Installazione di Vocera IP Phone nell'infrastruttura UWN

Sommario

Introduzione

Questo documento fornisce considerazioni sulla progettazione e linee guida per l'implementazione della tecnologia VoWLAN (Vocera® Badge Voice over WLAN) sull'infrastruttura di rete wireless unificata Cisco.

Nota: il supporto per i prodotti Vocera deve essere ottenuto direttamente dai canali di supporto Vocera. Il supporto tecnico Cisco non è qualificato per supportare i problemi relativi a Vocera.

Questa guida è un supplemento alla Cisco Wireless LAN Controller Deployment Guide e tratta solo i parametri di configurazione che sono specifici dei dispositivi VoWLAN Vocera in un'architettura leggera. per ulteriori informazioni, fare riferimento a Implementazione dei Cisco Wireless LAN Controller serie 440X.

Prerequisiti

Requisiti

Si presume che i lettori abbiano familiarità con i termini e i concetti presentati in Cisco IP Telephony SRND e Cisco Wireless LAN SRND. .

Guida alla progettazione UC wireless:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_wireless_uc.html

SRND per Cisco Unified Communications basato su Cisco Unified Communications Manager 7.x:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_uc_mgr.html

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Sintesi

Nella tabella vengono riepilogate le quattro funzioni chiave e il loro comportamento all'interno di una rete wireless unificata Cisco.

	Controller singolo	Roaming da controller a controller di livello 2	Roaming da controller a controller di livello 3
Badge-to-Badge	Nessuna configurazione speciale	Nessuna configurazione speciale	Nessuna configurazione speciale
Badge-to-Phone	Nessuna configurazione speciale	Nessuna configurazione speciale	Nessuna configurazione speciale
Badge-to-Broadcast	Abilita multicast controller	Abilitare il multicast del controller Disabilitare lo snooping IGMP della VLAN Vocera o eseguire 4.0.206.0 o versioni successive	4.0.206.0 o successiva
Posizione badge	Nessuna configurazione speciale	Nessuna configurazione speciale	Nessuna configurazione speciale

Panoramica dei badge Vocera

I badge di comunicazione consentono una comunicazione istantanea con qualsiasi altro utente che li indossa, nonché l'integrazione Private Branch Exchange (PBX) e il rilevamento della

posizione dei badge. L'utilizzo di una rete wireless 802.11b/g richiede l'utilizzo di pacchetti unicast multicast e UDP con requisiti limitati per QoS (Quality of Service) a partire dal software server Vocera versione 3.1 (Build 1081). Le funzionalità di crittografia sono WEP (Wired Equivalent Privacy) a 64/128 bit, TKIP (Temporal Key Integrity Protocol), MIC (Message Integrity Check) e CKIP (Cisco Temporal Key Integrity Protocol), combinate con le funzionalità di autenticazione di Open, Wi-Fi Protected Access-Pre-shared Key (WPA-PSK), WPA-Protected Extensible Authentication Protocol (PEAP) e Lightweight Extensible Authentication Protocol (LEAP).

Con la pressione di un pulsante, il server Vocera risponde con Vocera, che è un prompt per emettere comandi come record, dove (am I) /is..., call, play, **broadcast**, **messaggi**, e così via. Il server Vocera fornisce i servizi e/o la configurazione delle chiamate necessari per completare la richiesta.

Il sistema di comunicazione 802.11b di Vocera utilizza la compressione vocale proprietaria e l'uso di un intervallo di porte UDP. Il software Vocera System viene eseguito su un server Windows che gestisce la configurazione delle chiamate, la connessione delle chiamate e i profili utente. Hanno collaborato con il software di riconoscimento vocale e impronta vocale Nuance 8.5 per abilitare le comunicazioni vocali tramite badge. Vocera consiglia di utilizzare un server Windows separato per eseguire il software delle soluzioni di telefonia Vocera e abilitare la connettività POTS (Plain Old Telephone Service) con i badge.

Considerazioni sulla capacità delle chiamate Vocera

Per ulteriori informazioni, vedere la sezione Dimensionamento della rete di questo documento.

Capacità di Vocera Communications Server

Per ulteriori informazioni sulla matrice di dimensionamento di Vocera Server, consultare le specifiche di Vocera Communications.

La soluzione Vocera

Il Vocera Badge utilizza sia la consegna di pacchetti unicast che multicast per fornire diverse caratteristiche chiave che costituiscono questa soluzione completa. Ecco quattro delle caratteristiche essenziali che si basano sulla corretta consegna del pacchetto. Viene inoltre fornita una descrizione di base di come ogni funzionalità utilizza la rete sottostante per la distribuzione e la funzionalità.

- Badge to Badge Communications: quando un utente di Vocera chiama un altro utente, il badge contatta per primo il server Vocera, che cerca l'indirizzo IP del badge del destinatario della chiamata e contatta l'utente del badge per chiedere all'utente se può ricevere una chiamata. Se il destinatario accetta la chiamata, il server Vocera notifica al badge chiamante l'indirizzo IP del badge destinatario per impostare la comunicazione diretta tra i badge senza ulteriori interventi del server. Tutte le comunicazioni con il server Vocera utilizzano il codec G.711 e tutte le comunicazioni badge-to-badge utilizzano un codec proprietario di Vocera.
- Comunicazione telefonica con badge: quando un server di telefonia Vocera viene installato e configurato con una connessione a un PBX, un utente può chiamare le estensioni interne del PBX o le linee telefoniche esterne. Vocera consente agli utenti di effettuare chiamate dicendo i numeri (cinque, sei, tre, due) o creando una voce di rubrica nel database Vocera per la

persona o la funzione a quel numero (ad esempio, farmacia, casa, pizza) il server Vocera determina il numero che viene chiamato, intercettando i numeri nell'estensione o cercando il nome nel database e selezionando il numero. Il server Vocera trasmette quindi tali informazioni al server di telefonia Vocera che si connette al PBX e genera i segnali di telefonia appropriati (ad esempio, DTMF). Tutte le comunicazioni tra il badge e il server Vocera e il server Vocera e il server Vocera Telephony utilizzano il codec G.711 su UDP unicast.

- Trasmissione Vocera: un utente Vocera Badge può chiamare e comunicare contemporaneamente con un gruppo di utenti Vocera badge utilizzando il comando Trasmissione. Quando un utente trasmette a un gruppo, il badge dell'utente invia il comando al server Vocera che cerca i membri di un gruppo, determina quali membri del gruppo sono attivi, assegna un indirizzo multicast da utilizzare per questa sessione di trasmissione e invia un messaggio al badge di ogni utente attivo per informarlo di unirsi al gruppo multicast con l'indirizzo multicast assegnato.
- Funzione di localizzazione dei badge: il server Vocera tiene traccia del punto di accesso a cui è associato ciascun badge attivo, in quanto ogni badge invia un keep-alive di 30 secondi al server con il BSSID associato. Questo permette al sistema Vocera di stimare approssimativamente la posizione di un utente di badge. La precisione di questa funzione è relativamente bassa in quanto è possibile che un badge non sia associato al punto di accesso al quale è più vicino.

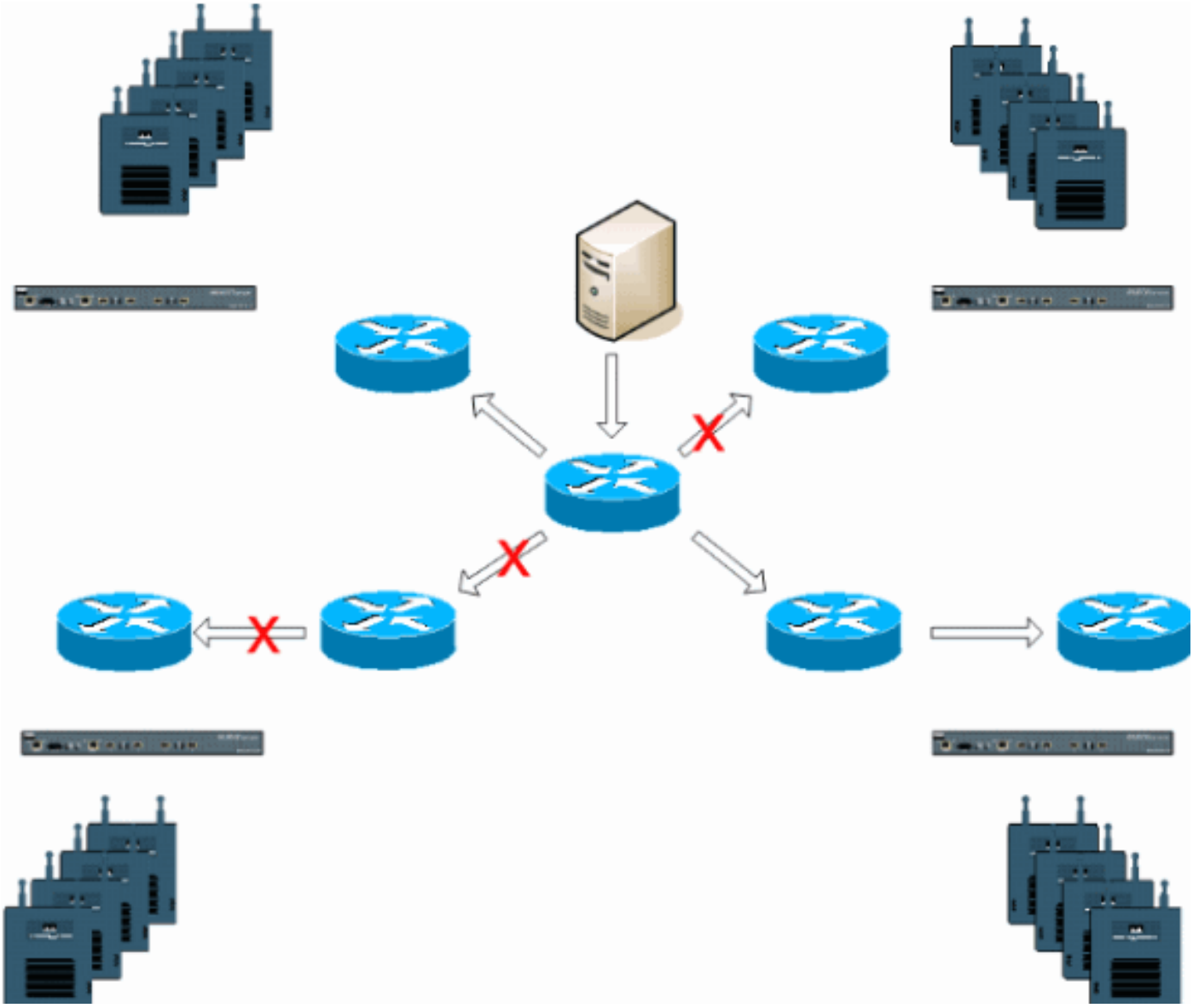
Pianificazione dell'infrastruttura di Vocera

Il white paper Vocera Vocera Infrastructure Planning Guide descrive i requisiti minimi del sondaggio del sito che mostrano che il badge deve avere un livello di potenza del segnale di ricezione minimo di -65 dBm, un rapporto segnale/rumore maggiore di 25 db e una corretta sovrapposizione dei punti di accesso e separazione dei canali. Sebbene i badge utilizzino un'antenna omnidirezionale simile come notebook utilizzato per un sondaggio del sito, non imita molto bene il comportamento del badge, dato che gli utenti influiscono sulla potenza del segnale. Tenuto conto di questo requisito unico e del comportamento del dispositivo trasmittente, l'utilizzo dell'architettura Cisco e la gestione delle risorse radio sono la soluzione ideale per garantire la mancanza di caratteristiche insolite del sito a radiofrequenza (RF).

Il distintivo Vocera è un dispositivo a bassa potenza, indossato vicino al corpo con limitate capacità di correzione dell'errore del segnale. I requisiti di Vocera descritti in questo documento possono essere soddisfatti con facilità. Tuttavia, può diventare eccessivamente difficile se ci sono troppi SSID per l'elaborazione e consentire al badge di funzionare efficacemente.

Panoramica dell'architettura

Figura 1 - Funzionalità generale di inoltro e cancellazione del multicast con tecnologia wireless LWAPP (Lightweight Access Point Protocol)



Multicast in una distribuzione LWAPP

La comprensione del multicast in una distribuzione LWAPP è necessaria per distribuire la funzione di trasmissione Vocera. Questo documento descrive in seguito i passaggi essenziali per abilitare il multicast all'interno della soluzione basata su controller. Al momento il controller LWAPP utilizza due metodi di recapito per recapitare multicast ai client:

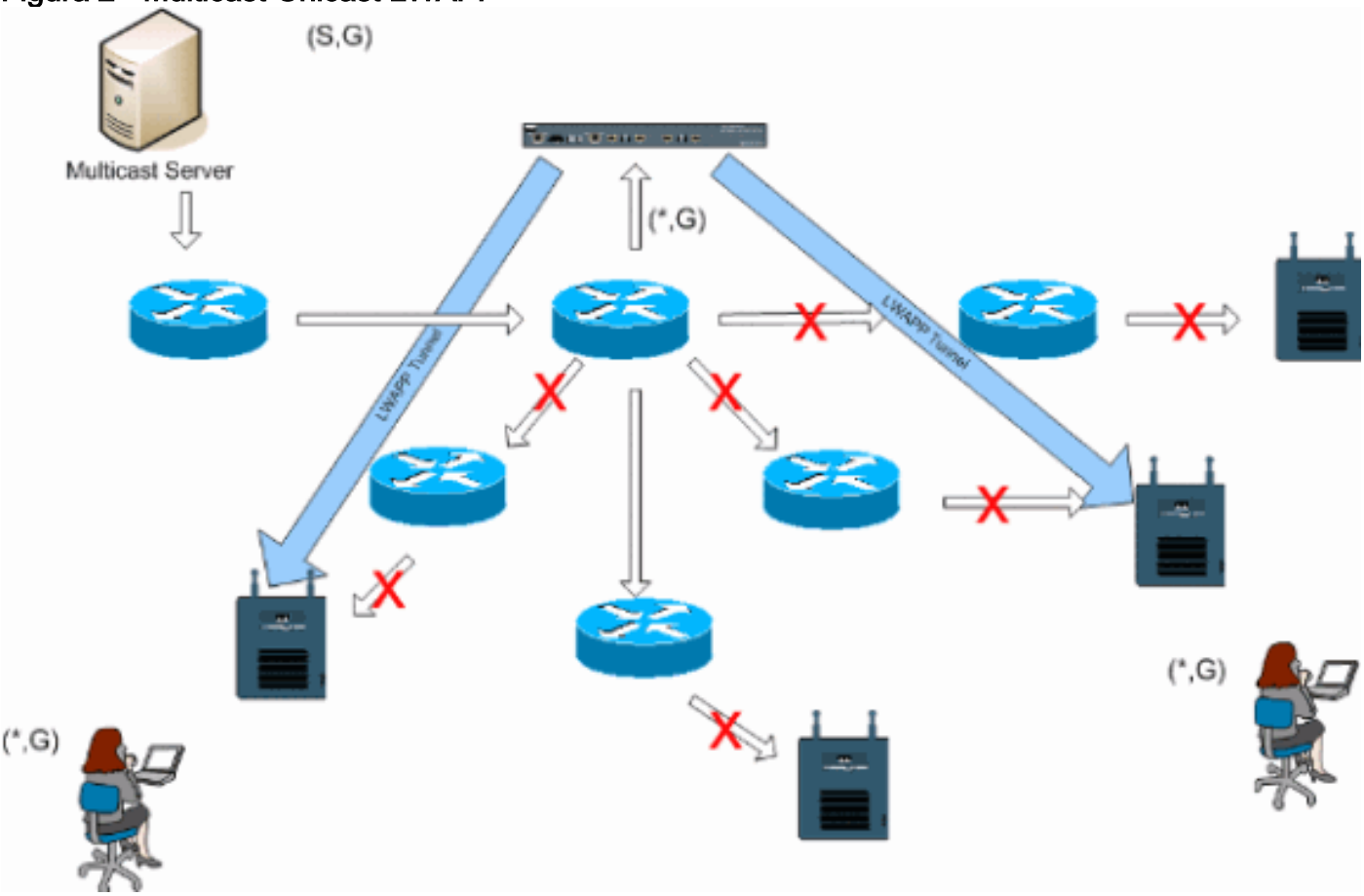
- Unicast-Multicast
- Multicast-Multicast

Metodo di recapito Unicast-Multicast

Il metodo di recapito unicast-multicast crea una copia di ogni pacchetto multicast e lo inoltra a ogni access point. Quando un client invia un join multicast alla LAN wireless, il punto di accesso inoltra il join al controller tramite il tunnel LWAPP. Il controller crea il bridge di questo join multicast sulla connessione diretta alla rete locale (LAN) che è la VLAN predefinita per la WLAN associata del client. Quando un pacchetto multicast IP arriva dalla rete al controller, il controller lo replica con un'intestazione LWAPP per ogni punto di accesso con un client nel dominio wireless che si è unito a questo gruppo specifico. Quando l'origine del multicast è anche un destinatario nel dominio wireless, il pacchetto viene anch'esso duplicato e inoltrato nuovamente allo stesso client che lo ha

inviato. Per i badge Vocera, questo non è il metodo preferito per il recapito multicast all'interno della soluzione controller LWAPP. Il metodo di recapito unicast funziona con distribuzioni di piccole dimensioni. Tuttavia, a causa del notevole sovraccarico sul controller WLC, questo non è mai il metodo di consegna multicast consigliato.

