設計手冊CX -大型公用網路專用無線

目錄

簡介

本檔案介紹大型公共Wi-Fi網路的設計和組態準則。

CX設計手冊

CX設計手冊由思科技術支援中心(TAC)和思科專業服務(PS)的專家撰寫，並由思科的專家進行同行評審；這些指南基於思科的領先實踐，以及多年來從無數客戶實施中獲得的知識和經驗。根據本文檔的建議設計和配置網路有助於避免常見缺陷並改善網路操作。

範圍和定義

本文檔提供大型公共無線網路的設計和配置指南。

定義：大型公用網路-通常以高密度進行無線部署，為數千台未知及/或未管理的使用者端裝置提供網路連線能力。

本文檔通常假定目標網路為大型和/或臨時事件提供服務。它還適用於接待許多訪客的場館的靜態永久網路。例如，商場或機場與體育場或音樂會場地的Wi-Fi網路有相似之處，因為無法控制終端使用者，而且它們通常僅存在於網路內幾個小時，或者最多只存在於網路內。

大型活動或場館的無線覆蓋有其自己的要求，往往與企業、製造業、甚至大型教育網路不同。大型公共網路可以有數千人，集中在一棟或幾棟建築中。它們可以經常或高峰期進行客戶端漫遊，並且網路必須儘可能與任何無線客戶端裝置相容，而不會控制客戶端裝置配置或安全性。

本指南介紹了高密度的一般RF概念以及實施細節。本指南中的許多無線電概念適用於所有高密度網路，包括Cisco Meraki。但是，實施細節和配置側重於使用Catalyst 9800無線控制器的Catalyst無線，因為這是當今為大型公共網路部署的最常見的解決方案。

本檔案會將「無線控制器」和「無線LAN控制器(WLC)」這兩個術語互換使用。

大型公用網路

大型公眾和活動網路在許多方面都是獨一無二的，本文檔對這些關鍵領域進行了探索並提供指導。

- 大型公共網路非常密集；在減少的射頻(RF)空間中有數千台裝置，並且隨著人們四處走動，某些活動和場地可能會更加靜態，在特定時間出現頻寬峰值。對於進入該區域並在該區域內移動的客戶端，基礎設施需要儘可能平穩地處理所有這些狀態更改。
- 重點在於輕鬆上線。關聯的客戶是快樂的客戶。這表示您希望使客戶端與網路的關聯儘可能快。未連線到Wi-Fi的客戶端會掃描可用的存取點，這會產生多餘的RF能量，從而導致額外的擁塞和空中的容量丟失。
- RF部署需要儘可能仔細地設計。如果需要超高密度，或者場地有大的開放空間和/或高天花板，必須使用方向性天線的適當RF設計。
- 另一個關鍵設計驅動器是相容性。某些功能是802.11規範中的標準功能，而其他功能是專有功能，不會給客戶端帶來任何問題。然而，現實情況卻有所不同，許多程式設計不當的客戶端驅動程式在看到它們不理解的複雜信標或功能/設定時行為不當。
- 由於規模和時間限制，故障排除非常困難。如果某些內容無法與特定客戶端配合使用，您將無法與該終端使用者配合使用來瞭解問題。使用者可能很難找到，但也可能因為他們在會場中的臨時訪問而變得不合作。
- 安全是一個重要因素。由於訪客數量龐大且攻擊面更大，因此控制較少。

外部參照

檔名稱	來源	位置
Cisco Catalyst 9800系列配置最佳實踐	思科	連結
無線區域網控制器CPU故障排除	思科	連結
驗證Wi-Fi傳輸量：測試和監控指南	思科	連結
Cisco Catalyst CW9166D1存取點部署指南	思科	連結
Catalyst 9104體育場天線(C-ANT9104)部署指南	思科	連結
監控Catalyst 9800 KPI（關鍵效能指標）	思科	連結

檔名稱	來源	位置
Catalyst 9800 用戶端連線問題流程疑難排解	思科	連結
Cisco Catalyst 9800系列無線控制器軟體組態設定指南(17.12)	思科	連結
Wi-Fi 6E：Wi-Fi 白皮書重要新篇章	思科	連結

免責宣告

本文檔根據某些場景、假設以及從大量部署中獲得的知識提供建議。但是，讀者負責確定網路設計、業務、合規性、安全性、隱私和其他要求，包括是否遵循本指南中提供的指導或建議。

設計網路

RF注意事項

場所型別

本指南側重於大型訪客網路，通常對公眾開放，對終端使用者和客戶端裝置型別的控制有限。這些型別的網路可以部署在多種位置，可以是臨時的或永久的。主要的使用案例通常是提供網際網路存取給訪客，雖然這很少是唯一的使用案例。

典型位置：

- 體育場館
- 會議地點
- 大型禮堂

從RF的角度來看，每種位置型別都有自己的一組細微差別。除會議場地外，大多數這類場地通常都是永久性設施，因為它們可以是永久性的或臨時為特定展會而設定。

其他位置：

- 郵輪
- 機場
- 購物中心/商場

機場和郵輪也是適合大型公共網路類別的部署示例；但是，這些示例還包含針對每種情況的額外考慮因素，並且通常使用內部全向AP。

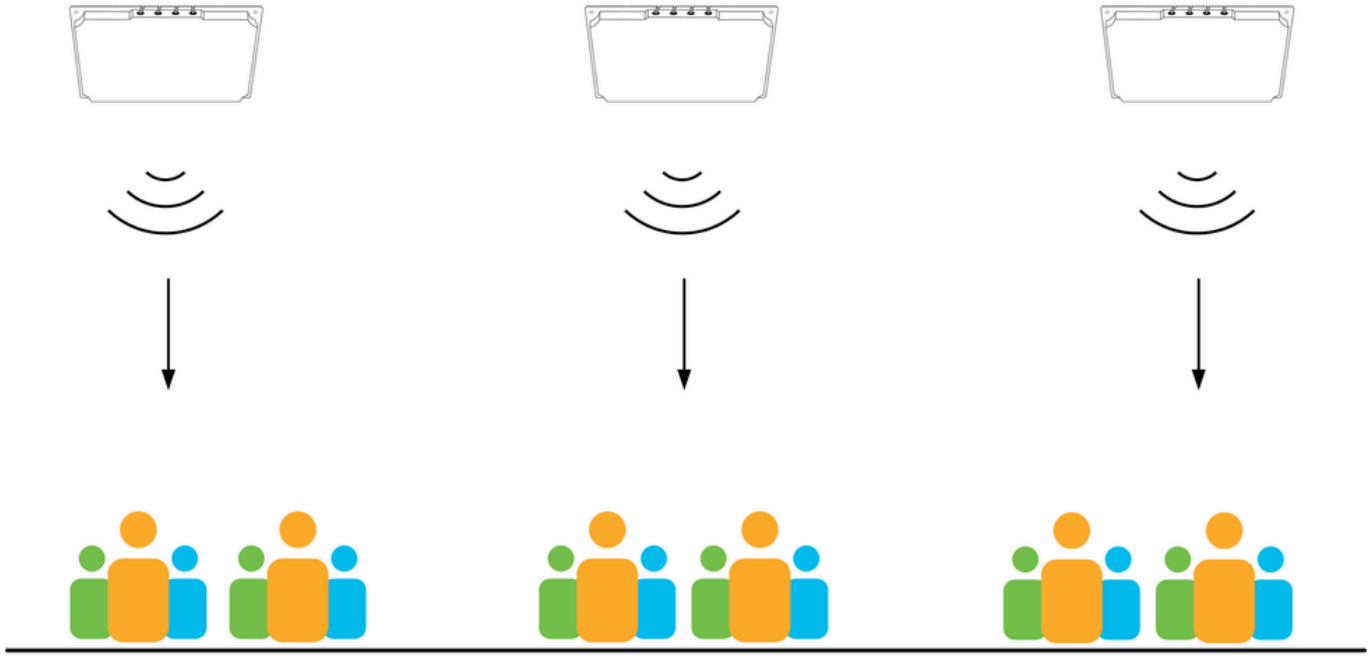
覆蓋策略

覆蓋策略主要取決於場所型別、使用的天線以及可用的天線安裝位置。

間接費用

儘可能優先使用開銷覆蓋。

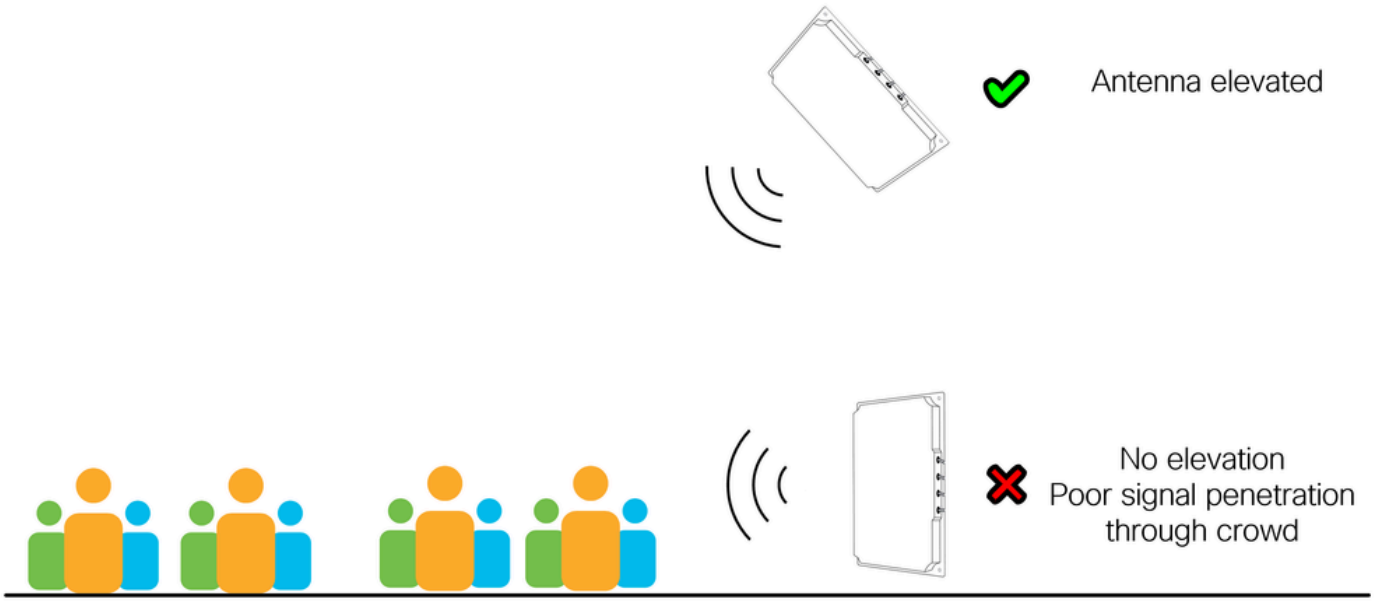
開銷解決方案有一個明顯的優勢，即所有客戶端裝置通常都能直接看到天線開銷，即使在擁擠的場景中也是如此。使用定向天線的開銷解決方案提供了更受控和定義明確的覆蓋區域，從無線電調諧的角度來看，使覆蓋區域變得不那麼複雜，同時提供了卓越的負載均衡和客戶端漫遊特性。有關其他資訊，請參閱功率平衡部分。



