Bereitstellung von Vocera IP-Telefonen in der Cisco Unified Wireless Network-Infrastruktur

Inhalt

Einführung

Dieses Dokument enthält Design- und Bereitstellungsrichtlinien für die Implementierung der Vocera® Badge Voice over WLAN (VoWLAN)-Technologie in der Cisco Unified Wireless Network-Infrastruktur.

Hinweis: Unterstützung für Vocera-Produkte sollte direkt von den Vocera-Support-Kanälen bezogen werden. Der technische Support von Cisco ist nicht für die Unterstützung von Problemen im Zusammenhang mit dem Vocera geschult.

Dieser Leitfaden ist eine Ergänzung zum Cisco Wireless LAN Controller Deployment Guide und behandelt nur die Konfigurationsparameter, die für Vocera VoWLAN-Geräte in einer Lightweight-Architektur spezifisch sind. Weitere Informationen finden Sie unter Bereitstellen der Cisco Wireless LAN Controller der Serie 440X.

Voraussetzungen

Anforderungen

Es wird davon ausgegangen, dass die Leser mit den Begriffen und Konzepten vertraut sind, die im Cisco IP-Telefonie-SRND und im Cisco Wireless LAN SRND vorgestellt werden. .

Wireless UC-Designleitfaden:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_wireless_uc.html

Cisco Unified Communications SRND basierend auf Cisco Unified Communications Manager 7.x:

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_uc_mgr.html

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Zusammenfassung

In dieser Tabelle sind die vier wichtigsten Funktionen und ihr Verhalten in einem Cisco Unified Wireless-Netzwerk zusammengefasst.

	Ein Controller	Layer-2-Roaming zwischen Controllern	Layer-3-Roaming zwischen Controllern
Badge-to-Badge	Keine spezielle Konfiguration	Keine spezielle Konfiguration	Keine spezielle Konfiguration
Badge-to-Phone	Keine spezielle Konfiguration	Keine spezielle Konfiguration	Keine spezielle Konfiguration
Badge-to-Broadcast	Controller-Multicast aktivieren	Aktivieren von Controller Multicast Deaktivieren des Vocera-VLAN IGMP-Snooping oder Ausführen von 4.0.206.0 oder höher	4.0.206.0 oder spätere Version
Badge-Standort	Keine spezielle Konfiguration	Keine spezielle Konfiguration	Keine spezielle Konfiguration

Vocera-Badge - Übersicht

Die Kommunikations-Badges ermöglichen eine sofortige Kommunikation mit jedem anderen Badge-Träger, eine Integration von Private Branch Exchange (PBX) und die Nachverfolgung des Badge-Standorts. Die Nutzung eines 802.11b/g-Wireless-Netzwerks erfordert die Bereitstellung von Multicast- und UDP-Unicast-Paketen mit eingeschränkten QoS-Anforderungen (Quality of Service) ab Version 3.1 der Vocera Server-Software (Build 1081). Die Verschlüsselungsfunktionen umfassen 64/128 Bit Wired Equivalent Privacy (WEP), Temporal Key Integrity Protocol (TKIP),

Message Integrity Check (MIC) und Cisco Temporal Key Integrity Protocol (CKIP) in Verbindung mit den Authentifizierungsfunktionen von Open, Wi-Fi Protected Access-Pre-Shared Key (WPA-PSK), WPA-Protected Extensible Authentication Protocol (PEAP) und LEAP (Lightweight Extensible Authentication Protocol)

Mit einem Tastendruck antwortet der Vocera-Server mit `Vocera`, einer Eingabeaufforderung für Befehle wie **Record**, **wobei (am I) /is....**, **Call**, **Play, Broadcast, Nachrichten usw. ist.** Der Vocera-Server stellt die erforderlichen Dienste und/oder die Anrufeinrichtung bereit, um die Anfrage abzuschließen.

Das 802.11b-fähige Kommunikationssystem von Vocera verwendet proprietäre Sprachkomprimierung und einen UDP-Port-Bereich. Die Vocera-Systemsoftware wird auf einem Windows-Server ausgeführt, der die Anrufeinrichtung, die Anrufverbindung und die Benutzerprofile verwaltet. Gemeinsam mit der Software Nuance 8.5 Speech Recognition und Voiceprint ermöglichen sie die Nutzung von Badge-Sprachkommunikation. Vocera empfiehlt einen separaten Windows-Server, um die Vocera Telefony Solutions Software auszuführen, um die Verbindung zwischen Plain Old Telefone Service (POTS) und den Badges zu ermöglichen.

Überlegungen zur Anrufkapazität bei Vocera

Weitere Informationen finden Sie im Abschnitt Netzwerkskalierung dieses Dokuments.

Kapazität des Vocerca Communications Servers

Weitere Informationen zur Bedarfsbestimmung des Vocera-Servers finden Sie in den Vocera Communications System Specifications (Systemspezifikationen für Vocera-Server).

Die Vocera-Lösung

Die Vocera-Plakette verwendet sowohl die Unicast- als auch die Multicast-Paketübermittlung, um mehrere wichtige Funktionen für diese Komplettlösung bereitzustellen. Im Folgenden sind vier grundlegende Funktionen aufgeführt, die auf eine ordnungsgemäße Paketübermittlung basieren. Außerdem wird erläutert, wie die einzelnen Funktionen das zugrunde liegende Netzwerk für die Bereitstellung und Funktionalität nutzen.

- Badge to Badge Communications (Badge-to-Badge-Kommunikation): Wenn ein Vocera-Benutzer einen anderen Benutzer anruft, kontaktiert das Badge zuerst den Vocera-Server, der die IP-Adresse des Ausweises des Angerufenen abfragt und den Badge-Benutzer kontaktiert, um den Benutzer zu fragen, ob er einen Anruf entgegennehmen kann. Wenn der Angerufene den Anruf annimmt, benachrichtigt der Vocera-Server das anrufende Badge über die IP-Adresse des angerufenen Badge, um eine direkte Kommunikation zwischen den Badges ohne weitere Servereingriffe einzurichten. Für die gesamte Kommunikation mit dem Vocera-Server wird der G.711-Codec verwendet, und für die Kommunikation zwischen Abzeichen wird ein proprietärer Vocera-Codec verwendet.
- Badge Telefony Communication (Badge-Telefonie-Kommunikation): Wenn ein Vocera-Telefonieserver installiert und mit einer Verbindung zu einem PBX-System eingerichtet wird, kann ein Benutzer interne Nebenstellen vom PBX-System oder von externen Telefonleitungen anrufen. Vocera ermöglicht es Benutzern, Anrufe zu tätigen, indem sie entweder die Zahlen

(fünf, sechs, drei, zwei) oder einen Adressbucheintrag in der Vocera-Datenbank für die Person oder Funktion unter dieser Nummer (z. B. Apotheke, zu Hause, Pizza) erstellen. Der Vocera-Server bestimmt die Nummer, die angerufen wird, entweder durch Abfangen der Nummern in der Durchwahl oder durch Aussehen des Namens in der Datenbank und Auswählen der Nummer. Der Vocera-Server leitet diese Informationen dann an den Vocera-Telefonieserver weiter, der eine Verbindung zum PBX herstellt und die entsprechende Telefonie-Signalisierung (z. B. DTMF) erzeugt. Für die Kommunikation zwischen dem Badge- und Vocera-Server und dem Vocera-Server und dem Vocera-Telefonieserver wird der G.711-Codec über Unicast-UDP verwendet.

- Vocera Broadcast - Ein Benutzer eines Vocera-Badge-Geräts kann gleichzeitig eine Gruppe von Vocera-Badge-Trägern anrufen und mit dieser kommunizieren, indem er den Befehl Broadcast verwendet. Wenn ein Benutzer an eine Gruppe sendet, sendet das Badge des Benutzers den Befehl an den Vocera-Server, der dann die Mitglieder einer Gruppe sucht, feststellt, welche Mitglieder der Gruppe aktiv sind, eine Multicast-Adresse für diese Broadcast-Sitzung zuweist und eine Nachricht an das Badge jedes aktiven Benutzers sendet, die ihn anweist, der Multicast-Gruppe mit der zugewiesenen Multicast-Adresse beizutreten.
- Badge Location Function (Ort der Plakette): Der Vocera-Server verfolgt den Access Point, dem jedes aktive Badge zugeordnet ist, da jedes Badge eine Keep-Alive-Dauer von 30 Sekunden an den Server mit der zugehörigen BSSID sendet. Auf diese Weise kann das Vocera-System den Standort eines Ausweisbenutzers grob schätzen. Diese Funktion hat eine relativ geringe Genauigkeit, da ein Badge möglicherweise nicht dem Access Point zugeordnet wird, dem es am nächsten liegt.

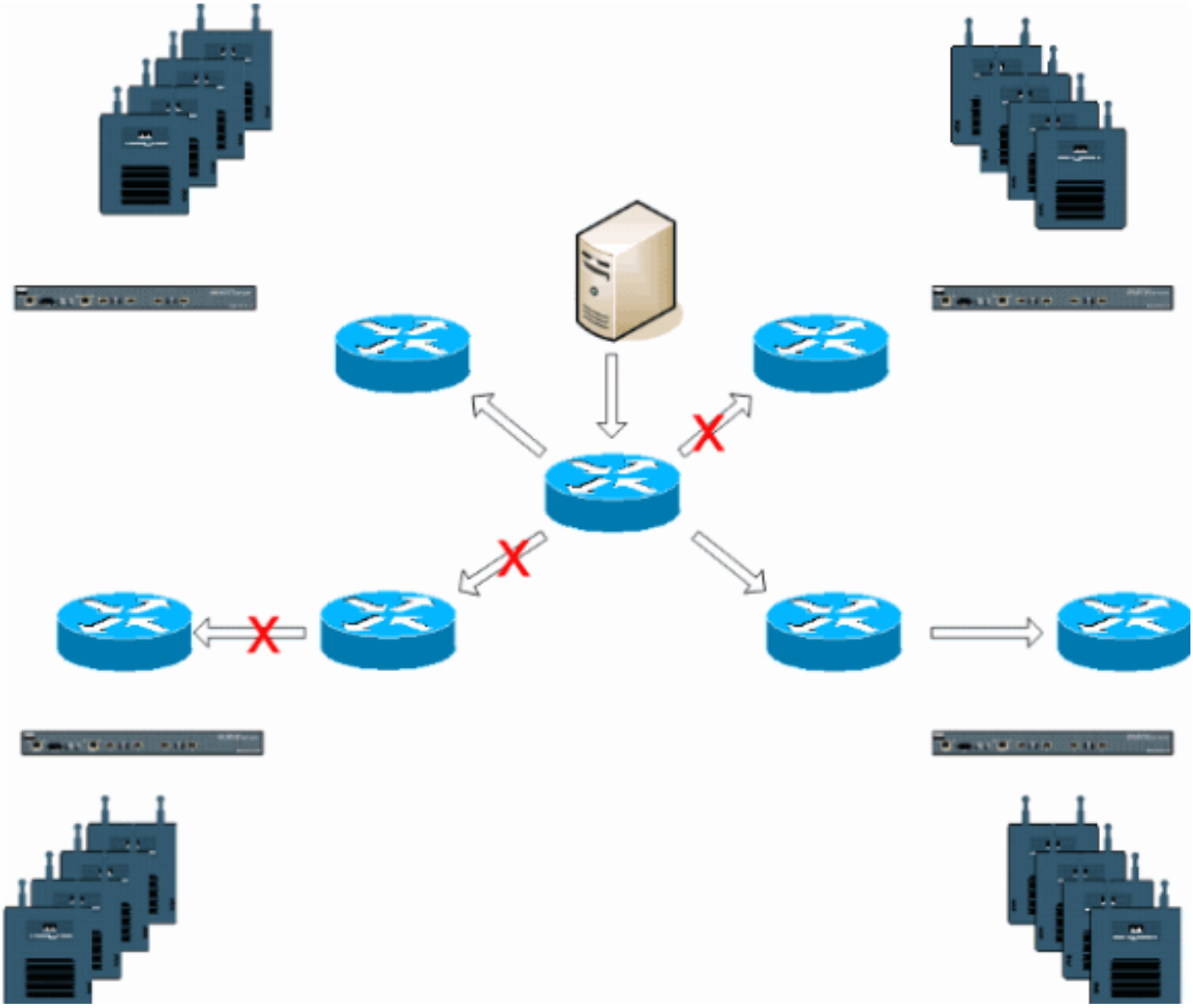
Infrastrukturplanung bei Vocera

Der Vocera Whitepaper Vocera Infrastructure Planning Guide beschreibt die Mindestanforderungen für die Standortprüfung, die belegen, dass das Badge über eine Empfangssignalstärke von mindestens -65 dBm, ein Signal-Rausch-Verhältnis von mehr als 25 dB und eine ordnungsgemäße Überlappung der Access Points und Kanaltrennung verfügen muss. Obwohl die Ausweise eine ähnliche Rundstrahlantenne als Notebook verwenden, das für eine Standortuntersuchung verwendet wird, imitiert sie das Verhalten des Ausweises nicht besonders gut, da die Wearers die Signalstärke beeinflussen. Angesichts dieser einzigartigen Anforderung und dieses Verhaltens des Sendegeräts ist die Verwendung der Cisco Architektur und des Radio Resource Management ideal, um sicherzustellen, dass es an ungewöhnlichen Funkfrequenzstandortmerkmalen mangelt.

Das Vocera-Badge ist ein stromsparendes Gerät, das neben dem Körper getragen wird und nur begrenzte Signalfehlerbehebungsfunktionen bietet. Die Vocera-Anforderungen in diesem Dokument lassen sich problemlos erreichen. Sie kann jedoch überlastet werden, wenn zu viele SSIDs vorhanden sind, die verarbeitet werden können und eine effektive Nutzung des Badge ermöglichen.

Architekturübersicht

Abbildung 1: Allgemeine Multicast-Weiterleitung und -Bereinigung mit LWAPP (Lightweight Access Point Protocol) Wireless



Multicast in einer LWAPP-Bereitstellung

Zur Bereitstellung der Vocera-Broadcast-Funktion ist es erforderlich, Multicast innerhalb einer LWAPP-Bereitstellung zu verstehen. In diesem Dokument werden später die wichtigsten Schritte zur Aktivierung von Multicast in der controllerbasierten Lösung beschrieben. Der LWAPP-Controller verwendet derzeit zwei Bereitstellungsmethoden, um Multicast für die Clients bereitzustellen:

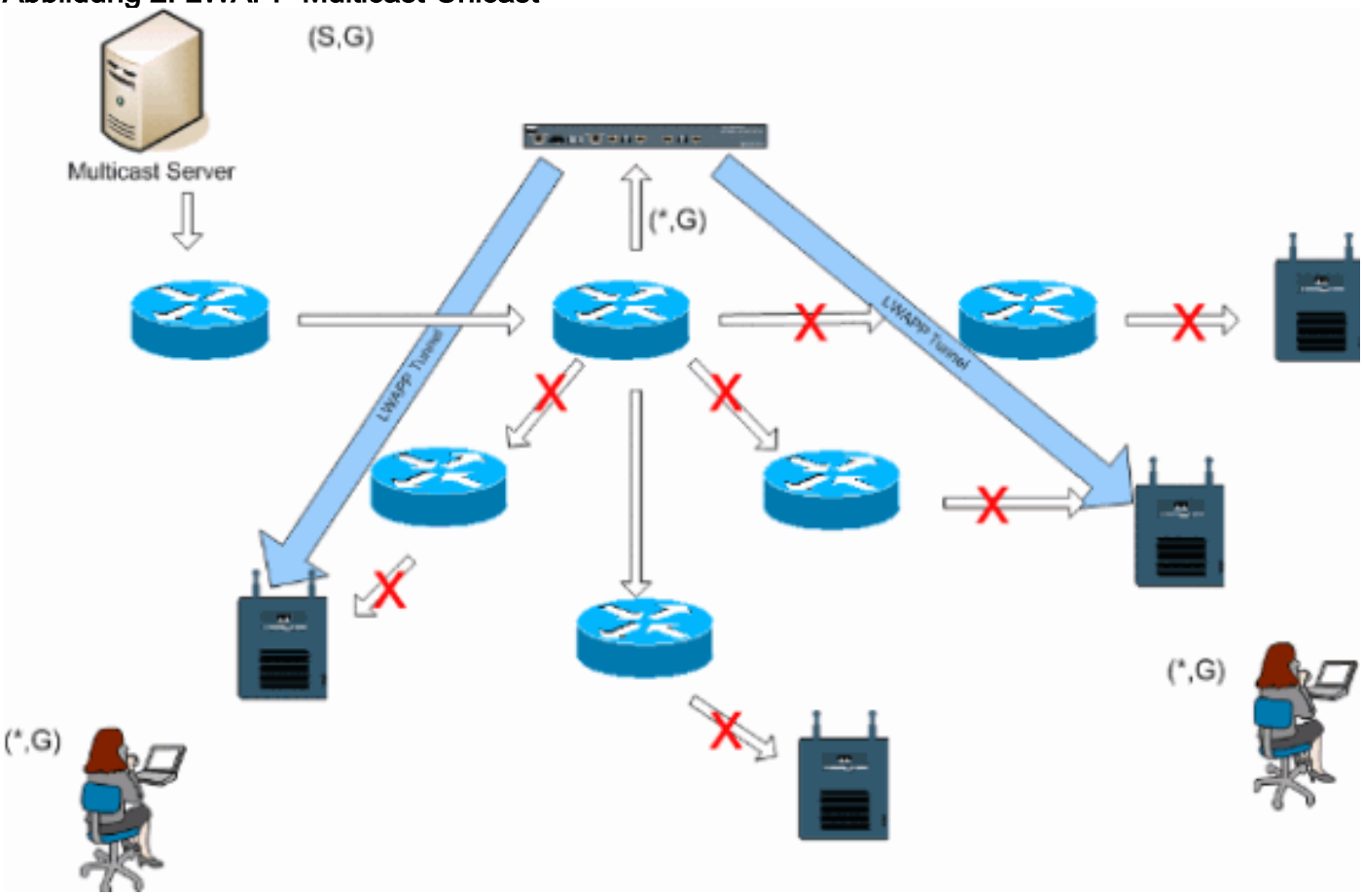
- Unicast-Multicast
- Multicast-Multicast

Bereitstellungsmethode für Unicast-Multicast

Die Unicast-Multicast-Zustellmethode erstellt eine Kopie jedes Multicast-Pakets und leitet es an jeden Access Point weiter. Wenn ein Client eine Multicast-Verbindung zum Wireless LAN sendet, leitet der Access Point diese Verbindung über den LWAPP-Tunnel an den Controller weiter. Der Controller verbindet diese Multicast-Verbindung mit der direkt verbundenen lokalen Netzwerkverbindung, die das Standard-VLAN für das zugeordnete WLAN des Clients ist. Wenn ein IP-Multicast-Paket vom Netzwerk zum Controller eingeht, repliziert der Controller dieses Paket mit einem LWAPP-Header für jeden Access Point, der über einen Client innerhalb der Wireless-

Domäne verfügt, der dieser spezifischen Gruppe beigetreten ist. Wenn die Quelle des Multicast auch ein Empfänger innerhalb der Wireless-Domäne ist, wird dieses Paket dupliziert und an denselben Client weitergeleitet, der das Paket gesendet hat. Bei Vocera-Badges ist dies nicht die bevorzugte Methode der Multicast-Bereitstellung innerhalb der LWAPP-Controller-Lösung. Die Unicast-Bereitstellungsmethode funktioniert bei kleinen Bereitstellungen. Aufgrund des beträchtlichen Overhead auf dem Wireless LAN Controller (WLC) ist dies jedoch niemals die empfohlene Multicast-Bereitstellungsmethode.

