Guida alla progettazione CX - Wireless per reti pubbliche di grandi dimensioni

Sommario

Introduzione

Questo documento descrive le linee guida di progettazione e configurazione per reti Wi-Fi pubbliche di grandi dimensioni.

Guida alla progettazione di CX

Le guide alla progettazione di sistemi CX sono redatte da specialisti dei centri Cisco TAC (Technical Assistance Center) e PS (Cisco Professional Services) e sono soggette alla revisione paritetica da parte di esperti di Cisco; le guide si basano sulle best practice di Cisco, nonché sulle conoscenze e sull'esperienza acquisite con innumerevoli implementazioni di clienti nel corso di molti anni. Le reti progettate e configurate in linea con i suggerimenti riportati in questo documento consentono di evitare i problemi comuni e migliorare il funzionamento della rete.

Ambito di applicazione e definizioni

Questo documento fornisce linee guida per la progettazione e la configurazione di reti wireless pubbliche di grandi dimensioni.

Definizione: reti pubbliche di grandi dimensioni - installazioni wireless, spesso ad alta densità, che forniscono connettività di rete a migliaia di dispositivi client sconosciuti e/o non gestiti.

In questo documento si presume spesso che la rete di destinazione fornisca servizi per eventi di grandi dimensioni e/o temporanei. Si adatta anche a reti statiche permanenti per luoghi che ricevono molti ospiti. Ad esempio, un centro commerciale o un aeroporto hanno analogie con la rete Wi-Fi di uno stadio o di una sede per concerti - nel senso che non vi è alcun controllo sugli utenti finali, e che esistono nella rete in genere solo per un paio d'ore, o al massimo per il giorno.

La copertura wireless di grandi eventi o eventi ha una propria serie di requisiti, che tendono ad essere diversi dalle reti aziendali, manifatturiere o persino dalle grandi reti educative. Le grandi reti pubbliche possono avere migliaia di persone, concentrate solo in uno o pochi edifici. Possono avere un roaming client molto frequente, costantemente o durante picchi, inoltre la rete deve essere il più possibile compatibile con qualsiasi cosa in termini di dispositivi client wireless, senza alcun controllo sulla configurazione o sicurezza dei dispositivi client.

Questa guida illustra i concetti generali di RF per l'alta densità e i dettagli di implementazione. Molti dei concetti relativi alla radio illustrati in questa guida si applicano a tutte le reti ad alta densità, incluso Cisco Meraki. Tuttavia, i dettagli e le configurazioni dell'implementazione sono focalizzati su Catalyst Wireless che utilizza Catalyst 9800 Wireless Controller, in quanto si tratta della soluzione più comune implementata per le reti pubbliche di grandi dimensioni.

Nel documento vengono usati indifferentemente i termini Controller wireless e Controller LAN wireless (WLC).

Grandi reti pubbliche

Le grandi reti pubbliche e di eventi sono uniche sotto molti aspetti; questo documento esplora e fornisce indicazioni su queste aree chiave.

- Le grandi reti pubbliche sono intense; ci sono migliaia di dispositivi in uno spazio a radiofrequenza ridotta (RF) e un roaming significativo mentre le persone camminano, alcuni eventi ed eventi possono essere più statici con picchi di larghezza di banda in momenti molto specifici. L'infrastruttura deve gestire tutti questi cambiamenti di stato nel modo più agevole possibile per i client che entrano e si spostano nell'area.
- La priorità chiave è la facilità di caricamento. Un cliente associato è un cliente soddisfatto. Ciò significa che si desidera eseguire l'associazione client alla rete il più rapidamente possibile. Un client non connesso al Wi-Fi cerca i punti di accesso disponibili generando energia RF indesiderata, che si traduce in ulteriore congestione e perdita di capacità via etere.
- L'installazione della RF deve essere progettata nel modo più accurato possibile. Se è richiesta una densità molto elevata o se la sede dispone di ampi spazi aperti e/o soffitti elevati, è indispensabile un'adeguata progettazione RF che utilizzi antenne direzionali.
- Un'altra importante unità di progettazione è la compatibilità. Alcune funzionalità sono standard nella specifica 802.11 mentre altre sono proprietarie e non pongono alcun problema ai client. Tuttavia, la realtà è diversa e ci sono molti driver client programmati in modo errato che si comportano in modo errato quando vedono beacon complicati o caratteristiche/impostazioni che non capiscono.
- La risoluzione dei problemi è difficile a causa delle limitazioni di scala e di tempo. Se qualcosa non funziona con un client specifico, non è possibile lavorare con quell'utente finale

per comprendere il problema. Gli utenti possono essere difficili da trovare, ma anche non cooperativi, a causa della natura transitoria della loro visita nella sede.
- La sicurezza è un fattore importante. C'è meno controllo a causa dell'enorme quantità di visitatori e una superficie d'attacco molto più grande.

Riferimenti esterni

Nome documento	Origine	Posizione
Best practice per la configurazione di Cisco Catalyst serie 9800	Cisco	Collegamento
Risoluzione dei problemi relativi alla CPU del controller LAN wireless	Cisco	Collegamento
Convalida throughput Wi-Fi: Guida al test e al monitoraggio	Cisco	Collegamento
Guida all'implementazione di Cisco Catalyst CW9166D1 Access Point	Cisco	Collegamento
Guida all'installazione dell'antenna dello stadio Catalyst 9104 (C-ANT9104)	Cisco	Collegamento
Monitor Catalyst 9800 KPI (indicatori prestazioni chiave)	Cisco	Collegamento
Flusso della risoluzione dei problemi di connettività client di Catalyst 9800	Cisco	Collegamento
Guida alla configurazione del software Cisco Catalyst serie 9800 Wireless Controller (17.12)	Cisco	Collegamento
Wi-Fi 6E: il prossimo grande capitolo nel white paper Wi-Fi	Cisco	Collegamento

Esclusione di responsabilità

Questo documento offre suggerimenti basati su alcuni scenari, presupposti e conoscenze acquisite da numerose distribuzioni. Il lettore è tuttavia responsabile della progettazione della rete, delle attività aziendali, della conformità alle normative, della sicurezza, della privacy e di altri requisiti, inclusa la conformità alle linee guida o ai suggerimenti forniti in questa guida.

Progettazione della rete

Considerazioni su RF

Tipi di luogo

Questa guida è incentrata sulle reti guest di grandi dimensioni, generalmente aperte al pubblico, e con un controllo limitato sugli utenti finali e sui tipi di dispositivi client. Questi tipi di reti possono essere implementati in diverse posizioni e possono essere temporanee o permanenti. Il caso d'uso principale consiste generalmente nel fornire l'accesso a Internet ai visitatori, anche se raramente questo è l'unico caso d'uso.

Ubicazioni tipiche:

- Stadi e arene
- Sale conferenze
- Grandi auditorium

Da un punto di vista RF, ognuno di questi tipi di posizione presenta un proprio insieme di sfumature. La maggior parte di questi esempi sono generalmente installazioni permanenti, ad eccezione delle sale conferenze, che possono essere permanenti o allestite temporaneamente per una specifica fiera.

Altri percorsi:

- Nave da crociera
- Aeroporto
- Centro commerciale/centro commerciale

Anche gli aeroporti e le navi da crociera sono esempi di installazioni che rientrano nella categoria delle grandi reti pubbliche; tuttavia, queste hanno considerazioni aggiuntive specifiche per ciascun caso e spesso utilizzano punti di accesso omnidirezionali interni.

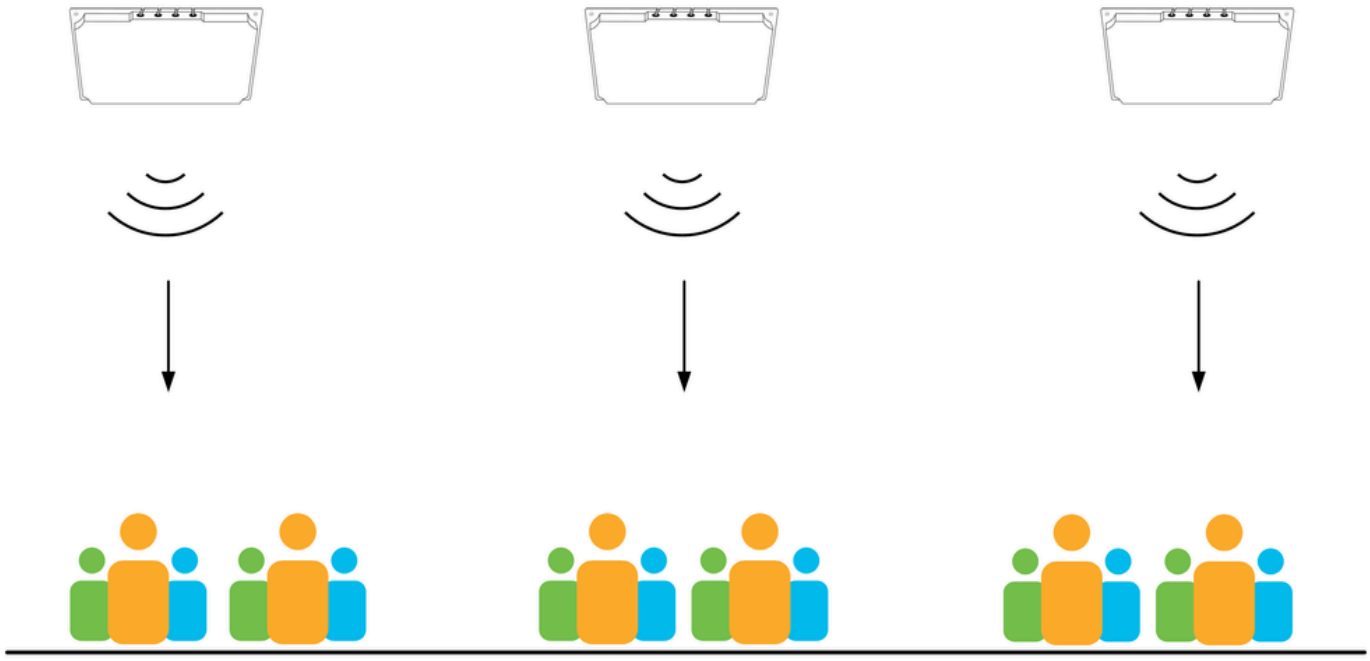
Strategie di copertura

Le strategie di copertura dipendono in gran parte dal tipo di sede, dalle antenne utilizzate e dalle posizioni disponibili per il montaggio dell'antenna.

Costi generali

Ove possibile, la copertura delle spese generali è sempre preferibile.

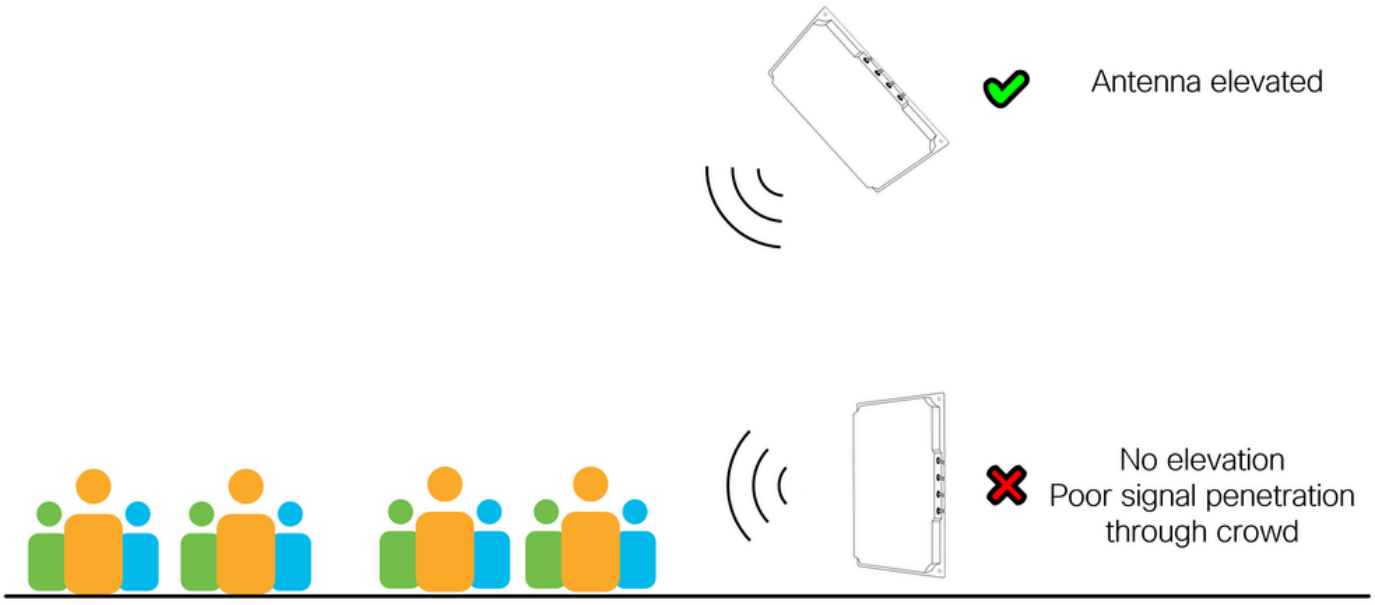
Le soluzioni di overhead hanno il vantaggio distinto che tutti i dispositivi client in genere hanno una linea diretta di visione al sovraccarico dell'antenna, anche in scenari affollati. Le soluzioni di overhead che utilizzano antenne direzionali forniscono un'area di copertura più controllata e ben definita, rendendole meno complicate dal punto di vista della sintonizzazione radio e fornendo al tempo stesso caratteristiche superiori di bilanciamento del carico e roaming dei client. Per ulteriori informazioni, vedere la sezione relativa al bilanciamento dell'alimentazione.



Punti di accesso sopra i client

Lato

Le antenne direzionali montate lateralmente sono una scelta diffusa e sono adatte a diversi scenari, in particolare quando il montaggio su tavolo non è possibile a causa dell'altezza o delle restrizioni di montaggio. Quando si utilizza il montaggio laterale è importante capire il tipo di area coperta dall'antenna, ad esempio è un'area aperta all'aperto o un'area interna densa? Se l'area di copertura è un'area ad alta densità con molte persone, allora l'antenna deve essere elevata il più possibile in quanto la propagazione del segnale attraverso una folla umana è sempre scarsa. Ricordate che la maggior parte dei dispositivi mobili viene utilizzata più in basso a livello di vita, non sopra la testa dell'utente! L'altezza dell'antenna è meno significativa Se l'area di copertura è un'area a densità inferiore.



L'elevazione dell'antenna è sempre migliore

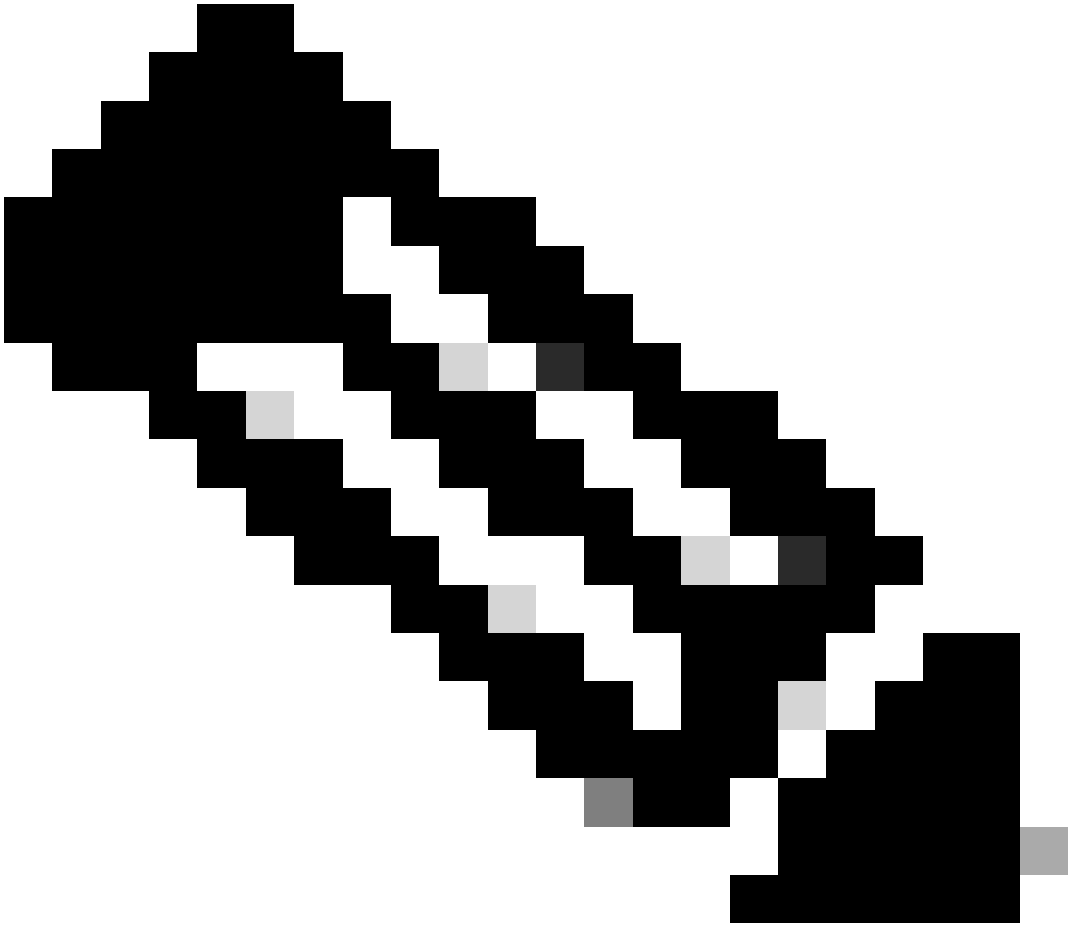
Omnidirezionale

L'uso di antenne omnidirezionali (interne o esterne) deve essere generalmente evitato in scenari ad altissima densità, ciò è dovuto alla potenziale elevata area di impatto per l'interferenza del co-canale. Le antenne omnidirezionali non devono essere utilizzate a un'altezza superiore a 6 m (non si applica alle unità esterne ad alto guadagno).

Sedile inferiore

In alcune arene o stadi possono verificarsi situazioni in cui non vi sono posizioni adatte per il montaggio dell'antenna. L'ultima alternativa disponibile consiste nel fornire una copertura dal basso posizionando i punti di accesso sotto i sedili a sedere degli utenti. Questo tipo di soluzione è più difficile da installare correttamente e in genere è più costosa e richiede un numero significativamente maggiore di punti di accesso e procedure di installazione specifiche.

La sfida principale nelle installazioni "sotto-sedile" è la grande differenza nella copertura tra un luogo pieno e un luogo vuoto. Un corpo umano è molto efficiente nell'attenuare il segnale radio, il che significa che quando c'è una folla di persone che circondano l'AP la copertura risultante è significativamente più piccola rispetto a quando quelle persone non sono lì. Questo fattore di attenuazione della folla umana consente l'installazione di più punti di accesso che possono aumentare la capacità complessiva. Tuttavia, quando la sede è vuota, non c'è attenuazione dai corpi umani e interferenze significative, e questo porta a complicazioni quando la sede è parzialmente piena.



> Nota: l'installazione in sede è una soluzione valida ma non comune, che deve essere valutata caso per caso. L'impiego sotto sede non è trattato più in dettaglio nel presente documento.

Estetica

In alcune implementazioni entra in gioco la questione dell'estetica. Si tratta di aree con progetti architettonici specifici, di valore storico o in cui la pubblicità e/o il branding richiedono dove è possibile (o meno) installare l'apparecchiatura. Soluzioni specifiche possono essere necessarie per ovviare a eventuali limitazioni di posizionamento. Alcune di queste soluzioni includono nascondere l'access point/antenna, colorare l'access point/antenna, montare l'apparecchiatura in un enclosure o semplicemente utilizzare una posizione diversa. Colorare l'antenna annullare la garanzia, se si sceglie di dipingere l'antenna usare sempre vernice non metallica. Cisco in genere non vende enclosure per antenne, ma molte di esse sono facilmente disponibili attraverso vari provider.

Tutte queste soluzioni hanno un impatto sulle prestazioni della rete. Gli architetti wireless iniziano

sempre con la proposta di posizioni di montaggio ottimali per una migliore copertura radio e queste posizioni iniziali di solito forniscono le migliori prestazioni. Qualsiasi modifica apportata a queste posizioni spesso comporta lo spostamento delle antenne dalla posizione ottimale.

Le posizioni in cui sono montate le antenne sono spesso sopraelevate, possono essere soffitti, passerelle, strutture del tetto, travi, passerelle e qualsiasi posizione che fornisce una certa elevazione sulla zona di copertura prevista. Queste posizioni sono generalmente condivise con altre installazioni, come: apparecchiature audio, aria condizionata, illuminazione e vari rilevatori / sensori. Ad esempio, le apparecchiature audio e di illuminazione devono essere installate in luoghi molto specifici - ma perché? Semplicemente perché le apparecchiature audio e di illuminazione non funzionano correttamente quando sono nascoste in una scatola o dietro un muro, e tutti lo riconoscono.

Lo stesso vale per le antenne wireless, che funzionano meglio quando c'è una linea di visuale al dispositivo client wireless. Assegnare priorità all'estetica può (e molto spesso lo fa) avere un effetto negativo sulle prestazioni wireless, riducendo il valore dell'investimento nelle infrastrutture.