客戶端上的AP

側面

側裝式定向天線是常用的選擇，在各種情況下都能良好運作，特別是當由於高度或安裝限制而無法進行額外安裝時。使用側面安裝時，必須瞭解天線所覆蓋的區域型別，例如，它是開放的室外區域還是密集的室內區域？如果覆蓋區域是人口眾多的高密度區域，則天線必須儘量提高，因為透過人群的訊號傳播總是很差。請記住，大多數流動裝置在腰部以下使用，而不是在使用者的頭上使用！如果覆蓋區域是密度較低的區域，則天線的高度不太重要。



天線仰角總是比較高

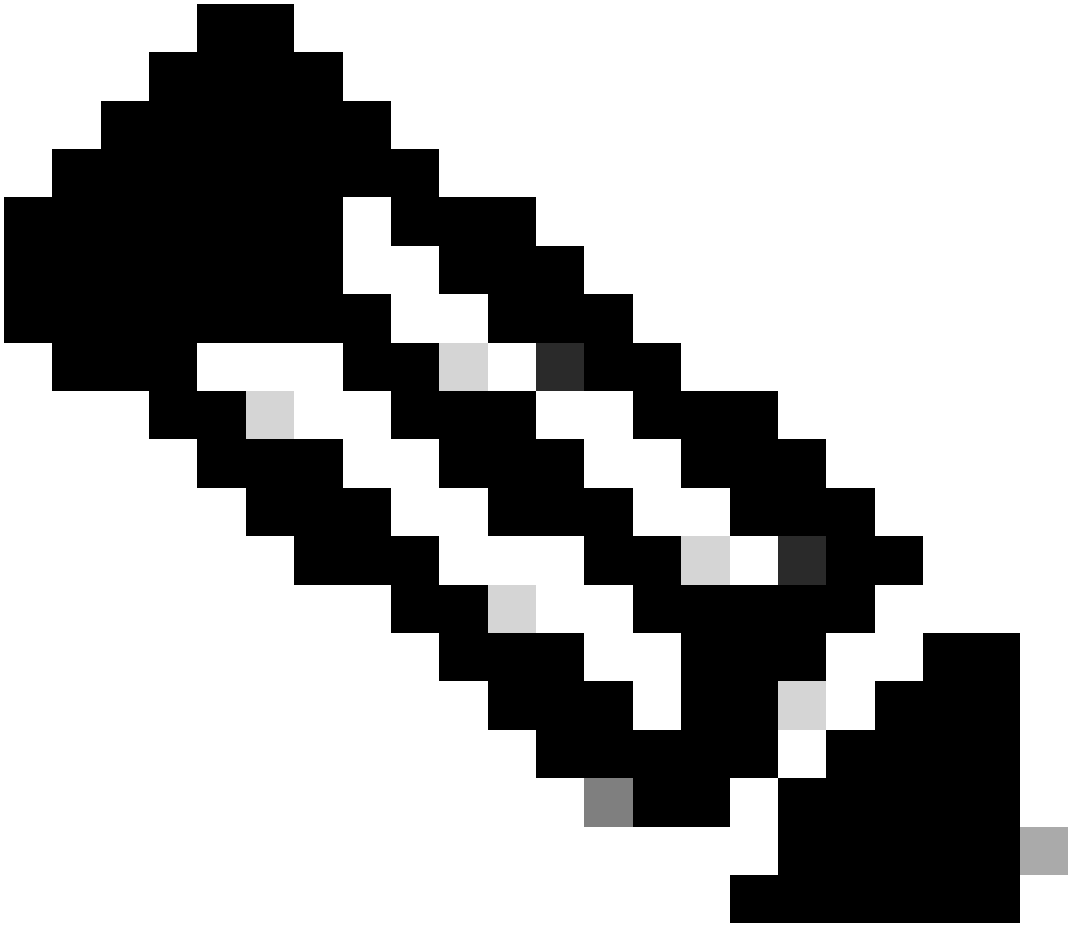
全向

在非常高密度的情況下，通常必須避免使用全向天線（內部或外部），這是因為同通道干擾的潛在高影響區域。6公尺以上的高度不得使用全向天線（不適用於高增益室外機）。

坐席

在某些場地或體育場中，可能會出現沒有合適天線安裝位置的情況。最後剩下的替代方案是透過將AP放置在使用者坐下的座位下來提供從下方覆蓋的功能。這種型別的解決方案更難以正確部署，並且通常成本更高，需要更多的AP和特定的安裝程式。

席位不足部署的主要挑戰在於全場與空場覆蓋範圍之間的巨大差異。人體在衰減無線電訊號方面非常有效，這意味著當無線存取點周圍有人群時，與沒有人群的人相比，產生的覆蓋範圍要小得多。這種人流量衰減係數允許部署更多AP，從而增加整體容量。然而，當場地空置時，人體沒有衰減，並且明顯干擾，當場地部分滿時，這會導致併發症。



注意：席位下部署是一個有效但不常見的解決方案，必須逐個進行評估。本文檔中不會進一步討論席位下部署。

美學

在一些部署中，美學問題開始發揮作用。這些區域可以是具有特定建築設計、歷史價值或廣告和/或品牌規定裝置可以（或不能）安裝的空間。需要特定的解決方案才能解決任何放置限制。其中一些解決方法包括隱藏AP/天線、繪製AP/天線、將裝置安裝在盤櫃中，或者只使用其他位置。如果選擇塗漆天線，則始終使用非金屬塗漆，則塗漆天線將失去保修期。思科一般不銷售天線外殼，但許多天線可以透過不同的提供商輕鬆獲得。

所有此類解決方法都會對網路效能產生影響。無線架構師總是從提出最佳安裝位置開始，以獲得最佳無線電覆蓋，而這些初始位置通常可提供最佳效能。對這些位置的任何改變通常會導致天線偏離其最佳位置。

安裝天線的地點通常是高架的，可以是天花板、T型台、屋頂結構、橫樑、人行道，以及任何在預定覆蓋範圍之上提供一定高度的位置。這些位置通常與其他裝置共用，例如：音訊裝置、空調、照

明和各種探測器/感測器。例如，音訊和照明裝置必須安裝在非常特定的位置-但這是為什麼？簡單來說，這是因為音訊和照明裝置在隱藏在箱子中或牆後時，無法正常工作，並且每個人都會承認這一點。

同樣的情況也適用於無線天線，當無線客戶端裝置有視線時，它們的工作效果最佳。優先考慮美學可能會對無線效能產生負面影響（而且通常確實如此），從而降低基礎設施投資的價值。

惡意網路

非法Wi-Fi網路是共用一個射頻空間但不由同一業者管理的無線網路。這些裝置可以是臨時裝置或永久裝置，包括基礎設施裝置(AP)和個人裝置（例如共用Wi-Fi熱點的行動電話）。非法Wi-Fi網路是干擾源，在某些情況下還會帶來安全風險。不可低估惡意程式對無線效能的影響。Wi-Fi傳輸僅限於在所有Wi-Fi裝置之間共用的相對較小的無線電頻譜，任何鄰近的不當裝置都有可能中斷許多使用者的網路效能。

在大型公共網路環境中，通常使用專用天線精心設計和調整這些網路。良好的RF設計僅涵蓋所需的區域，通常使用定向天線，並調整傳送和接收特性以獲得最大效率。

在頻譜的另一端是消費級裝置，或是由網際網路服務提供商提供的裝置。它們要麼是精細RF調整的選項有限，要麼是為最大範圍和感知效能而配置，通常採用高功率、低資料速率和寬通道。在大型事件網路中引入此類裝置可能會造成嚴重破壞。

我們能做些什麼？

就個人熱點而言，我們幾乎做不了什麼，因為要監控數萬人進入場館幾乎是不可能的。對於基礎設施或半永久裝置，有一些選擇。可能的補救措施始於簡單的教育，包括簡單的宣傳標牌，透過簽署的無線電政策檔案，以積極的實施和頻譜分析結束。在所有情況下，都必須就指定地點內的無線電頻譜保護做出商業決定，並採取具體步驟執行這一商業決定。

當受第三方控制的裝置通告與受管網路相同的SSID時，惡意網路的安全方面就開始發揮作用。這相當於蜜罐攻擊，可用作竊取使用者憑據的方法。始終建議建立一個惡意規則，以警告檢測到非受管裝置通告的基礎設施SSID。安全部分更詳細地討論了惡意程式。

單5GHz與雙5GHz

雙5GHz是指在支援的AP上使用兩個5GHz無線電。使用外部天線的雙5GHz與使用內部天線的雙5GHz（全向AP上的微/宏信元）之間存在一個關鍵區別。在外部天線的情況下，雙5GHz通常是一種有用的機制，可提供額外的覆蓋範圍和容量，同時減少總AP數量。

微/宏/MESO

內部AP的兩個天線都緊密相連（在AP內部），在使用雙5GHz時，存在與最大Tx功率相關的限制。第二個無線電被限制為低Tx功率（由無線控制器執行）導致無線電之間的Tx功率大幅失衡。這可能會導致主要（較高功率）無線電吸引許多客戶端，而輔助（較低功率）無線電使用不足。在這種情況下，第二個無線電會增加環境的能量，但不會給客戶帶來好處。如果出現這種情況，最好停用第二個無線電，並在需要額外容量時直接增加另一個（單個5GHz）AP。