Abbildung 2: LWAPP Multicast-Unicast



Hinweis: Wenn AP-Gruppen-VLANs konfiguriert sind und ein IGMP-Join von einem Client über den Controller gesendet wird, wird er im Standard-VLAN des WLAN platziert, in dem sich der Client befindet. Daher empfängt der Client diesen Multicast-Datenverkehr möglicherweise nur, wenn der Client Mitglied dieser standardmäßigen Broadcast-Domäne ist.

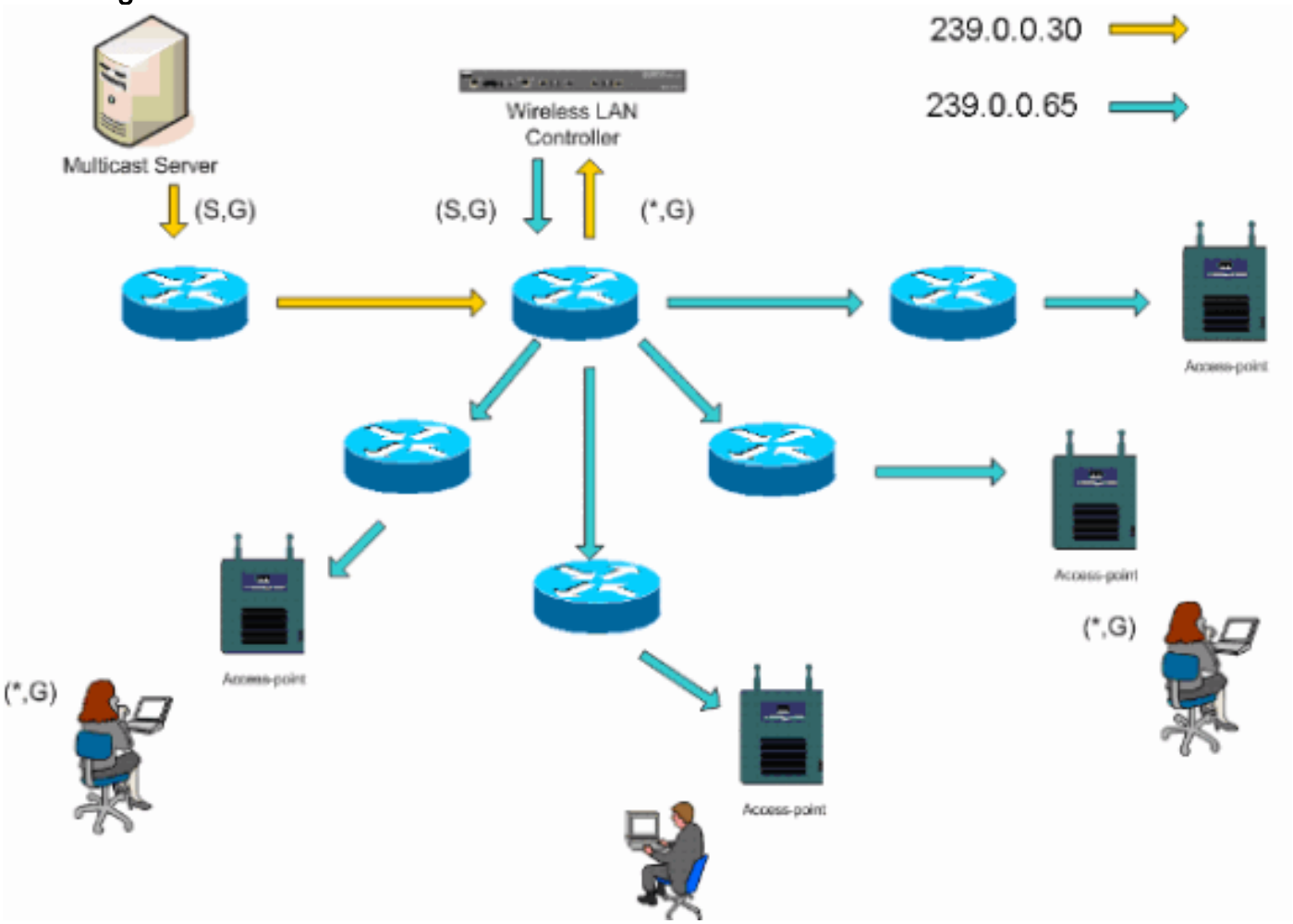
Multicast-Multicast-Bereitstellungsmethode

Bei der Multicast-Multicast-Zustellmethode muss der Controller nicht jedes empfangene Multicast-Paket replizieren. Der Controller ist für eine nicht verwendete Multicast-Gruppenadresse konfiguriert, der jeder Access Point angehört. In Abbildung 3 ist die vom WLC zum Access Point definierte Multicast-Gruppe 239.0.0.65. Wenn ein Client eine Multicast-Verbindung zum WLAN sendet, leitet der Access Point diese Verbindung über den LWAPP-Tunnel an den Controller weiter. Der Controller leitet dieses Link-Layer-Protokoll an die direkt verbundene LAN-Verbindung weiter, die das Standard-VLAN für das zugeordnete WLAN des Clients ist. Der lokale Router des Controllers fügt dieser Schnittstelle diese Multicast-Gruppenadresse für den Weiterleitungseintrag (*,G) hinzu. In Abbildung 3 wurde die Multicast-Beispielverbindung an die Multicast-Gruppe 239.0.0.30 gesendet. Wenn das Netzwerk jetzt Multicast-Datenverkehr weiterleitet, wird die Multicast-Adresse 239.0.0.30 an den Controller weitergeleitet. Der Controller kapselt das Multicast-Paket anschließend in ein an die Multicast-Gruppenadresse adressiertes LWAPP-

Multicast-Paket (Beispiel: 239.0.0.65), das auf dem Controller konfiguriert und an das Netzwerk weitergeleitet wird. Jeder Access Point auf dem Controller empfängt dieses Paket als Mitglied der Multicast-Gruppe der Controller. Der Access Point leitet dann das Multicast-Paket der Clients/Server (Beispiel: 239.0.0.30) als Broadcast an das im LWAPP-Multicast-Paket identifizierte WLAN/SSID weiter.

Hinweis: Wenn Sie Ihr Multicast-Netzwerk falsch konfigurieren, können Sie am Ende Multicast-Pakete eines anderen Controllers empfangen. Wenn der erste Controller dieses Multicast-Paket fragmentieren muss, wird das Fragment an das Netzwerk weitergeleitet, und jeder Access Point muss Zeit verbringen, dieses Fragment zu verwerfen. Wenn Sie den gesamten Datenverkehr, wie z. B. den 224.0.0.x-Multicast-Bereich, zulassen, wird dieser ebenfalls gekapselt und anschließend von jedem Access Point weitergeleitet.

Abbildung 3: LWAPP Multicast Multicast



Multicast-Konfiguration für Router und Switch

Dieses Dokument ist kein Netzwerk-Multicast-Konfigurationsleitfaden. Eine vollständige Beschreibung der Implementierung finden Sie unter Konfigurieren von IP-Multicast-Routing. In diesem Dokument werden die Grundlagen für die Aktivierung von Multicast in Ihrer Netzwerkumgebung erläutert.

IP-Multicast-Routing aktivieren

IP-Multicast-Routing ermöglicht der Cisco IOS®-Software die Weiterleitung von Multicast-Paketen. Der globale Konfigurationsbefehl **ip Multicast-Routing** ist erforderlich, damit Multicast in jedem

Multicast-fähigen Netzwerk ausgeführt werden kann. Der Befehl **ip multicast-routing** sollte auf allen Routern im Netzwerk zwischen den WLCs und den jeweiligen Access Points aktiviert werden.

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

Aktivieren von PIM an einer Schnittstelle

Dadurch wird die Routing-Schnittstelle für den IGMP-Betrieb (Internet Group Management Protocol) aktiviert. Der Protocol Independent Multicast (PIM)-Modus legt fest, wie der Router seine Multicast-Routing-Tabelle ausfüllt. Das hier gezeigte Beispiel erfordert nicht, dass der Rendezvous Point (RP) für die Multicast-Gruppe bekannt ist. Daher ist der Sparse-Dense-Modus der wünschenswerteste, wenn man bedenkt, dass Ihre Multicast-Umgebung unbekannt ist. Es wird nicht empfohlen, Multicast für die Funktion zu konfigurieren. Die direkt mit dem Controller verbundene Layer-3-Schnittstelle sollte jedoch PIM aktivieren, damit Multicast funktioniert. Alle Schnittstellen zwischen WLC(s) und den jeweiligen Access Points sollten aktiviert sein.

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

Deaktivieren des Switch-VLAN IGMP-Snoopings

IGMP-Snooping ermöglicht ein Switch-Netzwerk mit aktiviertem Multicast, um den Datenverkehr auf die Switch-Ports zu begrenzen, deren Benutzer Multicast anzeigen möchten, während die Multicast-Pakete von Switch-Ports entfernt werden, die den Multicast-Stream nicht anzeigen möchten. Bei einer Bereitstellung von Vocera kann es unerwünscht sein, CGMP- oder IGMP-Snooping auf dem Upstream-Switch-Port zum Controller zu aktivieren, wenn Softwareversionen vor 4.0.206.0 vorliegen.

Roaming und Multicast werden nicht mit einer Reihe von Anforderungen definiert, um zu überprüfen, ob Multicast-Verkehr einem abonnierten Benutzer folgen kann. Das Client-Badge ist sich dessen bewusst, dass es roamtet hat, leitet jedoch kein weiteres IGMP-Join weiter, um sicherzustellen, dass die Netzwerkinfrastruktur weiterhin den Multicast-Datenverkehr (Vocera-Broadcast) an das Badge weiterleitet. Gleichzeitig sendet der LWAPP-Access Point keine allgemeine Multicast-Abfrage an den Roaming-Client, um eine Aufforderung zur Teilnahme am IGMP zu erhalten. Bei einem Layer-2-Vocera-Netzwerkdesign ermöglicht die Deaktivierung von IGMP-Snooping die Weiterleitung des Datenverkehrs an alle Mitglieder des Vocera-Netzwerks, unabhängig davon, wo sie sich gerade aufhalten. So wird sichergestellt, dass die Vocera-Broadcast-Funktion unabhängig vom Roaming-Standort des Clients funktioniert. Die globale Deaktivierung von IGMP-Snooping ist eine sehr unerwünschte Aufgabe. Es wird empfohlen, IGMP-Snooping nur auf dem Vocera-VLAN zu deaktivieren, das direkt mit jedem WLC verbunden ist.

Weitere Informationen finden Sie unter Konfigurieren von IGMP-Snooping.

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

Multicast-Verbesserungen in Version 4.0.206.0 und höher

Mit der Version 4.0.206.0 führt Cisco eine IGMP-Abfrage ein, um Benutzern das Roaming auf Layer 2 zu ermöglichen, indem sie eine allgemeine IGMP-Abfrage senden, wenn dies auftritt. Der Client antwortet daraufhin mit der IGMP-Gruppe, zu der er gehört. Diese wird, wie in diesem Dokument beschrieben, an das kabelgebundene Netzwerk überbrückt. Wenn ein Client mit einem Controller ohne Layer-2-Verbindung oder einem Layer-3-Roam wechselt, wird synchrones Routing für Multicast-Quellpakete hinzugefügt. Wenn ein Client, der ein Layer-3-Roam abgeschlossen hat, ein Multicast-Paket aus dem Wireless-Netzwerk sendet, kapselt der ausländische Controller dieses Paket in den Ethernet over IP (EoIP) im IP-Tunnel mit dem Anker-Controller. Der Anker-Controller leitet diese dann an die lokal verknüpften Wireless-Clients weiter und überbrückt sie mithilfe der normalen Multicast-Routing-Methoden zurück zum kabelgebundenen Netzwerk, in dem sie geroutet werden.

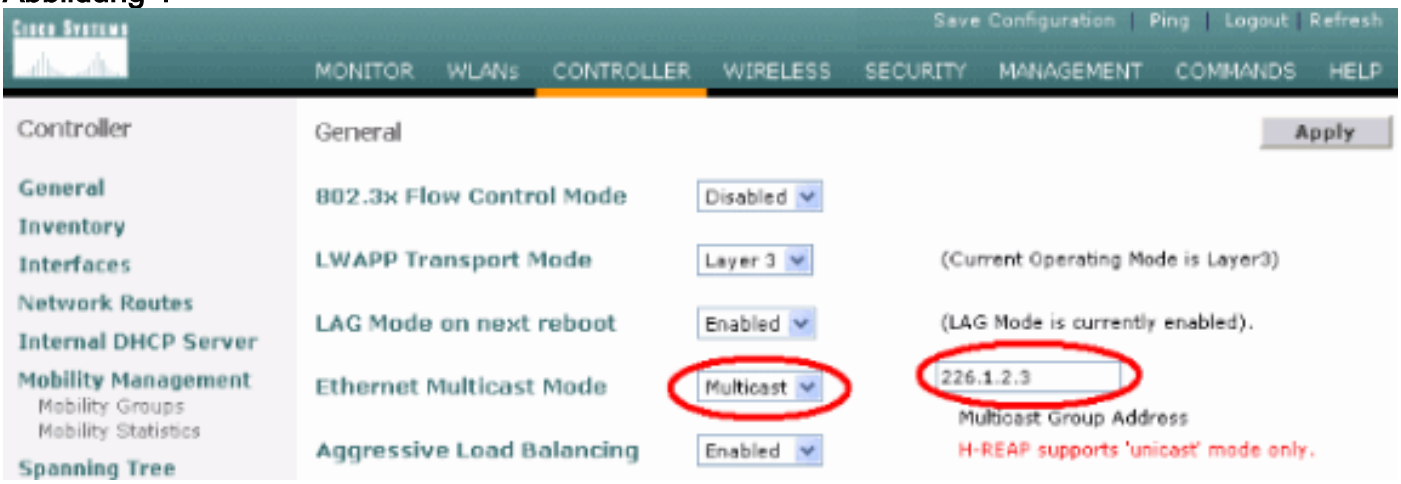
Bereitstellungsszenarien

Diese drei Bereitstellungsszenarien umfassen Best Practices und Entwurfsparameter für eine erfolgreiche Bereitstellung von Vocera Badge:

- Single Controller-Bereitstellung
- Layer-2-Bereitstellung für mehrere Controller
- Layer-3-Bereitstellung mehrerer Controller

Es ist wichtig zu verstehen, wie die Vocera-Badge-Funktionen in einer LWAPP Split MAC-Umgebung interagieren. Bei allen Bereitstellungsszenarien sollte Multicast aktiviert und der aggressive Lastenausgleich deaktiviert werden. Alle Badge-WLANs sollten in der gleichen Broadcast-Domäne im gesamten Netzwerk enthalten sein.

