Design Guide CX - Draadloos voor grote openbare netwerken

Inhoud

Inleiding

In dit document worden de ontwerp- en configuratierichtlijnen voor grote openbare Wi-Fi-netwerken beschreven.

CX-ontwerphandleiding

CX Design Guides zijn geschreven door specialisten van Cisco Technical Assistance Center (TAC) en Cisco Professional Services (PS) en zijn peer-review door experts binnen Cisco; de gidsen zijn gebaseerd op toonaangevende praktijken van Cisco en op kennis en ervaring die gedurende vele jaren is opgedaan met talloze klantimplementaties. Netwerken die in overeenstemming met de aanbevelingen in dit document zijn ontworpen en geconfigureerd, helpen gemeenschappelijke valkuilen te voorkomen en de netwerkwerking te verbeteren.

Toepassingsgebied en definities

Dit document bevat ontwerp- en configuratierichtlijnen voor grote openbare draadloze netwerken.

Definitie: Grote openbare netwerken - draadloze implementaties, vaak met hoge dichtheid, die netwerkconnectiviteit bieden voor duizenden onbekende en/of onbeheerde clientapparaten.

In dit document wordt er vaak van uitgegaan dat het doelnetwerk diensten verleent aan grote en/of tijdelijke gebeurtenissen. Het past ook statische permanente netwerken voor locaties die veel

gasten ontvangen. Een winkelcentrum of luchthaven heeft bijvoorbeeld overeenkomsten met het Wi-Fi-netwerk van een stadion of concertlocatie - in de zin dat er geen controle is over eindgebruikers, en ze bestaan in het netwerk meestal slechts voor een paar uur, of voor de dag op zijn best.

Draadloze dekking voor grote gebeurtenissen of plaatsen heeft zijn eigen reeks vereisten, die neigt om van onderneming, productie, of zelfs grote onderwijsnetwerken verschillend te zijn. Grote publieke netwerken kunnen duizenden mensen hebben, geconcentreerd in slechts een of enkele gebouwen. Ze kunnen zeer frequente client roaming, constant of tijdens pieken, plus het netwerk moet zo compatibel mogelijk zijn met alles in termen van draadloze client-apparaten, zonder controle over client-apparaat configuratie of beveiliging.

In deze handleiding worden algemene RF-concepten voor high-density en implementatiedetails gepresenteerd. Veel van de radioconcepten in deze handleiding zijn van toepassing op alle netwerken met hoge dichtheid, inclusief Cisco Meraki. De implementatiedetails en -configuraties zijn echter gericht op Catalyst Wireless met de Catalyst 9800 draadloze controller, aangezien dit de meest gebruikelijke oplossing is die momenteel voor grote openbare netwerken wordt geïmplementeerd.

Dit document maakt gebruik van de termen Draadloze controller en Draadloze LAN controller (WLC) door elkaar.

Grote publieke netwerken

Grote openbare netwerken en netwerken van evenementen zijn in veel opzichten uniek. In dit document worden deze belangrijke gebieden belicht en worden richtsnoeren gegeven.

- Grote publieke netwerken zijn intens; er zijn duizenden apparaten in een gereduceerde radiofrequentie (RF) ruimte en significante roaming als mensen rondlopen, sommige gebeurtenissen en locaties kunnen statisch zijn met bandbreedte pieken op zeer specifieke tijden. De infrastructuur moet al deze statusveranderingen zo zorgvuldig mogelijk verwerken voor klanten die het gebied binnenkomen en bewegen.
- De belangrijkste prioriteit is het gemak van onboarding. Een verbonden klant is een vrolijke klant. Dit betekent dat u de clientkoppeling naar het netwerk zo snel mogelijk wilt maken. Een client die niet is verbonden met Wi-Fi scant naar beschikbare toegangspunten die ongewenste RF-energie genereren, wat zich vertaalt in extra stremming en verloren capaciteit via de lucht.
- De RF-implementatie moet zo zorgvuldig mogelijk worden ontworpen. Een goed RF-ontwerp met richtingantennes is een must als er een zeer hoge dichtheid is vereist, of als de locatie grote open ruimtes en/of hoge plafonds heeft.
- Een andere belangrijke ontwerpfactor is de compatibiliteit. Sommige functies zijn standaard in de 802.11-specificatie, terwijl andere functies gepatenteerd zijn en geen van beide problemen opleveren voor klanten. De werkelijkheid is echter anders en er zijn veel slecht geprogrammeerde client drivers die zich misdragen wanneer ze ingewikkelde bakens zien of functies/instellingen die ze niet begrijpen.
- Problemen oplossen is moeilijk vanwege de beperkte schaal en tijd. Als iets niet werkt met een specifieke client, kunt u niet met die eindgebruiker werken om het probleem te

begrijpen. Gebruikers kunnen moeilijk te vinden zijn, maar kunnen ook niet-coöperatief zijn vanwege de tijdelijke aard van hun bezoek aan de locatie.
- Veiligheid is een belangrijke factor. Er is minder controle door de zeer grote hoeveelheid gastbezoekers en een veel groter aanvalsoppervlak.

Externe referenties

Documentnaam	Bron	Location (Locatie)
Beste praktijken voor Cisco Catalyst 9800 Series configuratie	Cisco-software	Verband
Probleemoplossing voor draadloze LAN-controller en CPU	Cisco-software	Verband
Wi-Fi doorvoersnelheid valideren: test- en bewakingsgids	Cisco-software	Verband
Implementatiehandleiding voor Cisco Catalyst CW9166D1 access point	Cisco-software	Verband
Implementatiegids voor Catalyst 9104 Stadionantenne (C-ANT9104)	Cisco-software	Verband
Monitor Catalyst 9800 KPI's (toetsprestatie-indicatoren)	Cisco-software	Verband
Problemen met Catalyst 9800 clientconnectiviteit oplossen - Flow	Cisco-software	Verband
Software voor Cisco Catalyst 9800 Series draadloze controller, configuratiehandleiding (17.12)	Cisco-software	Verband
Wi-Fi 6E: Het volgende grote hoofdstuk in Wi-Fi White Paper	Cisco-software	Verband

Vrijwaring

Dit document biedt aanbevelingen op basis van bepaalde scenario's, veronderstellingen en kennis die is opgedaan tijdens verschillende implementaties. U als lezer bent echter verantwoordelijk voor het bepalen van het netwerkontwerp, de bedrijfsvoering, de naleving van de regelgeving, de beveiliging, de privacy en andere vereisten, inclusief de vraag of u de richtlijnen of aanbevelingen in deze handleiding moet volgen.

Het ontwerpen van het netwerk

RF-overwegingen

Venue types

Deze gids concentreert zich op grote gastnetwerken, typisch open voor het publiek, en met beperkte controle over eind - gebruikers en cliëntapparatenttypes. Dit soort netwerken kan op verschillende locaties worden ingezet en kan tijdelijk of permanent zijn. De primaire use case is meestal het bieden van internettoegang aan bezoekers, hoewel dit zelden de enige use case is.

Typische locaties:

- Stadions en arena’s
- Conferentieplaatsen
- Grote auditoria

Vanuit een RF-standpunt heeft elk van deze locatietypen zijn eigen set nuances. De meeste van deze voorbeelden zijn meestal vaste installaties, afgezien van conferentieplaatsen, aangezien deze permanent kunnen zijn of tijdelijk kunnen worden opgezet voor een specifieke vakbeurs.

Andere locaties:

- cruiseschip
- Luchthaven
- Winkelcentrum / winkelcentrum

Luchthavens en cruiseschepen zijn ook voorbeelden van toepassingen die passen in de categorie van grote openbare netwerken; deze hebben echter specifieke extra overwegingen per geval en maken vaak gebruik van interne omnidirectionele AP's.

Bereikstrategieën

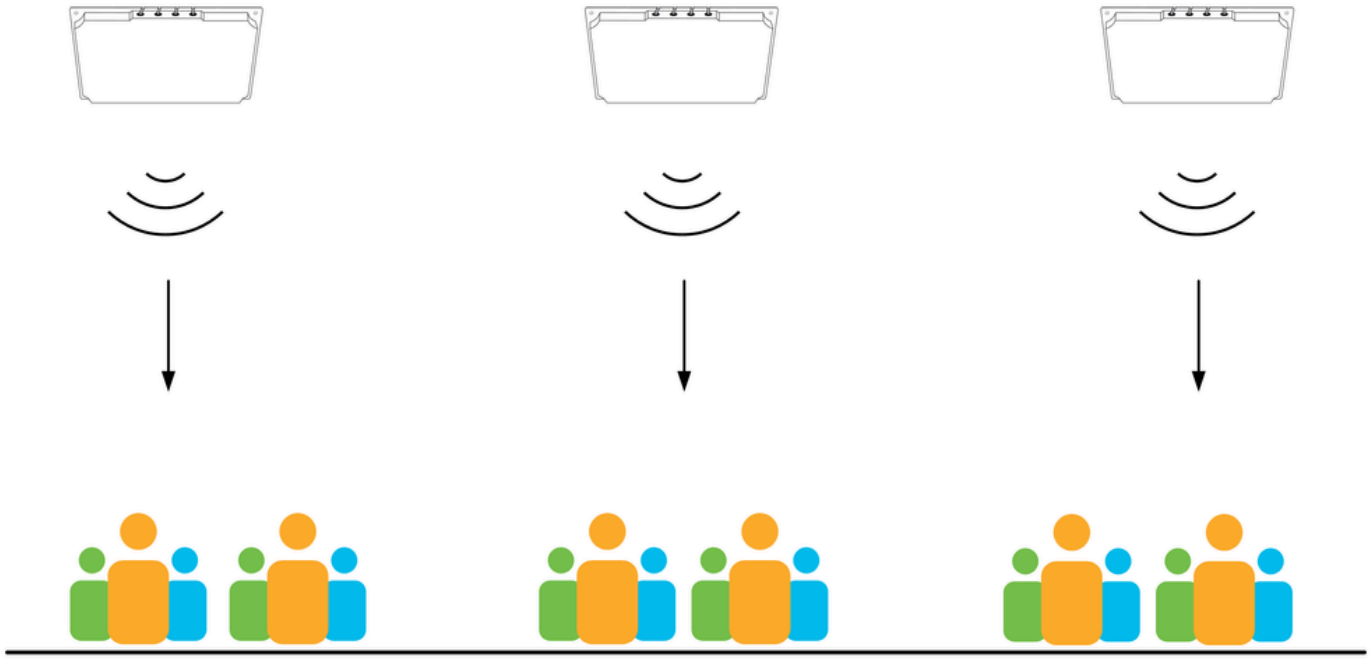
De dekkingsstrategieën hangen grotendeels af van het plaatstype, de gebruikte antennes, en de beschikbare antenne montageplaatsen.

overheadkosten

Overheaddekking wordt altijd waar mogelijk geprefereerd.

Overheadoplossingen hebben het duidelijke voordeel dat alle cliëntapparaten typisch directe lijn van zicht aan de antenneoverheadkosten, zelfs in overvolle scenario's hebben.

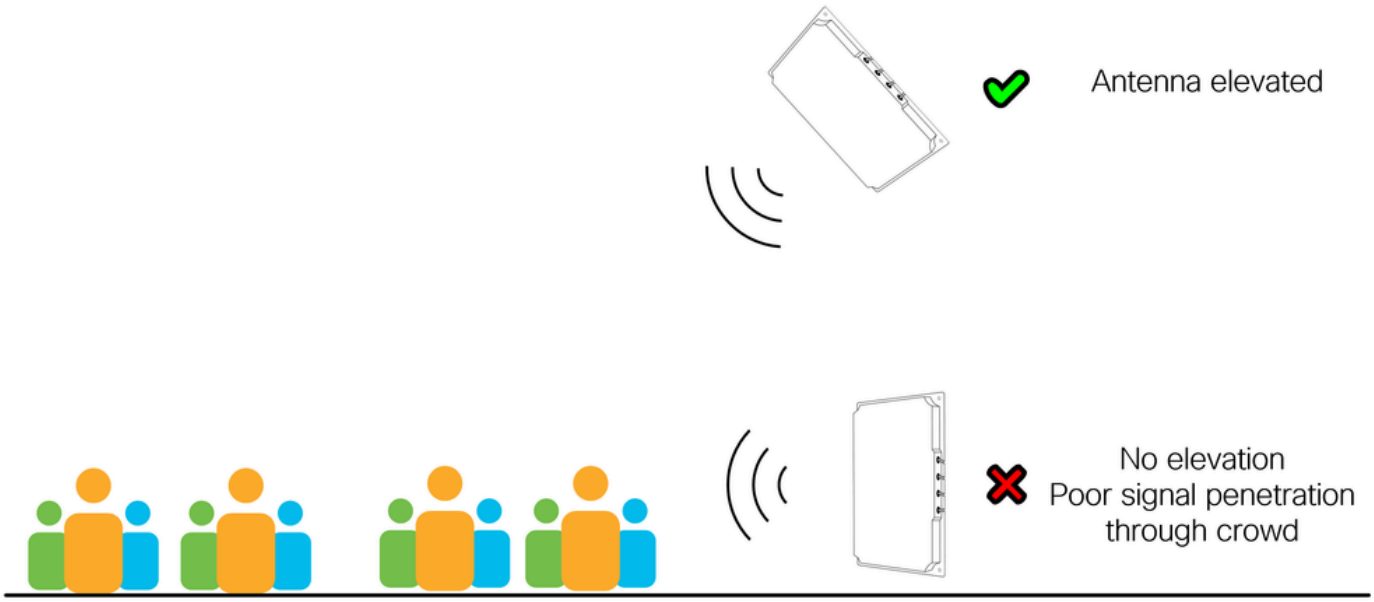
Overheadoplossingen die gebruik maken van directionele antennes bieden een meer gecontroleerd en goed gedefinieerd dekkingsgebied waardoor ze minder gecompliceerd zijn vanuit het oogpunt van radiotuning, terwijl ze superieure taakverdeling en client roaming kenmerken bieden. Zie de sectie over de voedingsbalans voor meer informatie.



AP's boven de clients

Zijde

Zijdelings gemonteerde richtingsantennes zijn een populaire keuze en werken goed in verschillende scenario's, met name wanneer overhead montage niet mogelijk is vanwege hoogte of montagebeperkingen. Wanneer u zijdelingse montage gebruikt, is het belangrijk om te begrijpen welk soort gebied door de antenne wordt bedekt, bijvoorbeeld is het een open buitenruimte of een dicht binnengebied? Als het dekkingsgebied een high-density gebied met veel mensen is, dan moet de antenne zoveel mogelijk worden verhoogd aangezien de signaalpropagatie door een mensenmenigte altijd slecht is. Denk eraan dat de meeste mobiele apparaten worden gebruikt beneden op taille niveau, niet boven het hoofd van de gebruiker! De hoogte van de antenne is minder significant Als het dekkingsgebied een gebied met lagere dichtheid is.



Antennehoogte is altijd beter

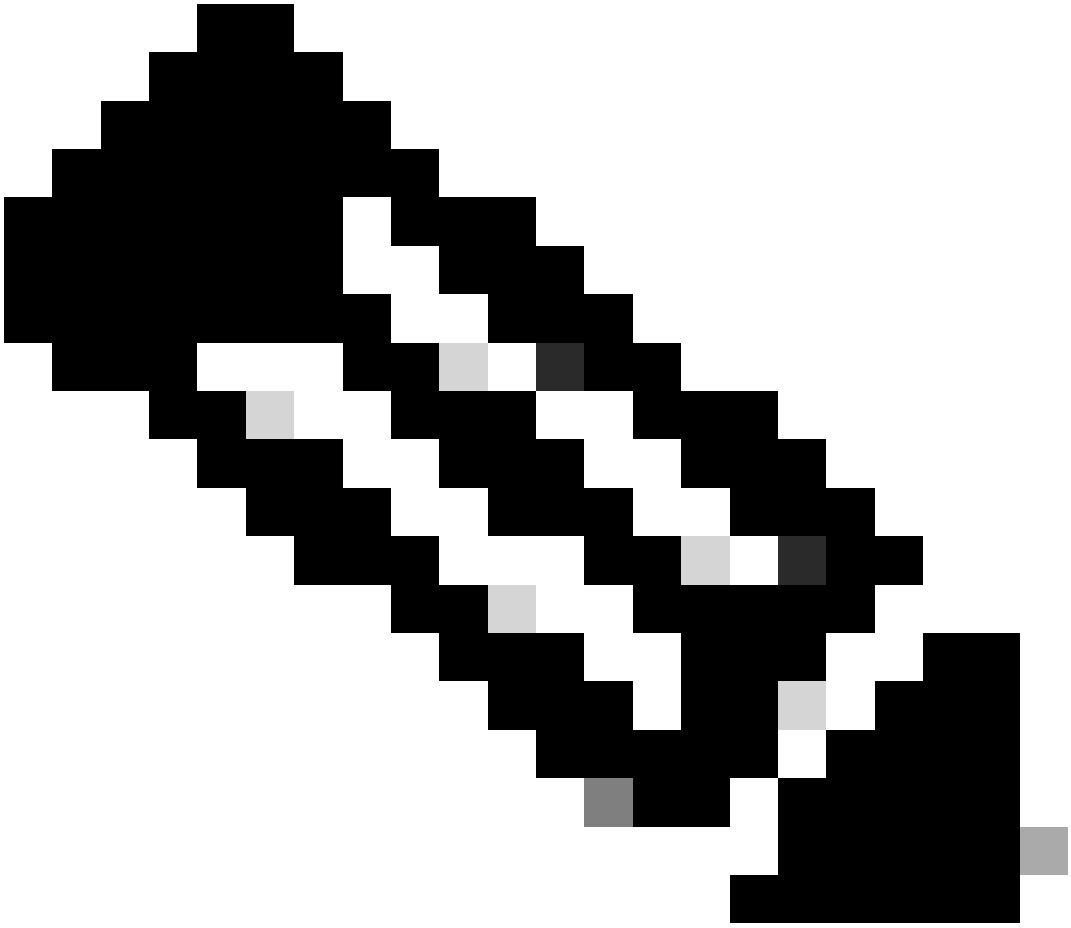
Omnidirectioneel

Het gebruik van omnidirectionele antennes (intern of extern) moet in het algemeen worden vermeden in scenario's met zeer hoge dichtheid, dit vanwege het potentieel hoge impactgebied voor interferentie met andere kanalen. Omnidirectionele antennes mogen niet worden gebruikt op een hoogte boven 6 m (geldt niet voor buiteneenheden met grote versterking).

Onder de stoel

In sommige arena's of stadions kunnen er situaties zijn waarin er geen geschikte antenne-montagelocaties zijn. Het laatste alternatief is om dekking van onderen te bieden door AP's onder de stoelen te plaatsen waar gebruikers zitten. Dit type oplossing is moeilijker correct te implementeren en is doorgaans duurder omdat er aanzienlijk meer AP’s en specifieke installatieprocedures nodig zijn.

De belangrijkste uitdaging met de plaatsing onder de stoelen is het grote verschil in dekking tussen wanneer een volledige plaats en een lege plaats. Een menselijk lichaam is zeer efficiënt in het verzwakken van radiosignaal, wat betekent dat wanneer er een menigte mensen rond de AP is de resulterende dekking beduidend kleiner is in vergelijking met wanneer die mensen er niet zijn. Deze menselijke factor van de menigte het dempen staat voor meer APs toe worden opgesteld die algemene capaciteit kunnen verhogen. Wanneer de locatie leeg is, is er echter geen verzwakking van het menselijk lichaam en is er sprake van significante inmenging, en dit leidt tot complicaties wanneer de locatie gedeeltelijk vol is.



Opmerking: de inzet onder de werkplek is een geldige maar ongebruikelijke oplossing, die per geval moet worden beoordeeld. De inzet onder de werkplek wordt in dit document niet verder besproken.

---

esthetica

In sommige toepassingen speelt de kwestie van esthetiek een rol. Dit kunnen gebieden zijn met specifieke architectonische ontwerpen, historische waarde, of ruimten waar reclame en/of branding dicteert waar apparatuur (of niet) kan worden gemonteerd. Om eventuele plaatsingsbeperkingen te omzeilen, kunnen specifieke oplossingen nodig zijn. Enkele van deze omzeilingen zijn het verbergen van de AP/antenne, het schilderen van de AP/antenne, het monteren van de apparatuur in een behuizing, of gewoon het gebruiken van een andere locatie. Als u de antenne schildert, vervalt de garantie, als u ervoor kiest om de antenne te schilderen altijd gebruik van niet-metalen verf. Cisco verkoopt over het algemeen geen behuizingen voor antennes, maar veel van deze behuizingen zijn eenvoudig beschikbaar via verschillende providers.

Al deze tijdelijke oplossingen zijn van invloed op de prestaties van het netwerk. Draadloze architecten beginnen altijd met het voorstellen van optimale montageposities voor de beste radiodekking, en deze beginposities bieden meestal de beste prestaties. Veranderingen in deze posities leiden vaak tot het verplaatsen van antennes van hun optimale locatie.

Plaatsen waar antennes zijn gemonteerd zijn vaak verhoogd, dit kunnen plafonds, catwalks, dakstructuren, balken, looppaden, en elke locatie die enige hoogte over het beoogde dekkingsgebied voorziet. Deze locaties worden meestal gedeeld met andere installaties, zoals: audio-apparatuur, airconditioning, verlichting en verschillende detectoren / sensoren. Bij wijze van voorbeeld: audio- en verlichtingsapparatuur moet op zeer specifieke locaties worden gemonteerd - maar waarom? Simpel gezegd komt dit doordat audio- en verlichtingsapparatuur niet goed werkt wanneer deze in een doos of achter een muur is verborgen, en iedereen erkent dit.

Hetzelfde geldt voor draadloze antennes, ze werken het beste wanneer er een kijklijn is naar het draadloze clientapparaat. Het stellen van prioriteit aan esthetiek kan (en doet dat zeer vaak) een negatief effect hebben op de draadloze prestaties, waardoor de waarde van de investering in infrastructuur afneemt.