不同AP型號有不同的配置選項，第二個5GHz無線電可在較新的宏/中 AP（如9130和9136）中以較

高的功率水準運行，而某些內部Wi-Fi 6E AP（如9160系列）甚至在某些情況下可在宏/宏模式下運行。請始終檢驗您準確的AP型號的功能。第二個5GHz插槽的通道使用也受到限制，當一個插槽在一個UNII頻帶中運行時，另一個插槽被限制為不同的UNII頻帶，這會影響通道規劃以及隨後的可用傳輸功率。請始終考慮雙5GHz無線電之間的Tx功率差異，在所有情況下都如此，包括內部AP。

FRA

靈活無線電分配(FRA)是一種透過將額外的2.4GHz無線電切換到5GHz模式，或將潛在未使用的5GHz無線電切換到monitor模式（適用於支援它的AP）來提高5GHz覆蓋率的技術。由於本文檔涵蓋大型公共網路，因此假設覆蓋區域和無線電設計使用定向天線定義良好，因此確定性配置優先於動態配置。建議不要在大型公共網路中使用FRA。

或者，在設定網路以幫助確定要轉換為5GHz的無線電時，可以使用FRA，但如果您對結果感到滿意，建議凍結FRA。

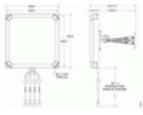
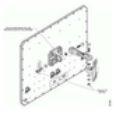
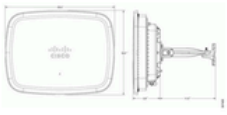
法規

每個監管領域都定義了可供使用的通道及其最大功率水準，並且對於哪些通道可在室內和室外使用，也有限制。根據法規領域，有時可能無法有效利用雙5GHz解決方案。例如，ETSI域在UNII-2e通道上允許30dBm，但在UNII1/2上僅允許23dBm。在本例中，如果設計要求使用30dBm（通常是因為與天線的距離較遠），則使用單個5GHz無線電可能是唯一可行的解決方案。

天線

大型公共網路可以使用任何型別的天線，並且通常選擇最適合工作的天線。在同一個覆蓋區域內混合天線會使無線電設計過程更具挑戰性，如果可能的話，必須加以避免。但是，大型公共網路通常覆蓋範圍較大，即使在同一區域內也具有不同的安裝選項，因此在某些情況下需要混合天線。全向天線非常容易理解，其功能與其他任何天線相同，本指南將討論外部定向天線。

此表列出了最常用的外部天線。

	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°

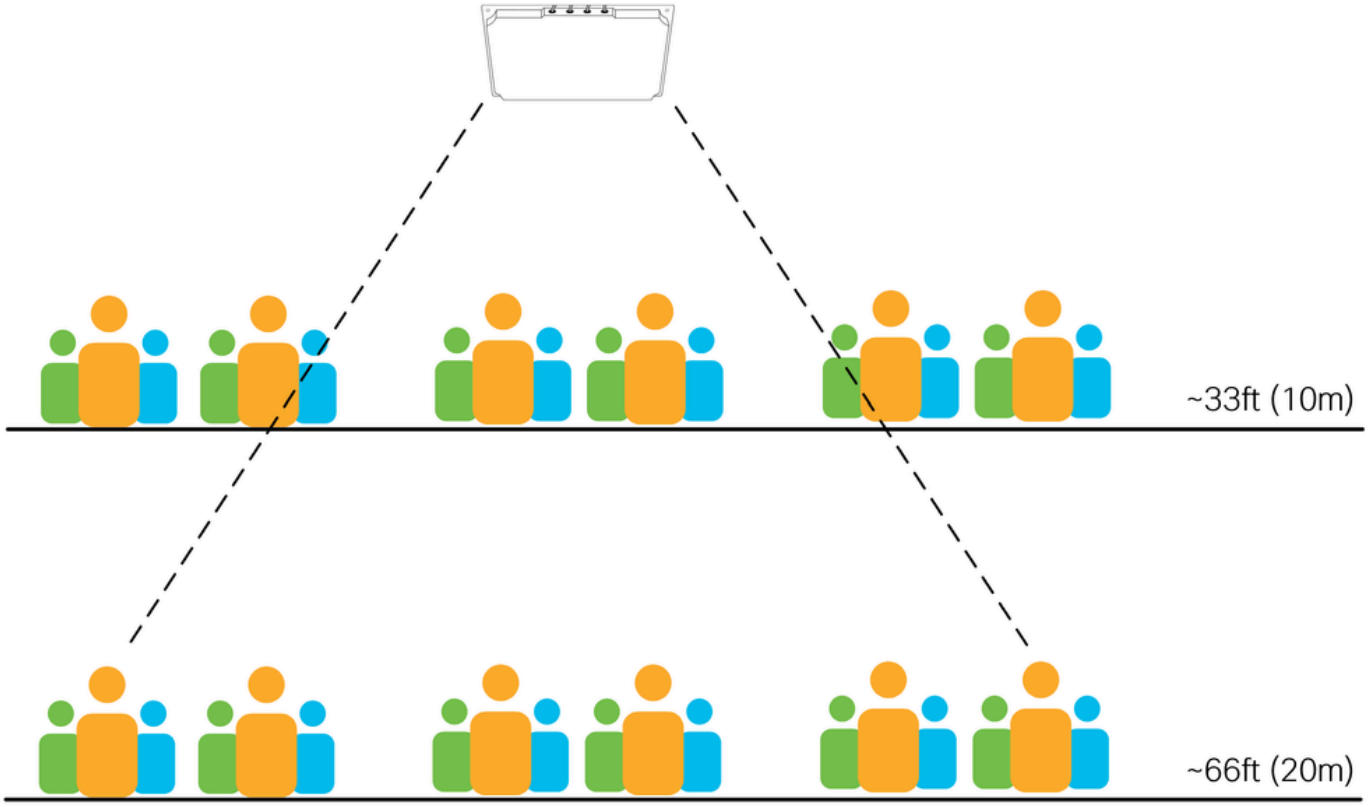
天線清單

選擇天線時，需要考慮的主要因素是天線波束寬度和天線安裝距離/高度。下表顯示了每個天線的5GHz波束寬度，括弧中的數字顯示圓角（且更易於記憶）值。

表中建議的距離不是硬性規則，而是基於經驗的指南。無線電波以光速移動，到達任意距離後不會簡單地停止。天線的工作距離均超出建議距離，但是，效能會隨著距離的增加而下降。安裝高度是規劃過程中的關鍵因素。

下圖顯示同一天線在高密度區域約33英呎（10公尺）和約66英呎（20公尺）的兩個可能安裝高度。請注意，天線可以看到（並接受來自）的客戶端數量會隨著距離增加而增加。隨著距離變長，維持更小的電池尺寸變得更具挑戰性。

一般說來，使用者密度越高，在指定距離內使用正確的天線就顯得越重要。



體育場天線

C9104體育場天線非常適合用於遠距離覆蓋高密度區域，請參閱Catalyst 9104體育場天線(C-ANT9104)部署指南瞭解相關資訊。

隨時間而變化

隨著時間推移，物理環境的變化在幾乎所有無線安裝中都很常見（例如內牆移動）。定期現場檢查和目視檢查始終是推薦的做法。對於事件網路來說，處理音訊和照明系統，以及在很多情況下處理其他通訊系統（例如5G）會更加複雜。所有這些系統通常安裝在使用者上方的高架位置，有時會導致對同一空間的爭用。無線體育場天線的理想位置通常也是5G天線的理想位置！此外，隨著時間推移，這些系統也會升級，因此可能會被重新定位到干擾和/或主動干擾無線系統的位置。務必跟蹤其他安裝情況，並與安裝這些系統的團隊進行溝通，以確保所有系統都安裝在適當的位置，而不會彼此干擾（物理或電磁干擾）。

高密度和6GHz

在撰寫本文時，外部天線只能選擇有限的6GHz頻段。只有CW9166D1整合AP/天線才能以6GHz的頻率工作，Cisco Catalyst CW9166D1存取點部署指南中提供了詳細的天線規格。CW9166D1提供6GHz的覆蓋範圍，波束寬度為60°x60°，可有效地用於任何滿足此類天線條件的部署。例如，聽眾廳和倉庫是CW9166D1部署的良好候選，因為整合裝置提供室內使用的定向天線功能。

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

9166D1

在大型公共網路環境中，這些網路通常具有各種大型區域，並且需要在各種高度上使用天線組合。由於距離仿製，僅使用60°x60°天線來端到端部署大型公共網路可能非常困難。因此，對於大型公共網路而言，僅使用CW9166D1來提供6GHz的端到端覆蓋也具有挑戰性。

一種可能的方法是使用5GHz作為主覆蓋頻帶，而僅在特定區域使用6GHz將支援客戶端裝置解除安裝到較乾淨的6GHz頻帶。這種型別的做法在較大的區域使用5GHz天線，同時在可能和需要額外容量的地方使用6GHz天線。

例如，在貿易會議中考慮大型活動廳，主大廳使用體育場天線提供5GHz的主覆蓋，安裝的高度要求使用體育場天線。在本例中，由於距離限制，CW9166D1不能用於主大廳，但可有效用於需要更高密度的鄰近VIP大廳或印刷機區。本文檔稍後將介紹在5GHz和6GHz頻帶之間漫遊的客戶端。

法規

與5GHz一樣，6GHz的可用電源和通道在法規領域之間差異很大。特別要注意的是，FCC和ETSI域之間的可用頻譜有很大的差異，並且對於室內和室外使用的可用Tx功率、低功率室內(LPI)和標準功率(SP)有嚴格的規定。使用6GHz時，其他限制包括使用者端電源限制、使用外部天線與天線向下傾斜，以及SP部署所需的自動頻率協調(AFC)（目前僅限美國地區）。

有關Wi-Fi 6E的詳細資訊，請參閱Wi-Fi 6E：Wi-Fi白皮書的下一篇重要章節。

無線電資源管理

無線電資源管理(RRM)是負責控制無線電操作的一組演算法。本指南參考兩個關鍵的RRM演算法，即動態通道分配(DCA)和傳輸功率控制(TPC)。RRM是靜態通道和電源配置的替代方案。

- DCA按照可配置的計畫運行（預設值為10分鐘）。
- TPC按自動計畫運行（預設值為10分鐘）。

Cisco Event Driven RRM (ED-RRM)是一個DCA選項，它允許在標準DCA計畫之外做出通道更改決定，通常是為了應對嚴重的RF情況。當檢測到過多的干擾水準時，ED-RRM可以立即更改通道。在噪音和/或不穩定的環境中，啟用ED-RRM會導致通道更改過多的風險，這對客戶端裝置有潛在負面影響。