Abbildung 4



Single Controller-Bereitstellung

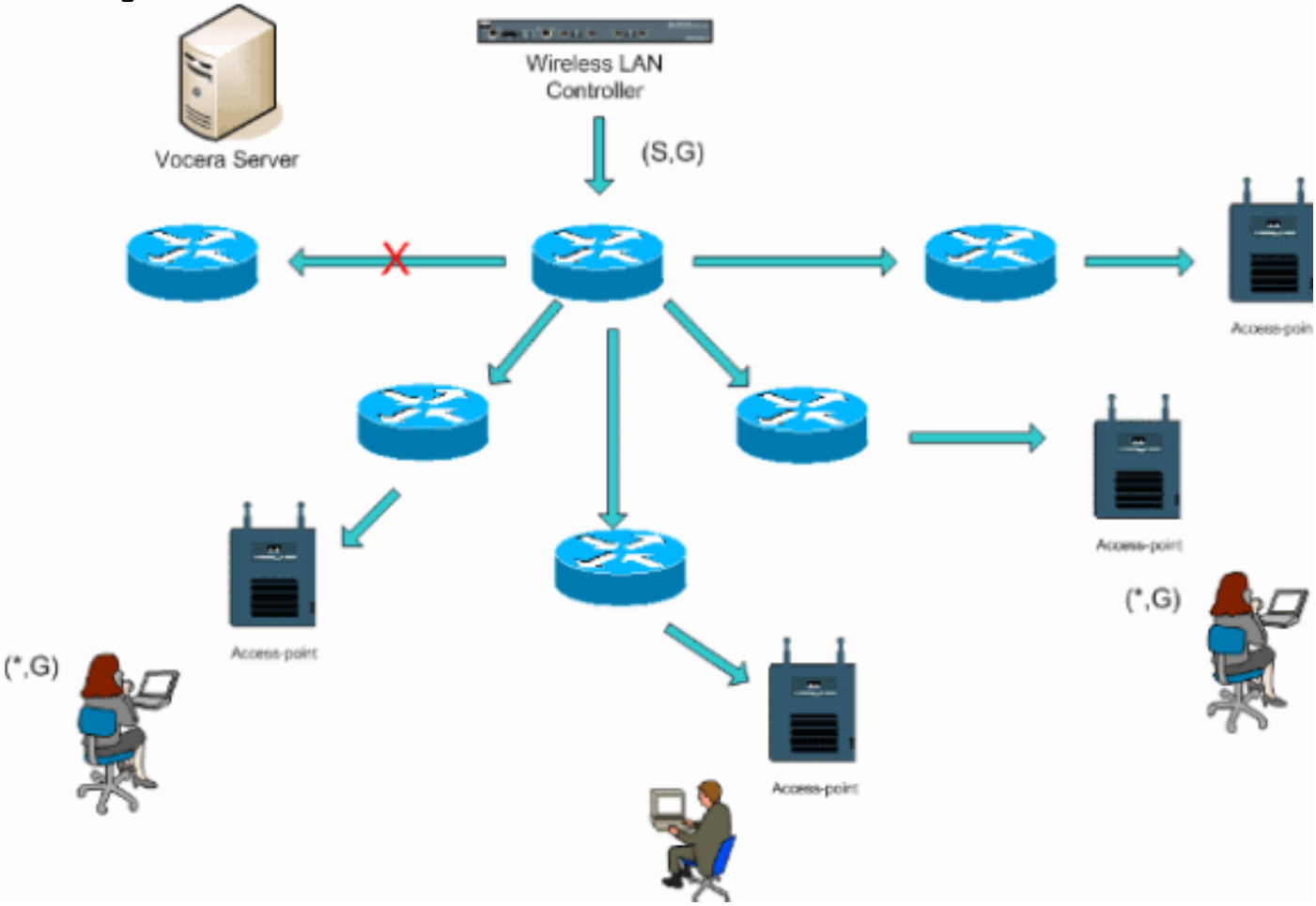
Dies ist das einfachste Bereitstellungsszenario. Mit dieser Lösung können Sie die Vocera Badge-Lösung ohne große Probleme bereitstellen. Ihr Netzwerk muss für IP-Multicast-Routing aktiviert sein, damit die Access Points die LWAPP-Multicast-Pakete empfangen können. Bei Bedarf können Sie die Multicast-Komplexität im Netzwerk begrenzen, indem Sie alle Router und Switches mit der Multicast-Gruppe der Controller konfigurieren.

Wenn Multicast global auf dem Controller konfiguriert ist, werden die richtige SSID, die Sicherheitseinstellungen und alle Access Points, die die Vocera Badge-Lösung registriert haben, und alle Funktionen wie erwartet ausgeführt. Mit der Vocera-Broadcast-Funktion werden ein Benutzer und der Multicast-Datenverkehr wie erwartet weitergeleitet. Es müssen keine

zusätzlichen Einstellungen konfiguriert werden, damit diese Lösung ordnungsgemäß funktioniert.

Wenn ein Vocera-Badge eine Multicast-Nachricht sendet, wie dies bei dem Vocera-Broadcast der Fall ist, wird diese an den Controller weitergeleitet. Der Controller kapselt dieses Multicast-Paket anschließend in ein LWAPP-Multicast-Paket. Die Netzwerkinfrastruktur leitet dieses Paket an jeden Access Point weiter, der mit diesem Controller verbunden ist. Wenn der Access Point dieses Paket empfängt, überprüft er anschließend den LWAPP-Multicast-Header, an welches WLAN/SSID das Paket gesendet wird.

Abbildung 5: Einzelner Controller im Multicast-Multicast-Modus



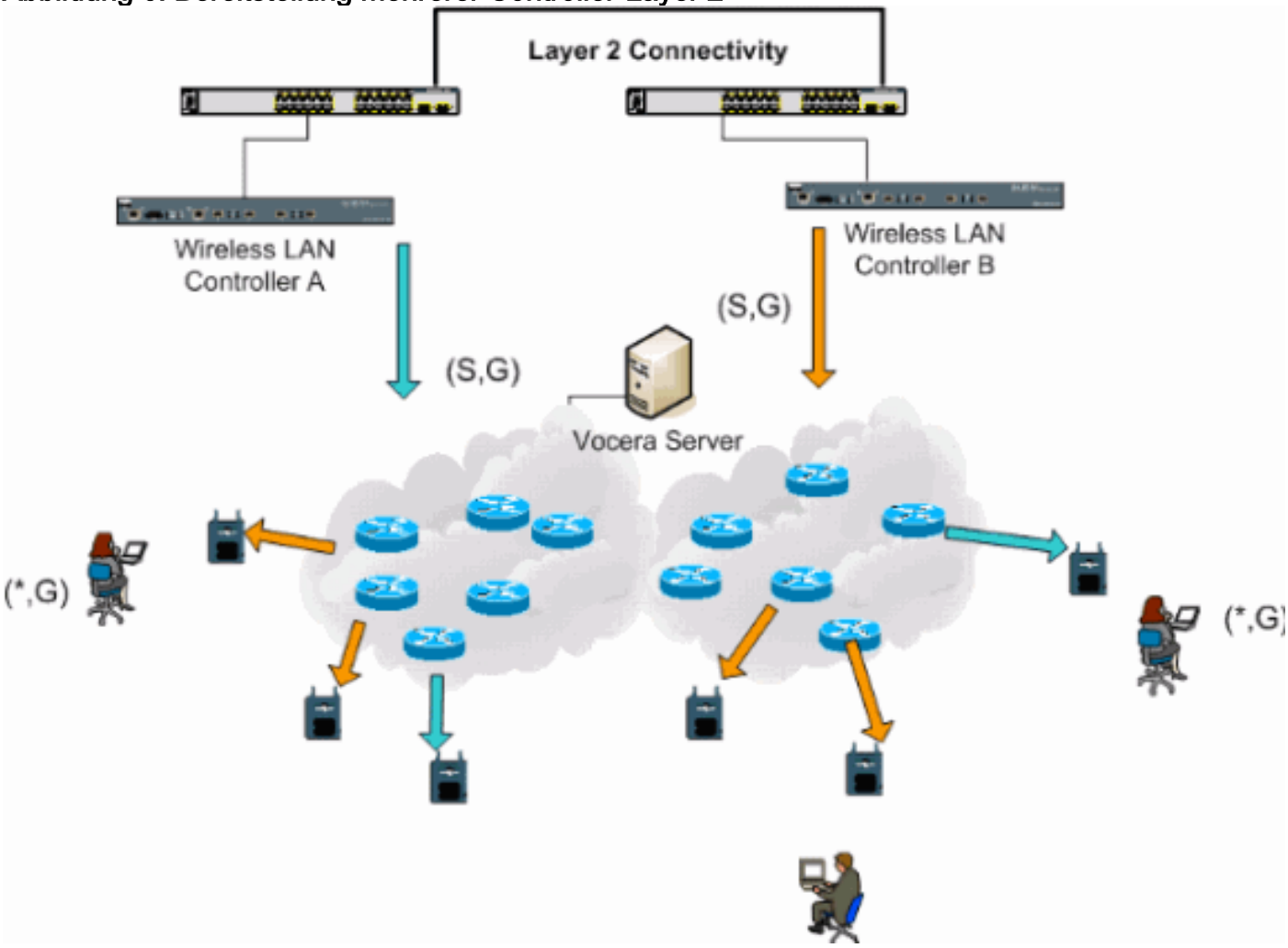
Layer-2-Bereitstellung für mehrere Controller

Mehrere Controller müssen über dieselbe Layer-2-Broadcast-Domäne miteinander verbunden sein. Beide Controller werden wie gezeigt für Multicast konfiguriert, wobei die identischen Access Point-Multicast-Gruppen auf jedem Controller verwendet werden, um die Fragmentierung zu begrenzen. Wenn diese Layer-2-Broadcast-Domäne über einen gemeinsamen Switch oder einen gemeinsamen Switch-Satz verbunden ist, muss CGMP/IGMP-Snooping auf diesen Switches für dieses einzelne VLAN deaktiviert oder die WLC-Software 4.0.206.0 oder höher ausgeführt werden. Mit der Vocera-Broadcast-Funktion und einem Roam von einem Access Point auf einem Controller zu einem Access Point auf einem anderen Controller gibt es keinen Mechanismus für die Weiterleitung von IGMP-Joins an den neuen Layer-2-Port, damit IGMP-Snooping funktioniert. Ohne ein IGMP-Paket, das den Upstream-CGMP oder IGMP-fähigen Switch erreicht, wird die angegebene Multicast-Gruppe nicht an den Controller weitergeleitet und daher nicht vom Client empfangen. In einigen Fällen kann dies funktionieren, wenn ein Client, der zur gleichen Vocera Broadcast-Gruppe gehört, dieses IGMP-Paket bereits gesendet hat, bevor der Roaming-Client auf den neuen Controller wechselt. Mit den Vorteilen von Version 4.0.206.0 erhält ein Client, der als Layer-2-Roam zu einem anderen Controller rommt, unmittelbar nach der Authentifizierung eine

allgemeine IGMP-Abfrage. Der Client sollte dann mit den interessierten Gruppen antworten, und der neue Controller wird dann mit dem lokal angeschlossenen Switch verbunden. Dadurch können die Vorteile von IGMP und CGMP auf Ihren Upstream-Switches genutzt werden.

Sie können zusätzliche Badge-SSIDs und Layer-2-Domänen für separate Badge-Netzwerke erstellen, solange Ihr Netzwerk so konfiguriert ist, dass Multicast-Datenverkehr ordnungsgemäß weitergeleitet wird. Darüber hinaus muss jede Layer-2-Broadcast-Domäne der Vocera überall dort vorhanden sein, wo ein Controller mit dem Netzwerk verbunden ist, damit Multicast nicht unterbrochen wird.

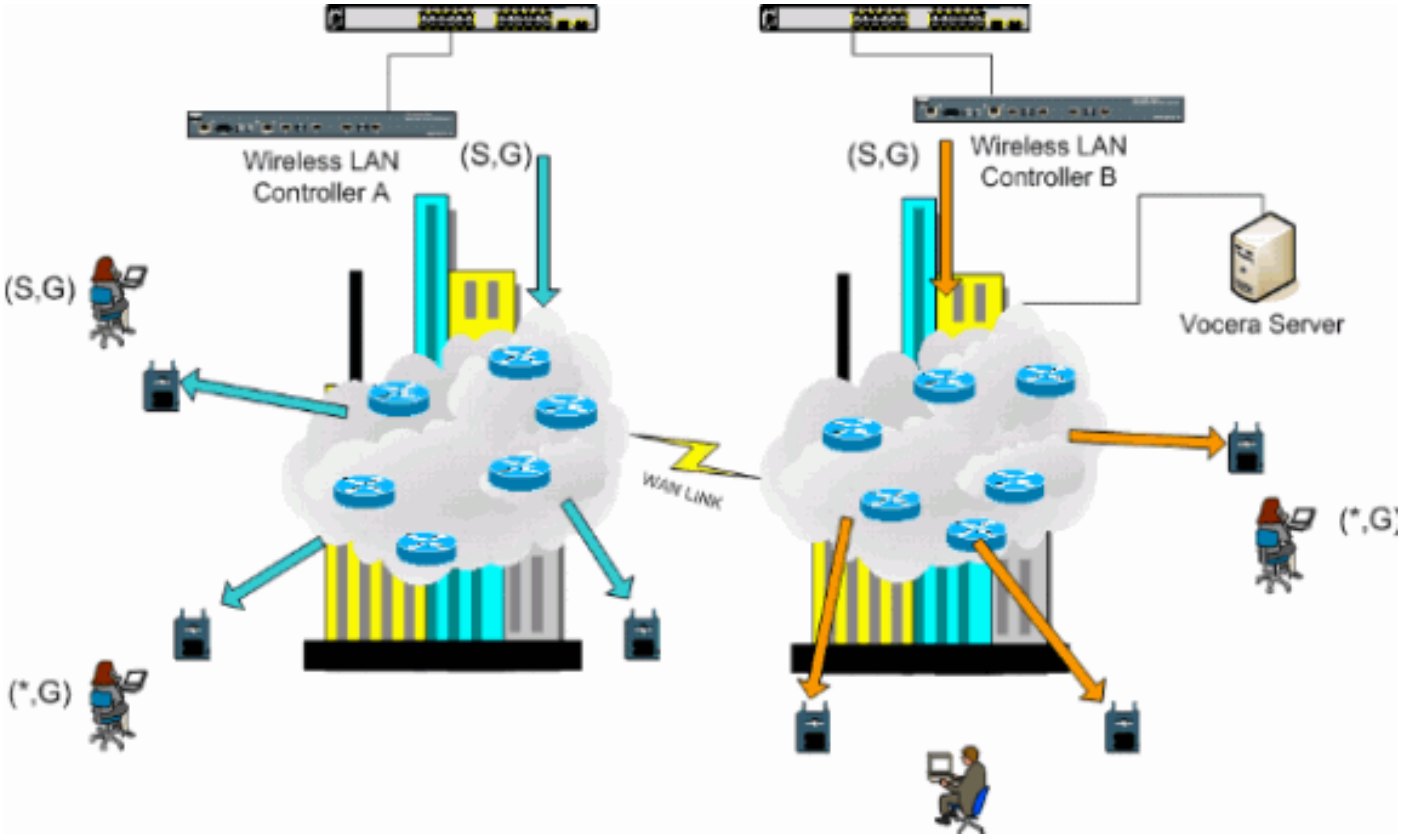
Abbildung 6: Bereitstellung mehrerer Controller-Layer 2



Layer-3-Bereitstellung mehrerer Controller

Die Layer-3-Roaming-Bereitstellungsstrategie sollte nur für das Roaming zwischen Controllern mit der WLC-Softwareversion 4.0.206.0 oder höher verwendet werden. Wenn ein Client, der mit der Vocera-Broadcast-Gruppe verbunden wurde und den entsprechenden Multicast-Stream empfängt und als Layer-3-Roaming mit konfiguriertem LWAPP-Layer-3-Roaming an einen anderen Controller rommt, wird dieser für interessierte Multicast-Gruppen abgefragt. Beim Sourcing an dieselbe Vocera-Broadcast-Gruppe werden diese Pakete über den EoIP-Tunnel an den Anker-Controller übermittelt und über normale Multicast-Routing-Methoden weitergeleitet.

Abbildung 7: Bereitstellung mehrerer Controller-Layer 3



VoWLAN-Bereitstellungen: Empfehlungen von Cisco

Drahtlose IP-Telefonnetzwerke erfordern eine sorgfältige Planung der Funkumgebung. Häufig ist eine gründliche Standortuntersuchung erforderlich, um die angemessene Wireless-Abdeckung zu ermitteln und Störungsquellen zu identifizieren. Die Positionierung von Access Points und die Antennenauswahl können mithilfe der Ergebnisse einer gültigen Umfrage für den Sprachstandort erheblich vereinfacht werden. Der wichtigste Aspekt ist die Übertragungsleistung des Wireless-Telefons. Im Idealfall bezieht das Telefon die Übertragungsleistung des Access Points und passt seine Übertragungsleistung an die des Access Points an.

Obwohl die meisten Wireless-Netzwerke heute nach einer umfassenden Standortuntersuchung bereitgestellt werden, sollten auch die Datenservices berücksichtigt werden. VoWLAN-Telefone haben wahrscheinlich andere Roaming-Eigenschaften und andere Abdeckungsanforderungen als ein typischer WLAN-Adapter für mobile Clients wie Laptops. Daher wird häufig eine zusätzliche Standortuntersuchung für Sprache empfohlen, um sich auf die Leistungsanforderungen mehrerer VoWLAN-Clients vorzubereiten. Diese zusätzliche Umfrage bietet die Möglichkeit, die Access Points so zu optimieren, dass sichergestellt ist, dass die VoWLAN-Telefone über genügend Funkabdeckung und Bandbreite verfügen, um eine angemessene Sprachqualität zu gewährleisten.

Weitere Informationen zu Überlegungen zum HF-Design finden Sie im Kapitel Überlegungen zum WLAN-Funkfrequenzdesign (RF) im Cisco Wireless LAN-Designleitfaden, der unter http://cisco.com/go/srnd verfügbar ist.

Empfehlungen für mehrstöckige Gebäude, Krankenhäuser und Lager

Betrachten Sie die in diesem Abschnitt aufgeführten Faktoren, wenn Sie Gebäude, Krankenhäuser und Lagerhäuser mit mehreren Stockwerken befragen.

