mögliche Verbindungsgeschwindigkeit. Warum ist dies jedoch bei der Konfiguration von Datenraten wichtig? Der Grund dafür ist, dass einige Datenraten eine besondere Bedeutung haben.

Klassische OFDM-Datenraten (802.11a) können in einer von drei Einstellungen konfiguriert werden: "Disabled" (Deaktiviert), "Supported" (Unterstützt) oder "Obligatorisch". Die OFDM-Raten sind (in Mbit/s): 6, 9, 12, 18, 24, 36, 48, 54. Der Client und der Access Point müssen beide eine Rate unterstützen, bevor sie verwendet werden können.

Unterstützt - der Access Point verwendet die Rate

Obligatorisch: Der WAP verwendet diese Rate und sendet Verwaltungsdatenverkehr mit dieser Rate.

Disabled (Deaktiviert): Der Access Point verwendet die Übertragungsrate nicht und zwingt den Client, eine andere Übertragungsrate zu verwenden.



Anmerkung: Obligatorische Sätze werden auch als Basissätze bezeichnet

Die obligatorische Übertragungsrate hat die Bedeutung, dass alle Management-Frames mit dieser Übertragungsrate gesendet werden sowie Broadcast- und Multicast-Frames. Wenn mehrere erforderliche Raten konfiguriert sind, verwenden Management-Frames die niedrigste konfigurierte erforderliche Rate, und Broadcast- und Multicast-Broadcast verwenden die höchste konfigurierte erforderliche Rate.

Management-Frames enthalten Beacons, die der Client hören muss, um sie dem Access Point zuordnen zu können. Durch die Erhöhung der obligatorischen Rate wird auch die SNR-Anforderung für diese Übertragung erhöht. Denken Sie daran, dass höhere Datenraten eine höhere SNR-Rate erfordern. Dies bedeutet in der Regel, dass der Client näher am AP sein muss, um das Beacon decodieren und verbinden zu können. Durch die Manipulation der obligatorischen Datenrate manipulieren wir daher auch den effektiven Zuordnungsbereich des WAP, wodurch Clients näher an den WAP gezwungen werden, oder hin zu einer potenziellen Roaming-Entscheidung. Clients in der Nähe des Access Points benötigen höhere Datenraten, und höhere Datenraten benötigen weniger Funkzeit - der beabsichtigte Effekt ist eine effizientere Zelle. Dabei

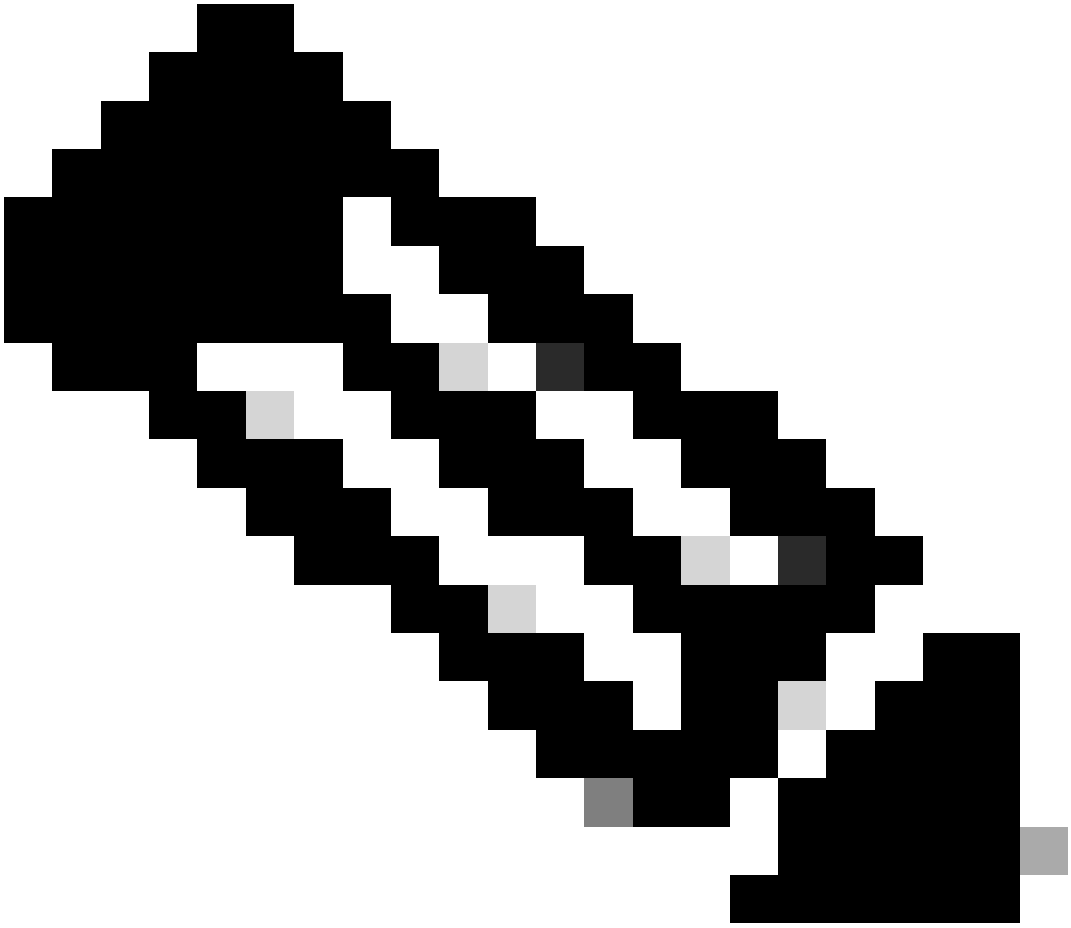
ist zu beachten, dass eine Erhöhung der Datenrate nur die Übertragungsrate bestimmter Frames beeinflusst, nicht aber die HF-Ausbreitung der Antenne oder den Interferenzbereich. Gute HF-Designverfahren sind weiterhin erforderlich, um Co-Channel-Interferenzen und Störungen zu minimieren.

Andererseits bedeutet das Belassen niedrigerer Raten als obligatorisch, dass Kunden in der Regel aus einer viel größeren Entfernung eine Verbindung herstellen können. Dies ist in Szenarien mit niedrigerer AP-Dichte nützlich, kann jedoch in Szenarien mit höherer Dichte zu Chaos beim Roaming führen. Jeder, der versucht hat, einen nicht autorisierten AP zu finden, der eine 6 Mbit/s sendet, weiß, dass Sie den AP sehr weit von seinem physischen Standort entfernt erkennen können!

Beim Thema Broadcast und Multicast wird in einigen Fällen eine zweite (höhere) obligatorische Rate konfiguriert, um die Übertragungsrate für Multicast-Datenverkehr zu erhöhen. Dies ist nur selten erfolgreich, da Multicast nie bestätigt und nie erneut übertragen wird, wenn Frames verloren gehen. Da in allen Wireless-Systemen Verluste auftreten, ist es unumgänglich, dass einige Multicast-Frames verloren gehen, unabhängig von der konfigurierten Rate. Ein besserer Ansatz für eine zuverlässige Multicast-Bereitstellung sind Multicast-zu-Unicast-Umwandlungstechniken, die Multicast als Unicast-Stream übertragen. Dies hat den Vorteil höherer Datenraten und einer zuverlässigen (bestätigten) Bereitstellung.

Verwenden Sie nur einen einzigen obligatorischen Tarif, deaktivieren Sie alle Tarife unterhalb des obligatorischen Tarifs, und belassen Sie alle Tarife oberhalb des obligatorischen Tarifs wie unterstützt. Die genaue Verwendungsrate hängt vom jeweiligen Anwendungsfall ab, da niedrigere Raten in Szenarien mit geringerer Dichte und in Szenarien mit größeren Abständen zwischen den APs im Außenbereich nützlich sind. Für Netzwerke mit hoher Dichte und für Veranstaltungen müssen niedrige Raten deaktiviert werden.

Wenn Sie sich nicht sicher sind, wo Sie anfangen sollen, legen Sie eine obligatorische Rate von 12 Mbit/s für Bereitstellungen mit geringer Dichte und von 24 Mbit/s für Bereitstellungen mit hoher Dichte fest. Viele Großveranstaltungen, Stadien und sogar Bereitstellungen in hochdichten Büros haben sich als zuverlässig erwiesen, wenn die erforderliche Übertragungsrate von 24 Mbit/s festgelegt wird. Für bestimmte Anwendungsfälle, bei denen Übertragungsraten von unter 12 Mbit/s oder über 24 Mbit/s erforderlich sind, werden geeignete Tests empfohlen.

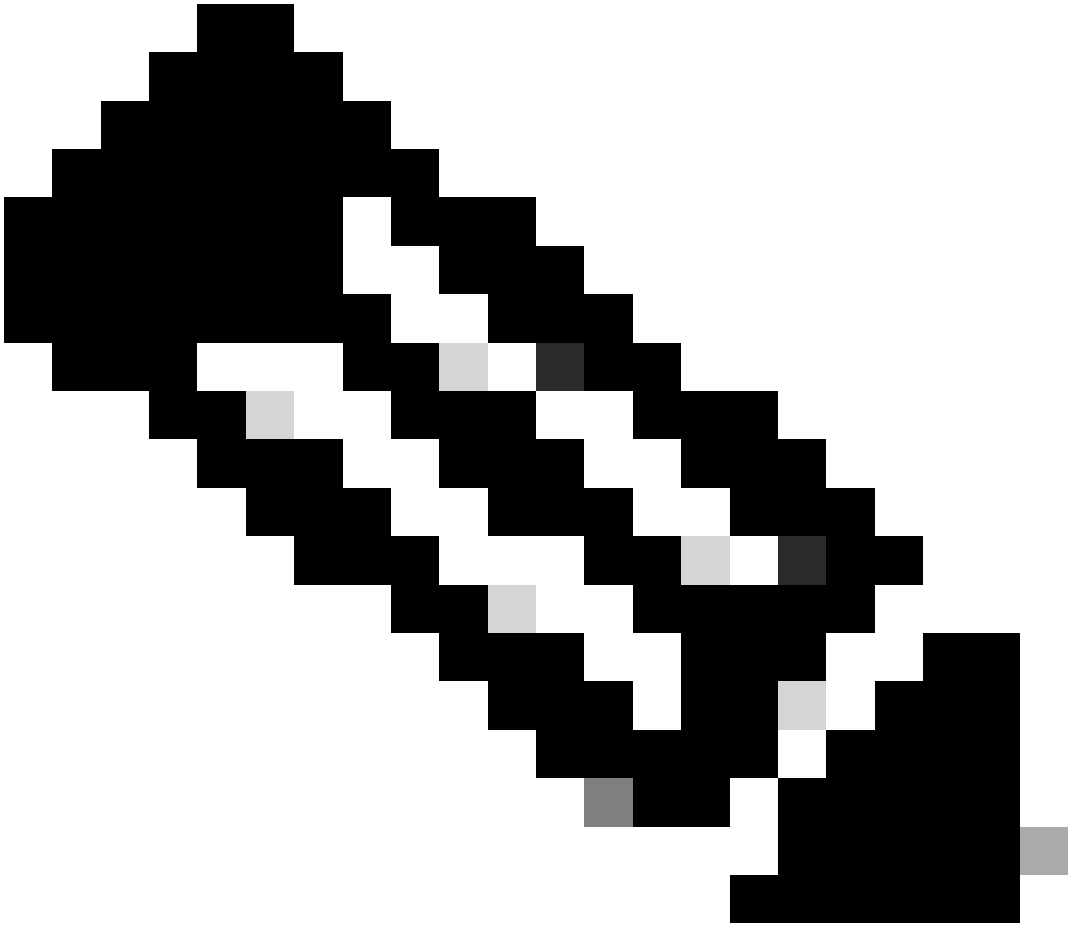


Hinweis: Es ist am besten, alle 802.11n/ac/ax-Raten aktiviert zu lassen (alle Raten im Abschnitt "Hoher Durchsatz" der WLC-GUI). Diese müssen nur selten deaktiviert werden.

Übertragungsleistung

Die Empfehlungen zur Sendeleistung unterscheiden sich je nach Bereitstellungstyp. Hierbei unterscheiden wir die Bereitstellung in Innenräumen mithilfe von Rundstrahlantennen von denen mit Rundstrahlantennen. Beide Antennentypen können in einem großen öffentlichen Netzwerk vorhanden sein, obwohl diese in der Regel verschiedene Arten von Bereichen abdecken.

Für omnidirektionale Bereitstellungen wird in der Regel die automatische Sendeleistungssteuerung (TPC) mit einem statisch konfigurierten Mindestschwellenwert und in bestimmten Fällen auch mit einem statisch konfigurierten Höchstschwellenwert verwendet.



Hinweis: TPC-Schwellenwerte beziehen sich auf die Funkübertragungsleistung und schließen die Antennengewinne aus. Achten Sie immer darauf, dass die Antennenverstärkung für das verwendete Antennenmodell richtig konfiguriert ist. Dies erfolgt bei internen Antennen und selbsterkennenden Antennen automatisch.

Beispiel 1

TPC Min.: 5 dBm, TPC Max.: Maximum (30 dBm)

Dies würde dazu führen, dass der TPC-Algorithmus die Übertragungsleistung automatisch bestimmt, jedoch niemals unter den konfigurierten Mindestschwellenwert von 5 dBm fällt.

Beispiel 2

TPC Min.: 2dBm, TPC Max.: 11 dBm

Dies würde dazu führen, dass der TPC-Algorithmus die Übertragungsleistung automatisch bestimmt, jedoch immer zwischen 2 dBm und 11 dBm bleibt.

Ein guter Ansatz besteht darin, mehrere Funkprofile mit unterschiedlichen Schwellenwerten zu erstellen, z. B. niedrige Leistung (2-5 dBm), mittlere Leistung (5-11 dBm) und hohe Leistung (11-17 dBM), und dann jedem Funkprofil nach Bedarf omnidirektionale APs zuzuweisen. Die Werte der RF-Profile können an den jeweiligen Anwendungsfall und die Abdeckungsfläche angepasst werden. So können die RRM-Algorithmen dynamisch arbeiten und gleichzeitig innerhalb vordefinierter Grenzen bleiben.

Der Ansatz für Richtantennen ist sehr ähnlich, der einzige Unterschied ist die erforderliche Genauigkeit. Die Platzierung der Richtantenne muss während einer RF-Überprüfung vor der Bereitstellung konzipiert und verifiziert werden. Die spezifischen Funkkonfigurationswerte sind in der Regel ein Ergebnis dieses Prozesses.

Wenn z. B. eine deckenmontierte Patch-Antenne erforderlich ist, um einen bestimmten Bereich ab einer Höhe von ~26 ft (8 m) abzudecken, muss die RF-Überwachung die erforderliche MindestSendeleistung bestimmen, um diese beabsichtigte Abdeckung zu erreichen (dies bestimmt den TPC-Mindestwert für das RF-Profil). Ebenso würden wir aus derselben RF-Untersuchung die mögliche Überlappung verstehen, die zwischen dieser und der nächsten Antenne erforderlich ist, oder sogar den Punkt, an dem die Abdeckung enden soll. Dies würde den maximalen TPC-Wert für das RF-Profil bereitstellen.

RF-Profile für Richtantennen werden in der Regel entweder mit den gleichen TPC-Mindest- und -Höchstwerten oder mit einem engen Bereich möglicher Werte (in der Regel <= 3 dBm) konfiguriert.

Zur Gewährleistung der Konfigurationskonsistenz werden RF-Profile bevorzugt. Eine statische Konfiguration einzelner APs wird nicht empfohlen. Es empfiehlt sich, Funkprofile nach Abdeckungsbereich, Antennentyp und Anwendungsfall zu benennen, z. B. RF-Auditorium-Patch-Decke.

Die korrekte Tx-Leistung liegt vor, wenn der erforderliche SNR-Wert vom schwächsten Client im vorgesehenen Abdeckungsbereich erreicht wird. Maximal ist dies der Fall. 30 dBm sind ein hervorragender SNR-Zielwert für Kunden unter realistischen Bedingungen (d. h. bei einem Veranstaltungsort mit zahlreichen Teilnehmern).

KHK

Coverage Hole Detection (CHD) ist ein separater Algorithmus zur Identifizierung und Behebung von Abdeckungslücken. CHD wird global und per WLAN konfiguriert. Ein möglicher Effekt von CHD ist die Erhöhung der Tx-Leistung, um Abdeckungslücken zu kompensieren (Bereiche mit Clients, die durchweg mit schlechtem Signal erkannt werden). Dieser Effekt ist auf Funkebene und betrifft alle WLANs, auch wenn er durch ein einzelnes WLAN ausgelöst wird, das für CHD konfiguriert ist.