Figura 2 - Multicast-Unicast LWAPP



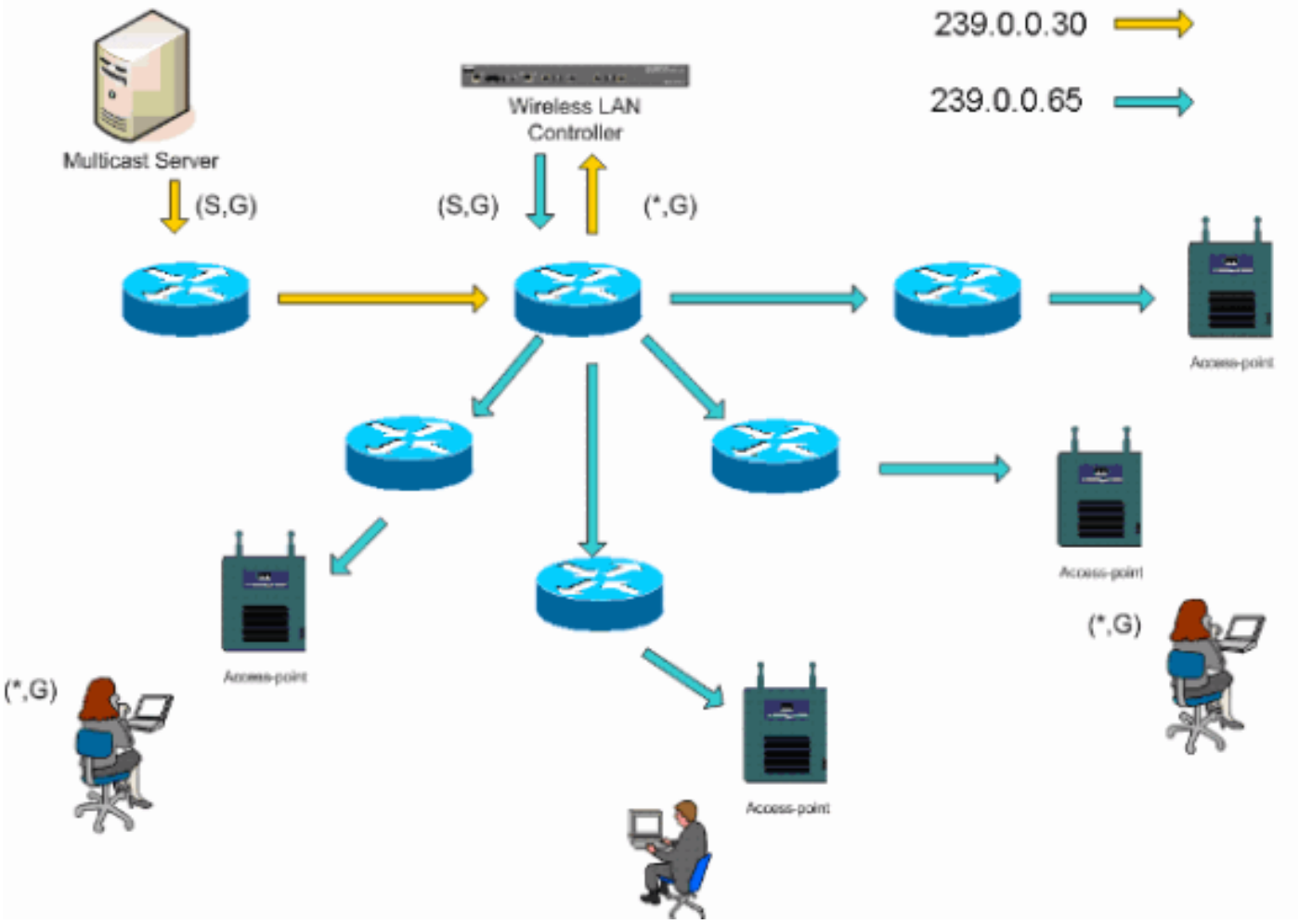
Nota: se sono configurate le VLAN del gruppo AP e un join IGMP viene inviato da un client tramite il controller, il join viene posizionato sulla VLAN predefinita della WLAN su cui si trova il client. Pertanto, il client potrebbe non ricevere questo traffico multicast a meno che non sia membro di questo dominio di trasmissione predefinito.

Metodo di recapito Multicast-Multicast

Il metodo di recapito multicast multicast non richiede che il controller replichi ogni pacchetto multicast ricevuto. Il controller è configurato per un indirizzo di gruppo multicast non utilizzato di cui ogni punto di accesso diventa membro. Nella Figura 3, il gruppo multicast definito dal WLC al punto di accesso è 239.0.0.65. Quando un client invia un join multicast alla WLAN, il punto di accesso inoltra il join al controller tramite il tunnel LWAPP. Il controller inoltra il protocollo del livello di collegamento sulla connessione diretta alla rete locale (LAN) che è la VLAN predefinita per la WLAN associata del client. Il router locale al controller aggiunge quindi l'indirizzo del gruppo multicast all'interfaccia per la voce di inoltro (*,G). Nella Figura 3, l'esempio di multicast join è stato inviato al gruppo multicast 239.0.0.30. Quando la rete inoltra il traffico multicast, l'indirizzo multicast 239.0.0.30 viene inoltrato al controller. Il controller incapsula quindi il pacchetto multicast in un pacchetto multicast LWAPP indirizzato all'indirizzo del gruppo multicast (ad esempio, 239.0.0.65) configurato sul controller e inoltrato alla rete. Ogni punto di accesso sul controller riceve questo pacchetto come membro del gruppo multicast dei controller. Il punto di accesso inoltra quindi il pacchetto multicast client/server (ad esempio, 239.0.0.30) come trasmissione alla WLAN/SSID identificata nel pacchetto multicast LWAPP.

Nota: se non si configura correttamente la rete multicast, è possibile che vengano ricevuti pacchetti multicast del punto di accesso di un altro controller. Se il primo controller deve frammentare il pacchetto multicast, il frammento viene inoltrato alla rete e ciascun punto di accesso deve perdere tempo per eliminare il frammento. Se si consente tutto il traffico compreso l'intervallo multicast 24.0.0.x, anche questo viene incapsulato e successivamente inoltrato da ciascun punto di accesso.

Figura 3 - Multicast-Multicast LWAPP



Configurazione multicast di router e switch

Questo documento non è una guida alla configurazione del multicast di rete. Per una descrizione completa dell'implementazione, consultare il documento sulla configurazione del routing multicast IP. Questo documento descrive le nozioni di base per abilitare il multicast nell'ambiente di rete.

Abilita routing multicast IP

Il routing IP multicast consente al software Cisco IOS® di inoltrare pacchetti multicast. il comando di configurazione globale **ip multicast-routing** è richiesto per consentire il funzionamento del multicast in qualsiasi rete abilitata per il multicast. Il comando **ip multicast-routing** deve essere abilitato su tutti i router della rete tra i WLC e i rispettivi punti di accesso.

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

Abilitare PIM su un'interfaccia

In questo modo viene abilitata l'interfaccia di routing per l'operazione IGMP (Internet Group Management Protocol). La modalità PIM (Protocol Independent Multicast) determina il modo in cui il router popola la relativa tabella di routing multicast. L'esempio fornito non richiede che il punto di rendering (RP) sia noto per il gruppo multicast e pertanto la modalità sparsa-densa è la più desiderabile data la natura sconosciuta dell'ambiente multicast. Questa non è una raccomandazione multicast da configurare per funzionare anche se l'interfaccia di layer 3 direttamente connessa al controller deve essere abilitata per PIM per il funzionamento del multicast. È necessario abilitare tutte le interfacce tra i WLC e i rispettivi punti di accesso.

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

Disabilitazione dello snooping Switch VLAN IGMP

Lo snooping IGMP consente a una rete a commutazione con multicast abilitato di limitare il traffico alle porte dello switch che hanno utenti che vogliono vedere il multicast mentre si eliminano i pacchetti multicast dalle porte dello switch che non vogliono vedere il flusso multicast. In un'implementazione di Vocera, può essere indesiderabile abilitare lo snooping CGMP o IGMP sulla porta dello switch a monte del controller con versioni software precedenti alla 4.0.206.0.

Il roaming e il multicast non sono definiti con una serie di requisiti per verificare che il traffico multicast possa seguire un utente sottoscritto. Sebbene il badge del client sia consapevole di aver effettuato il roaming, non inoltra un altro join IGMP per assicurarsi che l'infrastruttura di rete continui a consegnare il traffico multicast (broadcast Vocera) al badge. Allo stesso tempo, il punto di accesso LWAPP non invia una query multicast generale al client in roaming per richiedere questo join IGMP. Con una struttura di rete Vocera di layer 2, la disattivazione dello snooping IGMP consente l'inoltro del traffico a tutti i membri della rete Vocera, indipendentemente da dove si trovino. Ciò garantisce che la funzione di trasmissione di Vocera funzioni indipendentemente dal luogo in cui il client effettua il roaming. La disattivazione dello snooping IGMP a livello globale è un'operazione molto indesiderabile. Si consiglia di disabilitare lo snooping IGMP solo sulla VLAN Vocera collegata direttamente a ciascun WLC.

Per ulteriori informazioni, fare riferimento a Configurazione dello snooping IGMP.

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

Miglioramenti Multicast nella versione 4.0.206.0 e successive

Con la versione 4.0.206.0, Cisco introduce una query IGMP per consentire agli utenti di eseguire il roaming sul layer 2 inviando una query IGMP generale quando ciò si verifica. Il client risponde quindi con il gruppo IGMP di cui è membro e questo viene collegato alla rete cablata come descritto in precedenza in questo documento. Quando un client esegue il roaming a un controller che non dispone di connettività di livello 2 o a un router di livello 3, viene aggiunto il routing sincrono per i pacchetti di origine multicast. Quando un client che ha completato un roaming di layer 3 invia un pacchetto multicast dalla rete wireless, il controller esterno incapsula il pacchetto nel protocollo Ethernet over IP (EoIP) del tunnel IP per il controller di ancoraggio. Il controller di ancoraggio inoltra quindi il messaggio ai client wireless associati localmente e lo collega nuovamente alla rete cablata in cui viene instradato utilizzando i normali metodi di routing multicast.

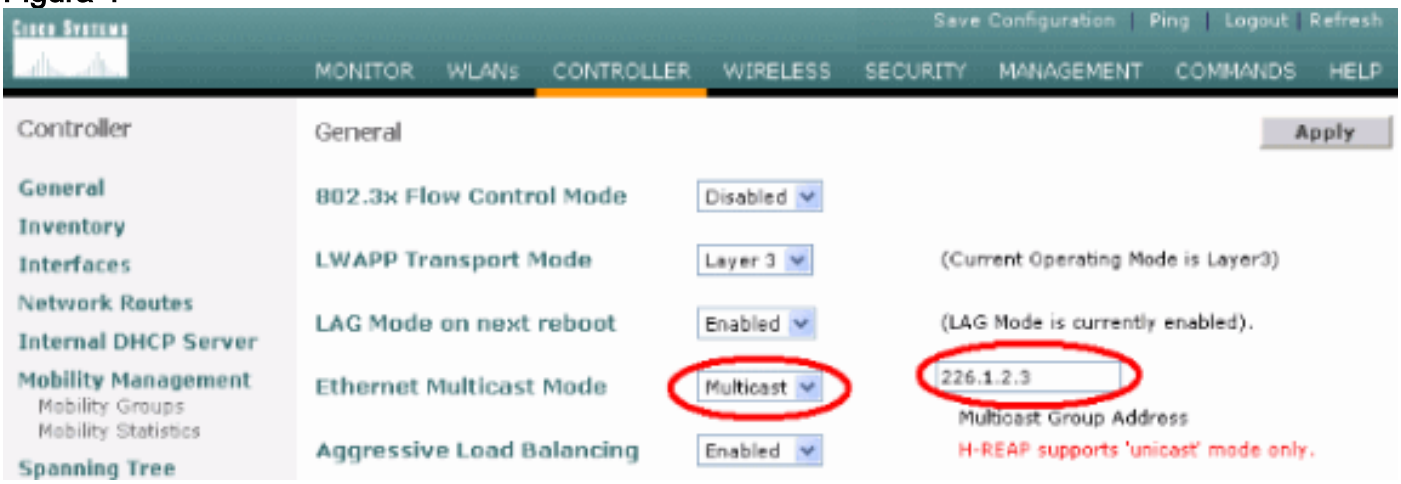
Scenari di distribuzione

Questi tre scenari di implementazione illustrano le best practice e i parametri di progettazione per un'installazione corretta di Vocera Badge:

- Distribuzione a controller singolo
- Distribuzione Layer 2 a più controller
- Distribuzione Layer 3 a più controller

Èessenziale comprendere come le funzioni Vocera Badge interagiscono all'interno di un ambiente MAC diviso LWAPP. In tutti gli scenari di distribuzione è consigliabile abilitare il multicast e disabilitare il bilanciamento aggressivo del carico. Tutte le WLAN di badge devono essere contenute nello stesso dominio di broadcast sull'intera rete.