Baumethoden und -materialien

Viele Aspekte des Gebäudebaus sind unbekannt oder von der Standortuntersuchung verborgen, sodass Sie diese Informationen aus anderen Quellen (z. B. Architekturzeichnungen) erfassen müssen. Einige Beispiele für typische Baumethoden und Materialien, die die Reichweite und den Abdeckungsbereich von Access Points beeinflussen, sind metallische Folien auf Fensterglas, bleites Glas, stahlverkleidete Wände, Zementböden und -wände mit Stahlverstärkung, foliengestützte Isolierung, Treppenschächte und Elevator-Wellen, Rohrleitungen und Vorrichtungen usw.

Bestand

Verschiedene Arten von Beständen können sich auf die HF-Reichweite auswirken, insbesondere solche mit hohem Stahl- oder Wassergehalt. Zu den Produkten, die Sie beachten müssen, gehören Kartons, Heimtierfutter, Farbe, Mineralölprodukte, Motorteile usw.

Lagerbestände

Stellen Sie sicher, dass Sie eine Standortuntersuchung bei maximalem Lagerbestand oder zu Zeiten mit höchster Aktivität durchführen. Ein Lagerhaus mit einem Lagerbestand von 50 % weist eine sehr unterschiedliche HF-Bilanz auf als dasselbe Lager mit einem Lagerbestand von 100 %.

Aktivitätsstufen

Auch außerhalb der Geschäftszeiten (ohne Mitarbeiter) ist die Funkumgebung anders als tagsüber voll besetzte Bereiche. Obwohl viele Teile der Standortuntersuchung ohne vollständige Belegung durchgeführt werden können, ist es wichtig, die Standortuntersuchung durchzuführen und die Schlüsselwerte in einer Zeit anzupassen, in der der Standort belegt ist. Je höher die Auslastungsanforderungen und die Benutzerdichte sind, desto wichtiger ist eine gut konzipierte Diversitätslösung. Wenn mehr Benutzer vorhanden sind, werden mehr Signale auf jedem Gerät des Benutzers empfangen. Zusätzliche Signale führen zu mehr Wettbewerb, mehr NULL-Punkte und mehr Multipath-Verzerrung. Die Vielfalt der Access Points (Antennen) trägt zur Minimierung dieser Bedingungen bei.

Mehrstöckige Gebäude

Beachten Sie diese Richtlinien, wenn Sie eine Standortuntersuchung für ein typisches Bürogebäude durchführen:

- Elevator-Wellen blockieren und reflektieren RF-Signale.
- Lieferräume mit Aufnahme von Signalen.
- Innenräume mit harten Wänden absorbieren HF-Signale.
- Break Rooms (Küchen) können durch die Verwendung von Mikrowellenherden Interferenzen im Bereich von 2,4 GHz verursachen.
- In Testlaboren können Interferenzen im 2,4-GHz- oder 5-GHz-Bereich auftreten, die zu Multipath-Verzerrungen und RF-Schatten führen.
- In der Regel absorbieren und blockieren sie Signale.
- Konferenzräume erfordern eine hohe Access Point-Abdeckung, da sie Bereiche mit hoher Auslastung sind.

Bei der Besichtigung von mehrstöckigen Einrichtungen müssen zusätzliche Vorsichtsmaßnahmen getroffen werden. Access Points auf verschiedenen Etagen können sich ebenso einfach gegenseitig stören wie Access Points auf derselben Etage. Sie können dieses Verhalten während einer Umfrage zu Ihrem Vorteil nutzen. Mit Antennen mit höherer Verstärkung können Fußböden und Decken durchbrochen und die Abdeckung der Böden über und unter dem Boden, auf dem der Access Point montiert ist, gewährleistet werden. Achten Sie darauf, dass sich die Kanäle zwischen Access Points auf verschiedenen Etagen oder Access Points auf derselben Etage nicht überschneiden. In Multi-Tenant-Gebäuden kann es zu Sicherheitsbedenken kommen, die die Verwendung einer geringeren Übertragungsleistung und Antennen mit geringerem Gewinn erfordern, um Signale von benachbarten Büros fernzuhalten.

Krankenhäuser

Der Befragungsprozess für ein Krankenhaus ist in etwa derselbe wie für ein Unternehmen, aber die Anordnung einer Krankenhauseinrichtung unterscheidet sich tendenziell in folgenden Punkten:

- Krankenhausgebäude durchlaufen in der Regel viele Umbauprojekte und Ergänzungen. Jede zusätzliche Konstruktion ist wahrscheinlich mit verschiedenen Baustoffen mit unterschiedlichen Dämpfungsstufen versehen.
- Die Signaldurchdringung durch Wände und Fußböden in den Patientenbereichen ist in der Regel minimal, was zur Bildung von Mikrozellen und Multipath-Variationen beiträgt.
- Der Bedarf an Bandbreite steigt mit der zunehmenden Verwendung von WLAN-Ultraschallgeräten und anderen tragbaren Bildverarbeitungsanwendungen. Der Bedarf an Bandbreite steigt auch durch zusätzliche Wireless-Sprachfunktionen.
- Die Zellen im Gesundheitswesen sind klein, und ein nahtloses Roaming ist besonders bei Sprachanwendungen unerlässlich.
- Die Zellüberschneidung kann hoch sein, ebenso wie die Wiederverwendung von Kanälen.
- Krankenhäuser können verschiedene Arten von Wireless-Netzwerken installieren. Dazu gehören Geräte mit 2,4 GHz, die nicht dem Standard 802.11 entsprechen. Dieses Gerät kann Konflikte mit anderen 2,4-GHz-Netzwerken verursachen.
- Patchantennen für die Wandmontage und Rundstrahlantennen für die Diversität an der Decke sind beliebt, aber beachten Sie, dass eine Vielfalt an Antennen erforderlich ist.

Warenlager

Die Lagerhäuser verfügen über große offene Bereiche, in denen häufig hohe Lagerbestände vorhanden sind. Häufig reichen diese Racks fast bis an die Decke, wo Access Points in der Regel platziert werden. Solche Storage-Racks können den Bereich, den der Access Point abdecken kann, einschränken. In diesen Fällen sollten Access Points an anderen Standorten außerhalb der Decke platziert werden, z. B. an Seitenwänden und Zementsäulen. Berücksichtigen Sie auch bei der Umfrage eines Lagers folgende Faktoren:

- Die Bestandsebenen beeinflussen die Anzahl der benötigten Access Points. Testabdeckung mit zwei oder drei Access Points an geschätzten Platzierungsorten.
- Unerwartete Zellüberschneidungen sind wahrscheinlich aufgrund von Multipath-Variationen. Die Qualität des Signals variiert mehr als die Stärke des Signals. Kunden können Access Points besser verbinden und betreiben, wenn sie weiter entfernt sind als Access Points in der Nähe.
- Während einer Umfrage verfügen Access Points und Antennen in der Regel nicht über ein

Antennenkabel, das sie miteinander verbindet. In einer Produktionsumgebung benötigen Access Point und Antenne jedoch möglicherweise Antennenkabel. Alle Antennenkabel führen zu Signalverlusten. Die genaueste Umfrage bezieht sich auf die Art der zu installierenden Antenne und die Länge des zu installierenden Kabels. Ein gutes Tool zur Simulation des Kabels und sein Verlust ist ein Dämpfer in einem Umfragekit.

Die Überwachung einer Produktionsstätte ähnelt der Überwachung eines Lagers, mit der Ausnahme, dass es in einer Fertigungsstätte möglicherweise noch viele weitere Störquellen für HF gibt. Darüber hinaus benötigen die Anwendungen in einer Fertigungsanlage in der Regel mehr Bandbreite als die in einem Lager. Diese Anwendungen können Videoaufnahmen und drahtlose Sprachübertragungen umfassen. Multipath-Verzerrung ist wahrscheinlich das größte Leistungsproblem in einer Fertigungsanlage.

Unterstützte Sicherheitsmechanismen

Neben statischem WEP und Cisco LEAP für Authentifizierung und Datenverschlüsselung unterstützen die Vocera-Badges auch WPA-PEAP (MS-CHAP v2)/WPA2-PSK.

LEAP-Überlegungen

LEAP ermöglicht die gegenseitige Authentifizierung von Geräten (Badge-to-Access Point und Access Point-to-Badge) anhand eines Benutzernamens und Kennworts. Bei der Authentifizierung wird zwischen dem Telefon und dem Access Point ein dynamischer Schlüssel zum Verschlüsseln des Datenverkehrs verwendet. Der ASLEAP-Wörterbuchangriff sollte jedoch in Betracht gezogen werden, wenn Sie LEAP als Sicherheitslösung einsetzen:

Weitere Informationen finden Sie unter Dictionary Attack on Cisco LEAP Vulnerability.

Bei Verwendung von LEAP ist ein LEAP-kompatibler RADIUS-Server wie der Cisco Access Control Server (ACS) erforderlich, um den Zugriff auf die Benutzerdatenbank zu ermöglichen. Der Cisco ACS kann die Datenbank für Benutzernamen und Kennwort entweder lokal speichern oder über ein externes Microsoft Windows NT-Verzeichnis auf diese Informationen zugreifen. Bei der Verwendung von LEAP ist sicherzustellen, dass auf allen Wireless-Geräten sichere Kennwörter verwendet werden. Starke Kennwörter sind als zwischen 10 und 12 Zeichen lang definiert und können sowohl Groß- als auch Kleinbuchstaben sowie Sonderzeichen enthalten.

Da alle Badges dasselbe Kennwort verwenden und im Badge gespeichert sind, empfiehlt Cisco, auf Daten-Clients und Wireless-Voice-Clients unterschiedliche Benutzernamen und Kennwörter zu verwenden. Diese Vorgehensweise unterstützt die Nachverfolgung und Fehlerbehebung sowie die Sicherheit. Obwohl es eine gültige Konfigurationsoption ist, eine externe (ACS-externe) Datenbank zum Speichern der Benutzernamen und Kennwörter für die Badges zu verwenden, empfiehlt Cisco diese Vorgehensweise nicht. Da der ACS immer dann abgefragt werden muss, wenn das Badge zwischen den Access Points wechselt, kann die unvorhersehbare Verzögerung beim Zugriff auf eine nicht ACS-basierte Datenbank zu übermäßiger Verzögerung und schlechter Sprachqualität führen.

Wireless-Netzwerkinfrastruktur

Das drahtlose IP-Telefonienetzwerk erfordert ebenso wie ein kabelgebundenes IP-Telefonienetzwerk eine sorgfältige Planung der VLAN-Konfiguration, der Netzwerkgröße, des Multicast-Verkehrs und der Geräteauswahl. Sowohl für kabelgebundene als auch Wireless-IP-

Telefonienetzwerke sind separate Sprach- und Daten-VLANs häufig die effektivste empfohlene Bereitstellung, um eine ausreichende Netzwerkbandbreite und eine einfache Fehlerbehebung sicherzustellen.

Sprach-, Daten- und Sprach-VLANs

VLANs bieten einen Mechanismus zur Segmentierung von Netzwerken in eine oder mehrere Broadcast-Domänen. VLANs sind besonders für IP-Telefonienetzwerke wichtig, in denen die typische Empfehlung besteht, den Sprach- und Datenverkehr in verschiedene Layer-2-Domänen zu unterteilen. Cisco empfiehlt, für die Vocera-Badges separate VLANs von anderem Sprach- und Datenverkehr zu konfigurieren: ein natives VLAN für den Verwaltungsverkehr der Access Points, ein Daten-VLAN für den Datenverkehr, ein Sprach- oder ein zusätzliches VLAN für den Sprachverkehr und ein VLAN für die Vocera-Badges. Ein separates Sprach-VLAN ermöglicht dem Netzwerk die Nutzung der Layer-2-Markierung und bietet Prioritätswarteschlangen am Access Switch-Port auf Layer 2. Dadurch wird sichergestellt, dass für verschiedene Datenverkehrsklassen angemessene QoS bereitgestellt wird und Probleme wie IP-Adressierung, Sicherheit und Netzwerkdimensionierung gelöst werden können. Die Vocera-Badges verwenden eine Broadcast-Funktion, die Multicast für die Bereitstellung verwendet. Dieses gemeinsame VLAN stellt sicher, dass ein Badge, das zwischen Controllern wechselt, Teil der Multicast-Gruppe bleibt. Dieser letzte Prozess wird ausführlich behandelt, wenn Multicast später in diesem Dokument behandelt wird.

Netzwerkgröße

Die Dimensionierung des IP-Telefonienetzwerks ist unerlässlich, um sicherzustellen, dass ausreichende Bandbreite und Ressourcen verfügbar sind, um die Anforderungen des Sprach-Datenverkehrs zu erfüllen. Zusätzlich zu den üblichen Richtlinien für das Design von IP-Telefonie-Geräten zur Bedarfsbestimmung von Komponenten wie PSTN-Gateway-Ports, Transcodern, WAN-Bandbreite usw. sollten Sie auch diese 802.11b-Probleme berücksichtigen, wenn Sie Ihr drahtloses IP-Telefonienetzwerk vergrößern. Die Vocera-Badges sind eine spezielle Anwendung, die die Anzahl der kabelgebundenen Clients über unsere typischen Implementierungsempfehlungen hinaus erhöht.

Anzahl der 802.11b-Geräte pro Access Point

Cisco empfiehlt, dass pro Access Point maximal 15 bis 25 802.11b-Geräte vorhanden sind.

Anzahl der aktiven Anrufe pro Access Point

Vocera verwendet zwei verschiedene Codecs, je nachdem, ob es sich um einen Abzeichen-to-Badge-Anruf (proprietärer Codec mit niedriger Bitrate) oder einen Badge-to-Phone-Anruf (G.711-Codec) handelt. Diese Tabelle zeigt einen Prozentsatz der verfügbaren Bandbreite nach Datenraten und gibt Ihnen ein klareres Bild des erwarteten Durchsatzes:

Anrufprozess	1 Mbit/s	2 Mbit/s	5,5 Mbit/s	11 Mbit/s
Badge-to-Phone (G.711)	20.7%	11.8%	6.3%	4.7%
Badge-to-Badge (proprietärer Codec mit niedriger Bitrate)	9.4%	6.1%	4.2%	3.6%

Switch-Empfehlungen

Hinweis: Wenn Sie einen Cisco Catalyst Switch der Serie 4000 als Hauptrouter im Netzwerk verwenden, stellen Sie sicher, dass er mindestens entweder ein Supervisor Engine 2+ (SUP2+)- oder ein Supervisor Engine 3 (SUP3)-Modul enthält. Das SUP1- oder SUP2-Modul kann Roaming-Verzögerungen verursachen, ebenso wie die Switches Cisco Catalyst 2948G, 2980G, 2980G-A, 4912 und 2948G-GE-TX.

Sie können eine Switch-Port-Vorlage erstellen, die zum Konfigurieren eines Switch-Ports für die Verbindung mit einem Access Point verwendet wird. Diese Vorlage sollte alle grundlegenden Sicherheits- und Ausfallsicherheitsfunktionen der Standard-Desktop-Vorlage hinzufügen. Wenn Sie den Access Point außerdem an einen Cisco Catalyst 3750-Switch anschließen, können Sie die Leistung des Access Points optimieren, indem Sie MLS-QoS-Befehle (Multilayer Switching) verwenden, um die Port-Rate zu begrenzen und die DSCP-Einstellungen (Class of Service) zuzuordnen.

Datenverkehr, der von WLAN-Clients nicht benötigt wird, sollte nicht an einen Access Point gesendet werden. Eine Vorlage sollte so konzipiert sein, dass eine sichere und ausfallsichere Netzwerkverbindung mit den folgenden Funktionen hergestellt werden kann:

- Return Port Configurations to default (Port-Standardkonfigurationen zurücksetzen): Diese Funktion verhindert Konfigurationskonflikte, indem alle vorhandenen Port-Konfigurationen gelöscht werden.
- Disable Dynamic Trunking Protocol (DTP) - Deaktiviert dynamisches Trunking, das für die Verbindung mit einem Access Point nicht erforderlich ist.
- Disable Port Aggregation Protocol (PagP) - PagP ist standardmäßig aktiviert, wird aber nicht für benutzerseitige Ports benötigt.
- Enable Port Fast - Ermöglicht einem Switch die schnelle Wiederaufnahme des Weiterleitungsdatenverkehrs, wenn eine Spanning Tree-Verbindung ausfällt.
- Konfigurieren eines Wireless-VLAN - Erstellt ein eindeutiges WLAN, das den WLAN-Datenverkehr von anderen Daten-, Sprach- und Management-VLANs isoliert. Dadurch wird der Datenverkehr isoliert, und der Datenverkehr wird besser kontrolliert.
- Quality of Service (QoS) aktivieren; "not trust port" (Port nicht vertrauen) (Markierung auf 0) - Gewährleistet die angemessene Behandlung von Datenverkehr mit hoher Priorität, einschließlich Softphones, und verhindert, dass Benutzer übermäßige Bandbreite durch eine Neukonfiguration ihrer PCs verbrauchen.

Mit den Inline-Power-Switches WS-C3750-48PS-S können Access Points mit Strom versorgt werden, die Inline-Stromversorgung empfangen können.

Der Catalyst 6500 ermöglicht die Weiterleitung von Paketen mit Leitungsgeschwindigkeit und allen hier beschriebenen Funktionen sowie die Integration zahlreicher Servicemodule. Mit dem Wireless Service Module (WiSM) können Sie über zwei Controller verfügen, die jeweils 150 Access Points steuern können. Mit bis zu fünf WiSMs pro Chassis können Sie so mehr als 1.500 Access Points steuern, die 50.000 Clients in einer leistungsstarken Switching-Architektur unterstützen.