Große öffentliche Netzwerke werden in der Regel mithilfe von RF-Profilen auf bestimmte Leistungspegel konfiguriert, einige können sich in offenen Bereichen befinden, in denen Clients in die und aus den Bereichen wechseln. Es ist kein Algorithmus erforderlich, um die AP-Tx-Leistung als Reaktion auf diese Client-Ereignisse dynamisch anzupassen.

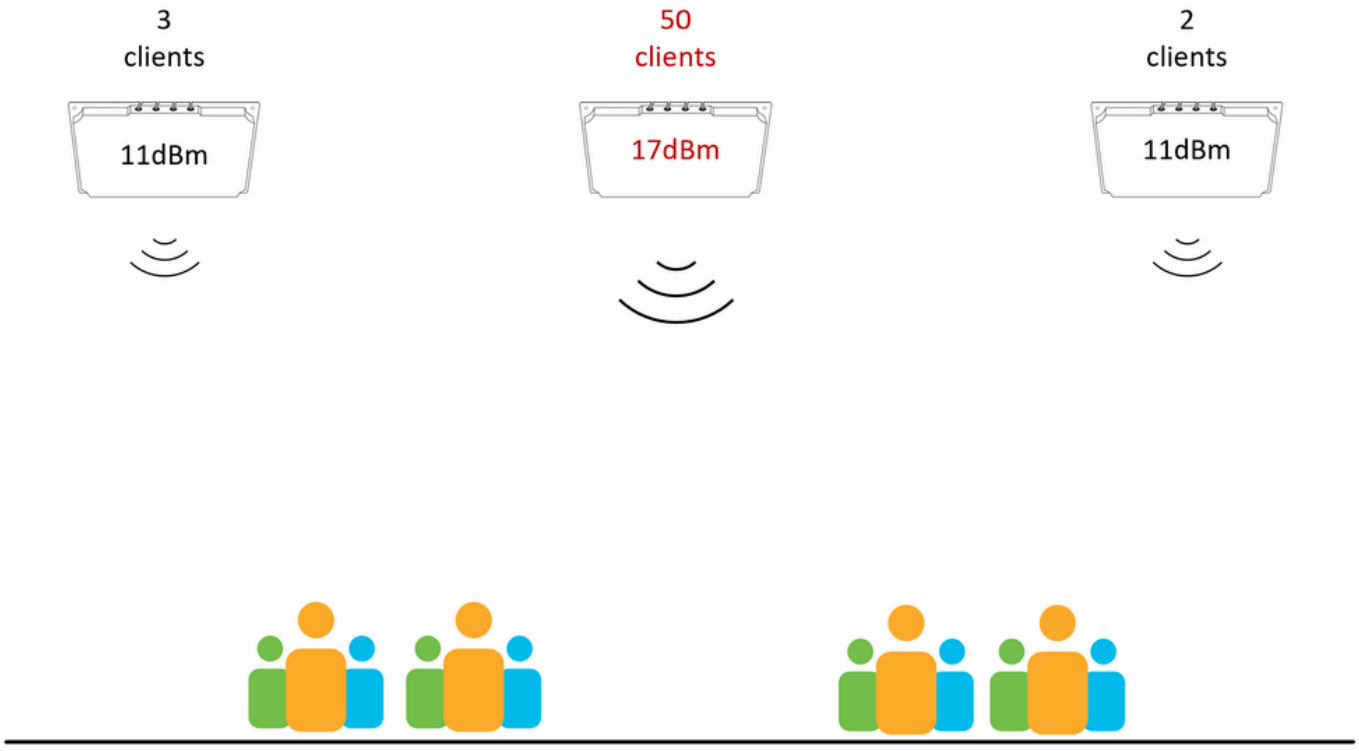
CHD muss für große öffentliche Netzwerke global deaktiviert werden.

Leistungsbilanz

Die meisten Client-Geräte bevorzugen ein höheres Empfangssignal, wenn sie sich für den AP entscheiden, dem sie zugeordnet werden möchten. Situationen, in denen ein Access Point im Vergleich zu anderen umgebenden Access Points mit einer wesentlich höheren Tx-Leistung konfiguriert ist, müssen vermieden werden. APs mit höherer Sendeleistung ziehen mehr Clients an, was zu einer ungleichmäßigen Client-Verteilung zwischen den APs führt (beispielsweise wird ein einzelner AP/ein Funkmodul mit Clients überlastet, während umgebende APs nicht ausgelastet sind). Diese Situation tritt häufig bei Bereitstellungen auf, bei denen sich die Abdeckung durch mehrere Antennen überschneidet, und in Fällen, bei denen ein Access Point über mehrere Antennen verfügt.

Stadionantennen wie der C9104 erfordern besondere Sorgfalt bei der Auswahl der Sendeleistung, da sich die Antennenstrahlen planmäßig überschneiden. Weitere Informationen hierzu finden Sie im Bereitstellungsleitfaden für Catalyst 9104 Stadium Antenna (C-ANT9104).

Im folgenden Diagramm ist die mittlere Antenne mit einer höheren Tx-Leistung konfiguriert als die umgebenden Antennen. Diese Konfiguration führt wahrscheinlich dazu, dass die Clients an der mittleren Antenne feststecken.

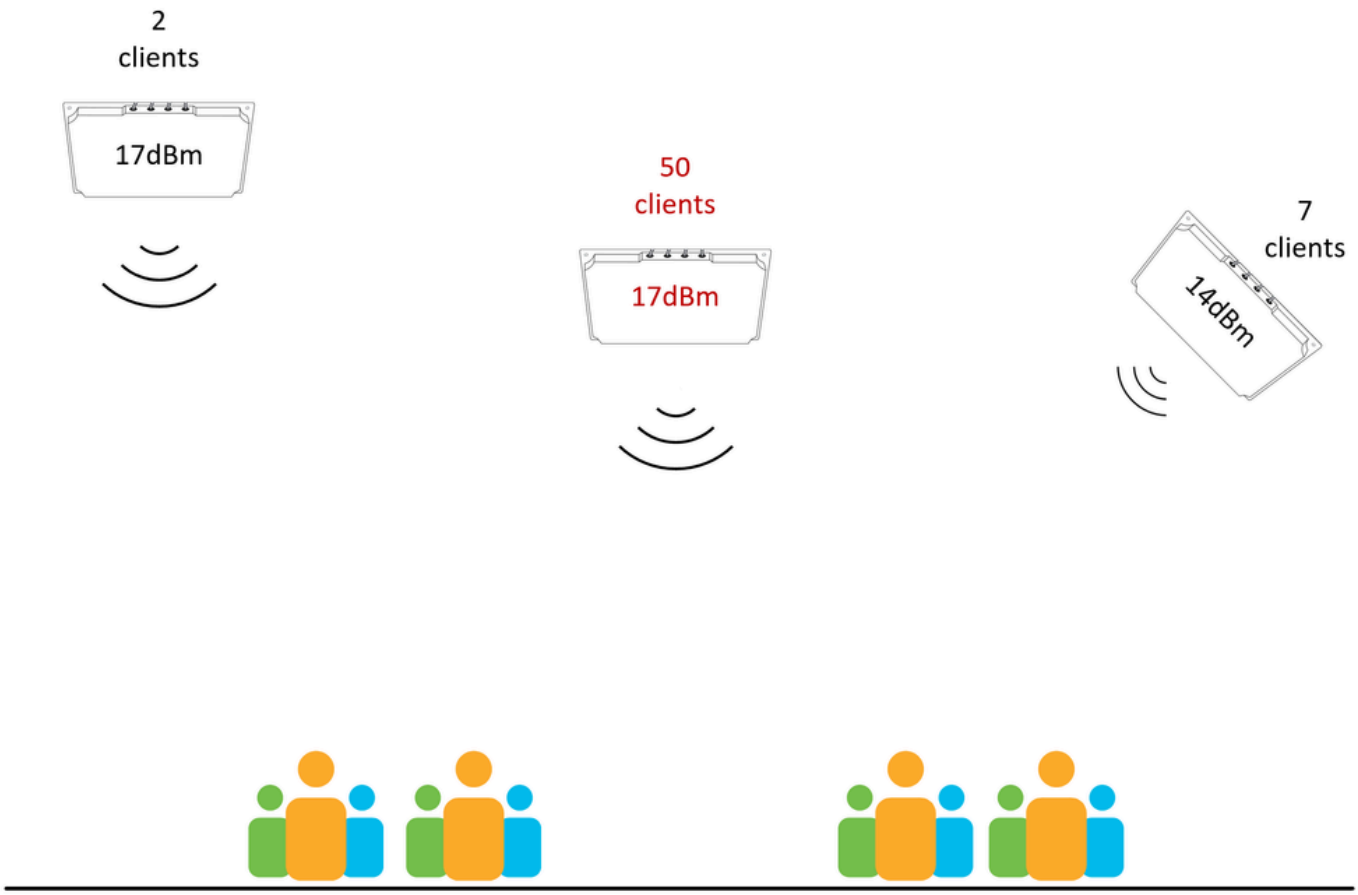


Ein Access Point mit höherer Leistung als die benachbarten Access Points zieht alle Clients im Umkreis an.

Das nächste Diagramm zeigt eine kompliziertere Situation: Nicht alle Antennen haben dieselbe Höhe, und nicht alle Antennen verwenden dieselbe Neigung/Ausrichtung. Eine ausgeglichene Leistung zu erreichen ist komplizierter, als alle Funkmodule mit derselben Sendeleistung zu konfigurieren. In Szenarien wie diesem kann eine Standortuntersuchung nach der Bereitstellung

erforderlich sein, um einen Überblick über die Abdeckung aus Sicht der Client-Geräte (vor Ort) zu erhalten. Anhand der Umfragedaten kann dann die Konfiguration für eine optimale Abdeckung und Client-Verteilung angepasst werden.

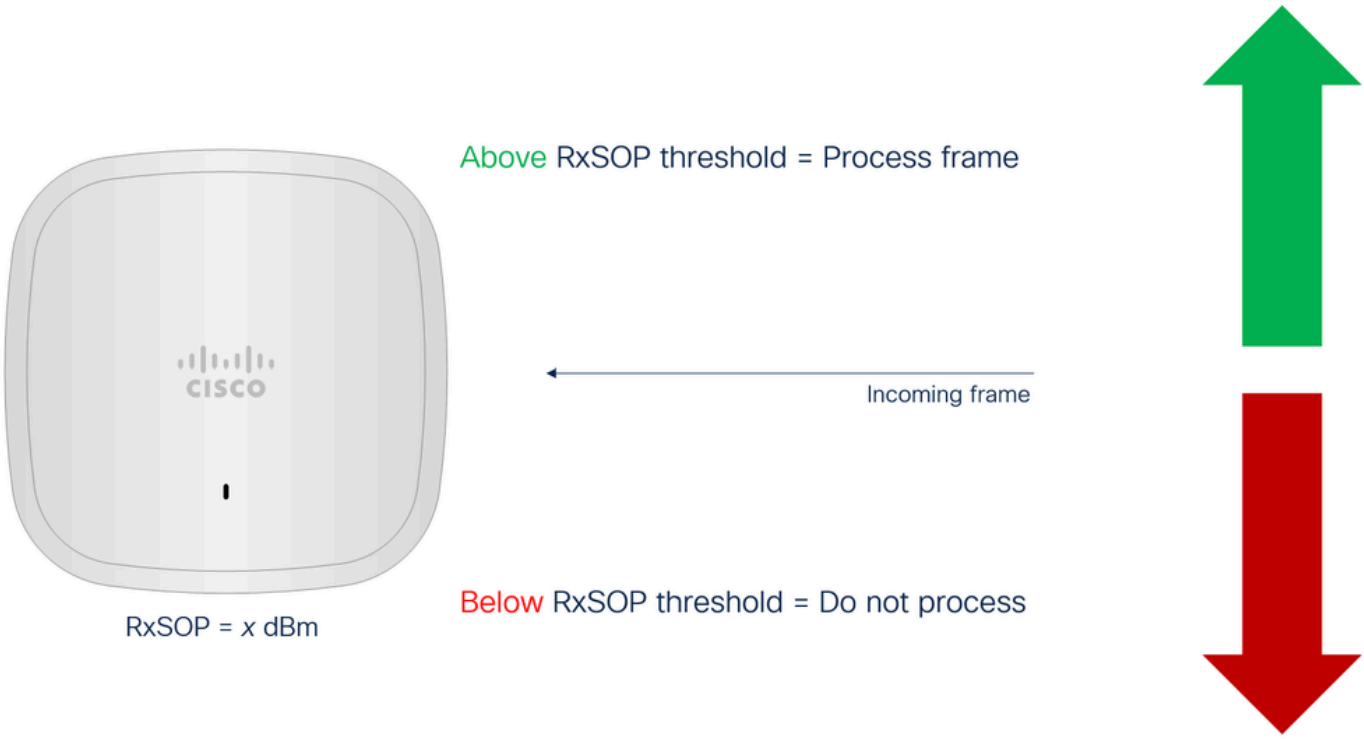
Die Entwicklung einheitlicher AP-Platzierungsorte, die komplizierte Situationen wie diese vermeiden, ist die beste Möglichkeit, anspruchsvolle RF-Tuning-Szenarien zu vermeiden (obwohl es manchmal keine andere Wahl gibt!).



Ein AP zieht alle Clients an, obwohl die Sendeleistung ähnlich ist, Höhe und Winkel spielen jedoch eine Rolle

RxSOP

Im Gegensatz zu Mechanismen wie Tx-Leistung oder Datenraten, die sich auf die Eigenschaften der Übertragungszelle auswirken, zielt RxSOP (Receiver Start of Packet Detection) darauf ab, die Größe der Empfangszelle zu beeinflussen. Im Wesentlichen kann RxSOP als Rauschschwelle gedacht werden, indem es den empfangenen Signalpegel definiert, unterhalb dessen der AP nicht versucht, Übertragungen zu decodieren. Übertragungen, deren Signalpegel unter dem konfigurierten RxSOP-Grenzwert liegt, werden vom Access Point nicht verarbeitet und werden effektiv als Rauschen behandelt.



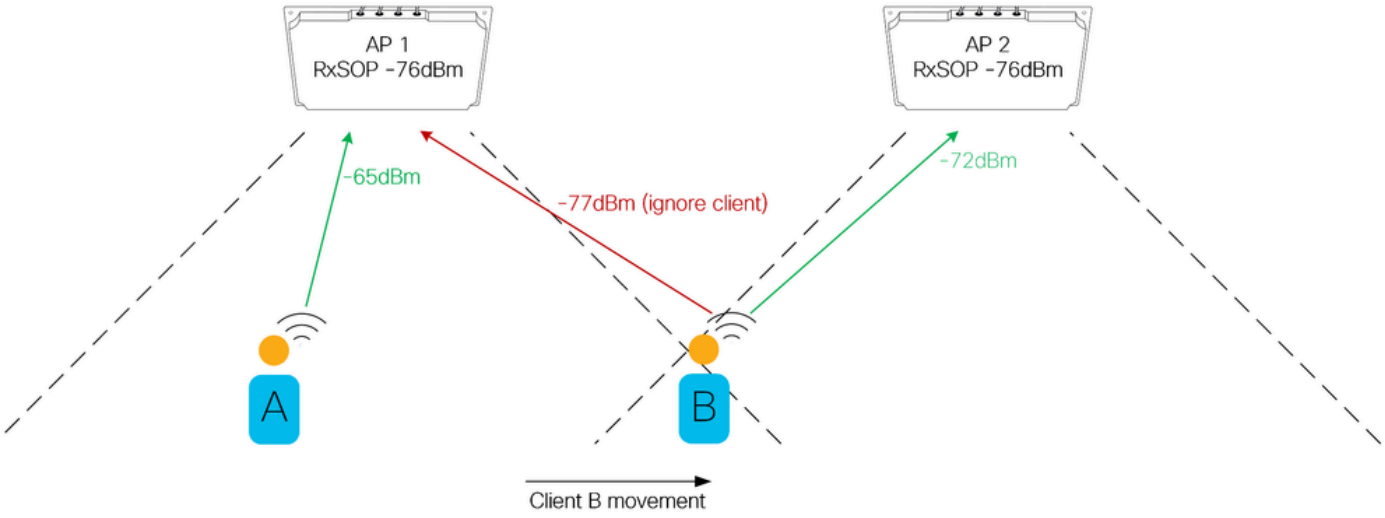
RxSOP-Konzept erklärt

Die Bedeutung von RxSOP

RxSOP hat mehrere Verwendungen. Sie kann verwendet werden, um die Fähigkeit der APs zur Übertragung in Umgebungen mit hohem Rauschen zu verbessern, die Verteilung der Clients zwischen Antennen zu steuern sowie um schwächere und empfindlichere Clients zu optimieren.

