Invoering van IP-telefoon in WAP-infrastructuur

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Conventies
Samenvatting
Overzicht van videogateway
Aandacht voor spraakcapaciteit
Capaciteit van videocommunicatieserver
De Vocera-oplossing
Infrastructuurplanning in Videoera
Overzicht van architectuur
Multicast voor toepassingen van LWAPP
Unicast-multicast levermethode
Multicast voor leveranciers
Configuratie van router en Switch-multicast
IP-multicast routing inschakelen
PIM op een interface inschakelen
Switch VLAN IGMP-signalering uitschakelen
Verbeteringen in multicast versie 4.0.206.0 en hoger
Plaatsingsscenario's
Implementatie van één controller
Meervoudige controller op Layer 2 implementatie
Meervoudige controller op Layer 3 implementatie
VoWLAN-implementaties Aanbevolen van Cisco
Aanbevelingen voor gebouwen op meerdere vloeren, ziekenhuizen en pakhuizen
Ondersteunde beveiligingsmechanismen
LEAP-overwegingen
Draadloze netwerkinfrastructuur
Voice-, data- en VLAN's
Netwerkgrootte
Aanbevelingen voor switch
implementaties en configuratie
Configuratie pagina
Tune AutoRF voor uw omgeving
Configuratie van draadloze netwerkinfrastructuur
Interfaces maken

De Vocera-spraakinterface maken
Draadloze specifieke configuratie
WLAN-configuratie
Detectie access point instellen
De 802.11b/g radio configureren
Verificatie van draadloze IP-telefonie
Associatie, verificatie en registratie
Gemeenschappelijke roaming-problemen
De band verliest verbinding met het netwerk of de spraakservice is verloren bij het roaming
Brug verliest spraakkwaliteit bij roaming
Audio-problemen
eenzijdig geluid
Choppy of Robotic Audio
Problemen met registratie en verificatie
Bijlage A
Plaatsing van AP en antenne
Interferentie en multipath-verstoring
Signaal
Gerelateerde informatie

Inleiding

Dit document bevat ontwerpoverwegingen en implementatierichtlijnen voor de implementatie van de Vocera® Band Voice over WLAN-technologie (VoWLAN) op de Cisco Unified Wireless Network-infrastructuur.

Opmerking: Ondersteuning voor Vocera-producten dient rechtstreeks te worden verkregen via de Vocera-ondersteuningskanalen. Cisco Technical Support is niet getraind om kwesties te ondersteunen die te maken hebben met vakantie.

Deze handleiding is een aanvulling op de Cisco Wireless LAN Controller Deployment Guide en richt zich alleen op de configuratieparameters die specifiek zijn voor Vocera VoWLAN-apparaten in een lichtgewicht architectuur. Raadpleeg het gedeelte Cisco 440X Series draadloze LAN-controllers voor meer informatie.

Voorwaarden

Vereisten

Het wordt verondersteld dat de lezers bekend zijn met de termen en concepten die in de Cisco IP-telefonie SRND en de Cisco Wireless LAN SRND worden gepresenteerd. .

Draadloze UC-ontwerphandleiding—
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_wireless_uc.html

Cisco Unified Communications SRD op basis van Cisco Unified Communications Manager 7.x-
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_uc_mgr.html

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Samenvatting

Deze tabel geeft een samenvatting van de vier hoofdfuncties en hoe deze zich binnen een Cisco Unified Wireless-netwerk gedragen.

	Enkelvoudige controller	Controller-to-Controller Layer 2 roaming	Controller-to-Controller Layer 3 roaming
Badge-to-Badge	Geen speciale configuratie	Geen speciale configuratie	Geen speciale configuratie
Pad-to-Phone	Geen speciale configuratie	Geen speciale configuratie	Geen speciale configuratie
Badge-to-Broadcast	Controller multicast inschakelen	Schakel Controller multicast Uitschakelen van VLAN IGMP-Snooping in of gebruik 4.0.206.0 of hoger	4.0.206.0 of later
Bandlocatie	Geen speciale configuratie	Geen speciale configuratie	Geen speciale configuratie

Overzicht van videogateway

De communicatiespecges maken het mogelijk dat de communicatie aan toonder met elke andere gebruiker van de badge, alsook met de integratie van de Private Branch Exchange (PBX) en het volgen van de locatie van de badge plaatsvindt. Het gebruik van een 802.11b/g draadloos netwerk vereist het gebruik van multicast en UDP unicast pakketlevering met beperkte vereisten voor Quality of Service (QoS) vanaf Vocera Server Software release 3.1 (Compilatie 1081). De coderingsmogelijkheden zijn 64/128-bits Wired Equivalent Privacy (EVN), Temporal Key Integrity Protocol (TKIP), Message Integrity Control (MIC) en Cisco Temporal Key Integrity Protocol (CKIP) gecombineerd met de verificatiemogelijkheden van Open, Wi-Fi Protected Access-Pre-Shared Key (WAP-PSK), WPEAP-Protected Extensible Authentication Protocol (EXTRA) Lichtgewicht

Extensible Authentication Protocol (LEAP).

Met het indrukken van een knop reageert de Vocera-server op Vocera, wat een aansporing is om opdrachten zoals record uit te geven, waar (am I) /..., aanroepen, spelen, **uitzenden**, **berichten** enzovoort. De Vocera-server biedt de benodigde services en/of CallConnector om het verzoek te voltooien.

Het 802.11b-kabelcommunicatiesysteem van Vocera maakt gebruik van een eigen spraakcompressie en het gebruik van een UDP-poortbereik. De software van het Systeem van Vocera loopt op een server van Windows die de vraag, ingesteld, verbinding en gebruikersprofielen beheert. Ze hebben samengewerkt met de software van Nuance 8.5 Speech Recognition en Voices om spraakcommunicatie mogelijk te maken. Vocera raadt een afzonderlijke Windows-server aan om de software voor Vocera Telephony Solutions te gebruiken om POTS-connectiviteit (Plain Old Telephone Service) met de badges mogelijk te maken.

Aandacht voor spraakcapaciteit

Zie het gedeelte Netwerkgrootte van dit document voor meer informatie.

Capaciteit van videocommunicatieserver

Raadpleeg de specificaties van het Vocera Communications System voor meer informatie over de matrixprinter Videoserver.

De Vocera-oplossing

Het Vocera Badge gebruikt zowel de levering van het unicast- als het multicast-pakket om verscheidene zeer belangrijke eigenschappen te leveren die deze volledige oplossing vormen. Hier zijn vier van de essentiële functies die afhankelijk zijn van een juiste pakketlevering. Tevens wordt een basisbegrip verschaft van de wijze waarop elke functie het onderliggende netwerk voor levering en functionaliteit gebruikt.

- Badge to Badge Communications—Wanneer een Vocera-gebruiker een andere gebruiker belt, contacteert de badge eerst de Vocera-server, die het IP-adres van de badge van de telefoon bekijkt en de gebruiker contacteert om de gebruiker te vragen of zij een gesprek kunnen voeren. Als de telefoon de vraag accepteert, meldt de server van Vocera de aanroepende badge van het IP adres van het kaartenadres aan opstelling directe communicatie tussen de badges zonder verdere serverinterventie. Alle communicatie met de Vocera-server gebruikt de G.711-codec en alle badge-to-badge communicatie gebruikt een eigen codec van Vocera.
- Telefoniecommunicatie-wanneer een Vocera-telefonieserver is geïnstalleerd en geïnstalleerd met een verbinding naar een PBX-systeem, kan een gebruiker interne uitbreidingen van PBX of externe telefoonlijnen bellen bellen. Vocera stelt gebruikers in staat om te bellen door de nummers (5, 6, 3, 2) te zeggen of door een adresboekingang in de Vocera-database te creëren voor de persoon of functie op dat nummer (bijvoorbeeld apotheek, huis, pizza) bepaalt de Vocera-server het nummer dat wordt opgeroepen, door de getallen in de extensie te onderscheppen of door de naam in de database op te zoeken en het nummer te selecteren. De Vocera-server geeft die informatie vervolgens door naar de Vocera-telefonieserver, die op

PBX aansluit en de juiste telefoniesignalering genereert (bijvoorbeeld DTMF). Alle communicatie tussen de badge- en Vocera-server en Vocera-telefonieserver en Vocera-telefonieserver gebruikt de G.711-codec via unicast UDP.

- De gebruiker van het Vocera Broadcast-A Vocera Badge kan tegelijkertijd een groep Vocera-badge-gebruikers bellen en communiceren met de opdracht Broadcast. Wanneer een gebruiker naar een groep uitzendt, stuurt de badge van de gebruiker het bevel naar de server van het Vocera die dan de leden van een groep bekijkt, bepaalt welke leden van de groep actief zijn, wijst een multicast adres toe om voor deze uitzending te gebruiken en stuurt een bericht naar de badge van elke actieve gebruiker die het om bij de multicast groep met het toegewezen multicast adres vertelt.
- Plaats van de pagina Functie - de server van de Vocera houdt van het toegangspunt waaraan elke actieve badge wordt geassocieerd aangezien elke badge een 30 seconden lang levend aan de server met de verbonden BSSID verstuurt. Hierdoor kan het Vocera-systeem de locatie van een badge-gebruiker ruwweg inschatten. Deze functie heeft een relatief lage nauwkeurigheid omdat een Badge misschien niet gekoppeld is aan het toegangspunt dat het dichtst bij deze functie staat.

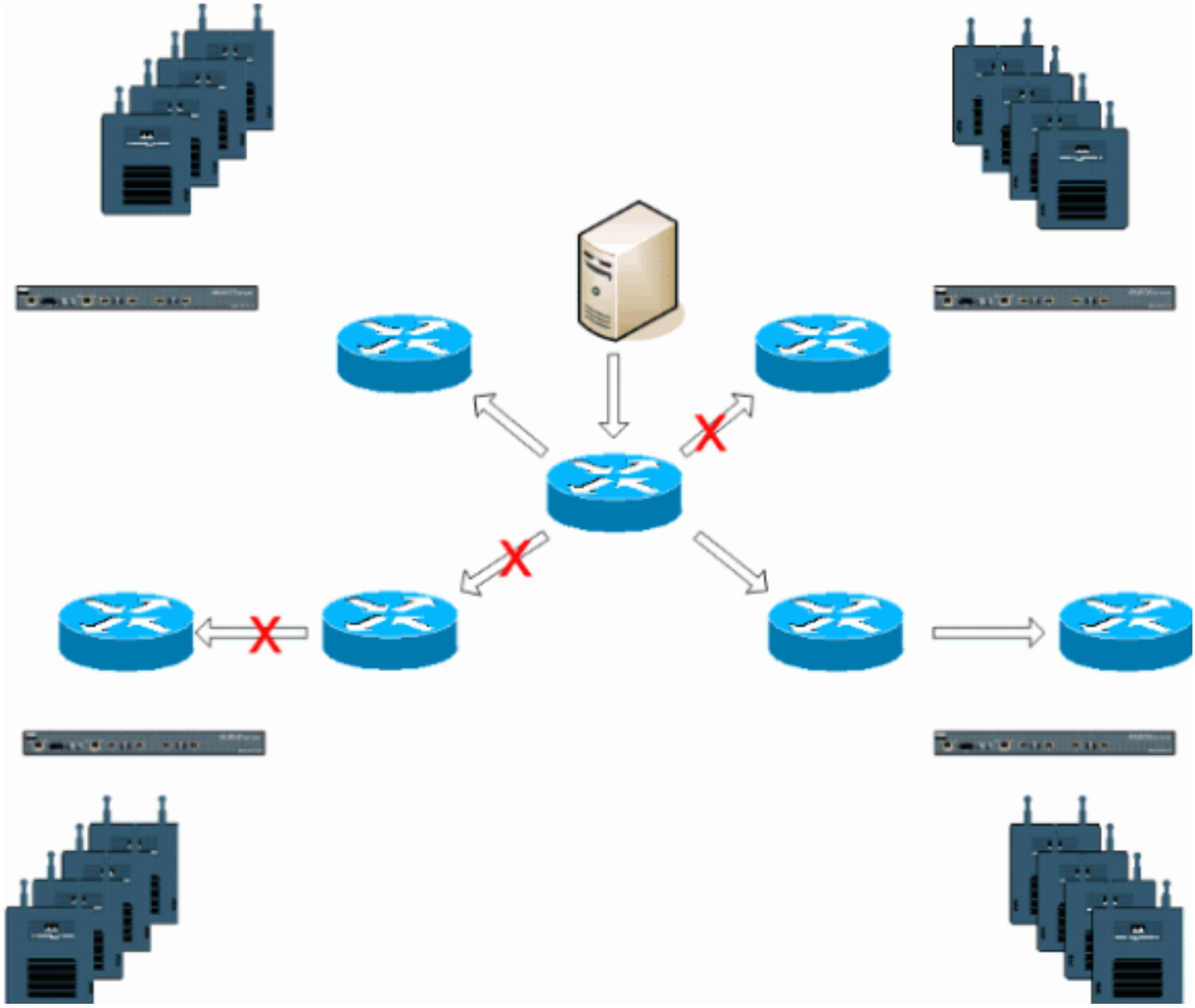
Infrastructuurplanning in Videoera

In de Vocera whitepaper Vocera Infrastructure Planning Guide worden de minimumeisen beschreven voor de plaatsenquête die aantonen dat de badge een signaalsterkte van minimaal -65 dBm moet hebben, een signaal-ruisverhouding van meer dan 25 db en een goede toegangspunten en kanaalscheiding. Hoewel de badges een soortgelijke omnidirectionele antenne als een notitieboek gebruiken dat gebruikt wordt voor een locatieonderzoek, bootst het gedrag van de badge niet goed na, gezien de effecten van de slijters op de signaalsterkte. Gezien deze unieke vereiste en dit gedrag van het verzendende apparaat, is het gebruik van de Cisco Architecture and Radio Resource Management ideaal om er zeker van te zijn dat er een gebrek is aan ongebruikelijke RF-kenmerken (radiofrequentie).

De Vocera-badge is een toestel met een laag vermogen, dat naast het lichaam wordt gedragen met beperkte signaalfoutcorrectiefuncties. De Vocera-eisen in dit document kunnen eenvoudig worden verwezenlijkt. Het kan echter overweldigd worden als er te veel SSID's zijn om het te verwerken en de badge effectief te laten werken.