Reti non autorizzate

Le reti Wi-Fi non autorizzate sono reti wireless che condividono uno spazio RF comune ma non sono gestite dallo stesso operatore. Questi possono essere temporanei o permanenti e includere i dispositivi dell'infrastruttura (AP) e i dispositivi personali (come i telefoni cellulari che condividono un hotspot Wi-Fi). Le reti Wi-Fi disoneste sono fonte di interferenze e in alcuni casi anche un rischio per la sicurezza. L'impatto dei truffatori sulle prestazioni wireless non deve essere sottovalutato. Le trasmissioni Wi-Fi sono limitate a una gamma relativamente piccola di spettro radio condiviso tra tutti i dispositivi Wi-Fi; eventuali dispositivi con comportamenti errati nelle vicinanze possono compromettere le prestazioni della rete per molti utenti.

Nel contesto di grandi reti pubbliche, queste sono di solito attentamente progettate e sintonizzate utilizzando antenne specializzate. Un buon design RF copre solo le aree richieste, spesso utilizzando antenne direzionali, e regola le caratteristiche di invio e ricezione per la massima efficienza.

All'altro estremo dello spettro ci sono i dispositivi di fascia consumer o i dispositivi forniti dai fornitori di servizi Internet. Questi sistemi dispongono di opzioni limitate per una regolazione precisa della frequenza RF o sono configurati per il range massimo e le prestazioni percepite, spesso con elevata potenza, bassa velocità di trasmissione dei dati e canali ampi. L'introduzione di tali dispositivi in una rete di eventi di grandi dimensioni può causare problemi.

Cosa si può fare?

Nel caso di hotspot personali, si può fare molto poco, poiché sarebbe quasi impossibile monitorare decine di migliaia di persone che entrano in un luogo. Nel caso dell'infrastruttura, o di dispositivi semi-permanenti, ci sono alcune opzioni. I possibili rimedi iniziano dalla semplice istruzione, compresa la semplice segnaletica a fini di sensibilizzazione, attraverso documenti di politica radiofonica firmati, che terminano con l'applicazione attiva e l'analisi dello spettro. In ogni caso, è necessario prendere una decisione commerciale sulla protezione dello spettro radio nella sede in

questione, insieme a misure concrete per far rispettare tale decisione commerciale.

L'aspetto della sicurezza delle reti non autorizzate entra in gioco quando i dispositivi controllati da una terza parte pubblicizzano lo stesso SSID della rete gestita. Equivale a un attacco honeypot e può essere utilizzato come metodo per sottrarre le credenziali dell'utente. Si consiglia sempre di creare una regola non autorizzata per attivare un avviso sul rilevamento di SSID di infrastruttura annunciati da dispositivi non gestiti. La sezione sulla sicurezza tratta più in dettaglio i truffatori.

Singolo da 5 GHz rispetto a doppio da 5 GHz

Il termine doppio da 5 GHz si riferisce all'uso di entrambe le radio da 5 GHz sui punti di accesso supportati. C'è una differenza fondamentale tra il doppio 5GHz con antenne esterne e il doppio 5GHz con antenne interne (micro/macro celle su access point omnidirezionali). Nel caso di antenne esterne, il doppio da 5 GHz è spesso un meccanismo utile, che fornisce una copertura e una capacità aggiuntive riducendo il numero totale di punti di accesso.

Micro/Macro/Meso

I punti di accesso interni hanno entrambe le antenne vicine (all'interno del punto di accesso) e ci sono restrizioni relative alla massima potenza Tx quando si utilizzano i 5 GHz doppi. La seconda radio è limitata a una bassa potenza Tx (imposta dal controller wireless) che determina un grande squilibrio di potenza Tx tra le radio. In questo modo la radio primaria (di maggiore potenza) può attirare molti client, mentre la radio secondaria (di minore potenza) è sottoutilizzata. In questo caso la seconda radio aggiunge energia all'ambiente senza offrire vantaggi ai clienti. Se si verifica questo scenario, è preferibile disabilitare la seconda radio e aggiungere semplicemente un altro access point (da 5 GHz) se è necessaria ulteriore capacità.

I diversi modelli di access point hanno opzioni di configurazione diverse, la seconda radio da 5 GHz può funzionare a livelli di potenza più elevati nei nuovi access point macro/meso come i modelli 9130 e 9136 e alcuni access point Wi-Fi 6E interni come la serie 9160 possono anche funzionare in macro/macro in alcuni casi. Verificare sempre la capacità del modello AP esatto. Anche il secondo slot da 5 GHz è limitato nell'utilizzo del canale, quando uno slot funziona in una banda UNII, l'altro slot è limitato a una banda UNII diversa, che influisce sulla pianificazione del canale e di conseguenza anche sulla potenza di trasmissione disponibile. Considerare sempre la differenza di potenza Tx tra due radio da 5 GHz, ciò è vero in tutti i casi, compresi i punti di accesso interni.

FRA

La tecnologia FRA (Flexible Radio Assignment) è stata introdotta per migliorare la copertura a 5 GHz passando altre radio da 2,4 GHz alla modalità a 5 GHz o radio da 5 GHz potenzialmente inutilizzate alla modalità monitor (per i punti di accesso che la supportano). Poiché il presente documento riguarda grandi reti pubbliche, si presume che le aree di copertura e la progettazione delle radio siano ben definite utilizzando antenne direzionali, pertanto si preferisce una configurazione deterministica a una dinamica. L'utilizzo della FRA non è raccomandato per le grandi reti pubbliche.

Facoltativamente, FRA può essere utilizzato quando la rete è configurata per aiutare a

determinare quali radio convertire a 5 GHz, ma una volta che si è soddisfatti del risultato, si consiglia di congelare FRA.

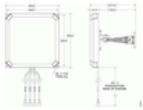
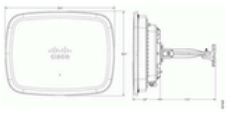
Normative

Ogni ambito normativo definisce quali canali sono disponibili per l'uso e i relativi livelli massimi di potenza; esistono anche restrizioni su quali canali possono essere utilizzati all'interno rispetto all'esterno. A seconda del dominio normativo, a volte non è possibile utilizzare una soluzione dual 5GHz in modo efficace. Un esempio di questo è il dominio ETSI dove 30dBm è consentito sui canali UNII-2e, ma solo 23dBm su UNII1/2. In questo esempio, se il progetto richiede l'uso di 30 dBm (solitamente a causa della distanza maggiore dall'antenna) l'uso di una singola radio da 5 GHz può essere l'unica soluzione fattibile.

Antenne

Le reti pubbliche di grandi dimensioni possono utilizzare qualsiasi tipo di antenna e in genere scelgono l'antenna più adatta per il lavoro. Miscelando le antenne all'interno della stessa zona di copertura si rende il processo di progettazione della radio più complesso e, se possibile, deve essere evitato. Tuttavia, le grandi reti pubbliche hanno spesso ampie aree di copertura con diverse opzioni di montaggio anche all'interno della stessa area, rendendo in alcuni casi necessario combinare le antenne. Le antenne omnidirezionali sono ben conosciute e funzionano come qualsiasi altra antenna. In questa guida vengono illustrate le antenne direzionali esterne.

In questa tabella vengono elencate le antenne esterne più utilizzate.

	C-ANT9103 Patch antenna (8x8) 6 dBi	5GHz Beamwidth 70°x70° ~33ft (10m)
	ANT2566P4W-R/S Patch antenna (4x4) 6 dBi	5GHz Beamwidth 110°x55° (120°x60°) ~33ft (10m)
	ANT2566D4M-R/S Patch antenna (4x4) 6 dBi	5GHz Beamwidth 55°x60° (60°x60°) ~33ft (10m)
	ANT2513P4M-N/S HD “Stadium” antenna 13 dBi	5GHz Beamwidth 31°x27° (30°x30°) ~66ft (20m)
	C-ANT9104 HD “Stadium” antenna Narrow 10dBi / Wide 7dBi	5GHz Beamwidth Narrow 25°x25° Wide 80°x25°

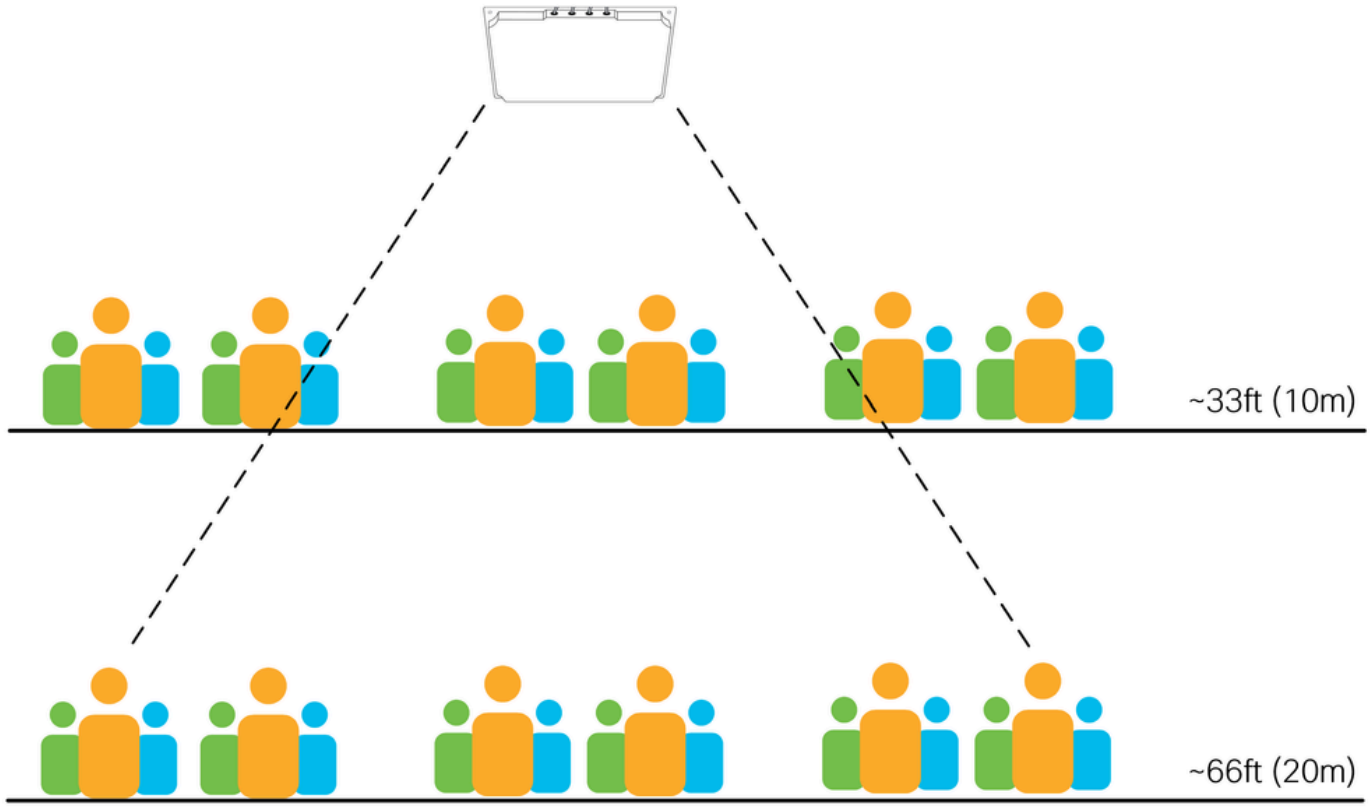
Elenco delle antenne

I fattori principali da prendere in considerazione quando si sceglie un'antenna sono la larghezza del raggio dell'antenna e la distanza/altezza a cui l'antenna è montata. La tabella mostra la larghezza del raggio di 5 GHz per ciascuna delle antenne, con i numeri tra parentesi che mostrano i valori arrotondati (e più facili da ricordare).

Le distanze suggerite nella tabella non sono regole rigide, ma solo linee guida basate sull'esperienza. Le onde radio viaggiano alla velocità della luce e non si fermano semplicemente dopo aver raggiunto una distanza arbitraria. Tutte le antenne funzionano oltre la distanza consigliata, tuttavia, le prestazioni diminuiscono con l'aumentare della distanza. L'altezza di installazione è un fattore chiave durante la pianificazione.

Il diagramma seguente mostra due possibili altezze di montaggio per la stessa antenna a circa 10 m e 20 m in un'area ad alta densità. Si noti che il numero di client che l'antenna è in grado di visualizzare (e da cui accettare connessioni) aumenta con la distanza. Mantenere dimensioni di cella più piccole diventa più difficile con distanze maggiori.

La regola generale è che più alta è la densità degli utenti, più importante è usare l'antenna corretta per la distanza data.



Antenna da stadio

L'antenna dello stadio C9104 è ideale per la copertura di aree ad alta densità e distanze elevate. Per ulteriori informazioni, consultare la Guida all'installazione dell'antenna dello stadio Catalyst 9104 (C-ANT9104).

Cambiamenti nel tempo

I cambiamenti dell'ambiente fisico nel tempo sono comuni in quasi tutte le installazioni wireless (ad esempio, il movimento delle pareti interne). Visite periodiche in loco e ispezioni visive sono sempre state una pratica raccomandata. Per le reti di eventi esiste l'ulteriore complessità di gestire i sistemi audio e di illuminazione e in molti casi anche altri sistemi di comunicazione (come il 5G). Tutti questi sistemi sono spesso installati in posizioni elevate sopra gli utenti, talvolta causando conflitti per lo stesso spazio. Una buona posizione per un'antenna wireless da stadio è spesso

anche una buona posizione per un'antenna 5G! Inoltre, una volta aggiornati nel tempo, questi sistemi possono essere spostati in luoghi in cui ostacolano e/o interferiscono attivamente con il sistema wireless. È importante tenere traccia delle altre installazioni e comunicare con i team che le installano, per garantire che tutti i sistemi siano installati in posizioni idonee senza interferire tra loro (fisicamente o elettromagneticamente).

Alta densità e 6 GHz

Al momento della stesura di questo documento vi è una selezione limitata di antenne esterne da 6 GHz. Solo il punto di accesso/antenna integrato CW9166D1 funziona a 6 GHz; le specifiche dettagliate dell'antenna sono disponibili nella Cisco Catalyst CW9166D1 Access Point Deployment Guide (informazioni in lingua inglese). CW9166D1 fornisce copertura a 6 GHz con una larghezza del raggio di 60° x60° e può essere utilizzato in modo efficace per qualsiasi installazione che soddisfi le condizioni per questo tipo di antenna. Ad esempio, gli auditorium e i magazzini sono ottimi candidati per l'installazione del CW9166D1, poiché l'unità integrata offre funzionalità di antenna direzionale per l'uso in interni.

	CW9166D1 6GHz (4x4) or XOR 5GHz	 60° x60° 8 dBi
	5GHz (4x4)	70° x70° 6 dBi
	2.4GHz (4x4)	70° x70° 6 dBi

9166D1

Nel contesto di grandi reti pubbliche, queste hanno spesso vaste aree e richiedono l'uso di una combinazione di antenne a varie altezze. L'installazione di una rete pubblica di grandi dimensioni, end-to-end, utilizzando solo un'antenna a 60° x60° può essere un'operazione complessa a causa delle limitazioni imposte dalla distanza. Pertanto, può essere anche impegnativo fornire una copertura end-to-end a 6 GHz utilizzando solo CW9166D1 per una rete pubblica di grandi dimensioni.

Un possibile approccio è quello di utilizzare i 5 GHz come banda di copertura primaria, mentre utilizzare i 6 GHz solo in aree specifiche per scaricare i dispositivi client in modo da ripulire la banda dei 6 GHz. Questo tipo di approccio si avvale di antenne solo da 5 GHz in aree più grandi, utilizzando le antenne da 6 GHz ove possibile e nei casi in cui è richiesta una capacità aggiuntiva.

Ad esempio, si consideri una grande sala per eventi in una conferenza commerciale, la sala principale utilizza antenne da stadio per fornire la copertura primaria a 5 GHz, l'altezza dell'installazione impone l'uso di antenne da stadio. Il CW9166D1 non può essere utilizzato nella

sala principale di questo esempio a causa di limiti di distanza - ma può essere utilizzato in modo efficace in una sala VIP adiacente o in un'area stampa dove è richiesta una maggiore densità. Il roaming dei client tra le bande da 5 GHz e 6 GHz viene illustrato più avanti in questo documento.

Normative

Come per i 5 GHz, la potenza disponibile e i canali per 6 GHz differiscono in modo significativo tra i domini normativi. In particolare, vi è una grande differenza nello spettro disponibile tra i domini FCC ed ETSI, così come linee guida rigorose sulla potenza Tx disponibile per l'uso interno ed esterno, Low Power Indoor (LPI) e Standard Power (SP) rispettivamente. Con 6 GHz, le restrizioni aggiuntive includono limiti di alimentazione dei client, l'uso di antenne esterne e inclinazione dell'antenna verso il basso e (solo negli Stati Uniti per il momento) la necessità di Automated Frequency Coordination (AFC) per le installazioni di SP.

Per ulteriori informazioni su Wi-Fi 6E vedere Wi-Fi 6E: il prossimo grande capitolo nel white paper Wi-Fi.

Gestione risorse radio

Radio Resource Management (RRM) è un insieme di algoritmi responsabili del controllo delle operazioni radio. Questa guida fa riferimento a due algoritmi RRM principali, ovvero Dynamic Channel Assignment (DCA) e Transmit Power Control (TPC). RRM è un'alternativa alla configurazione statica del canale e dell'alimentazione.

- DCA viene eseguito in base a una pianificazione configurabile (impostazione predefinita: 10 minuti).
- TPC viene eseguito in base a una pianificazione automatica (impostazione predefinita 10 minuti).

Cisco Event Driven RRM (ED-RRM) è un'opzione DCA che consente di prendere una decisione di cambio canale al di fuori del programma DCA standard, generalmente in risposta a condizioni RF gravi. ED-RM può cambiare canale immediatamente quando vengono rilevati livelli eccessivi di interferenza. In ambienti rumorosi e/o instabili, l'abilitazione di ED-RRM comporta il rischio di eccessive modifiche dei canali, con un potenziale impatto negativo sui dispositivi client.

L'utilizzo di RRM è consigliato e generalmente preferito rispetto alla configurazione statica, tuttavia con alcune avvertenze ed eccezioni.

- Il TPC deve essere limitato a un intervallo ristretto di valori utilizzando l'impostazione TPC min/max, in base alle esigenze, e sempre allineato al design RF.
    - Attivazione del riconoscimento del canale TPC in ambienti ad alta densità.

- Il ciclo DCA deve essere modificato dall'impostazione predefinita di 10 minuti.
    - Non utilizzare ED-RM in ambienti HD.
    - Disabilitare l'opzione Evita caricamento Cisco AP.
    - Le opzioni per evitare l'utilizzo di punti di accesso non autorizzati, ad esempio Evita interferenze esterne nei punti di accesso, possono generare un ambiente instabile se sono presenti molti utenti non autorizzati. È sempre meglio rimuovere la canaglia che

tentare di rispondere.
- Le decisioni RRM possono essere influenzate da punti di accesso/antenne che non si sentono correttamente, come nel caso delle antenne direzionali che puntano l'una dall'altra.
- Alcune antenne (ad esempio C9104) non supportano RRM e richiedono sempre una configurazione statica.
- RRM non risolve problemi di progettazione RF scadente.

In tutti i casi, RRM deve essere implementato con una comprensione del risultato previsto e ottimizzato per funzionare entro limiti appropriati per l'ambiente RF specifico. Nelle sezioni seguenti di questo documento questi punti vengono esaminati in dettaglio.

Configurazione RF

Canali

In generale, maggiore è il numero di canali, migliore è la qualità. In installazioni ad alta densità possono essere installati più punti di accesso e radio di ordini di grandezza rispetto ai canali disponibili, il che implica un elevato rapporto di riutilizzo dei canali e, insieme a ciò, livelli più elevati di interferenza tra i canali. È necessario utilizzare tutti i canali disponibili e si sconsiglia di limitare l'elenco dei canali disponibili.

In alcuni casi è necessario che un sistema wireless specifico (e distinto) coesista nello stesso spazio fisico e che vi vengano allocati canali dedicati, rimuovendo allo stesso tempo i canali allocati dall'elenco DCA del sistema primario. Questi tipi di esclusione dei canali devono essere valutati con molta attenzione e utilizzati solo quando necessario. Un esempio può essere un collegamento point-to-point che opera in un'area aperta adiacente alla rete primaria, o un'area stampa all'interno di uno stadio. Se più di uno o due canali sono esclusi dall'elenco DCA, si tratta di una causa per rivalutare la soluzione proposta. In alcuni casi, ad esempio in stadi ad altissima densità, l'esclusione di un singolo canale a volte non è un'opzione fattibile.

DCA (Dynamic Channel Assignment) può essere utilizzato con RRM basato su WLC o RRM avanzato con AI.