Bei lauten Umgebungen sei daran erinnert, dass die sendende Station (in diesem Fall der AP) vor der Übertragung eines 802.11-Frames zunächst die Verfügbarkeit des Mediums beurteilen muss, ein Teil dieses Prozesses ist es, zunächst auf bereits stattfindende Übertragungen zu hören. In dichten Wi-Fi-Umgebungen ist es üblich, dass viele Access Points auf relativ kleinem Raum nebeneinander bestehen und häufig dieselben Kanäle nutzen. In Umgebungen mit hohem Datenaufkommen kann der WAP die Kanalauslastung der umliegenden WAPs (einschließlich Reflexionen) melden und die eigene Übertragung verzögern. Durch Festlegen des entsprechenden RxSOP-Grenzwerts kann der WAP diese schwächeren Übertragungen ignorieren (Verringerung der wahrgenommenen Kanalnutzung), was zu häufigeren Übertragungschancen und einer verbesserten Leistung führt. Umgebungen, in denen APs eine signifikante Kanalauslastung (z. B. > 10 %) ohne Client-Last (z. B. eine leere Veranstaltungsstätte) melden, sind gute Kandidaten für RxSOP-Tuning.

Für die Client-Optimierung mit RxSOP beachten Sie dieses Diagramm.



Client-Roaming von rxsop betroffen

In diesem Beispiel gibt es zwei APs/Antennen mit genau definierten Abdeckungsbereichen. Client B wechselt vom Abdeckungsbereich von AP1 in den Abdeckungsbereich von AP2. Es gibt einen Crossover-Punkt, an dem AP2 den Client besser als AP1 hört, der Client jedoch noch nicht zu AP2 geroutet hat. Dies ist ein gutes Beispiel dafür, wie durch Festlegen des RxSOP-Grenzwerts die Grenze des Abdeckungsbereichs erzwungen werden kann. Durch die Gewährleistung, dass die Clients immer mit dem nächstgelegenen Access Point verbunden sind, wird die Leistung verbessert, da entfernte und/oder schwache Client-Verbindungen mit niedrigeren Datenraten wegfallen. Für eine solche Konfiguration der RxSOP-Schwellenwerte muss genau geklärt werden, wo der erwartete Abdeckungsbereich der einzelnen APs beginnt und endet.

Die Gefahren von RxSOP.

Wenn Sie den RxSOP-Grenzwert zu aggressiv festlegen, führt dies zu Abdeckungslücken, da der Access Point keine gültigen Übertragungen von gültigen Client-Geräten decodiert. Dies kann nachteilige Folgen für den Client haben, da der WAP nicht reagiert. Wenn die Client-Übertragung nicht gehört wurde, gibt es schließlich keinen Grund zu reagieren. Die RxSOP-Schwellenwerte müssen sorgfältig angepasst werden. Dabei ist stets sicherzustellen, dass gültige Clients im Abdeckungsbereich nicht von den konfigurierten Werten ausgeschlossen werden. Beachten Sie, dass einige Clients nicht gut darauf reagieren können, auf diese Weise ignoriert zu werden, zu aggressive RxSOP-Einstellungen geben dem Client nicht die Möglichkeit, auf natürliche Weise zu roamen, was den Client effektiv zwingt, einen anderen AP zu finden. Ein Client, der ein Beacon von einem WAP decodieren kann, geht davon aus, dass er an diesen WAP senden kann, sodass die Absicht der RxSOP-Abstimmung darin besteht, die Größe der Empfangszelle an den Beacon-Bereich des WAP anzupassen. Beachten Sie, dass ein (gültiges) Client-Gerät nicht immer über eine direkte Sichtlinie zum AP verfügt. Das Signal wird häufig durch Benutzer gedämpft, die von der Antenne abgewandt sind oder ihre Geräte in Taschen oder Taschen tragen.

Konfigurieren von RxSOP

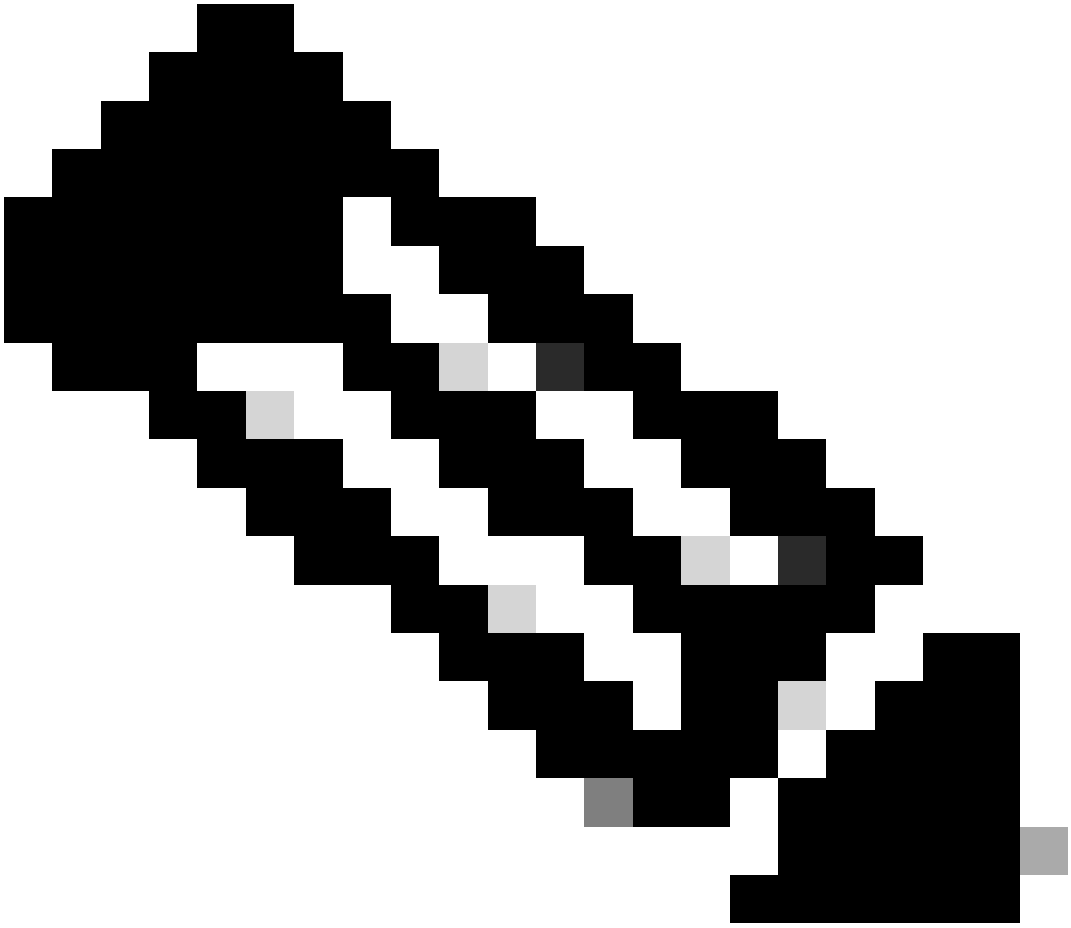
RxSOP wird pro RF-Profil konfiguriert.

Für jedes Band gibt es voreingestellte Schwellenwerte (Niedrig/Mittel/Hoch), die einen vordefinierten dBm-Wert festlegen. Es wird empfohlen, immer benutzerdefinierte Werte zu

verwenden, auch wenn der beabsichtigte Wert aus den verfügbaren Voreinstellungen stammt, sodass die Konfiguration besser lesbar ist.

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

RxSop-Einstellungstabelle



Hinweis: RxSOP-Änderungen erfordern kein Zurücksetzen der Funkübertragung und können ohne Verzögerung durchgeführt werden.

Skalierung des Netzwerks

Im Allgemeinen ist es keine gute Idee, ein Gerät so einzusetzen, wie es in den Unterlagen beschrieben ist. Datenblätter geben die Wahrheit wieder, aber die genannten Zahlen können sich in bestimmten Tätigkeitsbedingungen befinden. Wireless-Controller wurden getestet und zertifiziert, um eine bestimmte Anzahl von Clients und APs und einen bestimmten Durchsatz zu unterstützen. Dabei wird jedoch nicht davon ausgegangen, dass Clients jede Sekunde Roaming durchführen, dass Sie extrem lange eindeutige ACLs für jeden Client konfigurieren oder alle verfügbaren Snooping-Funktionen aktivieren können. Es ist daher wichtig, alle Aspekte sorgfältig abzuwägen, um sicherzustellen, dass das Netzwerk zu Spitzenzeiten skaliert werden kann und um auch eine Sicherheitsmarge für zukünftiges Wachstum zu erhalten.

Anzahl der APs

Eine der ersten Aufgaben bei der Bereitstellung eines Netzwerks besteht darin, die richtige Anzahl an Geräten zu planen und zu bestellen. Der größte variable Faktor ist die Anzahl und Art der Access Points und Antennen. Wireless-Lösungen müssen immer auf einem Funkfrequenzdesign basieren, jedoch (und leider) ist dies sehr oft der zweite Schritt im Projektlebenszyklus. Bei einfachen Bereitstellungen in Innenräumen gibt es zahlreiche Schätzverfahren, die mit hinreichender Sicherheit vorhersagen können, wie viele Access Points benötigt werden, noch bevor ein Wireless-Architekt die Grundrisse untersucht. Auch Vorhersagemodelle können in diesem Fall sehr nützlich sein.

Bei anspruchsvolleren Installationen, wie z. B. in industriellen, Outdoor- oder großen öffentlichen Netzwerken, oder an Orten, wo externe Antennen benötigt werden, reichen einfache Schätzverfahren häufig nicht aus. Bei früheren ähnlichen Anlagen ist ein gewisses Maß an Erfahrung erforderlich, um Typ und Menge der benötigten Ausrüstung angemessen schätzen zu können. Ein Standortbesuch durch einen Wireless-Architekten ist das absolute Minimum, um ein Verständnis für das Layout eines komplexen Veranstaltungsorts oder einer komplexen Einrichtung zu gewinnen.

Dieser Abschnitt enthält Richtlinien zur Festlegung der Mindestanzahl von APs und Antennen für die jeweilige Bereitstellung. Endmengen und spezifische Montageorte werden immer durch eine Bedarfsanalyse und ein Funkdesignverfahren ermittelt.

Die anfängliche Stückliste muss auf zwei Faktoren basieren: auf dem Antennentyp und der Anzahl der Antennen.

Antennentyp

Hier gibt es keine Abkürzungen. Der Antennentyp wird durch den abzudeckenden Bereich und die in diesem Bereich verfügbaren Montageoptionen bestimmt. Dies lässt sich nicht ohne ein Verständnis des physischen Raums feststellen, d. h. ein Standortbesuch wird von Personen mit einem Verständnis der Antennen und ihrer Abdeckungsmuster gefordert.

Anzahl der Antennen

Die Anzahl der erforderlichen Geräte kann aus dem Verständnis der erwarteten Anzahl von Client-Verbindungen abgeleitet werden.

Geräte pro Person

Die Anzahl der Benutzer kann anhand der Sitzplatzkapazität einer Sportstätte, der Anzahl der verkauften Tickets oder der erwarteten Anzahl von Besuchern auf der Grundlage historischer Statistiken bestimmt werden. Jeder menschliche Benutzer kann mehrere Geräte tragen, und es ist üblich, von mehr als einem Gerät pro Benutzer auszugehen, obwohl die Fähigkeit eines menschlichen Benutzers, mehrere Geräte gleichzeitig aktiv zu verwenden, fraglich ist. Die Anzahl der Besucher, die sich aktiv mit dem Netzwerk verbinden, hängt auch von der Art des Ereignisses und/oder der Bereitstellung ab.

Beispiel 1: Es ist normal, dass ein Stadion mit 80.000 Sitzplätzen nicht über 80.000 angeschlossene Geräte verfügt. Dieser Prozentsatz ist in der Regel deutlich niedriger. Bei

Sportveranstaltungen sind Benutzeranschlüsse von 20 % nicht ungewöhnlich, d. h. im Stadion mit 80.000 Sitzen können 16.000 Geräte angeschlossen werden (80.000 x 20 % = 16.000). Diese Anzahl hängt auch vom verwendeten Onboarding-Mechanismus ab. Wenn der Benutzer eine Aktion ausführen muss (z. B. auf ein Webportal klicken), sind die Zahlen niedriger als bei der automatischen Geräteintegration. Das automatische Onboarding kann so einfach sein wie ein PSK, das von einem vorherigen Ereignis in Erinnerung geblieben ist, oder etwas fortgeschritteneres wie die Verwendung von OpenRoaming, das Geräte ohne Benutzerinteraktion integriert. OpenRoaming-Netzwerke können dazu führen, dass Benutzer Nutzungsverhältnisse von weit über 50 % nutzen, was erhebliche Auswirkungen auf die Kapazitätsplanung haben kann.

Beispiel 2: Es kann davon ausgegangen werden, dass eine Technologiekonferenz ein hohes Maß an Benutzerverbindungen aufweist. Konferenzteilnehmer verbringen mehr Zeit damit, mit dem Netzwerk verbunden zu sein, und erwarten, dass sie auf ihre E-Mails zugreifen und tagtäglich Aufgaben erledigen können. Es ist zudem wahrscheinlicher, dass diese Art von Benutzern mehr als ein Gerät mit dem Netzwerk verbindet - obwohl ihre Fähigkeit, mehrere Geräte gleichzeitig zu verwenden, fraglich bleibt. Bei Technologiekonferenzen geht man davon aus, dass 100 % der Besucher eine Verbindung mit dem Netzwerk herstellen. Diese Zahl kann je nach Konferenztyp niedriger sein.

In beiden Beispielen besteht der Schlüssel darin, die erwartete Anzahl der verbundenen Geräte zu ermitteln. Daher gibt es keine einheitliche Lösung für jedes große öffentliche Netzwerk. In beiden Fällen wird eine Antenne an ein Funkgerät angeschlossen, und es sind Client-Geräte (keine menschlichen Benutzer), die eine Verbindung zu diesem Funkgerät herstellen. Client-Geräte pro Funk sind daher eine geeignete Kennzahl.

Geräte pro Funkmodul

Die maximale Client-Anzahl der Cisco APs beträgt 200 verbundene Geräte pro Funkmodul für 6 Wi-Fi-APs und 400 Geräte pro Funkmodul für 6 Wi-Fi-E-APs. Es ist jedoch nicht ratsam, eine maximale Kundenzahl einzuplanen. Aus Planungsgründen wird empfohlen, die Client-Anzahl pro Funkmodul deutlich unter 50 % der maximalen AP-Kapazität zu halten. Darüber hinaus hängt die Anzahl der Funkmodule vom Typ des verwendeten Access Points und der verwendeten Antenne ab. Im Abschnitt über Einzel- und Dual-5-GHz-Verbindungen wird dies genauer untersucht.

In dieser Phase empfiehlt es sich, das Netzwerk in verschiedene Bereiche aufzuteilen, wobei die Anzahl der Geräte pro Bereich erwartet wird. Wie erinnerlich soll in diesem Abschnitt eine Mindestanzahl von APs und Antennen geschätzt werden.

Ein Beispiel für drei unterschiedliche Abdeckungsbereiche zeigt die erwartete Client-Anzahl für jeden Bereich. Ein Wert von 75 Clients pro Funkeinheit (Health) wird zur Schätzung der erforderlichen Anzahl an Funkeinheiten verwendet.

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

Erwartete Anzahl an Funkmodulen/Clients pro Bereich

Diese Anfangszahlen müssen nun mit der Einsicht kombiniert werden, welche AP-Typen und Antennen in den einzelnen Bereichen eingesetzt werden und ob ein einzelnes oder duales 5-GHz-Band verwendet wird. 6-GHz-Berechnungen folgen derselben Logik wie 5 GHz. 2,4 GHz wird in diesem Beispiel nicht berücksichtigt.

Nehmen wir an, dass jeder der drei Bereiche eine Kombination aus einer 2566P-Patch-Antenne und der 9104-Stadionantenne verwendet, mit einer Kombination aus einem und zwei 5-GHz-Frequenzbändern. Dieses Szenario wird zur Veranschaulichung verwendet.

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)

Antennen pro Bereich

In jedem Bereich sind die benötigten Antennentypen und APs aufgeführt. Beachten Sie, dass bei einem Dual-5-GHz-Frequenzband das Verhältnis zwei Antennen zu einem AP beträgt.