Overzicht van architectuur

Afbeelding 1-General Multicast Forward en Prune met lichtgewicht access point Protocol (LWAPP) draadloos



Multicast voor toepassingen van LWAPP

Het begrijpen van multicast in een LWAPP-toepassing is noodzakelijk om de Vocera-uitzending-functie in te zetten. Dit document bevat later de essentiële stappen om multicast in de op een controller gebaseerde oplossing mogelijk te maken. Er zijn momenteel twee leveringsmethoden die de LWAPP-controller gebruikt om multicast aan de klanten te leveren:

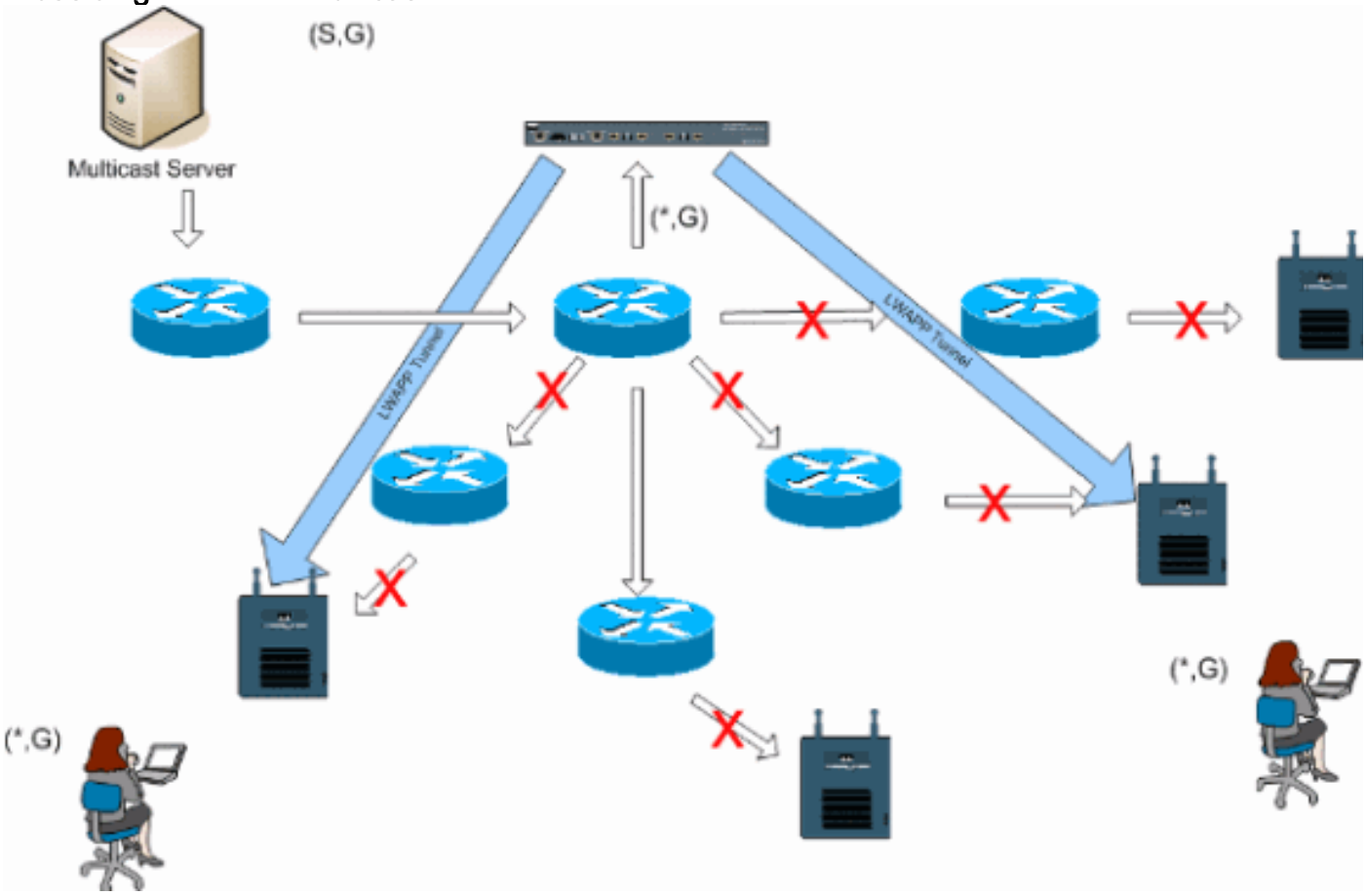
- Unicast-multicast
- Multicast voor multicast

Unicast-multicast levermethode

De unicast-multicast leveringsmethode creëert een kopie van elk multicast pakket en zendt het naar elk access point. Wanneer een client een multicast verbinding naar het draadloze LAN verstuurt, wordt dit toegangspunt doorgestuurd naar de LWAPP-tunnel naar de controller. De controller verbindt deze multicast zich aan tot het is direct verbonden lokale netwerkverbinding die het standaard VLAN is voor de verbonden WLAN van de client. Wanneer een IP multicast pakket van het netwerk naar de controller komt, repliceert de controller dit pakket met een LWAPP-header voor elk access point dat een client heeft binnen het draadloze domein dat zich heeft aangesloten bij deze specifieke groep. Wanneer de bron van de multicast ook een ontvanger

binnen het draadloze domein is, wordt dit pakket ook gedupliceerd en teruggestuurd naar dezelfde client die dit pakket heeft verzonden. Voor Vocera-badges is dit niet de voorkeurmethode voor multicast-levering binnen de LWAPP-controlleroplossing. De unicast-leveringsmethode werkt met kleine implementaties. Echter, door de aanzienlijke overhead op de Wireless LAN Controller (WLC) is dit nooit de aanbevolen multicast leveringsmethode.

Afbeelding 2-LWAPP multicast



Opmerking: Als AP Group VLAN's zijn geconfigureerd en een IGMP-verbinding van een client via de controller wordt verzonden, wordt deze geplaatst op het standaard VLAN van de WLAN-client waarop de client is geactiveerd. Daarom zou de client dit multicast verkeer niet kunnen ontvangen tenzij de client lid is van dit standaard uitzenden domein.

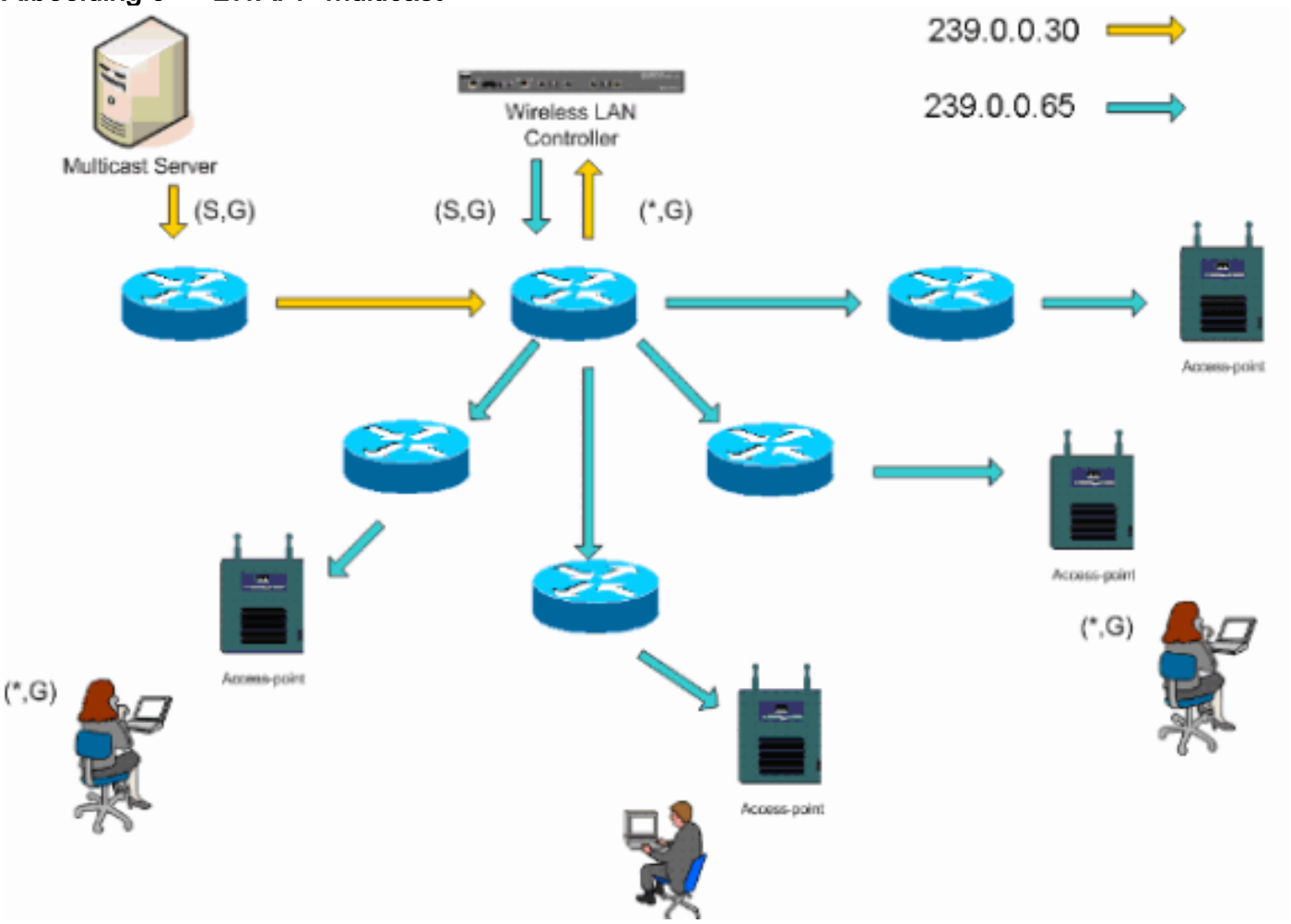
Multicast voor leveranciers

De multicast-multicast leveringsmethode vereist niet dat de controller elk ontvangen multicast pakket repliceert. De controller is ingesteld voor een niet-gebruikt multicast adres waar elk access point lid van wordt. Met afbeelding 3 is de multicast groep die van de WLC naar het access point is gedefinieerd, 239.0.65. Wanneer een client een multicast verbinding naar de WLAN-server verstuurt, zendt het access point dit onderdeel via de LWAPP-tunnel naar de controller. De controller stuurt dit link-laagprotocol door naar de direct aangesloten lokale netwerkverbinding die het standaard VLAN is voor de bijbehorende WLAN-client. De router die lokaal is aan de controller voegt vervolgens dit multicast groepsadres toe aan die interface voor het verzenden (*,G). Met afbeelding 3 werd de voorbeeld-multicast verbinding verzonden naar de multicast groep 239.0.30. Wanneer het netwerk nu multicast verkeer doorstuurt, wordt het multicast adres van 239.0.30 doorgestuurd naar de controller. De controller kapselt vervolgens het multicast pakket in een LWAPP multicast pakket dat is gericht op het multicast groepsadres (bijvoorbeeld hier is 239.0.0.65) dat is ingesteld op de controller en naar het netwerk wordt doorgestuurd. Elk toegangspunt op de controller ontvangt dit pakket als lid van de multicast-groep van controllers.

Het access point geeft vervolgens het multicastpakket klanten/servers door (hier is bijvoorbeeld 239.0.30) als een uitzending naar de WLAN/SSID die binnen het multicast Packet van LWAPP is geïdentificeerd.

N.B.: Als u het multicast netwerk niet correct configureren, kunt u multicast-pakketten van een ander controller ontvangen. Als de eerste controller dit multicast pakket moet fragmenteren, wordt het fragment naar het netwerk verzonden en moet elk access point tijd besteden om dit fragment te laten vallen. Als u al verkeer zoals iets van het multicast bereik 224.0.0.x toestaat, wordt dit ook ingekapseld en vervolgens door elk access point doorgestuurd.

Afbeelding 3 — LWAPP-multicast



Configuratie van router en Switch-multicast

Dit document is geen multicast netwerkconfiguratiegids. Raadpleeg IP-multicast routing configureren voor een compleet implementatieverhaal. Dit document bestrijkt de basisbeginselen om multicast in uw netwerkomgeving mogelijk te maken.

IP-multicast routing inschakelen

IP multicast routing stelt de Cisco IOS®-software in staat multicast pakketten naar voren te sturen. Het **IP multicast-routing** wereldwijde configuratieopdracht is nodig om multicast in een multicast geactiveerd netwerk te laten functioneren. De **ip multicast-routing** opdracht moet op alle routers in uw netwerk worden ingeschakeld tussen de WLC(s) en hun respectievelijke access points.

```
Router(config)#ip multicast-routing
```

PIM op een interface inschakelen

Dit maakt de routing interface mogelijk voor IGMP-handeling (Internet Group Management Protocol). De modus Protocol Independent Multicast (PIM) bepaalt hoe de router zijn multicast routingtabel bevolkt. Het hier gegeven voorbeeld vereist niet dat het rendezvous point (RP) bekend is voor de multicast groep en daarom is de sparse-dense-modus het meest wenselijk gezien de onbekende aard van uw multicast omgeving. Dit is geen multicast aanbeveling die moet worden geconfigureerd om te werken, hoewel de Layer 3-interface die direct op uw controller is aangesloten, PIM ingeschakeld moet zijn om multicast te laten functioneren. Alle interfaces tussen uw WLC(s) en hun respectieve access points moeten worden ingeschakeld.

```
Router(config-if)#ip pim sparse-dense-mode
```

Switch VLAN IGMP-signalering uitschakelen

IGMP-snooping maakt een geschakeld netwerk met multicast ingeschakeld om verkeer te beperken tot die knooppunten die multicast willen zien terwijl u de multicast-pakketten uit switchpoorten die de multicast-stream niet willen zien, wilt afdrukken. Bij een Vocera-inzet kan het ongewenst zijn om CGMP of IGMP in te schakelen door de upstream-schakelaar naar de controller met softwarereleases eerder dan 4.0.206.0.

Roaming en multicast worden niet gedefinieerd met een reeks vereisten om te controleren of multicast verkeer een geabonneerde gebruiker kan volgen. Hoewel de client-badge zich ervan bewust is dat het is gedraaid, wordt er niet nog een IGMP-verbinding verzonden om er zeker van te zijn dat de netwerkinfrastructuur het multicast (Vocera-uitzending) verkeer naar de badge blijft doorgeven. Tegelijkertijd stuurt het LWAPP access point geen algemene multicast query naar de geroamde client om dit IGMP aan te vragen. Met een ontwerp van het Vocera-netwerk van Layer 2 maakt het inschakelen van IGMP-snooping het doorsturen van verkeer naar alle leden van het Vocera-netwerk mogelijk, ongeacht de plaats waar het beweegt. Dit waarborgt dat de uitzendfunctie van Vocera werkt ongeacht de plaats waar de klant beweegt. Wereldwijd snooping door IGMP uitschakelen is een zeer onwenselijke opgave. Aanbevolen wordt om IGMP-snooping alleen uit te schakelen op het VLAN dat rechtstreeks op elke WLC is aangesloten.

Zie IGMP-signalering configureren voor meer informatie.

```
Router(config)#interface vlan 150
Router(config-if)#no ip igmp snooping
```

Verbeteringen in multicast versie 4.0.206.0 en hoger

Met de release van 4.0.206.0 introduceert Cisco een IGMP-query om gebruikers toe te staan om te roamen op Layer 2 door een algemene IGMP-query te verzenden wanneer dit gebeurt. De client reageert dan met de IGMP-groep dat ze lid zijn van de projector en dit wordt aangesloten op het bekabelde netwerk zoals eerder in dit document beschreven. Wanneer een client naar een controller stroomt die geen Layer 2 connectiviteit heeft, of een Layer 3 straal, wordt de synchrone routing toegevoegd voor multicast bronpakketten. Wanneer een client, die een Layer 3-routebronnen heeft voltooid, een multicastpakket van het draadloze netwerk inkapselt de buitenlandse controller dit pakket in de Ethernet-over-IP (EoIP) in IP-tunnel naar de

ankercontroller. De ankercontroller stuurt dan door dat naar de draadloze client lokaal gekoppeld, en overbrugt deze terug naar het bekabelde netwerk waar deze wordt routeerd met behulp van normale multicast-routingmethoden.

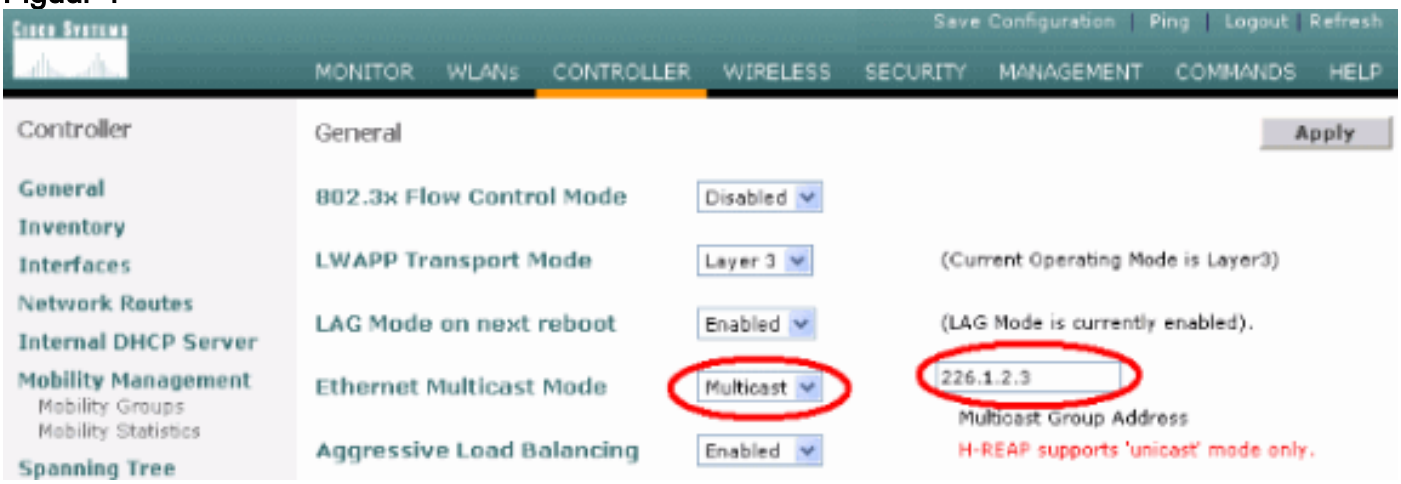
Plaatsingsscenario's

Deze drie inzetscenario's bestrijken beste praktijken en ontwerpparameters om te helpen met een succesvolle inzet van Vocera Badge:

- Implementatie van één controller
- Meervoudige controller op Layer 2 implementatie
- Meervoudige controller op Layer 3 implementatie

Het begrijpen van de interactie tussen de Vocera Badge-functies binnen een LWAPP gesplitste MAC-omgeving is van essentieel belang. Met alle inzetscenario's moet multicast ingeschakeld zijn en moet de agressieve taakverdeling uitgeschakeld worden. Alle WLAN's moeten binnen hetzelfde omroepdomein op uw gehele netwerk zijn ingesloten.