Figura 4



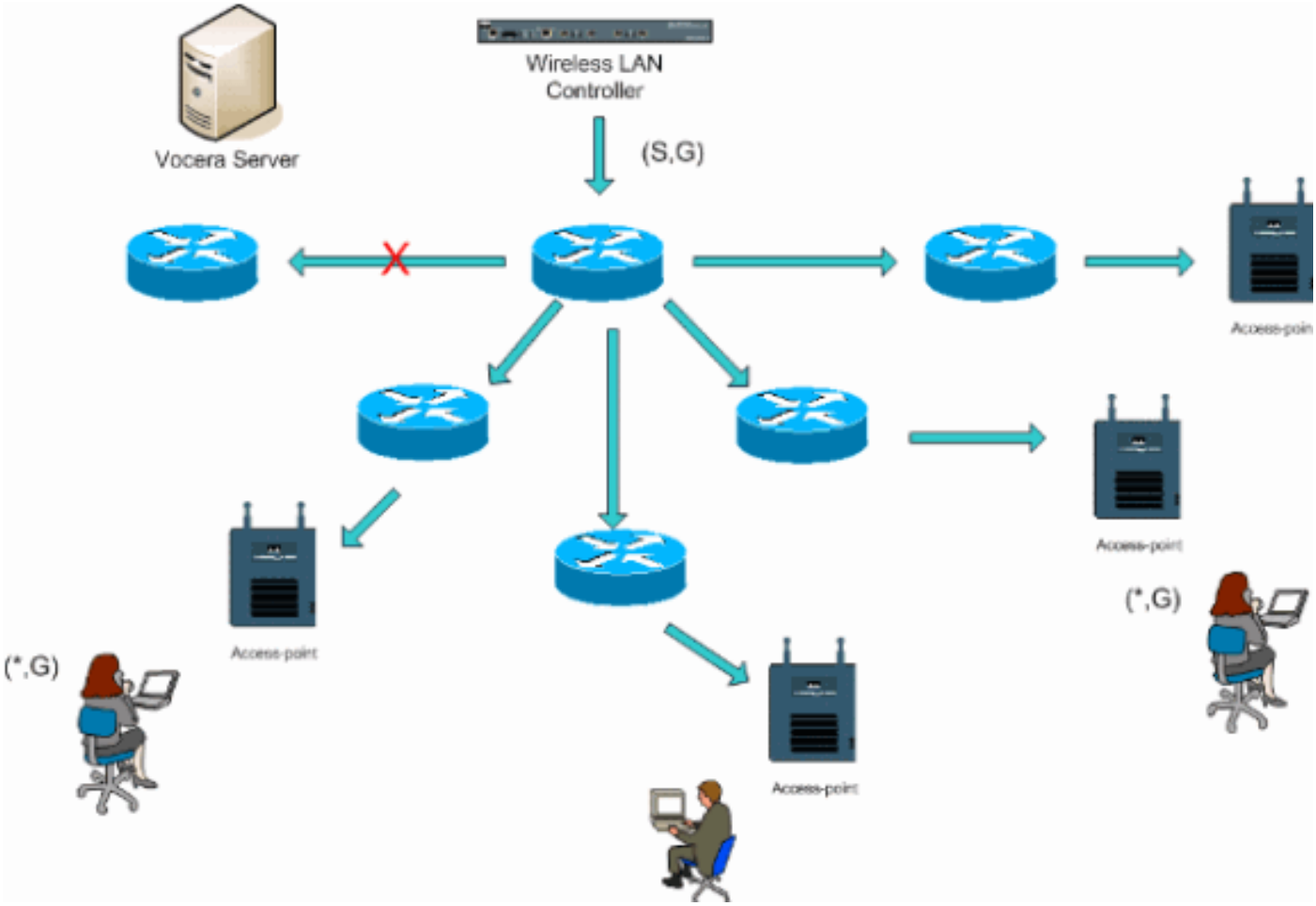
Distribuzione a controller singolo

Si tratta dello scenario di distribuzione più semplice. Consente di installare la soluzione Vocera Badge senza problemi di installazione. La rete deve essere abilitata per il routing multicast IP solo per consentire ai punti di accesso di ricevere i pacchetti multicast LWAPP. Se necessario, è possibile limitare la complessità del multicast di rete configurando tutti i router e gli switch con il gruppo multicast controller.

Con il multicast configurato globalmente sul controller, l'SSID, le impostazioni di sicurezza e tutti i punti di accesso appropriati hanno registrato la soluzione Vocera Badge e tutte le sue funzioni funzionano come previsto. Con la funzione Vocera Broadcast, l'utente viaggia e il traffico multicast segue come previsto. Non è necessario configurare ulteriori impostazioni per il corretto funzionamento di questa soluzione.

Quando un Vocera Badge invia un messaggio multicast, come nel caso di Vocera Broadcast, viene inoltrato al controller. Il controller incapsula quindi il pacchetto multicast all'interno di un pacchetto multicast LWAPP. L'infrastruttura di rete inoltra il pacchetto a tutti i punti di accesso connessi al controller. Quando il punto di accesso riceve il pacchetto, controlla l'intestazione multicast LWAPP per determinare a quale WLAN/SSID trasmette il pacchetto.

Figura 5 - Controller singolo in modalità multicast-multicast

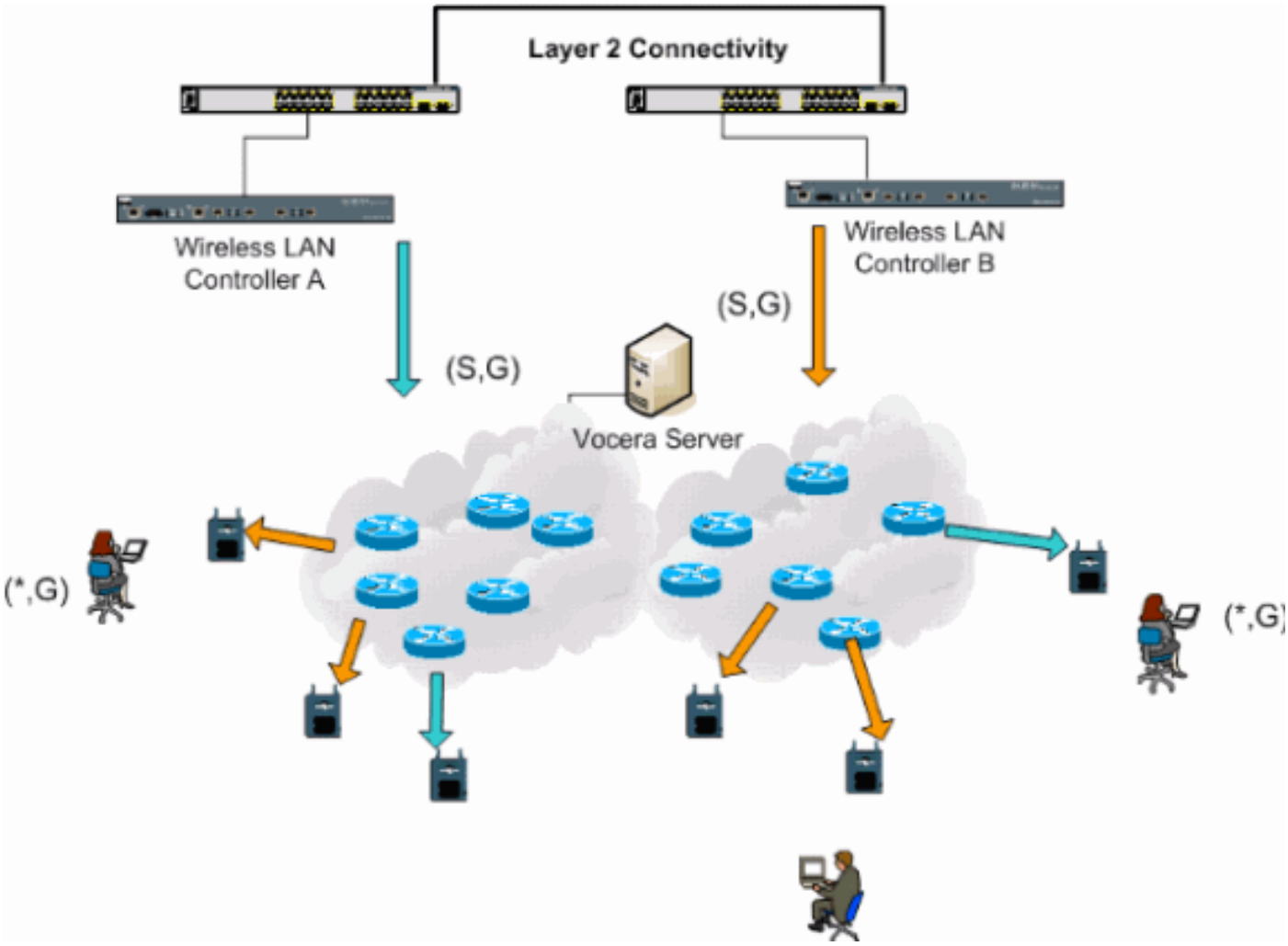


Distribuzione Layer 2 a più controller

Più controller devono essere collegati tra loro attraverso lo stesso dominio di broadcast di layer 2. Entrambi i controller sono configurati per il multicast come mostrato, utilizzando gli stessi gruppi multicast di punti di accesso su ciascun controller per limitare la frammentazione. Supponendo che questo dominio di broadcast di layer 2 sia connesso tramite uno switch comune o un set di switch comune, lo snooping CGMP/IGMP su questi switch deve essere disabilitato per questa singola VLAN o eseguire il software WLC 4.0.206.0 o versioni successive. Con la funzione Vocera Broadcast e un roaming utente da un punto di accesso su un controller a un punto di accesso su un controller diverso, non esiste alcun meccanismo per l'inoltro di join IGMP alla nuova porta di layer 2 per il funzionamento dello snooping IGMP. Se un pacchetto IGMP non raggiunge lo switch compatibile con CGMP o IGMP a monte, il gruppo multicast specificato non viene inoltrato al controller e pertanto non viene ricevuto dal client. In alcuni casi, questa procedura potrebbe funzionare se un client che fa parte dello stesso gruppo Vocera Broadcast ha già inviato questo pacchetto IGMP prima che il client in roaming esegua il roaming sul nuovo controller. Con i vantaggi della versione 4.0.206.0, un client che esegue il roaming su un altro controller come roaming di layer 2 riceve una query IGMP generale subito dopo l'autenticazione. Il client deve quindi rispondere con i gruppi interessati e il nuovo controller viene quindi collegato tramite bridge allo switch connesso localmente. Ciò consente i vantaggi di IGMP e CGMP sugli switch a monte.

Èpossibile creare SSID di badge e domini di livello 2 aggiuntivi per reti di badge separate, purché la rete sia configurata per passare il traffico multicast in modo appropriato. Inoltre, ogni dominio di broadcast di Vocera Layer 2 creato deve esistere ovunque un controller sia connesso alla rete in modo da non interrompere il multicast.

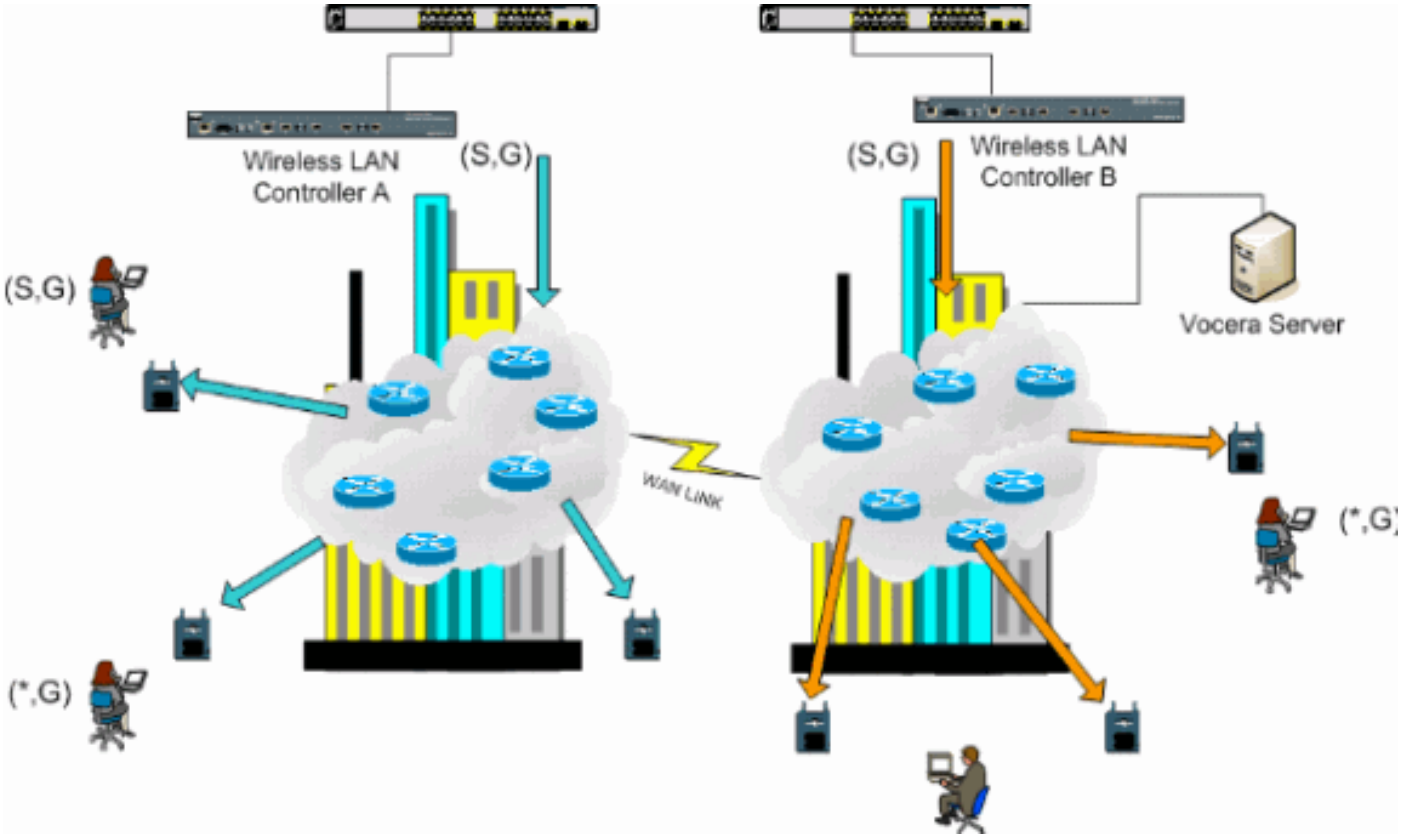
Figura 6 - Installazione di più controller di layer 2



Distribuzione Layer 3 a più controller

La strategia di distribuzione del roaming di layer 3 deve essere utilizzata solo con il roaming da controller a controller con il software WLC versione 4.0.206.0 o successive. Se un client che è stato connesso al gruppo di trasmissione Vocera e riceve il flusso multicast appropriato ed esegue il roaming a un altro controller come roaming di livello 3 con il roaming LWAPP di livello 3 configurato, viene richiesto di specificare i gruppi multicast interessati. Quando il client viene inviato allo stesso gruppo di trasmissione Vocera, questi pacchetti vengono consegnati al controller di ancoraggio tramite il tunnel EoIP e vengono instradati attraverso i normali metodi di routing multicast.

Figura 7 - Installazione di più controller di layer 3



Implementazioni VoWLAN: Raccomandazioni di Cisco

Le reti di telefonia IP wireless richiedono un'attenta pianificazione della radiofrequenza. Spesso è necessario effettuare un'accurata indagine sul sito vocale per determinare i livelli appropriati di copertura wireless e per identificare le fonti di interferenza. La selezione dei punti di accesso e delle antenne può essere notevolmente facilitata grazie ai risultati di un sondaggio valido sul sito vocale. La considerazione più importante è la potenza di trasmissione del telefono wireless. Idealmente il telefono apprende la potenza di trasmissione del punto di accesso e regola la sua potenza di trasmissione a quella del punto di accesso.

Sebbene oggi la maggior parte delle reti wireless venga implementata dopo un'ampia indagine sul sito RF, è necessario tenere presente anche il servizio dati. È probabile che i telefoni VoWLAN abbiano caratteristiche di roaming e requisiti di copertura diversi da quelli di una scheda WLAN tipica per un client mobile come un laptop. Pertanto, spesso è consigliabile eseguire un ulteriore sondaggio del sito per la comunicazione vocale per prepararsi ai requisiti di prestazioni di più client VoWLAN. Questo sondaggio aggiuntivo offre l'opportunità di regolare i punti di accesso per garantire che i telefoni VoWLAN abbiano una copertura RF e una larghezza di banda sufficienti a fornire una corretta qualità della voce.

Per ulteriori informazioni sulle considerazioni relative alla progettazione di RF, fare riferimento al capitolo sulle considerazioni di progettazione della frequenza radio (RF) WLAN nella Cisco Wireless LAN Design Guide, disponibile all'indirizzo http://cisco.com/go/srnd.

Consigli per edifici a più piani, ospedali e magazzini

Prendere in considerazione i fattori elencati in questa sezione quando si esaminano edifici, ospedali e magazzini a più piani.

Metodi e materiali di costruzione

Molti aspetti della costruzione dell'edificio sono sconosciuti o nascosti dal sondaggio del sito, quindi potrebbe essere necessario acquisire tali informazioni da altre fonti (come i disegni architettonici). Alcuni esempi di metodi e materiali costruttivi tipici che influenzano la gamma e l'area di copertura dei punti di accesso includono pellicola metallica su vetro finestra, vetro al piombo, pareti con chiodi di acciaio, pavimenti in cemento e pareti con rinforzo in acciaio, isolante a base di pellicola, trombe delle scale e alberi elevatori, tubi idraulici e attrezzature, e molti altri.