建議使用RRM，而且一般都優先於靜態配置-但是，某些注意事項和例外情況除外。

- TPC必須根據需要使用TPC最小/最大設定限制為有限的值範圍，並且始終與RF設計保持一致。
    - 在高密度環境中啟用TPC通道感知。

- DCA週期必須從10分鐘的預設設定更改。
    - 請勿在HD環境中使用ED-RRM。
    - 停用避免Cisco AP載入。
    - 如果有多個惡意程式，惡意AP避免選項(如避免外部AP干擾)可能會導致環境不穩定。移除惡意程式總比嘗試回應要好。
- RRM決策可能受到無法正確偵聽彼此的AP/天線的影響，例如定向天線相互指向遠方。
- 某些天線（例如C9104）不支援RRM，並且始終需要靜態配置。
- RRM無法修復不良的RF設計。

在所有情況下，RRM的部署必須理解預期結果，並調整為在適用於給定RF環境的邊界內運行。本文檔的後續部分詳細探討了這些要點。

RF配置

頻道

一般來說，頻道越多越好。在高密度部署中，所部署的AP和無線頻段可能會比可用通道多幾個數量級，這意味著通道重複使用率較高，而且同通道干擾級別也較高。必須使用所有可用頻道，一般不建議限制可用頻道清單。

某些情況下，特定（和獨立的）無線系統需要共存於同一物理空間，並且必須為其分配專用通道，同時從主系統的DCA清單中刪除已分配的通道。這些型別的通道排除必須非常仔細地評估，並且僅在必要時使用。例如，點對點鏈路在與主網路相鄰的開放區域內工作，或者在體育場內的印刷機區域內工作。如果從DCA清單中排除了一個或兩個以上的通道，則會導致重新評估建議的解決方案。在某些情況下，例如密度非常高的體育場館，甚至排除單個通道有時也不可行。

動態通道分配(DCA)可以與基於WLC的RRM或AI增強的RRM一起使用。

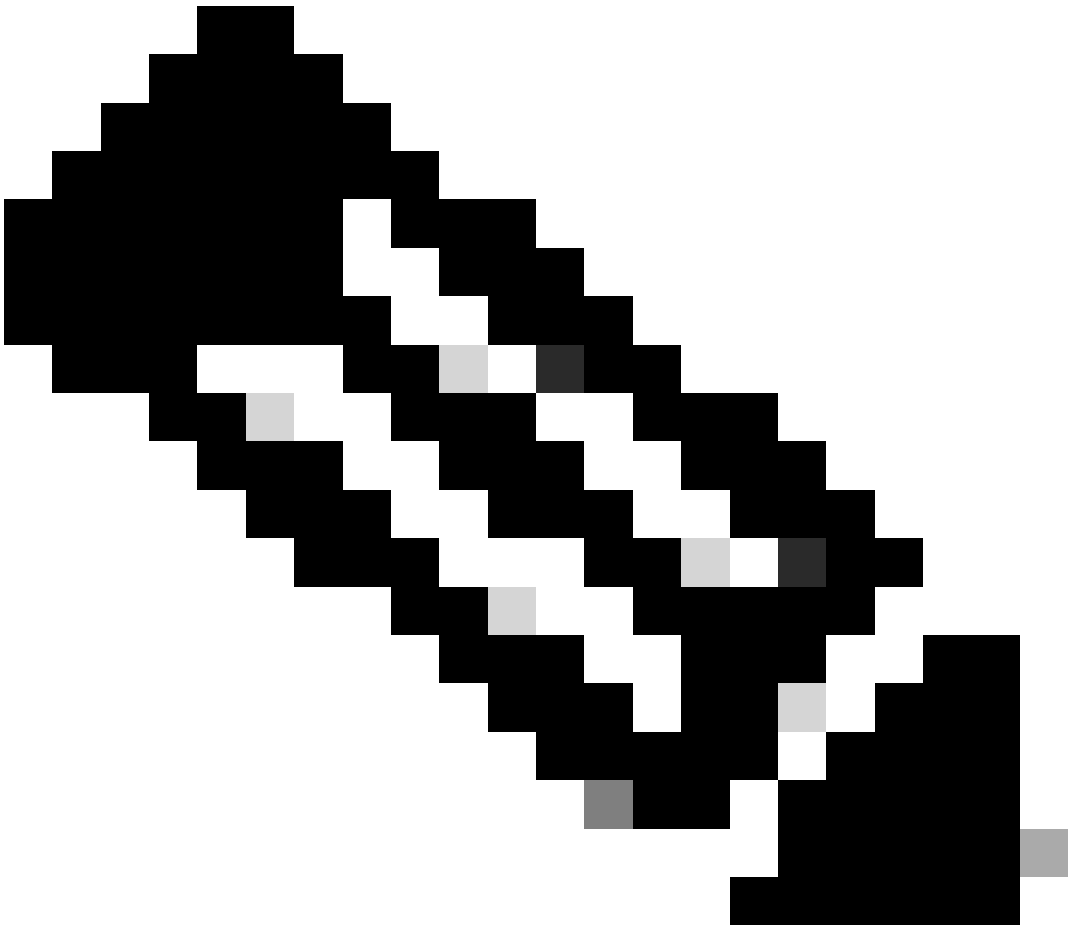
預設DCA間隔為10分鐘，這可能會導致不穩定的RF環境中頻繁發生通道更改。在所有情況下，預設DCA計時器都必須從預設的10分鐘增加，並且特定DCA間隔必須與所討論網路的運行要求保持一致。示例配置可以是：DCA間隔4小時，錨點時間8。這樣，從上午8點開始，通道更改將限制為每4小時一次。

由於干擾是必然發生的，因此適應每個DCA週期並不一定有價值，因為許多干擾都是暫時的。一個

好的方法是在最初幾個小時使用自動DCA，並在您滿意的穩定資料後凍結演算法和通道計畫。

重新啟動WLC後，DCA在主動模式下運行100分鐘，以查詢適當的通道計畫。當RF設計發生重大更改（例如增加或刪除多個AP或更改通道寬度）時，最好手動重新啟動該過程。要手動啟動此過程，請使用此命令。

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



注意：通道更改可能會對客戶端裝置造成中斷。

2.4吉赫

2.4GHz頻段經常受到批評。它只有三個不重疊的通道，而且除了Wi-Fi以外，還有許多其他技術也在使用它，這會產生不必要的干擾。一些組織堅持要提供這方面的服務，那麼合理的結論是什麼？事實上，2.4GHz頻段不能為終端使用者提供令人滿意的體驗。更糟糕的是，如果嘗試以

2.4GHz提供服務，則會影響其他2.4GHz技術，例如藍芽。在大型場地或活動中，許多人仍然期望在撥打電話時無線耳機能夠正常工作，或智慧可穿戴裝置能夠照常工作。如果您的密集Wi-Fi以2.4GHz運作，您將會影響那些甚至未使用2.4GHz Wi-Fi的裝置。

有一點是肯定的，如果您確實必須提供2.4GHz Wi-Fi服務，最好在單獨的SSID上執行此操作（專門用於IoT裝置或將其稱為「傳統」）。這意味著雙頻裝置不會非自願地連線到2.4GHz，並且只有單頻2.4GHz裝置連線到該裝置。

Cisco不建議或不支援在2.4GHz中使用40MHz通道。

5 GHz

高密度無線的典型部署。儘可能使用所有可用頻道。

通道數量因管制範圍而異。考慮雷達在特定位置的影響，儘可能使用DFS通道（包括TDWR通道）。

所有高密度部署都高度建議使用20MHz通道寬度。

40MHz可用於2.4GHz的相同基礎，這僅用於絕對需要的時機（和位置）。

評估特定環境中40MHz通道的需求和實際優勢。40MHz通道需要更高的訊雜比(SNR)才能實現吞吐量的任何可能的改進，如果不可能有更高的SNR，那麼40MHz通道就無用武之地。高密度網路將所有使用者的平均吞吐量優先於任何單個使用者的潛在較高吞吐量。與使用40MHz作為輔助通道的AP僅用於資料幀相比，在20MHz通道上放置更多的AP要好得多，因此使用效率比使用兩個不同的無線電信元（每個信元都以20MHz運行）要低得多（就總容量而言，而不是就單個客戶端吞吐量而言）。

6GHz

6GHz頻段尚未在每個國家提供。此外，某些裝置具有支援6GHz的Wi-Fi網路卡，但需要BIOS更新，才能針對您在其中操作裝置的特定國家啟用該網路卡。客戶目前發現6GHz無線電最常用的方式是透過5GHz無線電上的RNR廣告。這意味著6GHz不能在同一AP上單獨運行，沒有5GHz無線電。6GHz用於解除安裝客戶端和來自5GHz無線電的流量，並為有能力的客戶端提供通常更好的體驗。6GHz通道允許使用較大的通道頻寬，但很大程度上取決於管理域中的可用通道數量。歐洲有24個6GHz通道，因此與5GHz中可能使用的20MHz相比，使用40MHz通道提供更好的最大吞吐量並非不合理。在美國，通道數量幾乎是美國的兩倍，使用40MHz是理所當然之事，即使使用80MHz對於密度較大的事件來說也是不合理的。在高密度活動或場地中不得使用較大的頻寬。