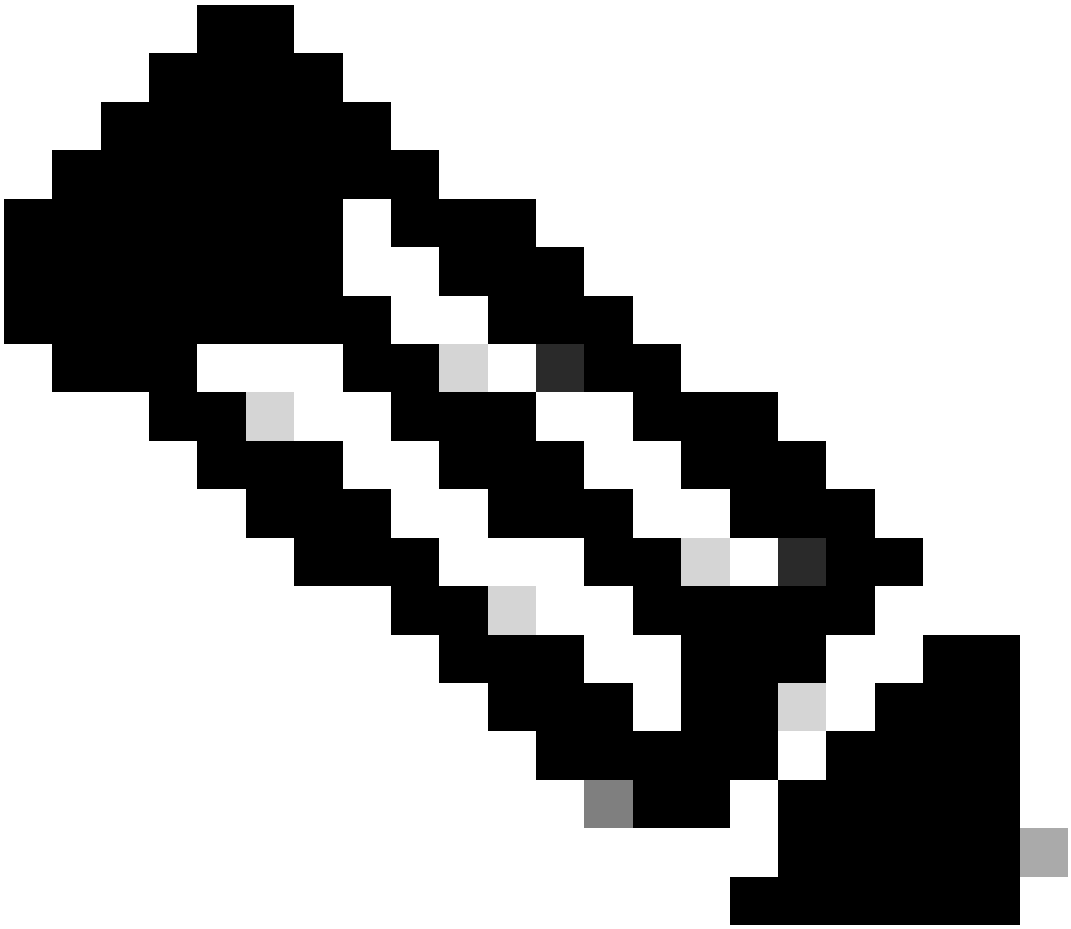
L'intervallo DCA predefinito è di 10 minuti, il che può determinare frequenti cambi di canale in ambienti RF instabili. Il timer DCA predefinito deve essere aumentato rispetto ai 10 minuti predefiniti in tutti i casi; l'intervallo DCA specifico deve essere allineato ai requisiti operativi per la rete in questione. Un esempio di configurazione può essere: intervallo DCA 4 ore, tempo di ancoraggio 8. In questo modo, le modifiche ai canali vengono limitate a una volta ogni 4 ore, a partire dalle 8 del mattino.

Poiché le interferenze sono destinate a verificarsi, l'adattamento ad esse in ogni ciclo DCA non porta necessariamente valore, poiché molte di queste interferenze sono temporanee. Una buona tecnica consiste nell'utilizzare il DCA automatico per le prime ore e bloccare l'algoritmo e il channel plan quando si dispone di qualcosa di stabile che si è soddisfatti.

Quando il WLC viene riavviato, DCA rimane in esecuzione in modalità aggressiva per 100 minuti per trovare un channel plan appropriato. È consigliabile riavviare il processo manualmente quando

vengono apportate modifiche significative al progetto RF, ad esempio aggiungendo o rimuovendo numerosi punti di accesso o modificando la larghezza del canale. Per avviare manualmente il processo, utilizzare questo comando.

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



Nota: le modifiche dei canali possono interrompere le attività dei dispositivi client.

2,4 GHz

La banda a 2,4 GHz è stata spesso criticata. Ha solo tre canali non sovrapposti e molte altre tecnologie oltre al Wi-Fi lo usano, creando interferenze indesiderate. Alcune organizzazioni insistono nel fornire servizi su di esso, quindi qual è una conclusione ragionevole? È un dato di fatto che la banda a 2,4 GHz non offre un'esperienza soddisfacente agli utenti finali. Inoltre, se si cerca di fornire servizi a 2,4 GHz, si risentono anche altre tecnologie a 2,4 GHz, come Bluetooth.

In occasione di grandi eventi o di grandi eventi, molte persone si aspettano ancora che le cuffie wireless funzionino quando effettuano una chiamata o che i loro indossabili intelligenti continuino a funzionare come al solito. Se il Wi-Fi ad alta densità funziona a 2,4 GHz, si ha un impatto diretto sui dispositivi che non utilizzano il Wi-Fi a 2,4 GHz.

Una cosa è certa: se si deve davvero fornire un servizio Wi-Fi a 2,4 GHz, è meglio farlo su un SSID separato (dedicarlo ai dispositivi IoT o chiamarlo "legacy"). Ciò significa che i dispositivi dual-band non si connettono involontariamente a 2,4 GHz e che solo i dispositivi single-band da 2,4 GHz vi si connettono.

Cisco non consiglia o supporta l'uso di canali a 40 MHz in 2,4 GHz.

5 GHz

Installazione tipica per reti wireless ad alta densità. Se possibile, utilizzare tutti i canali disponibili.

Il numero di canali varia a seconda del dominio normativo. Considerate l'impatto del radar in una posizione specifica, utilizzate i canali DFS (compresi i canali TDWR) quando possibile.

La larghezza del canale a 20 MHz è altamente consigliata per tutte le installazioni ad alta densità.

I 40 MHz possono essere utilizzati come 2,4 GHz, ovvero solo quando (e dove) assolutamente necessario.

Valutare la necessità e i vantaggi reali dei canali a 40 MHz nell'ambiente specifico. I canali a 40 MHz richiedono un rapporto segnale/rumore (SNR) più elevato per realizzare qualsiasi miglioramento nel throughput. Se non è possibile un SNR più elevato, i canali a 40 MHz non servono a nulla. Le reti ad alta densità assegnano priorità alla media per tutti gli utenti rispetto a un throughput potenzialmente più elevato per ogni singolo utente. È preferibile posizionare più punti di accesso sui canali a 20 MHz piuttosto che utilizzare i punti di accesso a 40 MHz, in quanto il canale secondario viene utilizzato solo per i frame dati e quindi utilizzato in modo molto meno efficiente rispetto all'avere due diverse celle radio, ognuna operante a 20 MHz (in termini di capacità totale, non in termini di throughput di un singolo client).

6 GHz

La banda a 6 GHz non è ancora disponibile in tutti i paesi. Inoltre, alcuni dispositivi dispongono di una scheda Wi-Fi compatibile con 6 GHz ma per attivarla è necessario un aggiornamento del BIOS per il paese in cui si sta utilizzando il dispositivo. Il modo più popolare in cui i clienti scoprono le radio da 6 GHz in questo momento è tramite l'annuncio RNR sulla radio da 5 GHz. Ciò significa che i 6 GHz non devono funzionare da soli senza una radio da 5 GHz sullo stesso punto di accesso. I 6 GHz sono disponibili per scaricare i client e il traffico dalla radio da 5 GHz e per offrire in genere un'esperienza migliore ai client in grado di supportare l'ambiente. I canali a 6 GHz consentono di utilizzare larghezze di banda di canale più ampie, ma dipendono in larga misura dal numero di canali disponibili nel dominio normativo. Con 24 canali da 6 GHz disponibili in Europa, non è irragionevole scegliere canali da 40 MHz per fornire un throughput massimo migliore rispetto ai 20 MHz che probabilmente si utilizzano in 5 GHz. Negli Stati Uniti, con un numero di canali quasi doppio, usare 40MHz è un gioco da ragazzi e anche andare a 80MHz non

è irragionevole per un evento di grande densità. Le larghezze di banda maggiori non devono essere utilizzate in eventi o luoghi ad alta densità.

Velocità dati

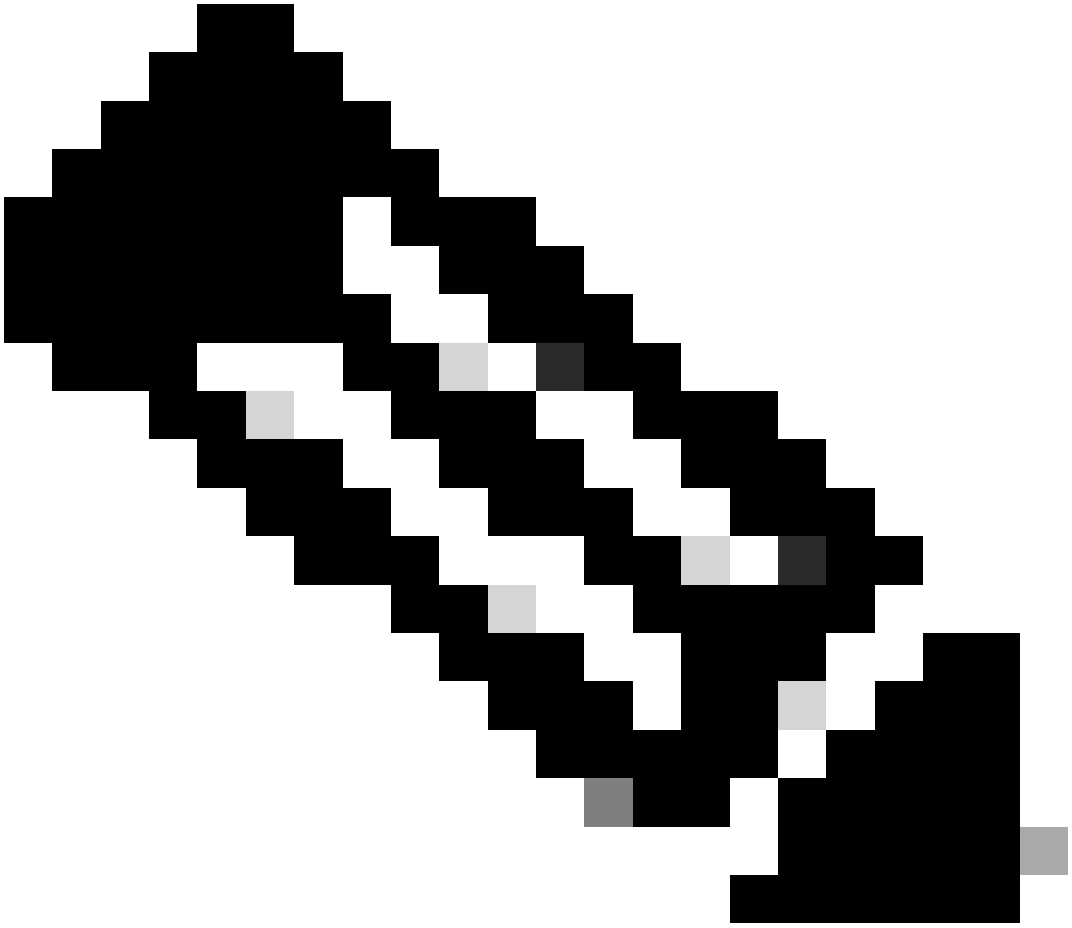
La velocità dati che un client negozia con un punto di accesso è in gran parte una funzione del rapporto segnale/rumore (SNR, Signal-to-Noise Ratio) di quella connessione, ed è vero anche il contrario, ossia velocità dati più elevate richiedono SNR più elevati. Infatti, è soprattutto la tecnologia SNR a determinare la velocità di collegamento massima possibile, ma perché è importante quando si configurano le velocità dei dati? È perché alcune velocità dati hanno un significato speciale.

Le velocità dati OFDM classiche (802.11a) possono essere configurate in una delle tre impostazioni seguenti: Disabilitato, Supportato o Obbligatorio. Le velocità OFDM sono (in Mbps): 6, 9, 12, 18, 24, 36, 48, 54. Il client e l'access point devono entrambi supportare una velocità prima di poterla utilizzare.

Supportato - l'access point utilizzerà la tariffa

Obbligatorio: l'access point utilizzerà la tariffa e invierà il traffico di gestione utilizzando questa tariffa

Disabilitato: l'access point non utilizzerà la velocità, obbligando il client a utilizzare un'altra velocità



Nota: i tassi obbligatori sono anche chiamati tassi base

Il significato della frequenza obbligatoria è che tutti i frame di gestione vengono inviati utilizzando questa frequenza, oltre ai frame broadcast e multicast. Se sono configurate più velocità obbligatorie, i frame di gestione utilizzano la velocità obbligatoria configurata più bassa e la velocità obbligatoria configurata più alta viene utilizzata dalla trasmissione e dal multicast.

I frame di gestione includono beacon che devono essere ascoltati dal client per essere in grado di associarsi all'access point. Aumentando la velocità obbligatoria aumenta anche il requisito SNR per quella trasmissione, ricordate che velocità di dati più elevate richiedono SNR più elevato, e questo in genere significa che il client deve essere più vicino all'AP per essere in grado di decodificare il beacon e associare. Pertanto, manipolando la velocità dati obbligatoria, manipoliamo anche l'effettiva gamma di associazioni dell'AP, costringendo i clienti più vicini all'AP, o verso una potenziale decisione di roaming. I client vicini al punto di accesso utilizzano velocità di trasmissione dei dati più elevate, mentre le velocità di trasmissione dei dati più elevate utilizzano una minore quantità di tempo di trasmissione. L'effetto desiderato è una cella più efficiente. È importante ricordare che l'aumento della velocità di trasmissione dei dati influisce solo sulla

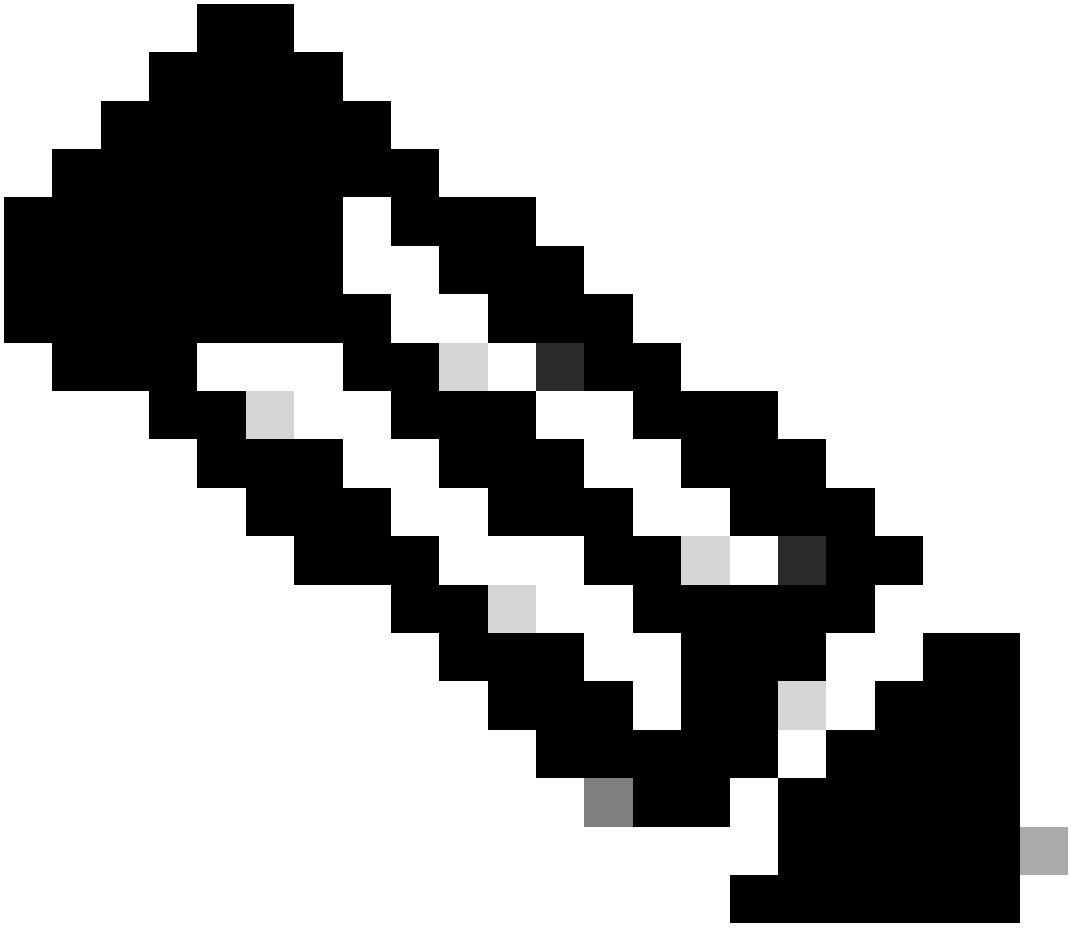
velocità di trasmissione di alcuni frame, non sulla propagazione RF dell'antenna o sull'intervallo di interferenza. Per ridurre al minimo le interferenze e i disturbi del canale condiviso, sono necessarie buone pratiche di progettazione della frequenza radio.

Viceversa, lasciare le tariffe più basse come obbligatorie significa in genere che i clienti saranno in grado di associarsi da una distanza molto più ampia, utile in scenari di densità più bassa, ma con il potenziale di causare il caos con il roaming in scenari di densità più alta. Chiunque abbia provato a individuare un access point non autorizzato che sta trasmettendo un 6 Mbps saprà che è possibile rilevare l'access point molto lontano dalla sua posizione fisica!

Per quanto riguarda la trasmissione e il multicast, in alcuni casi è configurata una seconda velocità obbligatoria (più alta) per aumentare la velocità di recapito del traffico multicast. Questa operazione ha raramente successo in quanto il multicast non viene mai riconosciuto e mai ritrasmesso in caso di perdita dei frame. Poiché una certa perdita è insita in tutti i sistemi wireless, è inevitabile che alcuni frame multicast vadano persi, a prescindere dalla velocità configurata. Un approccio migliore ad una consegna multicast affidabile è dato dalle tecniche di conversione da multicast a unicast che trasmettono il multicast come un flusso unicast, con il vantaggio di velocità di trasmissione dei dati più elevate e di una consegna affidabile (riconosciuta).

È preferibile utilizzare un'unica tariffa obbligatoria, disabilitare tutte le tariffe al di sotto della tariffa obbligatoria e lasciare supportate tutte le tariffe al di sopra della tariffa obbligatoria. La velocità specifica da utilizzare dipende dallo scenario d'uso, in quanto le velocità più basse sono utili negli scenari a bassa densità e all'aperto in cui le distanze tra i punti di accesso sono maggiori. Per le reti ad alta densità ed eventi, le velocità basse devono essere disabilitate.

Se non si è certi del punto di partenza, utilizzare una velocità obbligatoria di 12 Mbps per le distribuzioni a bassa densità e di 24 Mbps per le distribuzioni ad alta densità. Molti eventi su larga scala, stadi e persino installazioni aziendali ad alta densità hanno dimostrato di funzionare in modo affidabile con una velocità obbligatoria di 24 Mbps. Si raccomanda di effettuare test appropriati nei casi specifici in cui sono necessarie velocità inferiori a 12 Mbps o superiori a 24 Mbps.

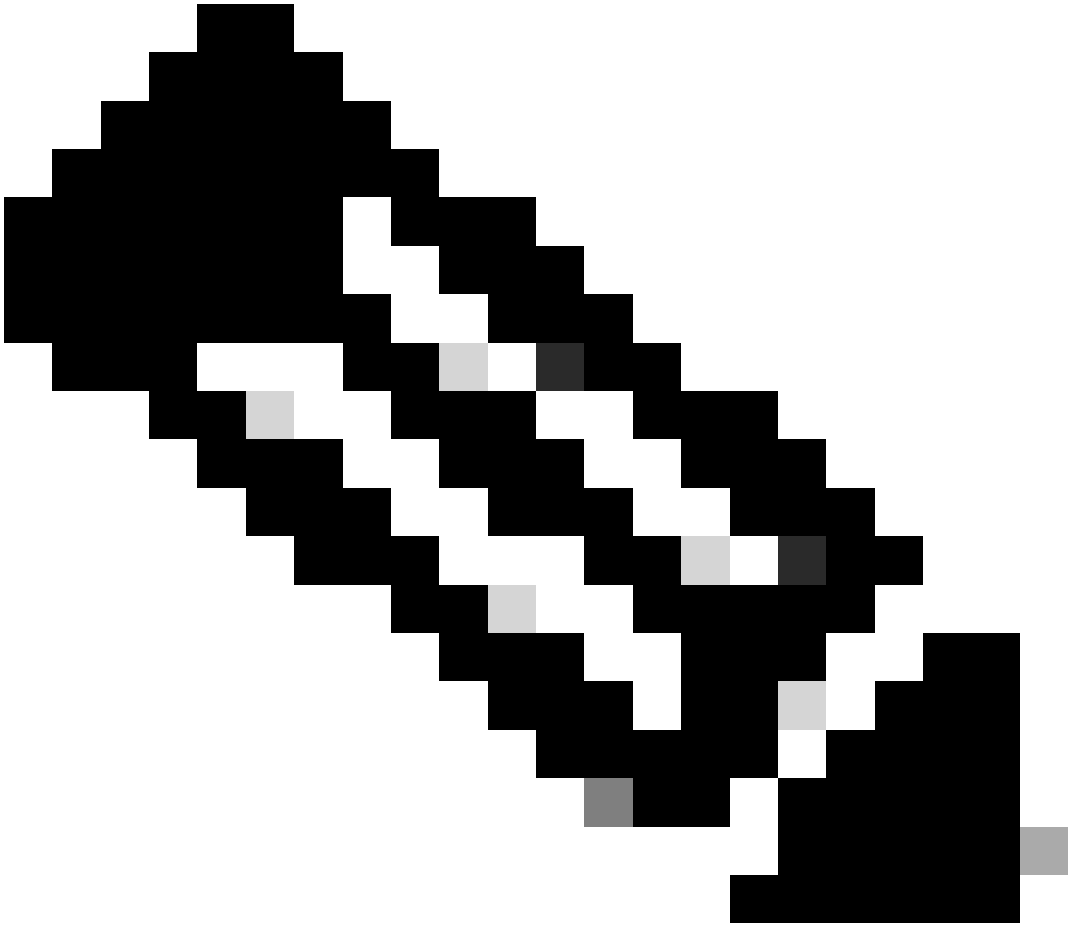


Nota: è meglio lasciare abilitate tutte le velocità 802.11n/ac/ax (tutte le velocità nella sezione High Throughput dell'interfaccia grafica del WLC); raramente è necessario disabilitare una di queste.