Inventario

Vari tipi di inventario possono influire sulla gamma RF, in particolare quelli con elevato contenuto di acciaio o acqua. Alcuni elementi da guardare includono scatole di cartone, cibo per animali domestici, vernice, prodotti petroliferi, parti di motore e così via.

Livelli di magazzino

Assicurarsi di eseguire un'indagine del sito ai livelli di inventario massimi o nei momenti di attività massima. Un magazzino con un livello di stoccaggio del 50% ha un'impronta RF molto diversa rispetto allo stesso magazzino con un livello di inventario del 100%.

Livelli di attività

Allo stesso modo, un ufficio fuori orario (senza personale) ha un'impronta RF diversa rispetto alla stessa area piena di persone durante il giorno. Anche se molte parti dell'indagine possono essere condotte senza una piena occupazione, è essenziale condurre la verifica del sito e regolare i valori chiave durante un periodo in cui il luogo è occupato. Più elevati sono i requisiti di utilizzo e la densità degli utenti, più importante è disporre di una soluzione Diversity ben progettata. Quando sono presenti più utenti, vengono ricevuti più segnali sul dispositivo di ogni utente. Segnali aggiuntivi causano più contesa, più punti nulli e più distorsione multipath. La diversità sul punto di accesso (antenne) aiuta a ridurre al minimo queste condizioni.

Edifici con più piani

Quando si esegue un sondaggio in un sito per un edificio tipico, tenere presenti le seguenti linee guida:

- Gli alberi di ascensore bloccano e riflettono i segnali RF.
- Fornire stanze con segnali di assorbimento dell'inventario.
- Gli uffici interni con pareti impenetrabili assorbono i segnali RF.
- Le sale di pausa (cucine) possono produrre interferenze a 2,4 GHz tramite l'uso di forni a microonde.
- I laboratori possono produrre interferenze a 2,4 GHz o 5 GHz, creando distorsioni a percorsi multipli e ombre RF.
- I cubicoli tendono ad assorbire e bloccare i segnali.
- Le sale conferenze necessitano di un punto di accesso di copertura elevato in quanto sono aree ad alto utilizzo.

Quando si esaminano le strutture a più piani è necessario adottare precauzioni supplementari. I punti di accesso situati su diversi piani possono interferire tra loro con la stessa facilità con cui si trovano sullo stesso piano. È possibile utilizzare questo comportamento a proprio vantaggio durante un sondaggio. Utilizzando antenne ad alto guadagno, potrebbe essere possibile penetrare

pavimenti e soffitti e fornire copertura ai pavimenti sopra e sotto il pavimento dove è montato il punto di accesso. Fare attenzione a non sovrapporre i canali tra punti di accesso su piani diversi o punti di accesso sullo stesso piano. Negli edifici multi-tenant, ci potrebbero essere problemi di sicurezza che richiedono l'uso di minori poteri di trasmissione e antenne di guadagno inferiore per tenere i segnali fuori dagli uffici vicini.

Ospedali

Il processo di indagine di un ospedale è molto simile a quello di un'azienda, ma la struttura di una struttura ospedaliera tende a differire nei seguenti modi:

- Gli edifici ospedalieri tendono a subire molti progetti di ricostruzione e aggiunte. Ogni costruzione aggiuntiva avrà probabilmente diversi materiali di costruzione con diversi livelli di attenuazione.
- La penetrazione del segnale attraverso pareti e pavimenti nelle aree dei pazienti è in genere minima, il che aiuta a creare micro-cellule e variazioni a percorsi multipli.
- La necessità di larghezza di banda aumenta con l'uso crescente di apparecchiature ad ultrasuoni WLAN e di altre applicazioni di imaging portatili. L'uso della larghezza di banda aumenta con l'aggiunta della voce wireless.
- Le celle sanitarie sono piccole e il roaming senza interruzioni è essenziale, soprattutto con le applicazioni vocali.
- La sovrapposizione delle celle può essere elevata e può quindi essere riutilizzata dal canale.
- Negli ospedali è possibile installare diversi tipi di reti wireless. Ciò include apparecchiature non 802.11 a 2,4 GHz. Questa apparecchiatura può causare il conflitto con altre reti a 2,4 GHz.
- Le antenne patch di diversità montate a parete e le antenne omnidirezionali di diversità montate a soffitto sono popolari, ma tenete presente che la diversità è richiesta.

Magazzini

I magazzini dispongono di ampie aree aperte che spesso contengono rack di storage elevati. Molte volte questi rack raggiungono quasi il soffitto, dove vengono solitamente posizionati i punti di accesso. Tali rack di storage possono limitare l'area che il punto di accesso può coprire. In questi casi, prendere in considerazione il posizionamento dei punti di accesso su altre posizioni oltre al soffitto, come pareti laterali e pilastri di cemento. Quando si esamina un magazzino, tenere in considerazione anche i seguenti fattori:

- I livelli di inventario influiscono sul numero di punti di accesso necessari. Copertura di prova con due o tre punti di accesso in posizioni stimate.
- Sovrapposizioni impreviste di celle sono probabilmente dovute a variazioni a percorsi multipli. La qualità del segnale varia più della forza del segnale. I client potrebbero associarsi e operare meglio con i punti di accesso più lontani rispetto ai punti di accesso vicini.
- Durante un sondaggio, i punti di accesso e le antenne in genere non sono collegati da un cavo dell'antenna. In un ambiente di produzione, tuttavia, il punto di accesso e l'antenna potrebbero richiedere cavi per l'antenna. Tutti i cavi dell'antenna introducono la perdita di segnale. Il sondaggio più accurato include il tipo di antenna da installare e la lunghezza del cavo da installare. Un buon strumento da usare per simulare il cavo e la sua perdita è un attenuatore in un kit di indagine.

L'osservazione di uno stabilimento di produzione è simile all'osservazione di un magazzino, con la

differenza che potrebbero esserci molte più fonti di interferenze RF in uno stabilimento di produzione. Inoltre, le applicazioni in una struttura di produzione richiedono in genere una larghezza di banda maggiore rispetto a quelle di un magazzino. Queste applicazioni possono includere immagini video e voce wireless. La distorsione a percorsi multipli è probabilmente il problema di prestazioni più grave in un impianto di produzione.

Meccanismi di sicurezza supportati

Oltre ai messaggi statici WEP e Cisco LEAP per l'autenticazione e la crittografia dei dati, i badge vocera supportano anche WPA-PEAP (MS-CHAP v2)/WPA2-PSK.

Considerazioni su LEAP

LEAP consente l'autenticazione reciproca dei dispositivi (badge-to-access point e access point-to-badge) in base a nome utente e password. Dopo l'autenticazione, viene utilizzata una chiave dinamica tra il telefono e il punto di accesso per crittografare il traffico. Tuttavia, l'attacco del dizionario ASLEAP deve essere preso in considerazione quando si decide di utilizzare LEAP come soluzione di sicurezza:

per ulteriori informazioni, fare riferimento a Attacco del dizionario sulla vulnerabilità Cisco LEAP.

Se si utilizza LEAP, è necessario un server RADIUS compatibile con LEAP, ad esempio Cisco Access Control Server (ACS), per consentire l'accesso al database utenti. Cisco ACS può archiviare il database dei nomi utente e delle password localmente oppure accedere a tali informazioni da una directory esterna di Microsoft Windows NT. Quando si utilizza LEAP, assicurarsi che su tutti i dispositivi wireless vengano utilizzate password complesse. Le password complesse sono definite come lunghe da 10 a 12 caratteri e possono includere sia caratteri maiuscoli che minuscoli, nonché caratteri speciali.

Poiché tutti i badge utilizzano la stessa password e sono memorizzati all'interno del badge, Cisco consiglia di utilizzare nomi utente e password diversi sui client dati e sui client voce wireless. Questa procedura consente di tenere traccia dei problemi, di risolverli e di proteggerli. Benché sia un'opzione di configurazione valida l'utilizzo di un database esterno (esterno ad ACS) per memorizzare i nomi utente e le password per i badge, Cisco sconsiglia questa pratica. Poiché è necessario eseguire una query sull'ACS ogni volta che il badge si sposta tra i punti di accesso, l'imprevedibile ritardo nell'accesso a un database esterno all'ACS potrebbe causare un ritardo eccessivo e una scarsa qualità della voce.

Infrastruttura di rete wireless

La rete di telefonia IP wireless, come una rete di telefonia IP cablata, richiede un'attenta pianificazione per la configurazione della VLAN, il dimensionamento della rete, il trasporto multicast e la scelta delle apparecchiature. Per le reti di telefonia IP cablate e wireless, il modo più efficace per assicurare una larghezza di banda sufficiente e una risoluzione dei problemi più semplice è utilizzare VLAN voce e dati separate.

VLAN voce, dati e video

Le VLAN forniscono un meccanismo per segmentare le reti in uno o più domini di broadcast. Le VLAN sono particolarmente importanti per le reti di telefonia IP, in cui in genere si consiglia di

separare il traffico voce e dati in diversi domini di layer 2. Cisco consiglia di configurare VLAN separate per i badge vocali da altre fonti di traffico dati e voce: una VLAN nativa per il traffico di gestione dei punti di accesso, una VLAN dati per il traffico dati, una VLAN vocale o ausiliaria per il traffico voce e una VLAN per i badge vocali. Una VLAN vocale separata consente alla rete di trarre vantaggio dal contrassegno di layer 2 e fornisce l'accodamento delle priorità alla porta dello switch di accesso di layer 2. Ciò garantisce che sia fornita la QoS appropriata per diverse classi di traffico e aiuta a risolvere problemi quali l'indirizzamento IP, la sicurezza e la dimensionamento della rete. I Vocera Badge utilizzano una funzione di trasmissione che utilizza il multicast per la distribuzione. Questa VLAN comune garantisce che, quando un badge viene spostato tra i controller, rimanga parte del gruppo multicast. Quest'ultimo processo viene descritto in dettaglio quando si parla di multicast più avanti in questo documento.

Dimensionamento della rete

Il dimensionamento della rete di telefonia IP è essenziale per garantire che siano disponibili larghezza di banda e risorse adeguate per soddisfare le esigenze poste dalla presenza di traffico vocale. Oltre alle consuete linee guida di progettazione della telefonia IP per il dimensionamento di componenti quali porte gateway PSTN, transcoder, larghezza di banda WAN e così via, tenere in considerazione questi problemi 802.11b quando si ridimensiona la rete di telefonia IP wireless. I badge Vocera sono un'applicazione specializzata che allunga il numero di client cablati oltre i nostri tipici consigli di installazione.

Numero di dispositivi 802.11b per punto di accesso

Cisco consiglia di non avere più di 15-25 dispositivi 802.11b per punto di accesso.

Numero di chiamate attive per punto di accesso

Vocera utilizza due codec diversi a seconda che si tratti di una chiamata badge-to-badge (codec proprietario a bassa velocità di bit) o di una chiamata badge-to-phone (codec G.711). Questa tabella mostra una percentuale della larghezza di banda disponibile per velocità dati e fornisce un'immagine più chiara del throughput previsto:

Processo di chiamata	1 Mbps	2 Mbps	5.5 Mbps	11 Mbps
Badge-to-Phone (G.711)	20.7%	11.8%	6.3%	4.7%
Badge-to-Badge (codec proprietario a bassa velocità)	9.4%	6.1%	4.2%	3.6%

Consigli per lo switch

Nota: se si usa uno switch Cisco Catalyst serie 4000 come router principale nella rete, verificare che contenga almeno un modulo Supervisor Engine 2+ (SUP2+) o Supervisor Engine 3 (SUP3). Il modulo SUP1 o SUP2 può causare ritardi nel roaming, come accade con gli switch Cisco Catalyst 2948G, 2980G, 2980G-A, 4912 e 2948G-GE-TX.

Èpossibile creare un modello di porta dello switch da utilizzare quando si configura una porta dello switch per la connessione a un punto di accesso. Questo modello dovrebbe aggiungere tutte le funzioni di sicurezza e resilienza di base del modello di desktop standard. Inoltre, quando si

collega il punto di accesso a uno switch Cisco Catalyst 3750, è possibile ottimizzare le prestazioni del punto di accesso utilizzando i comandi QoS Multilayer Switching (MLS) per limitare la velocità della porta e mappare le impostazioni CoS (Class of Service) su DSCP (Differentiated Services Code Point).

Il traffico non richiesto dai client WLAN non deve essere inviato a un punto di accesso. Un modello deve essere progettato in modo da consentire la creazione di una connessione di rete sicura e resiliente con le seguenti caratteristiche:

- Restituzione delle configurazioni delle porte ai valori predefiniti: impedisce i conflitti di configurazione cancellando le configurazioni delle porte preesistenti.
- Disable Dynamic Trunking Protocol (DTP): disabilita il trunking dinamico, non necessario per la connessione a un punto di accesso.
- Disable Port Aggregation Protocol (PagP): il protocollo PagP è abilitato per impostazione predefinita ma non è necessario per le porte destinate all'utente.
- Abilita velocità porta: consente a uno switch di riprendere rapidamente il traffico di inoltro se uno spanning tree link non è attivo.
- Configura VLAN wireless: crea una VLAN wireless unica che isola il traffico wireless da altre VLAN di dati, voce e gestione. Ciò isola il traffico e garantisce un maggiore controllo.
- abilitare Quality of Service (QoS); porta non attendibile (contrassegnata da 0): garantisce il trattamento appropriato del traffico ad alta priorità, inclusi i softphone, e impedisce agli utenti di utilizzare una larghezza di banda eccessiva riconfigurando i PC.

Gli interruttori di alimentazione in linea WS-C3750-48PS-S possono essere utilizzati per fornire alimentazione ai punti di accesso in grado di ricevere alimentazione in linea.

Catalyst 6500 consente di inoltrare pacchetti alla velocità della linea con tutte le funzionalità descritte qui e di integrare numerosi moduli di servizio. Il modulo WiSM (Wireless Service Module) consente di avere due controller ciascuno con la capacità di controllare 150 punti di accesso ciascuno. Con un massimo di cinque WiSM per chassis, è possibile controllare oltre 1500 punti di accesso che supportano 50.000 client all'interno di un'unica architettura di switching ad alte prestazioni.