Bedrieglijke netwerken

Wi-Fi-netwerken van schurkennetwerken zijn draadloze netwerken die een gemeenschappelijke RF-ruimte delen, maar niet door dezelfde operator worden beheerd. Deze kunnen tijdelijk of permanent zijn en omvatten infrastructuur apparaten (APs) en persoonlijke apparaten (zoals mobiele telefoons die een Wi-Fi hotspot delen). Bedrieglijke Wi-Fi-netwerken zijn een bron van interferentie en in sommige gevallen ook een beveiligingsrisico. De impact van hengsten op de draadloze prestaties moet niet worden onderschat. Wi-Fi-transmissies zijn beperkt tot een relatief klein radiospectrum dat wordt gedeeld tussen alle Wi-Fi-apparaten, elk apparaat dat zich in de buurt slecht gedraagt kan de netwerkprestaties voor veel gebruikers verstoren.

Binnen de context van grote openbare netwerken worden deze doorgaans zorgvuldig ontworpen en afgestemd met behulp van gespecialiseerde antennes. Een goed RF-ontwerp dekt alleen de gebieden die nodig zijn, vaak met richtantennes, en stemt de zend- en ontvangstkenmerken af voor maximale efficiëntie.

Aan de andere kant van het spectrum bevinden zich apparaten van consumentenkwaliteit of apparaten die door internetproviders worden geleverd. Deze hebben ofwel beperkte opties voor fijnafstelling van RF, of zijn geconfigureerd voor maximaal bereik en waargenomen prestaties, vaak met hoog vermogen, lage gegevenssnelheden en brede kanalen. De introductie van dergelijke apparaten in een netwerk met grote gebeurtenissen kan tot verwoesting leiden.

Wat kan hier aan gedaan worden?

In het geval van persoonlijke hotspots is er heel weinig dat kan worden gedaan, omdat het bijna onmogelijk zou zijn om tienduizenden mensen die een locatie betreden te controleren. In het geval van infrastructuur, of semi-permanente apparaten, zijn er enkele opties. Mogelijke remedies beginnen met eenvoudig onderwijs, met inbegrip van eenvoudige bewustmakingssignalen, via ondertekende documenten over het radiobeleid, en eindigen met actieve handhaving en

spectrumanalyse. In alle gevallen moet een zakelijke beslissing worden genomen over de bescherming van het radiospectrum binnen de betrokken locatie, samen met concrete stappen om die zakelijke beslissing te handhaven.

Het veiligheidsaspect van schurkennetwerken komt in werking wanneer de apparaten die door een derde partij worden gecontroleerd zelfde SSID adverteren zoals het beheerde netwerk. Dit is gelijk aan een honeypot-aanval en kan worden gebruikt als een methode om gebruikersreferenties te stelen. Het wordt altijd aanbevolen om een schurkenregel te creëren om te waarschuwen voor de detectie van infrastructurele SSID's die worden geadverteerd door onbeheerde apparaten. In het gedeelte over beveiliging worden de wegen gedetailleerder besproken.

Enkelvoudig 5 GHz vs. dubbel 5 GHz

Dual 5GHz verwijst naar het gebruik van beide 5GHz-radio's op ondersteunde AP's. Er is een belangrijk verschil tussen dubbele 5GHz met behulp van externe antennes en dubbele 5GHz met behulp van interne antennes (micro/macro cellen op omnidirectionele APs). In het geval van externe antennes is dubbel 5GHz vaak een nuttig mechanisme, dat extra dekking en capaciteit biedt terwijl het totale aantal AP-punten wordt verminderd.

Micro/Macro/Meso

Interne AP's hebben beide antennes dicht bij elkaar (binnen de AP) en er zijn beperkingen met betrekking tot maximum Tx vermogen bij gebruik van dubbele 5GHz. De tweede radio is beperkt tot een laag Tx vermogen (dit wordt afgedwongen door de draadloze controller) wat leidt tot een grote onbalans van Tx vermogen tussen de radio's. Dit kan ertoe leiden dat de primaire radio (met een hoger vermogen) veel klanten aantrekt terwijl de secundaire radio (met een lager vermogen) onderbenut is. In dit geval voegt de tweede radio energie toe aan het milieu zonder de klanten een voordeel te bieden. Als dit scenario wordt geobserveerd, kan het beter zijn om de tweede radio uit te schakelen en simpelweg een andere (enkele 5 GHz) AP toe te voegen als er extra capaciteit nodig is.

Verschillende AP-modellen hebben verschillende configuratieopties, de tweede 5GHz radio kan werken op hogere energieniveaus in nieuwere macro/meso AP's zoals de 9130 en 9136, en sommige interne Wi-Fi 6E AP's zoals de 9160 reeks kunnen zelfs functioneren in macro/macro in sommige gevallen. Controleer altijd de mogelijkheden van uw exacte AP-model. De tweede 5GHz slot is ook beperkt in kanaalgebruik, wanneer één slot in de ene UNII band werkt, de andere slot is beperkt tot een andere UNII band, die invloed heeft op kanaalplanning en vervolgens ook beschikbaar verzendenergie. Altijd rekening houden met het Tx-energieverschil tussen dubbele 5GHz-radio's, dit is waar in alle gevallen, inclusief interne AP's.

FRA

Flexible Radio Assignment (FRA) werd geïntroduceerd als een technologie om de dekking van 5 GHz te verbeteren door extra 2,4 GHz-radio's over te schakelen naar 5 GHz-modus, of potentieel ongebruikte 5 GHz-radio's naar monitormodus (voor AP's die deze ondersteunen). Aangezien dit document grote openbare netwerken bestrijkt, wordt ervan uitgegaan dat zowel de dekkingsgebieden als het radioontwerp goed gedefinieerd zijn door het gebruik van

richtingantennes, en daarom heeft een deterministische configuratie de voorkeur boven een dynamische. Het gebruik van FRA wordt niet aanbevolen voor grote openbare netwerken.

Naar keuze kan FRA worden gebruikt wanneer het netwerk is ingesteld om te helpen bepalen welke radio's naar 5GHz moeten worden geconverteerd, maar zodra u tevreden bent met het resultaat, is het raadzaam om FRA te bevriezen.

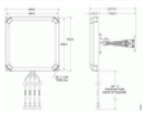
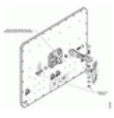
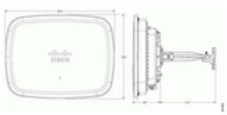
Regelgevend

Elk regulerend domein bepaalt welke kanalen beschikbaar zijn voor gebruik en hun maximale vermogensniveaus, er zijn ook beperkingen op welke kanalen binnen versus buiten kunnen worden gebruikt. Afhankelijk van het regelgevingsdomein kan het soms niet mogelijk zijn om een dubbele 5GHz-oplossing effectief te gebruiken. Een voorbeeld hiervan is het ETSI-domein waar 30dBm is toegestaan op UNII-2e kanalen, maar slechts 23dBm op UNII1/2. In dit voorbeeld, als het ontwerp het gebruik van 30dBm vereist (gewoonlijk wegens hogere afstand aan de antenne) kan het gebruik van één enkele radio 5GHz de enige haalbare oplossing zijn.

Antennes

Grote publieke netwerken kunnen elk type antenne gebruiken en kiezen doorgaans de meest geschikte antenne voor de taak. Het mengen van antennes binnen hetzelfde dekkingsgebied maakt het proces van het radioontwerp lastiger en moet indien mogelijk worden vermeden. Grote publieke netwerken hebben echter vaak grote dekkingsgebieden met verschillende montageopties, zelfs binnen hetzelfde gebied, wat het in sommige gevallen noodzakelijk maakt om antennes te combineren. Omnidirectionele antennes zijn goed begrepen en functioneren hetzelfde als alle andere antennes, deze gids bespreekt externe directionele antennes.

Deze tabel geeft de meest gebruikte externe antennes.

	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°

Antennallijst

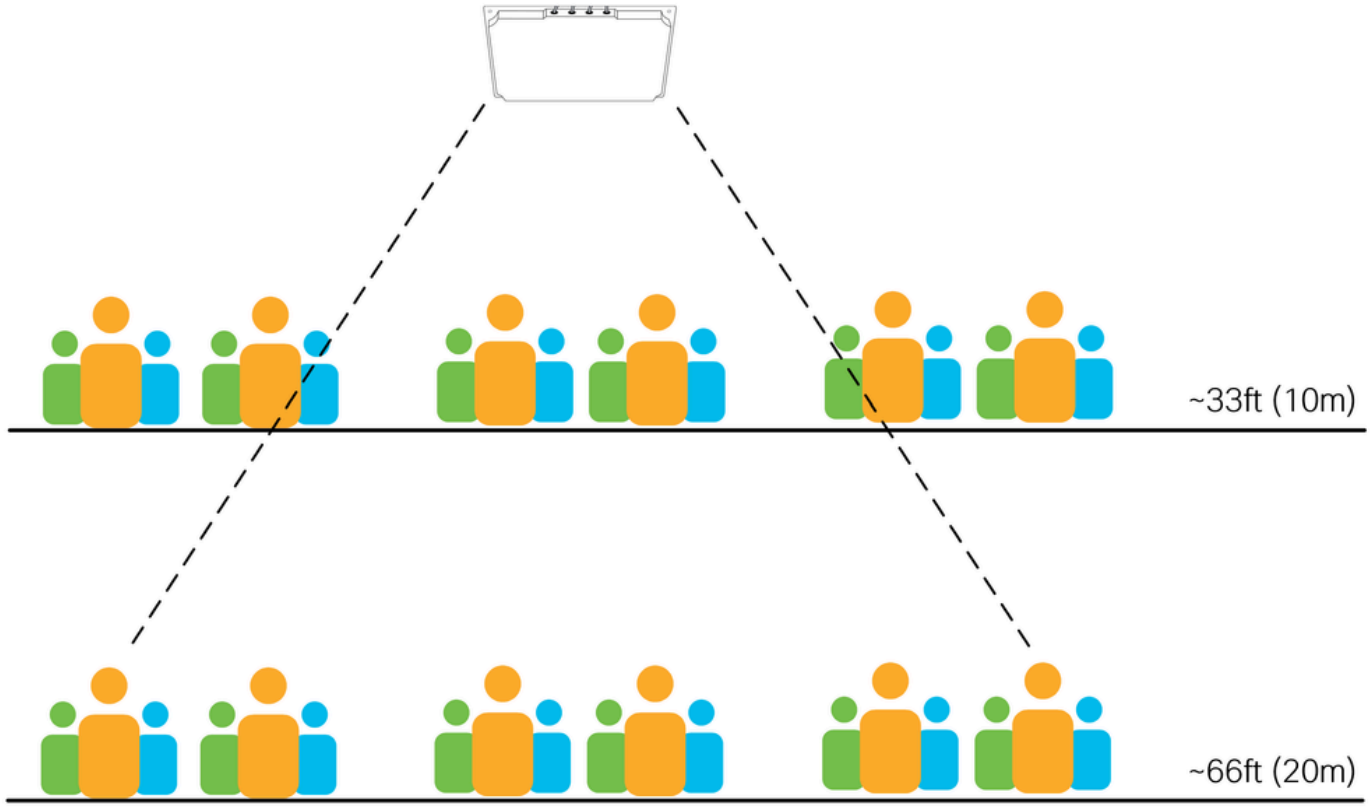
Belangrijkste factoren die bij het kiezen van een antenne in aanmerking moeten worden genomen

zijn de bundeldoorsnede van de antenne en de afstand/hoogte waarop de antenne is gemonteerd. De tabel toont de bundeldoorsnede van 5 GHz voor elk van de antennes, waarbij de cijfers tussen haakjes afgeronde (en makkelijker te onthouden) waarden tonen.

De voorgestelde afstanden in de tabel zijn geen harde regels, alleen richtlijnen gebaseerd op ervaring. Radiogolven reizen met de lichtsnelheid en stoppen niet simpelweg nadat ze een willekeurige afstand hebben bereikt. De antennes werken allemaal buiten de voorgestelde afstand, maar de prestaties dalen naarmate de afstand toeneemt. De hoogte van de installatie is de belangrijkste factor tijdens de planning.

In het onderstaande schema zijn twee mogelijke montagehoogten voor dezelfde antenne te zien op ~33ft (10m) en ~ 66ft (20m) in een gebied met hoge dichtheid. Merk op dat het aantal clients dat de antenne kan zien (en accepteren verbindingen van) toeneemt met de afstand. Kleinere celgrootte behouden wordt moeilijker bij grotere afstanden.

De algemene regel is hoe hoger de dichtheid van de gebruikers, hoe belangrijker het is om de juiste antenne voor de gegeven afstand te gebruiken.



Een stadionantenne

De C9104 stadionantenne is zeer geschikt voor het behandelen van high-density gebieden bij hoge afstanden, zie Catalyst 9104 Stadionantenne (C-ANT9104) de Gids van de Plaatsing voor van informatie.

Veranderingen in de tijd

Veranderingen in de fysieke omgeving in de tijd zijn gebruikelijk in bijna alle draadloze installaties (bijvoorbeeld de beweging van binnenmuren). Regelmatige bezoeken ter plaatse en visuele

inspecties zijn altijd aanbevolen. Voor gebeurtenisnetwerken is er de extra complexiteit van de omgang met audio- en verlichtingssystemen, en in veel gevallen ook andere communicatiesystemen (zoals 5G). Al deze systemen worden vaak geïnstalleerd op verhoogde locaties boven de gebruikers, soms resulterend in ruzie voor dezelfde ruimte. Een goede locatie voor een draadloze stadionantenne is vaak ook een goede locatie voor een 5G antenne! Meer nog, als deze systemen na verloop van tijd worden geüpgraded, kunnen ze worden verplaatst naar locaties waar ze uw draadloze systeem belemmeren en/of actief verstoren. Het is belangrijk om de andere installaties te volgen en te communiceren met de teams die ze installeren, om ervoor te zorgen dat alle systemen op geschikte locaties zijn geïnstalleerd zonder dat ze elkaar (fysiek of elektromagnetisch) storen.

Hoge dichtheid en 6 GHz

Bij het schrijven van dit document is er een beperkte selectie van 6GHz geschikte externe antennes. Alleen de CW9166D1 geïntegreerde AP/antenne werkt op 6 GHz. Er zijn gedetailleerde antennemonspecificaties beschikbaar in de Cisco Catalyst CW9166D1 access point implementatiegids. De CW9166D1 biedt een dekking van 6 GHz met een bundelbreedte van 60°x60° en kan effectief worden gebruikt voor elke inzet die voldoet aan de voorwaarden voor dit type antenne. Zo zijn auditorium en magazijnen goede kandidaten voor de inzet van de CW9166D1, omdat de geïntegreerde unit directionele antenne-functionaliteit biedt voor gebruik binnenshuis.

	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

In de context van grote openbare netwerken hebben deze vaak verschillende grote gebieden en vereisen het gebruik van een combinatie van antennes op verschillende hoogten. Het kan een uitdaging zijn om een groot openbaar netwerk van begin tot eind te implementeren met slechts een antenne van 60°x60° vanwege imitaties op afstand. Daarom kan het ook lastig zijn om end-to-end dekking op 6 GHz te bieden door alleen de CW9166D1 te gebruiken voor een groot openbaar netwerk.

Een mogelijke benadering is om gebruik te maken van 5GHz als de primaire dekkingsband, terwijl het gebruik van 6GHz alleen op specifieke gebieden om geschikte clientapparaten te offload naar de schonere 6GHz band. Bij dit soort benadering wordt gebruikgemaakt van antennes van 5 GHz

alleen in grotere gebieden, terwijl de antennes van 6 GHz waar mogelijk en waar extra capaciteit nodig is worden gebruikt.

Neem bijvoorbeeld een grote evenementenhal op een handelsconferentie, de hoofdhal gebruikt stadionantennes om primaire dekking op 5GHz te bieden, de hoogte van de installatie vereist het gebruik van stadionantennes. De CW9166D1 kan niet worden gebruikt in de hoofdhal in dit voorbeeld vanwege afstandbeperkingen - maar kan effectief worden gebruikt in een aangrenzende VIP-hal of persgebied waar hogere dichtheid is vereist. Clientroaming tussen 5 GHz en 6 GHz banden wordt later in dit document besproken.

Regelgevend

Net als bij 5GHz verschillen de beschikbare stroom en kanalen voor 6GHz aanzienlijk van gebied tot gebied. Met name is er een groot verschil in beschikbaar spectrum tussen FCC- en ETSI-domeinen, evenals strikte richtlijnen rond de beschikbare Tx-vermogen voor binnen- en buitengebruik, respectievelijk laag vermogen binnen (LPI) en standaard vermogen (SP). Met 6GHz, extra beperkingen omvatten de grenzen van het cliëntvermogen, het gebruik van externe antennes en antenne ondersteboven kantelen, en (slechts in de V.S. voor nu) de eis ten aanzien van Geautomatiseerde Frequentiecoördinatie (AFC) voor de plaatsingen van SP.

Voor meer informatie over Wi-Fi 6E zie Wi-Fi 6E: The Next Great Chapter in Wi-Fi White Paper.

Beheer van radiobronnen

Radio Resource Management (RRM) is een reeks algoritmen die verantwoordelijk zijn voor de controle van radioactiviteit. Deze gids verwijst naar twee zeer belangrijke algoritmen RRM, namelijk Dynamic Channel Assignment (DCA) en Transmit Power Control (TPC). RRM is een alternatief voor statische kanaal- en stroomconfiguratie.

- DCA draait op een configureerbaar schema (standaard 10 minuten).
- TPC wordt automatisch uitgevoerd (standaard 10 minuten).

Cisco Event Driven RRM (ED-RRM) is een DCA-optie die het mogelijk maakt dat een beslissing over kanaalwijziging wordt genomen buiten het standaard DCA-schema, gewoonlijk in reactie op ernstige RF-omstandigheden. ED-RRM kan een kanaal direct wijzigen als er te veel interferentie wordt gedetecteerd. In lawaaierige en/of instabiele omgevingen die ED-RRM mogelijk maken, vormt dit een risico op buitensporige kanaalwijzigingen, wat een potentieel negatieve impact op clientapparaten is.

Het gebruik van RRM wordt aangemoedigd en over het algemeen de voorkeur boven statische configuratie - echter, met bepaalde voorbehouden en uitzonderingen.

- TPC moet worden beperkt tot een smal bereik van waarden met behulp van de TPC min/max instelling, zoals nodig, en altijd uitgelijnd op RF ontwerp.
    - TPC Channel Aware inschakelen in omgevingen met hoge dichtheid.

- DCA-programma moet worden gewijzigd ten opzichte van de standaardinstelling van 10 minuten.

    - Gebruik de ED-RRM niet in HD omgevingen.
    - Schakel de lading van Cisco AP uit.
    - Omzeilende AP vermijdingsopties zoals vermijd Buitenlandse AP Interferentie kunnen in een onstabiele omgeving resulteren als er vele kwaden zijn. Het is altijd beter om de schurk te verwijderen dan te proberen om er op te reageren.
- RRM beslissingen kunnen worden beïnvloed door AP's/antennes die elkaar niet goed horen, zoals in het geval van richtantennes die van elkaar wegwijzen.
- Sommige antennes (bijvoorbeeld C9104) ondersteunen geen RRM en vereisen altijd een statische configuratie.
- RRM repareert geen slecht RF ontwerp.

In alle gevallen moet het gespecificeerd risicomateriaal worden ingezet met inzicht in het verwachte resultaat en zo worden afgestemd dat het werkt binnen grenzen die geschikt zijn voor de gegeven RF-omgeving. In de volgende delen van dit document wordt nader op deze punten ingegaan.

RF-configuratie

Kanalen

In het algemeen geldt dat hoe meer kanalen, hoe beter. In implementaties met hoge dichtheid kunnen er ordes van grootte meer AP's en radio's worden ingezet dan beschikbare kanalen, wat een grote kanaalhergebruikratio impliceert, en, samen met dat, hogere niveaus van interferentie met andere kanalen. Alle beschikbare kanalen moeten worden gebruikt, en het beperken van de lijst van beschikbare kanalen wordt over het algemeen ontmoedigd.

Er kunnen gevallen zijn waarin een specifiek (en afzonderlijk) draadloos systeem moet coëxisteren in dezelfde fysieke ruimte, en er moeten speciale kanalen aan worden toegewezen, waarbij tegelijkertijd de toegewezen kanalen worden verwijderd uit de DCA-lijst van het primaire systeem. Dit soort kanaaluitsluitingen moet zeer zorgvuldig worden beoordeeld en alleen worden gebruikt wanneer dat nodig is. Een voorbeeld hiervan kan een point-to-point link zijn die in een open gebied grenst aan het primaire netwerk, of een persgebied binnen een stadion. Indien meer dan een of twee kanalen van de DCA-lijst worden uitgesloten, is dit een reden voor een herevaluatie van de voorgestelde oplossing. In sommige gevallen, zoals zeer dichte stadions, kan zelfs het uitsluiten van één enkel kanaal soms geen haalbare optie zijn.

Dynamic Channel Assignment (DCA) kan worden gebruikt met WLC-gebaseerde RRM of AI-verbeterde RRM.