Potenza di trasmissione

Le raccomandazioni relative alla potenza di trasmissione variano in base al tipo di distribuzione. In questa sezione vengono differenziate le installazioni in interni che utilizzano antenne omnidirezionali da quelle che utilizzano antenne direzionali. Entrambi i tipi di antenne possono esistere in una rete pubblica di grandi dimensioni, anche se in genere coprirebbero diversi tipi di aree.

Per le distribuzioni omnidirezionali è comune utilizzare il controllo automatico della potenza di trasmissione (TPC, Transmit Power Control) con una soglia minima configurata staticamente e, in alcuni casi, anche una soglia massima configurata staticamente.



Nota: le soglie TPC si riferiscono alla potenza di trasmissione radio ed escludono il guadagno dell'antenna. Accertarsi sempre che il guadagno dell'antenna sia configurato correttamente per il modello di antenna utilizzato; questa operazione viene eseguita automaticamente nel caso di antenne interne e di antenne con identificazione automatica.

Esempio 1

TPC min.: 5 dBm, TPC max.: massimo (30 dBm)

In questo modo, l'algoritmo TPC determina automaticamente la potenza di trasmissione, ma non può mai scendere al di sotto della soglia minima configurata di 5 dBm.

Esempio 2

TPC min.: 2 dBm, TPC max.: 11 dBm

In questo modo, l'algoritmo TPC determina automaticamente la potenza di trasmissione, ma rimane sempre tra 2 dBm e 11 dBm.

È consigliabile creare diversi profili RF con soglie diverse, ad esempio basso consumo (2-5 dBm), medio consumo (5-11 dbM) e alto consumo (11-17 dBm), quindi assegnare punti di accesso omnidirezionali a ogni profilo RF in base alle esigenze. I valori di ciascun profilo RF possono essere regolati in base all'uso previsto e all'area di copertura. Ciò consente agli algoritmi RRM di funzionare in modo dinamico rispettando i limiti predefiniti.

L'approccio per le antenne direzionali è molto simile, l'unica differenza è il livello di precisione richiesto. Il posizionamento dell'antenna direzionale deve essere progettato e verificato durante un'indagine RF pre-installazione e i valori specifici della configurazione della radio sono in genere il risultato di questo processo.

Ad esempio, se è necessaria un'antenna patch montata a soffitto per coprire una determinata area da un'altezza di circa 8 m, l'indagine RF deve determinare la potenza Tx minima richiesta per ottenere la copertura prevista (ciò determina il valore TPC minimo per il profilo RF). Allo stesso modo, dalla stessa indagine RF comprenderemmo la possibile sovrapposizione richiesta tra questa e l'antenna successiva, o anche il punto in cui vogliamo che la copertura termini - questo fornirebbe il valore TPC massimo per il profilo RF.

I profili RF per le antenne direzionali sono in genere configurati con gli stessi valori TPC minimo e massimo o con un intervallo ristretto di valori possibili (generalmente <= 3dBm).

I profili RF sono preferiti per garantire la coerenza della configurazione; si sconsiglia la configurazione statica dei singoli access point. È buona norma assegnare un nome ai profili RF in base all'area di copertura, al tipo di antenna e al caso di utilizzo, ad esempio RF-Auditorium-Patch-Ceiling.

La quantità corretta di potenza Tx si ha quando il valore SNR richiesto viene raggiunto dal client più debole nell'area di copertura prevista, e non più di questo. 30dBm è un ottimo valore di destinazione per i clienti SNR in condizioni reali (vale a dire, in un luogo pieno di persone).

CHD

Il rilevamento dei fori di copertura (CHD, Coverage Hole Detection) è un algoritmo separato per l'identificazione e la correzione dei fori di copertura. CHD è configurato a livello globale e per WLAN. Un possibile effetto del CHD è l'aumento della potenza Tx per compensare i fori di copertura (aree con client costantemente rilevati con segnale debole), questo effetto è a livello di radio e interessa tutte le WLAN, anche quando viene attivato da una singola WLAN configurata per il CHD.

Le reti pubbliche di grandi dimensioni sono in genere configurate su livelli di alimentazione specifici utilizzando profili RF, alcune possono trovarsi in aree aperte con client in roaming in entrata e in uscita dalle aree, non è necessario un algoritmo per regolare dinamicamente l'alimentazione Tx AP in risposta a questi eventi client.

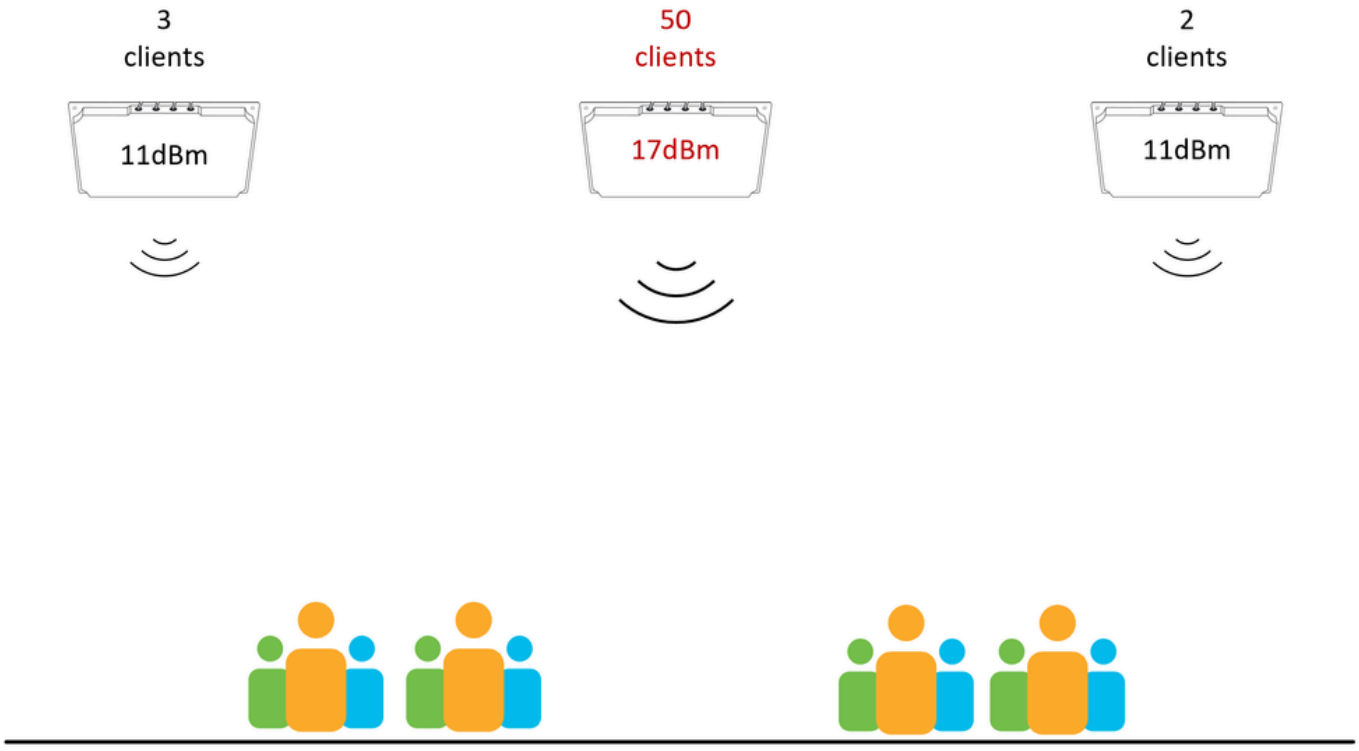
Per le reti pubbliche di grandi dimensioni, CHD deve essere disabilitato a livello globale.

Bilanciamento dell'alimentazione

La maggior parte dei dispositivi client preferisce un segnale di ricezione più alto quando si sceglie il punto di accesso da associare. È necessario evitare situazioni in cui un access point è configurato con una potenza Tx significativamente superiore rispetto ad altri access point circostanti. I punti di accesso che funzionano con una maggiore potenza di trasmissione attraggono un numero maggiore di client, determinando una distribuzione non uniforme tra i punti di accesso (ad esempio, un singolo punto di accesso/radio è sovraccarico di client mentre i punti di accesso circostanti sono sottoutilizzati). Questa situazione è comune nelle implementazioni con ampia copertura sovrapposta da più antenne e nei casi in cui a un punto di accesso sono collegate più antenne.

Per la scelta dell'alimentazione Tx, le antenne da stadio come la C9104 richiedono particolare attenzione in quanto i raggi dell'antenna si sovrappongono in base alla progettazione. Per ulteriori informazioni, consultare la Guida all'installazione dell'antenna da stadio Catalyst 9104 (C-ANT9104).

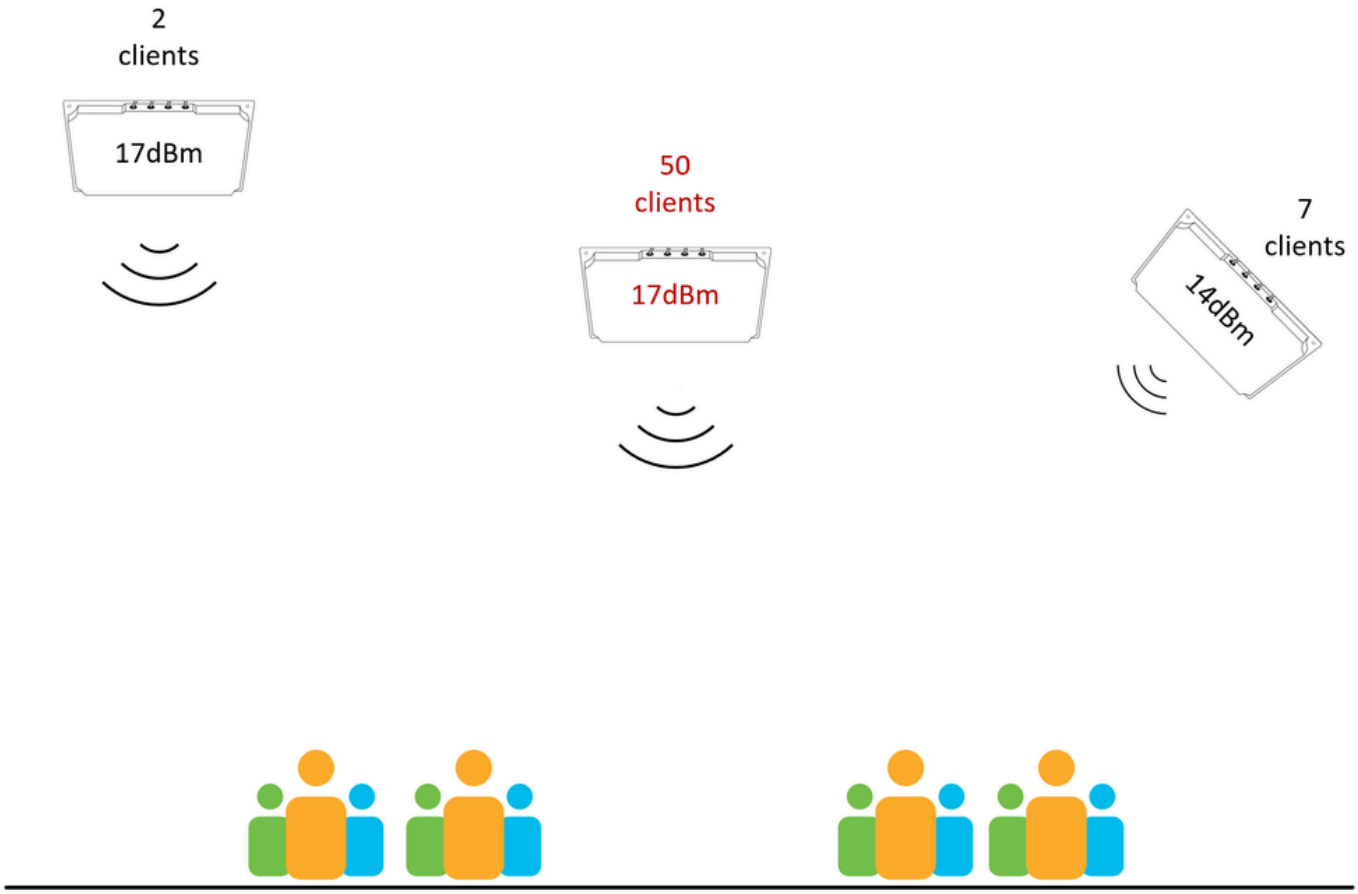
Nel diagramma sottostante, l'antenna centrale è configurata con una maggiore potenza Tx rispetto alle antenne circostanti. Questa configurazione potrebbe causare il blocco dei client all'antenna centrale.



Un punto di accesso con una potenza superiore rispetto ai punti di accesso adiacenti attrae tutti i client

Il diagramma seguente mostra una situazione più complicata: non tutte le antenne sono alla stessa altezza e non tutte utilizzano la stessa inclinazione/orientamento. Ottenere un'alimentazione bilanciata è più complicato che configurare semplicemente tutte le radio con la stessa alimentazione Tx. In scenari come questo, può essere richiesto un sondaggio del sito post-installazione, che fornisce una vista della copertura dal punto di vista del dispositivo client (sul campo). I dati dell'indagine possono quindi essere utilizzati per bilanciare la configurazione in modo da ottenere la copertura migliore e la distribuzione ottimale dei client.

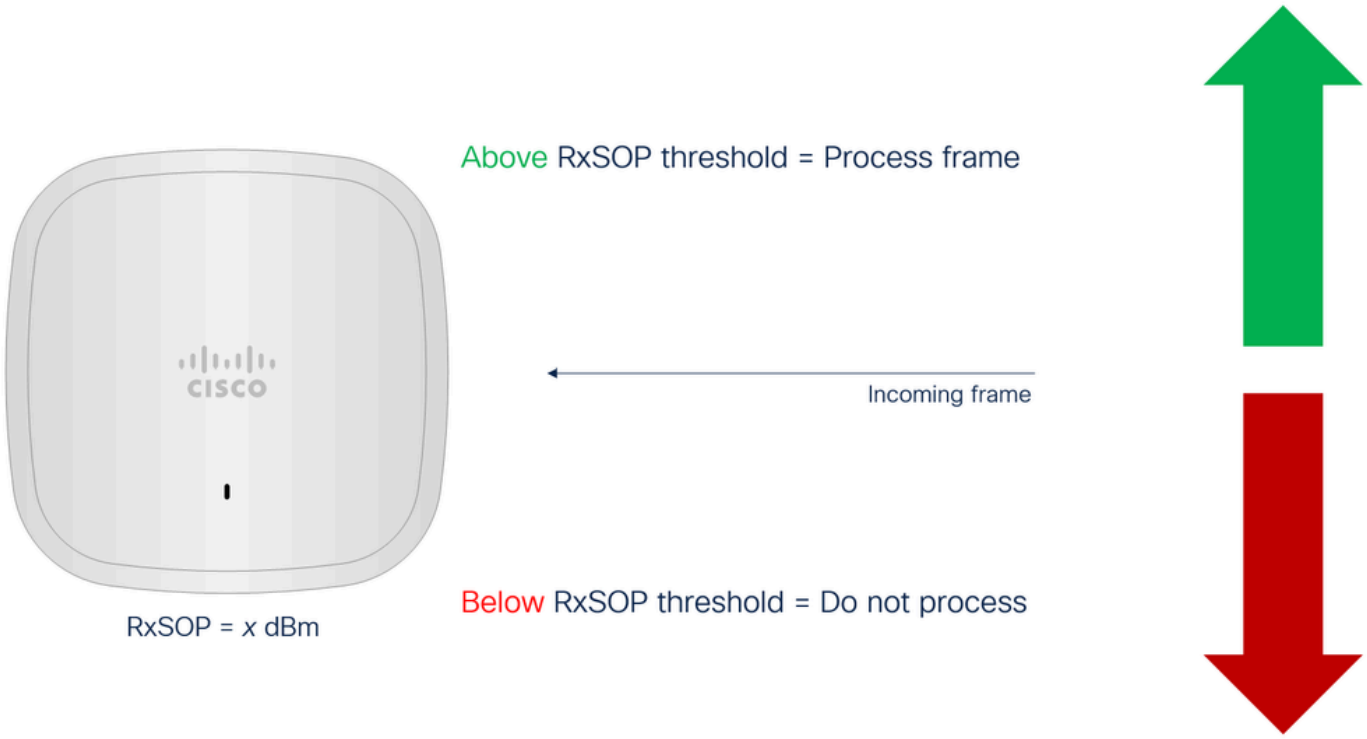
Progettare posizioni di posizionamento AP uniformi che evitano situazioni complicate come questa è il modo migliore per prevenire impegnative scenari di sintonizzazione RF (anche se a volte non ci sono altre scelte!).



Un punto di accesso attrae tutti i clienti nonostante la potenza Tx sia simile, ma l'altezza e le angolazioni giocano un ruolo importante

RxSOP

A differenza di meccanismi come la potenza Tx o la velocità dei dati che influenzano le caratteristiche della cella di trasmissione, RxSOP (Receiver Start of Packet Detection) ha lo scopo di influenzare le dimensioni della cella di ricezione. In sostanza, RxSOP può essere considerato come una soglia di rumore, in quanto definisce il livello del segnale ricevuto al di sotto del quale l'AP non tenta di decodificare le trasmissioni. Tutte le trasmissioni in arrivo con un livello di segnale più debole della soglia RxSOP configurata non vengono elaborate dall'access point e vengono trattate come disturbi.



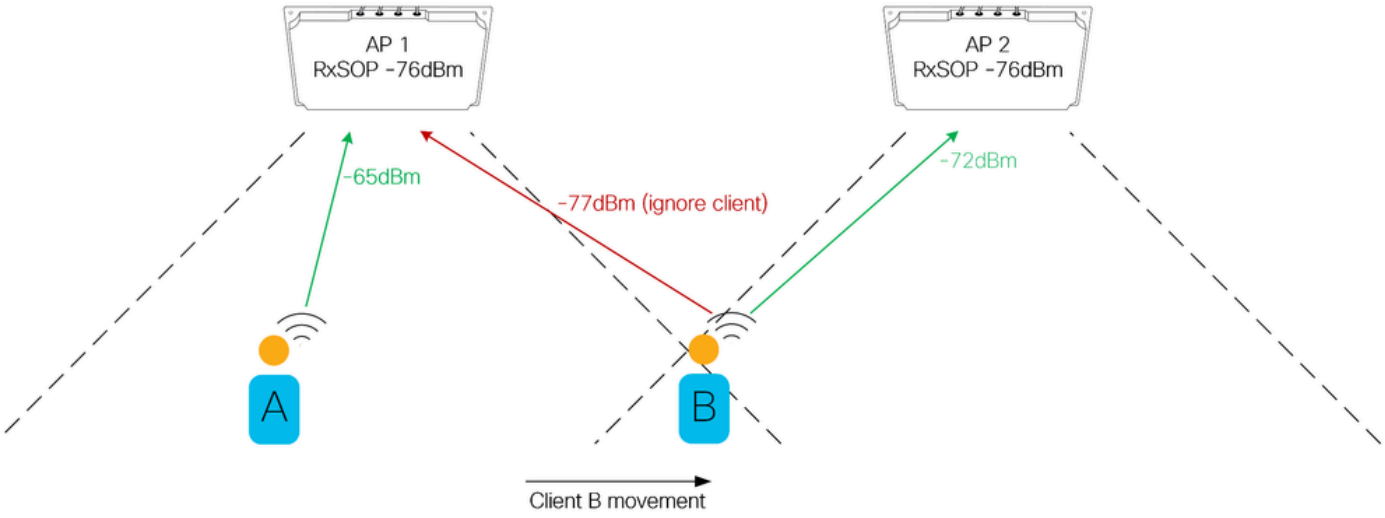
Spiegazione del concetto RxSOP

Il significato di RxSOP

RxSOP può essere utilizzato in più modi. Può essere utilizzato per migliorare la capacità dei punti di accesso di trasmettere in ambienti rumorosi, controllare la distribuzione dei client tra le antenne e ottimizzare per i client più deboli e appiccicosi.

Nel caso di ambienti rumorosi, ricordare che prima di trasmettere un frame 802.11 la stazione trasmittente (in questo caso l'access point) deve prima valutare la disponibilità del supporto, parte di questo processo è ascoltare per prima le trasmissioni che stanno già avvenendo. Negli ambienti Wi-Fi ad alta densità è comune per molti AP coesistere in uno spazio relativamente limitato, spesso utilizzando gli stessi canali. In ambienti con tale traffico elevato, l'access point può segnalare l'utilizzo dei canali da parte degli access point circostanti (incluse le riflessioni) e ritardare la propria trasmissione. Impostando la soglia RxSOP appropriata, l'access point può ignorare le trasmissioni più deboli (riduzione nell'utilizzo del canale percepito) che portano a opportunità di trasmissione più frequenti e prestazioni migliorate. Gli ambienti in cui i punti di accesso segnalano un utilizzo significativo dei canali (ad esempio > 10%) senza alcun carico del client (ad esempio un luogo vuoto) sono ottimi candidati per il tuning di RxSOP.