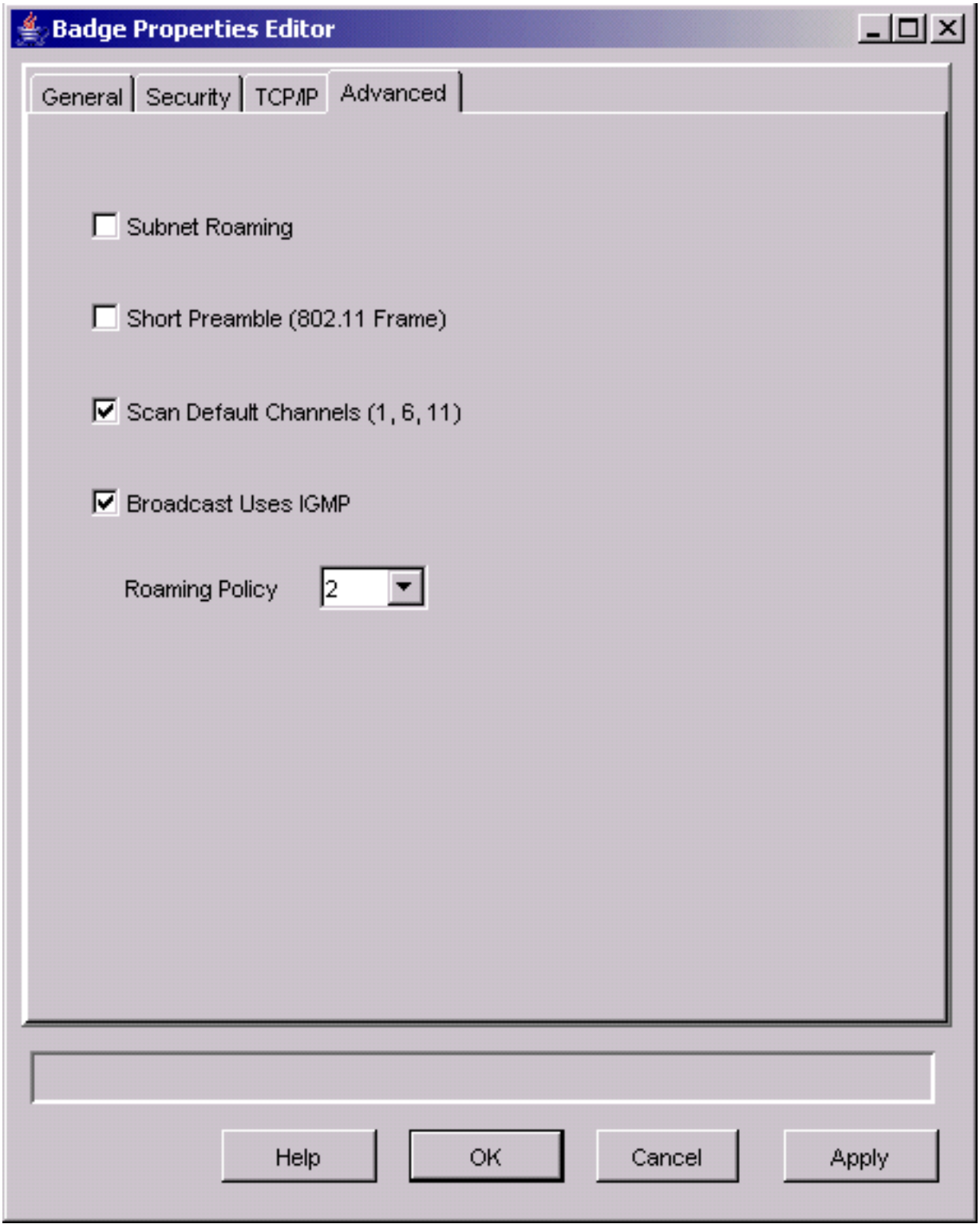
Distribuzioni e configurazione

Configurazione badge

L'utility di configurazione dei badge di Vocera (BCU) e la configurazione del badge possono introdurre roaming e latenza nell'ambiente se non vengono eseguiti correttamente. Utilizzando la BCU e l'Editor proprietà badge (BPE), verificare queste impostazioni (vedere la Figura 8):

- **Roaming subnet** disabilitato.
- **Canali predefiniti di scansione (1,6,11)** è selezionato.
- **La trasmissione utilizza IGMP** è abilitata.
- Il criterio di roaming è impostato su **2** o su un valore superiore.

Figura 8 - Scheda Vocera BCU Advanced



Quando l'opzione **Roaming subnet** è selezionata, indica al badge di richiedere un nuovo indirizzo IP dopo ogni roaming. Nell'ambiente LWAPP, l'infrastruttura aiuta a mantenere la connettività client al layer 3. Quando un client vocale deve attendere la risposta del server DHCP prima di poter inviare o ricevere pacchetti, vengono introdotti ritardo e jitter. Se l'opzione **Digitalizza canali predefiniti (1,6,11)** non è selezionata, il badge esegue la scansione di tutti i canali 802.11b quando il badge cerca di spostarsi. Ciò impedisce l'inoltro di pacchetti e il roaming ininterrotto.

Sintonizzare AutoRF per l'ambiente

Come descritto nella sezione Suggerimenti di questo documento, è importante tenere presente che ogni sito ha le proprie caratteristiche RF. Potrebbe essere necessario sintonizzare AutoRF o

Radio Resource Management (RRM), tenendo presente che ogni sito è diverso e che AutoRF/RRM deve essere sintonizzato per l'ambiente in uso.

Prima di regolare AutoRF, fare riferimento a Gestione risorse radio in Reti wireless unificate per ulteriori informazioni.

RRM consente di regolare la potenza di trasmissione di ciascun punto di accesso, regolando la potenza di ogni punto di accesso in base all'ascolto del terzo vicino più forte. Questo valore può essere regolato solo dalla CLI usando il comando **config advanced 802.11b tx-power-thresh** come descritto in Impostazioni di assegnazione del livello di potenza Tx.

Prima di regolare AutoRF, visitare il sito di installazione utilizzando il badge Vocera come indossato dall'utente finale e utilizzare uno strumento di indagine del sito per acquisire una solida comprensione di come il badge gira e a quale potenza ogni punto di accesso è visto. Una volta completata questa operazione e determinato che è necessario regolare questo valore, iniziare con un valore di -71 dBm per l'algoritmo di controllo della potenza di trasmissione. Utilizzare questo parametro CLI:

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

Consentire alla rete di superare questa regolazione con un minimo di 30 minuti a un'ora prima di osservare eventuali cambiamenti. Una volta che la rete ha un tempo sufficiente, camminare il sito utilizzando lo stesso strumento di indagine e badge di nuovo. Osservare le stesse caratteristiche di roaming e la stessa potenza del punto di accesso. L'obiettivo è quello di tentare di far girare i badge nel punto di accesso successivo o prima di esso per ottenere il miglior rapporto segnale/rumore possibile.

- **Come è possibile stabilire se la potenza di trasmissione è troppo calda o troppo fredda?**Per stabilire se la soglia della potenza di trasmissione è troppo alta o troppo bassa è necessario comprendere l'ambiente. Se avete percorso l'intera area di distribuzione (dove prevedete che funzionino i badge Vocera), dovreste sapere dove si trovano i vostri access point e sperimentare il comportamento di roaming del badge.
- **Cosa fare se la potenza di trasmissione è troppo elevata?**Il Vocera Badge gira unicamente sulla forza del segnale piuttosto che sulla qualità del segnale. Se il badge Vocera non gira dopo aver superato diversi punti di accesso durante l'esercitazione di benvenuto o il tono di prova, il badge viene considerato appiccicoso. Se questo comportamento è indicativo dell'intera area di distribuzione del campus, la soglia della potenza di trasmissione è troppo elevata e deve essere annullata. Se solo una o due aree isolate mostrano questo comportamento e il resto dell'area di distribuzione mostra caratteristiche di roaming più idealistiche, ciò non indica che la rete è troppo calda.
- **Cosa fare se la potenza di trasmissione è troppo fredda?**La soglia di trasmissione predefinita non fornisce quasi mai un'area di distribuzione in cui la rete è troppo fredda. Se la soglia della potenza di trasmissione viene abbassata e camminare nelle sale con il Vocera Badge fornisce un ambiente in cui il badge gira bene, ma perde la connettività e/o la copertura inattiva/sporca, allora la rete potrebbe essere stata sintonizzata troppo bassa. Se questa non è una caratteristica dell'intera rete, ma è isolata in una o due aree, allora è più indicativo di un buco di copertura piuttosto che di un problema a livello di rete.
- **Comportamento isolato**Se si riscontra che in una o due aree, il badge si attiene a un punto di accesso piuttosto che al roaming in modo idealistico, esaminare questa area.In che modo questa zona è diversa dal resto del campus?Se queste aree sono vicine a uscite di edifici o

aree in costruzione, la copertura per il rilevamento dei fori potrebbe costringere questi punti di accesso ad aumentare la potenza?Esaminare il file di log WLC e gli elenchi dei punti di accesso adiacenti per determinare il motivo per cui potrebbe verificarsi una tale anomalia.Se si scopre che in una o più aree isolate, il badge sperimenta la copertura morta o sporca, allora è necessario esaminare queste aree separatamente.Questa zona è vicina ad un ascensore, alla radiologia o ad una sala pausa?Queste aree potrebbero essere più adatte con l'installazione o una migliore collocazione di un punto di accesso per consentire una migliore copertura vocale.In entrambi i casi, è sempre consigliabile capire che si sta lavorando in uno spettro radio senza licenza e un comportamento idealistico potrebbe non essere mai raggiungibile. Questo può accadere quando si è situati vicino a una torre di trasmissione radio o un dispositivo, un trasmettitore televisivo o forse un non-802.11 2,4 GHz di riparazione (telefoni wireless, e così via).

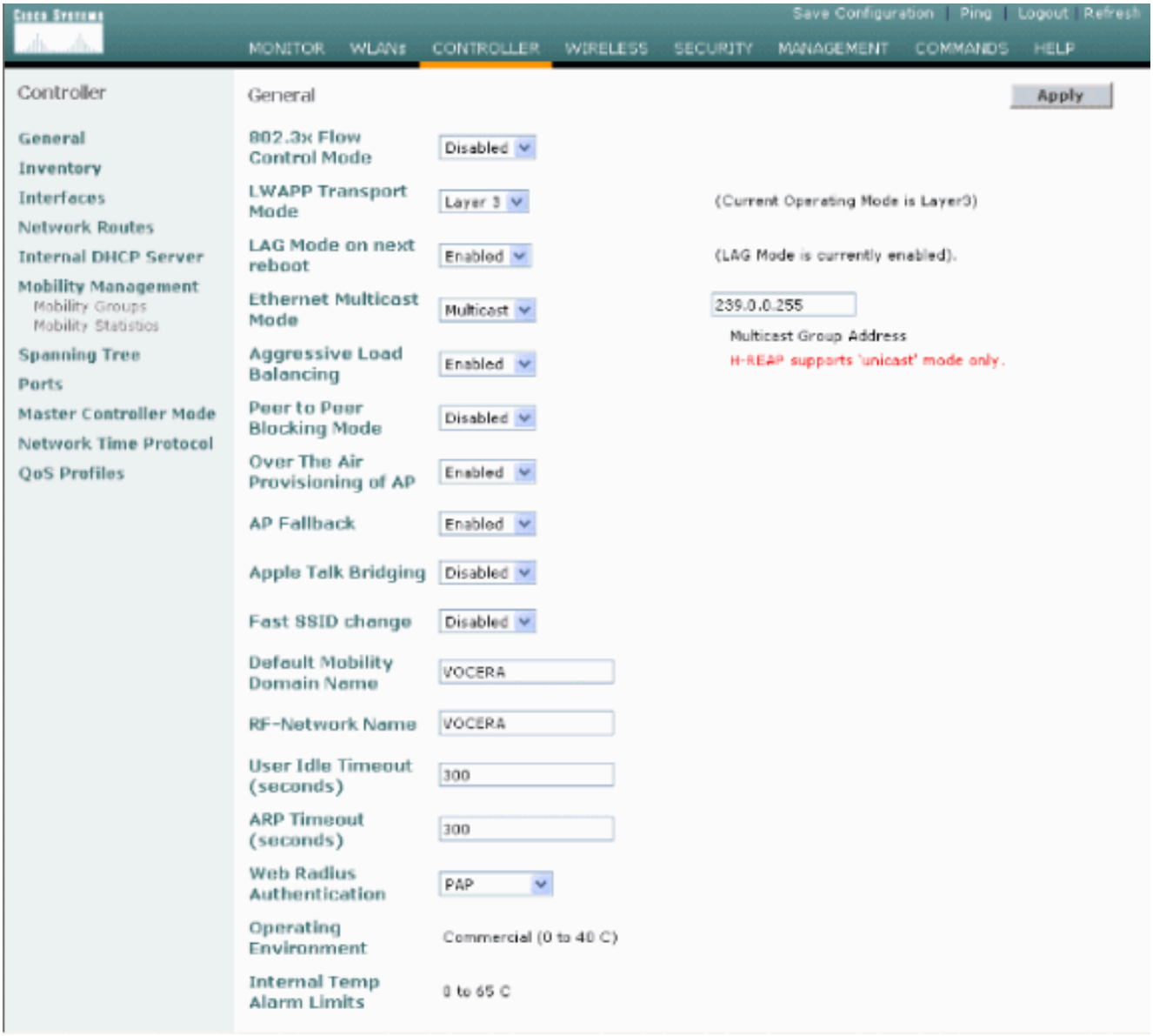
Configurazione dell'infrastruttura di rete wireless

Per la configurazione generale dei WLC, è necessario seguire la guida alla progettazione e all'installazione di Cisco Unified Wireless Network. In questa sezione vengono forniti ulteriori suggerimenti specifici per i badge di comunicazione Vocera®.

Nota: le modifiche non vengono salvate se non si preme il pulsante **Applica** prima di passare al passo successivo.

Completare questi passaggi nel menu di primo livello **Controller**:

1. Impostare la modalità multicast Ethernet su **Multicast**.
2. Impostare l'indirizzo del gruppo multicast su **239.0.0.255** (o su un altro indirizzo di gruppo multicast inutilizzato).
3. Impostare il nome del dominio di mobilità predefinito e il nome della rete RF sul progetto di rete.
4. Disabilitare Il **Load Balancing Aggressivo**.**Figura 9 - Configurazione generale WLC**

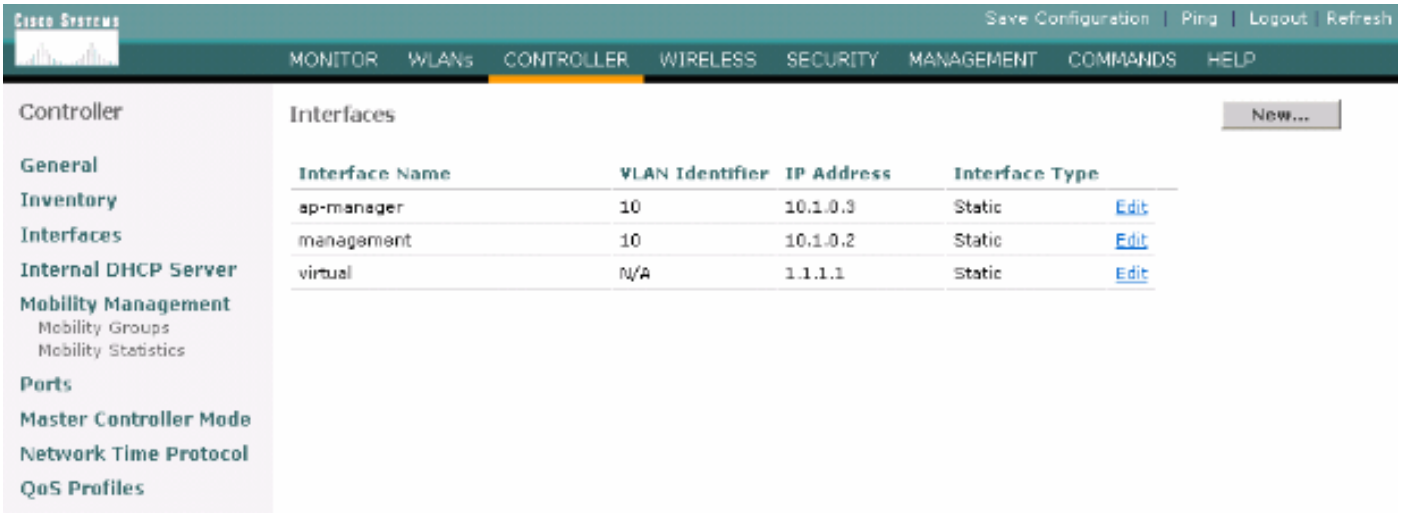


Crea interfacce

Fare clic su **Controller > Interfacce**.

Nota: l'indirizzo IP e la VLAN sono diversi. Le schermate che seguono forniscono esempi di indirizzamento che non devono essere seguiti direttamente.