Figuur 4



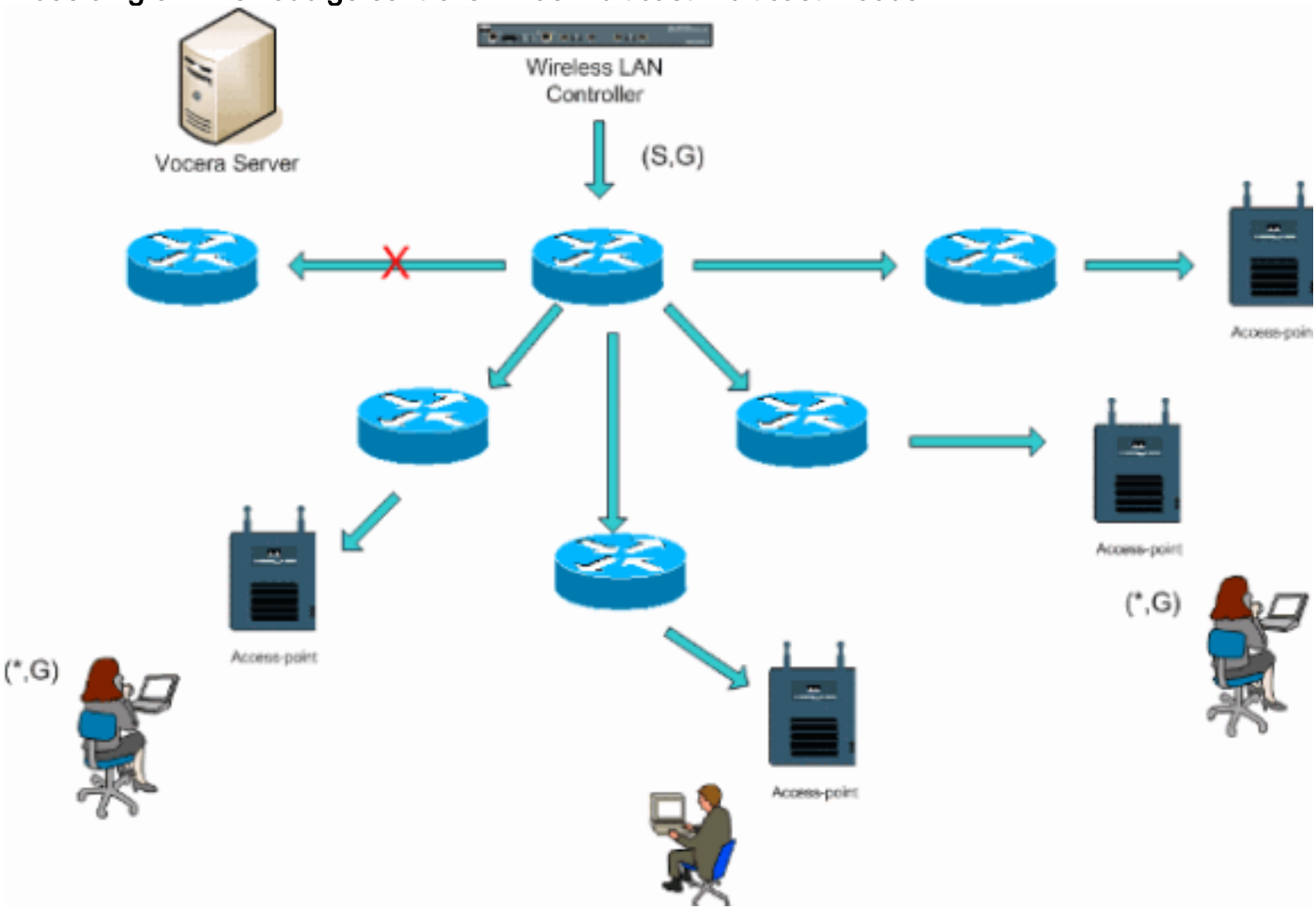
Implementatie van één controller

Dit is het meest rechtlijnige inzetscenario. Het stelt je in staat om de Vocera Badge oplossing in te zetten met weinig implementatiezorgen. Uw netwerk moet voor IP multicast routing alleen ingeschakeld zijn om de access points toe te staan om de LWAPP multicast-pakketten te ontvangen. Indien nodig kunt u de complexiteit van netwerk multicast beperken door alle routers en switches te configureren met de multicastgroep voor controllers.

Omdat multicast mondiaal zijn geconfigureerd op de controller, werkt de juiste SSID, beveiligingsinstellingen en alle access points de Vocera Badge-oplossing registreren en al zijn functies naar verwachting. Met de functie Uitzending Vocera volgen een gebruikersstromen en het multicast verkeer zoals verwacht. Er zijn geen extra instellingen nodig die ingesteld moeten worden om deze oplossing goed te laten werken.

Wanneer een Vocera Badge een multicast bericht verstuurt, zoals bij de Vocera Broadcast, wordt dit naar de controller verzonden. De controller kapselt dan dit multicast pakket in een LWAPP multicast pakket. De netwerkinfrastructuur stuurt dit pakket naar elk access point dat is aangesloten op deze controller. Wanneer het access point dit pakket ontvangt, bekijkt het dan de LWAPP multicast header om te bepalen welke WLAN/SSID het dan dit pakket uitzendt naar.

Afbeelding 5-Enkelvoudige controller in de multicast-multicast modus

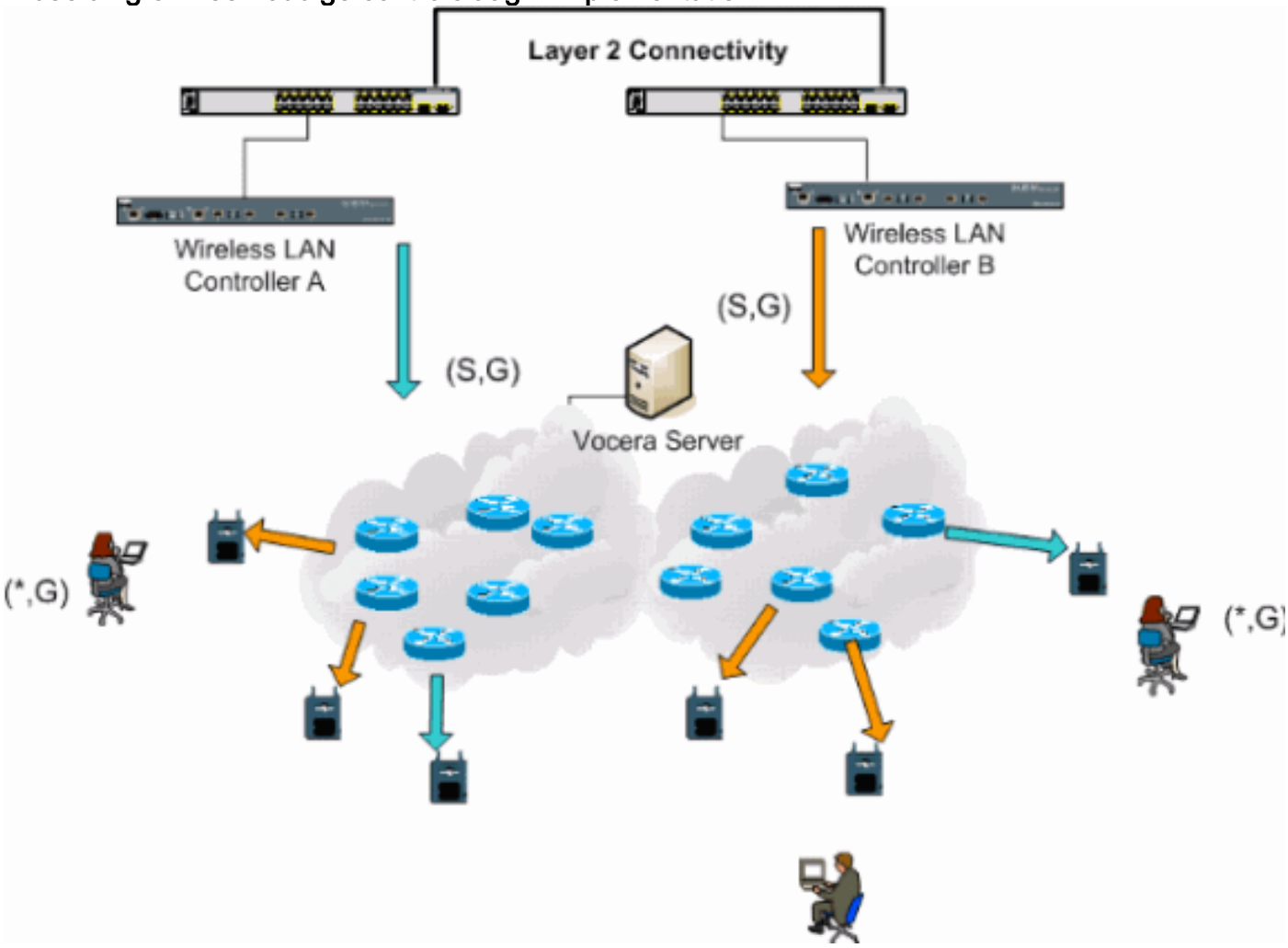


Meervoudige controller op Layer 2 implementatie

Meervoudige controllers moeten allen connectiviteit op elkaar hebben via hetzelfde Layer 2-omroepdomein. Beide controllers zijn ingesteld voor multicast zoals getoond, met behulp van de identieke access point multicast-groepen op elke controller om fragmentatie te beperken. Aangenomen dat dit Layer 2-omroepdomein via een gemeenschappelijke switch of een veel voorkomende reeks switches is verbonden, moet CGMP/IGMP-snooping op deze switches worden uitgeschakeld voor dit ene VLAN of 4.0.206.0 of hoger WLC-software worden uitgevoerd. Met de Vocera Broadcast-functie en een gebruikersstraal van een toegangspunt op één controller naar een toegangspunt op een andere controller is er geen mechanisme voor IGMP-verbindingen naar de nieuwe Layer 2-poort voor IGMP-communicatie naar het werk. Zonder een IGMP-pakket dat de upstream CGMP- of IGMP-switch bereikt, wordt de gespecificeerde multicast-groep niet naar de controller verzonden en wordt deze daarom niet door de client ontvangen. In sommige gevallen kan dit werken als een klant die deel uitmaakt van dezelfde Vocera Broadcast-groep dit IGMP-pakket al heeft verzonden voordat de roaming-client naar de nieuwe controller roamt Met de voordelen van versie 4.0.206.0, ontvangt een klant die naar een andere controller roam als Layer 2-roam, onmiddellijk na de verificatie een algemene IGMP-zoekopdracht. De klant dient dan te reageren met de betrokken groepen en de nieuwe controller wordt dan overbrugd naar de lokaal verbonden switch. Dit biedt de voordelen van IGMP en CGMP op uw stroomopwaarts gelegen switches.

U kunt extra badge SSIDs en Layer 2 domeinen voor afzonderlijke badge netwerken maken zolang uw netwerk wordt geconfigureerd om multicast verkeer correct door te geven. Bovendien moet elk Vocera Layer 2-omroepdomein dat is gemaakt, overal zijn waar een controller op het netwerk is aangesloten zodat de multicast niet wordt verbroken.

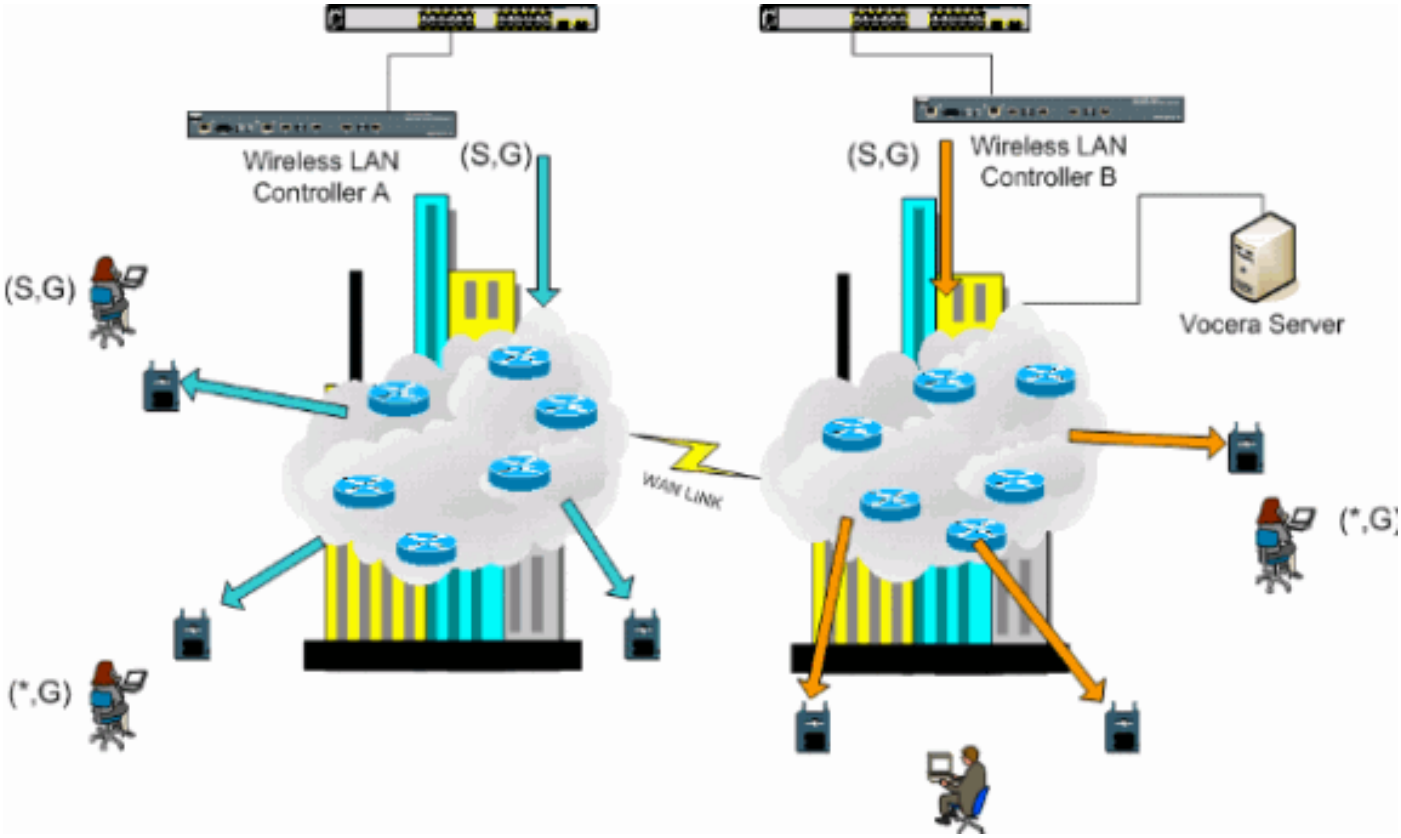
Afbeelding 6. Meervoudige controlelaag 2 implementatie



Meervoudige controller op Layer 3 implementatie

De Layer 3-implementatiestrategie mag alleen worden gebruikt bij roaming van controller-to-controller met WLC-softwarerelease 4.0.206.0 of hoger. Als een client die is aangesloten op de Vocera-omroepgroep en de juiste multicast-stream en -stromen naar een andere controller ontvangt als Layer 3-camera met de LWAPP Layer 3-roaming geconfigureerd, wordt deze op zoek naar geïnteresseerde multicastgroepen. De client heeft deze pakketten, wanneer hij aan dezelfde Vocera-uitzendgroep komt, aan de ankercontroller geleverd door de EoIP-tunnel en heeft deze pakketten routeerd door normale multicast-routingmethoden.

Afbeelding 7. Meervoudige controlelaag 3 implementatie



VoWLAN-implementaties Aanbevolen van Cisco

Draadloze IP-telefonienetwerken vereisen een zorgvuldige RF-planning. Een grondig onderzoek van de stemplaats is vaak vereist om de juiste niveaus van draadloze dekking te bepalen en bronnen van interferentie te identificeren. De selectie van toegangspunten en antennes kan enorm worden vergemakkelijkt met behulp van de resultaten van een geldig spraakplaatsonderzoek. De belangrijkste overweging is de uitzendkracht van de draadloze telefoon. Idealiter leert de telefoon de uitzendkracht van het access point en past de transmissiemodule aan die van het access point.