In diesem Abschnitt wird ein Ansatz zur Schätzung der anfänglichen Anzahl von Antennen und Access Points beschrieben, die für eine Bereitstellung benötigt werden. Die Schätzung erfordert

ein Verständnis der physischen Bereiche, der möglichen Montageoptionen in jedem Bereich, des Typs der Antennen, die in jedem Bereich verwendet werden sollen, und der Anzahl der erwarteten Client-Geräte.

Jede Bereitstellung ist anders, und oftmals werden zusätzliche Geräte benötigt, um bestimmte oder schwierige Bereiche abzudecken. Bei dieser Art von Schätzung wird nur die Client-Kapazität (nicht die Abdeckung) berücksichtigt, und es wird der Umfang der erforderlichen Investitionen ermittelt. Die endgültige Platzierung der APs/Antennen und die Gesamtanzahl der Geräte müssen immer von einem erfahrenen Wireless-Experten eingehend geprüft und vor Ort verifiziert werden.

Erwarteter Durchsatz

Jeder Wireless-Kanal kann eine bestimmte verfügbare Kapazität bereitstellen, die in der Regel in den Durchsatz umgerechnet wird. Diese Kapazität wird von allen Geräten gemeinsam genutzt, die mit dem Funkmodul verbunden sind. Das bedeutet, dass die Leistung für jeden Benutzer sinkt, wenn weitere Benutzerverbindungen zum Funkmodul hinzugefügt werden. Dieser Leistungsabfall ist nicht linear und hängt auch von der genauen Mischung der verbundenen Clients ab.

Die Client-Funktionen unterscheiden sich je nach Gerät, je nach Chipsatz des Clients und der Anzahl der vom Client unterstützten Signalströme. Die maximale Client-Datenrate für jede Anzahl unterstützter räumlicher Datenströme ist in der nachfolgenden Tabelle aufgelistet.

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

Erwarteter maximaler realer Durchsatz für jeden Clienttyp

Bei den angegebenen Raten handelt es sich um theoretische maximale MCS-Raten (Modulation and Coding Scheme), die vom Standard 802.11 abgeleitet werden und ein Signal-Rausch-Verhältnis (Signal-to-Noise Ratio, SNR) von > 30 dBm annehmen. Das wichtigste Designziel leistungsfähiger Wireless-Netzwerke ist es, dieses Maß an SNR für alle Clients an allen Standorten zu erreichen. Dies ist jedoch selten der Fall. Wireless-Netzwerke sind dynamisch und nutzen lizenzfreie Frequenzen. Verschiedene unkontrollierte Interferenzen haben Auswirkungen auf die SNR-Funktion des Clients und darüber hinaus auf die Funktionen des Clients.

Selbst in Fällen, in denen das erforderliche SNR-Niveau erreicht wird, berücksichtigen die zuvor aufgeführten Raten nicht den Protokoll-Overhead. Daher lassen sie sich nicht direkt dem

tatsächlichen Durchsatz zuordnen (gemessen mit verschiedenen Geschwindigkeitstesttools). In der Praxis liegt die Rate immer unter der MCS-Rate.

Für alle Wireless-Netzwerke (einschließlich großer öffentlicher Netzwerke) ist der Client-Durchsatz immer von folgenden Faktoren abhängig:

- Funktionen des Clients.
- Signal-Rausch-Verhältnis des Clients zu diesem bestimmten Zeitpunkt
- Anzahl der anderen Clients, die zu diesem bestimmten Zeitpunkt verbunden sind
- Funktionen anderer Clients zu einem bestimmten Zeitpunkt
- Aktivität anderer Clients zu diesem bestimmten Zeitpunkt
- Interferenz zu einem bestimmten Zeitpunkt

Aufgrund der Variabilität dieser Faktoren ist es nicht möglich, unabhängig vom Gerätehersteller einen durchgängigen Mindestanteil pro Client für Wireless-Netzwerke zu garantieren.

Weitere Informationen finden Sie im Leitfaden zur Überprüfung des Wi-Fi-Durchsatzes: Tests und Überwachung.

WLC-Plattform

Die Auswahl Ihrer WLC-Plattform kann einfach erscheinen. Als Erstes sollten Sie sich die geschätzte Anzahl der Access Points und Clients ansehen, die Sie verwalten möchten. Das Datenblatt für jede WLC-Plattform enthält alle maximal unterstützten Objekte auf der Plattform: ACLs, Client-Anzahl, Site-Tags usw. Das sind buchstäblich maximale Zahlen und oft gibt es eine harte Durchsetzung. 6001-APs können nicht mit einem 9800-80 verbunden werden, der beispielsweise nur 6000-APs unterstützt. Aber ist es klug, überall das Maximum anzustreben?

Die Cisco Wireless Controller wurden so getestet, dass sie diese Höchstwerte erreichen, sie können jedoch nicht notwendigerweise alle dokumentierten Höchstwerte unter allen Bedingungen gleichzeitig erreichen. Nehmen wir als Beispiel den Durchsatz. Ein 9800-80 kann bis zu 80 Gbit/s an Client-Datenweiterleitung erreichen. In diesem Fall entspricht jedoch jedes Client-Paket der maximalen und optimalen Größe von 1500 Byte. Bei einer Kombination verschiedener Paketgrößen ist der effektive maximale Durchsatz geringer. Wenn Sie die DTLS-Verschlüsselung aktivieren, wird der Durchsatz weiter reduziert. Das Gleiche gilt für die Anwendungstransparenz. Es ist optimistisch, mehr als 40 Gbit/s von 9800-80 unter realistischen Bedingungen in einem großen Netzwerk mit vielen aktivierten Funktionen zu erwarten. Da dies je nach den verwendeten Funktionen und der Art der Netzwerkaktivität stark variiert, kann eine tatsächliche Vorstellung von der Kapazität nur gewonnen werden, wenn die Datapath-Nutzung mit diesem Befehl gemessen wird. Konzentrieren Sie sich auf die Load Metric, die einen Prozentsatz des maximalen Durchsatzes darstellt, den der Controller weiterleiten kann.

```
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#
```

In ähnlicher Weise kann der 9800-80 problemlos 6000 APs mit regulärer Aktivität verarbeiten. 6000 APs in einem öffentlichen Raum wie einem Stadion oder einem Flughafen zählen jedoch nicht als reguläre Aktivität. Angesichts des Client-Roaming und der Umgebungsbedingungen können große öffentliche Netzwerke mit maximaler Skalierung eine erhöhte CPU-Auslastung auf einem einzelnen WLC verursachen. Wenn Sie Überwachungs- und SNMP-Traps hinzufügen, die bei jedem Wechsel des Clients gesendet werden, kann die Last schnell zu hoch werden. Eines der wichtigsten Merkmale eines großen Veranstaltungsorts oder einer großen Veranstaltung ist, dass die Anzahl der Client-Onboarding-Ereignisse erheblich zunimmt, wenn sich die Mitarbeiter frei bewegen und sich ständig miteinander in Verbindung setzen bzw. trennen. Dies führt zu einem zusätzlichen Druck auf die CPU und die Kontrollebene.

Zahlreiche Bereitstellungen haben gezeigt, dass ein einzelnes (HA) Paar Wireless-Controller der Serie 9800-80 eine Bereitstellung in großen Stadien mit weit über 1.000 APs bewältigen kann. Häufig werden die APs auch über zwei oder mehr Controller-Paare verteilt, um kritische Ereignisse zu behandeln, bei denen die Verfügbarkeit und Verfügbarkeit im Vordergrund stehen. Wenn große Netzwerke auf mehrere WLCs verteilt werden, ist das Roaming zwischen den Controllern noch komplexer. Das Client-Roaming muss daher auf engstem Raum, z. B. in einem Stadion, sorgfältig abgewogen werden.

Siehe auch den Abschnitt Site-Tag in diesem Dokument.

WLC Hochverfügbarkeit

Es wird empfohlen, ein Hochverfügbarkeits-Stateful Switch Over (HA SSO)-Paar zu verwenden, das Hardwareredundanz bietet und gleichzeitig vor Softwareausfällen schützt. Mit HA SSO ist ein Softwareabsturz auf einem Gerät für die Endbenutzer transparent, da der sekundäre WLC nahtlos übernimmt. Ein weiterer Vorteil eines HA SSO-Paars sind die unterbrechungsfreien Upgrades, die durch die In-Service Software Upgrade (ISSU)-Funktion ermöglicht werden.

Wenn das Netzwerk groß genug ist, wird außerdem empfohlen, einen zusätzlichen Controller (N+1) zu verwenden. Sie kann verschiedenen Zwecken dienen, die die Hochverfügbarkeits-SSO nicht erfüllen kann. Sie können eine neue Softwareversion auf diesem WLC testen, bevor Sie ein Upgrade des Produktionspaars durchführen (und nur wenige Test-APs migrieren, um einen bestimmten Netzwerkbereich zu testen). Einige seltene Bedingungen können sich auf beide WLCs in einem HA-Paar auswirken (wenn das Problem in den Standby repliziert wird), und hier ermöglicht N+1 einen sicheren WLC in einem Aktiv-Aktiv-Szenario, in dem Sie APs schrittweise zu

und von migrieren könnten. Sie können auch als Bereitstellungs-Controller für die Konfiguration neuer Access Points dienen.

Die 9800-CLs sind sehr skalierbar und leistungsstark. Es ist zu beachten, dass sie über eine deutlich geringere Datenweiterleitungskapazität verfügen (von 2 Gbit/s bis 4 Gbit/s für das SR-IOV-Image), was sie tendenziell auf lokale FlexConnect-Switching-Szenarien (und möglicherweise auf eine geringe Anzahl von APs im zentralen Switching) beschränkt. Sie können jedoch als N+1-Geräte hilfreich sein, wenn Sie während eines Wartungsfensters oder bei der Fehlerbehebung zusätzliche Controller benötigen.

Externe Systeme

Während sich dieses Dokument hauptsächlich auf die Wireless-Komponente großer Ereignisnetzwerke konzentriert, gibt es eine Reihe von unterstützenden Systemen, die während der Skalierungs- und Designphase berücksichtigt werden müssen. Einige davon werden hier behandelt.

Core-Netzwerk

Große Wireless-Netzwerke werden in der Regel im zentralen Switching-Modus und mit großen Subnetzen bereitgestellt. Dies impliziert, dass eine sehr große Anzahl von Client-MAC-Adressen- und ARP-Einträgen an die angrenzende kabelgebundene Infrastruktur weitergeleitet wird. Es ist von entscheidender Bedeutung, dass die benachbarten Systeme, die den verschiedenen L2- und L3-Funktionen zugeordnet sind, über ausreichende Ressourcen verfügen, um diese Last zu bewältigen. Bei L2-Switches ist eine gemeinsame Konfiguration die Anpassung der SDM-Vorlage (Switch Device Manager), die für die Zuweisung von Systemressourcen zuständig ist und je nach Funktion des Geräts im Netzwerk einen Ausgleich zwischen L2- und L3-Funktionen bietet. Es muss sichergestellt werden, dass L2-Core-Geräte die erwartete Anzahl von MAC-Adresseinträgen unterstützen können.

Gateway-NAT

Der häufigste Anwendungsfall öffentlicher Netzwerke ist die Bereitstellung von Internetzugriff für Besucher. Entlang des Datenpfads muss ein Gerät für die NAT/PAT-Übersetzung zuständig sein. Die Internet-Gateways müssen über die erforderlichen Hardwareressourcen und die IP-Pool-Konfiguration verfügen, um die Last zu bewältigen. Denken Sie daran, dass ein Wireless-Client-Gerät für zahlreiche NAT/PAT-Übersetzungen zuständig sein kann.

DNS/DHCP

Diese beiden Systeme sind entscheidend für ein gutes Kundenerlebnis. Sowohl DNS- als auch DHCP-Dienste erfordern nicht nur eine angemessene Skalierung für die Verarbeitung der Last, sondern auch eine Berücksichtigung der Platzierung innerhalb des Netzwerks. Schnelle und reaktionsschnelle Systeme, die am selben Standort wie der WLC aufgestellt werden, sorgen für ein optimales Anwendererlebnis und vermeiden lange Client-Onboarding-Zeiten.

AAA/Webportal

Eine langsame Webseite wird von niemandem gemocht. Die Wahl eines geeigneten und gut skalierten Systems für die externe Web-Authentifizierung ist wichtig für eine gute Client-Integration. Für AAA müssen die RADIUS-Authentifizierungsserver in der Lage sein, die Anforderungen des Wireless-Systems zu erfüllen. Beachten Sie, dass in einigen Fällen die Last in Schlüsselmomenten ansteigen kann, z. B. in der Halbzeit eines Fußballspiels, was eine hohe Authentifizierungslast in einer kleinen Zeitspanne erzeugen kann. Die Skalierung des Systems für eine angemessene gleichzeitige Auslastung ist entscheidend. Bei der Verwendung von Funktionen wie AAA Accounting ist besondere Vorsicht geboten. Vermeiden Sie eine zeitbasierte Abrechnung um jeden Preis, und wenn Sie die Abrechnung verwenden, versuchen Sie, die Zwischenabrechnung zu deaktivieren. Ein weiterer zu berücksichtigender Punkt ist die Verwendung von Load Balancern. Hierbei müssen Sitzungs-Pin-Mechanismen verwendet werden, um einen vollständigen Authentifizierungsfluss sicherzustellen. Achten Sie darauf, die RADIUS-Zeitüberschreitung bei 5 Sekunden oder höher zu belassen.

Wenn Sie eine 802.1X-SSID mit einer großen Client-Anzahl (z. B. bei OpenRoaming) verwenden, müssen Sie 802.11r Fast Transition (FT) aktivieren. Andernfalls können Clients bei jedem Roaming einen Authentifizierungssturm verursachen.

DNS/DHCP

Einige Empfehlungen für DHCP:

- Stellen Sie sicher, dass der DHCP-Pool mindestens dreimal so viele Clients umfasst wie erwartet. IPs bleiben auch nach dem Verbindungsabbruch des Clients für einige Zeit zugewiesen, sodass je nach Aufenthaltszeit der Gäste mehr IP-Adressen verbraucht werden können. Passen Sie die Leasingzeit an die voraussichtliche Dauer des Besuchs der Sportstätte an. Wenn die gewöhnliche Dauer eines Besuchs zwei Stunden beträgt, ist es sinnlos, eine IP-Adresse für eine Woche zuzuweisen. Auf diese Weise können veraltete Leasingverträge schrittweise abgeschafft werden.
- Es wird empfohlen, ein großes Subnetz für Clients zu verwenden. Der WLC verfügt über eine Proxy-ARP-Funktion und leitet standardmäßig keine Broadcasts weiter (mit Ausnahme von DHCP). Die Verwendung eines großen Client-Subnetzes (z. B. /16) für Ihre Clients stellt kein Problem dar. Ein einzelnes großes VLAN ist einfacher als eine VLAN-Gruppe mit vielen VLANs. Die Konfiguration zahlreicher kleinerer Subnetze (z. B. /24) und VLAN-Gruppen hat keinen Einfluss auf die Broadcast-Domäne und führt nur zu einer komplizierteren Konfiguration, was zu Problemen wie unsauberen VLANs führt und verschiedene DHCP-Pools verfolgen muss, die nicht gleichmäßig genutzt werden können.
- Bewahren Sie DHCP im Bridging-Modus auf dem Wireless-Controller auf. Die DHCP-Relay-Funktion wird vom Layer-3-Gateway des Subnetzes übernommen. Dies ermöglicht maximale Effizienz und Einfachheit. Der Wireless-Controller soll dabei überhaupt nicht in den DHCP-Prozess eingebunden werden.
- Verwenden Sie DHCP Required in jedem öffentlichen WLAN, unabhängig von der Authentifizierungsmethode. Dies kann zwar einen kleinen Prozentsatz der fehlerhaften Client-Zuordnungen auslösen, kann jedoch erhebliche Sicherheitsprobleme verhindern, indem Clients versuchen, sich selbst statische IP-Adressen zuzuweisen, oder indem sie sich falsch verhalten und versuchen, eine vorherige IP-Adresse ohne Erlaubnis

wiederzuverwenden.

Betrieb des Netzwerks

Die richtige Konfiguration

Es ist verführerisch, eine Vielzahl von Optionen zu ermöglichen, um von den neuesten Funktionen des modernen Wi-Fi zu profitieren. Bestimmte Funktionen eignen sich jedoch hervorragend für kleine Umgebungen, haben jedoch große Auswirkungen auf große und dichte Umgebungen. Ebenso können bestimmte Funktionen Kompatibilitätsprobleme verursachen. Obwohl die Geräte von Cisco alle Standards erfüllen und mit einer Vielzahl von getesteten Clients kompatibel sind, gibt es weltweit zahlreiche Client-Geräte, die manchmal über Treibersoftware-Versionen mit Fehlern oder nicht mit bestimmten Funktionen kompatibel sind.