資料速率

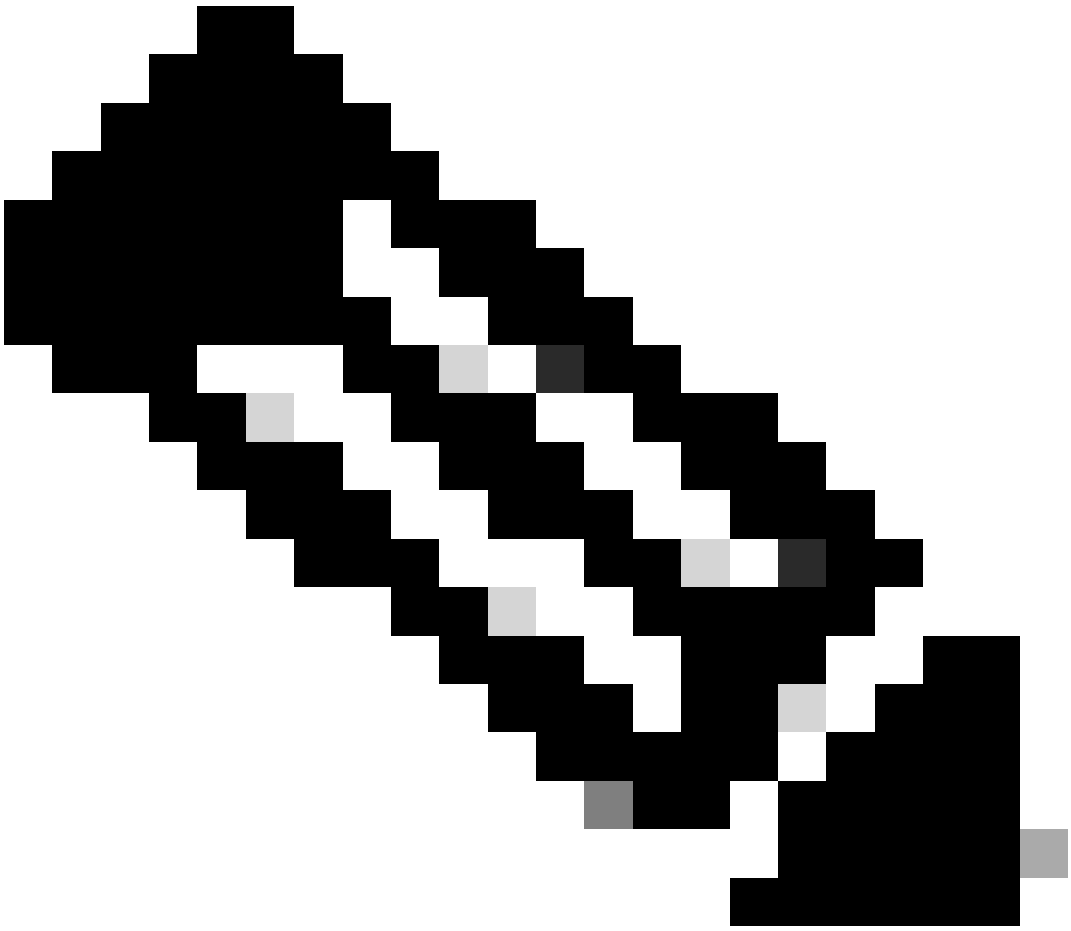
客戶端與AP協商的資料速率主要是該連線的訊雜比(SNR)的函式，而相反的情況也成立，即較高的資料速率需要較高的SNR。事實上，SNR決定最大可能的鏈路速度，但為什麼在配置資料速率時這一點很重要？這是因為一些資料速率具有特殊的意義。

傳統OFDM (802.11a)資料速率可以配置為以下三種設定之一：停用、支援或強制。OFDM速率是（以Mbps為單位）：6、9、12、18、24、36、48、54，客戶端和AP都必須支援一個速率才能使用。

支援- AP將使用速率

強制- AP將使用速率，並將使用此速率傳送管理流量

已停用- AP將不會使用該速率，從而強制客戶端使用另一個速率



註：強制匯率也稱為基本匯率

強制速率的意義在於，所有管理幀都使用此速率傳送，廣播和多播幀也是如此。如果配置了多個必需速率，管理幀將使用配置的最低必需速率，而廣播和組播使用配置的最高必需速率。

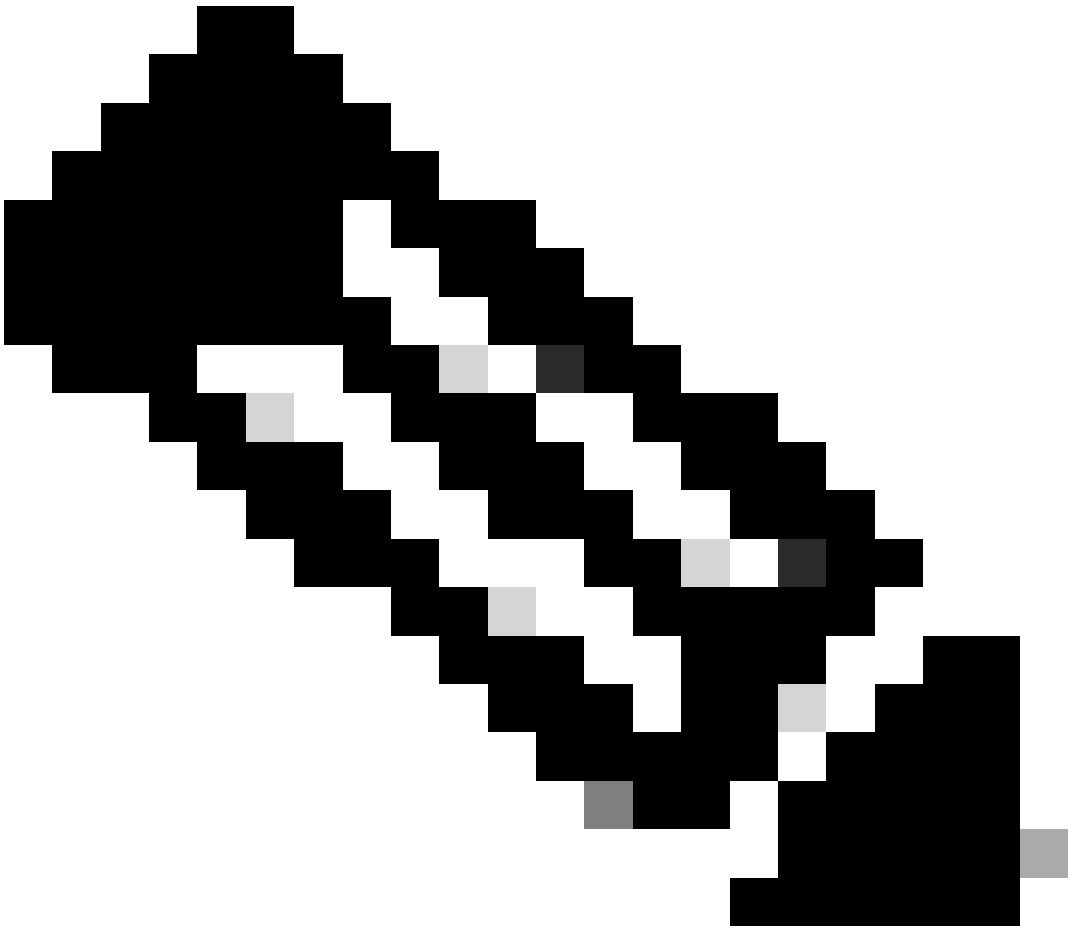
管理幀包括客戶端必須偵聽才能與AP關聯的信標。增加強制速率也會增加該傳輸的SNR要求，回想一下，較高的資料速率需要較高的SNR，這通常意味著客戶端需要更接近AP才能解碼信標並進行關聯。因此，透過操縱強制性資料速率，我們還可以操縱AP的有效關聯範圍，迫使客戶端更接近AP或做出可能的漫遊決定。接近AP的客戶端使用更高的資料速率，而更高的資料速率使用更少的傳輸時間-預期效果是更高效率的信元。請務必記住，提高資料速率只會影響某些幀的傳輸速率，而不會影響天線的RF傳播或干擾範圍。仍需要良好的射頻設計實踐來最小化同通道干擾和雜訊。

相反，將較低速率保留為必需速率通常意味著客戶端可以從更遠的距離建立關聯，這在較低的AP密度情況下很有用，但在較高密度的情況下可能會造成漫遊混亂。任何嘗試定位廣播6Mbps的惡意AP的人都知道，您可以檢測到遠離其物理位置的AP！

關於廣播和多播的主題，在某些情況下，第二個（較高）強制速率被配置為增加多播流量的傳送速率。這很少會成功，因為組播永遠不會得到確認，也不會在幀丟失時重新傳輸。由於某些丟失在所有無線系統中都是固有的，因此無論配置的速率如何，某些組播幀都必然會丟失。可靠組播傳送的更好方法是組播到單播轉換技術，將組播作為單播流傳輸，這具有更高的資料速率和可靠（已確認）傳送的優點。

建議僅使用單一強制費率，停用低於強制費率的所有費率，並將高於強制費率的所有費率保留為受支援。具體使用速率取決於使用案例，如前所述，較低的速率適用於密度較低和AP之間距離較大的室外場景。對於高密度和事件網路，必須停用低速率。

如果您不確定從哪裡開始，請將12Mbps的必要速率用於低密度部署，將24Mbps用於高密度部署。事實證明，許多大型活動、體育場甚至高密度企業辦公室部署都能可靠地運行24Mbps的強制性速率設定。對於需要低於12Mbps或高於24Mbps速率的特定使用案例，建議進行適當的測試。