Hoewel de meeste draadloze netwerken vandaag de dag worden ingezet na een uitgebreid RF site survey, worden ze ook uitgevoerd met het bijhouden van de dataservice in gedachten. VoWLAN-telefoons hebben waarschijnlijk verschillende roamingkenmerken en verschillende dekkingsvereisten dan die van een typische WLAN-adapter voor een mobiele client zoals een laptop. Daarom wordt een aanvullend site-onderzoek voor spraak vaak aanbevolen om zich voor te bereiden op de prestatievereisten van meerdere VoWLAN-clients. Dit extra onderzoek biedt de mogelijkheid om de toegangspunten te stemmen om te verzekeren dat de VoWLAN-telefoons genoeg RF-dekking en -bandbreedte hebben om juiste spraakkwaliteit te bieden.

Raadpleeg voor aanvullende informatie over RF-ontwerpoverwegingen het hoofdstuk over WLAN Radio Frequency (RF) Design Aanduiding in de Cisco Wireless LAN Design Guide, beschikbaar op http://cisco.com/go/srnd.

Aanbevelingen voor gebouwen op meerdere vloeren, ziekenhuizen en pakhuizen

Neem de factoren in deze sectie in overweging wanneer u gebouwen, ziekenhuizen en pakhuizen met meerdere vloer inspecteert.

Bouwmethoden en -materialen

Veel aspecten van de bouwwerkzaamheden zijn niet bekend of verborgen voor het bouwproject, zodat u deze informatie wellicht uit andere bronnen moet verkrijgen (zoals architectonische tekeningen). Enkele voorbeelden van typische bouwmethoden en materialen die van invloed zijn op het bereik en het dekkingsgebied van toegangspunten zijn metaalfolie op raamglas, loodglas, stalen muren, cementvloeren en -muren met staalversterking, isolatie met schuim en liften, buizen en bevestigingsmiddelen, en vele andere.

inventaris

Verschillende soorten inventarisaties kunnen van invloed zijn op RF-bereik, met name die met een hoog staal- of watergehalte. Tot de items die u kunt controleren behoren kartonnen dozen, huisdieren, verf, aardolieproducten, motoronderdelen, enz.

Niveaus van de inventaris

Zorg ervoor dat u een enquête op de hoogste inventarisniveaus of bij de hoogste activiteit uitvoert. Een entrepot met een voorraadniveau van 50% heeft een heel andere RF-voetafdruk dan hetzelfde entrepot op een voorraadniveau van 100%.

Activiteitsniveau

Op dezelfde manier heeft een kantoorruimte na uren (zonder mensen) een andere voetafdruk dan hetzelfde gebied vol mensen gedurende de dag. Hoewel veel onderdelen van het site survey zonder volledige bezetting kunnen worden uitgevoerd, is het van essentieel belang de site survey-verificatie uit te voeren en belangrijke waarden aan te passen tijdens een tijd dat de locatie wordt bezet. Hoe hoger de gebruiksbehoeften en de gebruikersdichtheid, des te belangrijker is het om een goed ontworpen diversiteitsoplossing te hebben. Wanneer meer gebruikers aanwezig zijn, worden er meer signalen ontvangen op het apparaat van elke gebruiker. Aanvullende signalen veroorzaken meer contentie, meer ongeldige punten en meer multipath vervorming. Diversiteit op het toegangspunt (antennes) helpt deze omstandigheden tot een minimum te beperken.

Vloergebouwen

Houd deze richtlijnen in gedachten wanneer u een site-enquête uitvoert voor een typisch kantoorgebouw:

- Verteller: Verteller: Verstopt blok en reflecteert RF-signalen.
- Toevoerruimtes met voorraden absorberen signalen.
- Binnenlandse kantoren met harde muren absorberen RF-signalen.
- Kookkamers (keukens) kunnen 2,4 GHz interferentie veroorzaken door het gebruik van microgolfovens.
- Testlabs kunnen 2,4 GHz of 5 GHz interferentie veroorzaken, waardoor multi-path vervorming en RF schaduwen ontstaan.
- Cubicles absorberen en blokkeren signalen.
- Conferencingruimten hebben een hoge dekking van toegangspunten nodig omdat zij gebieden zijn met een hoog gebruik.

Extra voorzichtigheid moet worden toegepast bij het controleren van faciliteiten met meerdere vloer. Access points op verschillende vloeren kunnen elkaar zo gemakkelijk beïnvloeden als toegangspunten op dezelfde vloer. Het is mogelijk om dit gedrag in je voordeel te gebruiken

tijdens een enquête. Met antennes met een hogere versterking kan het mogelijk zijn tot vloeren en plafonds door te dringen en dekking te bieden aan zowel boven als onder de vloer waar het toegangspunt is gemonteerd. Zorg ervoor dat er geen kanalen tussen toegangspunten op verschillende vloeren of toegangspunten op dezelfde vloer overlapt. In gebouwen met meerdere huurders kunnen er veiligheidsproblemen zijn die het gebruik van lagere transmissiemachten en lagere winstantennes vereisen om signalen uit buurkantoren te houden.

Ziekenhuizen

Het onderzoeksproces voor een ziekenhuis is vrijwel hetzelfde als dat voor een onderneming, maar de indeling van een ziekenhuisinrichting loopt op deze wijze uiteen:

- Ziekenhuisgebouwen hebben de neiging veel wederopbouwprojecten en toevoegingen te ondergaan. Elke verdere constructie zal waarschijnlijk verschillende bouwmaterialen met verschillende niveaus van verzwakking hebben.
- De signaalpenetratie door muren en vloeren in de patiëntgebieden is doorgaans minimaal, wat helpt om microcellen en multipath variaties te creëren.
- De behoefte aan bandbreedte neemt toe met het toenemende gebruik van WLAN-ultrasone apparatuur en andere draagbare beeldtoepassingen. De behoefte aan bandbreedte neemt ook toe met de toevoeging van draadloze stem.
- Gezondheidszorgcellen zijn klein en naadloos roaming is essentieel, vooral met spraaktoepassingen.
- De celoverlap kan hoog zijn, en dat geldt ook voor kanaalhergebruik.
- Ziekenhuizen kunnen verschillende typen draadloze netwerken laten installeren. Dit omvat 2,4 GHz niet-802.11 apparatuur. Deze apparatuur kan conflicten opleveren met andere 2,4 GHz netwerken.
- Op de muur gemonteerde veelzijdige antennes en op het plafond gemonteerde veelzijdige antennes zijn populair, maar houden in gedachten dat diversiteit noodzakelijk is.

pakhuizen

pakhuizen hebben grote open plekken die vaak hoge opslagracks bevatten. Vaak bereiken deze racks bijna het plafond, waar de toegangspunten doorgaans worden geplaatst. Zulke opslagracks kunnen het gebied beperken dat het toegangspunt kan bestrijken. In deze gevallen kunt u overwegen om toegangspunten op andere locaties dan het plafond te plaatsen, zoals zijmuren en pijlers van cement. Neem ook deze factoren in aanmerking wanneer je een pakhuis opzoekt:

- De inventarisniveaus beïnvloeden het aantal benodigde toegangspunten. Testdekking met twee of drie toegangspunten op geschatte plaatsingsplaatsen.
- Onverwachte celoverlappingen zijn waarschijnlijk veroorzaakt door variaties van meerdere snijpad. De kwaliteit van het signaal varieert meer dan de sterkte van dat signaal. Clients kunnen zich meer dan met toegangspunten in de buurt associëren en beter bedienen.
- Tijdens een enquête hebben toegangspunten en antennes doorgaans geen antenne-kabel die ze met elkaar verbindt. Maar in een productieomgeving, zouden het toegangspunt en de antenne wel eens voelkabels nodig kunnen hebben. Alle antenne kabels introduceren signaalverlies. Het meest accurate onderzoek omvat het type antenne dat moet worden geïnstalleerd en de lengte van de kabel die moet worden geïnstalleerd. Een goed gereedschap om de kabel en het verlies ervan te simuleren is een demper in een enquêteset.

Het onderzoeken van een productiefaciliteit is vergelijkbaar met het controleren van een pakhuis,

behalve dat er misschien nog veel meer bronnen van RF-interferentie in een productiefaciliteit zijn. Bovendien vereisen de toepassingen in een fabriek doorgaans meer bandbreedte dan die van een opslagplaats. Deze toepassingen kunnen videobeelden en draadloze stem omvatten. Multipath-vervorming is waarschijnlijk het grootste prestatieprobleem in een productiefaciliteit.

Ondersteunde beveiligingsmechanismen

Naast statische EFFECT en Cisco LEAP voor authenticatie en gegevensencryptie, steunen de Vocera Bigges ook PPP-PEAP (MS-CHAP v2)/WAP2-PSK.

LEAP-overwegingen

LEAP maakt het mogelijk dat apparaten wederzijds geauthentiseerd worden (badge-to-access point en access point-to-badge) op basis van een gebruikersnaam en een wachtwoord. Op authenticatie wordt een dynamische sleutel gebruikt tussen de telefoon en het access point om verkeer te versleutelen. U dient echter rekening te houden met de ASLEAP-woordenboekaanval wanneer u besluit LEAP als uw beveiligingsoplossing te gebruiken:

Raadpleeg woordenboekaanval op Cisco LEAP-kwetsbaarheid voor meer informatie.

Als LEAP wordt gebruikt, wordt een LEAP-conforme RADIUS-server, zoals de Cisco Access Control Server (ACS), vereist om toegang tot de gebruikersdatabase te geven. Cisco ACS kan of de gebruikersnaam en het wachtwoordgegevensbestand lokaal opslaan, of het heeft toegang tot die informatie van een externe Microsoft Windows NT folder. Zorg er bij gebruik van LEAP voor dat er sterke wachtwoorden worden gebruikt op alle draadloze apparaten. Sterke wachtwoorden zijn gedefinieerd als een lengte tussen 10 en 12 tekens. U kunt zowel hoofdletters als kleine tekens evenals de speciale tekens toevoegen.

Omdat alle badges het zelfde wachtwoord gebruiken en het binnen de badge wordt opgeslagen, adviseert Cisco u verschillende gebruikersnamen en wachtwoorden op gegevenscliënten en draadloze stemcliënten te gebruiken. Deze praktijk helpt met het volgen en oplossen van problemen evenals veiligheid. Hoewel het een geldige configuratieoptie is om een extern (off-ACS) gegevensbestand te gebruiken om de gebruikersnamen en wachtwoorden voor de badges op te slaan, adviseert Cisco deze praktijk niet. Omdat de ACS gevraagd moet worden wanneer de badge tussen toegangspunten loopt, kan de onvoorspelbare vertraging om toegang te krijgen tot een off-ACS database buitensporige vertraging en slechte spraakkwaliteit veroorzaken.

Draadloze netwerkinfrastructuur

Het draadloze IP-telefonienetwerk, net zoals een bekabeld IP-telefonienetwerk, vereist zorgvuldige planning voor de configuratie van VLAN's, de netwerkgrootte, het multicast-transport en de keuze van apparatuur. Voor zowel bekabelde als draadloze IP-telefonienetwerken zijn afzonderlijke spraak- en gegevensVLAN's vaak de meest effectieve manier om te zorgen voor voldoende netwerkbandbreedte en probleemoplossing.

Voice-, data- en VLAN's

VLAN's bieden een mechanisme voor het segmenteren van netwerken in een of meer uitzenddomeinen. VLAN's zijn in het bijzonder belangrijk voor IP-telefonienetwerken, waar de typische aanbeveling is om spraak- en gegevensverkeer in verschillende Layer 2-domeinen te

scheiden. Cisco raadt u aan om afzonderlijke VLAN's voor de Vocera-bruggen te configureren van ander spraak- en gegevensverkeer: een inheems VLAN voor toegangspoint Management-verkeer, data-VLAN voor gegevensverkeer, een spraak of hulp-VLAN voor spraakverkeer en een VLAN voor Vocera-bruggen. Een afzonderlijk spraak-VLAN maakt het netwerk in staat om voordeel te halen uit Layer 2-markering en biedt prioriteitswachtrij aan de Layer 2-toegangspoort van de switch. Dit waarborgt dat er geschikte QoS voor verschillende klassen van verkeer wordt geboden en helpt u bij het oplossen van adresseringskwesties zoals IP-adressering, beveiliging en netwerkdimensionering. De Vocera Badges gebruiken een uitzendingsfunctie die multicast gebruikt om te leveren. Dit gemeenschappelijk VLAN waarborgt dat wanneer een badge tussen controllers roert, het deel van de multicast groep blijft. Dit laatste proces wordt in detail besproken wanneer multicast later in dit document wordt aangepakt.

Netwerkgrootte

Het netwerk van IP-telefonie is van essentieel belang om te verzekeren dat er toereikende bandbreedte en middelen beschikbaar zijn om aan de eisen te voldoen die door de aanwezigheid van spraakverkeer worden voorgesteld. Naast de gebruikelijke ontwerprichtlijnen voor IP-telefonie voor het indelen van onderdelen zoals PSTN-poorten, transcoders, WAN-bandbreedte enzovoort, kunt u ook deze 802.11b-problemen overwegen wanneer u uw draadloze IP-telefonienetwerk instelt. De Vocera Badges zijn een gespecialiseerde toepassing die het aantal bekabelde klanten uitstrekt tot boven onze typische stationeringsaanbevelingen.

Aantal apparaten per access point

Cisco raadt u aan niet meer dan 15 tot 25 802.11b apparaten per access point te hebben.

Aantal actieve oproepen per access point

Vocera gebruikt twee verschillende codecs gebaseerd op of het een badge-to-badge (eigen lage-bit rate codec) aanroep of een badge-to-phone (G.711 codec) aanroep is. Deze tabel toont een percentage beschikbare bandbreedte aan de hand van gegevenssnelheden en geeft u een duidelijker beeld van de verwachte doorvoersnelheid:

Gespreksproces	1 Mbps	2 Mbps	5,5 Mbps	11 Mbps
Band-to-Phone (G.711)	20.7%	11.8%	6.3%	4.7%
Badge-to-Badge (Gecodec) (eigen lage-bit rate codec)	9.4%	6.1%	4.2%	3.6%

Aanbevelingen voor switch

Opmerking: Als u een Cisco Catalyst 4000 Series Switch als de hoofdrouter in het netwerk gebruikt, zorg er dan voor dat deze ten minste een Supervisor Engine 2+ (SUP2+) of Supervisor Engine 3 (SUP3) module bevat. De SUP1- of SUP2-module kan vertragingen veroorzaken bij roaming, net zoals de Cisco Catalyst 2948G-, 2980G-, 2980G-A-, 4912- en 2948G-GE-TX switches.

U kunt een switch poortsjabloon maken voor gebruik wanneer u een switch poort vormt voor de aansluiting op een access point. Deze sjabloon moet alle basisveiligheids- en veerkrachtkenmerken van de standaard desktopsjabloon toevoegen. Daarnaast kunt u, wanneer u

het access point aan een Cisco Catalyst 3750 Switch toevoegt, de prestaties van het access point optimaliseren door de opdrachten van Multilayer Switching (MLS) QoS te gebruiken om het poorttarief te beperken en CoS (Class of Service) in kaart te brengen met DSCP-instellingen (Distributed Services Code Point).

Elk verkeer dat niet door WLAN-clients wordt vereist, mag niet naar een access point worden verzonden. Een sjabloon moet zodanig zijn ontworpen dat er een beveiligde en veerkrachtige netwerkverbinding met deze functies ontstaat:

- Zet Port Configuraties terug om standaard te zijn: voorkomt configuratie conflicten door al bestaande poortconfiguraties te verwijderen.
- Schakel Dynamic Trunking Protocol (DTP) uit - schakelt dynamische trunking uit, wat niet nodig is voor verbinding met een access point.
- Uitschakelen van Port Aggregation Protocol (PagP) - PagP is standaard ingeschakeld, maar is niet nodig voor gebruikersgerichte poorten.
- Laat Port Fast-aan toe een switch om snel het doorsturen verkeer te hervatten als het omspannen van een boomverbinding daalt.
- Configureer draadloos VLAN-maakt een uniek draadloos VLAN dat draadloos verkeer isoleert van andere gegevens, spraak- en beheerVLAN's. Dit isoleert het verkeer en zorgt voor een betere controle van het verkeer.
- QoS-kwaliteit (Quality of Service) inschakelen; Vertrouw geen poort (markering op 0) - verzekert juiste behandeling van verkeer met hoge prioriteit, inclusief softphones, en voorkomt gebruikers buitensporige bandbreedte te consumeren door hun PC's te herconfigureren.