Figura 10 - Elenco delle interfacce WLC



Creazione dell'interfaccia vocale Vocera

Attenersi alla seguente procedura:

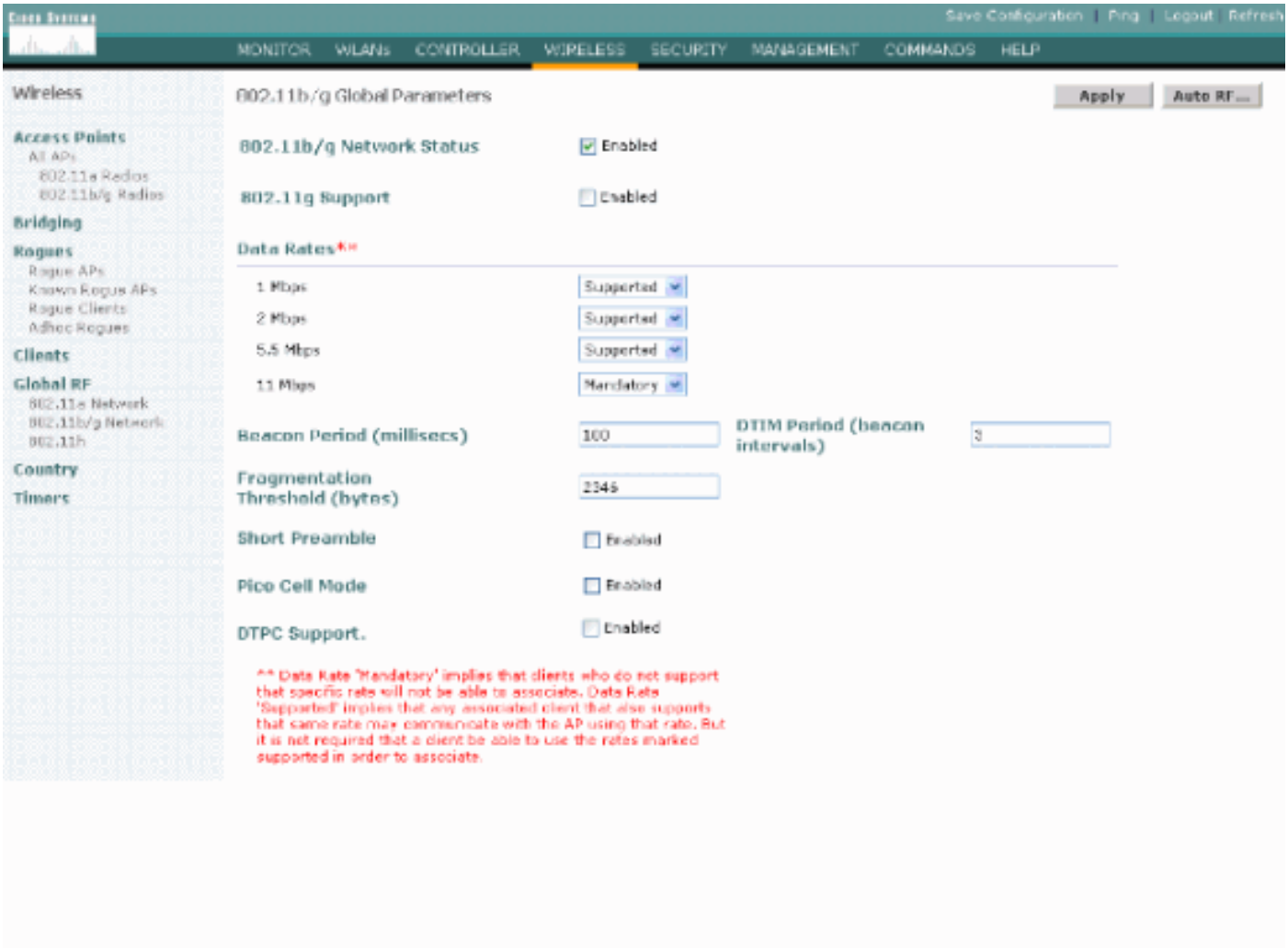
1. Fare clic su **New**.
2. Nel campo Interface Name (Nome interfaccia), immettere un tag rappresentativo della rete VoWLAN Vocera in uso.
3. Immettere il numero VLAN della rete VoWLAN nel campo VLAN ID.
4. Per modificare l'interfaccia appena creata, fare clic su **Apply** (Applica), quindi su **Edit** (Modifica).
5. Immettere l'indirizzo IP dell'interfaccia compresa nell'intervallo della VLAN e altre informazioni correlate.
6. Fare clic su **Apply** (Applica).

Configurazione specifica per la rete wireless

Per una WLAN con solo badge Vocera, questa configurazione fornisce impostazioni di esempio che supportano al meglio l'applicazione Vocera Broadcast.

- Il periodo DTIM è **1**.
- Il supporto per 802.11g è disabilitato. Solo la velocità dati 802.11b di **11 Mbps** è **obbligatoria**.
- Preambolo breve disabilitato.
- DTPC disabilitato.

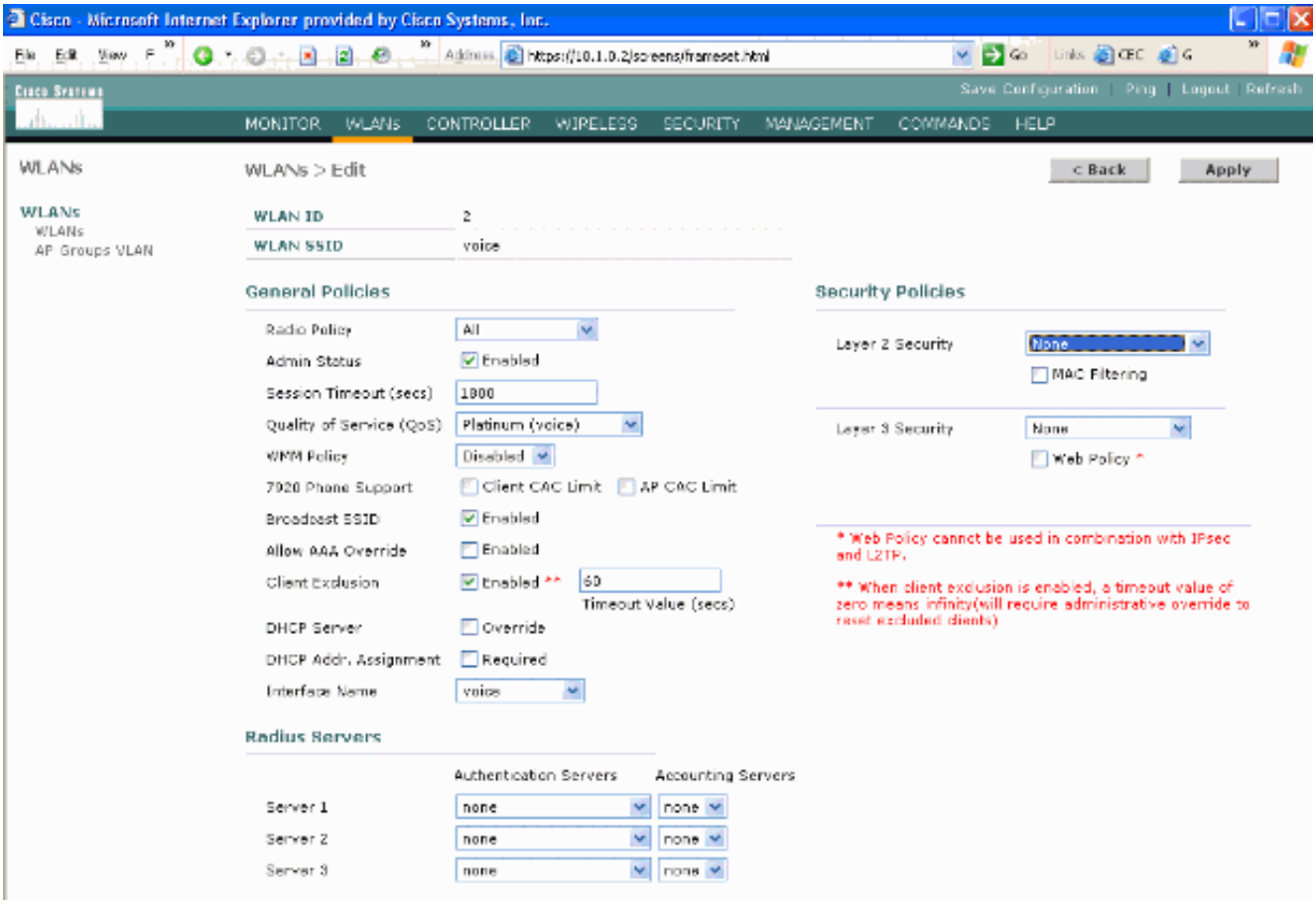
Figura 11 - Configurazione 802.11b/g



Configurazione della WLAN

Attenersi alla seguente procedura:

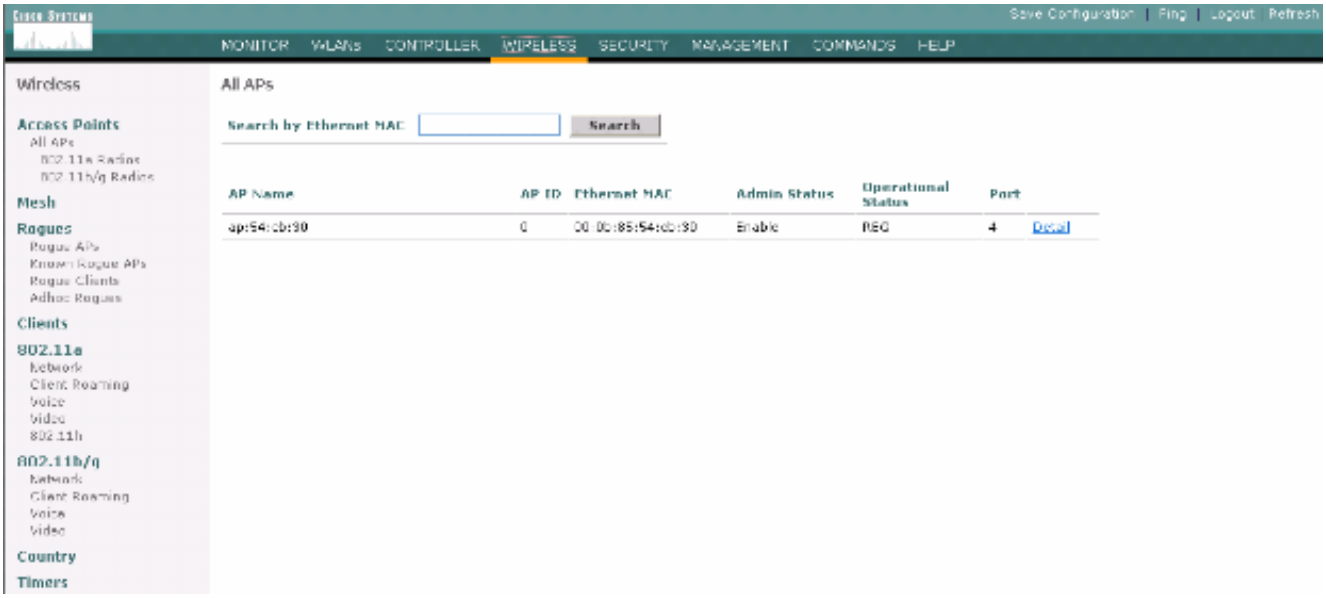
1. Aggiornare il campo Criteri radio in base al valore più adatto alle proprie esigenze.
2. Cambiare lo stato di amministrazione in **Abilitato**.
3. Impostare Session Timeout su **1800**.
4. Impostare Quality of Service su **Platinum**.
5. Impostare Broadcast SSID su **Enabled**.
6. Impostare il nome dell'interfaccia sull'interfaccia creata per i badge di comunicazione Vocera.
7. Impostare le opzioni di protezione in base ai criteri aziendali.**Figura 12 - Configurazione WLAN**



Configura dettagli Access Point

Attenersi alla seguente procedura:

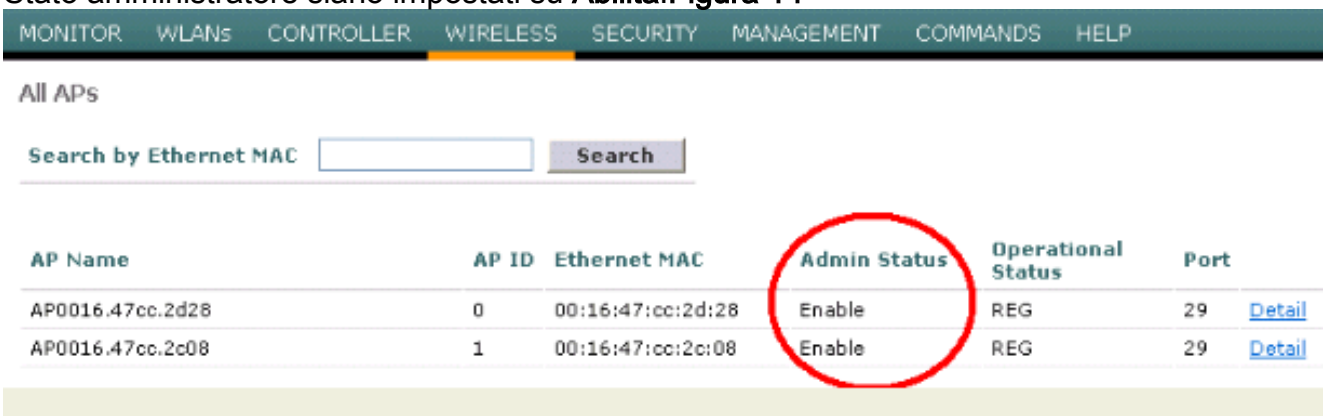
1. Fare clic su **Dettagli**.
2. Configurare il nome dell'access point.
3. Verificare che il punto di accesso sia configurato per DHCP.
4. Verificare che lo stato Amministratore sia **Abilitato**.
5. AP Mod" deve essere impostato su **local**.
6. Immettere la posizione del punto di accesso.
7. Immettere il nome del controller a cui appartiene il punto di accesso. Il nome del controller è disponibile nella pagina Monitor.
8. Fare clic su **Apply** (Applica).**Figura 13 - Dettagli punto di accesso**



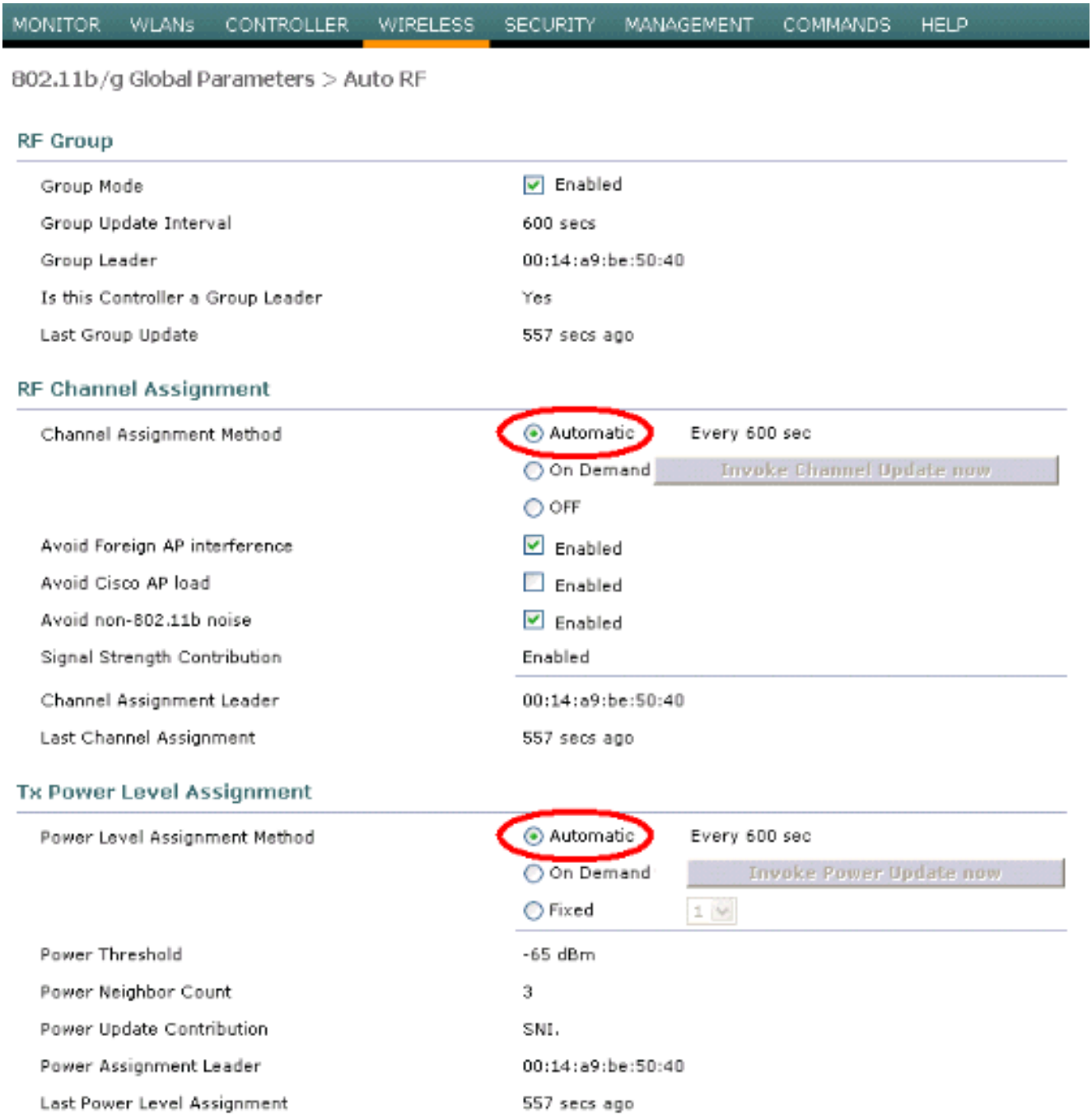
Configurazione della radio 802.11b/g

Attenersi alla seguente procedura:

1. Fare clic su **Wireless** nella parte superiore del WLC e verificare che tutti i punti di accesso in Stato amministratore siano impostati su **Abilita**.**Figura 14**



2. Fare clic su **Network** (vicino a 802.11b/g).
3. Fare clic su **AutoRF**.
4. Utilizzare AutoRF per creare una copertura completa con un canale RF non sovrapposto e una potenza di trasmissione. A tale scopo, selezionare **Automatico** sia per l'assegnazione del canale RF che per l'assegnazione del livello di potenza Tx.**Figura 15**



5. Fare clic su **Apply** (Applica).
6. Fare clic su **Salva configurazione** e vedere la sezione Sintonizzazione di AutoRF per l'ambiente in uso in questo documento.
7. Scegliete **Wireless > Access Point > Radio 802.11b/g**.**Figura 16**

Verifica telefonia IP wireless

Dopo aver condotto un'indagine sul sito RF e aver configurato i punti di accesso e i telefoni, è fondamentale eseguire dei test di verifica per verificare che tutto funzioni come desiderato. Le prove devono essere eseguite in tutti i seguenti punti:

- L'area primaria di ciascuna cella del punto di accesso (dove è più probabile che i badge si colleghino a quel particolare punto di accesso).
- Qualsiasi luogo in cui il volume delle chiamate potrebbe essere elevato.
- Luoghi in cui l'utilizzo potrebbe essere poco frequente ma la copertura deve ancora essere certificata (ad esempio, trombe delle scale, bagni e così via).
- A margine dell'area di copertura del punto di accesso.
- ·Questi test possono essere eseguiti in parallelo o in serie. Se eseguito in parallelo, verificare che i telefoni siano spenti tra i punti di test per verificare l'associazione completa, l'autenticazione e la registrazione in ogni posizione. I test di roaming e di carico devono essere i test finali.

Associazione, autenticazione e registrazione

Questa sezione spiega come verificare che il badge associ, autentichi e registri correttamente.

- In più punti dell'ambiente, accendere i badge e verificare l'associazione con il punto di accesso. Se il badge non è associato al punto di accesso, eseguire i seguenti controlli:Controllare la configurazione del badge per verificare che SSID, tipo di autenticazione e così via siano corretti.Controllare la configurazione WLC per verificare che SSID, tipo di autenticazione, canali radio e così via siano corretti.Controllare il sondaggio del sito per assicurarsi che la sede abbia una copertura RF adeguata.
- In più punti dell'ambiente, assicurarsi che il telefono esegua correttamente l'autenticazione tramite il punto di accesso. Se il client non esegue l'autenticazione, controllare la chiave WEP o il nome utente e la password LEAP sui badge. Verificare inoltre il nome utente e la password sul server AAA utilizzando un laptop wireless con credenziali identiche.
- In più punti dell'ambiente, assicurarsi che i badge vengano registrati con Vocera Communication Server. Se il client non si registra, eseguire i controlli seguenti:Verificare che l'indirizzo IP, la subnet mask, il gateway primario, il TFTP primario, il server primario/secondario e il server DNS siano corretti.
- Chiamate vocali fisse:In diversi punti dell'ambiente, mentre si è fermi, effettuare una chiamata a un altro badge ed effettuare test vocali da 60 a 120 secondi per verificare la qualità della voce. Se la qualità della voce non è accettabile, spostare un badge in una posizione migliore e provare di nuovo. La qualità della voce è accettabile? In caso contrario, verificare la copertura wireless.Se il server di telefonia è configurato, in più punti dell'ambiente, rimanere fermi ed effettuare una chiamata a un telefono cablato ed eseguire test vocali da 60 a 120 secondi per verificare la qualità della voce. Se la qualità della voce non è accettabile, chiedere se si effettua una chiamata utilizzando il telefono cablato. La qualità della voce è accettabile? In caso contrario, verificare la progettazione della rete cablata in base alle linee guida.
- Utilizzare gli strumenti di indagine del sito per verificare che non vi sia più di un punto di accesso per canale RF da quella posizione con un'intensità del segnale (indicatore RSSI (Received Signal Force Indicator) maggiore di 35. Se vi sono due punti di accesso presenti

sullo stesso canale, assicurarsi che il rapporto segnale/rumore (SNR) sia il più alto possibile per ridurre al minimo le interferenze. Ad esempio, se il punto di accesso più forte ha una RSSI di 35, idealmente il punto di accesso più debole dovrebbe avere una RSSI inferiore a 20. Per raggiungere questo obiettivo, potrebbe essere necessario ridurre la potenza di trasmissione di un punto di accesso o spostare il punto di accesso.
- Controllare le impostazioni QoS sul punto di accesso per confermare le impostazioni consigliate.
- Chiamate badge roaming:Se il server di telefonia non è disponibile, avviare l'Esercitazione su Vocera con il comando **Inizia l'Esercitazione**.OSe il server di telefonia è disponibile, avviare una chiamata sul badge con una periferica fissa.Controllare continuamente la qualità della voce mentre si attraversa l'area di copertura wireless totale. Se la qualità della voce è insufficiente, eseguire le seguenti attività:Ascolta tutte le modifiche inaccettabili nella qualità della voce e prendi nota dei valori relativi alla posizione e alla radio sul tuo notebook e dei valori CQ del badge.Guarda e ascolta il badge per spostarti al punto di accesso successivo.Prendere nota degli altri punti di accesso disponibili nell'indagine del sito per verificare copertura e interferenze.
- Apportare le modifiche necessarie al posizionamento e alle impostazioni del punto di accesso per ottimizzare la WLAN ed eseguire questi controlli per garantire la qualità della voce:Utilizzare gli strumenti di indagine del sito e verificare che non vi sia più di un punto di accesso per canale con un valore RSSI superiore a 35 in qualsiasi posizione. Idealmente, tutti gli altri punti di accesso sullo stesso canale dovrebbero avere valori RSSI il più bassi possibile (preferibilmente meno di 20). Al confine dell'area di copertura in cui l'RSSI è 35, l'RSSI per tutti gli altri punti di accesso sullo stesso canale dovrebbe idealmente essere inferiore a 20.Utilizzare gli strumenti di indagine del sito per verificare che vi siano almeno due punti di accesso (totale, su canali separati) visibili in tutte le posizioni con sufficiente intensità del segnale.Verificare che i punti di accesso in una determinata area di roaming si trovino tutti su una rete di layer 2.

Problemi comuni di roaming

Possono verificarsi i seguenti problemi di roaming:

- Il badge non si sposta quando è posizionato direttamente sotto il punto di accesso.
- Èmolto probabile che il badge non raggiunga le soglie differenziali di roaming per l'indicatore di potenza del segnale ricevuto (RSSI) e l'utilizzo del canale (CU). Regolare la soglia della potenza di trasmissione dal WLC.
- Il badge non riceve beacon o risposte di richiesta dal punto di accesso.
- Il distintivo gira troppo lentamente.

Il badge perde la connessione alla rete o al servizio vocale durante il roaming

- Controllare l'autenticazione per verificare una possibile mancata corrispondenza WEP.
- Il badge non invia join IGMP o la rete invia query IGMP durante un roaming. Di conseguenza, la funzione di trasmissione Vocera non funziona durante un roaming di layer 2/3.
- Il badge può essere utilizzato solo per il roaming di layer 2 (a meno che non sia configurato un meccanismo di mobilità di layer 3). Verificare che il nuovo WLC non stia servendo una subnet IP diversa.

- Verificare che il punto di accesso/controller associato disponga di connettività IP al server di comunicazione Vocera.
- Controllare la forza del segnale RF e i valori CQ del badge.

Il badge perde la qualità della voce durante il roaming

- Verificare la presenza di RSSI basso nel punto di accesso di destinazione.
- La sovrapposizione dei canali potrebbe essere insufficiente. Il badge deve avere il tempo di consegnare la chiamata senza problemi prima che perda il segnale con il punto di accesso originale.
- Il segnale proveniente dal punto di accesso originale potrebbe essere perso.

Problemi audio

Alcuni errori di configurazione comuni possono causare problemi audio facilmente risolvibili. Se possibile, controllare i problemi audio confrontandoli con un badge fisso (di riferimento) per limitare il problema a un problema wireless. I problemi audio più comuni includono:

- Audio unilaterale
- Audio discontinuo o robotico
- Problemi di registrazione e autenticazione

Audio unilaterale

- Questo problema può verificarsi nelle aree di margine di un punto di accesso, dove un segnale potrebbe essere troppo debole sul lato del badge o sul lato del punto di accesso. La corrispondenza delle impostazioni di alimentazione del punto di accesso al badge (20 mW), quando possibile, può risolvere il problema. Questo problema è più comune quando la variazione tra l'impostazione del punto di accesso e l'impostazione del badge è grande (ad esempio, 100 mW sul punto di accesso e 28 mW sul badge).
- Verificare la qualità della voce sul gateway e sul routing IP.
- Verificare se un firewall o un NAT è presente nel percorso dei pacchetti UDP proprietari. Per impostazione predefinita, i firewall e i NAT causano l'audio unidirezionale o l'assenza di audio. I Cisco IOS® e PIX NAT e i firewall hanno la capacità di modificare queste connessioni in modo che l'audio bidirezionale possa fluire.Se si utilizza la mobilità di layer 3, è possibile che la rete blocchi il traffico upstream con i controlli uRPF (Unicast Reverse Path Forwarding).
- L'audio unidirezionale può verificarsi se la memorizzazione nella cache ARP non è configurata sul WLC.

Audio discontinuo o robotico

- Un motivo comune per audio discontinuo o robotico è quando un microonde opera nelle vicinanze. Le microonde iniziano dal canale 9 e possono estendersi dai canali 6 a 14.
- Verificare la presenza di telefoni wireless da 2,4 GHz e altri dispositivi wireless per chiamate infermieristiche utilizzando strumenti come Cognio.

Problemi di registrazione e autenticazione

In caso di problemi di autenticazione, eseguire i controlli seguenti:

- Verificare che gli SSID corrispondano sul badge e sul punto di accesso (o rete). Verificare inoltre che la rete disponga di un percorso verso il server Vocera.
- Controllare le chiavi WEP per assicurarsi che corrispondano. È consigliabile reinserirli nell'utility di configurazione del badge (BCU) e riprogrammare il badge, in quanto è facile commettere un errore di digitazione quando si immette una chiave WEP o una password.

Possono verificarsi i seguenti messaggi o sintomi:

- Impossibile supportare tutte le funzionalità richieste. Probabilmente la crittografia del punto di accesso non corrisponde a quella del client.
- Autenticazione non riuscita/nessun access point trovato: verificare che i tipi di autenticazione corrispondano nel punto di accesso e nel client.
- No Service - Configurazione IP non riuscita. Se si utilizza un protocollo WEP statico, verificare che le chiavi siano configurate correttamente. Verificare che altri client possano ricevere DHCP utilizzando lo stesso SSID.
- Deautentica tutti i client TKIP dal punto di accesso: questo problema si verifica quando il punto di accesso rileva due errori MIC entro 60 secondi. Questa contromisura impedisce a tutti i client TKIP di eseguire nuovamente l'autenticazione per 60 secondi.
- Riautenticazione/Timeout sessione: se configurata, una sessione di timeout attiva una riautenticazione che causa interruzioni nel flusso vocale (300 ms + ritardo WAN per l'autenticazione 802.1x).

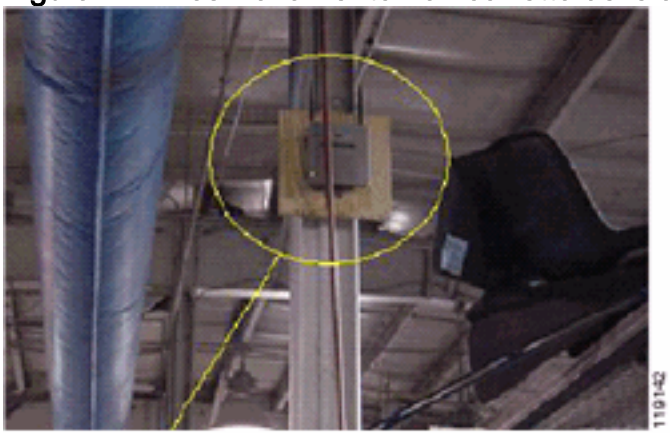
Appendice A

Posizionamento del punto di accesso e dell'antenna

In questa sezione vengono forniti esempi di posizionamento corretto e non corretto dei punti di accesso (AP) e delle antenne.

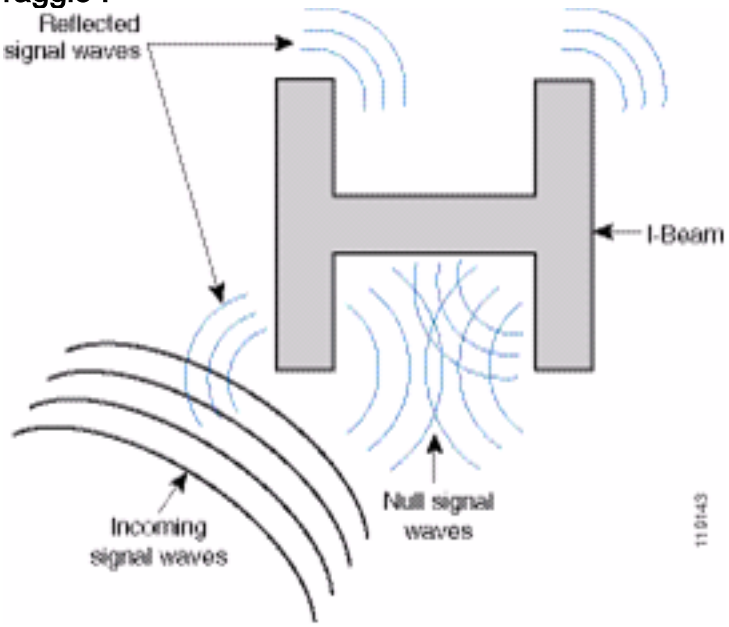
La Figura 17 mostra un posizionamento non corretto di un punto di accesso e di antenne vicino a un raggio I, che crea modelli di segnale distorti. Un punto nullo RF viene creato dall'incrocio delle onde di segnale e la distorsione multipath viene creata quando le onde di segnale vengono riflesse. Il posizionamento comporta una copertura molto ridotta dietro il punto di accesso e una qualità del segnale ridotta davanti al punto di accesso.

Figura 17 - Posizionamento non corretto delle antenne vicino a un raggio I



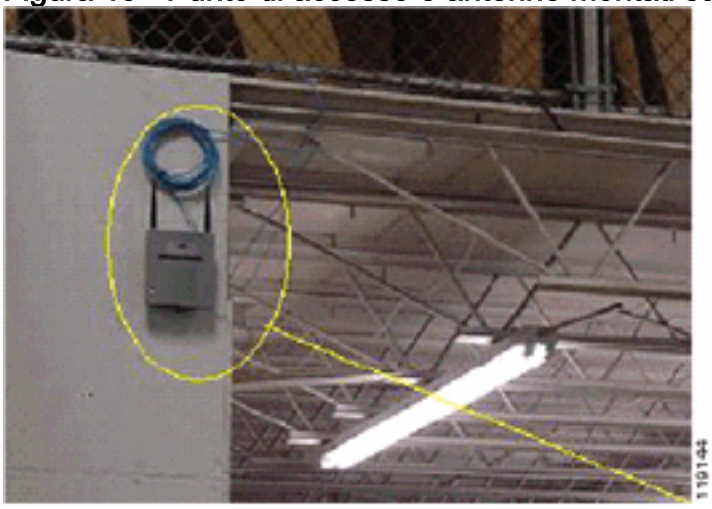
La Figura 18 mostra le variazioni o le distorsioni della propagazione del segnale causate da un fascio I. Il raggio I crea molti riflessi sia dai pacchetti ricevuti che da quelli trasmessi. I segnali riflessi determinano una qualità del segnale molto scadente a causa dei punti nulli e dell'interferenza a percorsi multipli. Tuttavia, la forza del segnale è alta perché le antenne del punto di accesso sono così vicine al raggio I.