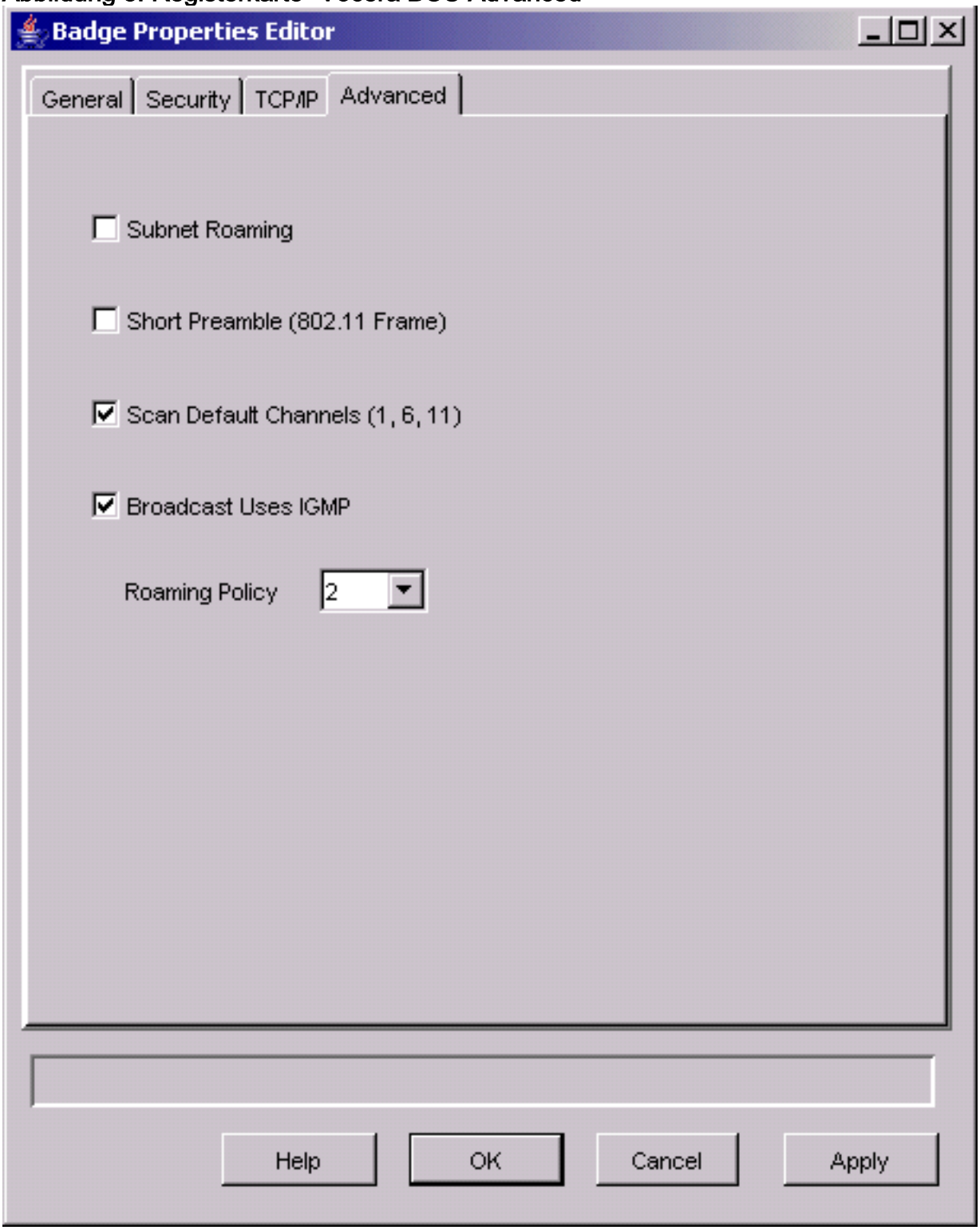
Bereitstellung und Konfiguration

Badge-Konfiguration

Das Vocera Badge Configuration Utility (BCU) und die Konfiguration des Badge können Roaming und Latenz in Ihrer Umgebung einführen, wenn dies falsch gemacht wird. Überprüfen Sie diese Einstellungen mit der BCU und dem Badge Properties Editor (BPE) (siehe Abbildung 8):

- **Subnetz-Roaming** ist deaktiviert.
- **Standard-Kanäle scannen (1,6,11)** ist aktiviert.
- **Broadcast verwendet IGMP** ist aktiviert.
- Die Roaming-Richtlinie ist auf **2** oder höher festgelegt.

Abbildung 8: Registerkarte "Vocera BCU Advanced"



Wenn **Subnetz-Roaming** aktiviert ist, wird das Badge angewiesen, nach jedem Roaming eine neue IP-Adresse anzufordern. In der LWAPP-Umgebung unterstützt die Infrastruktur die

Aufrechterhaltung der Client-Konnektivität auf Layer 3. Wenn ein Sprach-Client auf eine Antwort des DHCP-Servers warten muss, bevor er Pakete senden oder empfangen kann, werden Verzögerungen und Jitter eingeführt. Wenn **Standard-Scankanäle (1,6,11)** nicht aktiviert sind, prüft das Badge alle 802.11b-Kanäle, wenn das Badge nach Roaming sucht. Dies verhindert die Weiterleitung von Paketen und ein nahtloses Roaming.

Optimierung der AutoRF-Umgebung

Wie im Abschnitt Empfehlungen dieses Dokuments beschrieben, ist es wichtig, dass jeder Standort über eigene RF-Eigenschaften verfügt. Möglicherweise müssen AutoRF oder Radio Resource Management (RRM) angepasst werden, wobei jeder Standort unterschiedlich ist und AutoRF/RRM für Ihre Umgebung angepasst werden muss.

Bevor Sie die AutoRF-Funktion anpassen, erhalten Sie weitere Informationen unter Unified Wireless Networks (Unified Wireless-Netzwerke) im Abschnitt Radio Resource Management (Funkressourcenmanagement).

Mit RRM können Sie die Übertragungsleistung der einzelnen Access Points anpassen, indem Sie festlegen, wie stark jeder Access Point den drittstärksten Nachbarn hört. Dieser Wert kann nur über die CLI mit dem Befehl **config advanced 802.11b tx-power-thresh** angepasst werden, wie unter Tx Power Level Assignment Settings beschrieben.

Bevor Sie die AutoRF-Funktion anpassen, sollten Sie die Bereitstellungsstelle mithilfe des Vocera-Badge (vom Endbenutzer getragen) durchgehen und ein Tool für die Standortuntersuchung verwenden, um sich ein genaues Bild davon zu machen, wie das Badge funktioniert und wie die einzelnen Access Points mit Strom versorgt werden. Sobald dieser Vorgang abgeschlossen ist und festgestellt wird, dass eine Anpassung dieses Werts erforderlich ist, beginnen Sie mit einem Wert von -71 dBm für den Transmit Power Control-Algorithmus. Verwenden Sie diesen CLI-Parameter:

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

Lassen Sie das Netzwerk diese Anpassung mit mindestens 30 Minuten bis einer Stunde durchlaufen, bevor Sie Änderungen feststellen. Sobald dem Netzwerk eine ausreichende Zeitspanne zur Verfügung steht, können Sie die Website mit demselben Umfragetool und Badges erneut durchlaufen. Beobachten Sie dieselben Roaming-Eigenschaften und die Leistung des Access Points. Ziel ist es hier, vor oder am nächsten Access Point das Roaming der Badges zu ermöglichen, um das bestmögliche Signal-Rausch-Verhältnis zu erzielen.

- **Woher weiß ich, ob die Übertragungsleistung zu heiß oder zu kalt ist?**Um festzustellen, ob der Grenzwert für die Übertragungsleistung zu hoch oder zu niedrig ist, müssen Sie Ihre Umgebung gut verstehen. Wenn Sie Ihre gesamte Bereitstellungsfläche durchlaufen haben (wo Sie erwarten, dass Ihre Vocera-Ausweise funktionieren), sollten Sie wissen, wo sich Ihre Access Points befinden und das Roaming-Verhalten des Badge erleben.
- **Was mache ich, wenn meine Übertragungsleistung zu heiß ist?**Das Vocera-Badge rommt nur auf der Grundlage der Signalstärke und nicht der Signalqualität. Wenn die Vocera-Plakette nicht rommt, nachdem sie mehrere Access Points passiert hat, während sie im Begrüßungs- oder Testton aktiviert ist, gilt das Badge als klebrig. Wenn dieses Verhalten auf den gesamten Campus-Bereitstellungsbereich hinweist, ist Ihre Sendeleistung zu heiß und sollte gesichert werden. Wenn nur ein oder zwei isolierte Bereiche dieses Verhalten zeigen und der Rest der Bereitstellungszone idealistischere Roaming-Eigenschaften aufweist, ist dies kein Hinweis

darauf, dass Ihr Netzwerk zu heiß ist.

- **Was mache ich, wenn meine Übertragungsleistung zu kalt ist?**Der Standard-Übertragungsschwellenwert sollte Ihnen fast nie einen Bereitstellungsbereich bereitstellen, in dem Ihr Netzwerk zu kalt läuft. Wenn der Grenzwert für die Übertragungsleistung nach unten angepasst wird und Sie durch das Durchlaufen der Hallen mit dem Vocera-Badge eine Umgebung erhalten, in der das Badge gut rommt, aber die Verbindung verliert und/oder die Abdeckung durch einen Toten/Spotty fällt, dann ist Ihr Netzwerk möglicherweise zu niedrig eingestellt. Wenn dies nicht für Ihr gesamtes Netzwerk charakteristisch ist, sondern auf ein oder zwei Bereiche isoliert ist, ist dies eher ein Hinweis auf eine Abdeckungslücke als auf ein netzwerkweites Problem.
- **Isoliertes Verhalten**Wenn Sie feststellen, dass das Badge in einem oder zwei Bereichen an einem Access Point befestigt ist, anstatt auf idealistische Weise zu Roaming zu wechseln, überprüfen Sie diesen Bereich.Inwiefern unterscheidet sich dieser Bereich vom Rest des Campus?Wenn sich diese/diese Bereiche in der Nähe von Gebäudeausgängen oder in Gebieten befinden, die sich im Bau befinden, könnte die Erkennung von Abdeckungslücken diese Access Points zwingen, die Leistung zu erhöhen?Sehen Sie sich die WLC-Protokolldatei und die Nachbarlisten der Access Points an, um zu ermitteln, warum eine solche Anomalie auftreten kann.Wenn Sie feststellen, dass das Badge in einem oder mehreren isolierten Bereichen tote oder undichte Stellen aufweist, müssen Sie diese Bereiche separat untersuchen.Ist dieser Bereich in der Nähe einer Elevator-Welle, Radiologie oder eines Pausenraums?Diese Bereiche sind möglicherweise besser geeignet, wenn ein Access Point installiert oder besser platziert wird, um eine bessere Sprachabdeckung zu ermöglichen.In beiden Fällen ist es immer ratsam, zu verstehen, dass Sie in einem nicht lizenzierten Frequenzspektrum arbeiten und idealistisches Verhalten möglicherweise niemals zu erreichen ist. Dies kann passieren, wenn Sie sich neben einem Funkübertragungsturm oder -gerät, einem Fernsehsender oder möglicherweise einer Nicht-802.11-2,4-GHz-Reparatureinrichtung (Wireless-Telefone usw.) befinden.

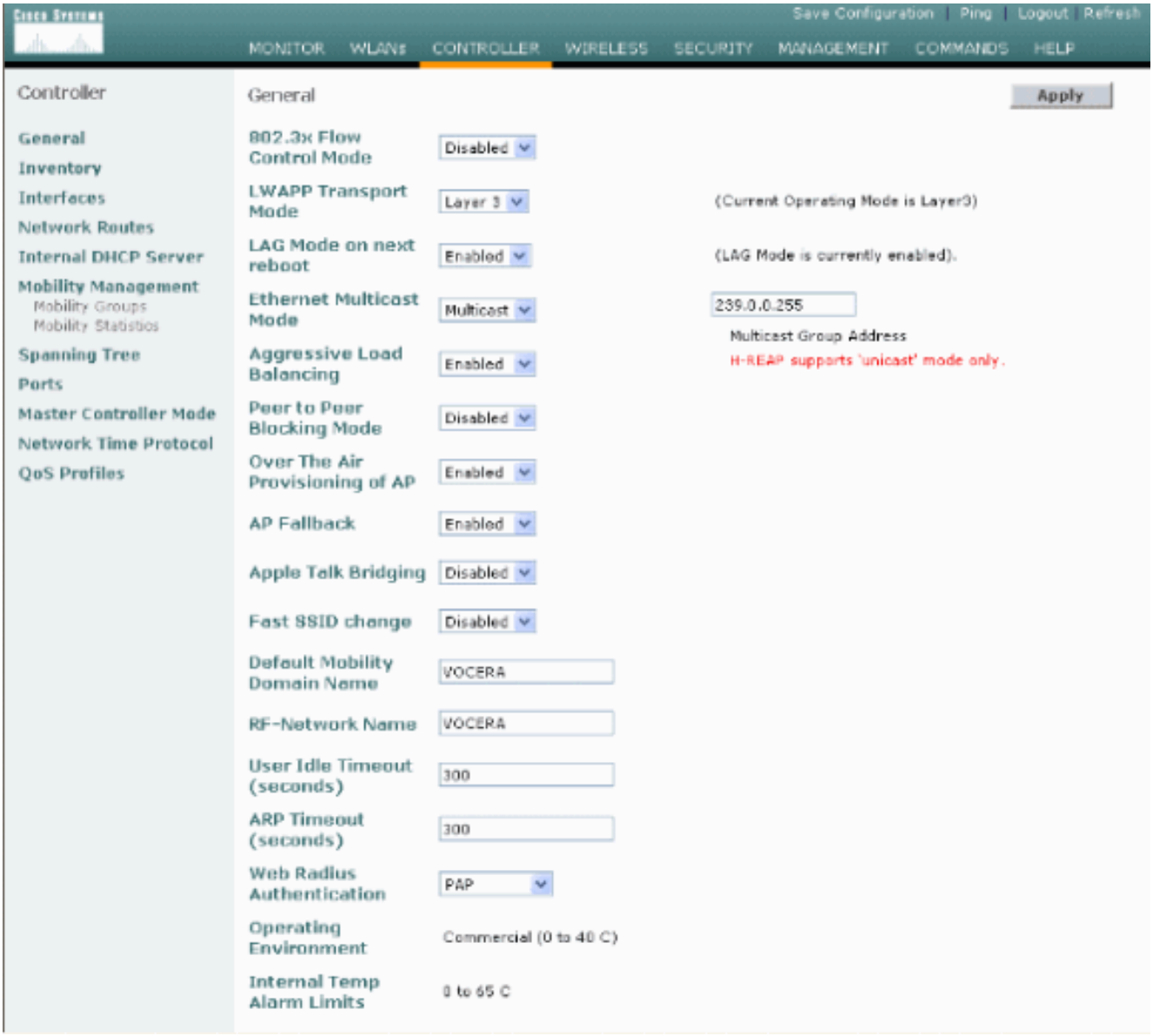
Konfiguration der Wireless-Netzwerkinfrastruktur

Der Cisco Unified Wireless Network-Design- und Bereitstellungsleitfaden sollte für die Gesamtkonfiguration Ihrer WLCs befolgt werden. Dieser Abschnitt enthält zusätzliche Empfehlungen speziell für Vocera® Communication Badges.

Hinweis: Die Änderungen werden nicht gespeichert, wenn Sie die Schaltfläche **Übernehmen** nicht drücken, bevor Sie mit dem nächsten Schritt fortfahren.

Führen Sie die folgenden Schritte im Menü "**Controller**" aus:

1. Ändern Sie den Ethernet-Multicast-Modus in **Multicast**.
2. Legen Sie für die Multicast-Gruppenadresse **239.0.0.255** (oder eine andere nicht verwendete Multicast-Gruppenadresse) fest.
3. Legen Sie den Standardnamen der Mobility-Domäne und den RF-Netzwerk-Namen auf Ihr Netzwerkdesign fest.
4. Deaktivieren Sie **Aggressive Load Balancing**.**Abbildung 9: Allgemeine WLC-Konfiguration**

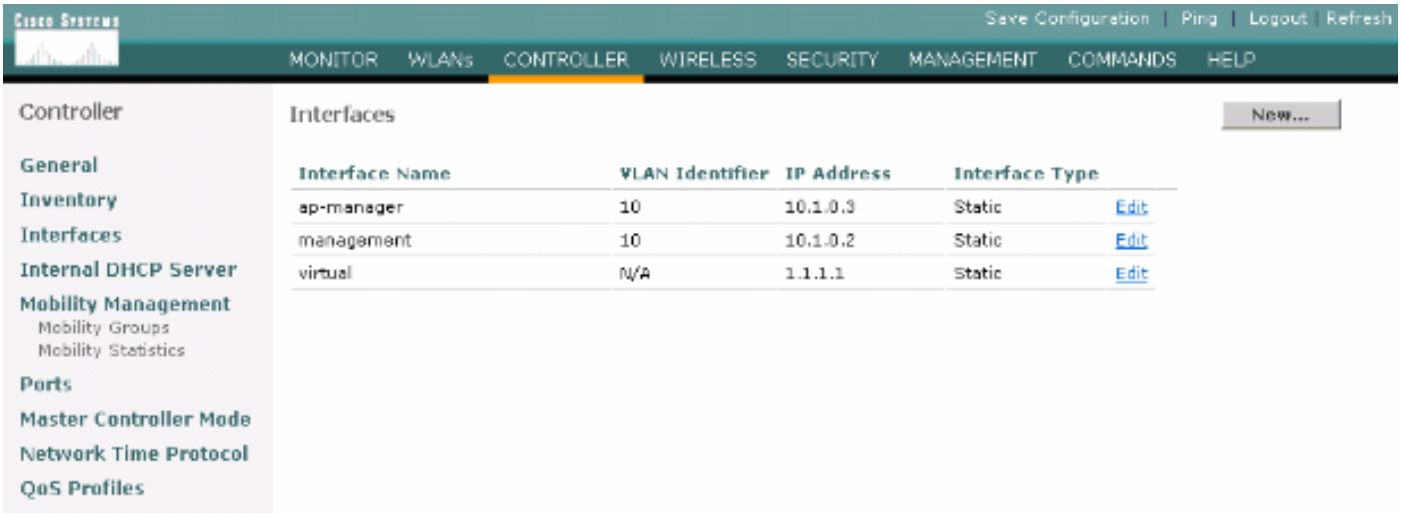


Schnittstellen erstellen

Klicken Sie auf **Controller > Schnittstellen**.