WS-C3750-48PS-S Switches met inline voeding kunnen worden gebruikt voor het verschaffen van elektriciteit aan toegangspunten die inline voeding kunnen ontvangen.

Catalyst 6500 staat u toe om pakketten met lijnsnelheid door te sturen met alle hier beschreven eigenschappen evenals talrijke servicemodules te integreren. Met de draadloze servicemodule (WiSM) kunt u twee controllers hebben die elk 150 access points kunnen controleren. Met maximaal vijf WiSM's per chassis kan u meer dan 1500 access points controleren die 50.000 klanten ondersteunen binnen één krachtige switcharchitectuur.

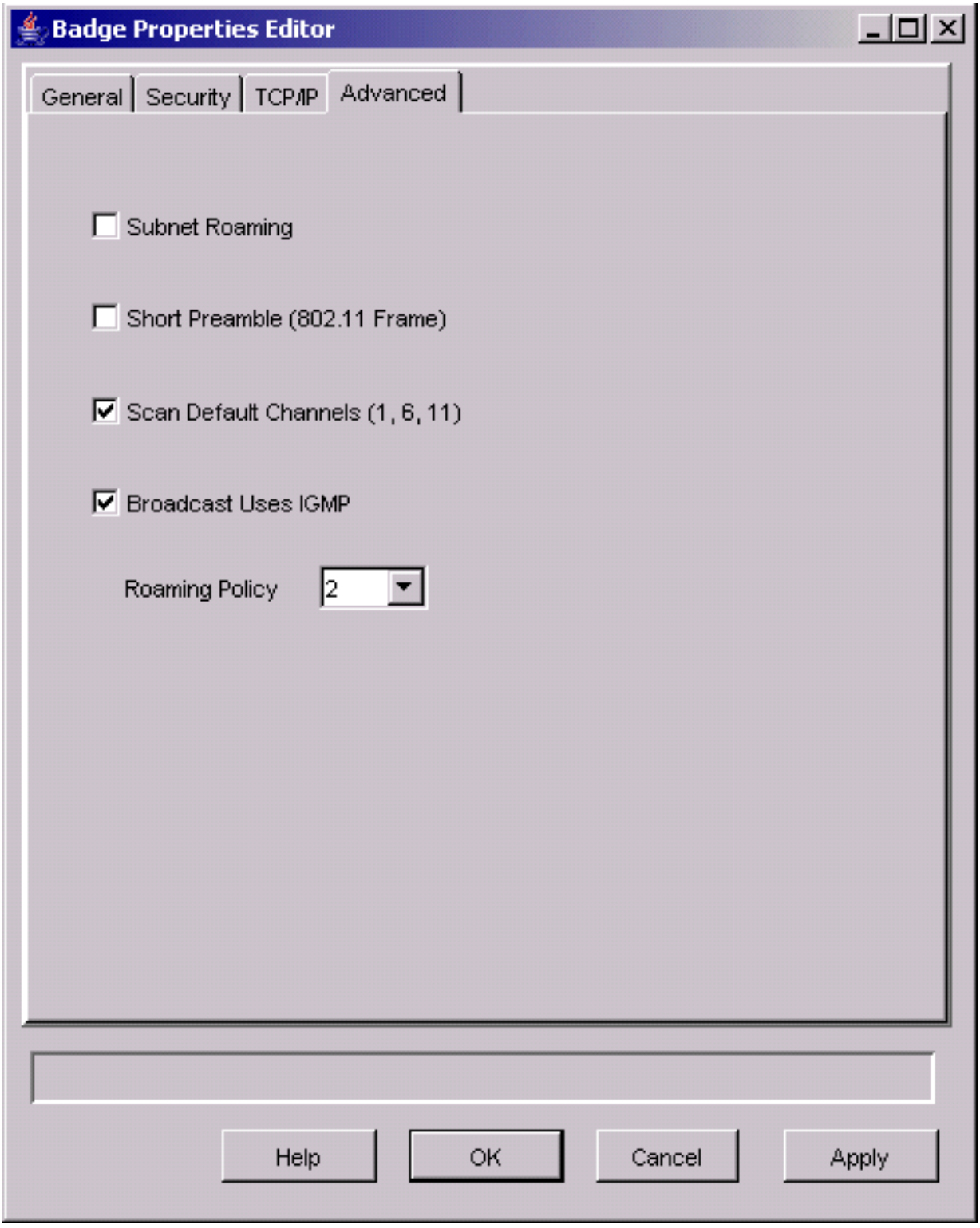
implementaties en configuratie

Configuratie pagina

Het Vocera Badge Configuration Utility (BCU) en de configuratie van de badge kunnen roaming en latentie in uw omgeving introduceren als dit niet correct gebeurt. Gebruik de BCU en de Brug Properties Editor (BPE) en controleer deze instellingen (zie afbeelding 8):

- **Subnet roaming** is uitgeschakeld.
- **Standaard scankanalen (1,6,11)** ingeschakeld.
- **Broadcast Uses IGMP** is ingeschakeld.
- Het roamingbeleid is ingesteld op **2** of hoger.

Afbeelding 8. Tabblad Verkenner BCU Advanced



Wanneer **Subnet Roaming** wordt gecontroleerd, geeft deze de badge op om een nieuw IP adres na elk programma aan te vragen. In de LWAPP-omgeving helpt de infrastructuur om clientconnectiviteit op Layer 3 te handhaven. Wanneer een spraakclient moet wachten tot de DHCP-server reageert voordat deze pakketten kan verzenden of ontvangen, wordt vertraging en jitter geïntroduceerd. Als **er** geen **scannen naar standaardkanalen (1,6,11)** is ingeschakeld, scant de badge alle 802.11b-kanalen wanneer de badge naar roam kijkt. Dit voorkomt het verzenden van pakketten en naadloze roaming.

Tune AutoRF voor uw omgeving

Zoals beschreven in het gedeelte Aanbevelingen van dit document, is het belangrijk te begrijpen

dat elke site zijn eigen RF-kenmerken heeft. AutoRF of Radio Resource Management (RRM) moet misschien worden aangepast, met dien verstande dat elke locatie anders is en AutoRF/RRM moet worden aangepast voor uw omgeving.

Voordat u AutoRF aanpast, raadpleegt u Radio Resource Management onder Unified Wireless Networks voor meer informatie.

RRM stelt u in staat om het zendvermogen van elk access point aan te passen, door aan te passen hoe sterk elk access point zijn derde sterkste buurman hoort. Deze waarde kan alleen van de CLI worden aangepast met behulp van de **configuratie geavanceerde 802.11b tx-power-thresh** opdracht zoals beschreven in Toestel Niveau Toekenningsinstellingen.

Voordat u AutoRF aanpast, moet u de implementatielocatie met behulp van de Vocera-badge laten lopen zoals die door de eindgebruiker wordt gedragen en een site-onderzoeksgereedschap gebruiken om een sterk inzicht te krijgen in hoe de badge roams en op welke kracht elk toegangspunt wordt gezien. Zodra dit is voltooid en wordt bepaald dat deze waarde moet worden aangepast, moet u beginnen met een waarde van -71 dBm voor het algoritme voor de regeling van het transmissievermogen. Gebruik deze CLI-parameter:

```
config advanced 802.11b tx-power-thresh -71
```

Laat het netwerk door deze aanpassing met een minimum van 30 minuten tot een uur werken voordat u enige veranderingen waarneemt. Zodra het netwerk voldoende tijd krijgt, kan je de site weer met dezelfde enquête-tool en badges laten lopen. Neem dezelfde roamingkenmerken en toegangspunten in acht. Het doel hier is om de badges te laten draaien op of voor het volgende toegangspunt om het best mogelijke signaal naar ruisverhouding te krijgen.

- **Hoe weet ik of de zendkracht te heet of te koud is?**Voor het bepalen of u de drempelwaarde voor het verzendvermogen te hoog of te laag hebt, is een goed begrip van uw omgeving vereist. Als je je hele implementatiegebied hebt gelopen (waar je verwacht dat je Vocera-badges werken), dan zou je moeten weten waar je toegangspunten zijn en het roaming-gedrag van de badge ervaren.
- **Wat doe ik als mijn transmissiemodule te heet is?**De Vocera Badge roams zijn uitsluitend gebaseerd op de signaalsterkte in plaats van de signaalkwaliteit. Indien de Vocera Badge niet beweegt nadat hij meerdere toegangspunten passeert terwijl hij zich bezighoudt met de welkomsttutorial of de testtoon, wordt de badge geacht kleverig te zijn. Als dit gedrag kenmerkend is voor het gehele kampeerterrein, is uw drempelwaarde voor de verzendkracht te heet en moet u deze beperken. Als slechts één of twee geïsoleerde gebieden dit gedrag laten zien en de rest van het stationeringsgebied idealistische roamingkenmerken vertoont, dan is dat geen aanwijzing dat uw netwerk te heet is.
- **Wat moet ik doen als mijn overbrengingskracht te koud is?**De standaard verzenddrempel zou u bijna nooit een implementatiegebied moeten bieden waar uw netwerk te koud loopt. Als de drempel voor de verzendenergie is aangepast en het lopen van de zalen met de Vocera-badge u een omgeving biedt waar de badge goed roomt, maar connectiviteit verliest en/of dood/spotty dekking, dan zou uw netwerk te laag kunnen zijn afgestemd. Als dit niet typisch is voor uw hele netwerk maar geïsoleerd is voor een of twee gebieden, dan is het eerder een indicatie van een gat in de dekking dan een netwerkbreed probleem.
- **Geïsoleerd gedrag**Als je dat op een of twee gebieden vindt, dan blijft de badge bij een toegangspunt liggen in plaats van op een idealistische manier te roaming, dan moet je dit gebied bekijken.Hoe verschilt dit gebied van de rest van de campus?Als dit/deze gebieden

nabij afstanden of gebieden in aanbouw zijn, zou de detectie van gaten deze toegangspunten dan dwingen om de stroom op te voeren?Kijk naar het logbestand van WLC en de buurlijsten van het toegangspunt om te helpen bepalen waarom zo'n anomalie zou kunnen voorkomen.Als je dat vindt in een of meer geïsoleerde gebieden, dan ervaart de badge dood of branddekking, dan moet je deze gebieden afzonderlijk onderzoeken.Is dit gebied bij een lift schacht, radiologie of een pauze?Deze gebieden zouden beter geschikt kunnen zijn door de installatie of betere plaatsing van een toegangspunt om een betere spraakdekking mogelijk te maken.In beide gevallen is het altijd raadzaam te begrijpen dat u werkt in een radiospectrum zonder vergunning en dat idealistisch gedrag misschien nooit haalbaar is. Dit zou kunnen gebeuren als u zich naast een radiotransmissietoren of -apparaat, een televisietranmitter of mogelijk een niet-802.11 2.4 GHz reparatie-voorziening bevindt (draadloze telefoons, enzovoort).

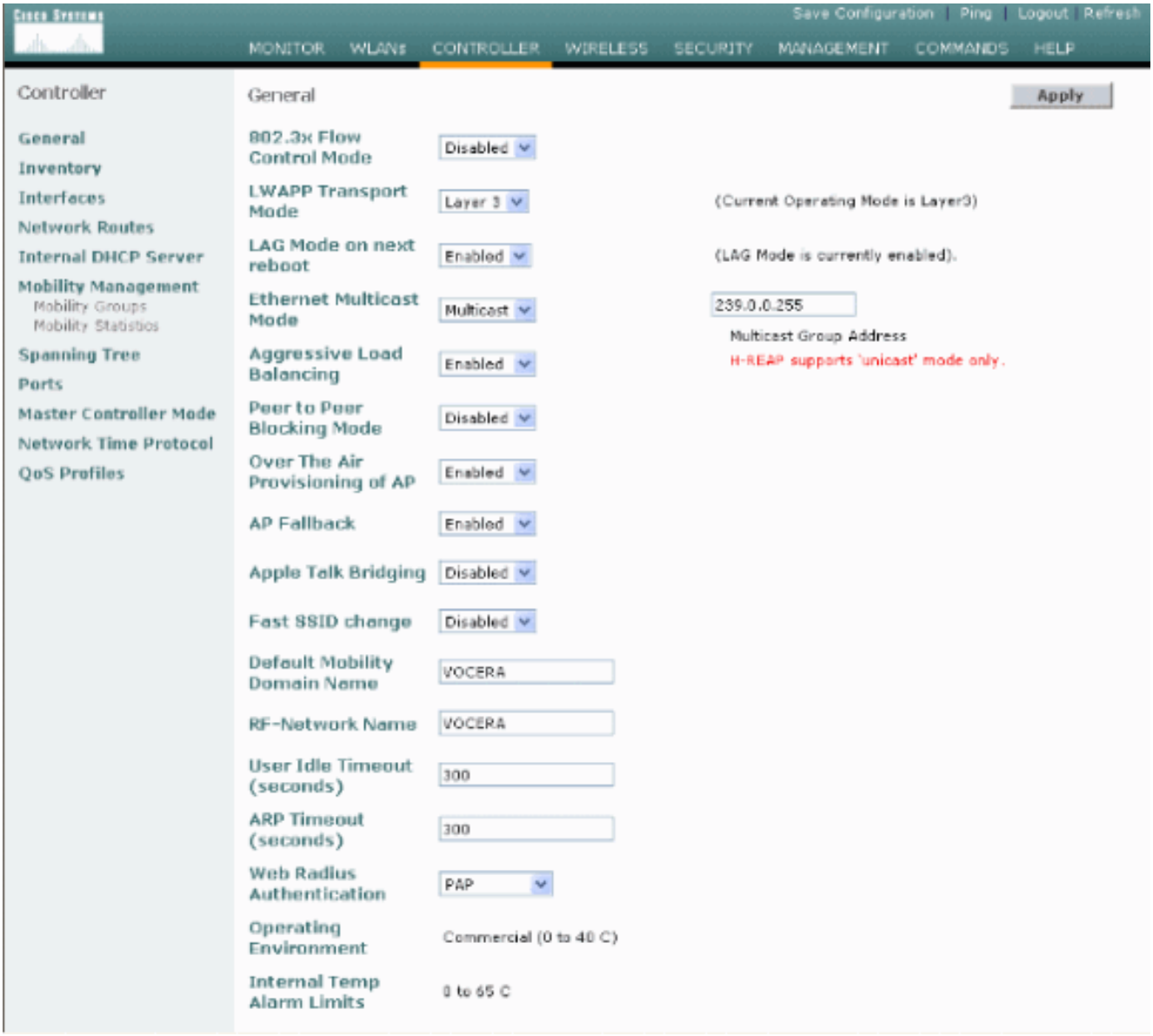
Configuratie van draadloze netwerkinfrastructuur

De Cisco Unified Wireless Network Design en de implementatiegids moeten worden gevolgd voor de algehele configuratie van uw WLC(s). Deze paragraaf bevat aanvullende aanbevelingen specifiek voor Vocera® Communication Badges.

Opmerking: Wijzigingen worden niet opgeslagen als u niet op de knop **Toepassen drukt** voordat u naar de volgende stap gaat.

Volg deze stappen onder het menu **Controller** top-level:

1. Verander Ethernet Multicast Mode in **Multicast**.
2. Stel het Multicastgroepsadres in op **239.0.255** (of een ander ongebruikt multicast groepsadres).
3. Stel de standaardnaam van het mobiliteitsdomein en de RF-netwerknaam in op het netwerkontwerp.
4. Schakel **agressieve taakverdeling uit**.**Afbeelding 9. - Algemene WLC-configuratie**

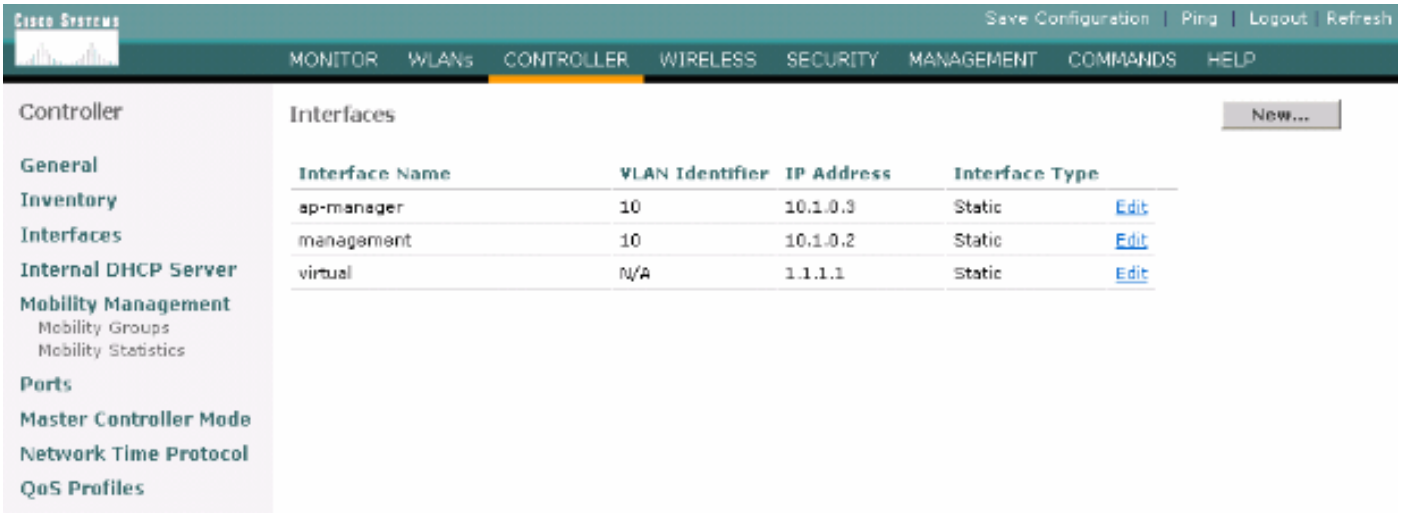


Interfaces maken

Klik op **Controller > Interfaces**.