Figura 18 - Distorsioni del segnale causate dal posizionamento delle antenne troppo vicino a un raggio I



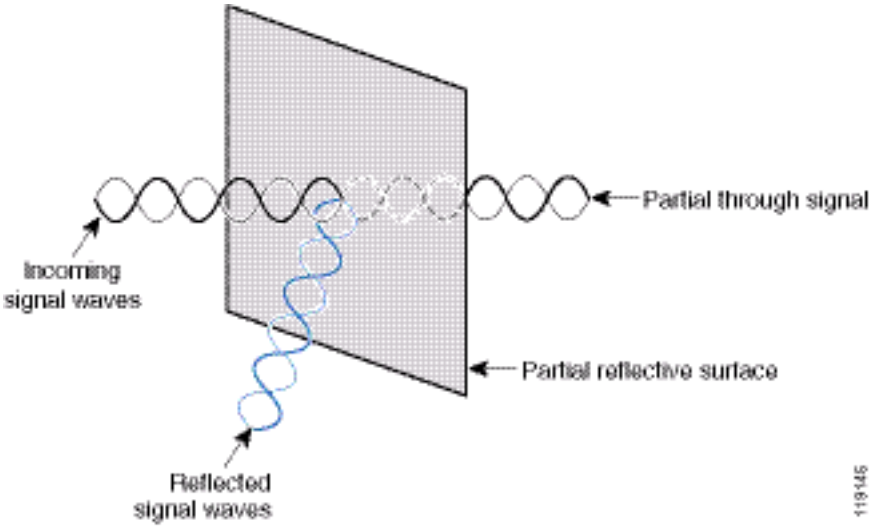
Il punto di accesso e il posizionamento dell'antenna nella Figura 19 sono migliori perché sono lontani dai raggi I e ci sono meno segnali riflessi, meno punti nulli e meno interferenze a percorsi multipli. Questo posizionamento non è ancora perfetto perché il cavo Ethernet non deve essere avvitato così vicino all'antenna. Inoltre, il punto di accesso può essere ruotato con le antenne da 2,4 GHz rivolte verso il pavimento. In questo modo è possibile ottenere una migliore copertura direttamente sotto il punto di accesso. Nessun utente al di sopra del punto di accesso.

Figura 19 - Punto di accesso e antenne montati su una parete, lontano dai raggi I



La Figura 20 mostra la propagazione del segnale causata dalla parete su cui è montato il punto di accesso.

Figura 20 - Riflessione del segnale causata da una parete

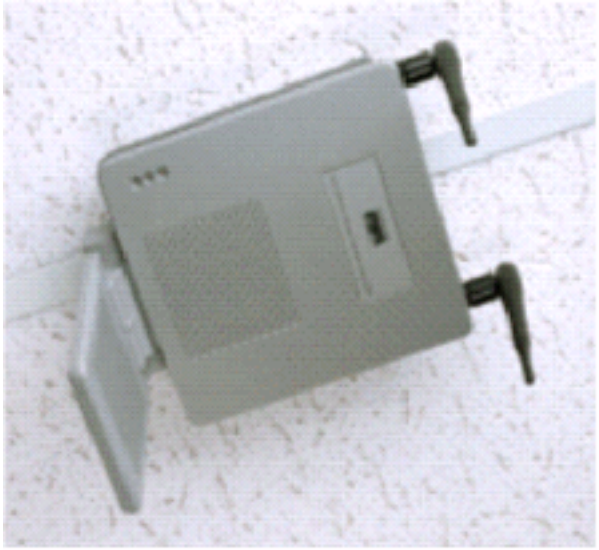


Gli esempi precedenti si applicano anche quando si posizionano punti di accesso e antenne all'interno o vicino al soffitto in un ambiente aziendale standard. Se vi sono condotte d'aria metalliche, alberi di elevazione o altre barriere fisiche che possono causare riflessione del segnale o interferenze a percorsi multipli, Cisco consiglia vivamente di spostare le antenne al di fuori di queste barriere. Nel caso dell'ascensore, spostare l'antenna di qualche metro di distanza per eliminare il riflesso del segnale e la distorsione. Lo stesso vale per le condotte d'aria nel soffitto.

Un'indagine condotta senza inviare e ricevere pacchetti non è sufficiente. L'esempio del cursore a I mostra la creazione di punti nulli che possono derivare da pacchetti con errori CRC. I pacchetti voce con errori CRC sono pacchetti mancanti che influiscono negativamente sulla qualità della voce. In questo esempio, questi pacchetti potrebbero essere al di sopra del livello minimo di rumore misurato da uno strumento di rilevamento. Pertanto, è molto importante che l'indagine del sito non solo misuri i livelli del segnale, ma generi anche pacchetti e poi segnali gli errori dei pacchetti.

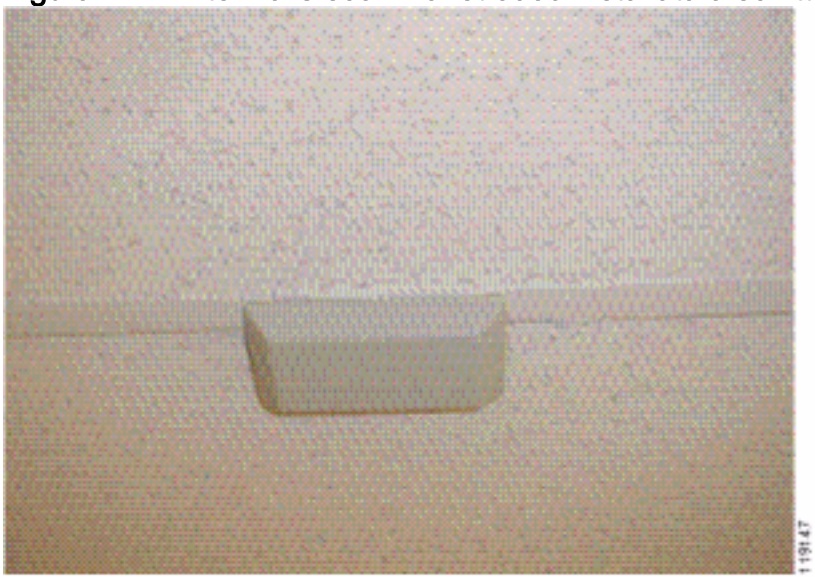
La Figura 21 mostra un Cisco AP1200 montato correttamente su una barra a T a soffitto, con le antenne in posizione omnidirezionale.

Figura 21 - Cisco AP1200 installato a soffitto



La Figura 22 mostra un'antenna di diversità omnidirezionale Cisco Aironet 5959 montata correttamente su una barra a T a soffitto. In questo caso, il Cisco AP1200 è montato al di sopra del soffitto.

Figura 22 - Antenna Cisco Aironet 5959 installata a soffitto

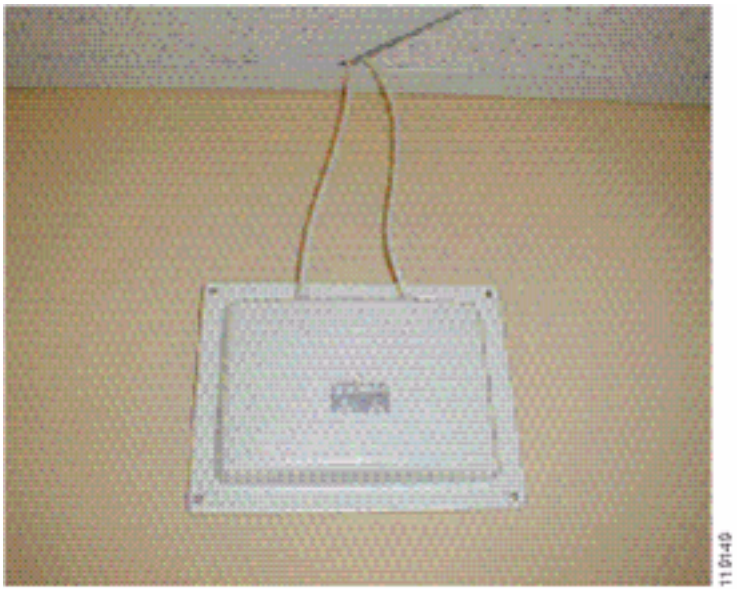


La Figura 23 mostra un Cisco AP1200 montato correttamente su una parete.

Figura 23 - Cisco AP1200 installato su una parete

La Figura 24 mostra l'antenna patch di diversità Cisco Aironet 2012 montata su una parete. In questo caso, il Cisco AP1200 è montato al di sopra del soffitto.

Figura 24 - Antenna Cisco Aironet 2012 montata su una parete



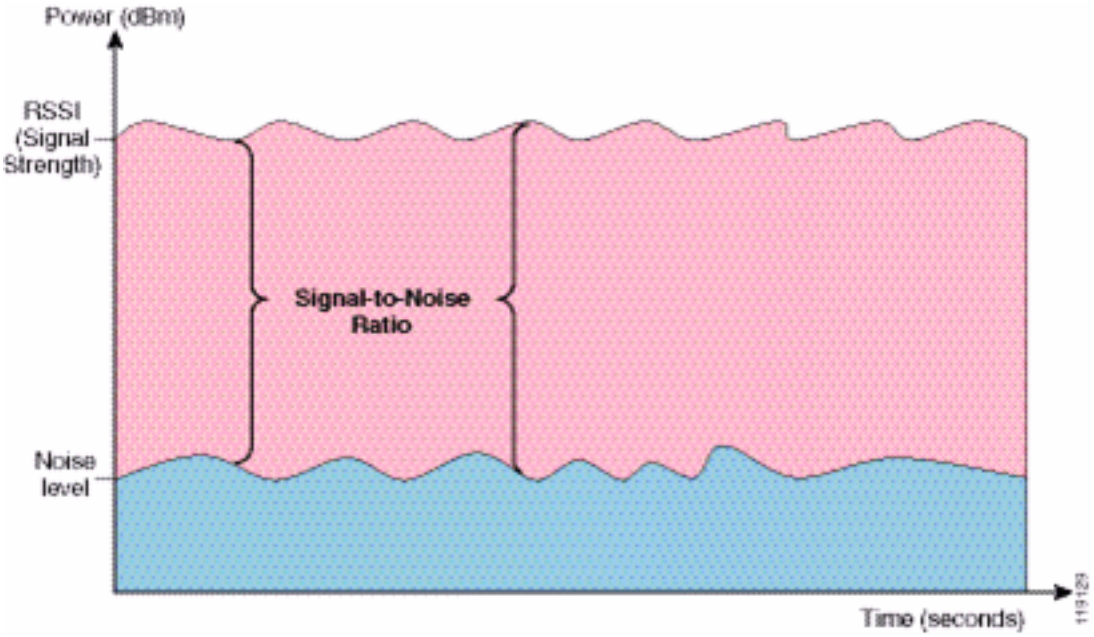
Per le aree in cui il traffico degli utenti è elevato (come uffici, scuole, negozi e ospedali), Cisco consiglia di posizionare il punto di accesso in modo che non sia visibile e di posizionare antenne discrete al di sotto del soffitto. La separazione per le antenne non-diversity non deve superare i 18 pollici.

Interferenza e distorsione a percorsi multipli

Le prestazioni di velocità effettiva della rete WLAN sono influenzate da segnali inutilizzabili. Le interferenze WLAN possono essere generate da forni a microonde, telefoni senza fili da 2,4 GHz, dispositivi Bluetooth o altre apparecchiature elettroniche che operano nella banda da 2,4 GHz. Le interferenze provengono in genere anche da altri punti di accesso e dispositivi client che appartengono alla WLAN ma sono sufficientemente lontani da indebolire il segnale o danneggiarlo. Anche i punti di accesso che non fanno parte dell'infrastruttura di rete possono causare interferenze WLAN e sono identificati come punti di accesso non autorizzati.

Le interferenze e la distorsione multipath causano la fluttuazione del segnale trasmesso. L'interferenza riduce il rapporto segnale/rumore (SNR) per una particolare velocità dati. Il numero di tentativi di pacchetto aumenta in un'area in cui l'interferenza e/o la distorsione a percorsi multipli sono elevate. L'interferenza viene anche definita livello di rumore o soglia di rumore. La potenza del segnale ricevuto dal punto di accesso associato deve essere sufficientemente elevata al di sopra del livello di rumore del ricevitore per essere decodificata correttamente. Questo livello di forza è noto come rapporto segnale-rumore, o SNR. L'SNR ideale per il Vocera Badge è 25 dB. Ad esempio, se la soglia del rumore è di 95 decibel per milliwatt (dBm) e il segnale ricevuto al telefono è di 70 dBm, il rapporto segnale/rumore è di 25 dB. (vedere Figura 25).

Figura 25 - Rapporto segnale/rumore (SNR)



Se si modificano il tipo e la posizione dell'antenna, è possibile ridurre la distorsione e l'interferenza a percorsi multipli. Il guadagno dell'antenna aumenta il guadagno del sistema e può ridurre le interferenze se il trasmettitore che interferisce non si trova direttamente davanti all'antenna direzionale.

Mentre le antenne direzionali possono essere molto utili per alcune applicazioni in interni, la maggior parte delle installazioni in interni utilizza antenne omnidirezionali. La direzionalità deve essere rigorosamente determinata da una corretta e corretta indagine del sito. Sia che si utilizzi un'antenna omnidirezionale o patch, gli ambienti interni richiedono antenne diversity per ridurre la distorsione multipath. Le radio Access Point Cisco Aironet serie 1000 supportano la diversità.

Attenuazione del segnale

L'attenuazione o la perdita del segnale si verificano anche quando il segnale passa attraverso l'aria. La perdita di forza del segnale è più pronunciata quando il segnale passa attraverso diversi oggetti. Una potenza di trasmissione di 20 mW equivale a 13 dBm. Pertanto, se la potenza trasmessa al punto di ingresso di una parete di cartongesso è a 13 dBm, la forza del segnale è ridotta a 10 dBm quando si esce da tale parete. Questa tabella mostra la probabile perdita di potenza del segnale causata da vari tipi di oggetti.

Attenuazione del segnale causata da vari tipi di oggetti

Oggetto nel percorso del segnale	Attenuazione del segnale attraverso l'oggetto
Parete in cartongesso	3 dB
Parete in vetro con struttura in metallo	6 dB
Muro a blocchi	4 dB
Finestra di Office	3 dB
Porta in metallo	6 dB
Porta in metallo nel muro di mattoni	12 dB
Corpo umano	3 dB

Ogni sito oggetto del sondaggio presenta diversi livelli di distorsione multipath, perdite di segnale e disturbi del segnale. Gli ospedali sono generalmente gli ambienti più difficili da sorvegliare a causa dell'elevata distorsione multipath, delle perdite di segnale e del rumore del segnale. Gli ospedali richiedono tempi di indagine più lunghi, una popolazione di punti di accesso più densa e prestazioni più elevate. Produzione e officina sono i prossimi più difficili da rilevare. Questi siti generalmente hanno dei lati metallici e molti oggetti metallici sul pavimento, il che produce segnali riflessi che ricreano la distorsione multipath. Gli edifici adibiti a uffici e le strutture ricettive generalmente hanno un'elevata attenuazione del segnale ma un minore grado di distorsione multipath.

Informazioni correlate

- Implementazione dei Cisco Wireless LAN Controller serie 440X
- Riferimento per la soluzione Progettazione della rete
- Specifiche del sistema di comunicazione Vocera
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).