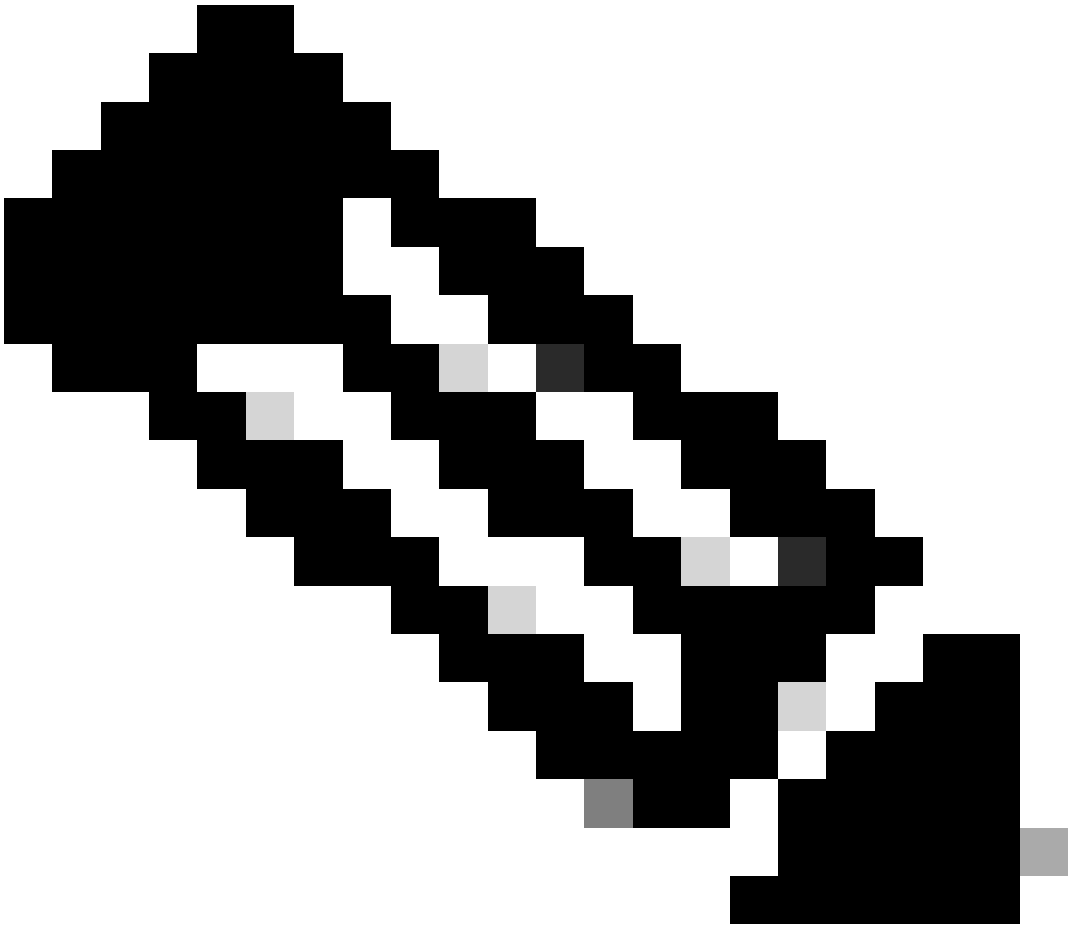


注意：最好是啟用所有802.11n/ac/ax速率（WLC GUI的「高吞吐量」部分中的所有速率），很少需要停用其中任何速率。

傳輸功率

傳輸功率建議因部署型別而異。在此，我們將使用全向天線的室內部署與使用定向天線的室內部署區分開來。這兩種天線型別都可以在大型公共網路中存在，儘管它們通常覆蓋不同型別的區域。

對於全向部署，通常使用自動傳輸功率控制(TPC)，具有靜態配置的最小閾值，在某些情況下也具有靜態配置的最大閾值。



注意：TPC閾值是指無線電發射功率和排除天線增益。請務必確保天線增益已針對所使用的天線型號正確配置，在內部天線和自辨識天線的情況下，此操作將自動完成。

範例 1

TPC最小：5dBm，TPC最大：最大(30dBm)

這將導致TPC演算法自動確定發射功率，但絕不會低於配置的5dBm最小閾值。

範例 2

TPC最小：2dBm，TPC最大：11 dBm

這將導致TPC演算法自動確定發射功率，但始終保持在2dBm和11dBm之間。

一個好方法是建立具有不同閾值的多個RF配置檔案，例如低功率(2-5dBm)、中等功率(5-11dbM)和高功率(11-17dBM)，然後根據需要為每個射頻配置檔案分配全向AP。每個RF配置檔案的值都可以根據預期的使用情況和覆蓋範圍進行調整。這允許RRM演算法動態運行，同時保持在預定義邊界內。

定向天線的方法非常類似，唯一的區別是所需的精度級別。在部署前的RF勘測期間，必須設計並驗證定向天線的放置，而此過程通常會使用特定的無線電配置值。

例如，如果天花板安裝貼片天線需要覆蓋約26英呎（8公尺）高度內的特定區域，則RF勘測必須確定達到此預定覆蓋範圍所需的最小Tx功率（這確定RF配置檔案的最小TPC值）。同樣地，在同一RF調查中，我們會瞭解此天線與下一天線之間可能需要的重疊，甚至我們希望覆蓋範圍結束的時間-這將為RF配置檔案提供最大TPC值。

定向天線的RF配置檔案通常配置有相同的最小和最大TPC值，或者配置有範圍很窄的可能值（通常小於<= 3dBm）。

首選使用RF配置檔案來確保配置的一致性，不建議對單個AP進行靜態配置。最好根據覆蓋區域、天線型別和使用案例來命名RF配置檔案，例如RF-Auditorium-Patch-Ceiling。

正確的Tx功率量是指預期覆蓋範圍內最弱的客戶端達到所需的SNR值，並且不超過該值。30dBm是真實世界條件下（即人滿為患的場所）的極佳客戶端SNR目標值。

CHD

覆蓋空洞檢測(CHD)是辨識和補救覆蓋空洞的單獨演算法。CHD是全局配置的，也是根據WLAN配置的。CHD的可能影響是增加Tx功率以補償覆蓋盲區（客戶端始終檢測到訊號較差的區域），此影響在無線電級別上並影響所有WLAN，即使由為CHD配置的單個WLAN觸發也是如此。

大型公用網路通常使用RF設定檔設定為特定的功率等級，有些可以位於使用者端漫遊進出區域的開放區域，不需要演演算法來動態調整AP Tx功率以回應這些使用者端事件。

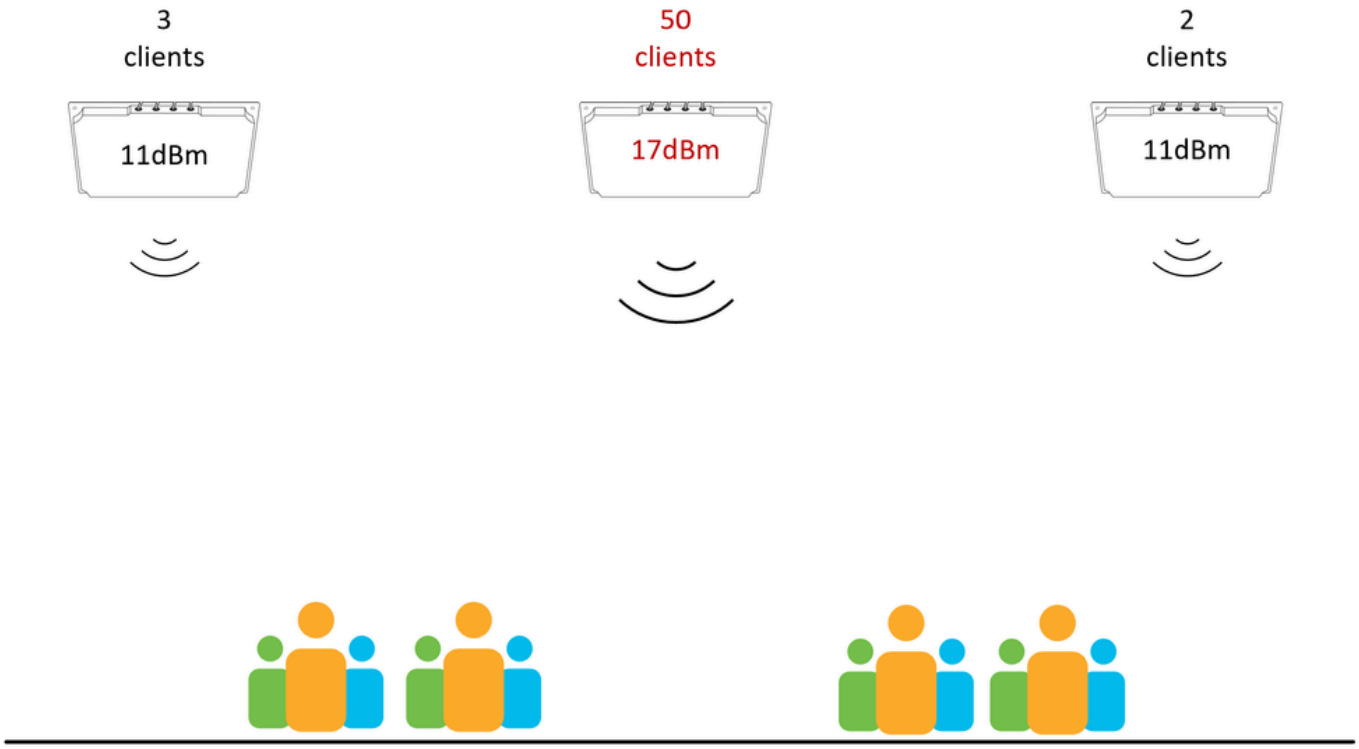
大型公共網路必須全局停用CHD。

功率平衡

大多數客戶端裝置在選擇要與哪個AP關聯時，會首選較高的接收訊號。必須避免配置AP時AP的Tx功率遠高於其他周圍AP的情況。以較高的Tx功率運行的AP會吸引更多的客戶端，導致AP之間的客戶端分佈不均（例如，單個AP/無線電過載了客戶端，而周圍AP的利用不足）。在多天線覆蓋範圍較大的部署中，以及在一個AP連線了多個天線的情況下，這種情況很常見。

選擇Tx電源作為天線波束重疊設計時，體育場天線（例如C9104）需要特別小心，請參閱Catalyst 9104體育場天線(C-ANT9104)部署指南瞭解詳細資訊。