Opmerking: uw VLAN- en IP-adres varieert. De screenshots hier bieden een voorbeeldadressering die niet direct gevolgd zou moeten worden.

Afbeelding 10-lijst van WLC-interfaces



De Vocera-spraakinterface maken

Voer de volgende stappen uit:

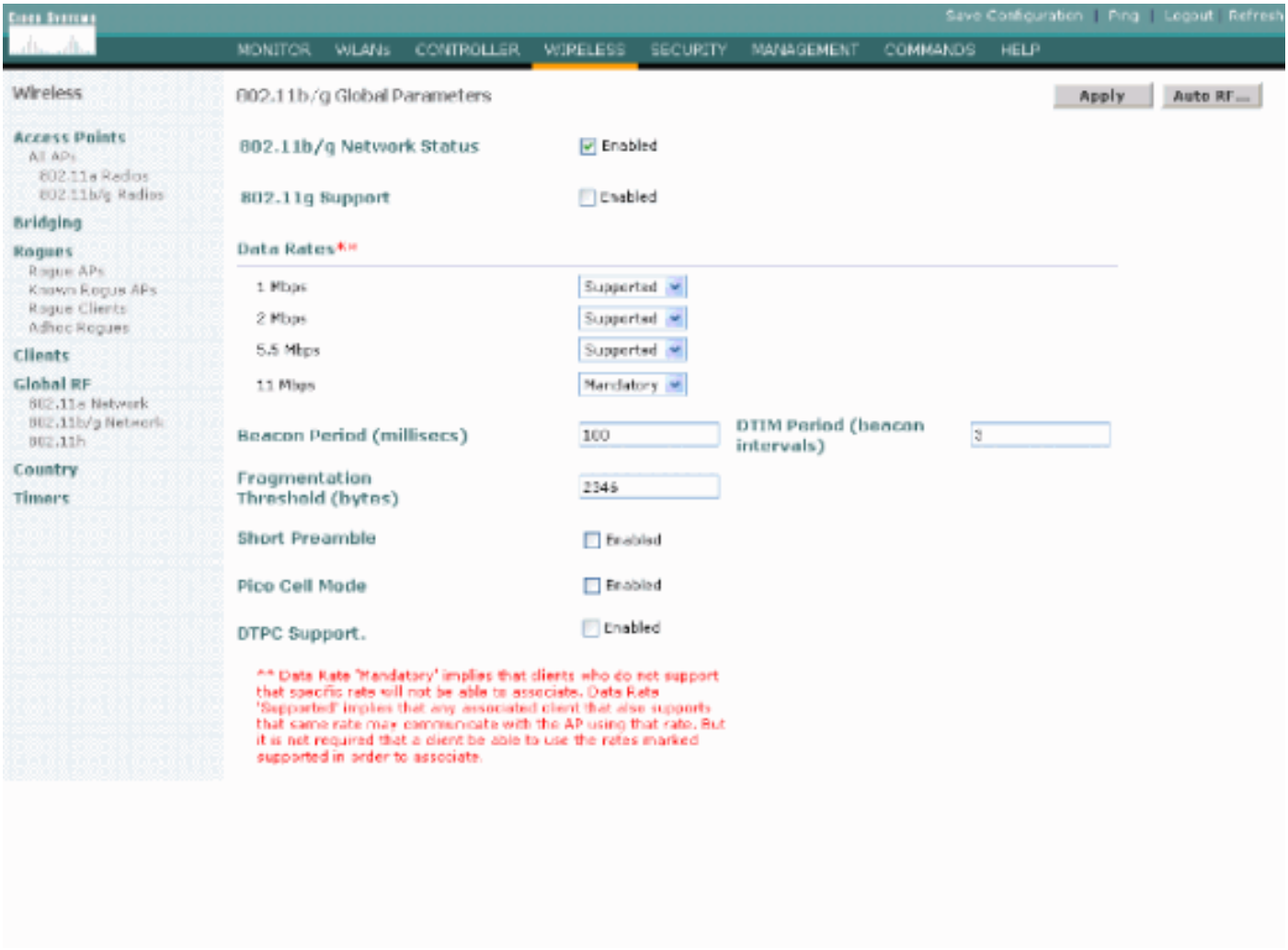
1. Klik op **New** (Nieuw).
2. Voer een tag-naam in die representatief is voor uw Vocera VoWLAN-netwerk in het veld Interfacenaam.
3. Voer het VLAN-nummer van dat VoWLAN-netwerk in het veld VLAN-id.
4. Klik op **Toepassen** en klik vervolgens op **Bewerken** om de interface te bewerken die u zojuist hebt gemaakt.
5. Voer de IP-adressering in voor deze interface die in het bereik van VLAN en andere verwante informatie ligt.
6. Klik op **Apply** (Toepassen).

Draadloze specifieke configuratie

Voor een WLAN-functie die alleen Vocera Badges heeft, biedt deze configuratie voorbeeldinstellingen die de Vocera Broadcast-toepassing het beste ondersteunen.

- De DTIM-periode is **1**.
- Ondersteuning voor 802.11g is uitgeschakeld. Alleen het gegevenstarief van 802.11b van **11 Mbps** is **verplicht**.
- Korte preambule is uitgeschakeld.
- DTPC is uitgeschakeld.

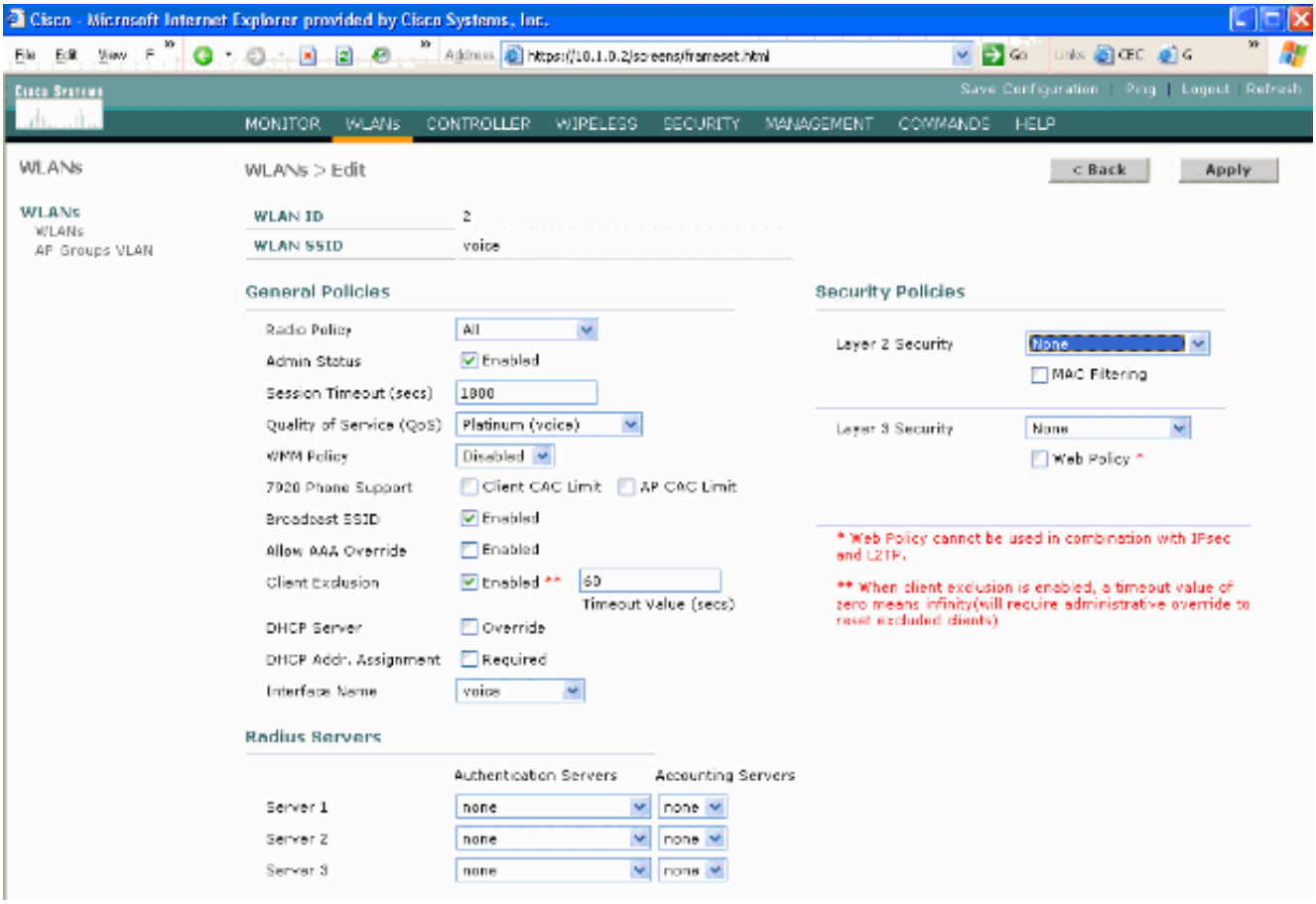
Afbeelding 11-802.11b/g configuratie



WLAN-configuratie

Voer de volgende stappen uit:

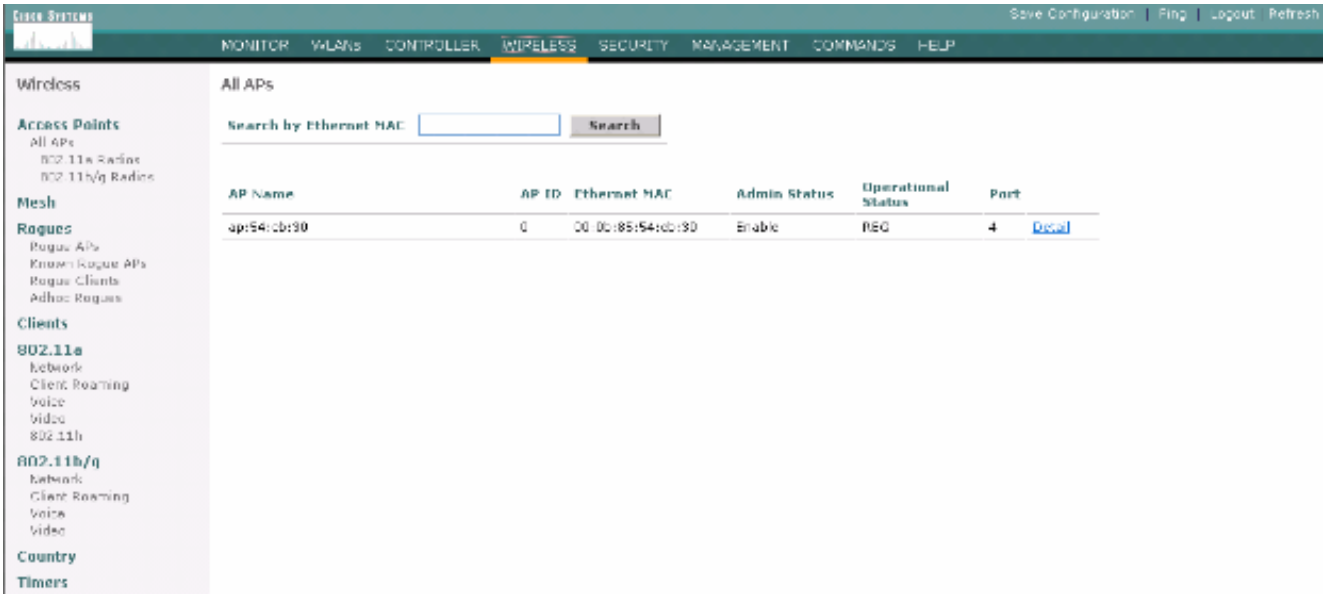
1. Werk het veld Radiobeleid aan tot een waarde die het best bij u past.
2. Wijzig de Admin-status in **Ingeschakeld**.
3. Time-out sessie instellen op **1800**.
4. Stel Quality-of-Service in op **Platinum**.
5. Stel Broadcast SSID in op **ingeschakeld**.
6. Stel de interfacenaam in op de interface die voor de Video Communication Badges is gemaakt.
7. Stel de beveiligingsopties in die overeenkomen met uw bedrijfsbeleid.**Afbeelding 12-WLAN-configuratie**



Detectie access point instellen

Voer de volgende stappen uit:

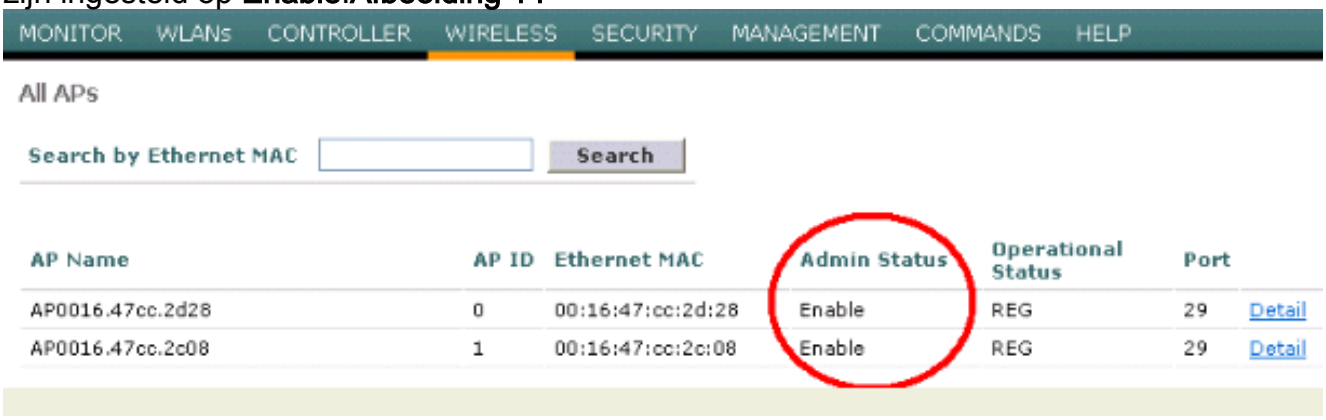
1. Klik op **Details**.
2. Configureer de AP-naam.
3. Zorg ervoor dat het access point voor DHCP is ingesteld.
4. Zorg ervoor dat de Admin-status is **ingeschakeld**.
5. AP Mod" moet op **lokaal** worden ingesteld.
6. Voer de locatie van het access point in.
7. Voer de naam in van de controller waarvan het access point deel uitmaakt. U vindt de naam van de controller op de webpagina van de monitor.
8. Klik op **Apply** (Toepassen).**Afbeelding 13-AP details**