Je nachdem, wie viel Kontrolle Sie über die Clients haben, müssen Sie vorsichtig sein. Wenn Sie das Wi-Fi beispielsweise für eine große Jahrestagung Ihres Unternehmens bereitstellen, wissen Sie, dass die meisten Clients Unternehmensgeräte sind, und Sie können den Funktionsumfang entsprechend planen. Wenn Sie jedoch ein Wi-Fi-Netzwerk am Flughafen nutzen, hängt Ihre Zufriedenheit der Gäste direkt von der Fähigkeit ab, eine Verbindung mit Ihrem Netzwerk herzustellen. Sie haben keinerlei Kontrolle über die Client-Geräte, die die Mitarbeiter verwenden können.

SSIDs

Wie viele SSIDs?

Es wurde immer empfohlen, so wenige SSIDs wie möglich zu verwenden. Dies wird in Netzwerken mit hoher Dichte noch verschärft, da die Möglichkeit, mehrere APs auf demselben Kanal zu verwenden, nahezu garantiert ist. In der Regel verwenden viele Bereitstellungen zu viele SSIDs. Sie erkennen an, dass zu viele SSIDs vorhanden sind, erklären jedoch, dass sie nicht weniger verbrauchen können. Sie müssen für jeden SSID eine geschäftliche und technische Studie durchführen, um die Ähnlichkeiten zwischen den SSIDs und die Optionen zum Zusammenfassen mehrerer SSIDs zu verstehen.

Sehen wir uns nun einige Sicherheits-/SSID-Typen und ihre Verwendung an.

WPA2/3 Personal

Eine Pre-Shared Key-SSID ist aufgrund ihrer Einfachheit sehr beliebt. Sie können den Schlüssel entweder irgendwo auf Abzeichen oder Papier oder auf Schildern drucken oder ihn den Besuchern irgendwie mitteilen. Manchmal wird eine Pre-Shared Key-SSID sogar für eine Gast-SSID bevorzugt (vorausgesetzt, der Schlüssel ist allen Teilnehmern bekannt). Sie kann dabei helfen, die Erschöpfung des DHCP-Pools aufgrund der absichtlichen Art der Verbindung zu verhindern. Vorbeigehende Geräte stellen keine automatische Verbindung mit dem Netzwerk her und können daher keine IP-Adresse aus dem DHCP-Pool nutzen.

WPA2 PSK bietet keinen Datenschutz, da der Datenverkehr leicht entschlüsselt werden kann, da alle denselben Schlüssel verwenden. Im Gegenteil, WPA3 SAE bietet Privatsphäre, und selbst wenn jeder den Master-Schlüssel hat, ist es nicht möglich, den von anderen Clients verwendeten Verschlüsselungsschlüssel abzuleiten.

WPA3 SAE ist die bessere Wahl für die Sicherheit und wird von vielen Smartphones, Laptops und Betriebssystemen unterstützt. Einige IoT-Geräte oder intelligente Wearables können weiterhin nur eingeschränkten Support bieten, und ältere Clients im Allgemeinen sind anfällig für Probleme, wenn sie keine aktuellen Treiber oder Firmware-Updates erhalten haben.

Es kann verführerisch sein, einen Übergangsmodus WPA2 PSK-WPA3 SAE SSID zu betrachten, um die Dinge zu vereinfachen, aber dies wurde im Feld gezeigt, um einige Kompatibilitätsprobleme zu verursachen. Unzureichend programmierte Clients erwarten nicht, dass zwei Typen von Methoden mit gemeinsam genutzten Schlüsseln auf derselben SSID vorhanden sind. Wenn Sie sowohl WPA2- als auch WPA3-Optionen anbieten möchten, wird empfohlen, separate SSIDs zu konfigurieren.

WPA2/3-Enterprise

WPA3 Enterprise (mit AES-128-Bit-Verschlüsselung) ist technisch die gleiche Sicherheitsmethode (mindestens wie in den SSID-Beacons angekündigt) wie WPA2 Enterprise, die für maximale Kompatibilität sorgt.

Für 802.1X wird eine SSID für den Übergangsmodus empfohlen, da Kompatibilitätsprobleme mit den neuesten Geräten nicht auftreten (Probleme wurden mit Android 8 oder alten Apple IOS-Versionen berichtet). IOS XE 17.12 und höhere Versionen ermöglichen die Verwendung einer einzelnen Transition Enterprise SSID, bei der nur WPA3 verwendet und mit 6 GHz angekündigt wird, während WPA2 als Option für das 5 GHz-Band angeboten wird. Wir empfehlen, WPA3 auf Enterprise-SSIDs so bald wie möglich zu aktivieren.

WPA Enterprise-SSIDs können für wichtige Benutzer verwendet werden, für die eine Identitätsanbieter-Datenbank vorhanden ist, die die Rückgabe von AAA-Parametern (z. B. VLANs oder ACLs) in Abhängigkeit von der Benutzeridentität ermöglicht. Solche Arten von SSIDs können eduroam oder OpenRoaming umfassen, die die Vorteile von Gast-SSIDs (durch die Möglichkeit für Besucher, sich ohne Eingabe von Anmeldeinformationen zu verbinden) mit der Sicherheit eines Unternehmens-SSID verbinden. Sie reduzieren die Komplexität des Onboarding in der Regel im Zusammenhang mit 802.1x, da Kunden nichts tun müssen, um der Eudroam- oder OpenRoaming-SSID beizutreten, vorausgesetzt sie haben ein Profil auf ihrem Telefon (das einfach über eine Event-App bereitgestellt werden kann).

Gast-SSID

Ein Gast-SSID ist oft gleichbedeutend mit offener Authentifizierung. Sie können ein Web-Portal (oder nicht) hinter ihm (je nach gewünschter Freundlichkeit oder lokalen Anforderungen) in seinen verschiedenen Formen: externe, lokale oder zentrale Web-Authentifizierung, aber das Konzept bleibt das gleiche. Bei Verwendung eines Gastportals kann die Skalierbarkeit in großen Umgebungen schnell zum Problem werden. Weitere Informationen hierzu finden Sie im Abschnitt

Configuring for Scalability (Konfigurieren der Skalierbarkeit).

Für den Betrieb im 6-GHz-Band muss der Gast-SSID statt nur Open Enhanced Open verwenden. Dies ermöglicht es dennoch jedem, eine Verbindung herzustellen, bietet aber Datenschutz (sogar einen besseren Datenschutz als WPA2-PSK!) und Verschlüsselung, ohne dass beim Herstellen einer Verbindung über die SSID irgendein Schlüssel oder Anmeldeinformationen angegeben werden müssen. Die wichtigsten Smartphone-Anbieter und Betriebssysteme unterstützen jetzt Enhanced Open, doch ist diese Unterstützung in der Wireless-Client-Basis noch nicht weit verbreitet. Der Enhanced Open-Übergangsmodus bietet eine gute Kompatibilitätsoption, bei der sich fähige Geräte mit der verschlüsselten Gast-SSID verbinden (mit Enhanced Open), und die nicht fähigen Geräte verwenden die SSID weiterhin wie zuvor geöffnet. Endbenutzer erkennen zwar nur eine einzelne SSID, beachten Sie jedoch, dass dieser Übergangsmodus zwei SSIDs in Ihren Beacons überträgt (obwohl nur eine sichtbar ist).

Bei großen Veranstaltungen und Veranstaltungsorten wird oft empfohlen, ein PSK auf der Gast-SSID zu konfigurieren, anstatt es rein offen zu lassen (der erweiterte offene Übergangsmodus wäre besser, dies führt jedoch zu zwei SSIDs, und die Client-Kompatibilität muss noch umfassend nachgewiesen werden). Obwohl dies das Onboarding etwas komplizierter macht (Sie müssen den PSK auf die Badges oder Tickets der Leute drucken oder auf irgendeine Weise bewerben), werden gelegentliche Clients, die sich automatisch mit dem Netzwerk verbinden, vermieden, ohne dass der Endbenutzer die Absicht hat, das Netzwerk zu nutzen. Immer mehr Anbieter mobiler Betriebssysteme räumen zudem offenen Netzwerken die Priorität ab und geben Sicherheitswarnungen aus. In anderen Situationen können Sie eine maximale Anzahl von Passanten zu verbinden wünschen und daher offen ist die bessere Wahl.

Schlussfolgerung zur Anzahl der SSID

Auf die Frage, an wie vielen SSID man sich halten muss, kann es keine befriedigende Antwort geben. Die Auswirkung hängt von der konfigurierten Mindestdatenrate, der Anzahl der SSIDs und der Anzahl der APs ab, die auf demselben Kanal senden. Bei einer großen Cisco Veranstaltung verwendete die Wireless-Infrastruktur 5 SSIDs: die wichtigste WPA2-PSK, eine WPA3-SAE-SSID für Sicherheit und 6 GHz-Abdeckung, eine Enterprise-Eduroam-SSID für den einfachen Zugriff für Schulungsteilnehmer, eine OpenRoaming-SSID für die sichere Aufnahme von Personen, die Wi-Fi über die Event-App konfiguriert haben, und eine separate 802.1X-SSID für die und Administrator-Netzwerkzugriff. Das war schon fast zu viel, aber der Effekt blieb dank der großen Anzahl verfügbarer Kanäle vernünftig, und die Richtantennen, die verwendet wurden, um Kanalüberschneidungen so weit wie möglich zu reduzieren.

Die ältere SSID im Vergleich zu den wichtigsten SSID-Konzepten

Es wurde empfohlen, den 2,4-GHz-Service für einen bestimmten Zeitraum auf eine separate "Legacy"-SSID zu beschränken, die nur im 2,4-GHz-Bereich angekündigt wurde. Dies wird immer weniger populär, da die Leute aufhören, 2,4-GHz-Dienste insgesamt bereitzustellen. Die Idee kann und muss jedoch bestehen bleiben, aber mit anderen Konzepten. Sie möchten WPA3 SAE einführen, aber der Übergangsmodus gibt Ihnen Kompatibilitätsprobleme mit Ihren Clients? Verfügen über eine WPA2 "Legacy"-SSID und eine WPA3 SAE-Haupt-SSID. Durch die

Benennung der leistungsschwächsten SSID "Legacy" zieht es keine Clients an, und Sie können leicht erkennen, wie viele Clients noch Kompatibilitätsprobleme mit Ihrer Haupt-SSID haben und diese Legacy-SSID benötigen.

Aber warum hier aufhören? Sie haben Gerüchte gehört, dass 802.11v Probleme mit einigen älteren Clients verursacht hat, oder dass einige Clienttreiber nicht gerne Geräteanalysen auf der SSID aktiviert sehen? Aktivieren Sie alle diese nützlichen Funktionen auf Ihrer erweiterten Haupt-SSID, und lassen Sie sie auf Ihrer Legacy-/Kompatibilitäts-SSID los. Dies ermöglicht Ihnen, die Einführung neuer Funktionen auf Ihrer Haupt-SSID zu testen und gleichzeitig eine maximale Kompatibilitäts-SSID für Clients bereitzustellen, auf die Sie zurückgreifen können. Dieses System funktioniert nur so. Wenn Sie den umgekehrten Namen für Ihre kompatibilitätsgesteuerte SSID als Haupt- und Ihren erweiterten SSID mit "<name>-WPA3" angeben, werden Sie feststellen, dass die Leute an der alten SSID festhalten, an die sie gewöhnt waren, und die Akzeptanz für viele Jahre bei Ihrer "neuen" SSID gering bleibt. Die Einführung neuer Einstellungen oder Funktionen hat dann aufgrund der geringeren Anzahl von Clients, die sich damit verbinden, keine eindeutigen Ergebnisse.

SSID-Funktionen

- Es ist am besten, die Aironet-Erweiterungen deaktiviert zu lassen. Diese sind besonders nützlich für Site-Umfragen und WGB-Operationen, aber manchmal verursachen Probleme mit einigen älteren Kunden. Aironet IE kündigt außerdem den Hostnamen des Access Points an, der bei sicherheitsbewussten Bereitstellungen unerwünscht ist.
- CCKM ist ein veraltetes Protokoll (zugunsten von FT) und muss deaktiviert werden.
- Zu diesem Zeitpunkt ist es am besten, AES-128-Verschlüsselung zu verwenden, auch in WPA3 aufgrund der geringen Client-Unterstützung von höheren Verschlüsselungen (es sei denn, Sie können sich eine bestimmte sicherere und restriktivere SSID leisten)
- Coverage-Bohrungserkennung ist am besten deaktiviert (für alle SSIDs). In großen Bereitstellungen werden in der Regel Richtantennen verwendet, die eine gründliche Standortprüfung erfordern. Die Leistungspegel jeder Antenne sind das Ergebnis des Designprozesses für die Funkumgebung und werden in der Regel auf bestimmte Pegel konfiguriert.
- Adaptive FT muss deaktiviert werden, da einige Clients Probleme haben können, wenn FT nicht vollständig angekündigt ist, aber in einigen Attributen vorhanden ist. Entweder vollständig deaktivieren FT (für maximale Kompatibilität) oder gehen Sie mit FT+802.1X, die die meisten Clients (es sei denn, sie sind alt oder mehr IoT-orientiert) unterstützen. Bei der Konfiguration von FT+802.1X sind sogar Nicht-FT-Clients berechtigt, der SSID beizutreten. Das einzig mögliche Problem besteht bei einigen Clients, die es nicht tolerieren würden, zwei Sicherheitsoptionen auf derselben SSID zu sehen.
- 802.11ac MU-MIMO deaktivieren Sie erhöht die Komplexität und bietet nur sehr geringe Vorteile bei 802.11ac.
- Deaktivieren der BSS-Zielaktivierungszeit. Derzeit ist die Akzeptanz bei den Kunden gering.
- Deaktivieren Sie aggressive Lastverteilung und Frequenzauswahl. Eine Frequenzauswahl ist nicht erforderlich, wenn Sie die SSID nicht im 2,4-GHz-Frequenzbereich ankündigen (oder wenn sie sich auf einem dedizierten SSID befindet) und aggressiver Lastenausgleich die Client-Zuordnung verzögert, indem der Client mehrmals abgelehnt wird, bevor er sie

schließlich akzeptiert, wenn er auf der Verbindung mit einem geladenen Access Point besteht. Sie haben die Access Points ohnehin in einer stark ausgelasteten Umgebung geladen, was sich negativ auf die Client-Umgebung auswirkt.
- Deaktivieren Sie Fastlane+.
- Deaktivieren Sie Universal Admin, diese Funktion war für 3700 AP und nur in der -UX-Domäne. Wenn Sie es aktiviert lassen, bleibt ein unnötiger Angriffsvektor offen.
- Opportunistic Key Caching (OKC) aktiviert lassen. Es dient als schneller Roaming-Mechanismus für Clients, die FT nicht unterstützen.
- Lassen Sie WMM zu. Durch eine Deaktivierung würde Ihr Netzwerk auf die 802.11g-Ära zurückgeführt, und die 9800-Plattform hätte keine Vorteile.
- Aktivieren Sie IP Source Guard.
- Deaktivieren der RADIUS-Profilerstellung. In einer stark ausgelasteten Umgebung können dadurch übermäßige RADIUS-Accounting-Meldungen gesendet werden (wenn die Clients DHCP oder HTTP-Pakete senden), und der RADIUS-Server kann sehr stark überlastet werden.
- Verwenden Sie keine versteckten SSIDs. Dies dient keinem Sicherheitszweck. Der SSID-Name kann dennoch leicht mit einfachen Anwendungen oder durch eine Sniffer-Erfassung erkannt werden. Durch das Ausblenden der SSID wird das Client-Roaming verlangsamt, da diese nicht mehr vom passiven Beacon-Scanning profitieren und aktiv gescannt werden müssen, um Informationen zu benachbarten APs zu erhalten.
- Versuchen Sie, nicht mehr als vier WLANs pro Funkeinheit zu verwenden, da dies die Funkauslastung erheblich beeinträchtigt. Die Nutzung von fünf WLANs ist keine feste Einschränkung, kann aber angesichts der verschwendeten Funkzeit durch die Verwendung von immer mehr WLANs durchaus sinnvoll sein.
- 802.11v und 802.11k sind Standards, die immer mehr von gängigen Client-Typen unterstützt werden. Sie stellen in der Regel kein Problem mit der Client-Verbindung dar. Die Vorteile, die sie mit sich bringen, hängen stark davon ab, wie Clients diese Protokolle verwenden und können manchmal (im Fall von 802.11k) eine etwas höhere CPU-Auslastung verursachen. Sie können sie aus dem IoT oder der Legacy-SSID fernhalten, sie müssen jedoch nach Möglichkeit auf der Produktions-SSID aktiviert sein.