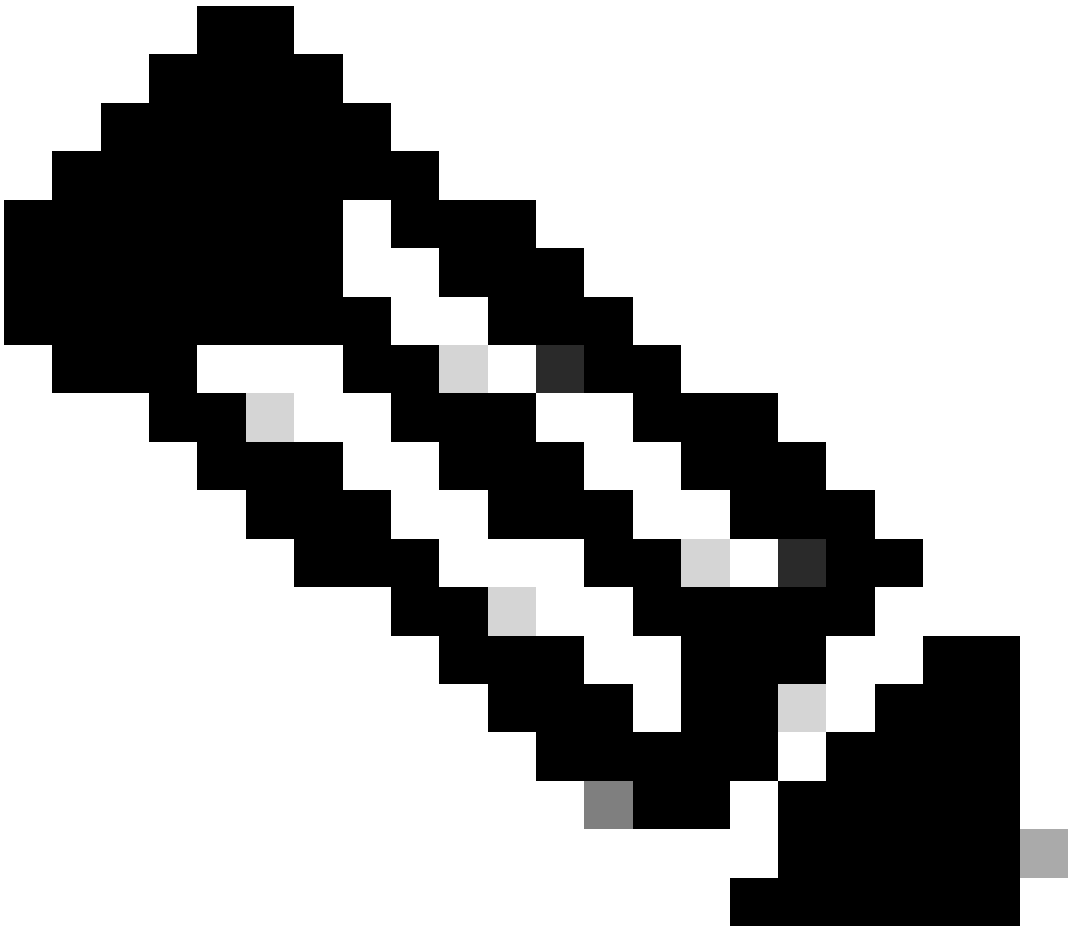
Het standaard DCA-interval is 10 minuten, wat kan resulteren in frequente kanaalwijzigingen in onstabiele RF-omgevingen. De standaard DCA timer moet worden verhoogd van de standaard 10 minuten in alle gevallen, het specifieke DCA interval moet worden afgestemd op de operationele vereisten voor het netwerk in kwestie. Een voorbeeldconfiguratie kan zijn: DCA-interval 4 uur, ankertijd 8. Dit beperkt het aantal kanaalwijzigingen tot één keer in de 4 uur, vanaf 8 uur 's ochtends.

Omdat interferenties onvermijdelijk zullen plaatsvinden, levert aanpassing aan deze interferenties

niet per se waarde op, omdat veel van deze interferenties tijdelijk zijn. Een goede techniek is om automatische DCA voor de eerste uren te gebruiken en het algoritme en kanaalplan te bevriezen wanneer je iets stabiel hebt waar je gelukkig mee bent.

Wanneer de WLC opnieuw wordt opgestart, draait DCA gedurende 100 minuten in agressieve modus om een geschikt kanaalplan te vinden. Het is een goed idee om het proces handmatig opnieuw te starten wanneer er significante wijzigingen in het RF-ontwerp worden aangebracht (bijv. het toevoegen of verwijderen van talrijke AP's of het wijzigen van de kanaalbreedte). Gebruik deze opdracht om dit proces handmatig te starten.

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



Opmerking: kanaalwijzigingen kunnen verstorend zijn voor clientapparaten.

2,4 GHz

De 2.4GHz band is vaak bekritiseerd. Het heeft slechts drie niet-overlappende kanalen en veel andere technologieën behalve Wi-Fi gebruiken het, waardoor ongewenste interferenties ontstaan. Sommige organisaties dringen erop aan dat deze dienst wordt geleverd, dus wat is een redelijke conclusie? Het is een feit dat de 2.4GHz band geen bevredigende ervaring voor eindgebruikers biedt. Erger nog, door te proberen om de dienst op 2.4GHz te verlenen beïnvloedt u andere 2.4GHz technologieën zoals Bluetooth. Bij grote evenementen of evenementen verwachten veel mensen nog steeds dat hun draadloze headset werkt wanneer ze een oproep plaatsen of hun smart wearables blijven werken zoals gewoonlijk. Als uw dichte Wi-Fi werkt op 2,4 GHz, heeft u invloed op die apparaten die niet eens uw 2.4 GHz Wi-Fi gebruiken.

Een ding is zeker, als je echt 2.4GHz Wi-Fi-service moet bieden, is het het beste om dat te doen op een afzonderlijke SSID (wijdt het aan IoT-apparaten of noem het "legacy"). Dit betekent dat dual-band apparaten niet onvrijwillig verbinding maken met 2.4GHz en alleen single-band 2.4GHz apparaten verbinding maken met het.

Cisco adviseert of ondersteunt het gebruik van 40 MHz-kanalen in 2,4 GHz niet.

5 GHz

Typische implementatie voor draadloze apparaten met hoge dichtheid. Gebruik waar mogelijk alle beschikbare kanalen.

Het aantal kanalen varieert afhankelijk van het regelgevingsdomein. Overweeg de impact van radar op de specifieke locatie, gebruik DFS-kanalen (inclusief TDWR-kanalen) waar mogelijk.

20 MHz kanaalbreedte wordt sterk aanbevolen voor alle implementaties met hoge dichtheid.

40MHz kan worden gebruikt op dezelfde basis als 2.4GHz, dat is alleen wanneer (en waar) absoluut nodig.

Evalueer de behoefte en de voordelen in de echte wereld van 40MHz-kanalen in de specifieke omgeving. 40MHz kanalen vereisen een hogere signaal-ruisverhouding (SNR) om een mogelijke verbetering van de doorvoersnelheid te realiseren, als een hogere SNR niet mogelijk is dan 40MHz kanalen dienen geen nuttig doel. Netwerken met hoge dichtheid geven prioriteit aan gemiddelde doorsnede voor alle gebruikers via potentieel hogere doorvoersnelheid voor elke gebruiker. Het is beter om meer AP's op 20MHz-kanalen te plaatsen dan AP's die 40MHz gebruiken omdat het secundaire kanaal alleen wordt gebruikt voor datakaders en daarom veel minder efficiënt wordt gebruikt dan twee verschillende radiocellen, elk werkend op 20MHz (in termen van totale capaciteit, niet in termen van doorvoersnelheid voor één client).

6 GHz

De 6GHz band is nog niet beschikbaar in elk land. Bovendien, sommige apparaten hebben een 6GHz geschikt Wi-Fi adapter maar vereisen een BIOS update voor het om toegelaten te worden voor het specifieke land u het apparaat in werking stelt. De populairste manier waarop klanten op dit moment 6GHz radio's ontdekken is via RNR advertentie op de 5GHz radio. Dit betekent dat 6GHz niet zonder een 5GHz radio op dezelfde AP moet werken. 6GHz is er om te ontladen cliënten en verkeer van de 5GHz radio en typisch een betere ervaring voor de bekwame cliënten

te verstrekken. 6GHz-kanalen maken gebruik van grotere kanaalbandbreedten, maar het hangt sterk af van het aantal kanalen dat beschikbaar is in het regelgevingsdomein. Met 24 6GHz kanalen beschikbaar in Europa, is het niet onredelijk om voor 40MHz kanalen te gaan om betere maximumproductie te verstrekken in vergelijking met de 20MHz u waarschijnlijk in 5GHz gebruikt. In de VS, met bijna het dubbele aantal kanalen, is het gebruik van 40MHz een no-brainer en zelfs het kiezen voor 80MHz is niet onredelijk voor een grote dichtheid gebeurtenis. Grotere bandbreedte mag niet worden gebruikt bij evenementen of locaties met hoge dichtheid.

Gegevenssnelheden

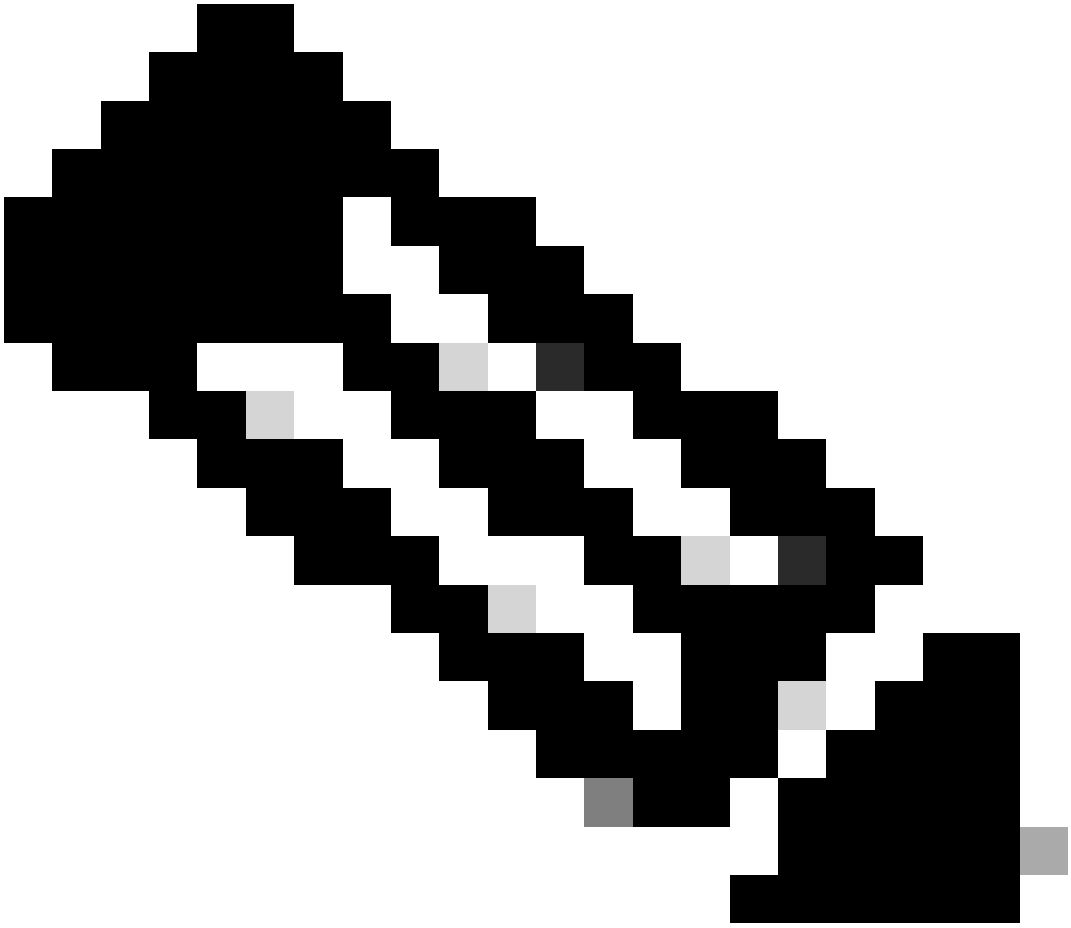
Het gegevenstarief dat een client onderhandelt met een AP is grotendeels een functie van de Signal-to-Noise Ratio (SNR) van die verbinding, en het tegenovergestelde is ook waar, d.w.z. hogere gegevenstarieven vereisen hogere SNR. In feite is het meestal SNR die de maximaal mogelijke linksnelheid bepaalt - maar waarom is dit belangrijk bij het configureren van gegevenssnelheden? Het is omdat sommige gegevenstarieven speciale betekenis hebben.

Classic OFDM (802.11a) gegevenssnelheden kunnen worden geconfigureerd in een van de drie instellingen: Uitgeschakeld, Ondersteund of Verplicht. De OFDM-snelheden zijn (in Mbps): 6, 9, 12, 18, 24, 36, 48, 54. De client en AP moeten beide een snelheid ondersteunen voordat deze kan worden gebruikt.

Ondersteund - het toegangspunt gebruikt de snelheid

Verplicht - AP zal het tarief gebruiken, en zal beheersverkeer verzenden die dit tarief gebruiken

Uitgeschakeld - het toegangspunt zal het tarief niet gebruiken, waardoor de klant gedwongen wordt een ander tarief te gebruiken



Toelichting: Verplichte tarieven worden ook aangeduid als Basistarieven

De betekenis van het verplichte tarief is dat alle beheerskaders worden verzonden met behulp van dit tarief, evenals broadcast- en multicastframes. Als er meerdere verplichte snelheden zijn ingesteld, gebruiken beheerframes de laagste geconfigureerde verplichte snelheid en gebruiken broadcast en multicast de hoogste geconfigureerde verplichte snelheid.

De beheerframes bevatten bakens die door de client moeten worden gehoord om aan het toegangspunt te kunnen worden gekoppeld. Het verhogen van het verplichte tarief verhoogt ook de vereiste SNR voor die transmissie, herinneren eraan dat hogere gegevenstarieven hogere SNR vereisen, en dit betekent typisch dat de cliënt dichter aan AP moet zijn kunnen het baken en de vennoot decoderen. Daarom manipuleren we met het manipuleren van het verplichte datarief ook het effectieve associatiebereik van het toegangspunt, waardoor klanten dichter bij het toegangspunt komen te staan, of naar een mogelijk roamingbesluit. Clients die dicht bij de AP staan gebruiken hogere gegevenssnelheden, en hogere gegevenssnelheden gebruiken minder zendtijd - het beoogde effect is een efficiëntere cel. Het is belangrijk om te onthouden dat het verhogen van de gegevenssnelheid alleen van invloed is op de transmissiesnelheid van bepaalde

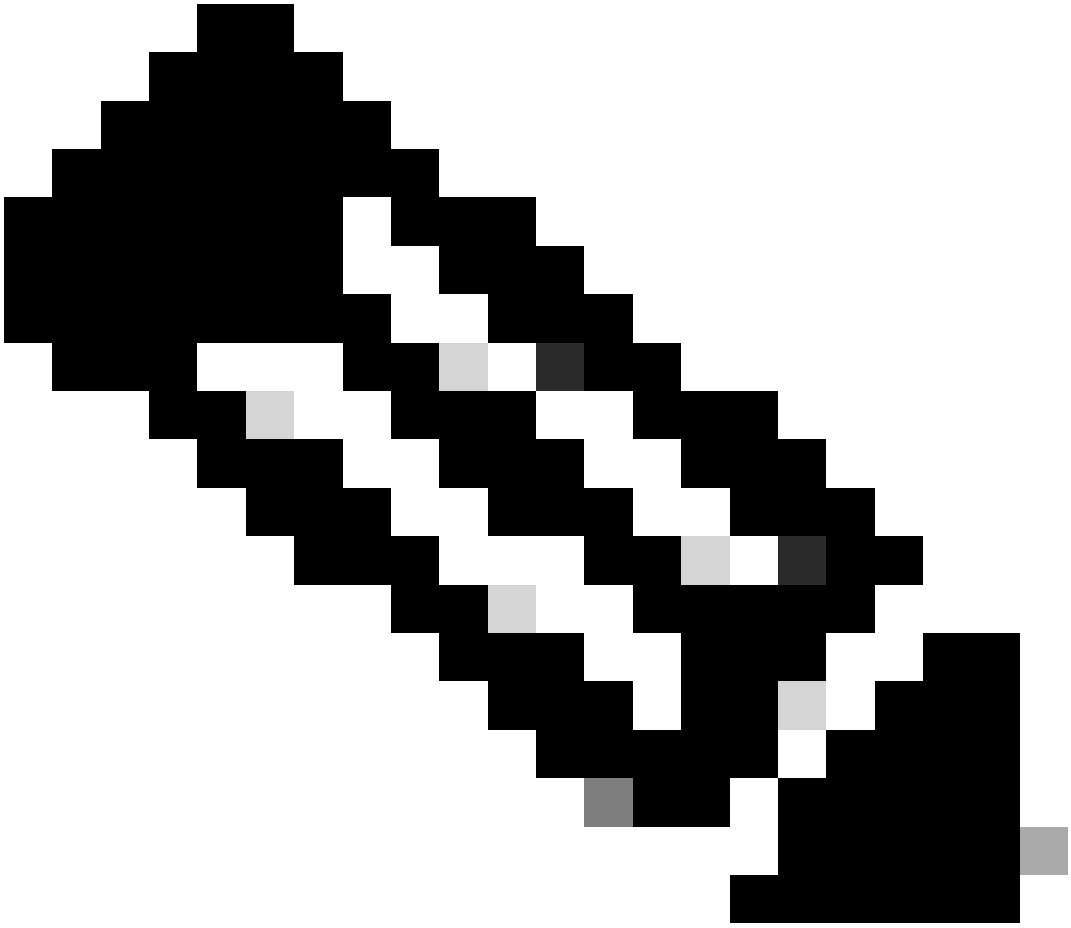
frames, het heeft geen invloed op de RF-propagatie van de antenne of het interferentiebereik. Goede RF-ontwerppraktijken zijn nog steeds nodig om interferentie met andere kanalen en ruis te minimaliseren.

Omgekeerd betekent het verplicht laten van lagere tarieven dat klanten doorgaans in staat zullen zijn om van een veel grotere afstand te associëren, nuttig in lagere AP-dichtheidsscenario's, maar met de mogelijkheid om ravage te veroorzaken met roaming in hogere dichtheidsscenario's. Iedereen die heeft geprobeerd om een schurkenAP die een 6Mbps uitzendt te vinden zal weten dat u de AP zeer ver weg van zijn fysieke plaats kunt ontdekken!

Op het onderwerp van uitzending en multicast, wordt in sommige gevallen een tweede (hoger) verplicht tarief gevormd om het tarief van levering van multicast verkeer te verhogen. Dit is zelden succesvol aangezien multicast nooit wordt erkend en nooit opnieuw wordt overgebracht in geval de kaders worden verloren. Aangezien één of ander verlies in alle draadloze systemen inherent is, is het onvermijdelijk dat sommige multicast kaders ongeacht het gevormde tarief zullen worden verloren. Een betere benadering van betrouwbare multicast levering zijn multicast-to-unicast conversietechnieken die multicast als een unicaststroom overbrengen, dit heeft het voordeel van zowel hogere gegevenssnelheden als betrouwbare (erkende) levering.

Gebruik slechts één verplichte rentevoet, schakel alle tarieven onder de verplichte rentevoet uit en laat alle tarieven boven de verplichte rentevoet zoals ondersteund. Het specifieke tarief om te gebruiken hangt af van het gebruiksgeval, zoals reeds vermeld lagere tarieven zijn nuttig in lagere dichtheid en buitenscenario's waar de afstanden tussen APs groter zijn. Voor netwerken met hoge dichtheid en gebeurtenisnetwerken moeten lage snelheden worden uitgeschakeld.

Als u niet zeker weet waar u moet beginnen, gebruikt u een verplichte snelheid van 12 Mbps voor implementaties met lage dichtheid en van 24 Mbps voor implementaties met hoge dichtheid. Vele grootschalige evenementen, stadions en zelfs bedrijfskantoorimplementaties met hoge dichtheid hebben bewezen betrouwbaar te werken met een verplichte 24 Mbps snelheidsinstelling. Een geschikte test wordt aanbevolen voor specifieke gebruikscategorieën waarbij snelheden van minder dan 12 Mbps of meer dan 24 Mbps vereist zijn.

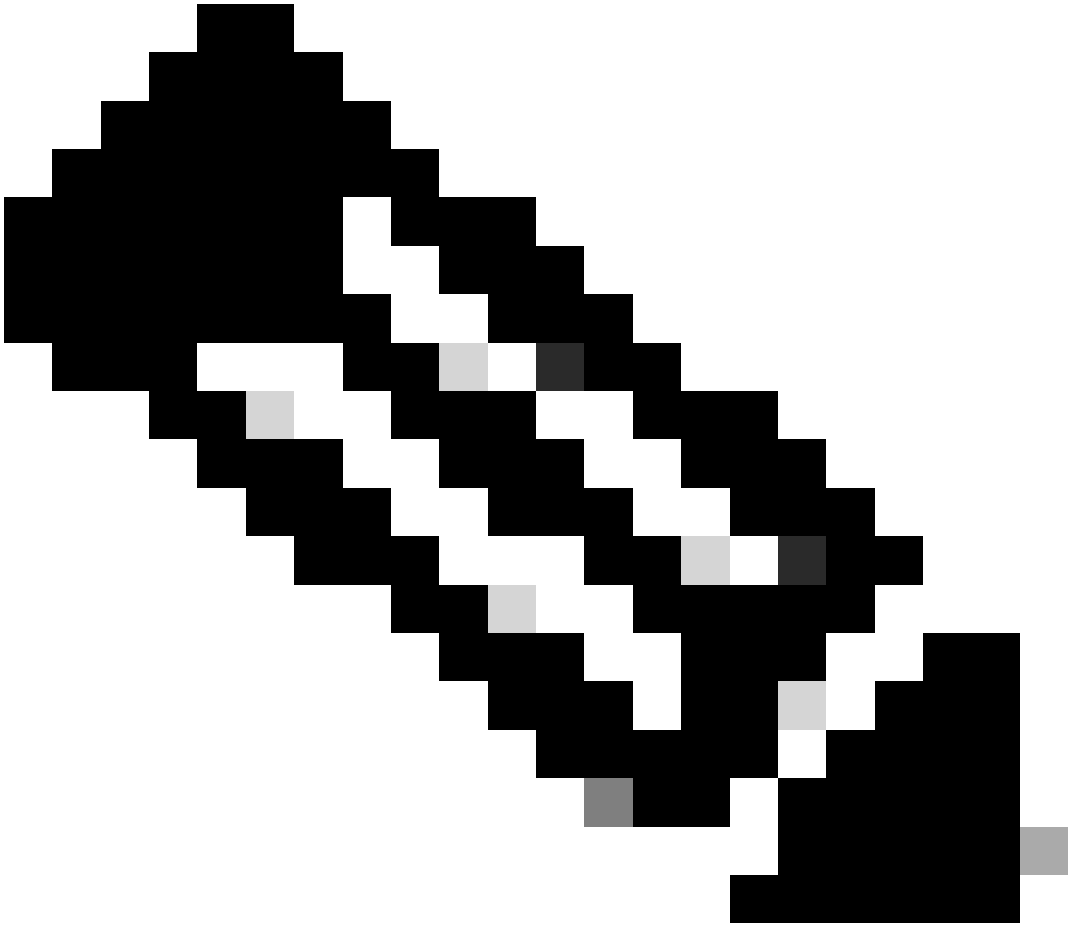


Opmerking: het is het beste om alle 802.11n/ac/ax tarieven ingeschakeld te laten (alle tarieven in de High Throughput sectie van de WLC GUI), er is zelden een noodzaak om een van deze uit te schakelen.