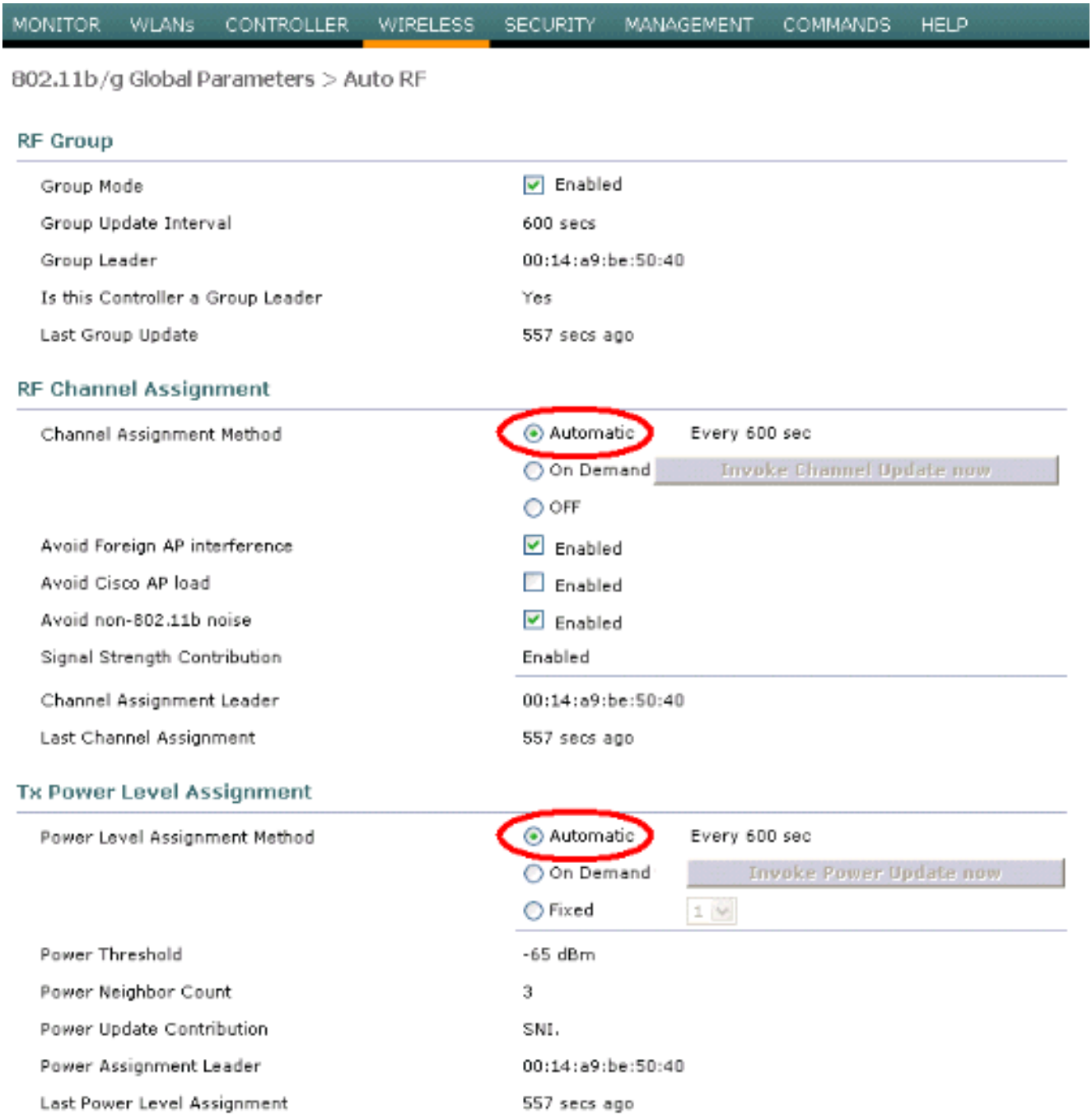
De 802.11b/g radio configureren

Voer de volgende stappen uit:

1. Klik op **Wireless** boven in de WLC en controleer of alle access points onder de Admin Status zijn ingesteld op **Enable**.**Afbeelding 14**



2. Klik op **Network** (bevindt zich in de buurt van 802.11b/g).
3. Klik op **AutoRF**.
4. Gebruik AutoRF om een volledige dekking te maken met niet-overlappend RF-kanaal en een verzendkracht. Selecteer hiervoor de optie **Automatisch** voor zowel RF-kanaaltoewijzing als Tx-Power Level Asessie.**Afbeelding 15**



5. Klik op **Apply** (Toepassen).
6. Klik op **Save Configuration** en zie het gedeelte Tune AutoRF voor uw omgeving van dit document.
7. Kies **Draadloos > access points > 802.11b/g radio.Afbeelding 16**

Verificatie van draadloze IP-telefonie

Nadat u een RF plaatsonderzoek uitvoert en de toegangspunten en de telefoons vormt, is het essentieel om controle testen uit te voeren om te verzekeren dat alles zoals gewenst werkt. Deze tests moeten op al deze locaties worden uitgevoerd:

- Het primaire gebied van elk toegangspunt cel (waar de badges waarschijnlijk met dat specifieke toegangspunt verbonden zullen zijn).
- Elke locatie waar een hoog oproepvolume kan zijn.
- Locaties waar het gebruik misschien zeldzaam is, maar waar de dekking nog steeds moet worden gecertificeerd (bijvoorbeeld trappenhuizen, toiletten, enzovoort).
- Aan de rand van het dekkingsgebied van het toegangspunt.
- ・ Deze tests kunnen parallel of in serie worden uitgevoerd. Indien parallel uitgevoerd, zorg er dan voor dat de telefoons tussen de testpunten worden uitgeschakeld om volledige associatie, verificatie en registratie op elke locatie te testen. De laatste tests moeten worden uitgevoerd op roaming en belasting.

Associatie, verificatie en registratie

In dit gedeelte wordt uitgelegd hoe u kunt controleren of de badge zich associeert, bevestigt en registreert.

- Op meerdere punten in de omgeving, de badges omhoog en de associatie met het toegangspunt controleren. Als de badge niet met het toegangspunt associeert, voert u deze controles uit:Controleer de badge configuratie om te zorgen voor juiste SSID, authenticatie type, enzovoort.Controleer de WLC-configuratie om te zorgen voor juiste SSID's, type verificatie, radiokanalen, enzovoort.Controleer uw plaatsonderzoek om er zeker van te zijn dat de locatie voldoende RF-dekking heeft.
- Op meerdere punten door het milieu, zorg ervoor dat de telefoon door het toegangspunt met succes authentiek verklaard. Als de client niet echt is, controleert u of de sleutel van de evenaar of de gebruikersnaam en het wachtwoord van de LEAP op de badges. Controleer ook de gebruikersnaam en het wachtwoord op de AAA-server door een draadloze laptop met identieke aanmeldingsgegevens te gebruiken.
- Zorg er op meerdere punten in de omgeving voor dat de badges worden geregistreerd bij de Videoserver. Als de client niet registreert, voert u deze controles uit:Controleer dat de badge het juiste IP adres, subnetmasker, primaire gateway, primaire TFTP, primair/secundair en DNS heeft.
- Stationaire spraakoproepen:Op meerdere punten in de omgeving, terwijl je stil staat, bel je naar een andere badge en voer 60 tot 120 seconden spraaktests uit om de spraakkwaliteit te controleren. Als de stemkwaliteit onacceptabel is, verplaats dan één badge naar een betere locatie en test opnieuw. Is de spraakkwaliteit aanvaardbaar? Als dit niet het geval is, controleer dan uw draadloze dekking.Als de telefonieserver wordt geconfigureerd, op meerdere punten door de omgeving, sta dan stil en bel een bekabelde telefoon aan en voer 60 tot 120-seconden spraaktests uit om de spraakkwaliteit te controleren. Als de stemkwaliteit onacceptabel is, vraag dan of u een gesprek voert met de bekabelde telefoon. Is de spraakkwaliteit aanvaardbaar? Zo niet, controleer het bekabelde netwerkontwerp aan de hand van de richtsnoeren.

- Gebruik de instrumenten van het plaatsonderzoek om te verifiëren dat er niet meer dan één toegangspunt per RF-kanaal van die locatie is met een signaalsterkte (ontvangen signaalsterkte-indicator [RSSI]) groter dan 35. Als er twee toegangspunten op hetzelfde kanaal zijn, zorg er dan voor dat de signaal-ruisverhouding (SNR) zo hoog mogelijk is om interferentie te minimaliseren. Bijvoorbeeld, als het sterkere toegangspunt een RSSI van 35 heeft, zou het zwakste toegangspunt idealiter een RSSI van minder dan 20 moeten hebben. Om dit doel te bereiken, zou u de transmissie-kracht van één toegangspunt moeten verminderen of het toegangspunt moeten verplaatsen.
- Controleer de QoS-instellingen op het access point om de juiste aanbevolen instellingen te bevestigen.
- Roaming badge-oproepen:Als de telefonieserver niet beschikbaar is, open dan de Videoscape Tutorial met de opdracht **Beginnen Tutorial**.OFAls de telefonieserver beschikbaar is, open een vraag met een stationair apparaat naar de badge.Controleer de spraakkwaliteit continu terwijl u het gehele draadloze dekkingsgebied doorkruist. Als de spraakkwaliteit onvoldoende is, voert u deze taken uit:Luister naar alle onaanvaardbare veranderingen in de spraakkwaliteit en neem kennis van de locatie- en radiowaarden op uw laptop en CQ-waarden vanaf de insigne.Kijk en luister naar de badge om naar het volgende toegangspunt te gaan.Let op de andere beschikbare toegangspunten in het site survey om dekking en interferentie te controleren.
- Maak aanpassingen aan access point plaatsing en instellingen om het WLAN te verfijnen en voer deze controles uit om spraakkwaliteit te garanderen:Gebruik de site survey tools en controleer of er niet meer dan één toegangspunt per kanaal is met een RSSI waarde groter dan 35 op een bepaalde locatie. Idealiter zouden alle andere toegangspunten op hetzelfde kanaal RSSI-waarden zo laag mogelijk moeten hebben (bij voorkeur minder dan 20). Aan de grens van het dekkingsgebied waar de RSSI 35 is, moet de RSSI voor alle andere toegangspunten op hetzelfde kanaal idealiter minder dan 20 zijn.Gebruik de site survey tools om te controleren of er ten minste twee toegangspunten (totaal, op afzonderlijke kanalen) zichtbaar zijn op alle locatie met voldoende signaalsterkte.Controleer of de toegangspunten in een bepaald roaminggebied allemaal op een Layer 2-netwerk liggen.

Gemeenschappelijke roaming-problemen

Deze roamingproblemen kunnen zich voordoen:

- De badge schuimt niet wanneer hij rechtstreeks onder het toegangspunt wordt geplaatst.
- De badge zal waarschijnlijk niet de gedifferentieerde roamingdrempels voor de ontvangen signaalkrachtindicator (RSSI) en kanaalgebruik (CU) bereiken. Pas de stroomdrempel van het WLC aan.
- De badge ontvangt geen bakens of sonde reacties van het toegangspunt.
- De badge is te langzaam.

De band verliest verbinding met het netwerk of de spraakservice is verloren bij het roaming

- Controleer authenticatie voor een mogelijk gebruik van het wiel.
- De badge stuurt geen IGMP-grappen uit of het netwerk stuurt IGMP-vragen tijdens een rondleiding door. Daarom faalt de Vocera-uitzendfunctie tijdens een Layer 2/Layer 3-straal.

- De badge is slechts in staat om Layer 2 roaming naadloos te maken (tenzij een Layer 3 mobiliteitsmechanisme is ingesteld). Zorg ervoor dat de nieuwe WLC geen andere IP-telefoon serveert.
- Controleer dat het aangesloten access point/controller IP-connectiviteit heeft op de Videocommunicatieserver.
- Controleer de RF-signaalsterkte en de CQ-waarden.

Brug verliest spraakkwaliteit bij roaming

- Controleer op een lage RSSI op het toegangspunt van de bestemming.
- Kanaaloverlap zou ontoereikend kunnen zijn. De badge moet tijd hebben om de oproep goed af te geven voordat het signaal verliest met het oorspronkelijke toegangspunt.
- Het signaal van het oorspronkelijke access point kan verloren gaan.

Audio-problemen

Er zijn een paar gebruikelijke configuratiefouten die gemakkelijk opgeloste audio-problemen kunnen veroorzaken. Controleer, indien mogelijk, audio problemen tegen een stationaire (referentie) badge om het probleem aan een draadloos probleem te verminderen. Vaak voorkomende geluidsproblemen zijn:

- eenzijdig geluid
- Choppy of Robotic Audio
- Problemen met registratie en verificatie

eenzijdig geluid

- Dit probleem kan zich voordoen in de randgebieden van een access point, waar een signaal te zwak kan zijn aan de badge kant of aan de kant van het access point. Wanneer het mogelijk is om de stroominstellingen op het toegangspunt af te stemmen op de badge (20 mW), kan dit probleem worden opgelost. Dit probleem komt het meest voor wanneer de variatie tussen de instelling van het toegangspunt en de insigne-instelling groot is (bijvoorbeeld 100 mW op het toegangspunt en 28 mW op de insigne).
- Controleer de gateway en IP routing voor spraakkwaliteit.
- Controleer of een firewall of NAT in het pad van de eigen UDP-pakketten zit. Standaard zorgen firewalls en NAT's voor eenrichtingsaudio of geen audio. Cisco IOS® en PIX NATs en firewalls hebben de mogelijkheid om die verbindingen aan te passen zodat tweerichtingsaudio kan stromen.Als u Layer 3 mobiliteit gebruikt, kan uw netwerk stroomopwaarts verkeer blokkeren met controles van Unicast omgekeerd pad doorsturen (uRPF).
- Er kan eenrichtingsaudio optreden als ARP-caching niet op de WLC is ingesteld.

Choppy of Robotic Audio

- Een veel voorkomende reden voor hakkelen of robotachtige audio is wanneer een magnetron in de buurt werkt. Microgolven beginnen bij kanaal 9 en kunnen zich uitstrekken van kanalen 6 tot 14.
- Controleer op 2,4 GHz draadloze telefoons en andere verplegers draadloze apparaten die

gereedschap zoals Cognio gebruiken.

Problemen met registratie en verificatie

Wanneer u problemen met authenticatie ondervindt, voer deze controles uit:

- Controleer SSID's om er zeker van te zijn dat ze op de badge en het toegangspunt (of netwerk) overeenkomen. Zorg er ook voor dat het netwerk een route naar de Vocera server heeft.
- Controleer de sleutels van de EVN om ervoor te zorgen dat ze overeenkomen. Het is een goed idee om ze opnieuw in te voeren op het BCU (Badge Configuration Utility) en de badge opnieuw te programmeren, omdat het gemakkelijk is om een typefout te maken wanneer u een de sleutel of het wachtwoord van de EVN ingaat.

Deze berichten of symptomen kunnen voorkomen:

- Kan niet alle gevraagde mogelijkheden ondersteunen—dit is waarschijnlijk een coderingsfout tussen het access point en de client.
- Verificatie mislukt/geen AP gevonden — Zorg dat de authenticatietypen op het toegangspunt en de client overeenkomen.
- Geen service - IP Config is mislukt - Als u statische EFN gebruikt, zorg er dan voor dat de toetsen correct zijn geconfigureerd. Zorg ervoor dat andere klanten DHCP kunnen ontvangen met behulp van de zelfde SSID.
- Schakel alle TKIP-clients uit AP-Dit probleem op wanneer het access point twee MIC-fouten binnen 60 seconden detecteert. Deze tegenmaatregel voorkomt dat alle TKIP-clients gedurende 60 seconden opnieuw worden geauthentificeerd.
- Herauthenticatie / Time-out sessie—Indien geconfigureerd leidt een sessie-tijdelijke versie tot een herverificatie die lacunes in de spraakstroom veroorzaakt (300 ms + WAN-vertraging voor 802.1x verificatie).

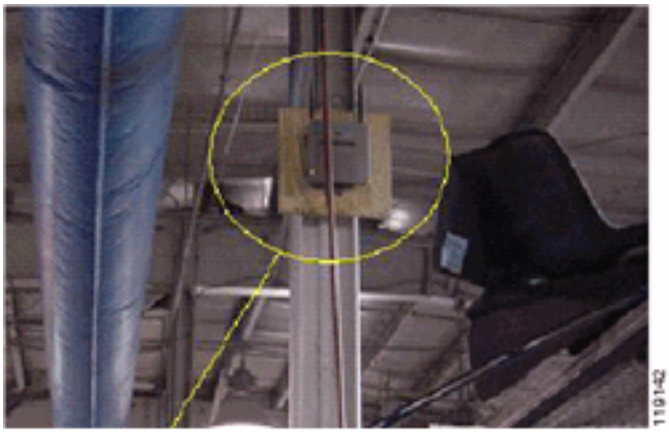
Bijlage A

Plaatsing van AP en antenne

In dit deel worden voorbeelden gegeven van zowel goede als ongeschikte plaatsing van toegangspunten (AP's) en antennes.