Per l'ottimizzazione client tramite RxSOP, considerare questo diagramma.



Roaming client interessato da rxsop

Nell'esempio vi sono due punti di accesso/antenne con aree di copertura ben definite. Il client B si sta spostando dall'area di copertura di AP1 all'area di copertura di AP2. Esiste un punto di crossover in cui AP2 sente il client meglio di AP1, ma il client non ha ancora effettuato il roaming verso AP2. Questo è un buon esempio di come l'impostazione della soglia RxSOP può applicare il limite dell'area di copertura. Garantire che i client siano sempre connessi all'access point più vicino migliora le prestazioni eliminando le connessioni client distanti e/o deboli gestite a velocità di trasferimento dati inferiori. Configurare le soglie RxSOP in questo modo richiede una comprensione approfondita di dove inizia e finisce l'area di copertura prevista di ogni access point.

I pericoli di RxSOP.

L'impostazione troppo aggressiva della soglia RxSOP provoca buchi di copertura, in quanto l'access point non decodifica le trasmissioni valide da dispositivi client validi. Questo può avere conseguenze negative per il cliente in quanto il punto di accesso non risponde; dopo tutto, se la trasmissione del client non è stata ascoltata non c'è motivo di rispondere. L'ottimizzazione delle soglie RxSOP deve essere eseguita con attenzione, assicurandosi sempre che i valori configurati non escludano i client validi all'interno dell'area di copertura. Notare che alcuni client potrebbero non rispondere bene ad essere ignorati in questo modo, impostazioni RxSOP troppo aggressive non danno al client una possibilità di roaming naturale, costringendo efficacemente il client a trovare un altro AP. Un client in grado di decodificare un beacon da un punto di accesso presuppone che sia in grado di trasmettere a tale punto di accesso, pertanto l'obiettivo del tuning RxSOP è quello di far corrispondere le dimensioni della cella di ricezione all'intervallo del beacon del punto di accesso. Tenere presente che un dispositivo client (valido) non sempre ha una linea diretta di visione verso il punto di accesso, il segnale è spesso attenuato da utenti rivolti verso l'antenna o che trasportano i loro dispositivi in sacchetti o tasche.

Configurazione di RxSOP

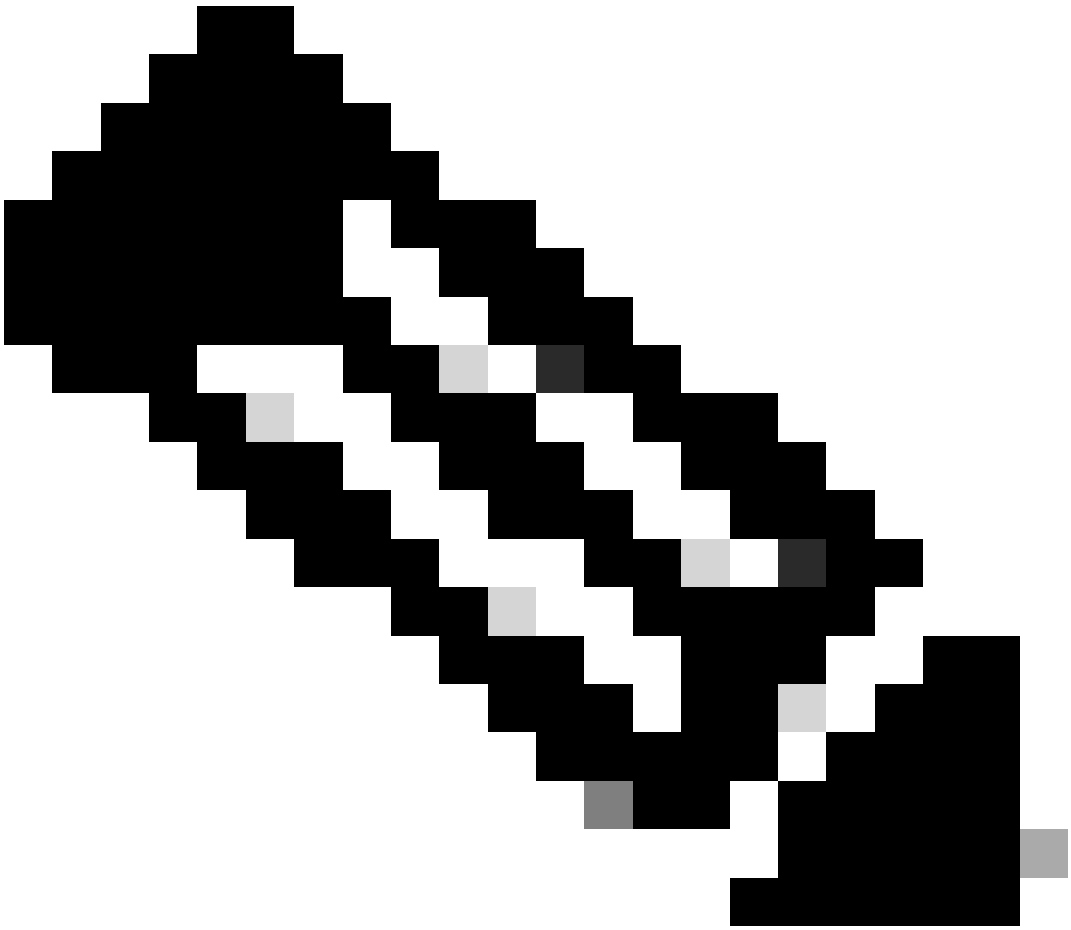
RxSOP è configurato per profilo RF.

Per ciascuna banda esistono soglie predefinite (Basso/Medio/Alto) che impostano un valore dBm predefinito. In questo caso si consiglia di utilizzare sempre valori personalizzati, anche se il valore desiderato è quello delle preimpostazioni disponibili, in modo da rendere la configurazione più

leggibile.

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

Tabella impostazioni RxSop



Nota: le modifiche RxSOP non richiedono un reset della radio e possono essere eseguite al volo.

Ridimensionamento della rete

In generale, utilizzare un dispositivo al massimo delle funzionalità documentate è una cattiva idea. Le schede di dati riportano la verità, ma i numeri citati possono essere in specifiche condizioni di attività. I controller wireless sono testati e certificati per supportare un determinato numero di client e access point e un determinato throughput, ma ciò non presuppone che i client siano in roaming ogni secondo, che sia possibile configurare ACL univoci e molto lunghi per ogni client o che siano state attivate tutte le funzionalità di snooping disponibili. È quindi importante considerare attentamente tutti gli aspetti per garantire che la rete sia scalabile durante le ore di punta e per mantenere un margine di sicurezza per la crescita futura.

Numero di access point

Una delle prime attività nell'implementazione di una rete è la definizione del budget e l'ordinazione della giusta quantità di apparecchiature, e il fattore variabile più grande è il numero e il tipo di punti di accesso e di antenne. Le soluzioni wireless devono sempre basarsi su un design a radiofrequenza, tuttavia (e purtroppo), molto spesso questo è il secondo passo del ciclo di vita del progetto. Nel caso di installazioni aziendali interne semplici, esistono numerose tecniche di stima che possono, a un livello ragionevole di certezza, prevedere quanti punti di accesso possono essere richiesti anche prima che un architetto wireless guardi i piani di pavimento. Anche i modelli di previsione possono essere molto utili in questo caso.

Per gli impianti più complessi, come quelli industriali, all'aperto, le grandi reti pubbliche, o dovunque siano necessarie antenne esterne, le semplici tecniche di stima sono spesso inadeguate. È necessario un certo livello di esperienza con precedenti impianti simili per stimare adeguatamente il tipo e la quantità di attrezzature necessarie. La visita di un architetto wireless è il minimo indispensabile per comprendere la disposizione di un complesso luogo o struttura.

In questa sezione vengono fornite linee guida per determinare il numero minimo di AP e di antenne per la distribuzione specificata. Le quantità finali e le posizioni di montaggio specifiche verranno sempre determinate mediante un processo di analisi dei requisiti e progettazione radio.

La distinta base iniziale deve essere basata su due fattori: il tipo di antenne e la quantità di antenne.

Tipo di antenne

Non ci sono scorciatoie. Il tipo di antenna è determinato dall'area da coprire e dalle opzioni di montaggio disponibili in quell'area. Non è possibile determinare questo senza una comprensione dello spazio fisico, questo significa che una visita in sito è richiesta da qualcuno con una comprensione delle antenne e dei loro modelli di copertura.

Quantità di antenne

La quantità di apparecchiature necessarie può essere ricavata dalla comprensione della quantità prevista di connessioni client.

Dispositivi per persona

Il numero di utenti umani può essere determinato dalla capacità di posti a sedere di un luogo, o dal numero di biglietti venduti, o dal numero previsto di visitatori sulla base di statistiche storiche. Ogni utente umano può trasportare più dispositivi ed è comune assumere più di un dispositivo per utente, anche se la capacità di un utente umano di utilizzare attivamente più dispositivi contemporaneamente è discutibile. Anche il numero di visitatori che si connettono attivamente alla rete dipende dal tipo di evento e/o di installazione.

Esempio 1: è normale che uno stadio da 80.000 posti non abbia 80.000 dispositivi collegati; questa percentuale è in genere significativamente inferiore. Le connessioni del 20% non sono un fenomeno insolito negli eventi sportivi, per esempio nello stadio da 80.000 posti a sedere il numero previsto di dispositivi collegati può essere 16.000 (80.000 x 20% = 16.000). Questo numero dipende anche dal meccanismo di caricamento utilizzato, se l'utente deve eseguire un'azione (ad esempio fare clic su un portale Web), i numeri saranno inferiori rispetto a quando l'accesso al dispositivo è automatico. L'onboarding automatico può essere semplice come un PSK che è stato ricordato da un evento precedente, o qualcosa di più avanzato come l'uso di OpenRoaming che onboard dispositivi senza interazione dell'utente. Le reti OpenRoaming possono spingere l'utente a prendere rapporti ben al di sopra del 50%, il che può avere un impatto significativo sulla pianificazione della capacità.

Esempio 2: è ragionevole aspettarsi che una conferenza tecnologica abbia un elevato rapporto di connessione degli utenti. I partecipanti alla conferenza trascorrono più tempo nella connessione alla rete e si aspettano di poter accedere alla posta elettronica ed eseguire attività quotidiane nel corso della giornata. È inoltre più probabile che questo tipo di utente connetta più di un dispositivo alla rete, anche se la possibilità di utilizzare più dispositivi contemporaneamente rimane discutibile. Per le conferenze tecnologiche, si presume che il 100% dei visitatori si connetta alla rete, ma questo numero può essere inferiore a seconda del tipo di conferenza.

In entrambi gli esempi, la chiave è capire il numero previsto di dispositivi connessi e non esiste un'unica soluzione per ogni rete pubblica di grandi dimensioni. In entrambi i casi, l'antenna è collegata a una radio e sono i dispositivi client (non gli utenti umani) che si connettono a tale radio. Pertanto, i dispositivi client per radio sono una metrica utilizzabile.

Dispositivi per radio

I Cisco AP hanno un numero massimo di client pari a 200 dispositivi connessi per radio per i 6 AP Wi-Fi e a 400 dispositivi per radio per i 6 AP Wi-Fi. Tuttavia, non è consigliabile progettare per il numero massimo di client. Per motivi di pianificazione, si consiglia di mantenere il numero di client per radio ben al di sotto del 50% della capacità massima dell'access point. Inoltre, il numero di radio dipende dal tipo di punto di accesso e antenna utilizzati, la sezione relativa a 5 GHz singolo e doppio esamina questo in modo più dettagliato.

In questa fase è consigliabile suddividere la rete in aree distinte, con un numero di dispositivi previsto per area. Tenere presente che in questa sezione si intende stimare un numero minimo di

punti di accesso e di antenne.

Si consideri un esempio di tre aree di copertura distinte, il numero di client previsto viene fornito per ogni area e un valore (integro) di 75 client per radio viene utilizzato per stimare il numero di radio richieste.

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

Conteggio previsto radio/client per area

Questi numeri iniziali devono ora essere combinati con la comprensione di quali tipi di access point e antenne sono implementati in ciascuna area e se viene utilizzato uno o due 5GHz. I calcoli a 6 GHz seguono la stessa logica dei 5 GHz. In questo esempio non si tiene conto dei 2,4 GHz.

Si supponga che ognuna delle tre aree utilizzi una combinazione di antenna patch 2566P e antenna stadio 9104, con una combinazione di single e dual 5GHz - questo scenario è utilizzato a scopo illustrativo.

Area	Total Radios	2566P (Dual 5GHz)	2566P (Single 5GHz)	9104 (Dual 5GHz)
Area 1	14	0	6	4
Area 2	27	6	3	6
Area 3	34	7	0	10
Total Antennas		26	9	20
Total APs		13	9	0 (integrated)

Antenne per area

In ogni area sono elencati i tipi di antenne e punti di accesso necessari. Notare che nel caso di 5 GHz doppi il rapporto è di due antenne per un punto di accesso.

In questa sezione viene illustrato un approccio per stimare il numero iniziale di antenne e punti di accesso necessari per un'installazione. La stima richiede la comprensione delle aree fisiche, delle possibili opzioni di montaggio in ciascuna area, del tipo di antenne da utilizzare in ciascuna area e del numero di dispositivi client previsti.

Ogni installazione è diversa e spesso sono necessarie apparecchiature aggiuntive per coprire aree specifiche o problematiche. Questo tipo di stima considera solo la capacità del cliente (non la copertura) e serve a delineare la scala dell'investimento necessario. Il posizionamento finale di punti di accesso/antenna e il totale delle apparecchiature sono sempre soggetti a una conoscenza approfondita del caso di utilizzo e alla verifica in loco da parte di un professionista wireless esperto.

Throughput previsto

Ciascun canale wireless può offrire una quantità di capacità disponibile che in genere si traduce in throughput. Questa capacità è condivisa tra tutti i dispositivi connessi alla radio, il che significa che le prestazioni per ogni utente diminuiscono man mano che vengono aggiunte ulteriori connessioni alla radio. Questo calo delle prestazioni non è lineare e dipende anche dall'esatto mix di client collegati.

Le funzionalità client variano a seconda del chipset client e del numero di flussi spaziali supportati dal client. Nella tabella seguente sono elencate le velocità massime dei dati client per ogni numero di flussi spaziali supportati.

Client Capability	20MHz channel Wi-Fi 5 (802.11ac)	20MHz channel Wi-Fi 6 (802.11ax)
1 Spatial Stream(s)	86.7Mbps	121.9Mbps
2 Spatial Stream(s)	173.3Mbps	243.8Mbps
3 Spatial Stream(s)	288.9Mbps	365.6Mbps
4 Spatial Stream(s)	346.7Mbps	487.5Mbps

Throughput reale massimo previsto per ogni tipo di client

Le velocità elencate sono velocità teoriche massime MCS (Modulation and Coding Scheme) derivate dallo standard 802.11 e presuppongono un rapporto segnale-rumore (SNR) >30dBm. L'obiettivo principale delle reti wireless a elevate prestazioni è quello di raggiungere questo livello di SNR per tutti i client in tutte le località, anche se questo accade raramente. Le reti wireless sono di natura dinamica e utilizzano frequenze senza licenza, varie interferenze non controllate hanno

un impatto sul servizio SNR del client, oltre a capacità del client.

Anche nei casi in cui viene raggiunto il livello richiesto di SNR, le velocità elencate in precedenza non considerano il sovraccarico del protocollo, quindi non mappano direttamente al throughput reale (misurato da vari strumenti di test della velocità). Il mondo reale nel suo complesso è sempre più basso del tasso MCS.

Per tutte le reti wireless (incluse le reti pubbliche di grandi dimensioni), la velocità di trasmissione dei client dipende sempre da:

- Capacità del client.
- Rapporto S/N del client in un determinato momento.
- Numero di altri client connessi nello specifico point in time.
- Capacità di altri client in quel determinato momento.
- Attività di altri client in quel momento specifico.
- Interferenza in quel momento specifico.

In base alla variabilità di questi fattori, non è possibile garantire un minimo per client in tutto per le reti wireless, indipendentemente dal fornitore dell'apparecchiatura.

Per ulteriori informazioni, fare riferimento alla Convalida del throughput Wi-Fi: Guida al test e al monitoraggio.

Piattaforma WLC

Scegliere la piattaforma WLC può sembrare facile. La prima cosa a cui si può pensare è esaminare il numero stimato di punti di accesso e di client che si intende gestire. Il data sheet per ciascuna piattaforma WLC contiene tutti i massimi oggetti supportati sulla piattaforma: ACL, conteggio dei client, tag del sito e così via. Questi sono numeri letterali massimi e spesso ci sono delle regole severe. Ad esempio, non è possibile unire 6001 AP a 9800-80 che supporta solo 6000 AP. Ma è saggio puntare al massimo dappertutto?

I controller wireless Cisco vengono testati per essere in grado di raggiungere questi valori massimi, ma non possono necessariamente raggiungere tutti i valori massimi documentati in tutte le condizioni contemporaneamente. Prendiamo l'esempio del throughput, un 9800-80 può raggiungere fino a 80 Gb/s di inoltro dati client, ma questo è il caso in cui ogni pacchetto client ha la dimensione massima e ottimale di 1500 byte. Con una combinazione di dimensioni dei pacchetti, il throughput massimo effettivo è inferiore. Se si abilita la crittografia DTLS, la velocità effettiva viene ulteriormente ridotta e lo stesso vale per la visibilità delle applicazioni. È ottimistico aspettarsi più di 40 Gbps su un 9800-80 in condizioni realistiche su una rete di grandi dimensioni con molte funzionalità abilitate. Poiché questa impostazione varia notevolmente a seconda delle funzionalità in uso e del tipo di attività di rete, l'unico modo per avere un'idea reale della capacità è misurare l'utilizzo del datapath utilizzando questo comando. Focalizzare l'attenzione sulla metrica di carico, che è una percentuale del throughput massimo che il controller può inoltrare.

```
WLC#show platform hardware chassis active qfp datapath utilization summary
```

```
  CPP 0:                    5 secs        1 min        5 min       60 min

Input:     Total (pps)            9            5            5            8

                  (bps)        17776         7632         9024        10568

Output:    Total (pps)            5            3            3            6

                  (bps)        11136        11640        11440        41448

Processing: Load (pct)            0            0            0            0


WLC#
```

Analogamente, il 9800-80 è in grado di gestire perfettamente 6000 punti di accesso con attività regolare. Tuttavia, 6000 punti di accesso in un luogo pubblico come uno stadio o un aeroporto non sono considerati attività regolari. Considerando la quantità di roaming dei client e di richieste ambientali, reti pubbliche di grandi dimensioni su scala massima possono causare un maggiore utilizzo della CPU su un singolo WLC. Se si aggiungono monitoraggio e trap SNMP da inviare ogni volta che i client si spostano, il carico può rapidamente diventare eccessivo. Una delle caratteristiche principali di un evento pubblico di grandi dimensioni è la presenza di un numero molto maggiore di eventi di caricamento client man mano che le persone si spostano e si associano/dissociano costantemente, il che produce una maggiore pressione sulla CPU e sul control plane.

Numerose implementazioni hanno dimostrato che una singola coppia (HA) di controller wireless 9800-80 può gestire un'installazione in un grande stadio con oltre 1000 punti di accesso. È inoltre comune distribuire i punti di accesso su due o più coppie di controller per eventi critici in cui il tempo di attività e la disponibilità sono problemi primari. Quando le reti di grandi dimensioni vengono distribuite su più WLC, l'ulteriore complessità del roaming tra controller comporta che il roaming dei client debba essere considerato attentamente in spazi limitati, come ad esempio nelle bocce degli stadi.

Vedere anche la sezione Site Tag in questo documento.

WLC High-Availability

Si consiglia di utilizzare una coppia di switch stateful over (HA SSO) ad alta disponibilità, che fornisce ridondanza hardware ma protegge anche da errori software. Utilizzando HA SSO, un blocco del software su un dispositivo è trasparente per gli utenti finali, in quanto il WLC secondario assume il controllo senza interruzioni. Un altro vantaggio di una coppia HA SSO è rappresentato dagli aggiornamenti hitless offerti dalla funzionalità di aggiornamento software in-service (ISSU).

Se la rete è abbastanza grande, si consiglia anche di utilizzare un controller aggiuntivo (N+1). Può servire a diversi scopi che l'SSO HA non è in grado di soddisfare. È possibile testare una nuova versione del software su questo WLC prima di aggiornare la coppia di produzione (e migrare solo alcuni punti di accesso di prova per testare una sezione specifica della rete). Alcune rare

condizioni possono influire su entrambi i WLC in una coppia HA (quando il problema viene replicato in standby) e qui il N+1 consente di avere un WLC sicuro in uno scenario attivo-attivo in cui è possibile eseguire la migrazione progressiva da e verso gli AP. Può anche servire come controller di provisioning per configurare i nuovi access point.

I 9800-CL sono molto scalabili e potenti. È da notare che hanno una capacità di inoltro dati molto più ridotta (da 2 Gbps a 4 Gbps per l'immagine SR-IOV) che tende a limitarli agli scenari di switching locale FlexConnect (e forse un piccolo numero di punti di accesso nello switching centrale). Possono tuttavia essere utili come dispositivi N+1 quando sono necessari controller aggiuntivi durante un intervento di manutenzione o per la risoluzione di un problema.