Verzendenergie

De aanbevelingen voor de verzendenergie zijn afhankelijk van het type installatie. Hier onderscheiden we de indooropstelling met omnidirectionele antennes, van die met directionele antennes. Beide soorten antennes kunnen in een groot openbaar netwerk bestaan, hoewel deze doorgaans verschillende soorten gebieden bestrijken.

Voor omnidirectionele implementaties is het gebruikelijk om automatische Transmit Power Control (TPC) te gebruiken met een statisch ingestelde minimumdrempel, en in bepaalde gevallen ook een statisch ingestelde maximumdrempel.



Opmerking: TPC-drempels verwijzen naar het zendvermogen van de radio en sluiten antenneversterking uit. Zorg er altijd voor dat de antenne correct is geconfigureerd voor het gebruikte antennemodel, dit wordt automatisch gedaan bij interne antennes en zelfidentificerende antennes.

Voorbeeld 1

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

Dit zou resulteren in het TPC algoritme die de transmissiemacht automatisch bepalen, maar nooit onder de gevormde minimumdrempel van 5dBm gaan.

Voorbeeld 2

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

Dit zou ertoe leiden dat het TPC-algoritme automatisch de zendkracht bepaalt, maar altijd tussen 2dBm en 11dBm blijft.

Een goede benadering is om verschillende RF-profielen te maken met verschillende drempels, bijvoorbeeld laag vermogen (2-5dBm), gemiddeld vermogen (5-11dbM), en hoog vermogen (11-17dBM), en vervolgens omnidirectionele AP's toe te wijzen aan elk RF-profiel zoals nodig. De waarden van elk RF-profiel kunnen worden aangepast aan het beoogde gebruiksgeval en dekkingsgebied. Hierdoor kunnen de RRM-algoritmen dynamisch werken terwijl ze binnen vooraf gedefinieerde grenzen blijven.

De benadering voor richtingantennes is zeer vergelijkbaar, het enige verschil is het vereiste nauwkeurigheidsniveau. Directionele antenneplaatsing moet worden ontworpen en geverifieerd tijdens een pre-implementatie RF-onderzoek, en de specifieke radioneconfiguratiewaarden zijn typisch een resultaat van dit proces.

Bijvoorbeeld, als een plafondgemonteerde patchantenne vereist is om een bepaald gebied vanaf een hoogte van ~26ft (8m) te bedekken, moet het RF-onderzoek het minimum Tx vermogen bepalen dat vereist is om deze beoogde dekking te bereiken (dit bepaalt de minimum TPC waarde voor het RF-profiel). Op dezelfde manier zouden we uit hetzelfde RF-onderzoek de mogelijke overlap begrijpen die nodig is tussen dit, en de volgende antenne, of zelfs het punt waarop we willen dat de dekking eindigt - dit zou de maximale TPC-waarde voor het RF-profiel.

RF-profielen voor richtantennes worden doorgaans geconfigureerd met dezelfde minimum- en maximumTPC-waarden of een smal bereik van mogelijke waarden (meestal <= 3dBm).

RF-profielen hebben de voorkeur om te zorgen voor een consistente configuratie en statische configuratie van afzonderlijke AP's wordt niet aanbevolen. Het is een goede praktijk om RF-profielen te benoemen op basis van het dekkingsgebied, het antennetype en het gebruiksgeval, bijvoorbeeld RF-Auditorium-Patch-Ceiling.

De juiste hoeveelheid Tx power is wanneer de vereiste SNR waarde wordt bereikt door de zwakste klant in het beoogde dekkingsgebied, en niet meer dan dat. 30dBm is een grote client SNR streefwaarde onder reële omstandigheden (dat wil zeggen, in een locatie vol mensen).

CHD

Coverage Hole Detection (CHD) is een apart algoritme voor het identificeren en herstellen van gaten in de dekking. CHD is wereldwijd en per WLAN geconfigureerd. Een mogelijk effect van CHD is de verhoging van de Tx-kracht om te compenseren voor dekkingsgaten (gebieden met clients die consistent worden gedetecteerd met een slecht signaal), dit effect is op radioniveau en beïnvloedt alle WLAN’s, zelfs wanneer ze worden geactiveerd door één WLAN dat voor CHD is geconfigureerd.

Grote openbare netwerken zijn doorgaans ingesteld op specifieke energieniveaus met behulp van RF-profielen, sommige kunnen zich in open gebieden bevinden met klanten die in en uit de gebieden zwerven, er is geen behoefte aan een algoritme om AP Tx-vermogen dynamisch aan te passen in reactie op deze clientgebeurtenissen.

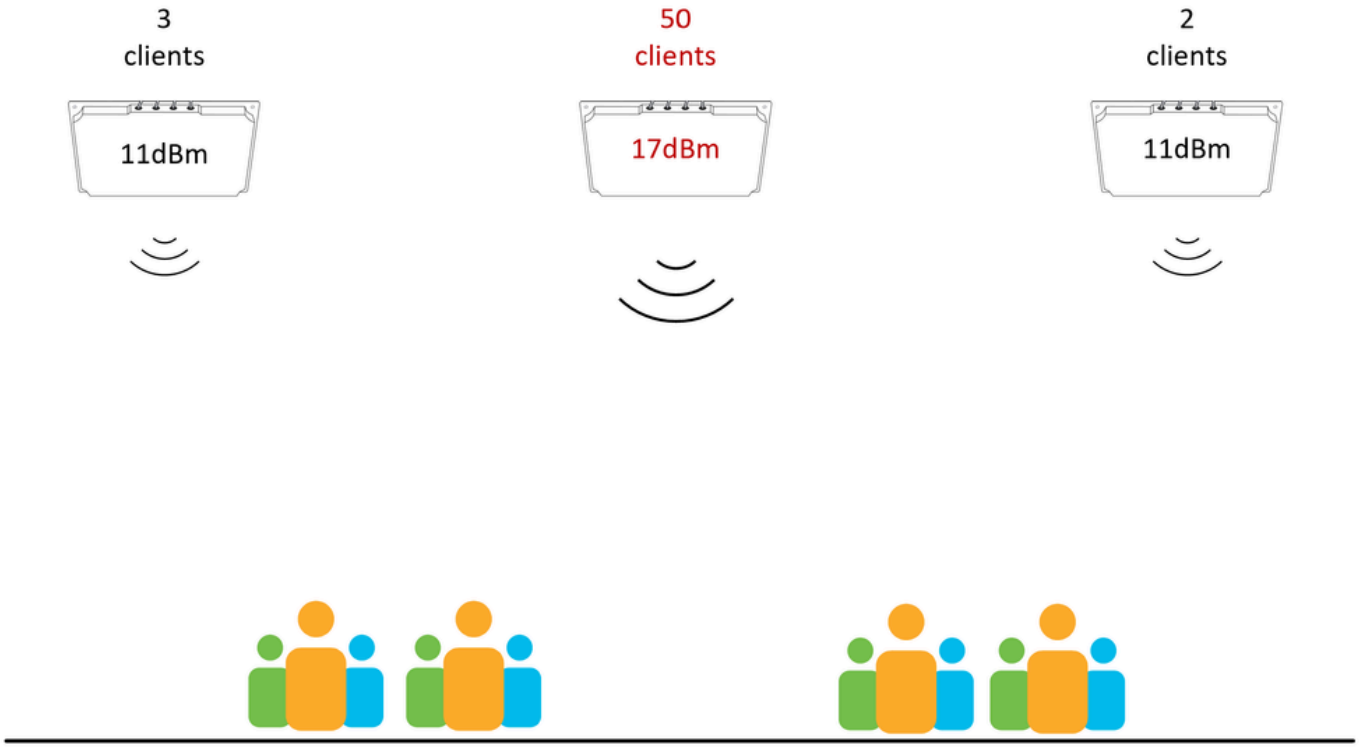
CHD moet wereldwijd worden uitgeschakeld voor grote publieke netwerken.

Voedingsbalans

De meeste cliëntapparaten verkiezen een hoger ontvangen signaal wanneer het kiezen van welke AP om te associëren aan. Situaties waarin een toegangspunt is geconfigureerd met een aanzienlijk hoger Tx-vermogen in vergelijking met andere omliggende toegangspunten moeten worden vermeden. AP's die werken met een hogere belasting vermogen trekken meer clients aan, wat leidt tot een ongelijke clientdistributie tussen AP's (een enkele AP/radio is bijvoorbeeld overbelast met clients, terwijl omliggende AP's onderbenut zijn). Deze situatie komt vaak voor in implementaties met een grote dekking overlap van meerdere antennes, en in gevallen waarin één AP meerdere antennes heeft aangesloten.

Stadionantennes zoals de C9104 vereisen bijzondere zorg wanneer het selecteren van Tx macht aangezien de antennebundels door ontwerp overlappen, te zien gelieve Catalyst 9104 Stadionantenne (C-ANT9104) de Gids van de Plaatsing voor meer informatie over dit.

In het onderstaande schema is de middenantenne ingesteld op een hoger Tx-vermogen dan de omliggende antennes. Deze configuratie zal er waarschijnlijk toe leiden dat clients worden ‘geplakt’ op de middelste antenne.

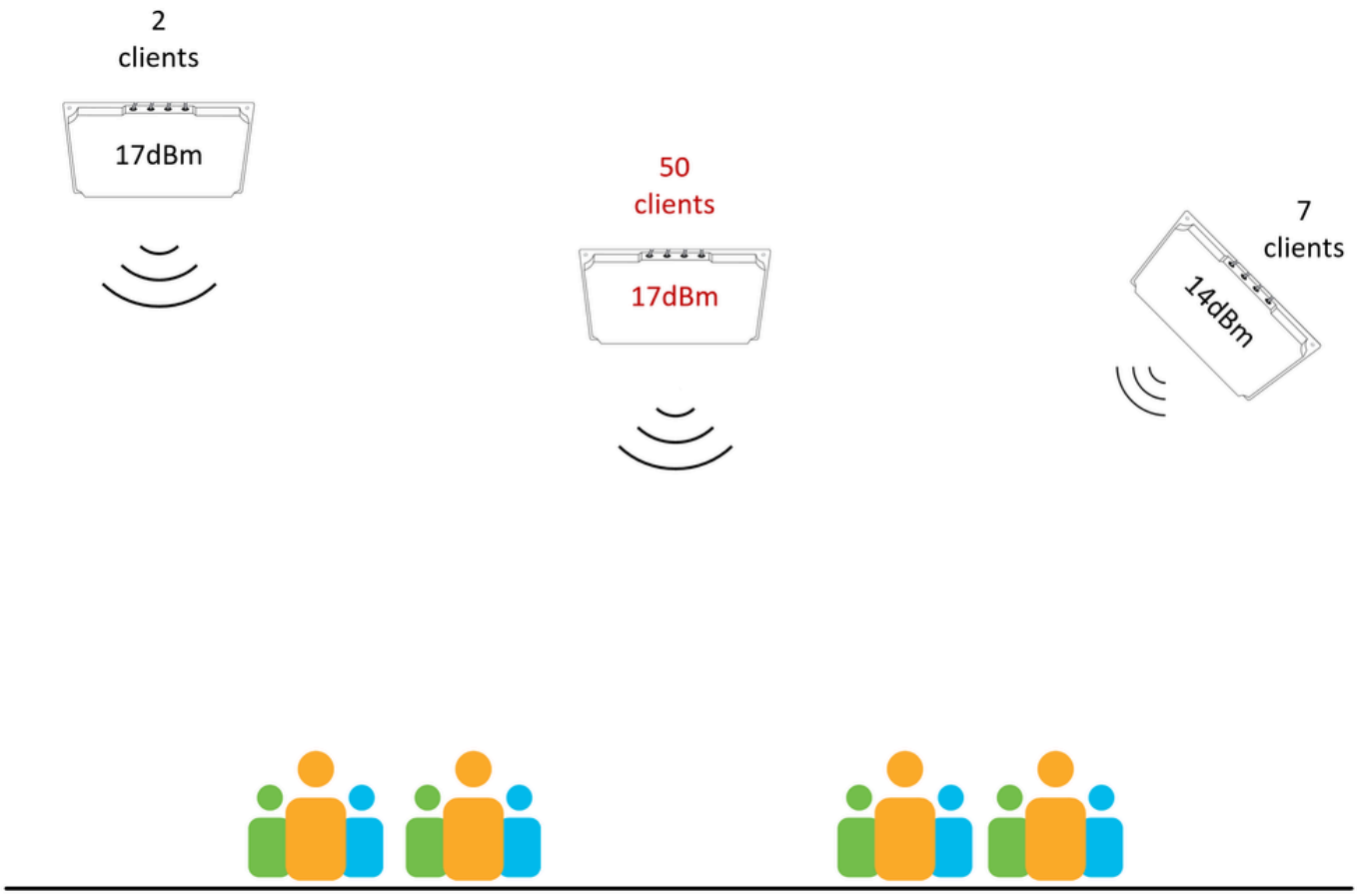


Een AP met een hoger vermogen dan de naburige AP's trekt alle klanten rond aan

Het volgende diagram toont een ingewikkelder situatie, niet alle antennes zijn op dezelfde hoogte, en niet alle antennes gebruiken dezelfde kanteling/oriëntatie. Het bereiken van een gebalanceerde voeding is gecompliceerder dan het configureren van alle radio's met dezelfde Tx-voeding. In scenario's zoals deze kan een post-implementatielocatie onderzoek worden vereist, dit verstrekt een mening van de dekking vanuit het standpunt van het cliëntapparaat (op de grond). De enquêtegegevens kunnen dan worden gebruikt om de configuratie voor de beste dekking en clientdistributie in balans te brengen.

Het ontwerpen van uniforme AP plaatsingsplaatsen die ingewikkelde situaties als dit vermijden is de beste manier om het uitdagen van RF stemmende scenario's (alhoewel er soms geen andere

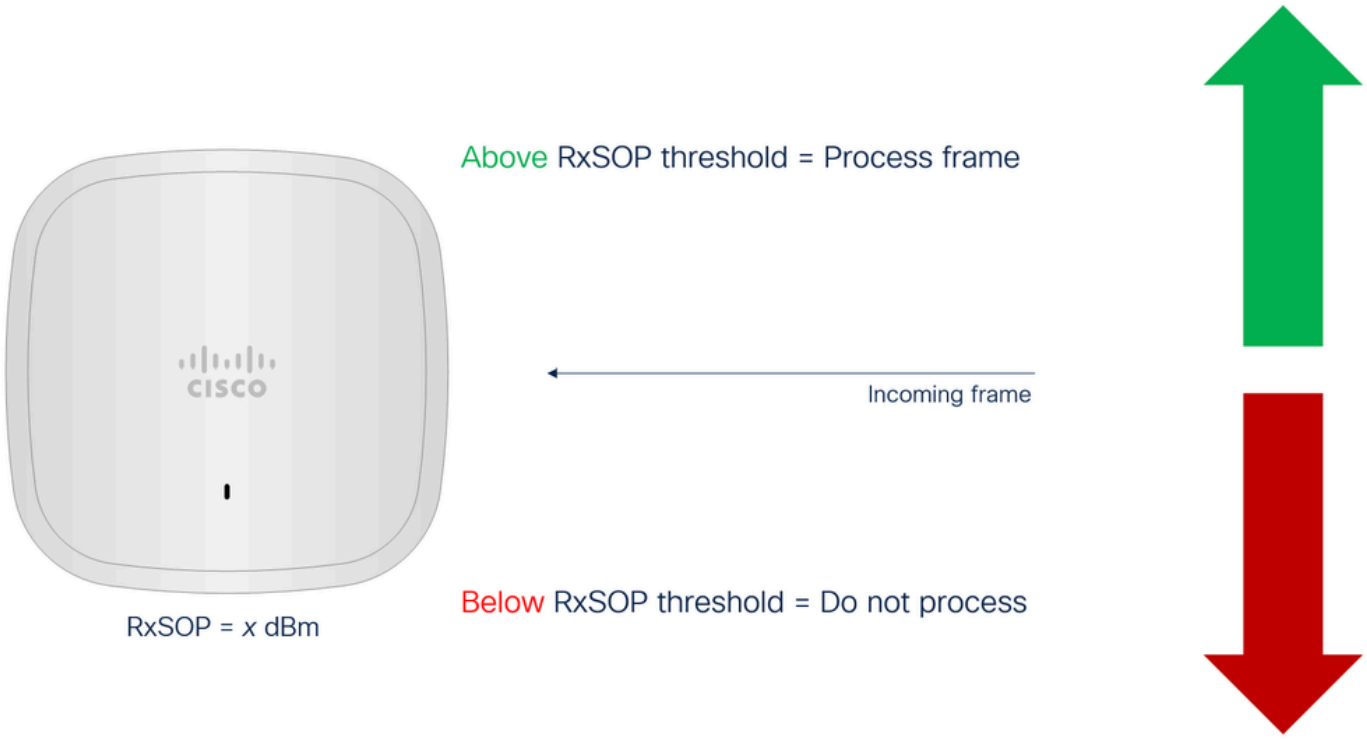
keus is!) te verhinderen.



Eén AP trekt alle klanten aan ondanks dat Tx power gelijk is, maar hoogte en hoeken spelen een rol

RXSOP

In tegenstelling tot mechanismen zoals Tx-vermogen of gegevenssnelheden die de kenmerken van de transmissiecel beïnvloeden, streeft RxSOP (Ontvangerbegin van pakketdetectie) ernaar de grootte van de ontvangstcel te beïnvloeden. In essentie kan RxSOP worden beschouwd als een ruisdrempel, in die zin dat het het ontvangen signaalniveau definieert waaronder de AP geen transmissies probeert te decoderen. Eventuele transmissies met een signaalniveau dat zwakker is dan de ingestelde RxSOP-drempel worden niet verwerkt door het toegangspunt en worden effectief behandeld als ruis.



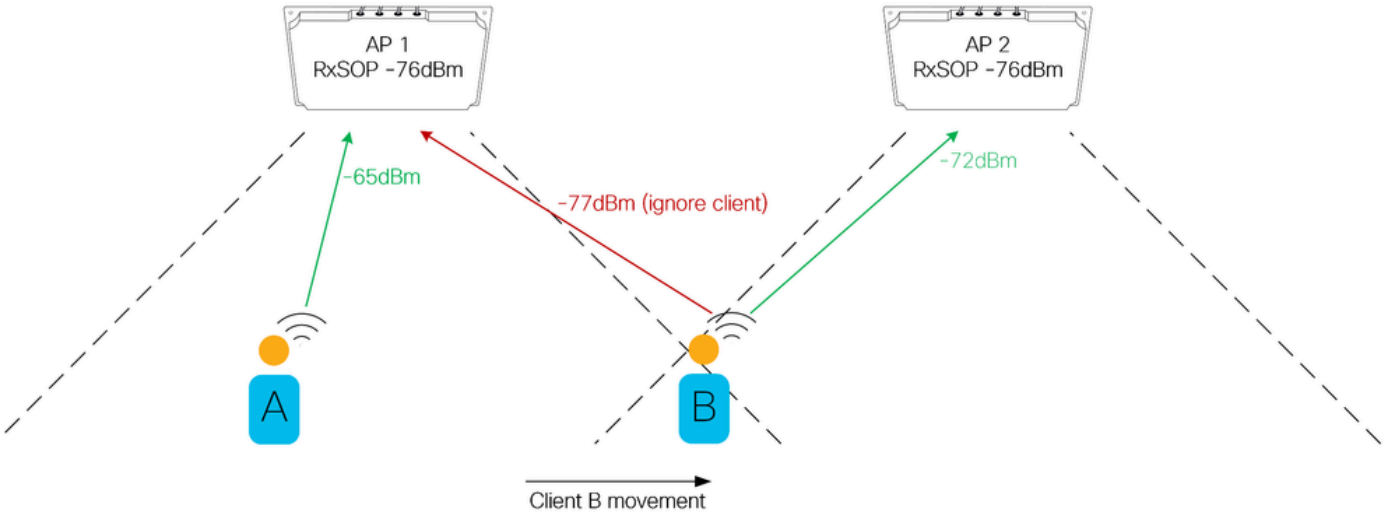
RxSOP concept uitgelegd

Het belang van RxSOP

RxSOP heeft meerdere toepassingen. Het kan worden gebruikt om de APs capaciteit te verbeteren om in lawaaierige milieu's te overbrengen, om de distributie van cliënten tussen antennes te controleren, evenals te optimaliseren voor zwakkere en kleverige cliënten.