Hinweis: Ihr VLAN und Ihre IP-Adresse variieren. Die Screenshots hier bieten eine Beispieladressierung, die nicht direkt befolgt werden sollte.

Abbildung 10: Liste der WLC-Schnittstellen



Erstellen der Vocera-Sprachschnittstelle

Führen Sie diese Schritte aus:

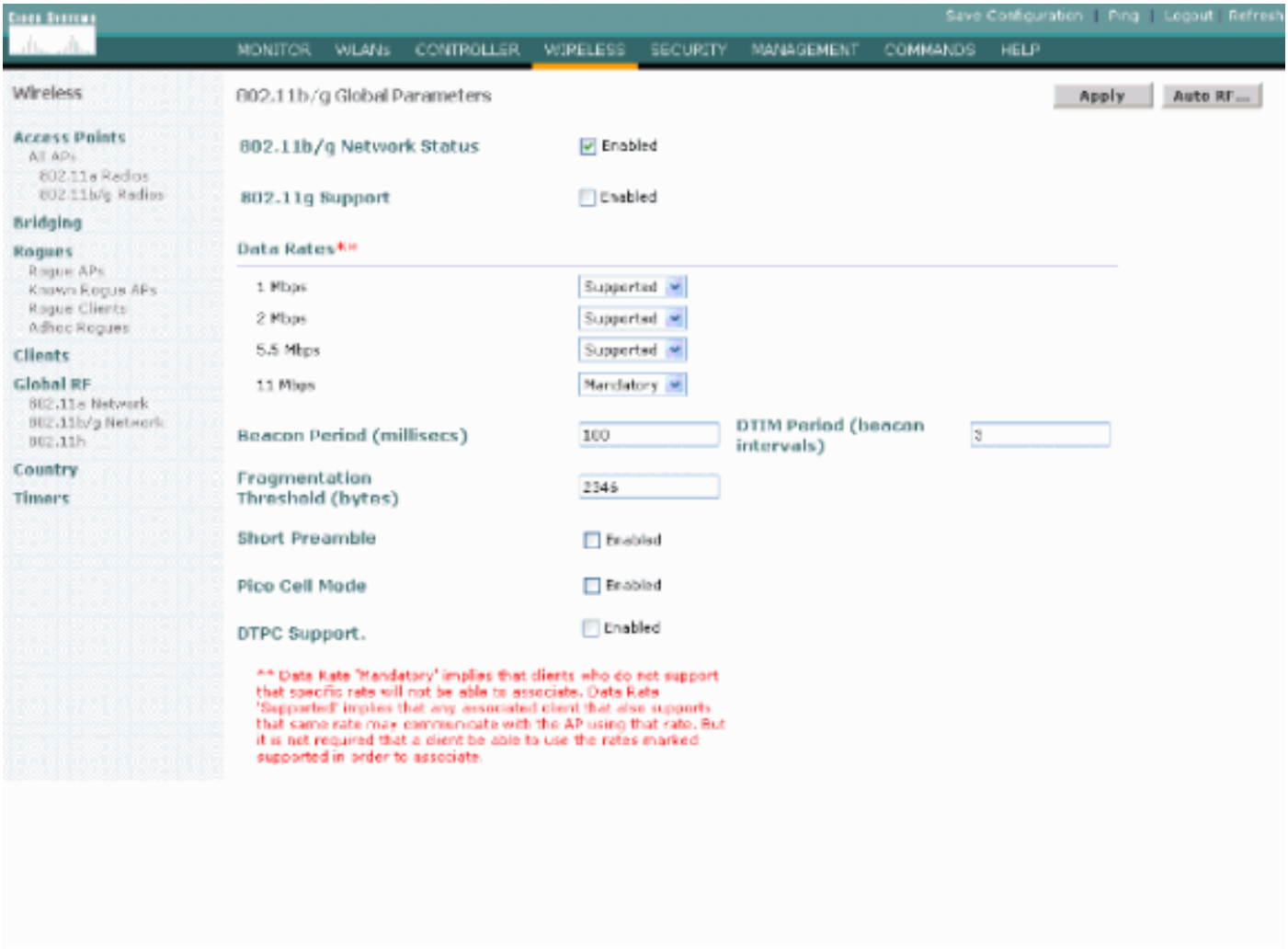
1. Klicken Sie auf **Neu**.
2. Geben Sie im Feld "Interface Name" (Schnittstellenname) einen Tagnamen ein, der das VoWLAN-Netzwerk Ihres Vocera darstellt.
3. Geben Sie die VLAN-Nummer dieses VoWLAN-Netzwerks im Feld VLAN ID (VLAN-ID) ein.
4. Klicken Sie auf **Übernehmen** und dann auf **Bearbeiten**, um die soeben erstellte Benutzeroberfläche zu bearbeiten.
5. Geben Sie die IP-Adressierung für diese Schnittstelle ein, die sich im Bereich des VLAN und anderer verwandter Informationen befindet.
6. Klicken Sie auf **Apply** (Anwenden).

Wireless-spezifische Konfiguration

Für ein WLAN, das nur Vocera-Abzeichen enthält, enthält diese Konfiguration Beispieleinstellungen, die die Vocera-Broadcast-Anwendung am besten unterstützen.

- Der DTIM-Zeitraum ist **1**.
- Die Unterstützung für 802.11g ist deaktiviert. Nur die 802.11b-Datenrate von **11 Mbit/s** ist **obligatorisch**.
- Die kurze Präambel ist deaktiviert.
- DTPC ist deaktiviert.

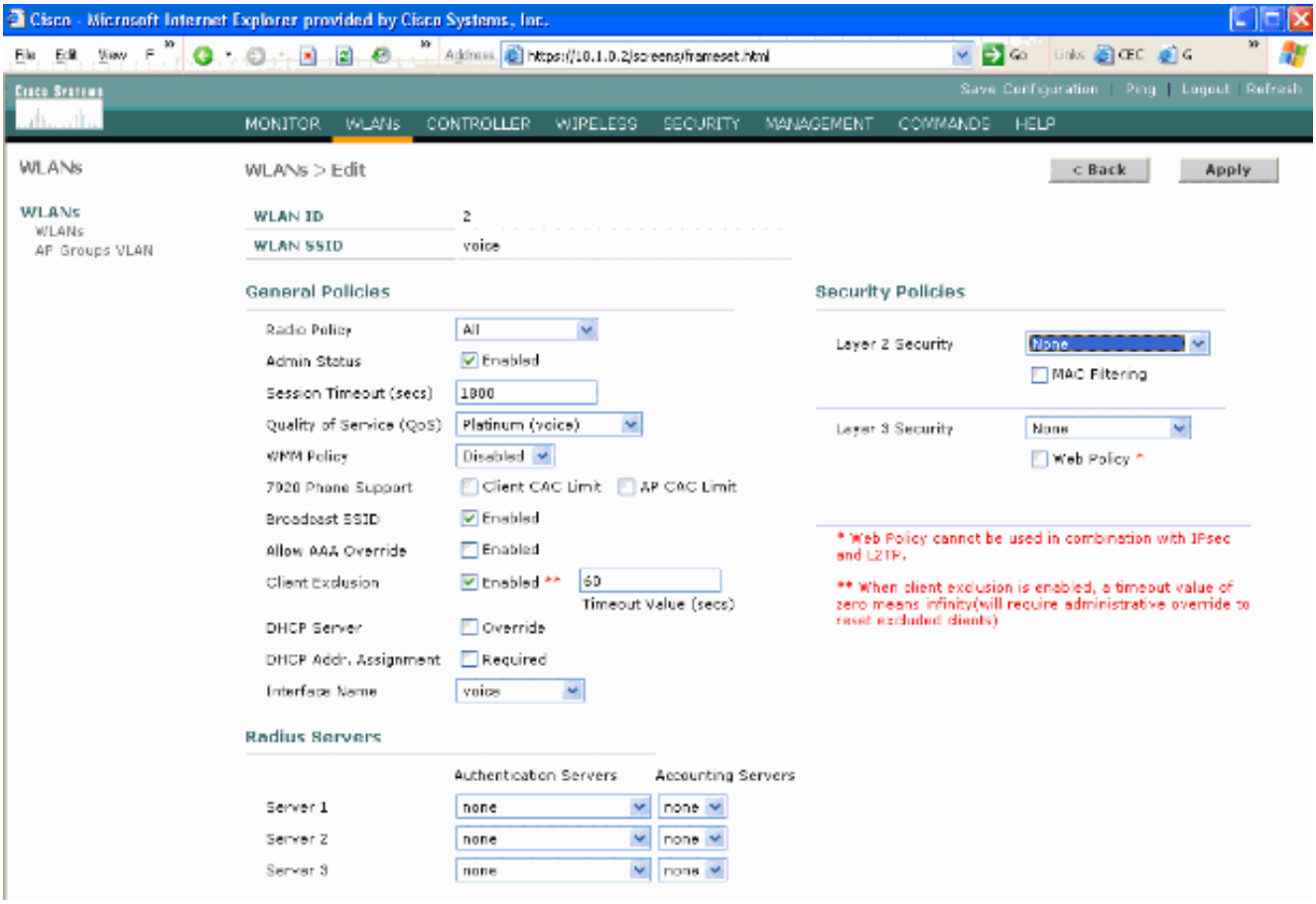
Abbildung 11: Konfiguration von 802.11b/g



WLAN-Konfiguration

Führen Sie diese Schritte aus:

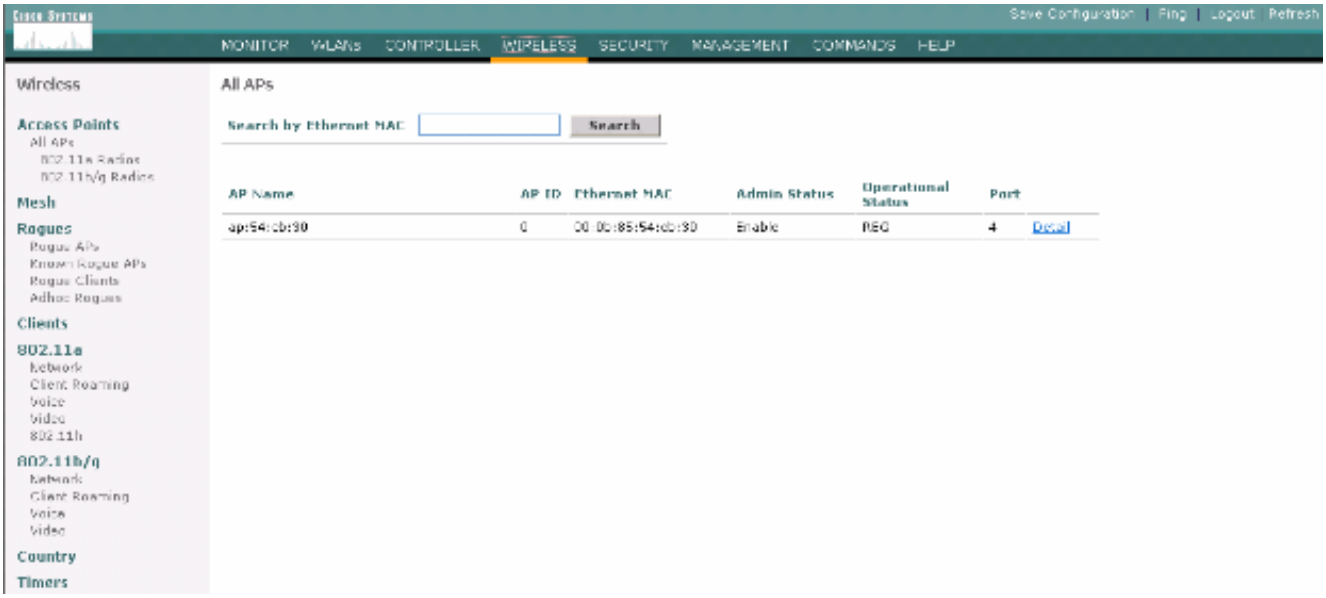
1. Aktualisieren Sie das Feld "Radio Policy" (Funkrichtlinie) auf einen Wert, der Ihren Anforderungen am besten entspricht.
2. Ändern Sie den Admin-Status in **Aktiviert**.
3. Sitzungs-Timeout auf **1800** festgelegt.
4. Legen Sie Quality of Service auf **Platinum fest**.
5. SSID für Broadcast auf **Aktiviert** eingestellt.
6. Legen Sie den Schnittstellennamen auf die Schnittstelle fest, die für die Sprachkommunikationszeichen erstellt wurde.
7. Legen Sie die Sicherheitsoptionen entsprechend Ihrer Unternehmensrichtlinien fest.**Abbildung 12: WLAN-Konfiguration**



Konfiguration der Access Point-Details

Führen Sie diese Schritte aus:

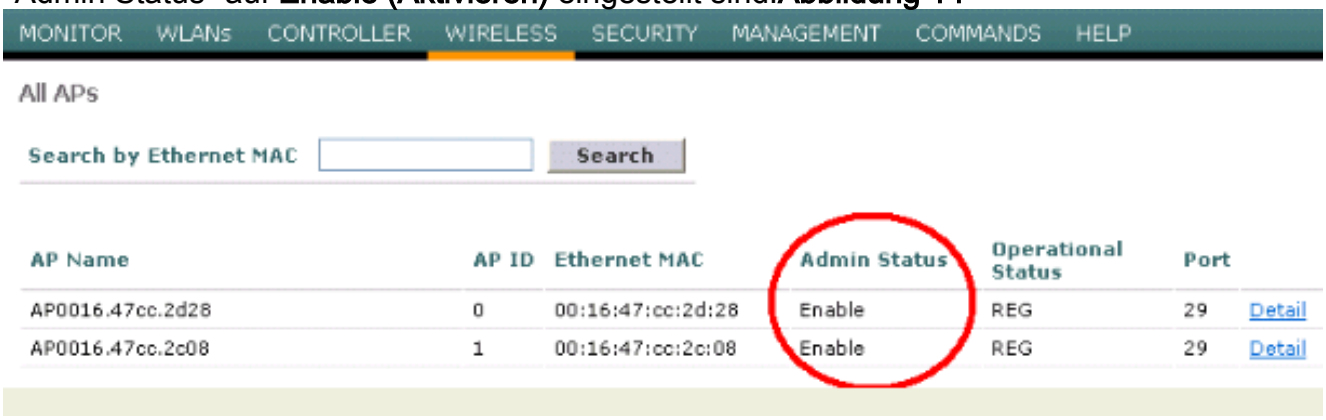
1. Klicken Sie auf **Details**.
2. Konfigurieren Sie den AP-Namen.
3. Stellen Sie sicher, dass der Access Point für DHCP konfiguriert ist.
4. Stellen Sie sicher, dass Admin Status **aktiviert** ist.
5. AP Mod" sollte auf **lokal** eingestellt sein.
6. Geben Sie die Position des Access Points ein.
7. Geben Sie den Controller-Namen ein, zu dem der Access Point gehört. Der Controller-Name befindet sich auf der Seite Monitor (Monitor).
8. Klicken Sie auf **Apply** (Anwenden).**Abbildung 13: AP-Details**