Sistemi esterni

Anche se questo documento si concentra principalmente sul componente wireless di grandi reti di eventi, ci sono anche numerosi sistemi di supporto che devono essere presi in considerazione durante la fase di scalabilità e progettazione, alcuni di questi sono discussi qui.

Rete principale

Le reti wireless di grandi dimensioni vengono in genere implementate in modalità di commutazione centrale e con subnet di grandi dimensioni. Ciò implica che un numero molto elevato di indirizzi MAC client e voci ARP viene trasferito all'infrastruttura cablata adiacente. È fondamentale che i sistemi adiacenti dedicati alle varie funzioni L2 e L3 dispongano delle risorse adeguate per gestire questo carico. Nel caso degli switch L2, una configurazione comune è la regolazione del modello Switch Device Manager (SDM), responsabile dell'allocazione delle risorse di sistema, che bilancia le funzionalità L2 e L3 a seconda della funzione del dispositivo all'interno della rete. È importante verificare che i dispositivi L2 di base possano supportare il numero di voci di indirizzi MAC previsto.

NAT gateway

Il caso di utilizzo più comune delle reti pubbliche è quello di fornire l'accesso a Internet ai visitatori. In qualsiasi punto del percorso dati deve essere presente un dispositivo responsabile della traduzione NAT/PAT. I gateway Internet devono disporre delle risorse hardware e della configurazione del pool IP necessarie per gestire il carico. Ricorda che un singolo dispositivo client wireless può essere responsabile di numerose traduzioni NAT/PAT.

DNS/DHCP

Questi due sistemi sono fondamentali per garantire una buona esperienza ai clienti. I servizi DNS e DHCP richiedono non solo la scalabilità appropriata per gestire il carico, ma anche considerazioni relative al posizionamento all'interno della rete. I sistemi veloci e reattivi, posizionati nella stessa posizione del WLC, garantiscono un'esperienza ottimale ed evitano lunghi tempi di caricamento dei client.

AAA/portale Web

A nessuno piace una pagina Web lenta, la scelta di un sistema appropriato e ben scalato per

l'autenticazione Web esterna è importante per una buona esperienza di caricamento del client. Analogamente, i server di autenticazione RADIUS devono essere in grado di gestire le richieste del sistema wireless. Tenete presente che in alcuni casi il carico può impennarsi durante i momenti chiave, ad esempio l'intervallo di tempo durante una partita di calcio, che può generare un carico di autenticazione elevato in una piccola quantità di tempo. È fondamentale scalare il sistema per un carico concorrente adeguato. È necessario prestare particolare attenzione quando si utilizzano funzioni quali la contabilità AAA. Evitare la contabilità basata sul tempo a tutti i costi e se si utilizza la contabilità provare a disabilitare la contabilità provvisoria. Un altro elemento importante da considerare è l'uso dei load balancer, in cui i meccanismi di ping delle sessioni devono essere utilizzati per garantire flussi di autenticazione completi. Assicurarsi di mantenere il timeout RADIUS a 5 secondi o superiore.

Se si utilizza un SSID 802.1X con un numero elevato di client (ad esempio con OpenRoaming), assicurarsi di abilitare 802.11r Fast Transition (FT), altrimenti i client possono causare un problema di autenticazione ogni volta che eseguono il roaming.

DNS/DHCP

Alcuni consigli per DHCP:

- Verificare che il pool DHCP sia almeno il triplo del numero di client previsto. Gli indirizzi IP rimangono assegnati anche dopo la disconnessione del client, quindi a seconda del tempo di permanenza degli ospiti questo può consumare più indirizzi IP. Cercare di far corrispondere la durata del lease alla durata prevista della visita dell'utente, non ha senso allocare un indirizzo IP per una settimana se la durata tipica della visita è di due ore, in modo da eliminare i lease non più validi.
- Si consiglia di utilizzare un'unica subnet grande per i client, il WLC ha una funzione ARP proxy e non inoltra le trasmissioni per impostazione predefinita (diversa da DHCP). L'utilizzo di una subnet client di grandi dimensioni (ad esempio /16) per i client non rappresenta un problema. Una singola VLAN di grandi dimensioni è più semplice rispetto a un gruppo VLAN con molte VLAN. La configurazione di molte subnet più piccole (ad esempio /24) e di gruppi di VLAN non influenza il dominio di broadcast e comporta solo una configurazione più complessa, che comporta problemi come le VLAN modificate e la necessità di tenere traccia di vari pool DHCP che non possono essere utilizzati uniformemente.
- Mantenere DHCP in modalità bridging sul controller wireless con la funzionalità di inoltro DHCP gestita dal gateway di layer 3 della subnet. Ciò consente la massima efficienza e semplicità. L'idea è di non coinvolgere per niente il controller wireless nel processo DHCP.
- Usa DHCP obbligatorio su qualsiasi rete WLAN pubblica, indipendentemente dal metodo di autenticazione. Sebbene ciò possa attivare una piccola percentuale di associazioni client non riuscite, potrebbe evitare problemi significativi di sicurezza sia quando i client tentano di assegnarsi indirizzi IP statici sia quando si comportano in modo errato e tentano di riutilizzare un indirizzo IP precedente senza autorizzazione.

Funzionamento della rete

La giusta configurazione

È invitante consentire un sacco di opzioni per trarre vantaggio da tutte le più recenti caratteristiche del Wi-Fi moderno. Alcune funzionalità, tuttavia, sono ideali per ambienti di piccole dimensioni, ma hanno un impatto notevole in ambienti di grandi dimensioni e ad alta densità. Analogamente, alcune funzionalità possono causare problemi di compatibilità. Anche se le apparecchiature Cisco rispettano tutti gli standard e offrono compatibilità con un'ampia varietà di client testati, nel mondo sono presenti dispositivi client unici che talvolta dispongono di versioni software dei driver con bug o incompatibilità con alcune funzionalità.

A seconda del livello di controllo che si ha sui client, è necessario essere conservatori. Ad esempio, se si distribuisce il Wi-Fi per il grande raduno annuale della propria azienda, si sa che la maggior parte dei client sono dispositivi aziendali e si può pianificare il set di funzionalità per abilitarlo di conseguenza. D'altra parte, se si gestisce un aeroporto Wi-Fi, il livello di soddisfazione degli ospiti è direttamente correlato alla loro capacità di connettersi alla rete e non si dispone di alcun controllo sui dispositivi client che gli utenti possono utilizzare.

SSID

Quanti SSID?

Si è sempre consigliato di utilizzare il minor numero di SSID possibile. Ciò si aggrava nelle reti ad alta densità poiché la possibilità di avere più access point sullo stesso canale è quasi garantita. In genere, molte distribuzioni utilizzano troppi SSID. Riconoscere di avere troppi SSID, ma dichiarare che non possono utilizzarne di meno. È necessario eseguire uno studio tecnico e aziendale per ogni SSID per comprendere le analogie tra gli SSID e le opzioni per la compressione di più SSID in uno solo.

Analizziamo alcuni tipi di sicurezza/SSID e il loro utilizzo.

WPA2/3 Personale

Grazie alla sua semplicità, un SSID con chiave già condivisa è estremamente diffuso. È possibile stampare la chiave da qualche parte su badge o su carta oppure firmarla o comunicarla in qualche modo ai visitatori. A volte è preferibile un SSID chiave già condiviso anche per un SSID ospite (a condizione che la chiave sia ben nota a tutti i partecipanti). Consente di evitare l'esaurimento del pool DHCP a causa della natura intenzionale della connessione. I dispositivi che passano non si connettono automaticamente alla rete, pertanto non sono in grado di utilizzare un indirizzo IP del pool DHCP.

WPA2 PSK non garantisce la privacy in quanto il traffico può essere facilmente decrittografato poiché tutti utilizzano la stessa chiave. Al contrario, WPA3 SAE garantisce la privacy e, anche se tutti dispongono della chiave master, non è possibile derivare la chiave di crittografia utilizzata da altri client.

WPA3 SAE è la scelta migliore per la sicurezza e molti smartphone, notebook e sistemi operativi lo supportano. Alcuni dispositivi IoT o smart wearables possono ancora avere un supporto limitato e i client meno recenti in generale sono soggetti a problemi se non hanno ricevuto i driver o gli aggiornamenti del firmware recenti.

Per semplificare le operazioni, può essere utile prendere in considerazione una modalità di transizione WPA2 PSK-WPA3 SAE SSID, ma è stato dimostrato nel campo che ciò causa alcuni problemi di compatibilità. I client non programmati correttamente non si aspettano due tipi di metodi con chiave condivisa sullo stesso SSID. Se si desidera offrire entrambe le opzioni WPA2 e WPA3, si consiglia di configurare SSID separati.

WPA2/3 Enterprise

WPA3 Enterprise (con crittografia AES a 128 bit) è tecnicamente lo stesso metodo di sicurezza (almeno come annunciato nei beacon SSID) di WPA2 Enterprise, che assicura la massima compatibilità.

Per 802.1X, si consiglia una modalità di transizione SSID in quanto i problemi di compatibilità non vengono rilevati con i dispositivi recenti (i problemi sono stati segnalati con Android 8 o versioni precedenti di Apple IOS). IOS XE 17.12 e versioni successive consentono di avere un singolo Transition Enterprise SSID in cui solo WPA3 viene utilizzato e pubblicizzato su 6 GHz, mentre WPA2 è disponibile come opzione sulla banda a 5 GHz. È consigliabile abilitare WPA3 sugli SSID aziendali il prima possibile.

Gli SSID aziendali WPA possono essere utilizzati per gli utenti chiave per i quali esiste un database del provider di identità che consente di restituire parametri AAA (ad esempio VLAN o ACL) a seconda dell'identità dell'utente. Questi tipi di SSID possono includere l'eduroam o l'OpenRoaming, che combinano i vantaggi degli SSID ospiti (consentendo ai visitatori di connettersi facilmente senza immettere credenziali) con la sicurezza di un SSID aziendale. Riducono notevolmente la complessità dell'onboarding tipicamente associato con 802.1X in quanto i client non devono fare nulla per aderire a eudroam o OpenRoaming SSID, a condizione che abbiano un profilo sul loro telefono (che può essere facilmente fornito attraverso un'app di eventi)

SSID guest

Un SSID guest è spesso sinonimo di autenticazione aperta. È possibile aggiungere un portale Web (o meno) dietro di esso (a seconda della facilità di utilizzo desiderata o dei requisiti locali) nelle sue varie forme: autenticazione Web esterna, locale o centrale, ma il concetto rimane lo stesso. Quando si utilizza un portale guest, la scalabilità può rapidamente diventare un problema in ambienti di grandi dimensioni. Per ulteriori informazioni su questo argomento, vedere la sezione Configurazione della scalabilità.

Per le operazioni a 6 GHz è necessario che il SSID guest utilizzi l'apertura avanzata anziché solo l'apertura. Ciò consente a chiunque di connettersi, ma fornisce privacy (una privacy migliore persino di WPA2-PSK!) e crittografia, il tutto senza fornire alcuna chiave o credenziali quando ci si connette all'SSID. I principali fornitori di smartphone e sistemi operativi supportano ora Enhanced Open, ma il supporto non è ancora diffuso nella base di client wireless. La modalità di transizione Apertura avanzata fornisce una buona opzione di compatibilità in cui i dispositivi compatibili si connettono all'SSID guest crittografato (utilizzando Apertura avanzata) e i dispositivi non compatibili utilizzano ancora l'SSID come se fosse semplicemente aperto. Benché gli utenti finali notino solo un SSID, questa modalità di transizione trasmette due SSID nei beacon (sebbene ne

sia visibile solo uno).

In eventi e luoghi di grandi dimensioni, si consiglia spesso di configurare una chiave PSK sull'SSID guest anziché lasciarla completamente aperta (la modalità Enhance Open Transition sarebbe migliore, ma ciò crea due SSID e la compatibilità con i client deve ancora essere ampiamente dimostrata). Sebbene ciò renda l'onboarding un po' più complicato (è necessario stampare il PSK sui badge o i biglietti delle persone o pubblicizzarlo in qualche modo), evita che i client occasionali si connettano automaticamente alla rete senza che l'utente finale abbia alcuna intenzione di utilizzare la rete. Un numero sempre maggiore di fornitori di sistemi operativi mobili riduce inoltre le priorità delle reti aperte e visualizza un avviso di protezione. In altre situazioni, si può desiderare un numero massimo di passanti per connettersi e quindi aperto è la scelta migliore.

Conclusione sul numero di SSID

Non può esserci una risposta soddisfacente alla domanda su quanti SSID bisogna rispettare. L'effetto dipende dalla velocità dati minima configurata, dal numero di SSID e dal numero di AP che trasmettono sullo stesso canale. In un grande evento Cisco, l'infrastruttura wireless ha utilizzato 5 SSID: il PSK WPA2 principale, un SSID WPA 3 SAE per la sicurezza e la copertura a 6 GHz, un SSID Eduroam aziendale per la facilità di accesso per i partecipanti all'istruzione, un SSID OpenRoaming per dare il benvenuto in modo sicuro a chiunque abbia configurato il Wi-Fi dall'app dell'evento e un SSID 802.1X separato per il personale e l'accesso alla rete dell'amministratore. Questo era già quasi troppo, ma l'effetto è rimasto ragionevole grazie al gran numero di canali disponibili, e le antenne direzionali utilizzate per ridurre la sovrapposizione dei canali il più possibile.

I concetti di SSID legacy e SSID principale

Per un certo periodo, è stato consigliato di limitare il servizio a 2,4 GHz a un SSID separato "legacy" pubblicizzato solo in 2,4 GHz. Questa pratica sta diventando sempre meno popolare in quanto le persone smettono completamente di fornire il servizio a 2,4 GHz. Tuttavia, l'idea può e deve persistere, ma con altri concetti. Si desidera implementare il SAE WPA3, ma la modalità di transizione genera problemi di compatibilità con i client? Disporre di un SSID "legacy" WPA2 e di un SSID SAE WPA3 principale. Denominando il SSID con le prestazioni meno elevate "legacy" non attira i client e si è in grado di individuare facilmente il numero di client che ancora presentano problemi di compatibilità con il SSID principale e che richiedono questo SSID legacy.

Ma perché fermarsi qui? Si è sentito dire che 802.11v ha causato problemi con alcuni client meno recenti o che ad alcuni driver client non piace vedere l'analisi dei dispositivi abilitata su SSID? Abilitare tutte queste utili funzionalità sul SSID principale avanzato e lasciarle spente sul SSID legacy/compatibilità. In questo modo è possibile testare l'implementazione delle nuove funzionalità nell'SSID principale, fornendo al contempo un SSID di compatibilità massimo a cui i client possono tornare. Questo sistema funziona solo in questo modo. Se si utilizza il nome opposto al SSID basato sulla compatibilità come principale e si assegna un nome all'SSID avanzato, ad esempio "<nome>-WPA3", si noteranno persone che si attengono al SSID precedente a cui erano abituati e l'adozione di questo nuovo SSID è rimasta ridotta per molti anni. L'implementazione di nuove

impostazioni o funzionalità ha quindi risultati inconcludenti a causa del minor numero di client che si connettono.

Funzioni SSID

- È consigliabile mantenere disabilitate le estensioni di Aironet. Queste funzionalità sono particolarmente utili per le indagini del sito e le operazioni WGB, ma talvolta causano problemi con alcuni client legacy. Aironet IE inoltre annuncia il nome host dell'access point che non è richiesto nelle installazioni sicure.
- La CCKM è un protocollo deprecato (a favore di FT) e deve essere disabilitata.
- Al momento, è preferibile utilizzare la crittografia AES-128, anche in WPA3 a causa del basso supporto dei client per la crittografia più elevata (a meno che non ci si possa permettere un SSID specifico più sicuro e restrittivo)
- Il rilevamento dei fori di copertura è meglio disabilitato (per tutti gli SSID). Le implementazioni di grandi dimensioni utilizzano in genere antenne direzionali, che richiedono un'indagine approfondita del sito. I livelli di potenza di ciascuna antenna sarebbero il risultato del processo di progettazione RF e in genere configurati su livelli specifici.
- Il FT adattivo deve essere disabilitato in quanto alcuni client possono avere problemi quando il FT non è completamente annunciato ma è presente in alcuni attributi. Disabilitare completamente FT (per la massima compatibilità) o utilizzare FT+802.1X che è supportato dalla maggior parte dei client (a meno che non siano più orientati all'IoT). Quando si configura FT+802.1X, anche i client non FT possono unirsi all'SSID. L'unico problema possibile è con alcuni client che non tollerano la visualizzazione di due opzioni di sicurezza sullo stesso SSID.
- Disabilitare 802.11ac MU-MIMO. Aggiunge complessità e offre vantaggi minimi in 802.11ac.
- Disabilitare l'ora di riattivazione della destinazione BSS. Attualmente è poco adottata sul lato client.
- Disabilitare il bilanciamento del carico aggressivo e la selezione della banda. La selezione della banda non è necessaria se non si annuncia il SSID a 2,4 GHz (o se si trova su un SSID dedicato) e l'associazione aggressiva del client con bilanciamento del carico ritarda l'associazione rifiutando il client un paio di volte prima di accettarlo definitivamente se insiste per la connessione a un punto di accesso caricato. I punti di accesso sono stati comunque caricati in un ambiente occupato e questo è negativo per l'esperienza del client.
- Disabilitare Fastlane+.
- Disabilitare Universal Admin. Questa funzionalità era disponibile per l'access point 3700 e solo nel dominio -UX. Lasciandolo su lascia aperto un inutile vettore di attacco.
- Mantenere abilitata la memorizzazione nella cache delle chiavi opportunistiche (OKC). Funge da meccanismo di roaming veloce per i client che non supportano FT.
- Non consentire WMM. La disattivazione di questa funzionalità riporterebbe la rete all'era 802.11g e la sua richiesta non apporterebbe alcun vantaggio sulla piattaforma 9800.
- Abilitare IP Source Guard.
- Disabilita profilatura RADIUS. In un ambiente molto occupato, questo può inviare un numero eccessivo di messaggi di accounting RADIUS (ogni volta che i client eseguono DHCP o inviano pacchetti HTTP) ed è potenzialmente in grado di sovraccaricare il server RADIUS.
- Evitare di utilizzare SSID nascosti. In questo modo non è necessario alcun scopo di protezione, il nome SSID può comunque essere individuato facilmente con applicazioni

semplici o acquisendo tramite sniffer. Nascondere l'SSID rallenta il roaming di tutti i client in quanto non traggono più vantaggio dalla scansione del beacon passivo e devono fare affidamento sulla scansione attiva per ottenere le informazioni dell'access point adiacente.
- Provare a non utilizzare più di quattro WLAN per radio, in quanto influisce in modo significativo sull'utilizzo della RF. L'uso di cinque reti WLAN non è un limite insuperabile, ma consente di tenere ben presente lo spreco di tempo di trasmissione dovuto all'uso di un numero sempre maggiore di WLAN.
- 802.11v e 802.11k sono standard sempre più supportati da tipi di client comuni. In genere non costituiscono un problema per quanto riguarda la connessione del client. I vantaggi che apportano dipendono in larga misura dal modo in cui i client utilizzano tali protocolli e possono talvolta (nel caso di 802.11k) causare un utilizzo leggermente più elevato della CPU. È possibile tenerli fuori dall'IoT o dall'SSID legacy, ma devono essere abilitati se possibile sull'SSID di produzione.

Tag sito

I tag del sito sono un elemento di configurazione che consente di raggruppare i punti di accesso che condividono le stesse impostazioni FlexConnect e le impostazioni del profilo di join AP (ad esempio credenziali, dettagli SSH e codice del paese). Perché i tag del sito sono importanti? I tag del sito definiscono inoltre il modo in cui i punti di accesso vengono gestiti dal processo WNCD all'interno di Catalyst 9800. Ecco alcuni esempi da illustrare:

- Se si configurano quattro tag di sito in un 9800-80 che dispone di otto processi WNCD, ogni tag di sito viene assegnato a un processo WNCD diverso (in esecuzione su un core CPU separato) e quattro processi WNCD non eseguono alcuna operazione. Ciò significa che non si utilizzano tutte le CPU del modello 9800-80 e non si consiglia di caricarlo con il massimo di 6000 punti di accesso supportati.

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

Primo esempio di bilanciamento dei tag del sito

- Se si configurano 10 tag laterali su un 9800-80 che dispone di otto processi WNCD, due processi WNCD si occupano di due tag sito ciascuno, mentre gli altri sei gestiscono un tag sito ciascuno.

Site tag 1 Site tag 9	Site tag 2 Site tag 10	Site tag 3	Site tag 4	Site tag 5	Site tag 6	Site tag 7	Site tag 8
WNCD 1	WNCD 2	WNCD 3	WNCD 4	WNCD 5	WNCD 6	WNCD 7	WNCD 8
CPU	CPU	CPU	CPU	CPU	CPU	CPU	CPU

Secondo esempio di bilanciamento dei tag del sito

Per distribuzioni di grandi dimensioni geografiche con molti siti e molti tag sito, il numero di tag sito è un multiplo del numero di processi WNCD sulla piattaforma in uso.

Tuttavia, per le reti di eventi che si trovano generalmente sotto un unico tetto o in più edifici nello stesso luogo, si consiglia di far corrispondere il numero di tag del sito al numero esatto di WNCD sulla piattaforma in questione. L'obiettivo finale è che ogni processo WNCD (e quindi ogni core CPU allocato alle attività wireless) gestisca un numero approssimativamente simile di eventi di roaming client in modo che il carico sia bilanciato tra tutti i core CPU.