In het geval van lawaaierige omgevingen, herinneren eraan dat alvorens een kader 802.11 over te brengen het overbrengende station (in dit geval AP) eerst de beschikbaarheid van het middel moet beoordelen, een deel van dit proces is eerst te luisteren naar transmissies die reeds plaatsvinden. In dichte Wi-Fi-omgevingen is het voor veel AP's heel gewoon om in een relatief beperkte ruimte samen te leven, vaak met dezelfde kanalen. In dergelijke drukke omgevingen kan het toegangspunt het kanaalgebruik van de omliggende toegangspunten (inclusief reflecties) rapporteren en zijn eigen transmissie vertragen. Door de juiste RxSOP-drempel in te stellen, kan het toegangspunt die zwakkere transmissies negeren (vermindering van het waargenomen kanaalgebruik), wat leidt tot frequentere transmissiemogelijkheden en betere prestaties. Omgevingen waar AP's aanzienlijke kanaalbenutting rapporteren (bijvoorbeeld > 10%) zonder enige clientbelasting (bijvoorbeeld een lege locatie) zijn goede kandidaten voor RxSOP-tuning.

Raadpleeg dit diagram voor clientoptimalisatie met RxSOP.



Clientroaming beïnvloed door rxsop

In dit voorbeeld zijn er twee AP's/antennes met goed gedefinieerde dekkingsgebieden. Cliënt B beweegt zich van het dekkingsgebied van AP1 in het dekkingsgebied van AP2. Er is een oversteekplaats waar AP2 de cliënt beter hoort dan AP1, maar de cliënt heeft nog niet aan AP2 geroamd. Dit is een goed voorbeeld van hoe het instellen van de RxSOP-drempel de grens van het dekkingsgebied kan afdwingen. Ervoor zorgen dat clients altijd zijn verbonden met het dichtstbijzijnde toegangspunt verbetert de prestaties door het elimineren van verafgelegen en/of zwakke clientverbindingen die worden aangeboden met lagere gegevenssnelheden. Als u de RxSOP-drempels op deze manier configureert, is een grondig begrip nodig van de plaats waar het verwachte dekkingsgebied van elke AP begint en eindigt.

De gevaren van RxSOP.

Als de RxSOP-drempel te agressief wordt ingesteld, ontstaan er dekkingsgaten, aangezien het toegangspunt geen geldige transmissies van geldige clientapparaten decodeert. Dit kan nadelige gevolgen hebben voor de klant, aangezien AP niet reageert; als de cliënttransmissie niet werd gehoord is er immers geen reden om te reageren. Stemmende RxSOP drempels moeten zorgvuldig worden gedaan, altijd ervoor zorgend de gevormde waarden geen geldige cliënten binnen het dekkingsgebied uitsluiten. Merk op dat sommige clients niet goed kunnen reageren op deze manier worden genegeerd, te agressieve RxSOP-instellingen geven de client geen kans om te zwerven natuurlijk, waardoor de client effectief wordt gedwongen om een andere AP te vinden. Een cliënt die een beacon van AP kan decoderen veronderstelt het aan dat AP kan overbrengen, zo, is de bedoeling van RxSOP het stemmen de grootte van de ontvangstcel aan de bakenwaaier van AP aan te passen. Houd in gedachten dat een (geldig) cliëntapparaat niet altijd een directe lijn van zicht aan AP heeft, wordt het signaal vaak verzwakt door gebruikers die van de antenne onder ogen zien of hun apparaten dragen in zakken of zakken.

RXSOP configureren

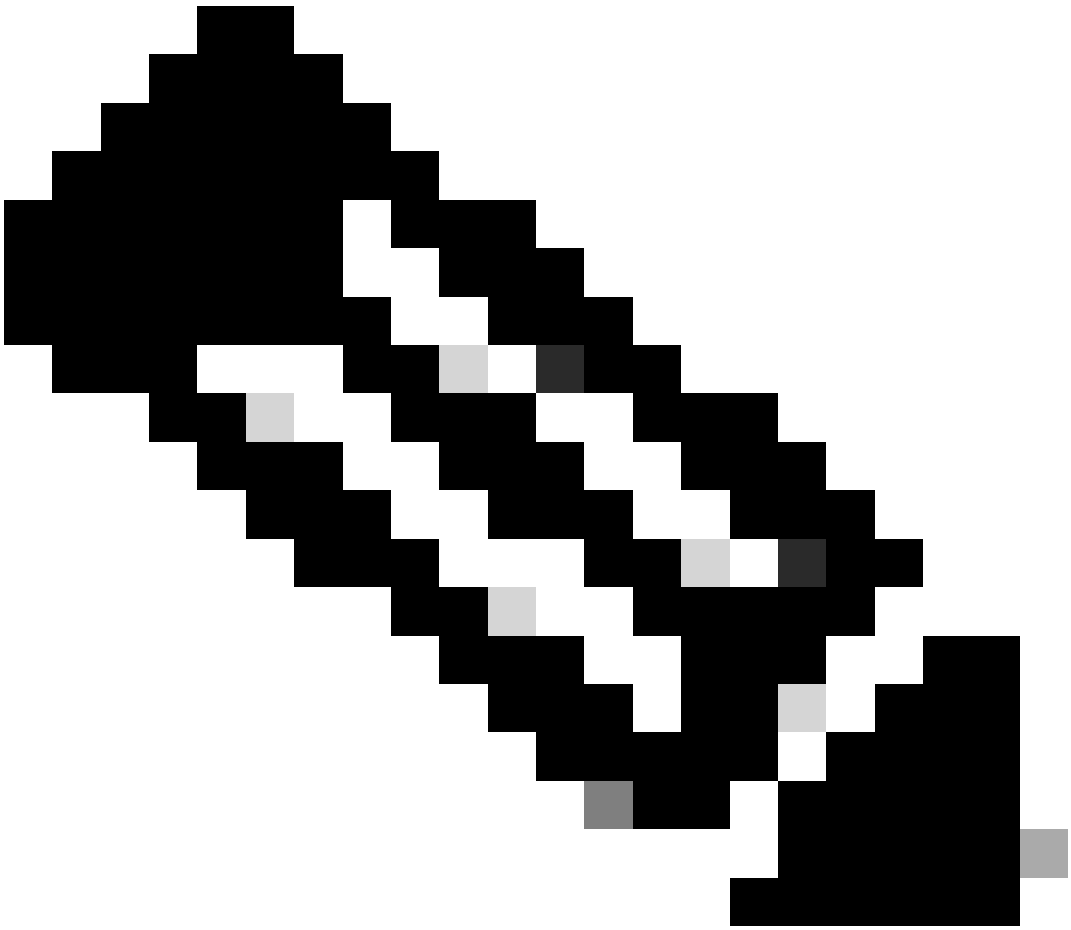
RxSOP is ingesteld per RF-profiel.

Voor elke band zijn er vooraf ingestelde drempels (Laag/Gemiddeld/Hoog) die een vooraf bepaalde dBm waarde plaatsen. Het is aan te raden om altijd aangepaste waarden te gebruiken, zelfs als de bedoelde waarde van de beschikbare voorinstellingen is, maakt dit de configuratie

leesbaarder.

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

Tabel met RXs-instellingen



Opmerking: RxSOP veranderingen vereisen geen radio reset en kunnen worden gedaan tijdens de vlucht.

Het netwerk schalen

Over het algemeen is het gebruik van een apparaat maximaal gedocumenteerd. Dat is een slecht idee. Gegevensbladen geven de waarheid aan, maar de vermelde cijfers kunnen in specifieke omstandigheden van activiteit zijn. Draadloze controllers zijn getest en gecertificeerd om een bepaald aantal clients en AP's te ondersteunen, en een bepaalde doorvoersnelheid, maar dit veronderstelt niet dat clients elke seconde zwerven, dat u zeer lange unieke ACL's voor elke client kunt hebben geconfigureerd of alle beschikbare snuffelfuncties hebt ingeschakeld. Het is daarom belangrijk om alle aspecten zorgvuldig te overwegen om ervoor te zorgen dat het netwerk tijdens piekuren kan worden geschaald en om ook een veiligheidsmarge voor toekomstige groei te behouden.

Aantal toegangspunten

Een van de eerste taken bij de implementatie van een netwerk is het budgetteren en bestellen van de juiste hoeveelheid apparatuur, en de grootste variabele factor is het aantal en type toegangspunten en antennes. Draadloze oplossingen moeten echter altijd gebaseerd zijn op een radiofrequentieontwerp (en helaas), vaak is dit de tweede stap in de levenscyclus van het project. In het geval van eenvoudige indoor enterprise implementaties zijn er tal van schattingstechnieken die, tot een redelijk niveau van zekerheid, kunnen voorspellen hoeveel AP's kunnen worden vereist, zelfs voordat een draadloze architect kijkt naar de vloerplannen. Voorspelmodellen kunnen in dit geval ook zeer nuttig zijn.

Voor uitdagender installaties, zoals industriële, buitenshuis, grote openbare netwerken of waar externe antennes nodig zijn, zijn eenvoudige schattingstechnieken vaak ontoereikend. Bij eerdere soortgelijke installaties is enige ervaring vereist om het soort en de hoeveelheid benodigde apparatuur adequaat in te schatten. Een bezoek aan de site door een draadloze architect is het absolute minimum om inzicht te krijgen in de lay-out van een complexe locatie of faciliteit.

Deze paragraaf bevat richtlijnen voor het bepalen van het minimumaantal AP's en antennes voor de betreffende implementatie. De uiteindelijke hoeveelheden en specifieke montageplaatsen zullen altijd worden bepaald via een proces van behoeftenanalyse en radioontwerp.

De aanvangsrekening van het materiaal moet op twee factoren zijn gebaseerd: het type antennes en de hoeveelheid antennes.

Type antennes

Er zijn hier geen sneltoetsen. Het type antenne wordt bepaald door het gebied dat moet worden bedekt en door de beschikbare montageopties in dat gebied. Het is niet mogelijk om dit te bepalen zonder een begrip van de fysieke ruimte, dit betekent dat een bezoek ter plaatse wordt vereist door iemand met een begrip van antennes en hun dekking patronen.

Hoeveelheid antennes

De benodigde hoeveelheid apparatuur kan worden afgeleid uit een begrip van de verwachte hoeveelheid cliëntverbindingen.

Apparaten per persoon

Het aantal menselijke gebruikers kan worden bepaald aan de hand van de zitcapaciteit van een plaats, het aantal verkochte tickets of het verwachte aantal bezoekers op basis van historische statistieken. Elke menselijke gebruiker kan meerdere apparaten dragen en het is gebruikelijk om meer dan één apparaat per gebruiker aan te nemen, hoewel de mogelijkheid van een menselijke gebruiker om actief meerdere apparaten tegelijk te gebruiken twijfelachtig is. Het aantal bezoekers dat actief verbinding maakt met het netwerk, is ook afhankelijk van het type evenement en/of implementatie.

Voorbeeld 1: Het is normaal dat een stadion met 80.000 zitplaatsen geen 80.000 aangesloten apparaten heeft, dit percentage is gewoonlijk aanzienlijk lager. Verbonden gebruikersverhoudingen van 20% zijn niet ongewoon tijdens sportevenementen, dit betekent dat voor het stadionvoorbeeld met 80.000 zitplaatsen het verwachte aantal aangesloten apparaten 16.000 kan zijn (80.000 x 20% = 16.000). Dit nummer is ook afhankelijk van het gebruikte onboarding mechanisme, als de gebruiker is vereist om een actie uit te voeren (zoals klik op een webportal) dan zijn de nummers lager dan wanneer het apparaat automatisch aan boord gaat. Automatisch onboarden kan net zo eenvoudig zijn als een PSK die is onthouden van een eerdere gebeurtenis, of iets geavanceerder zoals het gebruik van OpenRoaming dat onboard-apparaten zonder gebruikersinteractie. OpenRoaming-netwerken kunnen de gebruiker ertoe aanzetten verhoudingsgetallen van meer dan 50% te nemen, wat een aanzienlijke invloed kan hebben op de capaciteitsplanning.

Voorbeeld 2: het is redelijk om te verwachten dat een technologieconferentie een hoge gebruikersverbindingsverhouding heeft. De aanwezigen van de conferentie besteden langer verbonden met het netwerk en verwachten hun e-mail te kunnen toegang hebben en dagelijkse taken door de dag uit te voeren. Het is ook waarschijnlijker dat dit type gebruiker meer dan één apparaat met het netwerk verbindt - hoewel hun vermogen om meerdere apparaten tegelijk te gebruiken twijfelachtig blijft. Voor technologieconferenties wordt ervan uitgegaan dat 100% van de bezoekers verbinding maakt met het netwerk, dit aantal kan lager zijn voor afhankelijk van het conferentietype.

In beide voorbeelden is het belangrijk om het verwachte aantal verbonden apparaten te begrijpen en er is geen enkele oplossing voor elk groot openbaar netwerk. In beide gevallen is een antenne aangesloten op een radio en zijn het clientapparaten (geen menselijke gebruikers) die verbinding maken met die radio. Daarom zijn clientapparaten per radio een bruikbare metriek.

Apparaten per radio

Cisco AP's hebben een maximum aantal clients van 200 verbonden apparaten per radio voor Wi-Fi 6 AP's en 400 apparaten per radio voor Wi-Fi 6E AP's. Het is echter niet aan te raden om te ontwerpen voor een maximaal aantal klanten. Voor planningsdoeleinden wordt aanbevolen het aantal klanten per radio ruim onder de 50% van de maximale AP-capaciteit te houden. Bovendien,

het aantal radio's hangt af van het type van AP en antenne dat wordt gebruikt, onderzoekt het gedeelte op single vs dual 5GHz dit meer in detail.

In dit stadium is het een goed idee om het netwerk op te delen in verschillende gebieden, met verwachte apparatentellingen per gebied. In dit deel wordt een minimumaantal AP's en antennes geschat.

Neem een voorbeeld van drie verschillende dekkingsgebieden, wordt de verwachte cliënttelling verstrekt voor elk gebied, en een (gezonde) waarde van 75 cliënten per radio wordt gebruikt om het aantal vereiste radio's te schatten.

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

Verwacht aantal radio's/clients per gebied

Deze begingetallen moeten nu worden gecombineerd met het begrip van welke soorten AP's en antennes worden ingezet in elk gebied, en als enkele of dubbele 5GHz wordt gebruikt. 6 GHz berekeningen volgen dezelfde logica als 5 GHz. 2.4GHz wordt niet in overweging genomen in dit voorbeeld.

Laten we aannemen dat elk van de drie gebieden een combinatie van 2566P pleisterantenne en de 9104 stadionantenne gebruikt, met een combinatie van enkele en dubbele 5GHz - dit scenario wordt gebruikt voor illustratiedoeleinden.

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)

Antennes per gebied

Elk gebied geeft het type van de benodigde antennes en AP's aan. Merk op dat in het geval van dubbele 5GHz de verhouding twee antennes aan één AP is.

In dit deel wordt een benadering getoond om een eerste aantal antennes en AP’s te schatten die nodig zijn voor een implementatie. De schatting vereist inzicht in de fysieke gebieden, mogelijke montageopties in elk gebied, het type antennes dat in elk gebied moet worden gebruikt en het aantal clientapparaten dat wordt verwacht.

Elke implementatie is anders en er is vaak extra apparatuur nodig voor specifieke of uitdagende gebieden, bij dit soort schattingen wordt alleen rekening gehouden met de capaciteit van de klant (niet de dekking) en wordt de omvang van de benodigde investering geschetst. Laatste AP/antenne plaatsingslocaties en apparatuurtotalen zijn altijd afhankelijk van een gedegen begrip van de use-case en on-site verificatie door een ervaren draadloze professional.

verwachte doorvoersnelheid

Elk draadloos kanaal kan een hoeveelheid beschikbare capaciteit bieden die meestal wordt vertaald naar de doorvoersnelheid. Deze capaciteit wordt gedeeld tussen alle apparaten die op de radio zijn aangesloten, wat betekent dat de prestaties voor elke gebruiker afnemen naarmate er meer gebruikersverbindingen aan de radio worden toegevoegd. Deze daling in prestaties is niet lineair en is ook afhankelijk van de exacte mix van verbonden cliënten.

Clientfuncties verschillen tussen apparaten, afhankelijk van de client-chipset en het aantal ruimtelijke stromen dat de client ondersteunt. De maximale klantgegevenssnelheden voor elk aantal ondersteunde ruimtelijke stromen worden in de onderstaande tabel vermeld.

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

Verwachte maximale reële doorvoersnelheid voor elk clienttype

De vermelde tarieven zijn theoretische maximale MCS (Modulation and Coding Scheme)-tarieven afgeleid van de 802.11-standaard en gaan uit van een signaal-ruisverhouding (SNR) > 30dBm. Het belangrijkste ontwerpdoel van goed presterende draadloze netwerken is om dit niveau van SNR te bereiken voor alle clients in alle locaties, dit is echter zelden het geval. Draadloze netwerken zijn dynamisch van aard en gebruiken frequenties zonder licentie, verschillende ongecontroleerde interferenties hebben een impact op client-SNR, naast de mogelijkheden van de client.

Zelfs in gevallen waar het vereiste niveau van SNR wordt bereikt, houden de eerder vermelde tarieven geen rekening met protocol overhead, daarom, niet direct in kaart aan echte wereld doorvoersnelheid (zoals gemeten door diverse snelheidstestinstrumenten). De werkelijke wereld is altijd lager dan de MCS-snelheid.

Voor alle draadloze netwerken (inclusief grote openbare netwerken) is de doorvoersnelheid van clients altijd afhankelijk van:

- Mogelijkheden van de klant.
- De signaalruisverhouding van de client op dat specifieke tijdstip.
- Aantal andere clients die op dat specifieke tijdstip zijn verbonden.
- Mogelijkheden van andere klanten op dat specifieke tijdstip.
- Activiteit van andere cliënten op dat specifieke tijdstip.
- Inmenging op dat specifieke tijdstip.

Gebaseerd op de variabiliteit van deze factoren is het niet mogelijk om een minimum per-client door voor draadloze netwerken, ongeacht de apparatuurverkoper te waarborgen.

Raadpleeg voor meer informatie de Validate Wi-Fi Throughput: Testing and Monitoring Guide.

WLC-platform

Het kiezen van uw WLC platform kan eenvoudig lijken. Het eerste waar je aan kunt denken is om te kijken naar de geschatte AP-telling en de klant telling die je wilt beheren. Het gegevensblad

voor elk WLC-platform bevat alle maximale ondersteunde objecten op het platform: ACL's, aantal klanten, sitetags, enzovoort. Dit zijn letterlijke maximumaantallen en vaak is er een harde handhaving. U kunt geen 6001 AP's toevoegen aan een 9800-80 die slechts 6000 AP's ondersteunt, bijvoorbeeld. Maar is het verstandig om overal het maximum na te streven?

De draadloze controllers van Cisco worden getest om deze maxima te kunnen bereiken, maar ze kunnen niet noodzakelijk alle gedocumenteerde maxima in alle omstandigheden tegelijk bereiken. Laten we het voorbeeld van doorvoersnelheid nemen: een 9800-80 kan tot 80 Gbps clientgegevens doorsturen, maar dit is het geval wanneer elk clientpakket de maximale en optimale grootte van 1500 bytes heeft. Bij een combinatie van pakketgroottes is de effectieve maximale doorvoersnelheid lager. Als u DTLS-codering inschakelt, wordt de doorvoersnelheid verder verlaagd en geldt hetzelfde voor Application Visibility. Het is optimistisch om meer dan 40Gbps van 9800-80 in realistische voorwaarden op een groot netwerk met vele toegelaten eigenschappen te verwachten. Aangezien dit sterk varieert afhankelijk van de functies in gebruik en het type netwerkactiviteit, is de enige manier om een echt idee van de capaciteit te krijgen het datapath-gebruik te meten met deze opdracht. Stel scherp op de belastingsmetriek, die een percentage is van de maximale doorvoersnelheid die de controller kan doorsturen.

```
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#
```

Op dezelfde manier kan de 9800-80 6000 AP's perfect verwerken met regelmatige activiteit. 6000 AP's op een openbare locatie zoals een stadion of een luchthaven tellen echter niet als reguliere activiteit. Gezien de hoeveelheid client roaming en omgevingscontrole, kunnen grote openbare netwerken op maximale schaal een verhoogd CPU-gebruik op één WLC veroorzaken. Als u bewakings- en SNMP-traps toevoegt die elke keer dat clients zich verplaatsen moeten worden verzonden, kan de lading snel te veel worden. Een van de belangrijkste kenmerken van een grote openbare locatie of grote gebeurtenis is dat er aanzienlijk meer client-onboarding-gebeurtenissen zijn als mensen bewegen en voortdurend associëren/disassociëren, dus dit veroorzaakt extra druk op de CPU en het besturingsplane.

Talrijke implementaties hebben aangetoond dat één enkel (HA) paar van 9800-80 draadloze controllers een grote stadionplaatsing met goed meer dan 1000 APs kan behandelen. Het is ook

gebruikelijk om de AP's te verdelen over twee of meer controller paren voor kritieke gebeurtenissen waar uptime en beschikbaarheid primaire zorgen zijn. Wanneer grote netwerken worden gedistribueerd via meerdere WLC's is er de extra complexiteit van intercontroller roaming, client roaming moet zorgvuldig worden overwogen in beperkte ruimtes zoals een stadionbowl.

Zie ook de sectie Site Tag in dit document.

WLC met hoge beschikbaarheid

Het wordt aangeraden om een High-Availability Stateful Switch Over (HA SSO)-paar te gebruiken, dit biedt hardwareredundantie maar beschermt ook tegen softwarestoringen. Met behulp van HA SSO, een software crash op één apparaat is transparant voor de eindgebruikers als de secundaire WLC neemt naadloos over. Een ander voordeel van een HA SSO-paar zijn de hitless upgrades die worden aangeboden door de In-Service Software Upgrade (ISSU) functie.