Site-Tag

Site-Tags sind ein Konfigurationselement, mit dem Access Points, die dieselben FlexConnect-Einstellungen verwenden, sowie Access Point-Join-Profileinstellungen (z. B. Anmeldedaten, SSH-Details und Ländercode) gruppiert werden können. Warum sind Site-Tags wichtig? Site-Tags definieren außerdem, wie APs vom WNCD-Prozess innerhalb des Catalyst 9800 behandelt werden. Lassen Sie uns ein paar Beispiele geben, um dies zu veranschaulichen:

- Wenn Sie vier Standort-Tags auf einem 9800-80 konfigurieren, der acht WNCD-Prozesse umfasst, wird jedes Standort-Tag einem anderen WNCD-Prozess zugewiesen (jeder auf einem separaten CPU-Core ausgeführt), und vier WNCD-Prozesse führen keine Aktionen aus. Dies bedeutet, dass Sie nicht alle CPUs Ihres 9800-80 verwenden und es wird nicht empfohlen, ihn mit den maximal 6000 unterstützten APs zu laden.

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

Erstes Beispiel für das Ausgleichen von Site-Tags

- Wenn Sie auf einem 9800-80 mit acht WNCD-Prozessen 10 Side Tags konfigurieren, übernehmen zwei WNCD-Prozesse jeweils zwei Site Tags, während die übrigen sechs jeweils ein Site Tag behandeln.

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

Zweites Beispiel für das Ausbalancieren von Site-Tags

Für geografisch große Bereitstellungen mit vielen Standorten und vielen Standort-Tags wird empfohlen, die Anzahl der Standort-Tags auf ein Vielfaches der Anzahl der WNCD-Prozesse auf der von Ihnen verwendeten Plattform zu erhöhen.

Für Veranstaltungsnetzwerke, die in der Regel unter einem Dach oder in mehreren Gebäuden am selben Standort stattfinden, wird jedoch empfohlen, die Anzahl der Site-Tags der genauen Anzahl der WNCDs auf der jeweiligen Plattform anzupassen. Das Endziel besteht darin, dass jeder WNCD-Prozess (und damit jeder CPU-Kern, der Wireless-Aufgaben zugewiesen ist) eine ungefähr ähnliche Anzahl von Client-Roam-Ereignissen verarbeitet, sodass die Last auf alle CPU-Kerne verteilt wird.

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

Im Kern geht es darum, APs, die sich in derselben physischen Nachbarschaft befinden, in derselben Site-Tag-Nummer zu gruppieren, sodass die häufigen Client-Roaming-Ereignisse zwischen diesen APs im gleichen CPU-Prozess verbleiben. Das bedeutet, dass es selbst bei einem großen Veranstaltungsort ratsam ist, den Veranstaltungsort in mehrere Standort-Tags aufzuteilen (so viele wie WNCD-Prozesse den Veranstaltungsort handhaben) und die APs so logisch wie möglich in diese zu gruppieren, um logische RF-Nachbarschaftsgruppen zu bilden, die ebenfalls gleichmäßig auf die Standort-Tags verteilt sind.

Ab IOS XE 17.12 kann ein Load Balancing-Algorithmus aktiviert werden, sodass der WLC die APs nach ihrer RF-Nähe gruppiert. Dies entlastet Sie und sorgt für eine ausgewogene Verteilung der APs über den WNCD-Prozess. Dies kann hilfreich sein, wenn Sie nicht einfach Gruppen von benachbarten APs zeichnen können, die in der richtigen Anzahl von Site-Tags platziert werden. Eine Besonderheit dieses Algorithmus besteht darin, dass er dem WNCD-Prozess APs unabhängig von ihrer Site-Tag-Zuweisung zuweist. Dies bedeutet, dass er die Site-Tag-Zuweisung des APs nicht ändert. Sie können dann Site-Tags ganz einfach einer Konfigurationslogik zuweisen, damit der Algorithmus die APs möglichst gleichmäßig auf die CPUs verteilt.

Die RF-basierte Funktion für automatischen AP-Lastenausgleich ist im Cisco Catalyst 9800 Wireless Controller Software Configuration Guide, Cisco IOS XE Dublin 17.12.x, dokumentiert.

Die CPU-Auslastung von WNCD-Prozessen muss bei großen Ereignissen überwacht werden. Wenn ein oder mehrere WNCD-Prozesse eine hohe Auslastung aufweisen, kann es sein, dass der WNCD zu viele APs oder Clients verarbeitet, oder dass die APs oder Clients, die er verarbeitet, geschäftiger sind als der Durchschnitt (wenn alle ständig roamen, z. B. in einem Flughafen).

Richtlinienprofil

- Aktivieren Sie ARP und Duplicate Address Detection (DAD) Proxy. Dadurch kann der WLC im Namen von Wireless-Clients antworten, wenn ein Gerät versucht, die MAC-Adresse eines Wireless-Geräts zu ermitteln. Dadurch werden auch Wireless-Client-Batterien eingespart.
- Aktivieren Sie die WGB-Funktionen nur bei Bedarf.
- Aktivieren Sie DHCP erforderlich, um Clients mit statischen IP-Adressen zu vermeiden.
- Halten Sie die Leerlaufzeitüberschreitung kurz (300 Sekunden). Manche Administratoren lassen es lange auf sich warten, bis sich Clients nicht erneut authentifizieren müssen, aber lange Leerlaufzeitüberschreitungen führen zu Geisterclienteinträgen (die die Berichterstellung beeinflussen), da sich die Client-Anzahl in Echtzeit verzögert. Es ist am besten, die Leerlaufzeitüberschreitung niedriger zu halten als die Zeitüberschreitung für die Gruppenschlüsselrotation, um Überlastungen bei der Abrechnung zu vermeiden, wenn die Clients gelöscht werden. Das Gruppenschlüssel-Rotationsintervall kann in der Webbenutzeroberfläche unter Configuration > Security > Advanced EAP als "EAP-Broadcast Key Interval" (EAP-Broadcast-Schlüsselintervall) konfiguriert werden.
- Setzen Sie das Sitzungs-Timeout auf 86400 Sekunden, um unnötige Verbindungstrennungen und erneute Authentifizierungen zu vermeiden.

AP-Teilnahmeprofil

- Stellen Sie sicher, dass TCP MSS anpassen aktiviert ist.
- Aktivieren Sie "Trust DSCP Upstream". Viele Wireless-Clients führen das 802.11e WMM UP-Tagging unglücklicherweise nicht aus. Das Vertrauen auf das DSCP-Feld ist eine sichere Methode, um Sprachanwendungen die richtige Priorität zuzuweisen.
- Aktivieren Sie Syslog für Ihre Access Points. Bei der Konfiguration einer Syslog-Server-IP werden die Konsolenprotokolle der Access Points per Unicast an diese Adresse gesendet. Es ist nicht nur nützlich, APs zu reparieren, es ist auch besser für das Netzwerk als die Standardeinstellung, bei der APs ihr Syslog im lokalen VLAN übertragen. Die AP-Protokollierung kann zu einer erheblichen Nachrichtenlast führen, selbst in Fällen, in denen das AP-Syslog nicht überwacht wird, empfiehlt es sich dennoch, die Anzahl der Ereignisse durch Einstellen des entsprechenden Schweregrads für die Nachricht zu begrenzen und/oder eine Syslog-IP-Adresse (z. B. 0.0.0.0) zu konfigurieren, um die Nachrichtenübertragung zu verhindern.
- Maximieren Sie CAPWAP-Wiederholungsversuche und -Zeitüberschreitung. Probleme werden weniger schnell erkannt, das Netzwerk ist jedoch resistenter gegen geringfügige vorübergehende Paketverluste.
- Aktivieren Sie SSH, und konfigurieren Sie Anmeldeinformationen. Deaktivieren Sie die AP-Konsole.
- Aktivieren Sie ggf. die AP-Überwachung, nicht jedoch die Funküberwachung.
- Aktivieren Sie die Erkennung von unberechtigten Geräten, und konfigurieren Sie einen RSSI-Schwellenwert von -70 dBm.

Überwachen des Netzwerks

Sobald das Netzwerk betriebsbereit ist, müssen Sie es auf Probleme hin genau überwachen. In einer normalen Büroumgebung kennen die Benutzer das Netzwerk und können sich bei Problemen gegenseitig helfen oder ein internes Helpdesk-Ticket eröffnen. In einer größeren Veranstaltungsstätte mit vielen Besuchern sollten Sie sich auf die größten Probleme konzentrieren und nicht auf bestimmte Personen, die nur eine Fehlkonfiguration aufweisen können. Sie benötigen daher die richtige Überwachungsstrategie.

Eine Überwachung des Netzwerks über die Kommandozeile oder GUI des Catalyst 9800 ist möglich, jedoch nicht das beste Tool zur täglichen Überwachung. Es ist die direkteste, wenn Sie bereits Verdachtsmomente und/oder Daten über das Problem haben und bestimmte Befehle in Echtzeit ausführen möchten. Die wichtigsten Überwachungsoptionen sind Cisco Catalyst Center oder ein benutzerdefiniertes Telemetrie-Dashboard. Es ist möglich, Überwachungstools von Drittanbietern zu verwenden, aber wenn diese SNMP als Protokoll verwenden, sind die Daten bei weitem nicht in Echtzeit und die üblichen Überwachungstools von Drittanbietern sind nicht detailliert genug, um alle Besonderheiten des Wireless-Anbieters zu berücksichtigen. Wenn Sie das SNMP-Protokoll auswählen, stellen Sie sicher, dass SNMPv3 verwendet wird, da SNMPv2 veraltete Sicherheitsfunktionen aufweist.

Cisco Catalyst Center ist die beste Option, da sie Ihnen die Verwaltung Ihres Netzwerks zusätzlich zur Überwachung ermöglicht. Es ermöglicht nicht nur die Überwachung, sondern auch die direkte

Fehlerbehebung und die Behebung zahlreicher Situationen.

Ein benutzerdefiniertes Telemetrie-Dashboard kann hilfreich sein, wenn Sie auf einem Bildschirm sehr spezifische Metriken und Widgets für ein NOC oder SOC permanent anzeigen möchten. Wenn es sehr spezifische Bereiche Ihres Netzwerks gibt, die Sie im Auge behalten möchten, können Sie dedizierte Widgets erstellen, um die Netzwerkmetriken in diesen Bereichen auf die Art und Weise Ihrer Wahl anzuzeigen.

Für Ereignisnetzwerke ist es sinnvoll, systemweite RF-Statistiken zu überwachen, insbesondere die Kanalnutzung und die Anzahl der Clients pro AP. Dies kann über die CLI erfolgen, es wird jedoch nur ein Snapshot zu einem bestimmten Zeitpunkt bereitgestellt. Die Kanalnutzung ist tendenziell dynamisch und eignet sich besser für die Überwachung im Laufe der Zeit. Für diese Art der Überwachung ist ein benutzerdefiniertes Dashboard in der Regel ein guter Ansatz. Weitere Kennzahlen, die im Laufe der Zeit besser überwacht werden können, sind die WNCD-Nutzung, die Anzahl der Clients und deren Status sowie standortspezifische Kennzahlen. Ein Beispiel für standortspezifische Kennzahlen wäre die Überwachung der Nutzung und/oder Auslastung für einen bestimmten Bereich oder Standort, beispielsweise Halle X bei einem Konferenzzentrum oder Sitzbereich Y bei einem Veranstaltungsort.

Für die benutzerdefinierte Überwachung sind sowohl die NETCONF RPC- (Pull) als auch die NETCONF-Streaming-Telemetrie (Push) gültige Ansätze. Die Verwendung von benutzerdefinierter Streaming-Telemetrie in Verbindung mit Catalyst Center erfordert jedoch eine gewisse Sorgfalt, da die Anzahl der Telemetrie-Abonnements, die auf dem WLC konfiguriert werden können, begrenzt ist und viele von diesen vorab auslastet.

Bei der Verwendung von NETCONF RPC müssen einige Tests durchgeführt werden, um sicherzustellen, dass der WLC nicht mit NETCONF-Anforderungen überlastet wird. Besonders wichtig ist, dass die Aktualisierungsraten für einige Datenpunkte und die Zeit für die Rückgabe der Daten berücksichtigt werden. Beispielsweise wird die AP-Kanalnutzung alle 60 Sekunden aktualisiert (vom Access Point zum WLC), und das Erfassen von Funkkennzahlen für 1.000 Access Points (vom WLC) kann mehrere Sekunden in Anspruch nehmen. In diesem Beispiel wäre es nicht sinnvoll, den WLC alle 5 Sekunden abzufragen. Ein besserer Ansatz wäre, systemweite Funkkennzahlen alle 3 Minuten zu erfassen.

NETCONF wird gegenüber SNMP immer bevorzugt.

Schließlich darf die Überwachung der Kernnetzwerkkomponenten, einschließlich der Nutzung des DHCP-Pools, der Anzahl der NAT-Einträge auf den Core-Routern usw. nicht außer Acht gelassen werden. Da der Ausfall eines dieser Geräte leicht die Ursache für einen Wireless-Ausfall sein kann.

Spezifische Probleme bei großen Netzwerken

Wenn Sie eine SSID mit Web-Authentifizierung haben, können ein Problem Clients sein, die sich mit dieser SSID verbinden und eine IP-Adresse erhalten, sich aber nie authentifizieren, da der Endbenutzer nicht aktiv versucht, eine Verbindung herzustellen (das Gerät wird automatisch verbunden). Der Controller muss alle HTTP-Pakete abfangen, die von Clients gesendet werden,

die sich im Status "Web Authentication Pending" (Webauthentifizierung ausstehend) befinden und WLC-Ressourcen verwenden. Wenn Ihr Netzwerk ausgeführt wird, achten Sie regelmäßig darauf, wie viele Clients sich zu einem bestimmten Zeitpunkt im Wartezustand der Webauthentifizierung befinden, um einen Vergleich mit den Basiszahlen zu erhalten. Dasselbe gilt für Clients im IP-Lernstatus. Clients befinden sich immer in diesem Zustand, wenn sie ihren DHCP-Prozess durchführen. Wenn Sie jedoch wissen, welche Nummer für Ihr Netzwerk geeignet ist, können Sie eine Basislinie erstellen und die Momente identifizieren, in denen diese Zahl zu hoch sein kann, was auf ein größeres Problem hindeutet.

Bei großen Veranstaltungsorten ist es nicht ungewöhnlich, dass ~10 % der Clients den Status Web Auth Pending (Webauthentifizierung ausstehend) aufweisen.

Day-2-Monitoring: Zufriedenheit der Benutzer im Auge

Wenn das Netzwerk betriebsbereit ist, gibt es zwei typische Arten von Endbenutzerbeschwerden: Sie können keine Verbindung herstellen oder haben Probleme mit der Verbindung (Trennung der Verbindungen), oder das Wi-Fi arbeitet langsamer als erwartet. Letztere ist sehr schwer zu identifizieren, da sie zunächst von den Geschwindigkeitserwartungen und der Echtzeitdichte eines bestimmten Bereichs abhängt. Sehen wir uns nun einige Ressourcen an, die Ihnen bei der täglichen Überwachung eines großen Netzwerks an einem Veranstaltungsort helfen können.

Validierung des Wi-Fi-Durchsatzes: Leitfaden für Tests und Überwachung In diesem Dokument von cisco.com wird beschrieben, wie Sie ein Netzwerk überwachen, um Durchsatzprobleme zu erkennen. Sie ermittelt, wie viel Durchsatz Clients in Ihrem Netzwerk erwarten können, wenn die Dinge ruhig sind, und schätzt, wie viel diese Schätzungen bei steigender Client-Anzahl und -Auslastung ausfallen. Dies ist entscheidend, um zu bewerten, ob eine vom Endbenutzer geäußerte Beschwerde über den Durchsatz aus technischer Sicht gerechtfertigt ist oder nicht, und ob Sie diesen Bereich für die möglicherweise anstehende Last neu gestalten müssen.

Wenn Kunden Verbindungsprobleme melden, nachdem diese mit Catalyst Center isoliert und geklärt wurden, werfen Sie einen Blick auf die Fehlerbehebung bei Verbindungsproblemen mit Catalyst 9800-Clients.

Schließlich sollten Sie mithilfe der Catalyst 9800 KPIs (Key Performance Indicators) die allgemeinen Schlüsselmetriken des WLC im Auge behalten.