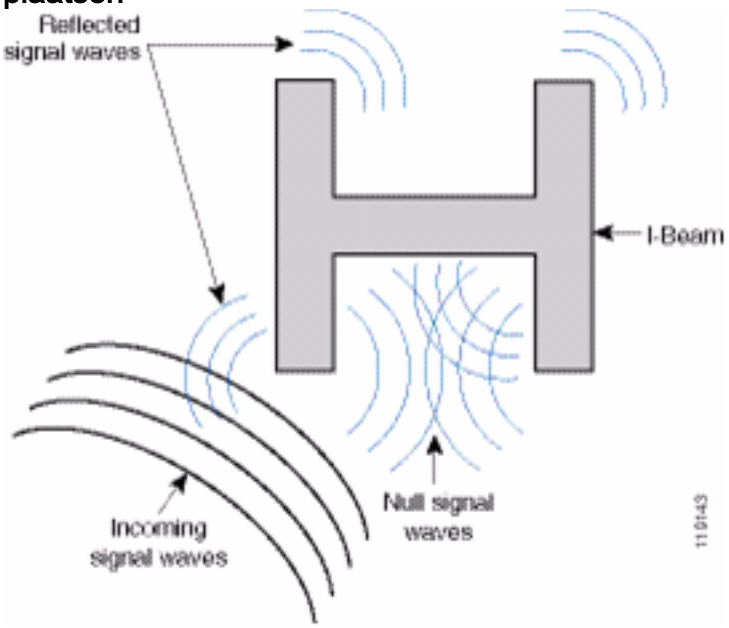
Afbeelding 17 toont de ongepaste plaatsing van een toegangspunt en antennes in de buurt van een I-bundel, hetgeen vervormde signaalpatronen creëert. Een RF nul-punt wordt gecreëerd door de oversteek van signaalgolven en multipath vervorming wordt gecreëerd wanneer signaalgolven worden gereflecteerd. Deze plaatsing resulteert in zeer weinig dekking achter het toegangspunt en verminderde signaalkwaliteit voor het toegangspunt.

Afbeelding 17 — Onjuiste plaats van antennes bij een I-straal



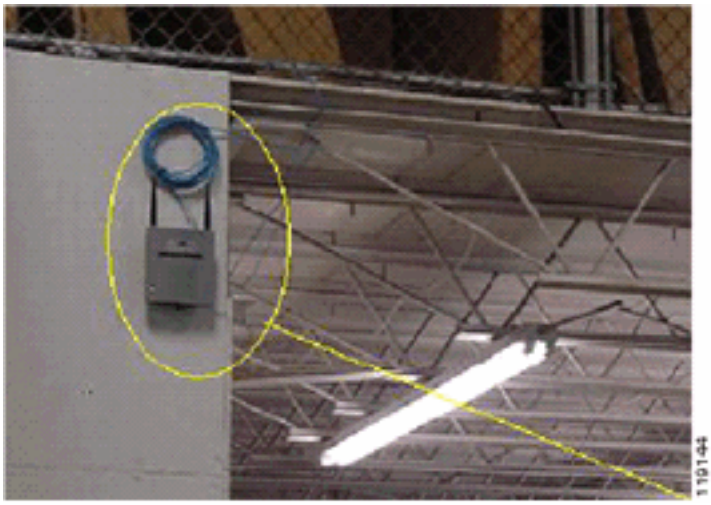
Afbeelding 18 toont de door een I-straal veroorzaakte wijzigingen of vervormingen van de signaaldoorgifte. De I-straal maakt veel reflecties van zowel ontvangen pakketten als verzonden pakketten. De gereflecteerde signalen resulteren in zeer slechte signaalkwaliteit wegens nul punten en multipath interferentie. De signaalsterkte is echter hoog omdat de antennes van het toegangspunt zich zo dicht bij de I-straal bevinden.

Afbeelding 18. Signaalvervormingen veroorzaakt door de antennes te dicht bij een I-straal plaatsen



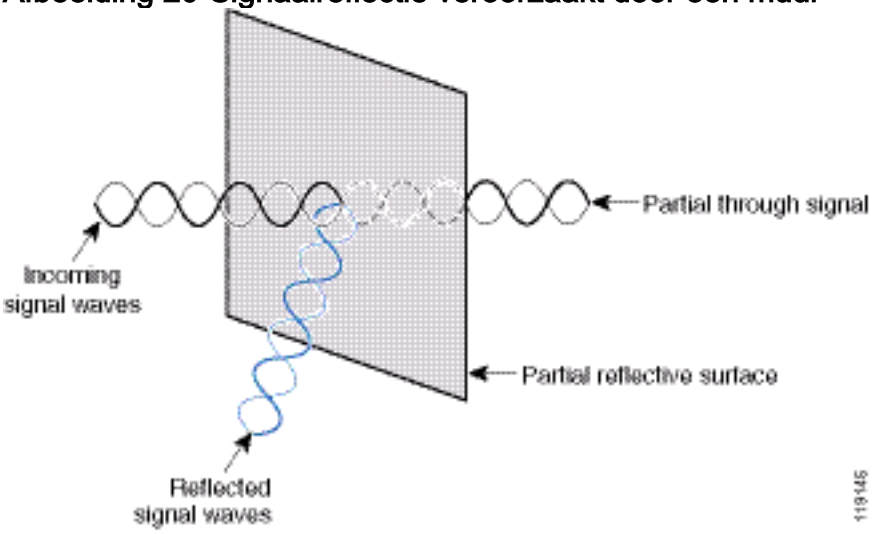
De plaatsing van het toegangspunt en de antenne in figuur 19 is beter omdat het weg is van de I-balken en er minder gereflecteerde signalen, minder ongeldige punten, en minder multipath interferentie zijn. Deze plaatsing is nog niet perfect omdat de Ethernet kabel niet zo dicht bij de antenne zou moeten worden besproeid. Het toegangspunt zou ook kunnen worden gedraaid met de 2,4 GHz antennes die op de vloer worden gericht. Dit biedt een betere dekking direct onder het toegangspunt. Er zijn geen gebruikers boven het toegangspunt.

Afbeelding 19. Access Point en Antennes gemonteerd op een muur, niet in I-bochten



Afbeelding 20 toont de signaalpropagatie veroorzaakt door de muur waarop het toegangspunt is gemonteerd.

Afbeelding 20-Signaalreflectie veroorzaakt door een muur

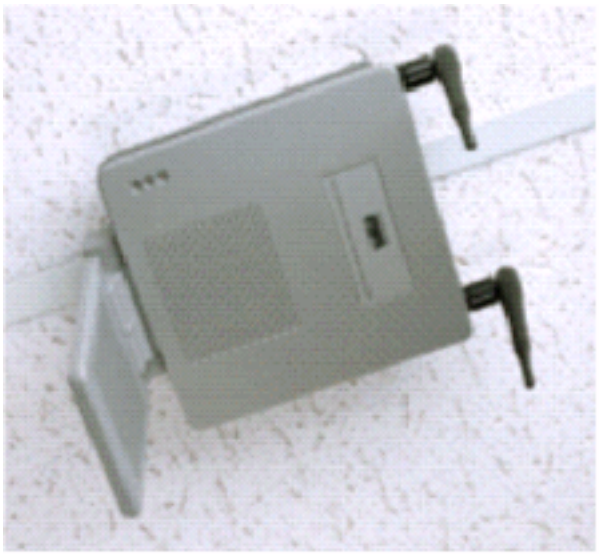


De bovenstaande voorbeelden zijn ook van toepassing wanneer u toegangspunten en antennes in of bij het plafond plaatst in een standaard ondernemingsomgeving. Als er metalen luchtafvoerslangen, liftschachten of andere fysieke barrières zijn die signaalreflectie of multipath-interferentie kunnen veroorzaken, raadt Cisco u ten zeerste aan om de antennes uit die barrières te halen. Verplaats de antenne een paar meter weg in het geval van de lift om de reflectie en vervorming van het signaal te voorkomen. Hetzelfde geldt voor luchtslangen aan het plafond.

Een enquête die wordt uitgevoerd zonder verzending en ontvangst van pakketten is niet voldoende. Het voorbeeld I-straal toont de creatie van ongeldige punten die uit pakketten kunnen voortkomen die CRC fouten hebben. Spraakpakketten met CRC-fouten worden gemist pakketten die de spraakkwaliteit nadelig beïnvloeden. In dit voorbeeld zouden deze pakketten boven de lawaaivloer kunnen zijn die door een enquêtegereedschap wordt gemeten. Daarom is het zeer belangrijk dat het site-onderzoek niet alleen signaalniveaus meet, maar ook pakketten genereert en vervolgens pakketfouten meldt.

Afbeelding 21 toont een Cisco AP1200 die correct aan een plafond T-bar wordt bevestigd, met de antennes in een omnidirectionele positie.

Afbeelding 21-Cisco AP1200 gemonteerd in een plafondinstallatie



Afbeelding 22 toont een omnidirectionele diversiteit-antenne van Cisco Aironet 5959 die correct op een plafond T-bar is gemonteerd. In dit geval wordt Cisco AP1200 boven de plafondtegel gemonteerd.

Afbeelding 22-Cisco Aironet 5959 antenne gemonteerd op plafond

Afbeelding 23 toont een Cisco AP1200 dat correct op een muur is bevestigd.

Afbeelding 23-Cisco AP1200 gemonteerd in een muur

Afbeelding 24 toont de Cisco Aironet 2012-patchantenne voor verscheidenheid die aan een muur is bevestigd. In dit geval wordt Cisco AP1200 boven de plafondtegel gemonteerd.

Afbeelding 24-Cisco Aironet 2012 antenne gemonteerd op een muur

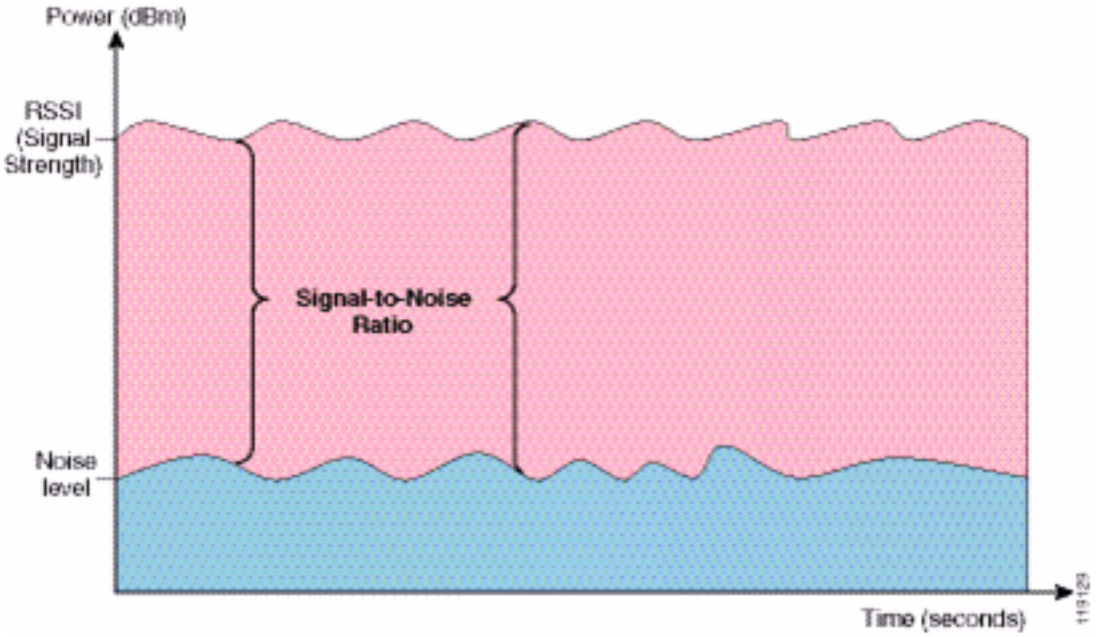
Voor gebieden waar het gebruikersverkeer hoog is (zoals kantoorruimten, scholen, winkels en ziekenhuizen) raadt Cisco u aan het toegangspunt uit het zicht te plaatsen en onopvallende antennes onder het plafond te plaatsen. De afstand voor antennes die geen diversiteit vertonen mag niet meer bedragen dan 18 inch.

Interferentie en multipath-verstoring

De doorvoerprestaties van het WLAN-netwerk worden beïnvloed door onbruikbare signalen. WLAN-interferentie kan worden gegenereerd door microgolfovens, 2,4 GHz draadloze telefoons, Bluetooth-apparaten of andere elektronische apparatuur die in de 2,4 GHz-band werken. Interferentie komt ook doorgaans van andere access points en clientapparaten die behoren tot de WLAN's maar ver genoeg verwijderd zijn, zodat hun signaal wordt verzwakt of beschadigd is. Access points die geen deel uitmaken van de netwerkinfrastructuur kunnen ook WLAN-interferentie veroorzaken en worden geïdentificeerd als knooppunten voor robuuste toegang.

Vervorming door interferentie en multipath oorzaak dat het overgebrachte signaal fluctueert. Interferentie vermindert de signaal-ruis ratio (SNR) voor een bepaald gegevenstarief. Het aantal pakketreizen gaat omhoog in een gebied waar de interferentie en/of multipath-vervorming hoog zijn. Interferentie wordt ook aangeduid als ruis- of geluidsniveau. De sterkte van het ontvangen signaal van het bijbehorende toegangspunt moet hoog genoeg zijn boven het geluidsniveau van de ontvanger om correct te worden gedecodeerd. Dit sterkte wordt de signaal-ruisverhouding of SNR genoemd. De ideale SNR voor het Vocera-badge is 25 dB. Als de geluidsvloer bijvoorbeeld 95 decibel per milliwatt (dBm) is en het ontvangen signaal aan de telefoon 70 dBm is, is de signaal-ruisverhouding 25 dB. (Zie afbeelding 25.)

Afbeelding 25-Signal-to-Noise verhouding (SNR)



Wanneer u het type en de locatie van de antenne wijzigt, kunnen er minder multipath vervorming en interferentie optreden. Een versterking van de antenne draagt bij aan de systeemversterking en kan de interferentie verminderen indien de storende zender niet rechtstreeks voor de richtantenne staat.

Hoewel gerichte antennes voor bepaalde binnentoepassingen van grote waarde kunnen zijn, gebruikt het overgrote deel van de binneninstallaties omnidirectionele antennes. De directionaliteit moet strikt worden vastgesteld door middel van een correct en juist onderzoek ter plaatse. Of u nu een omnidirectionele of een patchantenne gebruikt, binnenomgevingen hebben diversiteitantennes nodig om multipath-vervorming tegen te gaan. De Cisco Aironet Series Access Point-radio's bieden ondersteuning voor diversiteit.

Signaal

Signaalverzwakking of -verlies treedt op, zelfs wanneer het signaal door de lucht gaat. Het verlies van de signaalsterkte is meer uitgesproken wanneer het signaal door verschillende objecten passeert. Een transmissievermogen van 20 mW is gelijk aan 13 dBm. Als het overdraagvermogen op het ingangspunt van een gipsplaten 13 dBm bedraagt, wordt de signaalsterkte bij het verlaten van die muur teruggebracht tot 10 dBm. In deze tabel wordt het waarschijnlijke verlies in signaalsterkte weergegeven dat door verschillende typen objecten wordt veroorzaakt.

Signaal veroorzaakt door verschillende soorten objecten

Object in signaalpad	Signaal via object
Plasterboard	3 dB
Glaswand met metalen frame	6 dB
Cinder blok muur	4 dB
Office-venster	3 dB
Metalen deur	6 dB
Metalen deur in stenen muur	12 dB
Menselijk lichaam	3 dB

Elke geïnterviewde site heeft verschillende niveaus van vervorming via meerdere snijpad,

signaalverlies en signaalruis. Ziekenhuizen zijn doorgaans de meest uitdagende omgeving om te onderzoeken door hoge vervorming via meerdere paden, signaalverliezen en signaalruis. Ziekenhuizen nemen langer tijd in beslag om te onderzoeken, hebben een grotere populatie toegangspunten nodig en hebben betere prestatienormen nodig. De volgende moeilijkst te onderzoeken zijn fabrieksvloeren en fabrieksvloeren. Deze locaties hebben meestal metalen zijden en veel metalen objecten op de vloer, wat resulteert in gereflecteerde signalen die multipath-vervorming herscheppen. Kantoorgebouwen en ziekenhuislocaties hebben over het algemeen een hoge signaalvermindering maar een geringere mate van vervorming op meerdere aansluitingen.

Gerelateerde informatie

- Deploying Cisco 440X Series Wireless LAN Controllers (Cisco 440X Series wireless LAN-controllers implementeren)
- ReferentiNetwork-ontwerp van oplossing
- Videoscape Communications systeemspecificaties
- Technische ondersteuning en documentatie – Cisco Systems