Als het netwerk groot genoeg is, is het ook aangeraden om een extra controller te gebruiken (N+1). Het kan meerdere doelen dienen die de HA SSO niet kan vervullen. U kunt een nieuwe softwareversie op deze WLC testen alvorens het productiepaar te upgraden (en slechts een paar test-AP's naar het migreren om een specifieke sectie van het netwerk te testen). Sommige zeldzame omstandigheden kunnen zowel de WLC's in een HA-paar beïnvloeden (wanneer het probleem wordt gerepliceerd naar de stand-by modus) en hier zorgt de N+1 voor een veilige WLC in een actief-actief scenario waar je progressief AP's naar en van kan migreren. Het kan ook dienen als een provisioningcontroller om nieuwe AP's te configureren.

De 9800-CL's zijn zeer schaalbaar en krachtig. Opgemerkt moet worden dat zij een veel kleinere capaciteit voor het doorsturen van gegevens hebben (van 2 Gbps tot 4 Gbps voor het SR-IOV beeld), wat hen vaak beperkt tot FlexConnect lokale switchingscenario's (en mogelijk een klein aantal AP's in centrale switching). Ze kunnen echter wel nuttig zijn als N+1-apparaten wanneer u extra controllers nodig hebt tijdens een onderhoudsvenster of bij het oplossen van een probleem.

Externe systemen

Hoewel dit document zich voornamelijk richt op de draadloze component van grote evenementennetwerken, zijn er ook talloze ondersteunende systemen die aandacht vereisen tijdens de schalings- en ontwerpfase, worden sommige hiervan hier besproken.

Core-netwerk

De grote draadloze netwerken worden typisch opgesteld op centrale omschakelingswijze en met grote subnets. Dit impliceert dat een zeer groot aantal cliëntMAC-adres en ARP-vermeldingen naar de aangrenzende bekabelde infrastructuur worden geduwd. Het is van cruciaal belang dat de aangrenzende systemen die gewijd zijn aan de verschillende L2- en L3-functies over de juiste middelen beschikken om deze belasting te kunnen verwerken. In het geval van L2-switches is een gemeenschappelijke configuratie de Switch Device Manager (SDM) template, die verantwoordelijk is voor de toewijzing van systeembronnen, balancering tussen L2- en L3-functies afhankelijk van de functie van het toestel binnen het netwerk. Het is belangrijk om ervoor te zorgen dat de kern L2 apparaten het aantal verwachte MAC-adresingangen kunnen ondersteunen.

Gateway NAT

Het meest voorkomende gebruiksgeval van openbare netwerken is om internettoegang te bieden aan bezoekers. Ergens langs het gegevenspad moet er een apparaat zijn dat verantwoordelijk is voor NAT/PAT-vertaling. Internetgateways moeten beschikken over de vereiste hardwarematige bronnen en IP-poolconfiguratie om de werklast te kunnen verwerken. Vergeet niet dat één draadloos clientapparaat verantwoordelijk kan zijn voor talloze NAT/PAT-vertalingen.

DNS/DHCP

Deze twee systemen zijn essentieel voor een goede klantervaring. Zowel DNS- als DHCP-services vereisen niet alleen de juiste schaling om de lading te verwerken, maar ook aandacht met betrekking tot plaatsing binnen het netwerk. Snel reagerende systemen, geplaatst op dezelfde locatie als de WLC zorgt voor de beste ervaring en vermijd lange client onboarding tijden.

AAA/webportal

Niemand houdt van een langzame webpagina, het kiezen van een geschikt en goed-geschaald systeem voor externe web authenticatie is belangrijk voor een goede client onboarding ervaring. Op dezelfde manier moeten RADIUS-verificatieservers voor AAA kunnen voldoen aan de eisen van het draadloze systeem. Houd in gedachten dat in sommige gevallen de belasting kan pieken tijdens belangrijke momenten, bijvoorbeeld halftijds tijdens een voetbalwedstrijd, die een hoge authenticatielast kan genereren in een kleine hoeveelheid tijd. Het is van belang het systeem op te schalen voor een adequate gelijktijdige lading. Bij het gebruik van functies zoals AAA-accounting moet specifieke voorzichtigheid in acht worden genomen. Vermijd op tijd gebaseerde accounting ten koste van alles en als je boekhouding gebruikt, probeer dan tussentijdse accounting uit te schakelen. Een ander belangrijk punt om na te denken is het gebruik van load-balancers, waar de sessie-pining mechanismen moeten worden gebruikt om volledige authenticatiestromen te verzekeren. Zorg ervoor dat de RADIUS-timeout 5 seconden of langer is.

Als u een 802.1X SSID met een groot aantal clients gebruikt (bijvoorbeeld met OpenRoaming), zorg er dan voor dat u 802.11r Fast Transition (FT) inschakelt, anders kunnen clients een verificatiestorm veroorzaken telkens wanneer ze rondzwerven.

DNS/DHCP

Een paar aanbevelingen voor DHCP:

- Zorg ervoor dat de DHCP-pool ten minste driemaal het verwachte aantal clients is. IP's blijven toegewezen voor enige tijd, zelfs nadat de client is losgekoppeld, dus afhankelijk van de verblijftijd van de gasten kan dit meer IP-adressen verbruiken. Probeer de leasetijd af te stemmen op de verwachte duur van het bezoek van de gebruiker aan de locatie, het heeft geen zin om een IP-adres voor een week toe te wijzen als een gemiddelde duur van het bezoek twee uur is, dit helpt om verouderde leases uit te voeren.
- Het gebruik van één grote subnetverbinding voor clients wordt aanbevolen, de WLC heeft een proxy-ARP-functie en stuurt geen uitzendingen standaard door (anders dan DHCP). Het gebruik van een grote (bijvoorbeeld /16) clientsubnetverbinding voor uw clients vormt geen probleem. Eén groot VLAN is eenvoudiger dan een VLAN-groep met veel VLAN’s. Het

configureren van veel kleinere subnetten (bijvoorbeeld /24) en VLAN-groepen heeft geen invloed op het broadcast-domein en resulteert alleen in een meer gecompliceerde configuratie, wat resulteert in problemen zoals vuile VLAN's en het moeten bijhouden van verschillende DHCP-pools die niet gelijk kunnen worden gebruikt.
- Houd DHCP in overbruggingsmodus op de draadloze controller met de DHCP-relay-functionaliteit die wordt verwerkt door Layer 3-gateway van het subsysteem. Dit zorgt voor maximale efficiëntie en eenvoud. Het idee is dat de draadloze controller helemaal niet bij het DHCP-proces betrokken moet worden.
- Gebruik DHCP vereist op elk openbaar WLAN, ongeacht de verificatiemethode. Hoewel dit kan leiden tot een klein percentage van mislukte cliëntenverenigingen, kan het belangrijke veiligheidskwesties voorkomen door cliënten die proberen om zichzelf statische IP-adressen toe te wijzen of door cliënten die zich misdragen en proberen om een vorig IP-adres zonder toestemming te hergebruiken.

Het netwerk bedienen

De juiste configuratie

Het is verleidelijk om een heleboel opties toe te staan om van alle recentste eigenschappen van moderne WiFi te profiteren. Bepaalde functies werken echter prima in kleine omgevingen, maar hebben een grote impact in grote en dichte omgevingen. Op dezelfde manier kunnen bepaalde eigenschappen verenigbaarheidsproblemen veroorzaken. Hoewel Cisco-apparatuur aan alle normen voldoet en compatibiliteit met een groot aantal geteste clients biedt, is de wereld gevuld met unieke clientapparaten die soms driver-softwareversies met bugs of incompatibiliteit met bepaalde functies hebben.

Afhankelijk van het niveau van controle dat je hebt op de klanten, moet je conservatief zijn. Bijvoorbeeld, als u WiFi voor de grote jaarlijkse vergadering van uw bedrijf opstelt, weet u dat de meeste cliënten bedrijfsapparaten zijn en u kunt de eigenschap plannen die dienovereenkomstig wordt geplaatst toe te laten. Aan de andere kant, als u een luchthaven Wi-Fi bedient, heeft uw niveau van gasttevredenheid direct betrekking op hun vermogen om verbinding te maken met uw netwerk, en u hebt geen enkele controle over de clientapparaten die mensen kunnen gebruiken.

SSID's

Hoeveel SSID's?

Het is altijd de aanbeveling geweest om zo min mogelijk SID's te gebruiken. Dit wordt nog eens verscherpt in netwerken met hoge dichtheid, omdat de mogelijkheid om meerdere AP's op hetzelfde kanaal te hebben vrijwel gegarandeerd is. Typisch, gebruiken vele implementaties teveel SSIDs, erkennen zij teveel SSIDs hebben, maar verklaren dat zij niet minder kunnen gebruiken. U moet een zakelijke en technische studie voor elke SSID uitvoeren om de overeenkomsten tussen SSID's en opties voor het samenvouwen van meerdere SSID's in één te begrijpen.

Laten we een paar security/SSID types en het gebruik ervan bespreken.

WPA2/3 persoonlijk

Een vooraf gedeelde sleutel SSID is immens populair vanwege zijn eenvoud. U kunt de sleutel ergens op badges of op papier afdrukken of op borden zetten of op een of andere manier communiceren met bezoekers. Soms wordt een vooraf gedeelde sleutel SSID zelfs voor een gast SSID verkozen (op voorwaarde dat de sleutel door alle aanwezigen bekend is). Het kan helpen voorkomen dat DHCP-pool uitputting als gevolg van de opzettelijke aard van de verbinding. Apparaten die voorbijgaan, maken geen automatische verbinding met het netwerk en kunnen daarom geen IP-adres uit de DHCP-pool gebruiken.

WPA2 PSK biedt geen privacy omdat verkeer gemakkelijk kan worden ontsleuteld omdat iedereen dezelfde sleutel gebruikt. In tegendeel, WPA3 SAE biedt wel privacy, en zelfs als iedereen de master key heeft is het niet mogelijk om de encryptie sleutel die door andere klanten gebruikt wordt af te leiden.

WPA3 SAE is de betere keuze voor beveiliging en veel smartphones, laptops en besturingssystemen ondersteunen dit. Sommige IoT-apparaten of smart wearables kunnen nog steeds beperkte ondersteuning hebben en oudere klanten zijn over het algemeen gevoelig voor problemen als ze geen recente stuurprogramma- of firmware-updates hebben ontvangen.

Het kan verleidelijk zijn om een Transition Mode WPA2 PSK-WPA3 SAE SSID te overwegen om dingen te vereenvoudigen, maar dit is in het veld getoond om bepaalde compatibiliteitsproblemen te veroorzaken. Slecht geprogrammeerde clients verwachten niet twee soorten gedeelde sleutelmethoden op dezelfde SSID. Als u zowel WPA2- als WPA3-opties wilt bieden, is het raadzaam afzonderlijke SSID's te configureren.

WPA2/3 voor ondernemingen

WPA3 Enterprise (met behulp van AES 128-bit encryptie) is technisch dezelfde beveiligingsmethode (tenminste zoals geadverteerd in de SID bakens) als WPA2 Enterprise, die maximale compatibiliteit biedt.

Voor 802.1X wordt een overgangsmodus SSID aangeraden omdat compatibiliteitsproblemen niet worden gezien met recente apparaten (problemen werden gemeld met Android 8 of oude Apple IOS versies). IOS XE 17.12 en latere releases maken het mogelijk om één Transition Enterprise SSID te hebben waar alleen WPA3 wordt gebruikt en geadverteerd op 6 GHz terwijl WPA2 als optie wordt aangeboden op de 5 GHz band. We adviseren om WPA3 op Enterprise SSID's zo snel mogelijk in te schakelen.

WPA Enterprise SSID's kunnen worden gebruikt voor belangrijke gebruikers waarvoor er een database van de identiteitsprovider is waarmee AAA-parameters (zoals VLAN's of ACL's) kunnen worden geretourneerd, afhankelijk van de gebruikersidentiteit. Zulke soorten SSID's kunnen eduroam of OpenRoaming omvatten die de voordelen van gast-SSID's (door bezoekers toe te staan om gemakkelijk verbinding te maken zonder enige referenties in te voeren) combineren met de beveiliging van een zakelijke SSID. Ze verminderen de complexiteit van onboarden, die normaal geassocieerd wordt met 802.1X, omdat clients niets hoeven te doen om zich aan te sluiten bij de eudroam of OpenRoaming SSID, mits ze een profiel op hun telefoon hebben (die

eenvoudig kan worden geleverd via een event app)

Gast-SSID’s

Een gast-SSID is vaak synoniem met open authenticatie. U kunt een webportal (of niet) erachter toevoegen (afhankelijk van de gewenste vriendelijkheid of lokale vereisten) in zijn verschillende vormen: externe, lokale of centrale webverificatie, maar het concept blijft hetzelfde. Wanneer het gebruik van een guest portal, kan schaalbaarheid snel een probleem worden in grote omgevingen. Raadpleeg het gedeelte Configuration for Scalability voor meer informatie over dit onderwerp.

6GHz operaties vereisen dat uw gast SSID gebruik maakt van Enhanced Open in plaats van alleen Open. Dit staat nog steeds iedereen toe om verbinding te maken maar biedt privacy (een betere privacy dan WPA2-PSK zelfs!) en encryptie, allemaal zonder enige sleutel of referenties bij het verbinden op de SSID. De belangrijkste leveranciers van smartphones en besturingssystemen ondersteunen nu Enhanced Open, maar de ondersteuning is nog niet wijdverbreid in de draadloze clientbasis. Enhanced Open Transfer Mode biedt een goede compatibiliteitsoptie waarin geschikte apparaten verbinding maken met de versleutelde gast-SSID (met Enhanced Open) en de niet-geschikte apparaten nog steeds de SSID gebruiken als gewoon open zoals voorheen. Terwijl slechts één SSID door eindgebruikers wordt opgemerkt, me ervan bewust ben dat deze overgangswijze twee SSIDs in uw bakens uitzendt (hoewel slechts één zichtbaar is).

In grote evenementen en locaties, is het vaak aangeraden om een PSK op de Guest SSID te configureren in plaats van het puur open te laten (Enhance Open Transition mode zou beter zijn, maar dat creëert twee SSID's en client compatibiliteit moet nog steeds uitgebreid worden bewezen). Hoewel dit het onboarden wat ingewikkelder maakt (je moet de PSK op de badges of tickets van mensen afdrukken of op de een of andere manier adverteren), vermijdt het casual klanten die automatisch met het netwerk verbinden zonder dat de eindgebruiker van plan is om het netwerk te gebruiken. Steeds meer mobiele besturingssysteemverkopers geven ook de prioriteit aan open netwerken en tonen een veiligheidswaarschuwing. In andere situaties kunt u een maximaal aantal voorbijgangers willen verbinden en daarom is openen de betere keuze.

Conclusie over het aantal SSID’s

Er kan geen bevredigend antwoord zijn op de vraag aan hoeveel SSID's u moet vasthouden. Het effect hangt af van de minimale gegevenssnelheid, het aantal SSID's en het aantal AP's die op hetzelfde kanaal uitzenden. Bij één groot Cisco-evenement gebruikte de draadloze infrastructuur 5 SSID's: de belangrijkste WPA2 PSK, een WPA 3 SAE SSID voor beveiliging en 6GHz dekking, een ondernemings-Eduroam SSID voor gemakkelijke toegang voor studenten, een OpenRoaming SSID om iedereen die Wi-Fi geconfigureerd had, veilig te verwelkomen vanuit de gebeurtenisapp en een aparte 802.1X SSID voor het personeel en de beheerder netwerktoegang. Dit was al bijna te veel, maar het effect bleef redelijk dankzij het grote aantal beschikbare kanalen en de richtantennes die worden gebruikt om kanaaloverlapping zoveel mogelijk te beperken.

Verouderde SSID versus de belangrijkste concepten van SSID

Voor een bepaalde periode werd geadviseerd om 2.4GHz-dienst te beperken tot een "Verouderde" afzonderlijke SSID alleen geadverteerd in 2.4GHz. Dit wordt steeds minder populair

omdat mensen stoppen met het leveren van 2.4GHz service. Het idee kan en moet echter blijven bestaan, maar met andere concepten. U wilt WPA3 SAE uitrollen, maar transitiemodus geeft u compatibiliteitsproblemen met uw klanten? Zorg voor een WPA2 "Legacy"-SSID en een WPA3 SAE-SSID. Door het noemen van de minst presterende SID "legacy" trekt het geen cliënten aan en u kunt gemakkelijk zien hoeveel cliënten nog compatibiliteitskwesties met uw belangrijkste SSID onder ogen zien en deze erfenis één vereisen.

Maar waarom stoppen we hier? U hoorde geruchten dat 802.11v problemen veroorzaakte met sommige oudere clients of dat sommige client drivers niet graag Apparaatanalyse ingeschakeld zien op de SSID? Schakel al die handige functies op uw geavanceerde hoofd-SSID in en laat ze weg op uw legacy/compatibiliteit-SSID. Dit stelt u in staat om de uitrol van nieuwe functies op uw belangrijkste SSID te testen terwijl nog steeds een maximale compatibiliteit SSID voor cliënten om terug te vallen naar. Dit systeem werkt alleen op deze manier. Als u de tegenovergestelde naam uw compatibiliteit-gedreven SSID als uw hoofd en noem uw geavanceerde SSID met iets als "<name>-WPA3", merkt u mensen die aan de oude SSID vasthouden zij aan, en adoptie blijven klein voor vele jaren op uw "nieuwe" SSID. Het uitrollen van nieuwe instellingen of functies heeft dan onovertuigende resultaten als gevolg van het lagere aantal clients die er verbinding mee maken.

SSID-functies

- Het is het beste om Aironet Extensions uitgeschakeld te houden. Deze zijn bijzonder nuttig voor site-enquêtes en WGB-activiteiten, maar veroorzaken soms problemen met sommige oudere klanten. Aironet IE adverteert ook met de AP hostname die ongewenst is in security-bewuste implementaties.
- CCKM is een afgekeurd protocol (ten gunste van FT) en moet worden uitgeschakeld.
- Op dit moment is het het beste om AES-128 encryptie te gebruiken, zelfs in WPA3 vanwege de lage clientondersteuning van hogere encrypties (tenzij u zich een specifieke veiligere en beperkende SSID kunt veroorloven)
- De Opsporing van de Gat van de dekking is best gehandicapt (voor alle SSIDs). Grote implementaties maken doorgaans gebruik van directionele antennes, waarvoor een grondige controle van de locatie vereist is. De vermogensniveaus van elke antenne zouden het resultaat zijn van het RF-ontwerpproces en doorgaans worden ingesteld op specifieke niveaus.
- Adaptieve FT moet worden uitgeschakeld omdat sommige cliënten problemen kunnen hebben wanneer FT niet volledig wordt geadverteerd maar in sommige eigenschappen aanwezig is. Ofwel volledig uitschakelen FT (voor maximale compatibiliteit) of gaan met FT+802.1X wat de meeste clients (tenzij ze oud of meer IoT georiënteerd zijn) wel ondersteunen. Bij het configureren van FT+802.1X mogen zelfs niet-FT-clients zich bij de SSID aansluiten. Het enige mogelijke probleem is met sommige cliënten die niet het zien van twee veiligheidsopties op de zelfde SSID zouden tolereren.
- Schakel 802.11ac MU-MIMO uit. Het voegt complexiteit toe en heeft een zeer laag voordeel in 802.11ac.
- Schakel de BSS Target Wake Time uit. Het heeft lage adoptie aan de cliëntkant momenteel.
- Schakel agressieve taakverdeling en bandselectie uit. Band Select is niet nodig als u niet de SSID in 2.4GHz (of als het op een speciale SSID) en agressieve load-balancing vertragingen

cliëntvereniging door het afwijzen van de client een paar keer alvorens het definitief te accepteren als het erop staat om verbinding te maken met een geladen AP. U hebt toch AP's geladen in een drukke omgeving en dit is negatief voor de client ervaring.
- Fastlane+ uitschakelen.
- Schakel Universal Admin uit, deze optie was voor 3700 AP en alleen in het -UX domein. Laat het op bladeren open een onnodige aanvalsvector.
- Opportunistische Key Caching (OKC) ingeschakeld houden. Het is een snel roamingmechanisme voor klanten die geen FT ondersteunen.
- Hou WMM toegestaan. Als u het zou uitschakelen, zou uw netwerk weer teruggaan naar het 802.11g-tijdperk en als u het zou gebruiken, zou het geen voordeel opleveren voor het 9800-platform.
- IP-bronbewaking inschakelen.
- RADIUS-profilering uitschakelen. In een zeer drukke omgeving kan dit buitensporige RADIUS-boekhoudingsberichten verzenden (wanneer de clients DHCP- of HTTP-pakketten verzenden) en heeft dit een zeer reëel potentieel om uw RADIUS-server te overladen.
- Vermijd het gebruik van verborgen SSID's. Dit dient geen veiligheidsdoel, de SSID naam kan nog steeds gemakkelijk worden ontdekt met eenvoudige toepassingen of door een snuffelopname te nemen. Het verbergen van de SSID vertraagt alle client roaming omdat ze niet meer profiteren van passief beacon scannen en moeten vertrouwen op actief scannen om naburige AP informatie te krijgen.
- Probeer niet meer dan vier WLAN’s per radio te gebruiken omdat dit een aanzienlijk effect heeft op RF-gebruik. Het is geen moeilijke grens, kan het gebruiken van vijf WLANs werken maar zeer bewust van de verspilde zendtijd zijn door meer en meer WLANs te gebruiken.
- 802.11v en 802.11k zijn standaarden die steeds meer worden ondersteund door populaire clienttypen. Zij vormen doorgaans geen probleem met betrekking tot de verbinding met de klant. De voordelen die ze bieden, hangen sterk af van de manier waarop clients die protocollen gebruiken en kunnen soms (in het geval van 802.11k) een iets hoger CPU-gebruik veroorzaken. U kunt ze uit uw IoT of Legacy SSID houden, maar ze moeten indien mogelijk worden ingeschakeld op uw productie-SSID.