Konfigurieren für Skalierbarkeit

SVIs und Schnittstellen am 9800

Vermeiden Sie die Erstellung von SVIs für Client-VLANs auf dem WLC. Administratoren, die mit älteren AireOS-WLCs vertraut sind, neigen dazu, eine Layer-3-Schnittstelle für jedes Client-VLAN zu erstellen. Dies ist jedoch selten erforderlich. Schnittstellen erhöhen den Angriffsvektor der Kontrollebene und können mehr ACLs mit komplexeren Einträgen erfordern. Auf den WLC kann standardmäßig über jede seiner Schnittstellen zugegriffen werden. Es ist mehr Arbeit erforderlich, um einen WLC mit mehr Schnittstellen zu schützen. Außerdem wird das Routing kompliziert, daher ist es am besten, dies zu vermeiden.

Ab IOS XE 17.9 sind die SVI-Schnittstellen nicht mehr für mDNS-Snooping oder DHCP-Relay erforderlich. Es gibt daher nur sehr wenige Gründe, eine SVI-Schnittstelle in einem Client-VLAN zu konfigurieren.

Aggregierte Testantwort

Bei großen öffentlichen Netzwerken ist es ratsam, das standardmäßige Intervall für Aggregationstests zu ändern, das von Access Points gesendet wird. Standardmäßig aktualisieren die APs den WLC alle 500 ms über die von den Clients gesendeten Tests. Diese Informationen werden von Funktionen für Lastenausgleich, Bandauswahl, Standort und 802.11k verwendet. Wenn es viele Clients und Access Points gibt, ist es ratsam, das Aktualisierungsintervall zu ändern, um Leistungsprobleme auf der Kontrollebene im WLC zu vermeiden. Empfohlen wird eine Einstellung von 50 aggregierten Testantworten alle 64 Sekunden. Stellen Sie außerdem sicher, dass Ihre APs keine Stichproben von lokal verwalteten MAC-Adressen melden, da es keine Punktverfolgung gibt. Wenn ein einzelner Client während des Scannens viele lokal verwaltete MACs verwenden könnte, um eine zweckmäßige Verfolgung zu vermeiden.

```
wireless probe limit 50 64000

no wireless probe localy-administered-mac
```

IPv6

Viele Netzwerkadministratoren sind noch immer gegen IPv6. Es gibt nur zwei akzeptable Optionen für IPv6: entweder Sie unterstützen IPv6 und müssen die entsprechende Konfiguration überall bereitstellen, oder Sie tun es nicht, und Sie müssen es blockieren. Es ist nicht akzeptabel, sich nicht um IPV6 zu kümmern und es an einigen Orten ohne ordnungsgemäße Konfiguration aktiviert zu lassen. Damit bliebe die gesamte IP-Welt erhalten, für die Ihre Netzwerksicherheit keine Verantwortung trägt.

Wenn Sie IPv6 aktivieren, müssen Sie eine virtuelle IPv6-Adresse im Bereich 2001:DB8::/32 konfigurieren (dies wird oft vergessen).

Es ist wichtig zu beachten, dass IPv6 für seine grundlegenden Vorgänge zwar in hohem Maße auf Multicast angewiesen ist, aber dennoch funktionieren kann, wenn Sie die Multicast-Weiterleitung auf dem WLC deaktivieren. Multicast-Weiterleitung bezieht sich auf die Multicast-Datenweiterleitung durch den Client und nicht auf die Ermittlung von Netznachbarn, Router-Anfragen und andere für den Betrieb von IPv6 erforderliche Protokolle.

Wenn Ihre Internetverbindung oder Ihr Internetdienstanbieter IPv6-Adressen bereitstellt, können Sie IPv6 für Ihre Clients zulassen. Das ist eine andere Entscheidung als IPv6 in Ihrer Infrastruktur zu aktivieren. Ihre APs konnten den Betrieb nur unter IPv4 aufrechterhalten, aber dennoch IPv6-Client-Datenverkehr innerhalb ihrer CAPWAP-Pakete übertragen. Wenn Sie IPv6 in Ihrer Infrastruktur aktivieren, müssen Sie den Client-Zugriff auf Ihre APs, den WLC und das Management-Subnetz schützen.

Überprüfen Sie die RA-Frequenz Ihrer Client-Gateways. Der WLC bietet eine RA-Drosselungsrichtlinie, die die Anzahl der RAs begrenzt, die an die Clients weitergeleitet werden, da diese manchmal chatty erhalten.

mDNS

Im Allgemeinen ist es am besten, mDNS in einer großen Bereitstellung am Veranstaltungsort vollständig zu deaktivieren.

mDNS-Bridging bezieht sich auf das Konzept, das Senden der mDNS-Pakete als Layer-2-Multicast (also an das gesamte Client-Subnetz) zuzulassen. mDNS wurde in Heim- und kleinen Büroszenarien populär, in denen es sehr praktisch ist, Dienste in Ihrem Subnetz zu erkennen. In einem großen Netzwerk bedeutet dies jedoch, dass das Paket an alle Clients im Subnetz gesendet wird, was aus Datenverkehrsperspektive in einem großen öffentlichen Netzwerk problematisch ist. Andererseits verursacht das Bridging keinen Overhead für die AP- oder WLC-CPU, da es als regulärer Datenverkehr angesehen wird. mDNS Proxy oder mDNS Gateway bezieht sich auf das Konzept, den WLC als Verzeichnis für alle Dienste im Netzwerk zu verwenden. Auf diese Weise können mDNS-Services über Layer-2-Grenzen hinweg effizient bereitgestellt und der gesamte Datenverkehr reduziert werden. Beim mDNS-Gateway sendet beispielsweise ein Drucker seine periodische Serviceankündigung über mDNS mit einem Layer-2-Multicast mit demselben Subnetz, der WLC leitet sie jedoch nicht an alle anderen Wireless-Clients weiter. Stattdessen nimmt es den angebotenen Dienst zur Kenntnis und registriert ihn in seinem Dienstverzeichnis. Immer wenn ein Client Dienste eines bestimmten Typs anfordert, antwortet der WLC im Namen des Druckers mit der Ankündigung. Auf diese Weise können alle anderen Wireless-Clients nicht mehr über unnötige Anfragen und Serviceangebote informiert werden, sondern erhalten nur eine Antwort, wenn sie fragen, welche Services vorhanden sind. Obwohl die Effizienz des Datenverkehrs deutlich verbessert wird, verursacht sie aufgrund des Snoopings von mDNS-Datenverkehr einen Overhead auf dem WLC (oder dem AP, wenn Sie in FlexConnect-Szenarien auf AP mDNS zugreifen). Bei Verwendung des mDNS-Gateways ist es wichtig, die CPU-Auslastung im Auge zu behalten.

Die Überbrückung führt zu einem Multicast-Sturm in Ihrem großen Subnetz, und das Snooping (mit der mDNS-Gateway-Funktion) verursacht eine hohe CPU-Auslastung. Deaktivieren Sie sie global und in jedem WLAN.

Einige Administratoren aktivieren mDNS, da einige Dienste es an bestimmten Orten benötigen. Es ist jedoch wichtig zu wissen, wie viel unerwünschter Datenverkehr dadurch hinzukommt. Apple-Geräte werben oft für sich selbst und suchen ständig nach Diensten, was ein Hintergrundgeräusch von mDNS-Abfragen verursacht, selbst wenn niemand einen bestimmten Dienst nutzt. Wenn Sie mDNS aufgrund einer bestimmten Geschäftsanforderung zulassen müssen, aktivieren Sie es global und dann nur im WLAN, wo es erforderlich ist, und versuchen Sie, den Bereich einzuschränken, in dem mDNS zulässig ist.

Sicherung des Netzwerks

Sicherheit

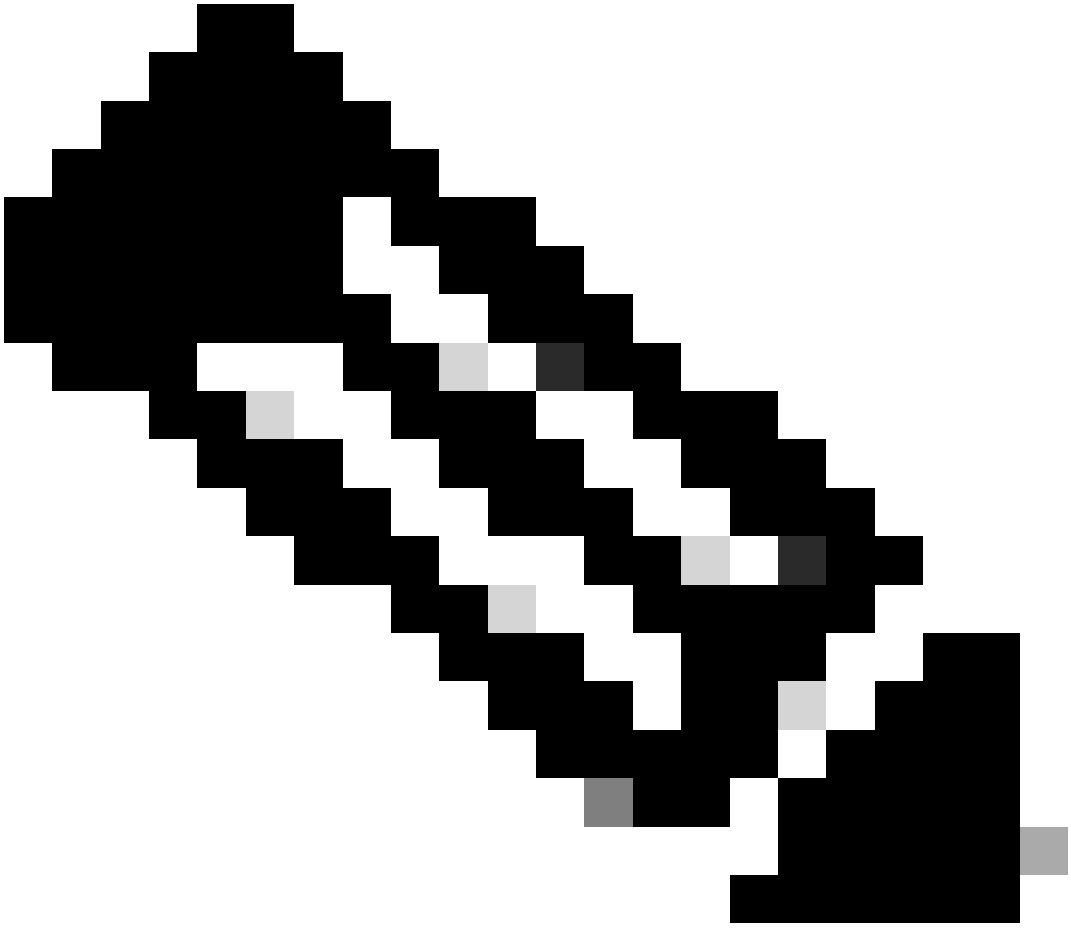
In großen öffentlichen Netzwerken kann vieles passieren, ohne dass der Administrator davon weiß. Die Leute bitten an zufälligen Stellen um Kabelverluste, oder stecken einen Switch für den Heimgebrauch an einen Ort, um mehr Switchports für ihre Machenschaften zu haben... Sie probieren diese Dinge normalerweise aus, ohne vorher um Erlaubnis zu fragen. Dies bedeutet, dass auch ohne einen Angreifer die Sicherheit bereits durch gutwillige Kunden und/oder Mitarbeiter beeinträchtigt werden kann. Für einen Angreifer wird es dann sehr einfach, einfach herumzulaufen und ein Kabel zu finden, an das er sich anschließen kann, um zu sehen, welchen Netzwerkzugriff er von dort erhält. Die Konfiguration der 802.1X-Authentifizierung auf allen Switch-Ports ist eine wichtige Voraussetzung für die Aufrechterhaltung angemessener Sicherheit in einem großen Netzwerk. Catalyst Center kann Sie bei der Automatisierung dieser Bereitstellung unterstützen. Ausnahmen sind für bestimmte Geräte möglich, die keine 802.1X-Authentifizierung unterstützen. Verlassen Sie sich dabei jedoch so wenig wie möglich auf die MAC-basierte Authentifizierung, da dies (aufrichtig) keine echte Sicherheit ist.

Nicht autorisierte Access Points

Ihre Strategie zur Bekämpfung von Schurken hängt von einigen Faktoren ab. Viele Administratoren wenden instinktiv sehr strenge Regeln an, aber die wichtigsten Fragen sind:

- Wenn Sie Hunderte (wenn nicht Tausende) von unberechtigten Warnmeldungen erhalten, haben Sie dann die Humanressourcen, um sie alle zu untersuchen und entsprechende Maßnahmen zu ergreifen?
- Ist Ihr Ziel darin, unberechtigte Geräte physisch zu entfernen, um ein sauberes Funkspektrum zu erhalten? Wenn ja, benötigen Sie viele Personen, um diese Operation durchzuführen. Oder vielleicht ist Ihr Ziel, nur ein Auge auf den Sicherheitsfaktor und nur sicherzustellen, dass die Schurken keine Gefahr darstellen? Dies führt zu viel überschaubareren menschlichen Arbeitskosten.
- Die Aktivierung von Erkennung nicht autorisierter APs kann sich auf Ihre Funkzeit auswirken, und die Eindämmung von nicht autorisierten APs hat in der Regel noch größere Auswirkungen. Haben Sie diese Auswirkungen analysiert und berücksichtigt?

Was die Auswirkungen von nicht autorisierter Erkennung angeht, verfügen die 9120 und 9130s über einen speziellen CleanAir-Chip, der das Off-Channel-Scannen (und somit die Erkennung von nicht autorisierten Access Points) übernimmt. Dadurch sind die Auswirkungen auf das Client-Funkgerät nahezu null. APs der Serie 9160 mit ihrem CleanAir Pro-Chip verfügen über eine ähnliche Scanning-Funktion ohne Auswirkungen, aber andere APs, die nicht über den CleanAir-Chip verfügen, müssen ihren Client-Funksender vom Kanal abziehen, um nach unberechtigten Geräten zu suchen oder Eindämmung zu betreiben. Das verwendete AP-Modell spielt daher eine Rolle bei der Entscheidung, dedizierte APs im Überwachungsmodus für die Erkennung und Eindämmung von unautorisierten Access Points zu verwenden.

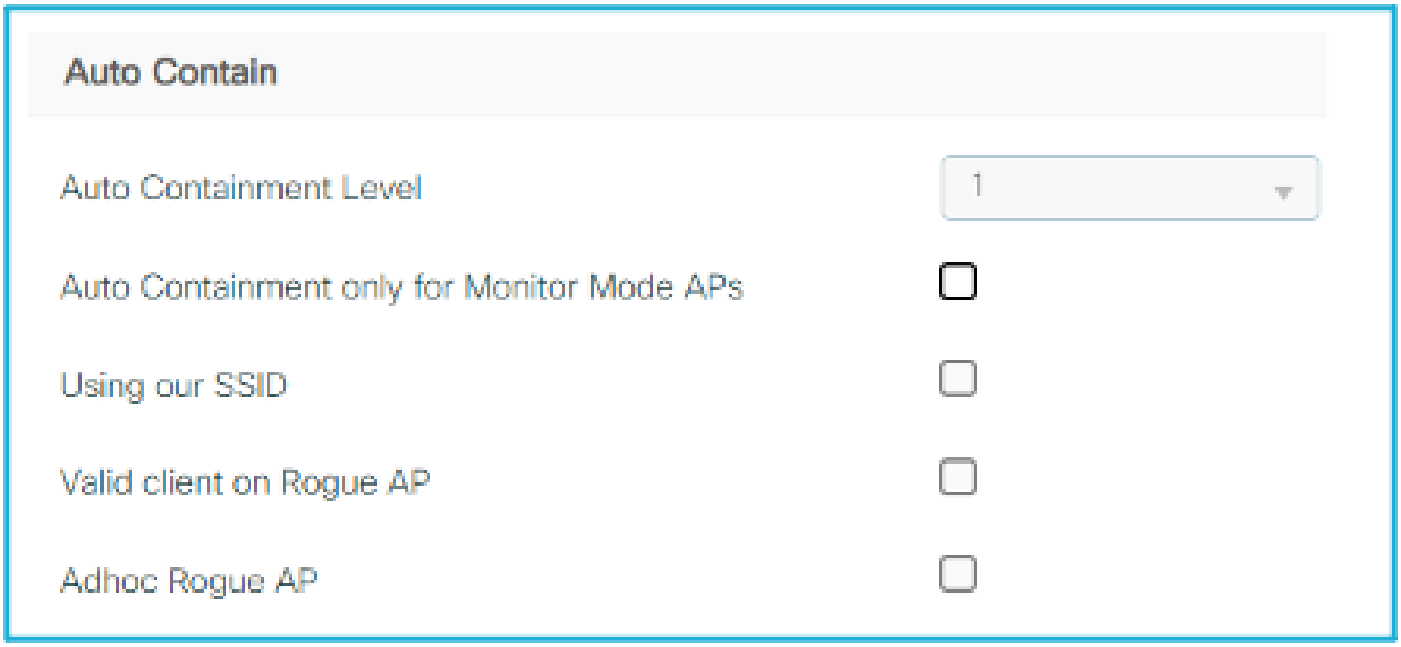


Hinweis: Mobiltelefone, die einen Wi-Fi-Hotspot gemeinsam nutzen, arbeiten wie traditionelle APs im Infrastrukturmodus. Der Ad-hoc-Modus bezieht sich auf eine direkte Verbindung zwischen Mobilgeräten und ist seltener erforderlich.