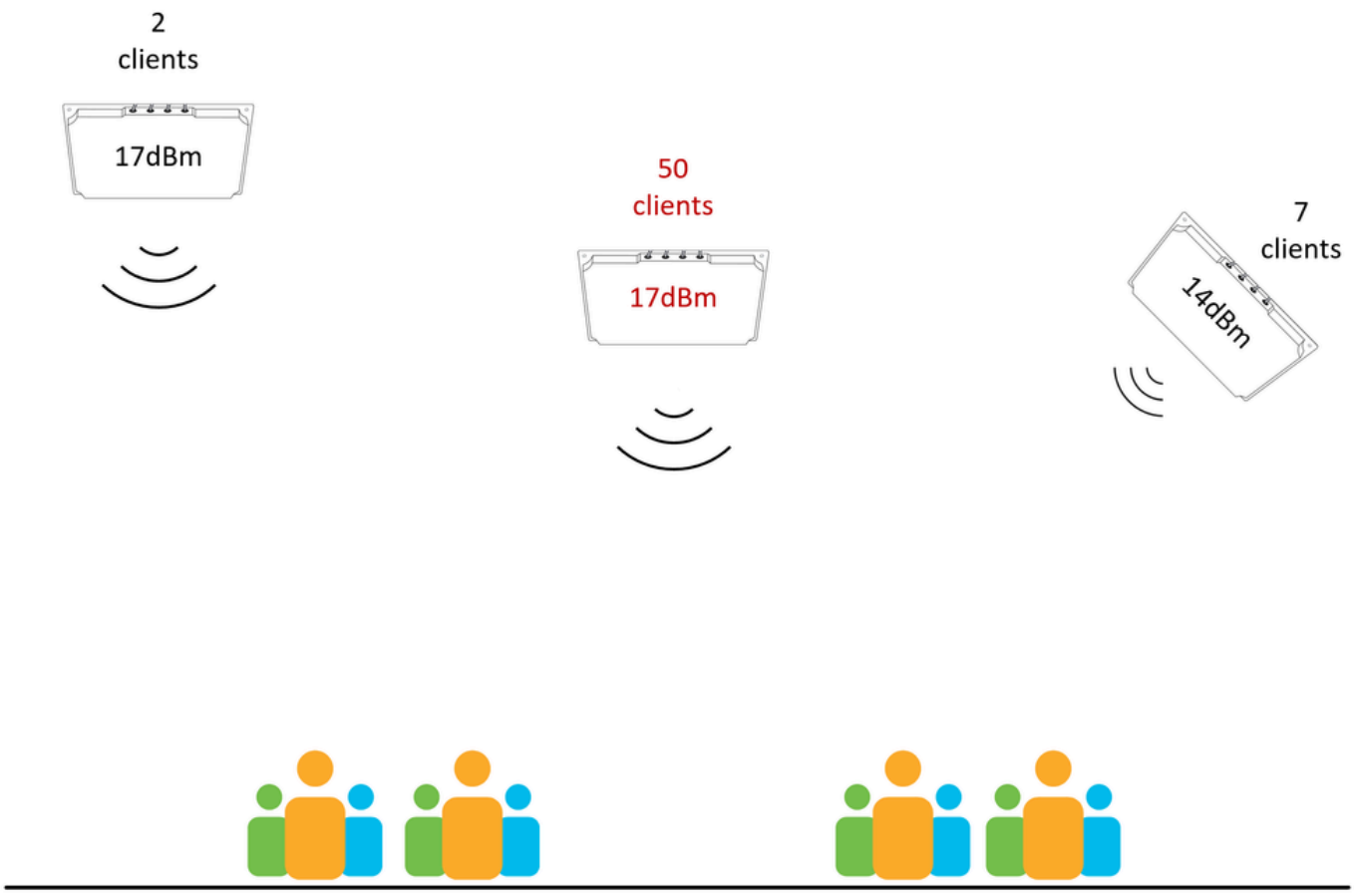
在下圖中，中間天線配置的Tx功率高於周圍天線。此配置可能會導致客戶端「粘滯」到中間天線。



功率高於其鄰居AP的AP會吸引周圍的所有客戶端

下圖顯示的情況較為複雜，並非所有天線的高度都相同，而且並非所有天線都使用相同的傾斜/定向。與簡單地配置所有無線電裝置使用相同的Tx功率相比，實現均衡功率更為複雜。在諸如此類的場景中，可能需要進行部署後站點勘察，這樣可以從客戶端裝置的角度（在地面上）檢視覆蓋範圍。然後，可使用調查資料來平衡配置，以獲得最佳覆蓋範圍和客戶端分佈。

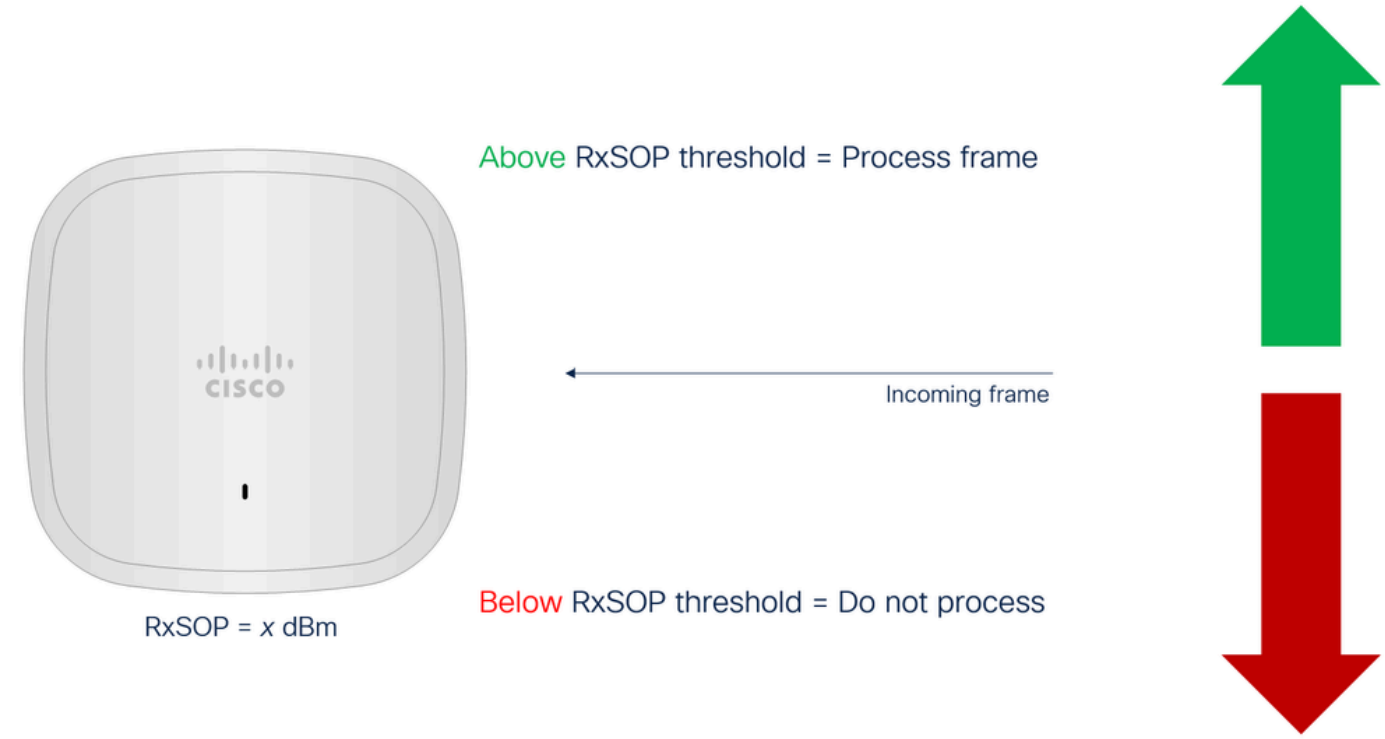
設計統一的無線存取點放置位置來避免類似複雜的情況，是防止具有挑戰性的RF調整場景的最佳方法（儘管有時沒有其他選擇！）。



儘管Tx功率相似，但一個AP正在吸引所有客戶端，但高度和角度在其中起著作用

RxSOP

與諸如發射功率或資料速率等影響發射單元特性的機制不同，RxSOP（接收方開始分組檢測）旨在影響接收單元的大小。實際上，RxSOP可以視為雜訊閾值，因為它定義了接收訊號電平，AP在該電平以下不會嘗試解碼傳輸。到達訊號電平小於配置的RxSOP閾值的所有傳輸均不由AP處理，並被有效視為雜訊。



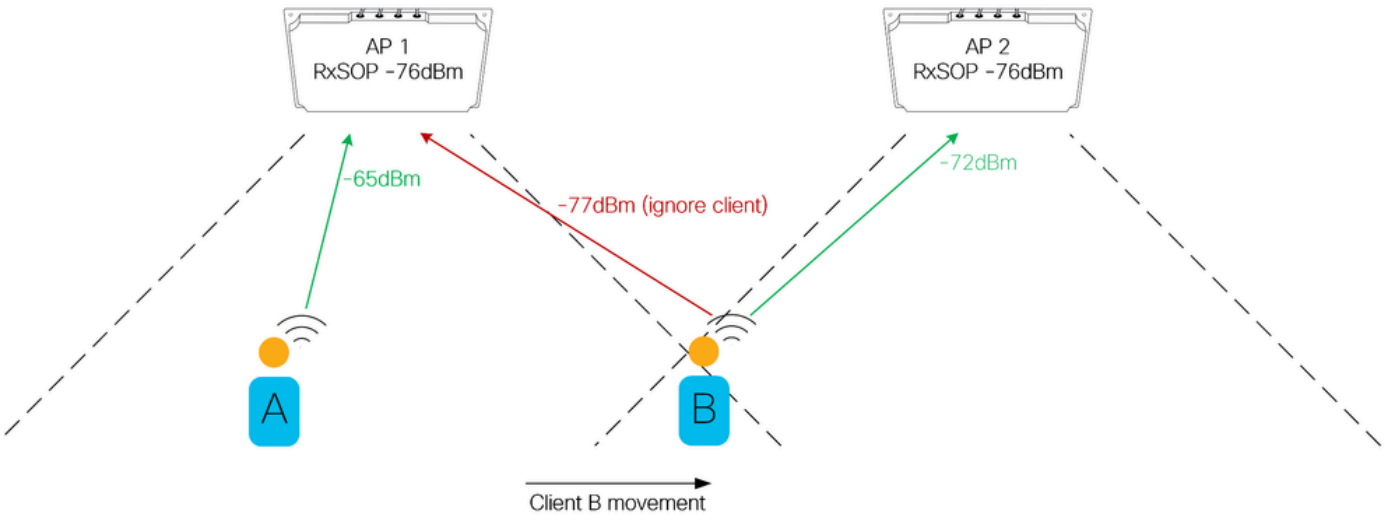
RxSOP概念說明

RxSOP的意義

RxSOP具有多種用途。它可用於提高AP在雜訊環境中傳輸的能力，控制天線之間的客戶端分佈，以及最佳化較弱和粘滯的客戶端。

在嘈雜的環境中，請回想一下，在傳輸802.11幀之前，傳輸站（此例中的AP）首先需要評估介質的可用性，此過程的一部分是先偵聽已經發生的傳輸。在密集Wi-Fi環境中，許多AP通常會在相對有限的空間內共存，且通常使用相同的通道。在這種繁忙的環境中，AP可以報告周圍AP的通道利用率（包括反射），並延遲其自身的傳輸。透過設定適當的RxSOP閾值，AP可以忽略那些較弱的傳輸（感知通道利用率的降低），從而帶來更頻繁的傳輸機會和提高的效能。AP報告沒有任何客戶端負載的顯著通道利用率（例如>10%）的環境（例如，空場地）是RxSOP調整的良好候選環境。