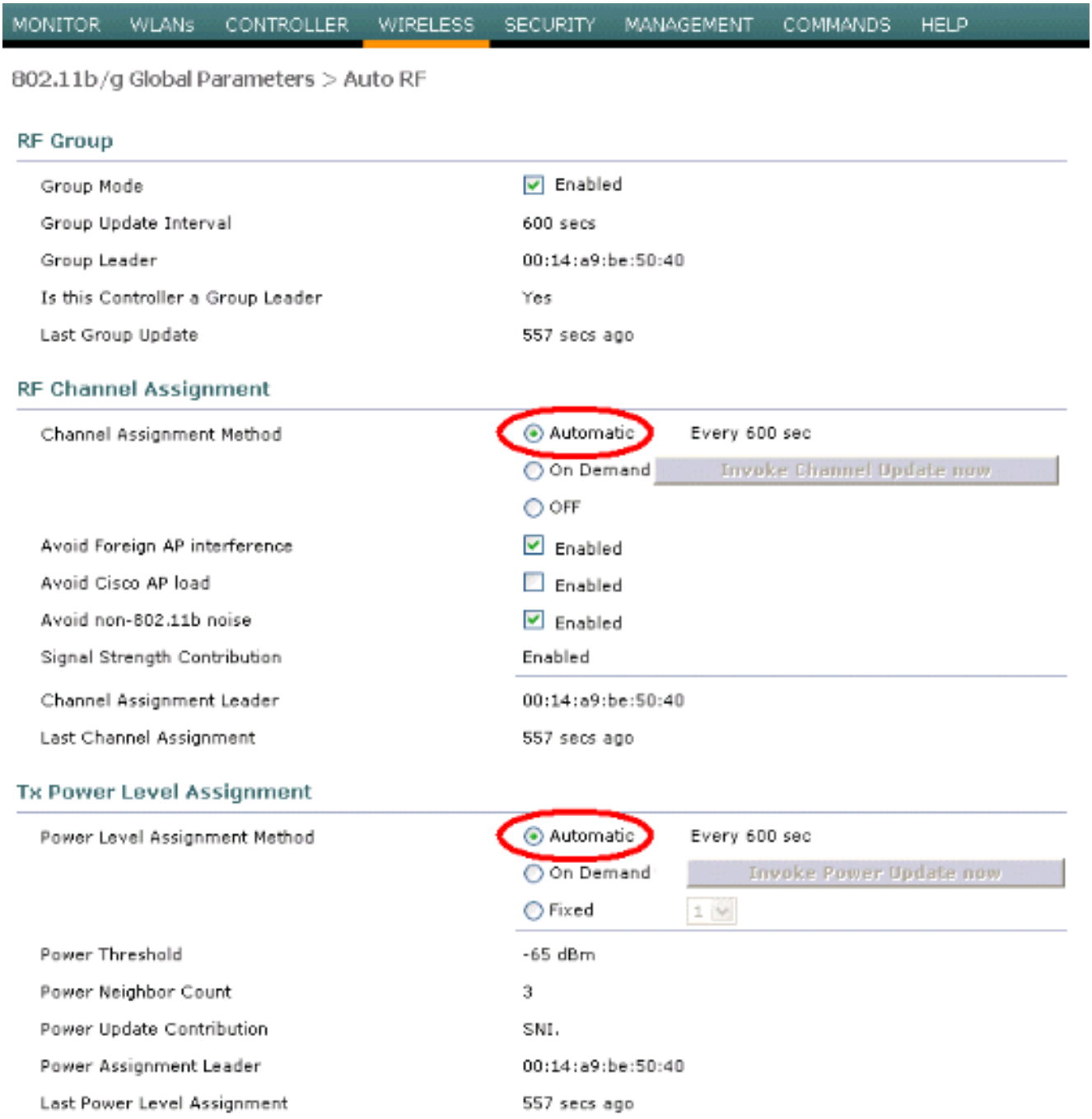
Konfigurieren der 802.11b/g-Funkeinheit

Führen Sie diese Schritte aus:

1. Klicken Sie oben im WLC auf **Wireless**, und überprüfen Sie, ob alle Access Points unter "Admin Status" auf **Enable (Aktivieren)** eingestellt sind.**Abbildung 14**



2. Klicken Sie auf **Netzwerk** (in der Nähe von 802.11b/g).
3. Klicken Sie auf **AutoRF**.
4. Verwenden Sie AutoRF, um eine vollständige Abdeckung mit nicht überlappenden Funkkanälen und Übertragungsleistung zu erstellen. Wählen Sie dazu **Automatisch** für die RF-Kanalzuweisung und die Tx-Leistungsstufen-Zuweisung aus.**Abbildung 15**



5. Klicken Sie auf **Apply** (Anwenden).
6. Klicken Sie auf **Save Configuration** und sehen Sie sich den Abschnitt Tune AutoRF for Your Environment an.
7. Wählen Sie **Wireless > Access Points > 802.11b/g Radios aus.Abbildung 16**

Wireless IP-Telefonieüberprüfung

Nach der Durchführung einer Standortprüfung und der Konfiguration der Access Points und Telefone ist es entscheidend, dass Sie Verifizierungstests durchführen, um sicherzustellen, dass alle Funktionen wie gewünscht funktionieren. Diese Tests sollten an allen folgenden Stellen durchgeführt werden:

- Der primäre Bereich jeder Access Point-Zelle (in dem die Badges mit hoher Wahrscheinlichkeit mit dem jeweiligen Access Point verbunden werden).
- Jeder Standort, an dem ein hohes Anrufvolumen möglich ist.
- Standorte, an denen die Nutzung selten ist, die Abdeckung jedoch noch zertifiziert sein muss (z. B. Treppen, Toiletten usw.).
- Am Rande des Abdeckungsbereichs des Access Points.
- ·Diese Tests können parallel oder seriell durchgeführt werden. Bei paralleler Ausführung müssen Sie sicherstellen, dass die Telefone zwischen den Testpunkten ausgeschaltet sind, um die vollständige Zuordnung, Authentifizierung und Registrierung an jedem Standort zu testen. Roaming- und Auslastungstests müssen die abschließenden Tests sein.

Zuordnung, Authentifizierung und Registrierung

In diesem Abschnitt wird erläutert, wie Sie überprüfen, ob das Badge richtig zugeordnet, authentifiziert und registriert wird.

- Schalten Sie an mehreren Stellen in der Umgebung die Badges ein, und überprüfen Sie die Zuordnung zum Access Point. Wenn das Badge nicht mit dem Access Point verknüpft ist, führen Sie die folgenden Prüfungen durch:Überprüfen Sie die Badge-Konfiguration, um die richtige SSID, den Authentifizierungstyp usw. sicherzustellen.Überprüfen Sie die WLC-Konfiguration, um sicherzustellen, dass die richtige SSID, der richtige Authentifizierungstyp, Funkkanäle usw. verwendet werden.Prüfen Sie Ihre Standortuntersuchung, um sicherzustellen, dass der Standort ausreichend HF-Abdeckung aufweist.
- Stellen Sie an mehreren Stellen in der Umgebung sicher, dass sich das Telefon erfolgreich über den Access Point authentifiziert. Wenn der Client sich nicht authentifiziert, überprüfen Sie entweder den WEP-Schlüssel oder den LEAP-Benutzernamen und das Kennwort auf den Badges. Überprüfen Sie außerdem den Benutzernamen und das Kennwort auf dem AAA-Server, indem Sie einen Wireless-Laptop mit identischen Anmeldeinformationen verwenden.
- Stellen Sie an mehreren Stellen in der Umgebung sicher, dass sich die Badges beim Vocera Communication Server registrieren. Wenn sich der Client nicht registriert, führen Sie folgende Prüfungen durch:Überprüfen Sie, ob das Badge über die richtige IP-Adresse, Subnetzmaske, das primäre Gateway, das primäre TFTP, das primäre/sekundäre Netzwerk und DNS verfügt.
- Stationäre Sprachanrufe:Rufen Sie an mehreren Stellen in der Umgebung während der Pause ein anderes Badge an, und führen Sie 60 bis 120 Sekunden Sprachtests durch, um die Sprachqualität zu überprüfen. Wenn die Sprachqualität nicht akzeptabel ist, verschieben Sie ein Abzeichen an einen besseren Ort, und testen Sie es erneut. Ist die Sprachqualität akzeptabel? Wenn nicht, überprüfen Sie Ihre Wireless-Abdeckung.Wenn der Telefonieserver konfiguriert ist, stehen Sie an mehreren Stellen in der Umgebung still, rufen Sie ein kabelgebundenes Telefon an, und führen Sie 60 bis 120 Sekunden Sprachtests durch, um die Sprachqualität zu überprüfen. Wenn die Sprachqualität nicht akzeptabel ist, fragen Sie, ob Sie

einen Anruf über das kabelgebundene Telefon tätigen. Ist die Sprachqualität akzeptabel? Andernfalls sollten Sie das kabelgebundene Netzwerkdesign anhand der Richtlinien überprüfen.

- Verwenden Sie die Standortprüfungstools, um sicherzustellen, dass von diesem Standort aus nicht mehr als ein Access Point pro Funkkanal mit einer Signalstärke (RSSI = Received Signal Stärke Indicator) größer als 35 vorhanden ist. Wenn zwei Access Points im selben Kanal vorhanden sind, stellen Sie sicher, dass das Signal-Rausch-Verhältnis (SNR) so hoch wie möglich ist, um Interferenzen zu minimieren. Wenn der sicherere Access Point beispielsweise über einen RSSI von 35 verfügt, sollte der schwächere Access Point im Idealfall einen RSSI von weniger als 20 aufweisen. Um dieses Ziel zu erreichen, müssen Sie möglicherweise die Übertragungsleistung eines Access Points reduzieren oder den Access Point verschieben.
- Überprüfen Sie die QoS-Einstellungen am Access Point, um die korrekten empfohlenen Einstellungen zu bestätigen.
- Roaming-Badge-Anrufe:Wenn der Telefonieserver nicht verfügbar ist, starten Sie das Vocera Tutorial mit dem Befehl **Tutorial beginnen**.ODERWenn der Telefonieserver verfügbar ist, starten Sie einen Anruf mit einem stationären Gerät zum Badge.Überprüfen Sie die Sprachqualität kontinuierlich, während Sie die gesamte Wireless-Abdeckung durchlaufen. Wenn die Sprachqualität unzureichend ist, führen Sie folgende Schritte aus:Achten Sie auf alle inakzeptablen Änderungen der Sprachqualität, und notieren Sie die Orts- und Funkwerte auf Ihrem Laptop und die CQ-Werte des Badge.Achten Sie auf das Badge, um zum nächsten Access Point zu wechseln.Beachten Sie die anderen verfügbaren Access Points in der Standortuntersuchung, um die Abdeckung und Interferenzen zu überprüfen.
- Passen Sie die Platzierung von Access Points und die Einstellungen an, um das WLAN zu optimieren, und führen Sie diese Prüfungen durch, um die Sprachqualität sicherzustellen:Verwenden Sie die Standortprüfungstools, und stellen Sie sicher, dass pro Kanal nicht mehr als ein Access Point vorhanden ist, dessen RSSI-Wert 35 pro Standort übersteigt. Im Idealfall sollten alle anderen Access Points auf demselben Kanal möglichst niedrige RSSI-Werte aufweisen (vorzugsweise weniger als 20). An der Grenze des Abdeckungsbereichs, in dem der RSSI 35 ist, sollte der RSSI für alle anderen Access Points auf demselben Kanal idealerweise weniger als 20 betragen.Verwenden Sie die Standortprüfungstools, um sicherzustellen, dass an allen Standorten mindestens zwei Access Points (insgesamt, auf separaten Kanälen) mit ausreichender Signalstärke sichtbar sind.Überprüfen Sie, ob sich die Access Points in einem bestimmten Roaming-Bereich in einem Layer-2-Netzwerk befinden.

Häufige Roaming-Probleme

Diese Roaming-Probleme können auftreten:

- Das Badge rommt nicht, wenn es direkt unter dem Access Point platziert wird.
- Das Badge erreicht höchstwahrscheinlich nicht die Roaming-Differenzialschwellen für den empfangenen Signalstärkeindikator (RSSI) und die Channel-Auslastung (CU). Passen Sie den Grenzwert für die Übertragungsleistung vom WLC an.
- Das Badge empfängt keine Beacons oder Sonde-Antworten vom Access Point.
- Das Badge rommt zu langsam.

Das Badge verliert die Verbindung zum Netzwerk oder Sprachdienst beim Roaming.

- Überprüfen Sie die Authentifizierung auf mögliche WEP-Diskrepanzen.
- Das Badge sendet keine IGMP-Joins, oder das Netzwerk sendet während eines Roamings IGMP-Abfragen. Daher schlägt die Vocera-Broadcast-Funktion während eines Layer-2-/Layer-3-Roams fehl.
- Das Badge ist nur für nahtloses Layer-2-Roaming geeignet (es sei denn, ein Layer-3-Mobilitätsmechanismus ist konfiguriert). Stellen Sie sicher, dass der neue WLC kein anderes IP-Subnetz bedient.
- Überprüfen Sie, ob der zugeordnete Access Point/Controller über eine IP-Verbindung zum Vocera Communication Server verfügt.
- Überprüfen Sie die HF-Signalstärke und die CQ-Werte.

Badge verliert Sprachqualität beim Roaming

- Überprüfen Sie den Zielzugriffspunkt auf niedrige RSSI.
- Die Kanalüberschneidung ist möglicherweise unzureichend. Das Badge muss Zeit haben, den Anruf reibungslos abzugeben, bevor es sein Signal beim ursprünglichen Access Point verliert.
- Das Signal vom ursprünglichen Access Point kann verloren gehen.

Audioprobleme

Es gibt einige häufige Konfigurationsfehler, die einige leicht zu behebende Audioprobleme verursachen können. Wenn möglich sollten Sie die Audioprobleme mit einem stationären (Referenz-)Badge abgleichen, um das Problem auf ein Wireless-Problem einzugrenzen. Häufige Audioprobleme sind:

- Einseitige Audiofunktion
- Choppy- oder Roboteraudio
- Probleme bei der Registrierung und Authentifizierung

Einseitige Audiofunktion

- Dieses Problem kann in Randbereichen eines Access Points auftreten, in denen ein Signal entweder auf der Badge- oder der Access Point-Seite zu schwach sein kann. Wenn die Energieeinstellungen des Access Points dem Badge (20 mW) entsprechen, kann dieses Problem behoben werden. Dieses Problem tritt am häufigsten auf, wenn die Abweichung zwischen der Access Point-Einstellung und der Badge-Einstellung groß ist (z. B. 100 mW auf dem Access Point und 28 mW auf dem Badge).
- Prüfen Sie das Gateway und das IP-Routing auf Sprachqualität.
- Überprüfen Sie, ob sich eine Firewall oder NAT im Pfad der proprietären UDP-Pakete befindet. Standardmäßig verursachen Firewalls und NATs unidirektionales Audio oder keine Audiowiedergabe. Cisco IOS® und PIX NATs und Firewalls können diese Verbindungen so modifizieren, dass bidirektionaler Audio-Datenfluss möglich ist.Wenn Sie Layer-3-Mobilität verwenden, blockiert Ihr Netzwerk möglicherweise Upstream-Datenverkehr mithilfe von uRPF-Prüfungen (Unicast Reverse Path Forwarding).
- Einseitiges Audio kann auftreten, wenn das ARP-Caching auf dem WLC nicht konfiguriert ist.

Choppy- oder Roboteraudio

- Ein häufiger Grund für abgehacktes oder robotisches Audio ist die Mikrowelle, die in der Nähe betrieben wird. Mikrowellen beginnen bei Kanal 9 und können von Kanal 6 bis 14 reichen.
- Suchen Sie mithilfe von Tools wie Cognio nach 2,4-GHz-Wireless-Telefonen und anderen Wireless-Geräten für Krankenpfleger.

Probleme bei der Registrierung und Authentifizierung

Wenn bei der Authentifizierung Probleme auftreten, führen Sie folgende Prüfungen durch:

- Überprüfen Sie die SSIDs, um sicherzustellen, dass sie auf dem Badge und dem Access Point (oder Netzwerk) übereinstimmen. Stellen Sie außerdem sicher, dass das Netzwerk eine Route zum Vocera-Server hat.
- Überprüfen Sie die WEP-Schlüssel, um sicherzustellen, dass sie übereinstimmen. Es empfiehlt sich, diese erneut im Badge Configuration Utility (BCU) einzugeben und das Badge neu zu programmieren, da bei der Eingabe eines WEP-Schlüssels oder eines WEP-Kennworts leicht ein Schreibfehler auftritt.

Diese Meldungen oder Symptome können auftreten:

- Nicht alle angeforderten Funktionen unterstützen - Dies ist höchstwahrscheinlich eine Verschlüsselungsungleichheit zwischen dem Access Point und dem Client.
- Authentifizierung fehlgeschlagen / Kein AP gefunden - Stellen Sie sicher, dass die Authentifizierungstypen auf dem Access Point und dem Client übereinstimmen.
- No Service - IP Config Failed (Kein Dienst - IP-Konfiguration fehlgeschlagen) - Wenn Sie statisches WEP verwenden, stellen Sie sicher, dass die Schlüssel korrekt konfiguriert sind. Stellen Sie sicher, dass andere Clients DHCP über dieselbe SSID empfangen können.
- Die Authentifizierung aller TKIP-Clients vom Access Point wird aufgehoben - Dieses Problem tritt auf, wenn der Access Point innerhalb von 60 Sekunden zwei MIC-Fehler erkennt. Diese Gegenmaßnahme verhindert, dass alle TKIP-Clients 60 Sekunden lang erneut authentifiziert werden.
- Re-Authentication/Session Timeout (Erneute Authentifizierung/Sitzungs-Timeout): Bei Konfiguration löst ein Sitzungs-Timeout eine erneute Authentifizierung aus, die Lücken im Sprach-Stream verursacht (300 ms + WAN-Verzögerung für 802.1x-Authentifizierung).

Anhang A

Platzierung von APs und Antennen

Dieser Abschnitt enthält Beispiele für die korrekte und unsachgemäße Platzierung von Access Points (APs) und Antennen.

Abbildung 17 zeigt die unsachgemäße Platzierung eines Access Points und Antennen in der Nähe eines I-Strahls, wodurch verzerrte Signalmuster entstehen. Ein RF-Null-Punkt wird durch die Überquerung von Signalwellen erzeugt, und eine Multi-Path-Verzerrung wird erzeugt, wenn Signalwellen reflektiert werden. Diese Anordnung führt zu einer sehr geringen Abdeckung hinter dem Access Point und einer geringeren Signalqualität vor dem Access Point.