Platform type	Number of WNCD processes
9800-CL small OVA	1
9800-CL medium OVA	3
9800-CL large OVA	7
9800-L	1
9800-40/CW9800-M	5
9800-80/CW9800-H	8

Numero di processi WNCD per ogni tipo di piattaforma

In sostanza, è importante raggruppare i punti di accesso che si trovano nella stessa area fisica nello stesso tag di sito, in modo che gli eventi di roaming dei client frequenti tra questi punti di accesso rimangano nello stesso processo CPU. Ciò significa che, anche se si dispone di un singolo spazio di grandi dimensioni, si consiglia di dividere il luogo in diversi tag sito (quanti ne sono i processi WNCD che gestiscono il luogo) e raggruppare i punti di accesso nel modo più logico possibile in questi per formare gruppi di vicinato RF logici che sono anche equamente distribuiti tra i tag sito.

A partire da IOS XE 17.12, è possibile abilitare un algoritmo di bilanciamento del carico in modo che il WLC raggruppi gli AP in base alla loro vicinanza RF. In questo modo il carico di lavoro non sarà più necessario e si creerà una distribuzione equilibrata degli access point nel processo WNCD. Ciò può essere utile se non è possibile disegnare facilmente gruppi di access point adiacenti da posizionare nella quantità corretta di tag del sito. Una specificità di questo algoritmo è

che assegna gli access point al processo WNCD indipendentemente dall'assegnazione dei tag di sito, ovvero non modifica l'assegnazione dei tag di sito dell'access point. È quindi possibile assegnare tag di sito puramente di base in una logica di configurazione e consentire all'algoritmo di bilanciare i punti di accesso tra le CPU nel modo ottimale.

La funzione di bilanciamento automatico del carico basata su RF è documentata in Cisco Catalyst serie 9800 Wireless Controller Software Configuration Guide, Cisco IOS XE Dublin 17.12.x.

L'utilizzo della CPU dei processi WNCD deve essere monitorato durante eventi di grandi dimensioni. Se uno o più processi WNCD mostrano un utilizzo elevato, è possibile che WNCD gestisca troppi punti di accesso o client o che i punti di accesso o i client che gestisce siano più occupati della media (se tutti girano costantemente, ad esempio in un aeroporto).

Profilo criterio

- Abilitare ARP e il proxy DAD (Duplicate Address Detection). In questo modo il WLC può rispondere per conto dei client wireless quando un dispositivo sta tentando di apprendere l'indirizzo MAC di un dispositivo wireless. Ciò consente inoltre di risparmiare le batterie dei client wireless.
- Non abilitare le funzionalità WGB se non necessario.
- Abilitare DHCP necessario per evitare client con indirizzi IP statici.
- Mantieni timeout di inattività breve (300 secondi). Alcuni amministratori impiegano molto tempo per evitare che i client debbano ripetere l'autenticazione, ma il timeout di inattività prolungato comporta voci client fantasma (che influiscono sulla creazione di report), in quanto il conteggio dei client viene ritardato dal tempo reale. È consigliabile mantenere il timeout di inattività inferiore al timer di rotazione della chiave di gruppo per evitare che si verifichino problemi di accounting quando i client vengono eliminati. L'intervallo di rotazione della chiave di gruppo può essere configurato nell'interfaccia utente Web in Configurazione > Sicurezza > EAP avanzato come "Intervallo chiave di trasmissione EAP"
- Impostare il timeout della sessione su 86400 secondi per evitare disconnessioni e riautenticazioni non necessarie.

Profilo di join AP

- Verificare che il parametro TCP adjust MSS sia abilitato.
- Abilitare il DSCP di attendibilità a monte. Molti client wireless non eseguono il tagging 802.11e WMM UP. Sfortunatamente, considerare attendibile il campo DSCP è un modo sicuro per fornire la giusta priorità alle applicazioni vocali.
- Abilitare Syslog per i punti di accesso. Configurando l'IP di un server Syslog, gli access point vengono resi unicast come log della console. Non solo è utile per risolvere i problemi dei punti di accesso, ma è anche migliore per la rete rispetto all'impostazione predefinita che permette ai punti di accesso di trasmettere il syslog nella VLAN locale. La registrazione AP può generare un carico significativo di messaggi, anche nei casi in cui il syslog AP non viene monitorato. È comunque consigliabile limitare il numero di eventi impostando la gravità appropriata del messaggio e/o configurando un indirizzo IP del syslog fittizio (ad esempio 0.0.0.0) per impedire la trasmissione dei messaggi.
- Massimizzare i tentativi e il timeout di CAPWAP. I problemi vengono rilevati meno

rapidamente, ma la rete è più resistente alle piccole perdite di pacchetti temporanei.
- Abilitare SSH e configurare le credenziali. Disabilitare la console AP.
- Se necessario, abilitare il monitor del punto di accesso, ma non il monitor della radio.
- Abilitare il rilevamento rogue e configurare una soglia RSSI di -70 dBm.

Monitoraggio della rete

Una volta che la rete è operativa, è necessario monitorarla attentamente per rilevare eventuali problemi. In un normale ambiente di ufficio, gli utenti conoscono la rete e possono aiutarsi a vicenda in caso di problemi o aprire una richiesta di assistenza interna. In un luogo più grande, dove arrivano molti visitatori, è necessario concentrarsi sui problemi più importanti piuttosto che su individui specifici, che possono avere una configurazione errata.

È possibile monitorare la rete dalla CLI o dalla GUI di Catalyst 9800, ma non è lo strumento migliore per farlo ogni giorno. Si tratta della procedura più diretta quando si hanno già dei sospetti e/o dei dati sul problema e si desidera eseguire comandi specifici in tempo reale. Le opzioni di monitoraggio principali sono Cisco Catalyst Center o potenzialmente un dashboard di telemetria personalizzato. È possibile utilizzare strumenti di monitoraggio di terze parti, ma quando questi utilizzano il protocollo SNMP, i dati sono ben lungi dall'essere in tempo reale e i comuni strumenti di monitoraggio di terze parti non sono sufficientemente granulari con tutte le specificità dei fornitori wireless. Se si sceglie il protocollo SNMP, assicurarsi di utilizzare SNMPv3 poiché SNMPv2 ha una protezione obsoleta.

Cisco Catalyst Center è l'opzione migliore in quanto consente di gestire la rete oltre a monitorarla. Non solo il monitoraggio, ma permette anche di risolvere i problemi in tempo reale e di risolvere molte situazioni.

Un dashboard di telemetria personalizzato può essere utile se si desidera visualizzare metriche e widget molto specifici su uno schermo in modo sempre attivo per un NOC o un SOC. Se ci sono aree molto specifiche della rete che si desidera tenere d'occhio, è possibile creare widget dedicati per mostrare le metriche di rete in quelle aree nel modo desiderato.

Per le reti di eventi, è consigliabile monitorare le statistiche RF a livello di sistema, in particolare l'utilizzo dei canali e il numero di client per access point. Questa operazione può essere eseguita dalla CLI, ma fornisce solo un'istantanea in uno specifico point in time, l'utilizzo del canale tende ad essere dinamico ed è più adatto al monitoraggio nel tempo. Per questo tipo di monitoraggio, un dashboard personalizzato rappresenta in genere un approccio valido. Altre metriche che risultano più utili quando vengono monitorate nel tempo possono includere l'utilizzo di WNCD, il numero di client e i relativi stati e metriche specifiche del luogo. Un esempio di metrica specifica di un luogo potrebbe essere il monitoraggio dell'uso e/o del carico per un'area o un luogo specifico, ad esempio la hall X nel caso di un centro conferenze, o l'area di seduta Y nel caso di un luogo di un evento.

Per il monitoraggio personalizzato, sia l'approccio pull (NETCONF RPC) che quello push (NETCONF streaming telemetry) sono validi, anche se l'utilizzo della telemetria di streaming personalizzato in combinazione con Catalyst Center richiede una certa diligenza, in quanto esiste un limite al numero di sottoscrizioni di telemetria che è possibile configurare sul WLC e Catalyst

Center prepopola (e utilizza) molte di queste.

Quando si utilizza la RPC NETCONF, è necessario eseguire alcuni test per assicurarsi che il WLC non sia sovraccarico di richieste NETCONF. È importante tenere presente che le frequenze di aggiornamento per alcuni datapoint e il tempo necessario per la restituzione dei dati sono fattori particolarmente importanti. Ad esempio, l'utilizzo del canale AP viene aggiornato (da AP a WLC) ogni 60 secondi e la raccolta delle metriche RF per i 1000 AP (da WLC) può richiedere diversi secondi. In questo esempio, non sarebbe utile eseguire il polling del WLC ogni 5 secondi; un approccio migliore sarebbe quello di raccogliere le metriche RF a livello di sistema ogni 3 minuti.

NETCONF è sempre il protocollo preferito rispetto a SNMP.

Infine, non è possibile ignorare il monitoraggio dei componenti della rete principale, tra cui l'utilizzo del pool DHCP, il numero di voci NAT sui router principali e così via. Poiché il guasto di uno di questi può facilmente essere la causa di un'interruzione del collegamento wireless.

Maggiore è la durata del monitoraggio, maggiore è la possibilità di causare problemi

Esistono alcuni scenari classici in cui un monitoraggio eccessivo crea problemi:

- I sensori wireless che agiscono come client possono essere utili per misurare il throughput e la connettività in punti specifici della rete, ma ricordate che impostare una frequenza elevata di test significa che il sensore impiegherà molto tempo a trasferire grandi quantità di dati e quindi a rendere il canale e la rete effettivamente occupati, anche se non lo erano altrimenti. Questo è il primo esempio di "più difficile controlli, peggiore è il tuo aspetto metrico".
- Come già accennato, il protocollo SNMP è un protocollo legacy che ha un impatto elevato sulla CPU. L'esecuzione di polling SNMP di grandi dimensioni può saturare facilmente la CPU della rete wireless con le richieste non appena si monitorano di frequente tutti i client o gli access point wireless quando ne è presente un numero elevato. Prima di impostare un intervallo di polling aggressivo, considerare sempre la quantità di oggetti su cui si sta eseguendo il polling. Il daemon SNMP si trova all'interno del processo IOSd in IOS-XE, quindi quando si trova su una CPU elevata può avere un impatto sul resto delle funzionalità IOS.
- Anche se la telemetria è più efficiente di SNMP, le grandi reti wireless possono avere un numero molto elevato di client, punti di accesso ma anche di interfacce e dispositivi non autorizzati. Se la configurazione di telemetria è impostata in modo troppo aggressivo e il WLC deve segnalare costantemente qualsiasi variazione del segnale di qualsiasi dispositivo non autorizzato, questo può anche saturare facilmente qualsiasi dispositivo di controllo. Accertarsi di tenere sotto controllo il processo "pubd" che si occupa della telemetria e di non utilizzare la CPU in modo eccessivo. In tal caso, riconsidera le soglie e assicurati di seguire le best practice di 9800.

Problemi specifici delle reti di grandi dimensioni

Se si dispone di un SSID che utilizza l'autenticazione Web, un problema può essere rappresentato dai client che si connettono a tale SSID e ottengono un indirizzo IP ma non eseguono l'autenticazione perché l'utente finale non sta tentando attivamente di connettersi (il dispositivo si

connette automaticamente). Il controller deve intercettare ogni pacchetto HTTP inviato dai client che si trovano nello stato autenticazione Web in sospeso e che utilizza risorse WLC. Una volta che la rete è in esecuzione, controllare periodicamente il numero di client in attesa di autenticazione Web in un determinato momento per verificare come viene confrontato con i numeri di base. Stessa cosa per i client con stato IP Learn. I client si trovano sempre in questo stato quando eseguono il processo DHCP, ma la conoscenza di un numero di funzionamento corretto per la rete consente di impostare una linea di base e di identificare i momenti in cui tale numero può essere troppo alto, indicando un problema più grave.

Per i grandi eventi non è raro vedere circa il 10% dei client in stato Web Auth Pending.

Monitoraggio del secondo giorno: monitoraggio costante della soddisfazione degli utenti

Una volta che la rete è operativa, ci sono due tipi tipici di reclami da parte degli utenti finali: non possono collegarsi o hanno difficoltà a connettersi (disconnessioni), o il Wi-Fi funziona più lentamente del previsto. Quest'ultimo è molto difficile da identificare perché dipende in primo luogo dalle aspettative della velocità e dalla densità in tempo reale di una data area. Esaminiamo ora alcune risorse che possono essere utili nel monitoraggio quotidiano di una rete di grandi spazi pubblici.

Convalida throughput Wi-Fi: Guida al test e al monitoraggio. Questo documento cisco.com descrive come monitorare una rete per individuare eventuali problemi di throughput. Viene analizzata la quantità di throughput che i client possono ragionevolmente aspettarsi nella rete quando le condizioni sono silenziose e viene stimata la quantità di questi valori che diminuisce con l'aumentare del numero di client e del carico. Questa funzionalità è fondamentale per valutare se un reclamo dell'utente finale relativo al throughput è legittimo dal punto di vista tecnico o meno e se è necessario riprogettare l'area per il carico che potrebbe sostenere.

Quando i client segnalano problemi di connettività, dopo che questi sono stati isolati e chiariti con Catalyst Center, dare un'occhiata alla sezione Risoluzione dei problemi di connettività dei client di Catalyst 9800.

Infine, come buona norma generale, tieni d'occhio le metriche chiave generali del WLC con l'aiuto di Monitor Catalyst 9800 KPI (Key Performance Indicators).

Configurazione della scalabilità

SVI e interfacce su 9800

Evitare di creare SVI per VLAN client sul WLC. Gli amministratori abituati ai precedenti WLC di AireOS tendono a creare un'interfaccia di layer 3 per ciascuna VLAN client, ma questa procedura è raramente richiesta. Le interfacce aumentano il vettore di attacco del control plane e possono richiedere più ACL con voci più complesse. Per impostazione predefinita, è possibile accedere al WLC su una qualsiasi delle interfacce. Per proteggere un WLC con più interfacce, è necessario un impegno maggiore. Inoltre, complica il routing, quindi è meglio evitarlo.

A partire da IOS XE 17.9, le interfacce SVI non sono più necessarie per gli scenari di snooping

mDNS o inoltro DHCP. Pertanto, non ci sono molti motivi per configurare un'interfaccia SVI in una VLAN client.

Risposta probe aggregata

Per le reti pubbliche di grandi dimensioni, si consiglia di modificare l'intervallo di probe aggregato predefinito inviato dai punti di accesso. Per impostazione predefinita, gli AP aggiornano il WLC ogni 500 ms circa le richieste inviate dai client. Queste informazioni vengono utilizzate dal bilanciamento del carico, dalla selezione della banda, dalla posizione e dalle funzioni 802.11k. Se sono presenti molti client e punti di accesso, si consiglia di modificare l'intervallo di aggiornamento per evitare problemi di prestazioni del control plane nel WLC. L'impostazione consigliata è di 50 risposte di probe aggregate ogni 64 secondi. Verificare inoltre che i punti di accesso non segnalino richieste provenienti da indirizzi MAC amministrati localmente, in quanto non è disponibile il rilevamento dei punti di accesso per coloro che prendono in considerazione un singolo client potrebbero utilizzare molti MAC amministrati localmente durante la scansione per evitare il rilevamento di scopo.

```
wireless probe limit 50 64000

no wireless probe localy-administered-mac
```

IPv6

Molti amministratori di rete continuano a negare IPv6. Con IPv6 sono disponibili solo due opzioni accettabili: supportarlo e installare una configurazione adeguata ovunque oppure non installarlo e bloccarlo. Non è accettabile non preoccuparsi di IPV6 e lasciarlo abilitato in alcuni punti senza una corretta configurazione. Questo lascerebbe l'intero mondo IP a cui la sicurezza della vostra rete sarebbe cieca.

Se si abilita IPv6, è obbligatorio configurare un indirizzo IPv6 virtuale nell'intervallo 2001:DB8::/32 (passaggio spesso dimenticato).

È importante notare che, sebbene IPv6 si basi molto sul multicast per le sue operazioni di base, può comunque funzionare se si disabilita l'inoltro multicast sul WLC. Per inoltro multicast si intende l'inoltro di dati multicast del client e non l'individuazione dei router adiacenti, le richieste router e altri protocolli necessari per il funzionamento di IPv6.

Se la connessione Internet o il provider di servizi Internet fornisce indirizzi IPv6, è possibile decidere di consentire IPv6 per i client. Si tratta di una decisione diversa dall'abilitazione di IPv6 nell'infrastruttura. I punti di accesso possono continuare a funzionare solo in IPv4, ma il traffico di dati dei client IPv6 rimane all'interno dei pacchetti CAPWAP. L'abilitazione di IPv6 anche sull'infrastruttura richiede una riflessione sulla protezione dell'accesso client ai punti di accesso, al WLC e alla subnet di gestione.

Verificare la frequenza RSA dei gateway client. Il WLC offre un criterio di limitazione RA che limita

il numero di RA inoltrate ai client in quanto queste possono a volte diventare chiacchiere.

mDNS

In generale, è consigliabile mantenere i mDNS completamente disattivati in un'installazione in grandi spazi.

Il bridging mDNS si riferisce al concetto di invio dei pacchetti mDNS come multicast di layer 2 (quindi all'intera subnet client). mDNS è diventato popolare in scenari domestici e di piccoli uffici dove è molto pratico trovare servizi nella subnet. Tuttavia, in una rete di grandi dimensioni, questo significa inviare il pacchetto a tutti i client della subnet, il che è problematico dal punto di vista del traffico in una rete pubblica di grandi dimensioni. D'altra parte, il bridging non causa alcun sovraccarico per il punto di accesso o la CPU del WLC, in quanto è considerato traffico di dati regolare. Il proxy mDNS o il gateway mDNS si riferisce al concetto di utilizzare il WLC come directory per tutti i servizi della rete. Ciò consente di offrire servizi mDNS attraverso i confini del layer 2 in modo efficiente e anche di ridurre il traffico complessivo. Con il gateway mDNS, ad esempio, una stampante invia il proprio annuncio periodico di servizio tramite mDNS con un multicast di layer 2 della stessa subnet, ma il WLC non lo inoltra a tutti gli altri client wireless. Anzi, prende nota del servizio offerto e lo registra nella sua directory di servizi. Ogni volta che un client richiede servizi di un determinato tipo disponibili, il WLC risponde per conto della stampante con l'annuncio. In questo modo, tutti gli altri client wireless non saranno in grado di ricevere informazioni su richieste e offerte di servizi non necessarie e riceveranno una risposta solo ogni volta che verranno richiesti i servizi disponibili. Anche se migliora notevolmente l'efficienza del traffico, provoca un sovraccarico sul WLC (o sull'access point, se ci si affida a mDNS nell'ambito di FlexConnect) dovuto allo snooping del traffico mDNS. Se si utilizza un gateway mDNS, è fondamentale tenere sotto controllo l'utilizzo della CPU.

Il bridging porta a una tempesta multicast nella sottorete di grandi dimensioni e lo snooping (con la funzione gateway mDNS) provoca un elevato utilizzo della CPU. Disabilitarla sia a livello globale che su ciascuna WLAN.

Alcuni amministratori abilitano i servizi mDNS perché un paio di servizi ne hanno bisogno in luoghi specifici, ma è importante capire quanto traffico indesiderato ciò aggiunge. I dispositivi Apple spesso pubblicizzano se stessi e cercano costantemente i servizi, causando un rumore di fondo delle query mDNS anche quando nessuno fa un particolare uso di qualsiasi servizio. Se è necessario consentire mDNS a causa di un determinato requisito aziendale, attivarlo globalmente e quindi solo sulla WLAN in cui è richiesto e provare a limitare l'ambito in cui mDNS è consentito.