Site-tag

Site-tags zijn een configuratie-item dat het mogelijk maakt om access points te groeperen die dezelfde FlexConnect-instellingen delen, evenals AP-leden van profielinstellingen (zoals referenties, SSH-gegevens en landcode). Waarom zijn site tags belangrijk? De markeringen van de plaats bepalen ook hoe APs door het proces WNCD binnen Catalyst 9800 worden behandeld. Laten we een paar voorbeelden geven om te illustreren:

- Als u vier site-tags configureert op een 9800-80 die acht WNCD-processen heeft, wordt elke site-tag toegewezen aan een ander WNCD-proces (elk op een afzonderlijke CPU-kern draaien) en vier WNCD-processen doen niets. Dit betekent dat u niet alle CPU's van uw 9800-80 gebruikt en het is niet aan te raden om deze te laden met de maximaal 6000 ondersteunde AP's.

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

Eerste voorbeeld van site tag balancing

- Als u 10 zijtags instelt op een 9800-80 die acht WNCD-processen heeft, dan zorgen twee WNCD-processen elk voor twee sitetags, terwijl de resterende zes elk één sitetag behandelen.

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

Tweede voorbeeld van site tag balancing

Voor geografisch grote implementaties met vele sites en vele site-tags, wordt het aantal site-tags aanbevolen om een veelvoud te zijn van het aantal WNCD-processen op het platform dat u gebruikt.

Voor evenementennetwerken die zich doorgaans onder één dak bevinden, of meerdere gebouwen op dezelfde locatie, is het raadzaam het aantal sitetags aan te passen aan het exacte aantal WNCD's op het betreffende platform. Het einddoel is dat elk WNCD-proces (en dus elke CPU-kern die is toegewezen aan draadloze taken) een vergelijkbaar aantal clientroamgebeurtenissen verwerkt, zodat de werklast over alle CPU-kernen wordt verdeeld.

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

Aantal WNCD-processen voor elk platform

In de kern gaat het erom AP's die in dezelfde fysieke omgeving zijn gegroepeerd in dezelfde site-tag, zodat de frequente client roaming-gebeurtenissen tussen deze AP's in hetzelfde CPU-proces blijven. Dit betekent dat, zelfs als u één grote locatie hebt, het is aan te raden om de locatie te verdelen in verschillende site tags (zo veel als je WNCD processen behandeling van de locatie) en groep AP's zo logisch mogelijk in deze te vormen logische RF-buurt groepen die ook gelijkmatig verdeeld zijn onder site tags.

Vanaf IOS XE 17.12 kan een taakverdelingsalgoritme worden ingeschakeld, zodat de WLC de AP's groepeert op basis van hun RF-nabijheid. Dit neemt de last uit uw handen en creëert een evenwichtige spreiding van de AP's over het WNCD-proces. Dit kan nuttig zijn als u niet gemakkelijk groepen van naburige APs kunt tekenen die in de juiste hoeveelheid site-tags moeten worden geplaatst. Een specifiek kenmerk van dit algoritme is dat het AP's toewijst aan WNCD-proces ongeacht hun site tag toewijzing, dit betekent dat het de site tag toewijzing van de AP niet wijzigt. U kunt dan site tags puur basis toewijzen op een configuratie logica en het algoritme de AP's over CPU's op de meest optimale manier laten balanceren.

De op RF gebaseerde automatische AP-taakverdeling is gedocumenteerd in de Cisco Catalyst 9800 Series softwareconfiguratiegids voor draadloze controllers, Cisco IOS XE Dublin 17.12.x.

Het CPU-gebruik van WNCD-processen moet tijdens grote gebeurtenissen worden bewaakt. Als een of meer WNCD-processen een hoge benuttingsgraad laten zien, kan het zijn dat de WNCD te veel AP's of klanten verwerkt, of dat de AP's of klanten die zij verwerkt drukker zijn dan het gemiddelde (als alle AP's constant rondzwerven zoals op een luchthaven bijvoorbeeld).

Beleidsprofiel

- Schakel ARP en Duplicate Address Detection (DAD) Proxy in. Hierdoor kan de WLC reageren namens draadloze clients wanneer een apparaat het MAC-adres van een draadloos apparaat probeert te leren. Hierdoor worden ook draadloze clientbatterijen opgeslagen.
- Schakel WGB-functies niet in tenzij dit nodig is.
- DHCP inschakelen vereist om clients met statische IP-adressen te vermijden.
- Houd de ongebruikte tijd kort (300 seconden). Sommige beheerders maken het lang om te voorkomen dat clients opnieuw moeten authenticeren, maar lange idle-time resultaten in ghost client-vermeldingen (die van invloed zijn op rapportage) als het aantal clients wordt vertraagd van real-time. Het is het beste om de inactiviteitstimer lager te houden dan de groepssleutelrotatietimer om boekhoudkundige overstromingen te voorkomen wanneer de clients worden verwijderd. Het rotatieinterval van de groepssleutel kan in de web-UI worden geconfigureerd onder Configuration > Security > Advanced EAP als "EAP-Broadcast Key Interval"
- Maak de sessie 86400 seconden uit om onnodige onderbrekingen en opnieuw verificaties te voorkomen.

Profiel van AP Join

- Zorg ervoor dat TCP MSS is ingeschakeld.
- Schakel DSCP upstream in. Veel draadloze clients doen helaas geen 802.11e WMM UP-

tagging en vertrouwen op het DSCP-veld is een veilige manier om de juiste prioriteit te geven aan spraaktoepassingen.
- Schakel Syslog in voor uw access points. Als u een Syslog-server IP configureert, worden de AP's unicast en hun console logt in. Het is niet alleen nuttig om APs problemen op te lossen, maar het is ook beter voor het netwerk dan de standaardinstelling die APs hun Syslog in het lokale VLAN maakt uitzenden. AP-vastlegging kan aanzienlijke berichtbelasting genereren, zelfs in gevallen waarin AP Syslog niet wordt bewaakt, is het nog steeds een goed idee om het aantal gebeurtenissen te beperken door de juiste berichternst in te stellen en/of een dummy Syslog IP-adres te configureren (bijvoorbeeld 0.0.0.0) om te voorkomen dat berichten worden uitgezonden.
- Optimaliseer CAPWAP-herhalingen en time-out. Problemen worden minder snel gedetecteerd, maar het netwerk is beter bestand tegen kleine tijdelijke pakketdruppels.
- Schakel SSH in en configureer referenties. AP-console uitschakelen.
- Schakel de AP monitor in indien nodig, maar niet de radio monitor.
- Schakel de detectie van abnormaliteiten in en configureer een RSSI-drempel van -70 dBm.

Het netwerk bewaken

Als het netwerk eenmaal in bedrijf is, moet u het nauwgezet controleren op problemen. In een standaard kantooromgeving kennen gebruikers het netwerk en kunnen ze elkaar helpen bij problemen of een intern helpdeskticket openen. In een grotere locatie met veel bezoekers kom je te focussen op de grootste problemen in plaats van op specifieke individuen die gewoon een misconfiguratie kunnen hebben, dus je moet de juiste monitoringstrategie hebben.

De bewaking van het netwerk vanaf Catalyst 9800 CLI of GUI is mogelijk, maar het is niet de beste tool om dagelijks te controleren. Het is het meest direct wanneer u al verdenkingen en/of gegevens over het probleem hebt en specifieke opdrachten in real time wilt uitvoeren. De belangrijkste controleopties zijn Cisco Catalyst Center of mogelijk een aangepast telemetriedashboard. Het is mogelijk om 3rd party monitoring tools te gebruiken, maar wanneer die SNMP als een protocol gebruiken, de gegevens is ver van real-time en de gebruikelijke 3rd party monitoring tools zijn niet granulair genoeg met alle draadloze leveranciers specifieke eigenschappen. Als u het SNMP-protocol kiest, zorg er dan voor dat u SNMPv3 gebruikt omdat SNMPv2 verouderde beveiliging heeft.

Cisco Catalyst Center is de beste optie omdat u hiermee uw netwerk kunt beheren en niet alleen kunt controleren. Meer dan controle, maakt het ook mogelijk om live problemen op te lossen en veel situaties te verhelpen.

Een aangepaste telemetrie dashboard kan handig zijn als u zeer specifieke metriek en widgets op een scherm wilt weergeven in een altijd-on mode voor een NOC of SOC. Als er zeer specifieke gebieden van uw netwerk zijn die u in de gaten wilt houden, kunt u speciale widgets bouwen om de netwerkmetriek in die gebieden op de manier van uw keuze te tonen.

Voor gebeurtenisnetwerken is het een goed idee om systeembrede RF-statistieken te monitoren, in het bijzonder kanaalgebruik en aantal clients per AP. Dit kan vanaf de CLI worden gedaan, maar biedt alleen een momentopname op een specifiek tijdstip, het kanaalgebruik is meestal dynamisch en is beter geschikt voor monitoring in de tijd. Voor dit soort controle is een aangepast

dashboard meestal een goede aanpak. Andere metriek die waardevoller zijn wanneer ze in de loop van de tijd worden bewaakt, kunnen zijn: WNCD-gebruik, aantal klanten en hun status, en locatiespecifieke metriek. Een voorbeeld van locatiespecifieke maatstaven zou het monitoren van het gebruik en/of de belasting voor een specifiek gebied of een specifieke locatie zijn, bijvoorbeeld hal X in het geval van een conferentiecentrum, of zitruimte Y in het geval van een evenementenlocatie.

Voor aangepaste monitoring zijn zowel NETCONF RPC (pull) als NETCONF streaming telemetry (push) geldige benaderingen, hoewel het gebruik van aangepaste streaming telemetrie in combinatie met Catalyst Center enige zorgvuldigheid vereist, omdat er een limiet is aan het aantal telemetrie-abonnementen die kunnen worden geconfigureerd op de WLC en Catalyst Center pre-populates (en gebruikt) veel van deze.

Bij het gebruik van NETCONF RPC is een aantal testen nodig om te verzekeren dat de WLC niet overbelast is met NETCONF verzoeken, vooral belangrijk om in gedachten te houden zijn vernieuwingssnelheden voor sommige van de datapunten en de tijd die nodig is om de gegevens te retourneren. Bijvoorbeeld, AP het kanaalgebruik wordt verfrist (van AP aan WLC) om de 60 seconden, en de inzameling van RF metriek voor 1000 APs (van WLC) kan verscheidene seconden vergen, in dit voorbeeld die WLC om de 5 seconden pollen niet nuttig zou zijn, zou een betere benadering zijn om systeem-brede RF metriek om de 3 minuten te verzamelen.

NETCONF heeft altijd de voorkeur boven SNMP.

Tot slot kan de controle van de componenten van het kernnetwerk niet worden overzien, met inbegrip van het poolgebruik van DHCP, aantal NAT ingangen op kernrouters etc. Omdat het falen van een van deze kan gemakkelijk de oorzaak van een draadloze storing.

Specifieke kwesties voor grote netwerken

Als u een SSID hebt met web-authenticatie, kan een probleem zijn clients die verbinding maken met die SSID en een IP-adres krijgen maar nooit verifiëren omdat de eindgebruiker niet actief probeert verbinding te maken (het apparaat automatisch verbonden). De controller moet elk HTTP-pakket onderscheppen dat wordt verzonden door die clients die zich in de staat bevinden, webverificatie in behandeling en dit maakt gebruik van WLC-bronnen. Zodra uw netwerk wordt uitgevoerd, houd periodiek een oog op het aantal cliënten die in Webauthentificatie hangende staat op een gegeven ogenblik zijn om te zien hoe het met basislijnaantallen vergelijkt. Hetzelfde voor clients in IP Leer status. U hebt altijd klanten in die staat wanneer zij hun DHCP-proces doen, maar weten wat een goed werknummer voor uw netwerk is helpt om een basislijn in te stellen en momenten te identificeren waar dit nummer te hoog kan zijn en een groter probleem aan te geven.

Voor grote locaties is het niet ongewoon om te zien ~ 10% van de klanten in Web Auth Pending staat.

Monitoring op dag 2: aandacht voor gebruikerstevredenheid

Wanneer het netwerk eenmaal in gebruik is, zijn er twee typen klachten van eindgebruikers: zij kunnen geen verbinding maken of moeite hebben om verbinding te maken (verbindingen worden

verbroken), of de Wi-Fi werkt langzamer dan verwacht. Het laatste is erg lastig te identificeren, omdat het eerst afhangt van de verwachtingen van de snelheid en de real-time dichtheid van een bepaald gebied. Laten we een paar hulpmiddelen behandelen die nuttig kunnen zijn bij uw dagelijkse controle van een groot openbaar netwerk van plaatsen.

Valideren Wi-Fi Doorvoersnelheid: test- en bewakingsgids. Dit cisco.com document behandelt hoe u een netwerk kunt controleren om doorvoerproblemen op te sporen. Het gaat door het uitzoeken van hoeveel productie de cliënten redelijkerwijs in uw netwerk kunnen verwachten wanneer de dingen stil zijn en te schatten hoeveel deze schattingen als cliënttelling en ladingsverhogingen dalen. Dit is van cruciaal belang om te beoordelen of een klacht van eindgebruikers over doorvoersnelheid al dan niet legitiem is vanuit een technisch standpunt, en of u dat gebied opnieuw moet ontwerpen voor de belasting die het potentieel te wachten staat.

Wanneer clients connectiviteitsproblemen melden, nadat dit was geïsoleerd en verduidelijkt met Catalyst Center, neem dan een kijkje bij Problemen met Catalyst 9800 clientconnectiviteit Flow oplossen.

Tot slot, als algemene goede praktijk, houd een oog op de algemene belangrijkste metriek van WLC met behulp van Monitor Catalyst 9800 KPIs (de Zeer belangrijke Indicatoren van Prestaties).

Configureren voor schaalbaarheid

SVI's en interfaces op de 9800

Vermijd het maken van SVI’s voor client-VLAN’s op de WLC. Beheerders die worden gebruikt om oudere AireOS WLC's te maken hebben de reflex om een Layer 3-interface te maken voor elke client-VLAN, maar dit is zelden nodig. De interfaces verhogen de vector van de controlevliegtuigaanval en kunnen meer ACLs met complexere ingangen vereisen. De WLC kan standaard worden benaderd op elk van zijn interfaces, er is meer werk nodig om een WLC met meer interfaces te beschermen. Het bemoeilijkt ook de routing, dus het is het best om het te vermijden.

Vanaf IOS XE 17.9 zijn de SVI-interfaces niet langer nodig voor mDNS-spionage of DHCP-relais scenario's. Er zijn daarom heel weinig redenen om een SVI-interface in een client-VLAN te configureren.

Geaggregeerde sonde-respons

Voor grote openbare netwerken, is het raadzaam om het standaard geaggregeerde die sonde interval te wijzigen door toegangspunten wordt verzonden. Standaard wordt de WLC elke 500 ms over de door clients verzonden probes bijgewerkt door de AP's. Deze informatie wordt gebruikt voor taakverdeling, bandselectie, locatie en 802.11k-functies. Als er veel clients en toegangspunten zijn, is het raadzaam om het updateinterval aan te passen om problemen met de prestaties van het besturingsplane in de WLC te voorkomen. De aanbevolen instelling is 50 geaggregeerde sonde-responsen om de 64 seconden. Zorg er ook voor dat uw AP's geen sondes van lokaal beheerde MAC-adressen melden, omdat er geen punt tracking die overwegen een enkele client zou kunnen gebruiken veel lokaal beheerde MAC's tijdens het scannen om te

voorkomen dat volgen op doel.

```
wireless probe limit 50 64000

no wireless probe localy-administered-mac
```

IPv6-server

Veel netwerkbeheerders ontkennen IPv6 nog steeds. Er zijn slechts twee aanvaardbare opties voor IPv6: of u ondersteunt het en moet overal adequate configuratie implementeren, of u niet, en u moet het blokkeren. Het is niet acceptabel om IPV6 niet te geven en het op sommige plaatsen ingeschakeld te laten zonder de juiste configuratie. Dat zou die hele IP-wereld weglaten waar je netwerkbeveiliging blind voor zou zijn.

Als u IPv6 inschakelt, is het verplicht om een virtueel IPv6-adres in het bereik 2001:DB8::/32 (dat is een vaak vergeten stap) te configureren.

Het is belangrijk om op te merken dat, hoewel IPv6 veel op multicast vertrouwt voor zijn basisverrichtingen, het nog kan werken als u multicast het door:sturen op WLC onbruikbaar maakt. Multicast-doorsturen verwijst naar client-multicast gegevensdoorsturen en niet naar de buurdetectie, routertoepassingen en andere vereiste protocollen om IPv6 te gebruiken.

Als uw internetverbinding of internetprovider IPv6-adressen levert, kunt u beslissen om IPv6 voor uw klanten toe te staan. Dat is een andere beslissing dan IPv6 in uw infrastructuur in te schakelen. Uw AP's konden blijven werken in IPv4 maar nog steeds IPv6 client data verkeer binnen hun CAPWAP pakketten. Het inschakelen van IPv6 op uw infrastructuur vereist ook dat u nadenkt over het beschermen van de clienttoegang tot uw AP’s, WLC en beheersubnet.

Controleer de RA frequentie van uw client gateways. De WLC biedt een RA verstikkende beleid dat het aantal RA's dat wordt doorgestuurd naar de klanten beperkt, aangezien deze soms kunnen kletsen.

mDNS

Over het algemeen is het het beste om mDNS volledig uitgeschakeld te houden in een grote locatie.

mDNS-overbrugging verwijst naar het concept waarbij de mDNS-pakketten als Layer 2-multicast worden verzonden (dus naar de gehele clientsubnetprocessor). mDNS werd populair in scenario's voor thuis en kleine kantoren waar het zeer praktisch is om services in uw subnetprocessor te ontdekken. In een groot netwerk betekent dit echter dat het pakket naar alle klanten in het subnetnetwerk wordt verzonden, wat problematisch is vanuit het oogpunt van verkeer in een groot openbaar netwerk. Aan de andere kant veroorzaakt overbrugging geen overheadkosten voor de AP of WLC CPU, omdat het wordt beschouwd als regulier dataverkeer. mDNS Proxy of mDNS gateway verwijst naar het concept van het gebruik van de WLC als een directory voor alle

diensten in het netwerk. Dit maakt het mogelijk om mDNS-diensten over Layer 2-grenzen op een efficiënte manier aan te bieden en ook het totale verkeer te verminderen. Met mDNS gateway, een printer, bijvoorbeeld, verstuurt zijn periodieke de dienstaankondiging via mDNS met zelfde-Subnetnet Layer 2 multicast maar WLC door:sturen het niet aan alle andere draadloze cliënten. In plaats daarvan neemt zij nota van de aangeboden dienst en registreert zij deze in haar dienstenlijst. Wanneer een klant vraagt om diensten van een bepaald type beschikbaar, antwoordt de WLC namens de printer met de aankondiging. Dit voorkomt dat alle andere draadloze klanten te horen krijgen over onnodige verzoeken en diensten en krijgt alleen een antwoord wanneer ze vragen welke diensten er in de buurt zijn. Hoewel het de efficiëntie van het verkeer aanzienlijk verbetert, veroorzaakt het wel een overhead op de WLC (of de AP, als u zich baseert op AP mDNS in FlexConnect-scenario's) door het snuffelen van mDNS-verkeer. Als het gebruiken van mDNS gateway, is het kritiek om een oog op het gebruik van cpu te houden.

Overbrugging leidt tot een multicast storm in uw grote subnet en het snuffelen (met de mDNS gatewayfunctie) veroorzaakt veel CPU-gebruik. Schakel het wereldwijd en op elk WLAN uit.

Sommige beheerders laten mDNS toe omdat een paar diensten het op specifieke plaatsen nodig hebben, maar het is belangrijk om te begrijpen hoeveel ongewenst verkeer dit toevoegt. Apple-apparaten adverteren vaak zelf en jagen voortdurend op diensten, wat achtergrondlawaai veroorzaakt van mDNS-vragen, zelfs als niemand een bepaald gebruik van een dienst maakt. Als u mDNS moet toestaan vanwege een bepaalde bedrijfsvereiste, moet u het globaal inschakelen en vervolgens alleen op het WLAN inschakelen waar het nodig is en proberen om het bereik te beperken waar mDNS is toegestaan.

Verharding van het netwerk

Beveiliging

In grote openbare netwerken kan er veel gebeuren zonder dat de beheerder ervan op de hoogte is. Mensen vragen om kabeldruppels op willekeurige plaatsen, of steek een switch aan op een locatie waar meer telefoonpoorten nodig zijn voor hun shenanigans, ... Ze proberen dit meestal zonder eerst om toestemming te vragen. Dit betekent dat, zelfs zonder een slechte speler die in het spel komt, de veiligheid al kan worden gecompromitteerd door goedwillende klanten en/of werknemers. Het wordt dan heel gemakkelijk voor een slechte acteur om enkel rond te lopen en een kabel te vinden om aan te sluiten en te zien welke netwerktoegang zij van daar krijgen. Het configureren van 802.1X-verificatie op alle switchpoorten is een bijna-vereiste voor het handhaven van een behoorlijke beveiliging in een groot netwerk. Catalyst Center kan u helpen deze implementatie te automatiseren en er kunnen uitzonderingen worden gemaakt voor specifieke apparaten die geen 802.1X-verificatie ondersteunen, maar proberen zo weinig mogelijk te vertrouwen op op MAC-gebaseerde verificatie omdat dat (oprecht) geen echte beveiliging is.