Abbildung 17: Fehlerhafte Platzierung von Antennen in der Nähe eines I-Strahls

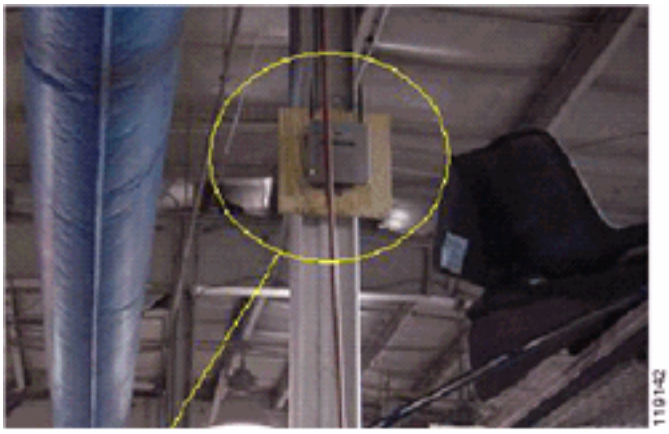
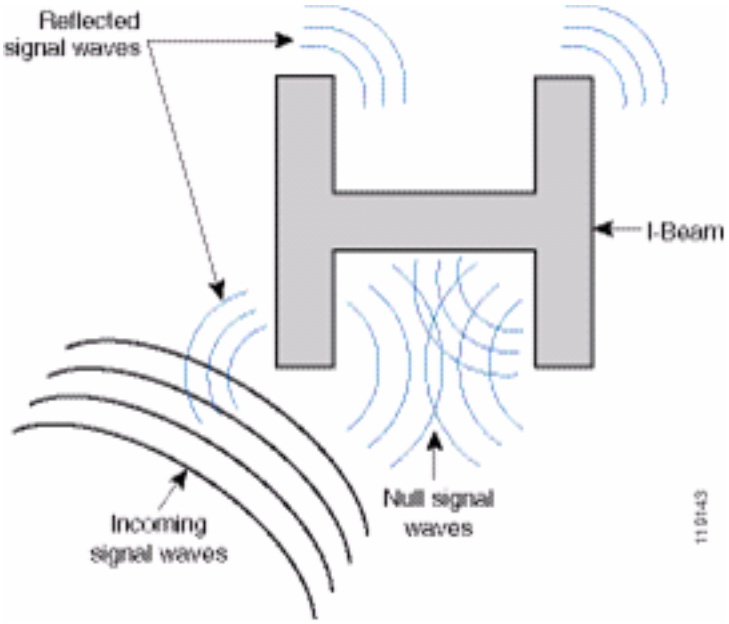


Abbildung 18 zeigt die Signalausbreitungsänderungen oder -verzerrungen, die durch einen I-Strahl verursacht werden. Der I-Strahl erzeugt viele Reflexionen sowohl von empfangenen Paketen als auch von übertragenen Paketen. Die reflektierten Signale führen aufgrund von Nullpunkten und Multipath-Interferenzen zu einer sehr schlechten Signalqualität. Die Signalstärke ist jedoch hoch, da sich die Antennen der Access Points so nahe am I-Strahl befinden.

Abbildung 18: Signalverzerrungen, die durch die Anordnung der Antennen zu nahe an einem E-Strahl verursacht werden



Die Positionierung des Access Points und der Antenne in Abbildung 19 ist besser, da sie sich nicht an den I-Strahlen befinden und weniger reflektierte Signale, weniger Null-Punkte und weniger Multipath-Interferenzen vorhanden sind. Diese Positionierung ist noch immer nicht perfekt, da das Ethernet-Kabel nicht so nahe an der Antenne befestigt werden sollte. Außerdem können die 2,4-GHz-Antennen des Access Points auf den Boden gerichtet werden. Dadurch wird eine bessere Abdeckung direkt unter dem Access Point gewährleistet. Über dem Access Point befinden sich keine Benutzer.

Abbildung 19: Access Point und an einer Wand montierte Antennen, abseits von I-Beams

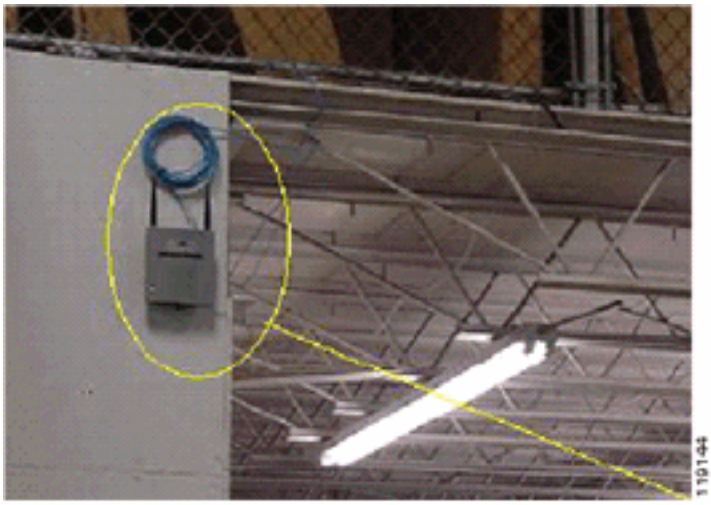
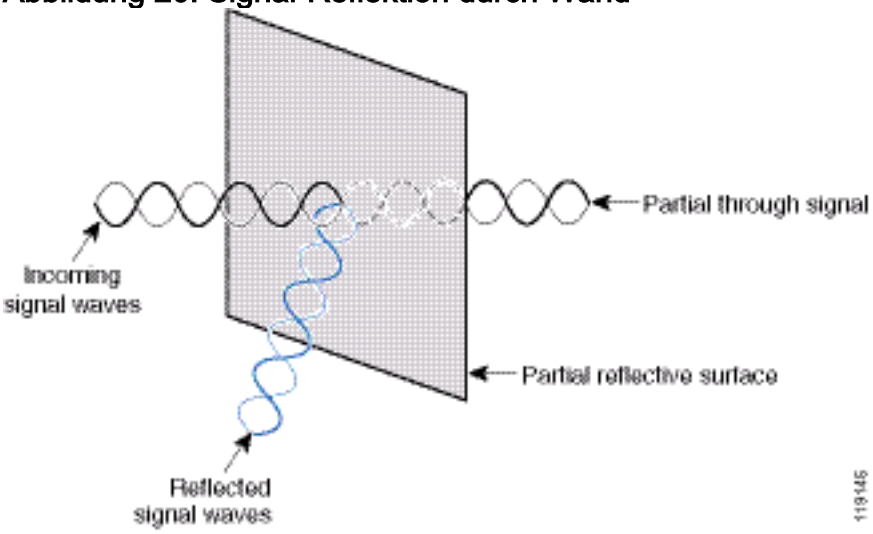


Abbildung 20 zeigt die Signalübertragung, die durch die Wand verursacht wird, an der der Access Point montiert ist.

Abbildung 20: Signal-Reflektion durch Wand



Die obigen Beispiele gelten auch, wenn Sie Access Points und Antennen in einer Standard-Enterprise-Umgebung in oder nahe der Decke platzieren. Wenn es Metallluftkanäle, Elevator-Schächte oder andere physische Barrieren gibt, die eine Signalreflexion oder Multipath-Interferenz verursachen können, empfiehlt Cisco dringend, die Antennen von diesen Hindernissen zu entfernen. Im Fall des Aufzugs die Antenne einige Meter entfernt bewegen, um die Signalreflexion und -verzerrung zu vermeiden. Dasselbe gilt für die Luftkanäle an der Decke.

Eine Umfrage ohne Senden und Empfangen von Paketen ist nicht ausreichend. Das I-beam-Beispiel zeigt die Erstellung von NULL-Punkten, die aus Paketen mit CRC-Fehlern resultieren können. Sprachpakete mit CRC-Fehlern sind verpasste Pakete, die die Sprachqualität beeinträchtigen. In diesem Beispiel könnten diese Pakete die von einem Umfragewerkzeug gemessene Rauschuntergrenze überschreiten. Daher ist es sehr wichtig, dass die Standortuntersuchung nicht nur die Signalpegel misst, sondern auch Pakete generiert und anschließend Paketfehler meldet.

Abbildung 21 zeigt einen Cisco AP1200, der ordnungsgemäß an einer T-Leiste an der Decke befestigt ist, wobei sich die Antennen in einer omnidirektionalen Position befinden.

Abbildung 21: Anbringung des Cisco AP1200 an der Decke

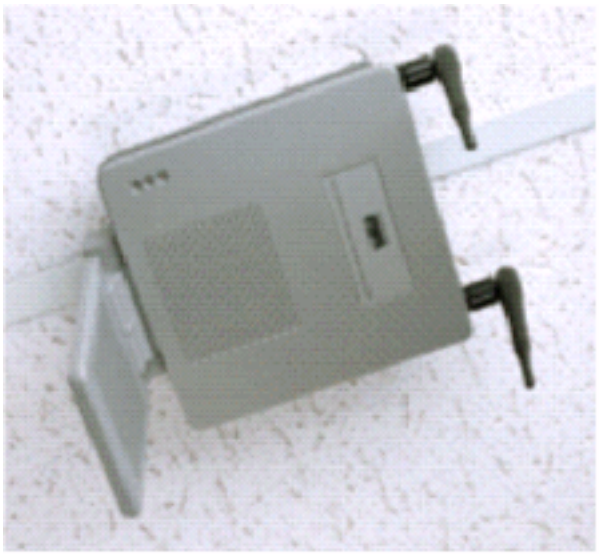


Abbildung 22 zeigt eine omnidirektionale Diversity-Antenne des Cisco Aironet 5959, die ordnungsgemäß an einer T-Leiste an der Decke montiert ist. In diesem Fall wird der Cisco AP1200 über der Deckenplatte montiert.

Abbildung 22: An der Decke montierte Cisco Aironet 5959-Antenne

Abbildung 23 zeigt einen Cisco AP1200, der ordnungsgemäß an der Wand befestigt ist.

Abbildung 23: Wandmontage des Cisco AP1200

Abbildung 24 zeigt die an einer Wand montierte Diversity-Patch-Antenne Cisco Aironet 2012. In diesem Fall wird der Cisco AP1200 über der Deckenplatte montiert.

Abbildung 24: Wandmontage der Cisco Aironet 2012-Antenne

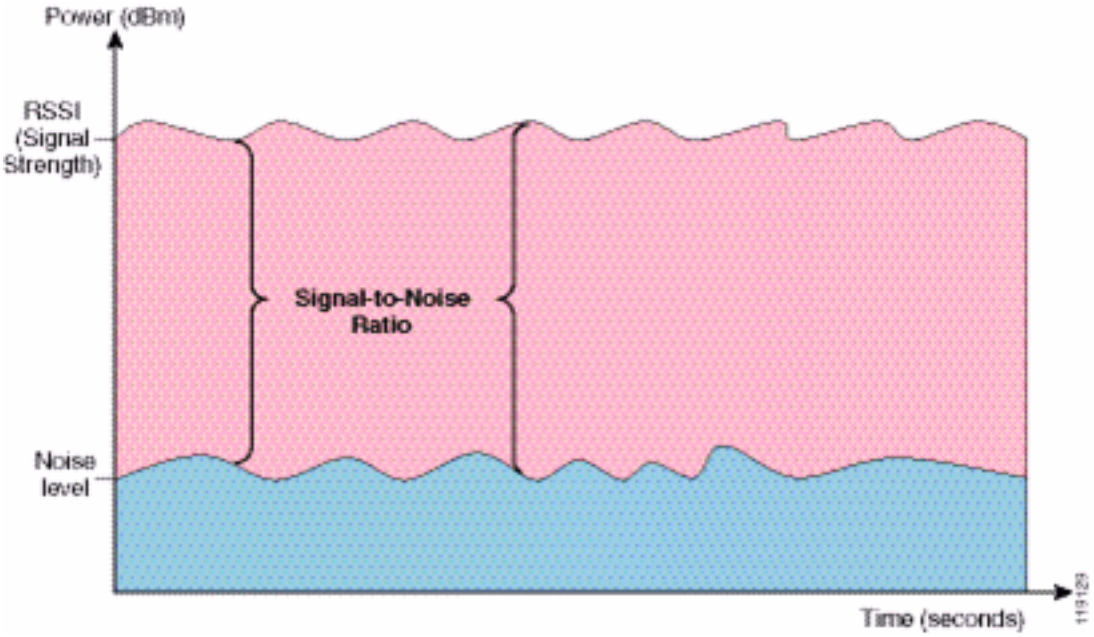
Für Bereiche mit hohem Benutzerdatenverkehr (z. B. Büroflächen, Schulen, Einzelhandelsgeschäfte und Krankenhäuser) empfiehlt Cisco, den Access Point außerhalb des Sichtbereichs zu platzieren und unauffällige Antennen unter die Decke zu stellen. Die Trennlinie für Antennen ohne Diversität darf nicht größer als 18 Zoll sein.

Störungen und Multipath-Verzerrung

Die Durchsatzleistung des WLAN-Netzwerks wird durch unbrauchbare Signale beeinflusst. WLAN-Interferenzen können durch Mikrowellenherde, schnurlose 2,4-GHz-Telefone, Bluetooth-Geräte oder andere elektronische Geräte im 2,4-GHz-Frequenzband verursacht werden. Interferenzen kommen in der Regel auch von anderen Access Points und Client-Geräten, die zum WLAN gehören, aber weit genug entfernt sind, sodass ihr Signal geschwächt oder beschädigt wird. Access Points, die nicht Teil der Netzwerkinfrastruktur sind, können ebenfalls WLAN-Interferenzen verursachen und als unautorisierte Access Points identifiziert werden.

Interferenzen und Multipath-Verzerrungen verursachen Schwankungen des übertragenen Signals. Interferenzen reduzieren das Signal-Rausch-Verhältnis (SNR) für eine bestimmte Datenrate. Die Anzahl der Wiederholungen von Paketen steigt in Bereichen an, in denen die Interferenz und/oder die Multipath-Verzerrung hoch sind. Störungen werden auch als Geräuschpegel oder Rauschpegel bezeichnet. Die Stärke des empfangenen Signals des zugehörigen Access Points muss hoch genug sein, um den Rauschpegel des Empfängers korrekt zu dekodieren. Diese Stärke wird als Signal-Rausch-Verhältnis (SNR) bezeichnet. Die optimale SNR-Funktion für das Vocera-Badge ist 25 dB. Wenn beispielsweise der Rauschpegel 95 Dezibel pro Milliwatt (dBm) beträgt und das Empfangssignal am Telefon 70 dBm beträgt, liegt das Signal-Rausch-Verhältnis bei 25 dB. (Siehe Abbildung 25.)

Abbildung 25: Signal-Rausch-Verhältnis (SNR)



Wenn Sie Typ und Position der Antenne ändern, können Sie die Verzerrung und Interferenzen bei mehreren Pfaden verringern. Die Antennenverstärkung erhöht die Systemverstärkung und kann Störungen reduzieren, wenn sich der Störsender nicht direkt vor der Richtungsantenne befindet.

Richtantennen können für bestimmte Anwendungen in Innenräumen zwar von großem Wert sein, die Mehrzahl der Installationen in Innenräumen verwendet jedoch Rundstrahlantennen. Die Richtlinien sollten durch eine korrekte und korrekte Standortuntersuchung streng festgelegt werden. Unabhängig davon, ob Sie eine Rundstrahlantenne oder eine Patch-Antenne verwenden: In Innenbereichen sind Diversity-Antennen erforderlich, um Multipath-Verzerrungen zu vermeiden. Die Cisco Aironet Access Point-Funkeinheiten ermöglichen die Unterstützung verschiedener Funktionen.

Signaldämpfung

Eine Signaldämpfung oder Signalverlust tritt auch dann auf, wenn das Signal durch die Luft geleitet wird. Der Verlust der Signalstärke ist ausgeprägter, wenn das Signal durch verschiedene Objekte geleitet wird. Eine Übertragungsleistung von 20 mW entspricht 13 dBm. Wenn also die Übertragungsleistung am Eintrittspunkt einer Gipsplatte bei 13 dBm liegt, wird die Signalstärke beim Verlassen dieser Wand auf 10 dBm reduziert. Diese Tabelle zeigt den wahrscheinlichen Verlust der Signalstärke, der durch verschiedene Objekttypen verursacht wird.

Signaldämpfung aufgrund verschiedener Objekttypen

Objekt in Signalpfad	Signaldämpfung durch Objekt
Plasterboard-Wand	3 dB
Glaswand mit Metallrahmen	6 dB
Wandhalterung	4 dB
Office-Fenster	3 dB
Metalltür	6 dB
Metalltür in Ziegelwand	12 dB
Körperkörper	3 dB

Jeder Standort hat unterschiedliche Ebenen von Multipath-Verzerrung, Signalverlusten und Signalrauschen. Krankenhäuser sind aufgrund hoher Multipath-Verzerrung, Signalverlusten und Signalrauschen in der Regel die schwierigsten bei der Untersuchung. Krankenhäuser benötigen mehr Zeit für die Erhebung, benötigen eine größere Anzahl von Access Points und benötigen höhere Leistungsstandards. Die Fertigungsbranche und der Einzelhandel sind die nächstschwierigsten Befragungen. Diese Standorte verfügen in der Regel über Metallteile und viele Metallgegenstände auf dem Boden, was zu reflektierten Signalen führt, die Multipfad-Verzerrungen wiedergeben. Bürogebäude und Beherbergungsstätten weisen in der Regel eine hohe Signaldämpfung auf, sind aber weniger verzerrt.

Zugehörige Informationen

- Bereitstellung der Cisco Wireless LAN Controller der Serie 440X
- Solution Reference Network Design
- Vocera Communications System - Spezifikationen
- Technischer Support und Dokumentation für Cisco Systeme