Das Eindämmen von nicht autorisierten Inhalten ist in vielen Fällen gesetzlich verboten. Daher ist es wichtig, dass Sie sich vor der Aktivierung an Ihre lokale Behörde wenden. Das Eindämmen eines unberechtigten Benutzers bedeutet nicht, den unberechtigten Benutzer aus der Ferne abzuschalten, sondern die Clients, die versuchen, eine Verbindung zum unberechtigten Access Point herzustellen, mit Deauthentifizierungs-Frames zu spammen, damit sie keine Verbindung herstellen. Dies funktioniert nur mit Legacy-Sicherheits-SSID (funktioniert nicht in WPA3 oder wenn PMF in WPA2 aktiviert ist), da Ihre Access Points die Deauthentifizierungsframes nicht richtig signieren können. Diese Beschränkung hat negative Auswirkungen auf die Funkleistung des Zielkanals, da die APs die Sendezeit mit Frames zur Deauthentifizierung füllen. Sie darf daher nur als Sicherheitsmaßnahme angesehen werden, um zu verhindern, dass Ihre legitimen Kunden versehentlich eine Verbindung zu einem nicht autorisierten Access Point herstellen. Aus allen genannten Gründen wird empfohlen, keine Eingrenzung vorzunehmen, da das Problem nicht autorisierter Access Points nicht vollständig gelöst wird und weitere Funkprobleme auftreten.

Wenn Sie Containment verwenden müssen, ist es nur sinnvoll, es für Schurken zu aktivieren, die einen Ihrer verwalteten SSID manipulieren, da es sich um einen offensichtlichen Honeypot-Angriff handelt.

Sie können entweder die automatische Eindämmung mit der Option "using our SSIDs" (Verwenden unserer SSIDs) konfigurieren:



Einstellungen zum automatischen Einfügen

Sie können auch Regeln für nicht autorisierte Access Points konfigurieren, um diese gemäß Ihren eigenen Kriterien als schädliche nicht autorisierte Access Points zu klassifizieren. Vergessen Sie nicht, den Namen Ihrer benachbarten und genehmigten SSIDs als unberechtigte Personen einzugeben, um diese aus Ihrer Alarmliste zu entfernen.

Aktivieren Sie die AP-Authentifizierung oder PMF, um Ihre APs vor Identitätswechsel zu schützen.

Ein nicht autorisierter Access Point ist mit Ihrem kabelgebundenen Netzwerk verbunden, was natürlich ein erhöhtes Sicherheitsrisiko darstellt. Die Erkennung von nicht autorisierten kabelgebundenen Geräten ist komplizierter, da sich die Ethernet-MAC-Adresse eines nicht autorisierten Geräts normalerweise von der seiner Funk-MAC-Adresse unterscheidet. Cisco Catalyst Center verfügt über Algorithmen, die weiterhin versuchen zu erkennen, ob ein unberechtigtes Gerät verkabelt ist, und nach unberechtigten Client-MACs suchen, die sowohl drahtlos als auch über die kabelgebundene Infrastruktur abgerufen werden können. Die beste Lösung, um unberechtigte kabelgebundene Zugriffe vollständig zu verhindern, ist die Sicherung aller Switch-Ports mit 802.1X-Authentifizierung.

Wenn Sie einen nicht autorisierten Access Point physisch überwachen möchten, ist die Nutzung von Cisco Spaces entscheidend für die Lokalisierung der nicht autorisierten Access Points. Wahrscheinlich müssen Sie noch einmal vor Ort suchen, da die Leute dazu neigen, unberechtigte APs manchmal zu verstecken, aber die Reduzierung des Suchbereichs auf ein paar Meter macht es ein sehr praktikables Unterfangen. Ohne Leerzeichen wird das unberechtigte Gerät auf der Karte neben dem AP angezeigt, der es am lautesten erkennt, was einen ziemlich großen

Suchbereich ergibt. Es gibt zahlreiche Wireless-Tools und -Geräte, die Ihnen das Signal des unautorisierten Access Points in Echtzeit anzeigen und Ihnen helfen, den unautorisierten Access Point physisch zu lokalisieren.

Nicht unbedingt verwandt mit unberechtigten Geräten, aber da CleanAir gerade behandelt wurde, ist es wichtig zu beachten, dass die Aktivierung von CleanAir keine nennenswerten negativen Auswirkungen auf die Leistung hat, mit Ausnahme der BLE-Beacon-Erkennung, da sich dies auf die 2,4-GHz-Leistung auswirkt. Sie können Ihr Wireless-Netzwerk so konfigurieren, dass Bluetooth-Störungsquellen vollständig ignoriert werden, da sie in der heutigen Welt allgegenwärtig sind. Außerdem können Sie Ihre Clients nicht daran hindern, ihre Bluetooth-Geräte zu aktivieren.

WiPS

WiPS deckt mehr Angriffsvektoren ab als nur die Erkennung nicht autorisierter Geräte. Zusätzlich zu diesen Angriffen bietet es manchmal auch eine PCAP des Ereignisses für die Forensische Analyse.

Dies ist zwar eine sehr nützliche Sicherheitsfunktion für Unternehmen, aber ein öffentlich zugängliches Netzwerk muss sich der ewigen Frage stellen: Was kann dagegen unternommen werden?

Da Sie viele Clients, die Sie nicht steuern können, nur schwer verwalten können, ist es möglich, die Alarme in zwei Kategorien aufzuteilen. Wenn Sie feststellen, dass zu viele Alarme von Cisco Catalyst Center ignoriert werden, gilt Folgendes:

- 10001: DoS: Überflutungsalarm für Authentifizierung
- 10002: DoS: Alarm zur Zuordnungsanforderung
- 10003: DoS: Broadcast Probe Flood Alarm
- 10004: DoS: Trennungsflutalarm
- 10005: DoS: Broadcast-Diszuordnungsalarm
- 10006: DoS: Deauthentifizierung Flutalarm
- 10007: DOS: Broadcast De-Authentifizierung Alarm
- 10008: DOS: EAPOL-Abmelde-Alarm
- 10009: CTS-Flutalarm
- 10010: Alarm zur RTS-Zuordnungsanforderung
- 10011: Deauthentifizierung Flood nach Paar
- 10021: Airdrop Session (diese findet in der Regel häufig in jedem Netzwerk statt und zeigt einfach die regulären Peer-to-Peer-Aktivitäten zwischen Apple-Geräten an)
- 10022: Ungültige Zuordnungsanforderung
- 10023: Überschwemmung mit Authentifizierungsfehler nach Signatur
- 10024: Ungültige MAC-OUI nach Signatur
- 10025: Falsche Authentifizierung

Diese Alarme können durch einen fehlerhaft ausgeführten Client verursacht werden. Es ist nicht möglich, einen Denial-of-Service-Angriff automatisch zu verhindern, da Sie im Grunde nicht verhindern können, dass ein fehlerhafter Client die Sendezeit belegt hält. Selbst wenn die Infrastruktur den Client ignoriert, könnte sie das Medium und die Funkzeit für die Übertragung

nutzen und würde damit die Leistung der Clients in ihrem Umfeld beeinträchtigen.

Die anderen Alarme sind so spezifisch, dass sie höchstwahrscheinlich einen tatsächlichen böswilligen Angriff darstellen und aufgrund schlechter Client-Treiber kaum passieren können. Es ist besser, diese Alarme weiterhin zu überwachen:

- 10012: Unscharfe Bake
- 10013: Anfrage für Fuzzed Probe
- 10014: Antwort von Fuzzed Probe
- 10015: PS Umfrage Flood nach Signatur
- 10016: EAPOL Start V1 Flood nach Signatur
- 10017: Wiederzuordnungsanforderung Flood nach Ziel
- 10018: Beacon Flood nach Signatur
- 10019: Testantwort-Flood nach Ziel
- 10020: Blockieren von Überschwemmungen durch Unterschrift
- 10026/10027: RTS und CTS Virtual Carrier Sense Attack

Die Wireless-Infrastruktur kann manchmal Maßnahmen zur Eindämmung ergreifen, z. B. das Auflisten eines Geräts blockieren, aber die einzige echte Maßnahme, um einen solchen Angriff zu beseitigen, besteht darin, das Gerät physisch zu entfernen.

Es wird empfohlen, alle Formen des Client-Ausschlusses zu aktivieren, um durch Interaktion mit fehlerhaften Clients verschwendete Funkzeit zu sparen.

Einschränken des Client-Zugriffs

Es wird empfohlen, die Peer-to-Peer-Blockierung in allen WLANs zu aktivieren (es sei denn, Sie haben eine schwierige Anforderung an die Client-to-Client-Kommunikation - dies muss jedoch sorgfältig erwogen und möglicherweise eingeschränkt werden). Diese Funktion verhindert, dass sich Clients im gleichen WLAN miteinander verbinden. Dies ist keine perfekte Lösung, da Clients in verschiedenen WLANs sich immer noch miteinander in Verbindung setzen können und Clients, die zu unterschiedlichen WLCs in der Mobilitätsgruppe gehören, diese Einschränkung ebenfalls umgehen können. Sie stellt jedoch eine einfache und effiziente erste Sicherheits- und Optimierungsebene dar. Ein weiterer Vorteil dieser Peer-to-Peer-Blockierungsfunktion besteht darin, dass sie auch Client-to-Client-ARP verhindert, sodass Anwendungen andere Geräte im lokalen Netzwerk nicht erkennen können. Ohne Peer-to-Peer-Blockierung könnte die Installation einer einfachen Anwendung auf dem Client alle anderen Clients anzeigen, die mit dem Subnetz verbunden sind, möglicherweise ihre IP-Adresse und Hostnamen.

Darüber hinaus wird empfohlen, sowohl eine IPv4- als auch eine IPv6-ACL (wenn Sie IPv6 in Ihrem Netzwerk verwenden) auf Ihre WLANs anzuwenden, um die Kommunikation zwischen Client und Client zu verhindern. Die Anwendung einer ACL, die die Kommunikation zwischen Client und Client auf WLAN-Ebene blockiert, funktioniert unabhängig davon, ob Sie über Client-SVIs verfügen oder nicht.

Ein weiterer obligatorischer Schritt besteht darin, den Zugriff von Wireless-Clients auf jede Art der Verwaltung des Wireless Controllers zu verhindern.

Beispiel:

```
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
```

Diese ACL kann auf die Verwaltungsschnittstelle SVI angewendet werden:

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

Dies erfolgt auf einem WLC mit den Client-VLANS 131 bis 137, die in der Layer-2-VLAN-Datenbank erstellt wurden, jedoch ohne entsprechende SVIs. Für VLAN 130 existiert nur eine SVI, über die der WLC verwaltet wird. Diese ACL verhindert, dass alle Wireless-Clients Datenverkehr vollständig an die Management- und Kontrollebenen des WLC senden. Vergessen Sie nicht, dass Sie nicht nur SSH oder die Verwaltung der Webbenutzeroberfläche zulassen müssen, da auch eine CAPWAP-Verbindung zu allen APs zulässig sein muss. Aus diesem Grund verfügt diese ACL über eine Standardzugangsberechtigung, blockiert jedoch Wireless-Client-Bereiche, anstatt sich auf eine Standardaktion zum Verweigern aller Aktionen zu verlassen, die die Angabe aller zulässigen AP-Subnetz-Bereiche und Verwaltungsbereiche erfordern würde.

Ebenso können Sie eine weitere ACL erstellen, die alle möglichen Management-Subnetze angibt:

```
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
```

Sie können diese ACL dann für den CLI-Zugriff anwenden:

```
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
```

Dieselbe ACL kann auch für den Web-Administratorzugriff angewendet werden.

Schutz vor Datenverkehrsstürmen

Multicasts und Broadcasts werden von einigen Anwendungen intensiver genutzt als andere. Bei rein kabelgebundenen Netzwerken ist der Schutz vor Broadcast-Stürmen oft die einzige Vorsichtsmaßnahme. Allerdings ist ein Multicast so schmerzhaft wie eine Übertragung, wenn er über das Funknetz gesendet wird, und es ist wichtig zu verstehen, warum. Stellen Sie sich zunächst ein Paket vor, das (per Broadcast oder Multicast) an alle Ihre Wireless-Clients gesendet wird und sich schnell auf viele Ziele summiert. Jeder WAP muss diesen Datenübertragungsblock dann so zuverlässig wie möglich übertragen (obwohl nicht garantiert, dass er zuverlässig ist). Dies wird durch eine obligatorische Datenrate erreicht (manchmal die niedrigste, manchmal konfigurierbare). Für Laien bedeutet dies, dass der Frame mit einer OFDM-Datenrate (802.11a/g) gesendet wird, was eindeutig nicht gut ist.

In einem großen öffentlichen Netzwerk ist es nicht ratsam, zur Wahrung der Funkzeit auf Multicast zu setzen. In einem großen Unternehmensnetzwerk kann es jedoch erforderlich sein, Multicast für eine bestimmte Anwendung zu aktivieren. Sie müssen das Multicast jedoch so weit wie möglich kontrollieren, um die Auswirkungen zu begrenzen. Es empfiehlt sich, die Anwendungsdetails, Multicast IP, zu dokumentieren und sicherzustellen, dass andere Formen von Multicast blockiert werden. Wie bereits erläutert, ist die Aktivierung der Multicast-Weiterleitung für die Aktivierung von IPv6 nicht erforderlich. Die Broadcast-Weiterleitung wird am besten vollständig deaktiviert. Broadcasts werden manchmal von Anwendungen verwendet, um andere Geräte im gleichen Subnetz zu erkennen, was in einem großen Netzwerk eindeutig ein Sicherheitsrisiko darstellt.

Wenn Sie die globale Multicast-Weiterleitung aktivieren, stellen Sie sicher, dass Sie die CAPWAP-Einstellung für Multicast-Multicast-AP verwenden. Wenn diese Option aktiviert ist und der WLC ein Multicast-Paket von der kabelgebundenen Infrastruktur empfängt, sendet er es mit einem einzigen Multicast-Paket an alle interessierten APs und spart so eine Menge Paketduplizierung. Stellen Sie sicher, dass Sie für jeden Ihrer WLCs eine andere CAPWAP-Multicast-IP-Adresse einrichten, da andernfalls die APs Multicast-Datenverkehr von anderen WLCs empfangen, was nicht erwünscht ist.

Wenn sich Ihre APs in anderen Subnetzen von der Wireless-Verwaltungsschnittstelle des WLC befinden (was in einem großen Netzwerk wahrscheinlich ist), müssen Sie Multicast-Routing in Ihrer kabelgebundenen Infrastruktur aktivieren. Mit dem folgenden Befehl können Sie überprüfen, ob alle Ihre APs den Multicast-Datenverkehr richtig empfangen:

```
show ap multicast mom
```

IGMP (für IPv4 Multicast) und MLD (für IPv6) Multicast sollten ebenfalls in allen Fällen aktiviert sein, wenn Sie Multicast verwenden möchten. Sie ermöglichen nur den interessierten Wireless-Clients (und somit nur den APs, die interessierte Clients haben) den Multicast-Datenverkehr. Der WLC leitet die Registrierung an den Multicast-Datenverkehr weiter und sorgt dafür, dass die Registrierung aufrechterhalten wird, wodurch die Clients entlastet werden.

Schlussfolgerung

Große öffentliche Netzwerke sind komplex, jedes einzelne ist einzigartig und hat spezifische Anforderungen und Ergebnisse.

Die Einhaltung der in diesem Dokument enthaltenen Richtlinien ist ein guter Ausgangspunkt, mit dem Sie eine erfolgreiche Bereitstellung erzielen und dabei die häufigsten Probleme vermeiden können. Die Richtlinien stellen jedoch lediglich Richtlinien dar und müssen möglicherweise im Kontext des jeweiligen Veranstaltungsorts ausgelegt oder angepasst werden.

Cisco CX verfügt über Teams von Wireless-Experten, die sich für große Wireless-Bereitstellungen engagieren und über Erfahrung bei zahlreichen Großveranstaltungen, darunter Sportveranstaltungen und Konferenzen, verfügen. Wenden Sie sich für weitere Unterstützung an

Ihr Account Team.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.