Rogue access points

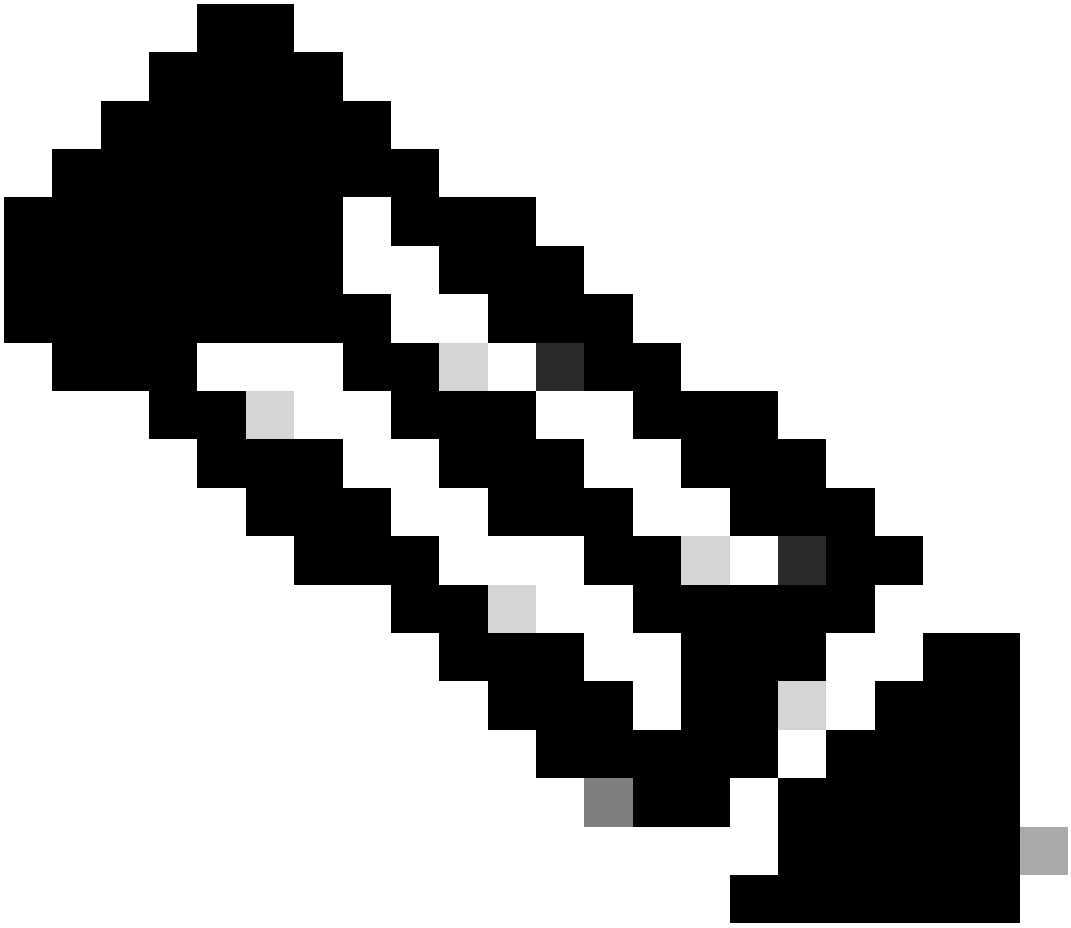
Je strategie om schurken te bestrijden hangt af van een paar factoren. Veel beheerders gaan instinctief voor zeer strikte regels, maar de belangrijkste vragen zijn:

- Wanneer je honderden (zo niet duizenden) frauduleuze waarschuwingen krijgt, heb je dan

de menselijke hulpbronnen om ze allemaal te bekijken en actie te ondernemen tegen ze allemaal?

- Is uw doel om fysiek de schurken te verwijderen om een schoon RF-spectrum te houden? Als dat zo is, heb je veel mensen nodig om deze operatie uit te voeren. Of misschien is je doel om alleen de veiligheidsfactor in de gaten te houden en ervoor te zorgen dat de schurken geen gevaar vertegenwoordigen? Dit heeft een veel hanteerbaarder menselijke werkkosten.
- Het toelaten van schurkendetectie kan een impact hebben op uw airtime en schurkeninsluiting heeft doorgaans een nog grotere impact, hebt u deze impact geanalyseerd en rekening gehouden met het?

Wat de impact van schurkendetectie betreft, hebben de 9120 en 9130s een speciale CleanAir chip die zorgt voor de off-channel scanning (en dus schurkendetectie) waardoor de impact op de client-dienen radio bijna nul. AP9160-serie met hun CleanAir Pro-chip heeft een vergelijkbare no-impact scanfunctie, maar andere APs die niet de CleanAir-chip hebben moeten hun client-bediende radio off-channel nemen om te scannen op schurken of om insluiting te doen. Het AP-model dat u gebruikt speelt daarom een rol in de beslissing om speciale monitor-mode AP's te gebruiken voor fraudedetectie en insluiting of niet.

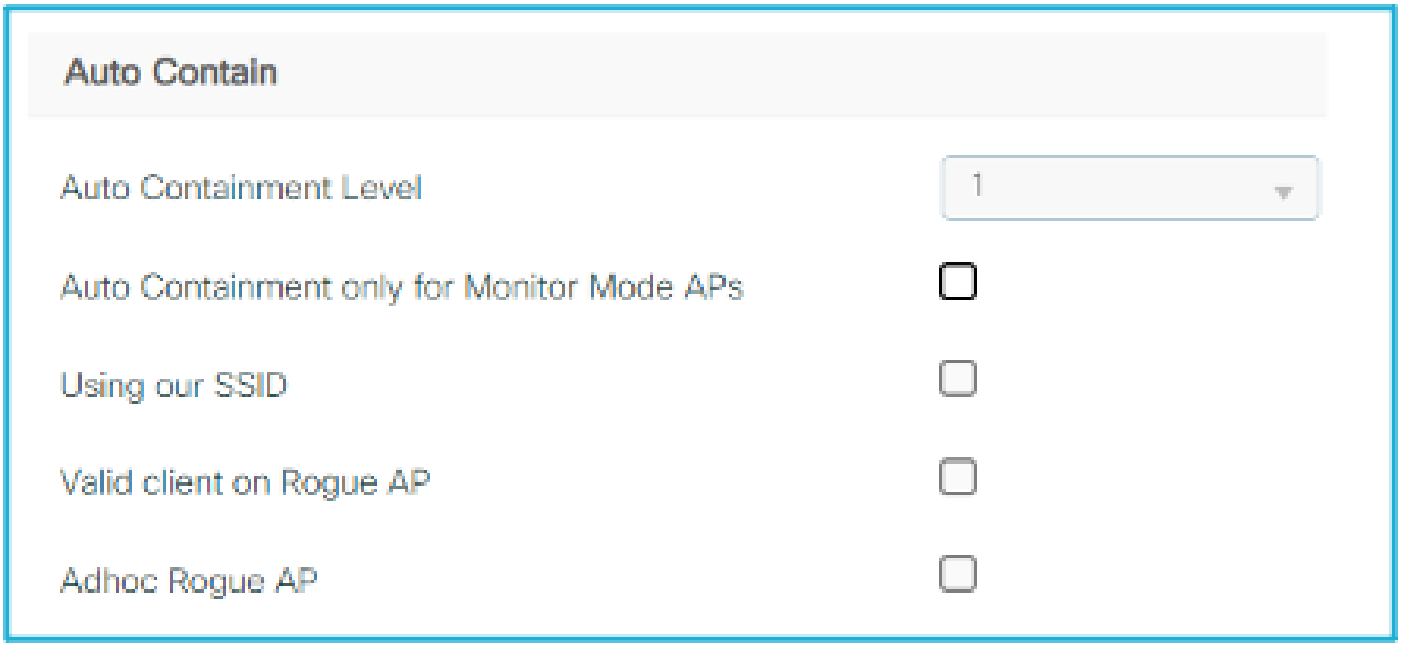


Opmerking: mobiele telefoons die een Wi-Fi-hotspot delen, werken in de ‘infrastructuur’-modus, net als traditionele AP's, ‘ad-hoc’-modus verwijst naar een directe verbinding tussen mobiele apparaten en is minder gebruikelijk.

Bedrieglijke insluiting wordt vaak verboden door regelgeving, dus het is essentieel dat u bij uw lokale overheid controleert voordat u het inschakelt. Het bevatten van een schurk betekent niet het afsluiten van de schurk op afstand maar spamming van de clients die proberen te verbinden met het schurkentoegangspunt met deauthenticatie frames zodat ze niet verbinden. Dit kan alleen werken op bestaande security SSID (het werkt niet in WPA3 of wanneer PMF is ingeschakeld in WPA2) omdat uw access points de deauthenticatie frames niet goed kunnen ondertekenen. Insluiting heeft een negatieve invloed op RF-prestaties op het doelkanaal, aangezien uw AP’s de airtime vullen met deauthenticatie frames. Het moet daarom alleen worden beschouwd als een veiligheidsmaatregel om te voorkomen dat uw eigen legitieme klanten per ongeluk met een bedrieglijk toegangspunt in contact komen. Om alle genoemde redenen, wordt het aanbevolen om geen insluiting te doen, aangezien het niet volledig het schurkenprobleem op te lossen en veroorzaakt meer RF-problemen. Als u insluiting moet gebruiken, is het alleen zinvol om het in te schakelen voor schurken die een van uw beheerde SSID bederven als het is een onmiskenbare

honeypot aanval.

U kunt automatische insluiting configureren met de optie "gebruik van onze SSID's":



Auto bevat instellingen

U kunt ook schurkenregels configureren om te classificeren als kwaadaardige schurkentoegangspunten volgens uw eigen criteria. Vergeet niet om de naam van uw naburige en goedgekeurde SSID's als vriendelijke schurken in te voeren om die te verwijderen uit uw alarmlijst.

AP-verificatie of PMF inschakelen om uw AP's te beschermen tegen imitatie.

Een bekabelde schurk is een schurkentoegangspunt verbonden met uw bekabeld netwerk, wat duidelijk een verhoogde veiligheidsdreiging is. Detectie van bekabelde schurken is gecompliceerder omdat het Ethernet MAC-adres van een schurk doorgaans verschilt van het radio MAC-adres. Cisco Catalyst Center heeft algoritmen die nog steeds proberen te detecteren of een schurk is bekabeld en zoekt naar schurkenclient-MAC's die zowel via de ether worden gehoord als op de bekabelde infrastructuur worden gezien. De beste oplossing om bedrade schurken helemaal te voorkomen is om al uw switchpoorten te beveiligen met 802.1X-verificatie.

Als u fysiek gaat optreden op een bedrieglijk access point, is het benutten van Cisco-ruimtes van cruciaal belang om een nauwkeurige locatie van de bedrieger te hebben. Je moet waarschijnlijk nog steeds één keer zoeken op de site als mensen de neiging hebben om schurken APs soms te verbergen, maar het beperken van het zoekgebied tot een paar meter maakt het een zeer haalbare onderneming. Zonder Spaces wordt de schurk getoond op de kaart naast de AP die het het luidst detecteert, wat zorgt voor een vrij groot zoekgebied. Er bestaan veel draadloze gereedschappen en apparaten die u het signaal van het bedrieglijke access point in real time tonen om u te helpen de bedrieger fysiek te lokaliseren.

Niet precies verwant aan schurken, maar omdat CleanAir net was afgedekt, is het belangrijk om op te merken dat het inschakelen van CleanAir geen merkbare negatieve invloed heeft op prestaties behalve BLE-beacon detectie, aangezien dit invloed heeft op 2.4GHz prestaties. U kunt

uw draadloze verbinding configureren om Bluetooth-interferers volledig te negeren, aangezien ze alomtegenwoordig zijn in de wereld van vandaag, en u kunt niet voorkomen dat uw klanten hun Bluetooth inschakelen.

WiPS

WiPS bestrijkt meer geavanceerde aanvalsvectoren dan alleen het detecteren van de aanwezigheid van een niet-geautoriseerd schurkenapparaat. Naast deze aanvallen, biedt het soms ook een PCAP van het evenement voor forensische analyse.

Terwijl dit een zeer nuttige veiligheidseigenschap voor de onderneming is, moet een openbaar-onder ogen ziet netwerk de eeuwige vraag onder ogen zien: wat te doen tegen het?

Met de moeilijkheid van het beheren van vele cliënten die u niet controleert, is het mogelijk om het alarm in twee categorieën te verdelen. De alarmen die u kunt negeren vanuit Cisco Catalyst Center als u er te veel ziet, zijn:

- 10001: DoS: Verificatie Overstromingsalarm
- 10002: DoS: Associatieaanvraag Alarmmelding
- 10003: DoS: Alarmmelding tegen overstromingen door radio-uitzendingen
- 10004: DoS: Alarmmelding tegen overstromingen
- 10005: DoS: Uitzending Dis-Associatie Alarmsignaal
- 10006: DoS: De-authenticatie van de overstromingsalarmmelding
- 10007: DOS: ontruimingsalarm voor uitzendingen
- 10008: DOS: alarmlampje bij afmelding van afmelding
- 10009: Overstromingsalarm CTS
- 10010: RTS-associatie-alarmmelding
- 10011: Deauthenticatie overstroming door paar
- 10021: Airdrop-sessie (deze is meestal veel in elk netwerk en toont gewoon regelmatige peer-to-peer activiteit tussen Apple-apparaten)
- 10022: Verzoek misvormde associatie
- 10023: Verificatiefout overstroming door handtekening
- 10024: Ongeldig MAC OUI door Handtekening
- 10025: foutieve verificatie

Deze alarmen kunnen mogelijk worden veroorzaakt door een slecht gedragscliënt. Het is niet mogelijk om een denial-of-service-aanval automatisch te voorkomen, omdat u in wezen niet kunt voorkomen dat een defecte klant de airtime bezet houdt. Zelfs als de infrastructuur de klant negeert, zou het nog steeds in staat zijn om het medium en de zendtijd te gebruiken om te verzenden, waardoor de prestaties van de klanten eromheen beïnvloed worden.

De andere alarmen zijn zo specifiek dat ze hoogstwaarschijnlijk een echte kwaadaardige aanval afschilderen en kunnen nauwelijks gebeuren door slechte cliëntbestuurders. Het is beter deze alarmen te blijven volgen:

- 10012: Fuzzed beacon
- 10013: Fuzzed Probe-verzoek

- 10014: Gefluzeerde sonde-respons
- 10015: PS Poll Flood by Signature
- 10016: EAPOL start V1 overstroming door ondertekening
- 10017: Reassociatieverzoek overstroming per bestemming
- 10018: Beacon Flood by Signature
- 10019: Probe Response Flood by Destination
- 10020: Blok tegen overstromingen door ondertekening
- 10026/10027: RTS- en CTS Virtual Carrier Sense Attack

De draadloze infrastructuur kan soms mitigatiemaatregelen nemen zoals het blokkeren van de lijst van het beledigende apparaat, maar de enige echte actie om van zo'n aanval af te komen is om er fysiek heen te gaan en het beledigende apparaat te verwijderen.

Aanbevolen wordt om alle vormen van uitsluiting van cliënten toe te laten om verspilde zendtijd te besparen door interactie met defecte cliënten.

Clienttoegang beperken

Het is raadzaam om peer-to-peer blokkering op al uw WLAN's mogelijk te maken (tenzij u een harde eis hebt voor client-to-client communicatie - maar dit moet zorgvuldig worden overwogen en mogelijk beperkt). Deze eigenschap verhindert cliënten op zelfde WLAN elkaar te contacteren. Dit is geen perfecte oplossing, omdat clients op verschillende WLAN's nog steeds contact met elkaar kunnen opnemen en klanten die tot verschillende WLC's in de mobiliteitsgroep behoren, ook deze beperking kunnen omzeilen. Maar het fungeert als een eenvoudige en efficiënte eerste laag van beveiliging en optimalisatie. Nog een voordeel van deze eigenschap van peer-to-peer blokkering is dat het ook client-to-client ARP voorkomt die verhindert dat toepassingen andere apparaten op het lokale netwerk ontdekken. Zonder peer-to-peer blokkering, kan het installeren van een eenvoudige toepassing op de client alle andere clients tonen die in het net zijn verbonden met mogelijk hun IP-adres en hostnamen.

Bovendien wordt aanbevolen om zowel een IPv4 als een IPv6 (als u IPv6 in uw netwerk gebruikt) ACL op uw WLAN's toe te passen om client-to-clientcommunicatie te voorkomen. Het toepassen van een ACL die client-naar-client communicatie op WLAN-niveau blokkeert, werkt ongeacht of u client-SVI's hebt of niet.

De andere verplichte stap is om draadloze client toegang tot elke vorm van beheer van uw draadloze controller te voorkomen.

Voorbeeld:

```
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
```

Deze ACL kan worden toegepast op de beheerinterface SVI:

```
interface Vlan130

 ip access-group ACL_DENY_CLIENT_VLANS in
```

Dit gebeurt op een WLC met client-VLAN's 131 tot 137 die in Layer 2 VLAN-database zijn gemaakt, maar zonder bijbehorende SVI's, en er is slechts één SVI voor VLAN 130, hoe de WLC wordt beheerd. Deze ACL verhindert dat alle draadloze clients elk verkeer naar de WLC-beheer- en besturingsplanen volledig kunnen verzenden. Vergeet niet dat SSH- of Web UI-beheer niet het enige is dat u moet doorlaten, aangezien een CAPWAP-verbinding met alle AP's ook toegestaan moet worden. Dit is de reden waarom deze ACL een standaardvergunning heeft, maar blokkeert draadloze clientbereiken, in plaats van te vertrouwen op een standaard ontkennen alle actie die zou vereisen om alle toegestane AP-subnetbereik en beheerbereiken te specificeren.

Op dezelfde manier kunt u een andere ACL maken die alle mogelijke beheersubnetten specificeert:

```
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
```

U kunt deze ACL vervolgens toepassen voor CLI-toegang:

```
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
```

Dezelfde ACL kan ook worden toegepast voor toegang tot webbeheer.

Bescherming tegen verkeersstormen

Multicast en uitzendingen worden zwaarder gebruikt door sommige toepassingen dan anderen. Wanneer het overwegen van een telegraferen-slechts netwerk, is het beschermen tegen uitzendingsonweer vaak de enige voorzorgsmaatregel die wordt genomen. Een multicast is echter net zo pijnlijk als een uitzending wanneer deze via de ether wordt uitgezonden en het is belangrijk om te begrijpen waarom. Stel je eerst een pakket voor dat wordt verzonden (via broadcast of multicast) naar al je draadloze klanten, dat snel optelt bij veel bestemmingen. Elke AP moet dan dit frame over de lucht op de meest betrouwbare manier (hoewel het niet gegarandeerd zo betrouwbaar) en dat wordt bereikt door gebruik te maken van een verplichte datasnelheid (soms de laagste, soms is het configureerbaar). In de termen van leken betekent dit dat frame wordt verzonden met behulp van een OFDM (802.11a/g) data rate, die duidelijk niet groot is.

In een groot openbaar netwerk, is het niet aangeraden om te vertrouwen op multicast om airtime te bewaren. In een groot ondernemingsnetwerk kunt u echter een vereiste hebben om multicast ingeschakeld te houden voor een specifieke toepassing, hoewel u het zoveel mogelijk moet controleren om de impact ervan te beperken. Het is een goed idee om het toepassingsdetail, multicast IP, te documenteren en ervoor te zorgen om andere vormen van multicast te blokkeren. Het inschakelen van multicast-doorsturen is geen vereiste voor het inschakelen van IPv6, zoals eerder is uitgelegd. Doorsturen van uitzendingen kan het best volledig uitgeschakeld worden gehouden. Uitzendingen worden soms gebruikt door toepassingen om andere apparaten op hetzelfde subnetje te ontdekken, wat duidelijk een beveiligingsprobleem is in een groot netwerk.

Als u wereldwijde multicast doorsturen inschakelt, zorg er dan voor dat u multicast-multicast AP CAPWAP-instelling gebruikt. Met dit toegelaten, wanneer WLC een multicast pakket van de getelegrafeerde infrastructuur ontvangt, verzendt het het naar alle geïnteresseerde APs met één enkel multicast pakket, die op veel pakketverdubbeling opslaan. Zorg ervoor dat u een andere CAPWAP multicast IP instelt voor elk van uw WLC's, anders ontvangen AP's multicast verkeer van andere WLC's, wat niet gewenst is.

Als uw AP's zich in andere subnetten bevinden vanaf uw draadloze beheerinterface van de WLC (wat waarschijnlijk in een groot netwerk is), moet u multicast routing op uw bekabelde infrastructuur inschakelen. U kunt verifiëren dat al uw APs correct het multicast verkeer met het bevel ontvangen:

```
show ap multicast mom
```

IGMP (voor IPv4 multicast) en MLD (voor IPv6) multicast worden ook geadviseerd om in alle gevallen te worden ingeschakeld als u op multicast moet vertrouwen. Zij staan slechts de geïnteresseerde draadloze cliënten (en daarom slechts APs die geinteresseerde cliënten) hebben toe om het multicast verkeer te ontvangen. De WLC proxies de registratie aan het multicast verkeer en zorgt ervoor dat de registratie levend wordt gehouden, waarbij de klanten worden geoffload.

Conclusie

Grote publieke netwerken zijn complex, elk ervan is uniek met specifieke eisen en resultaten.

Het naleven van de richtlijnen in dit document is een geweldig uitgangspunt en helpt om succes te bereiken met uw implementatie, terwijl de meest voorkomende problemen worden vermeden. De richtsnoeren zijn echter slechts richtsnoeren en kunnen worden geïnterpreteerd of aangepast in het kader van de specifieke lokatie.

Cisco CX beschikt over teams van draadloze professionals die zich toeleggen op grote draadloze implementaties, met ervaring in tal van grote evenementen, waaronder sportevenementen en conferenties. Neem contact op met uw accountteam voor verdere assistentie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.