Rafforzamento della rete

Sicurezza

Nelle grandi reti pubbliche, molte cose possono accadere senza che l'amministratore ne sia a conoscenza. Le persone richiedono il rilascio di cavi in posti casuali, o collegano uno switch per uso domestico in un posto per avere più porte per i loro shenangians, ... Di solito provano queste cose senza prima chiedere il permesso. Ciò significa che, anche senza l'intervento di un attore negativo, la sicurezza può già essere compromessa da clienti e/o dipendenti attenti. Diventa poi

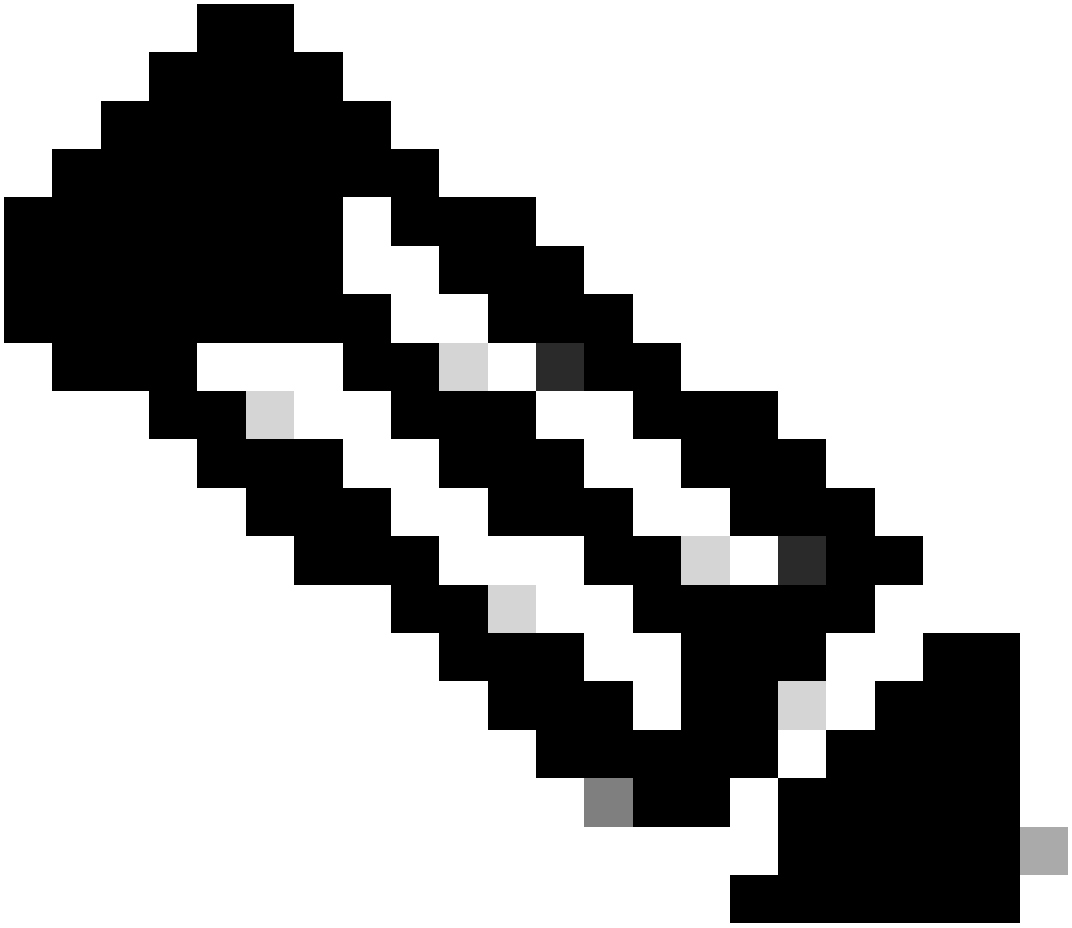
molto facile per un attore cattivo andare in giro e trovare un cavo a cui collegarsi e vedere quale accesso alla rete ottiene da lì. La configurazione dell'autenticazione 802.1X su tutte le porte degli switch è un requisito imprescindibile per mantenere una sicurezza decente in una rete di grandi dimensioni. Catalyst Center consente di automatizzare questo rollout e si possono fare eccezioni per dispositivi specifici che non supportano l'autenticazione 802.1X, ma che tentano di affidarsi il meno possibile all'autenticazione basata su MAC in quanto (sinceramente) non è una reale sicurezza.

Access point non autorizzati

La tua strategia per combattere i parassiti dipende da alcuni fattori. Molti amministratori istintivamente chiedono regole molto severe, ma le domande principali sono:

- Quando ricevete centinaia (se non migliaia) di allarmi anomali, avete le risorse umane per guardarli tutti e agire su tutti?
- L'obiettivo è quello di rimuovere fisicamente i truffatori per mantenere pulito lo spettro RF? In questo caso, sono necessarie molte persone per eseguire l'operazione. O forse il tuo obiettivo è solo tenere d'occhio il fattore sicurezza e assicurarsi che i truffatori non rappresentino alcun pericolo? Questo ha un costo del lavoro molto più gestibile.
- L'attivazione del rilevamento rogue può avere un impatto sul tempo di trasmissione e il contenimento rogue ha in genere un impatto ancora maggiore. Avete analizzato questo impatto e ne avete tenuto conto?

Per quanto riguarda l'impatto del rilevamento rogue, i 9120 e 9130 hanno un chip CleanAir dedicato che si occupa della scansione off-channel (e quindi del rilevamento rogue) rendendo l'impatto sulla radio client-serving quasi nullo. I access point serie 1960 con il chip CleanAir Pro hanno una capacità di scansione senza impatto simile, ma altri access point che non hanno il chip CleanAir devono togliere la radio client-serving dal canale per effettuare la ricerca di manomissioni o per effettuare il contenimento. Il modello AP in uso svolge quindi un ruolo determinante nella decisione di utilizzare o meno punti di accesso in modalità monitor dedicati per il rilevamento e il contenimento di anomalie.

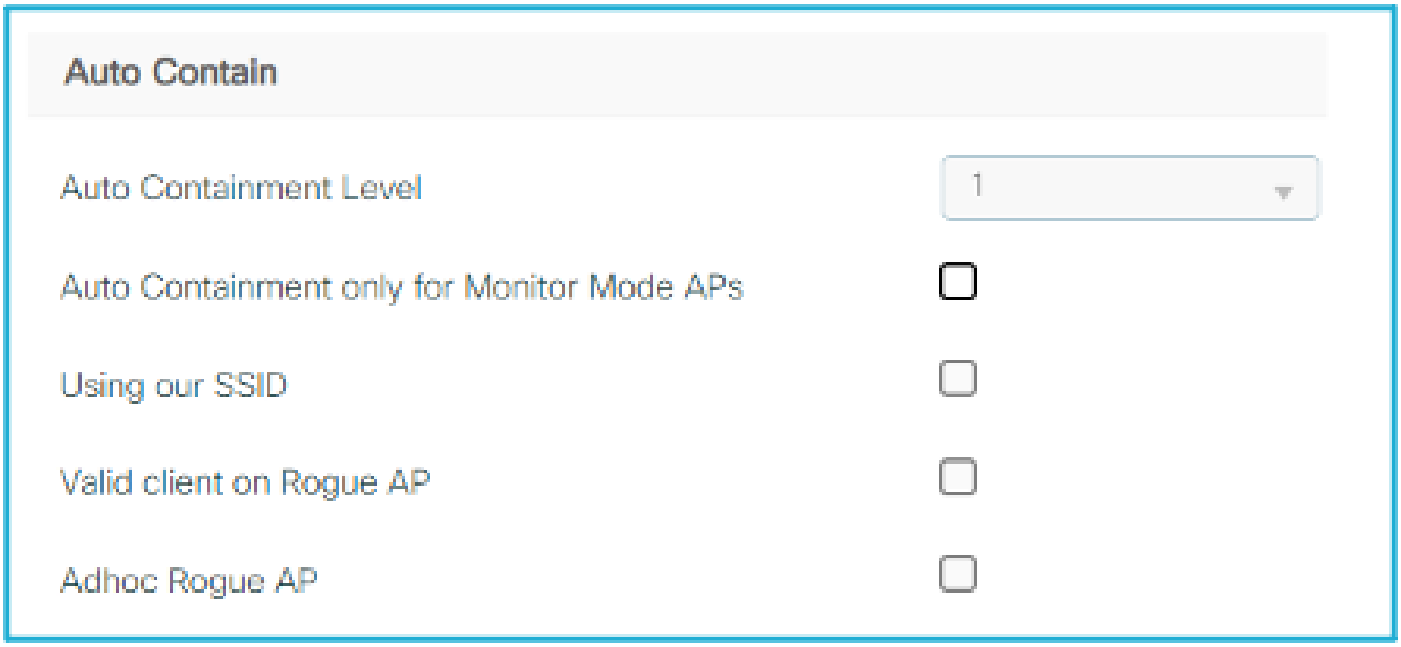


Nota: i telefoni cellulari che condividono un hotspot Wi-Fi funzionano in modalità "infrastruttura" proprio come i punti di accesso tradizionali, la modalità "ad-hoc" si riferisce a una connessione diretta tra dispositivi mobili ed è meno comune.

Il contenimento dei rifiuti tossici è spesso vietato da norme di legge, quindi è essenziale controllare con l'autorità locale prima di abilitarlo. Contenere un server non autorizzato non significa arrestare il server non autorizzato in remoto, ma inviare posta indesiderata ai client che tentano di connettersi al punto di accesso non autorizzato con frame di deautenticazione, in modo che non si connettano. Questa operazione può essere eseguita solo su SSID di protezione legacy (non funziona in WPA3 o quando PMF è abilitato in WPA2) perché i punti di accesso non sono in grado di firmare correttamente i frame di deautenticazione. Il contenimento ha un impatto negativo sulle prestazioni RF sul canale di destinazione, poiché i punti di accesso riempiono il tempo di trasmissione con frame di deautenticazione. Pertanto, deve essere considerata solo come una misura di sicurezza per impedire ai propri clienti legittimi di associarsi per errore a un punto di accesso non autorizzato. Per tutti i motivi menzionati, si consiglia di non fare alcun contenimento in quanto non risolve completamente il problema canaglia e causa più problemi RF. Se è necessario utilizzare il contenimento, ha senso solo abilitarlo per i truffatori che falsificano uno dei

SSID gestiti in quanto si tratta di un attacco honeypot ovvio.

È possibile configurare il contenimento automatico con l'opzione "using our SSIDs" (Usa SSID):



Impostazioni di Contenuto automatico

È inoltre possibile configurare regole non autorizzate per classificarle come punti di accesso non autorizzati dannosi in base ai propri criteri. Non dimenticare di immettere il nome dei SSID vicini e approvati come semplici utenti non autorizzati per rimuovere tali utenti dall'elenco degli allarmi.

Abilitare l'autenticazione AP o PMF per proteggere i punti di accesso dalla rappresentazione.

Un canaglia cablato è un punto di accesso canaglia collegato alla rete cablata, che rappresenta ovviamente una maggiore minaccia per la sicurezza. Il rilevamento dei router cablati è più complicato in quanto l'indirizzo MAC Ethernet di un router in genere è diverso dall'indirizzo MAC della radio. Il Cisco Catalyst Center dispone di algoritmi che tentano ancora di rilevare se un server non autorizzato è connesso via cavo e di individuare i MAC client non autorizzati che vengono entrambi ascoltati via etere e visualizzati sull'infrastruttura cablata. La soluzione migliore per prevenire completamente i problemi causati da cavi è proteggere tutte le porte degli switch con l'autenticazione 802.1X.

Se hai intenzione di agire fisicamente su un punto di accesso non autorizzato, sfruttare Cisco Spaces è fondamentale per avere una posizione accurata del server non autorizzato. È molto probabile che sia ancora necessario effettuare ricerche in loco poiché le persone tendono a nascondere i punti di accesso non autorizzati, ma ridurre l'area di ricerca a pochi metri lo rende un'impresa molto fattibile. Senza Spazi, la canaglia è mostrata sulla mappa accanto all'AP rilevandola il più forte che rende l'area di ricerca abbastanza grande. Esistono molti strumenti e dispositivi wireless che mostrano il segnale del punto di accesso non autorizzato in tempo reale per individuare fisicamente il dispositivo.

Non esattamente in relazione ai truffatori, ma dato che CleanAir è appena stato coperto, è importante notare che l'abilitazione di CleanAir non ha un impatto negativo notevole sulle

prestazioni tranne il rilevamento del beacon BLE, in quanto questo influisce sulle prestazioni 2.4GHz. È possibile configurare la rete wireless in modo che ignori completamente gli interferenti Bluetooth, in quanto sono onnipresenti nel mondo odierno, e non è possibile impedire ai client di abilitare il Bluetooth.

WiPS

WiPS copre vettori di attacco più avanzati rispetto al semplice rilevamento della presenza di un dispositivo non autorizzato. Oltre a questi attacchi, talvolta fornisce anche un PCAP dell'evento per l'analisi forense.

Sebbene si tratti di una funzionalità di sicurezza molto utile per l'azienda, una rete pubblica deve comunque affrontare l'eterna domanda: cosa fare?

Con la difficoltà di gestire molti client non controllati, è possibile dividere gli allarmi in due categorie. Se vengono visualizzati troppi allarmi, è possibile decidere di ignorarli dal Cisco Catalyst Center:

- 10001: DoS: allarme flood di autenticazione
- 10002: DoS: avviso richiesta associazione
- 10003: DoS: allarme Broadcast Probe flood
- 10004: DoS: disassociazione allarme inondazioni
- 10005: DoS: allarme broadcast disassociazione
- 10006: DoS: deautenticazione Flood Alarm
- 10007: DOS: Avviso di deautenticazione broadcast
- 10008: DOS: Allarme di attacco EAPOL-Logoff
- 10009: allarme inondazioni CTS
- 10010: Richiesta di avviso associazione RTS
- 10011: Deautenticazione Flood by Pair
- 10021: Airdrop Session (questa in genere si verifica molto in qualsiasi rete e descrive semplicemente l'attività peer-to-peer regolare tra i dispositivi Apple)
- 10022: richiesta di associazione non valida
- 10023: errore di autenticazione propagato dalla firma
- 10024: OUI MAC non valido per firma
- 10025: autenticazione non valida

Questi allarmi possono essere causati potenzialmente da un client che si comporta in modo errato. Non è possibile impedire automaticamente un attacco Denial of Service poiché, essenzialmente, non è possibile impedire a un client difettoso di mantenere occupato il tempo di trasmissione. Anche se l'infrastruttura ignora il client, sarebbe comunque in grado di utilizzare il supporto e il tempo di trasmissione, con un conseguente impatto sulle prestazioni dei client circostanti.

Gli altri allarmi sono così specifici che molto probabilmente rappresentano un attacco dannoso e possono difficilmente verificarsi a causa di cattivi driver del cliente. È meglio continuare a monitorare questi allarmi:

- 10012: beacon fuzzed
- 10013: richiesta sonda non elaborata
- 10014: risposta della sonda non elaborata
- 10015: Polling PS per firma
- 10016: EAPOL Start V1 Flood by Signature
- 10017: Richiesta di riassociazione inondazione per destinazione
- 10018: Beacon Flood per firma
- 10019: risposta della sonda Flood by Destination
- 10020: Blocca ACK flooding per firma
- 10026/10027: RTS e CTS Virtual Carrier Sense Attack

L'infrastruttura wireless a volte può adottare azioni di mitigazione come bloccare l'elencazione del dispositivo offensivo, ma l'unica azione reale per sbarazzarsi di un attacco di questo tipo è andare fisicamente lì e rimuovere il dispositivo offensivo.

Si consiglia di abilitare tutte le forme di esclusione dei client per risparmiare tempo di trasmissione sprecato interagendo con i client difettosi.

Limitazione dell'accesso client

Si consiglia di abilitare il blocco peer-to-peer su tutte le WLAN (a meno che non si abbia un requisito difficile per la comunicazione client-to-client, ma questo aspetto deve essere considerato attentamente ed eventualmente limitato). Questa funzione impedisce ai client della stessa WLAN di contattarsi reciprocamente. Questa non è una soluzione perfetta, in quanto i client su WLAN diverse sono ancora in grado di contattarsi e anche i client appartenenti a WLC diversi nel gruppo di mobilità possono ignorare questa restrizione. Ma agisce come un primo livello semplice ed efficiente di sicurezza e ottimizzazione. Un ulteriore vantaggio di questa funzione di blocco peer-to-peer è che impedisce anche la ARP client-to-client che impedisce alle applicazioni di rilevare altri dispositivi sulla rete locale. Senza il blocco peer-to-peer, l'installazione di una semplice applicazione sul client potrebbe mostrare tutti gli altri client connessi nella subnet con i relativi indirizzi IP e nomi host.

Inoltre, si consiglia di applicare un ACL IPv4 e un ACL IPv6 (se si utilizza IPv6 nella rete) alle WLAN per impedire la comunicazione tra client. L'applicazione di un ACL che blocchi le comunicazioni tra client e client a livello di WLAN funziona indipendentemente dal fatto che si disponga o meno di SVI client.

L'altro passaggio obbligatorio consiste nel impedire l'accesso dei client wireless a qualsiasi forma di gestione del controller wireless.

Esempio:

```
ip access-list extended ACL_DENY_CLIENT_VLANS

 10 deny ip any 10.131.0.0 0.0.255.255

 20 deny ip 10.131.0.0 0.0.255.255 any
```

```
 30 deny ip any 10.132.0.0 0.0.255.255

 40 deny ip 10.132.0.0 0.0.255.255 any

 50 deny ip any 10.133.0.0 0.0.255.255

 60 deny ip 10.133.0.0 0.0.255.255 any

 70 deny ip any 10.134.0.0 0.0.255.255

 80 deny ip 10.134.0.0 0.0.255.255 any

 90 deny ip any 10.135.0.0 0.0.255.255

 100 deny ip 10.135.0.0 0.0.255.255 any

 110 deny ip any 10.136.0.0 0.0.255.255

 120 deny ip 10.136.0.0 0.0.255.255 any

 130 deny ip any 10.137.0.0 0.0.255.255

 140 deny ip 10.137.0.0 0.0.255.255 any

 150 permit ip any any
```

Questo ACL può essere applicato all'interfaccia di gestione SVI:

```
interface Vlan130

 ip access-group ACL_DENY_CLIENT_VLANS in
```

Questa operazione viene eseguita su un WLC con le VLAN client da 131 a 137 create nel database di VLAN di layer 2, ma senza SVI corrispondenti. Esiste solo una SVI per la VLAN 130, ossia il modo in cui il WLC viene gestito. Questo ACL impedisce a tutti i client wireless di inviare completamente qualsiasi traffico ai piani di controllo e gestione WLC. Non dimenticate che la gestione SSH o dell'interfaccia utente Web non è l'unica cosa che dovete permettere, poiché è anche richiesta una connessione CAPWAP verso tutti gli access point. Per questo motivo, questo ACL ha un'autorizzazione predefinita, ma blocca gli intervalli di client wireless, invece di basarsi su un'azione di negazione predefinita che richiederebbe di specificare tutti gli intervalli di subnet AP e di gestione consentiti.

Analogamente, è possibile creare un altro ACL che specifichi tutte le possibili subnet di gestione:

```
ip access-list standard ACL_MGMT

 10 permit 10.128.0.0 0.0.255.255

 20 permit 10.127.0.0 0.0.255.255
```

```
 30 permit 10.100.0.0 0.0.255.255

 40 permit 10.121.0.0 0.0.255.255

 50 permit 10.141.0.0 0.0.255.255
```

È quindi possibile applicare questo ACL per l'accesso dalla CLI:

```
line vty 0 50

 access-class ACL_MGMT in

 exec-timeout 180 0

 ipv6 access-class ACL_IPV6_MGMT in

 logging synchronous

 length 0

 transport preferred none

 transport input ssh

 transport output ssh
```

Lo stesso ACL può essere applicato anche per l'accesso come amministratore Web.

Protezione da tempeste di traffico

I multicast e le trasmissioni sono utilizzati in modo più intensivo da alcune applicazioni rispetto ad altre. Quando si prende in considerazione una rete solo cablata, l'unica precauzione da adottare è spesso quella di proteggere la rete da interferenze. Tuttavia, un multicast è doloroso quanto una trasmissione quando viene trasmesso in diretta, ed è importante comprenderne le ragioni. Innanzitutto, immaginate un pacchetto inviato (via broadcast o multicast) a tutti i client wireless, che si aggiunge rapidamente a molte destinazioni. Ogni punto di accesso deve quindi trasmettere questo frame via etere nel modo più affidabile possibile (anche se non è garantito come affidabile) e ciò si ottiene utilizzando una velocità dati obbligatoria (talvolta la più bassa, talvolta è configurabile). In termini laici, questo significa che il frame viene inviato utilizzando una velocità dati OFDM (802.11a/g), che chiaramente non è ottima.

In una rete pubblica di grandi dimensioni, si sconsiglia di utilizzare il multicast per preservare il tempo di trasmissione. Tuttavia, in una rete aziendale di grandi dimensioni è possibile avere la necessità di mantenere il multicast abilitato per un'applicazione specifica, anche se è necessario controllarlo il più possibile per limitarne l'impatto. È consigliabile documentare i dettagli dell'applicazione, IP multicast, e assicurarsi di bloccare altre forme di multicast. L'abilitazione dell'inoltro multicast non è un requisito per l'abilitazione di IPv6, come spiegato in precedenza. È consigliabile mantenere disabilitato completamente l'inoltro di trasmissione. Le trasmissioni

vengono talvolta utilizzate dalle applicazioni per individuare altri dispositivi nella stessa subnet, il che rappresenta chiaramente un problema di sicurezza in una rete di grandi dimensioni.

Se si abilita l'inoltro multicast globale, assicurarsi di utilizzare l'impostazione CAPWAP multicast-multicast AP. Con questa opzione abilitata, quando il WLC riceve un pacchetto multicast dall'infrastruttura cablata, lo invia a tutti gli access point interessati con un unico pacchetto multicast, salvando una grande quantità di duplicazione dei pacchetti. Verificare di impostare un indirizzo IP multicast CAPWAP diverso per ciascuno dei WLC, altrimenti gli AP ricevono traffico multicast da altri WLC, il che non è desiderato.

Se gli access point si trovano in altre subnet dell'interfaccia di gestione wireless del WLC (probabilmente in una rete di grandi dimensioni), è necessario abilitare il routing multicast sull'infrastruttura cablata. È possibile verificare che tutti gli access point ricevano correttamente il traffico multicast con il comando:

```
show ap multicast mom
```

Si consiglia inoltre di abilitare il multicast IGMP (per multicast IPv4) e MLD (per IPv6) in tutti i casi se è necessario fare affidamento sul multicast. Consentono solo ai client wireless interessati (e quindi solo agli access point che hanno client interessati) di ricevere il traffico multicast. Il WLC inoltra la registrazione al traffico multicast e si occupa di mantenere la registrazione in vita, scaricando in tal modo i client.

Conclusioni

Le reti pubbliche di grandi dimensioni sono complesse, ognuna è unica e presenta requisiti e risultati specifici.

Il rispetto delle linee guida riportate in questo documento è un ottimo punto di partenza e consente di ottenere il successo dell'installazione evitando i problemi più comuni. Tuttavia, tali orientamenti sono solo linee guida e potrebbero richiedere un'interpretazione o un adeguamento nel contesto della sede specifica.

Cisco CX dispone di team di professionisti wireless dedicati a installazioni wireless di grandi dimensioni, con esperienza in numerosi eventi di grandi dimensioni, tra cui eventi sportivi e conferenze. Rivolgersi al team amministrativo per ulteriore assistenza.

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).