對於使用RxSOP的客戶端最佳化，請考慮下圖。



受rxsop影響的客戶端漫遊

在本示例中，有兩個具有明確定義的覆蓋區域的AP/天線。客戶端B正在從AP1的覆蓋區域進入AP2的覆蓋區域。存在一個交叉點，AP2在此點比起AP1更好地偵聽客戶端，但客戶端尚未漫遊到AP2。這是一個很好的示例，說明了設定RxSOP閾值可以如何強制執行覆蓋區域的邊界。確保客戶端始終連線到最接近的AP，透過消除以較低資料速率服務的遠端和/或弱客戶端連線來提高效能。以此方式配置RxSOP閾值需要透徹瞭解每個AP的預期覆蓋區域的開始和結束位置。

RxSOP的危險。

過於積極地設定RxSOP閾值會導致覆蓋盲區，因為AP無法解碼來自有效客戶端裝置的有效傳輸。由於AP不響應，這可能會給客戶端帶來不良後果；畢竟，如果沒有聽到客戶端傳輸，就沒有理由做出響應。必須謹慎調整RxSOP閾值，始終確保配置的值不會排除覆蓋區域內的有效客戶端。請注意，一些客戶端無法很好地響應被以這種方式忽略，過於積極的RxSOP設定無法讓客戶端有機會自然漫遊，從而有效地強制客戶端找到另一個AP。可以從AP解碼信標的客戶端假定它能夠向該AP傳輸，因此，RxSOP調整的意圖是將接收信元的大小與AP的信標範圍相匹配。請記住，（有效的）客戶端裝置並不總是能直接到達AP，訊號通常會被背向天線或將其裝置放在袋子或口袋中的使用者衰減。

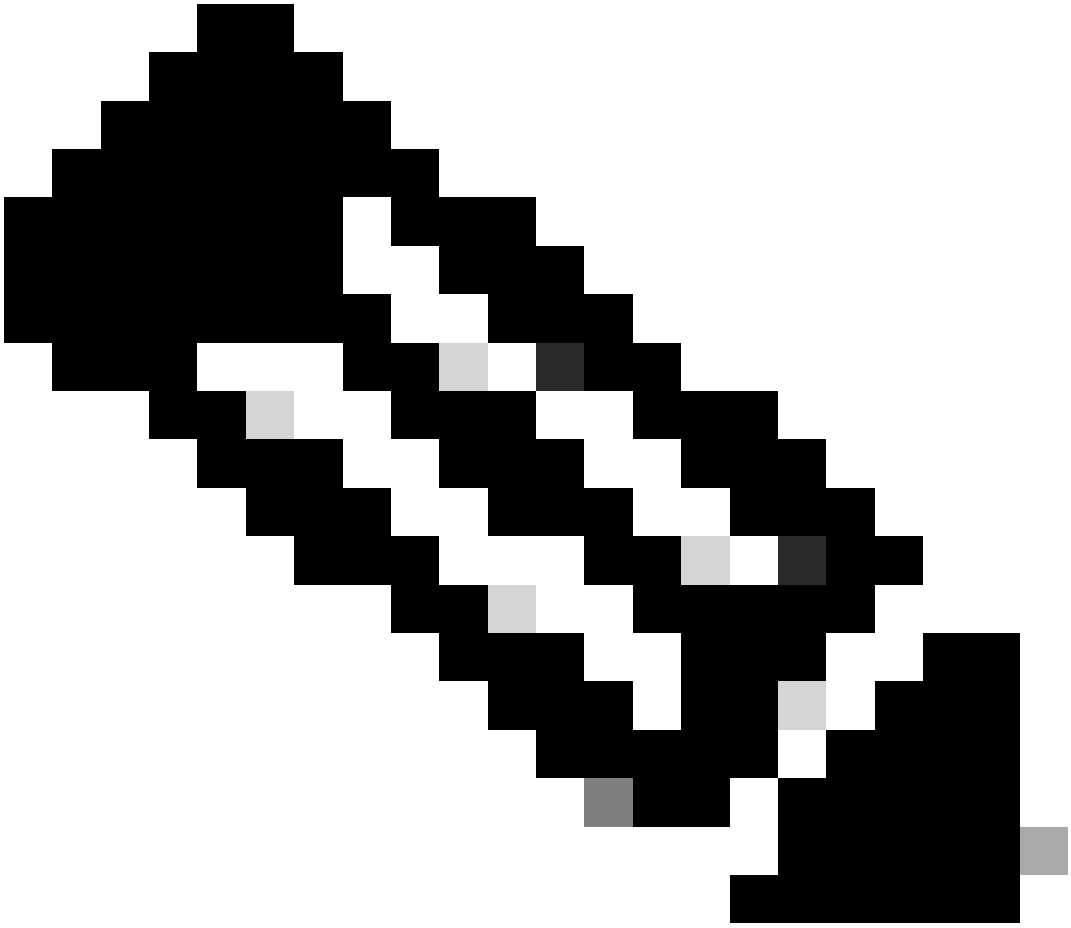
配置RxSOP

根據RF配置檔案配置RxSOP。

每個頻段都有預設的臨界值（低/中/高）會設定預先定義的dBm值。這裡的建議是始終使用自定義值，即使預期值是可用的預設，這樣配置也更易讀。

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

RxSop設定表格



注意：RxSOP更改不需要無線電重置，並且可以動態完成。

擴展網路

一般而言，使用裝置達到其記錄功能的最大限度是一個壞主意。資料表報告了真實情況，但所提及的數字可能處於特定的活動狀態。無線控制器經過測試和認證，可支援一定數量的客戶端和AP以及特定的吞吐量，但這不是假設客戶端每秒漫遊一次、您可以為每個客戶端配置超長唯一ACL或啟用所有可用的監聽功能。因此，必須仔細考慮所有方面，以確保網路在高峰時段進行擴展，並為未來成長保持安全邊際。

存取點數量

部署任何網路的首要任務之一是編制適當的裝置預算和訂購數量，而最大的可變因素則是存取點和天線的數量和型別。無線解決方案必須始終基於射頻設計，但是（不幸的是），這通常是專案生命週期的第二步。在簡單的室內企業部署中，有許多估計技術可以在無線架構師檢視樓層規劃之前，以合理的確定性級別預測可能需要多少個AP。這種情況下，預測模型也可能非常有用。

對於更具挑戰性的安裝，例如工業、室外、大型公共網路或需要外部天線的任何地方，簡單的估計技術通常是不夠的。在以前的類似安裝中，需要有一定程度的經驗才能充分估計所需裝置的型別和數量。無線架構師進行現場探訪是瞭解複雜場地或設施佈局的最低要求。

本部分提供了有關如何確定給定部署的AP和天線最小數量的準則。最終數量和特定安裝位置始終將透過需求分析和無線電設計流程來確定。

初始物料清單必須基於兩個因素：天線型別和天線數量。

天線型別

這裡沒有捷徑。天線型別取決於需要覆蓋的區域，以及該區域中可用的安裝選項。如果不瞭解物理空間，則不可能確定這一點，這意味著瞭解天線及其覆蓋模式的人需要進行站點訪問。

天線數量

所需裝置的數量可以透過瞭解客戶端連線的預期數量來確定。

每個人的裝置

使用者數量可以透過場館的座位數、售票數量或基於歷史統計的預期遊客數量來確定。每個人類使用者可攜帶多個裝置，通常每個使用者需要多個裝置，但人類使用者同時主動使用多個裝置的能力值得懷疑。主動連線到網路的訪客數量也取決於事件和/或部署的型別。

示例1：一個有80,000個座位的體育場通常沒有80,000個連線裝置，這個百分比通常要低得多。在體育賽事期間，20%的連線使用者比率並不罕見，這表示對於80,000個座位的體育場而言，連線裝置預期數量可能為16,000 (80,000 x 20% = 16,000)。此數字還取決於使用的自行啟用機制，如果使用者需要執行某些操作（例如點選網路門戶），則數字會低於裝置自動自行啟用時的值。自動啟用可以像從之前的活動中記住的PSK一樣簡單，也可以像使用OpenRoaming等更高級的功能，無需使用者互動即可啟用裝置。OpenRoaming網路可以促使使用者使用率遠高於50%，這可能會對容量規劃產生重大影響。

示例2：期望技術會議具有高使用者連線率是合理的。會議出席者花費較長的時間連線網路，並期望能夠存取其電子郵件，並於全天執行日常工作。此類使用者將多個裝置連線到網路的可能性也更大，儘管它們同時使用多個裝置的能力仍值得懷疑。對於技術會議，假設100%的訪客連線到網路，根據會議型別的不同，這個數字可能較低。

在這兩個示例中，關鍵是要瞭解所連線的裝置預期的數量，而且沒有針對每個大型公共網路的單一解決方案。無論哪種情況，天線都會連線到無線電，並且連線到該無線電的是客戶端裝置（非使用者裝置）。因此，每個無線電的客戶端裝置是一個可用度量。

每個無線電的裝置

對於Wi-Fi 6個AP，Cisco AP的最大客戶端計數為每無線電200個連線的裝置；對於Wi-Fi 6E AP，每無線電400個連線的裝置。但是，不建議設計最大客戶端計數。出於規劃目的，建議將每個無線電的客戶端計數保持在遠遠低於最大AP容量的50%。此外，無線電的數量取決於使用的無線存取點型別和天線，單頻和雙5GHz部分對此進行了更詳細的探討。

在此階段，最好將網路劃分為不同的區域，每個區域都有預期的裝置數量。回想一下，本部分旨在

估計AP和天線的最小數量。

以三個不同覆蓋區域的示例為例，為每個區域提供預期客戶端計數，並使用每個無線電75個客戶端的（正常）值來估計所需的無線電數量。

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

每個區域的預期無線電/客戶端計數

這些初始數字現在需要與瞭解每個區域部署的AP和天線型別以及是否使用單或雙5GHz結合使用。6GHz計算遵循與5GHz相同的邏輯。本例中未考慮2.4GHz。

讓我們假設三個區域都使用2566P貼片天線和9104體育場天線的組合，以及單頻和雙5GHz的組合-此場景用於說明目的。

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)

每個區域的天線

每個區域列出所需的天線和AP型別。請注意，在雙5GHz的情況下，比值為兩個天線與一個AP。

本節介紹一種估計部署所需的天線和AP初始數量的方法。此估算需要瞭解物理區域、每個區域可能

的安裝選項、每個區域要使用的天線型別以及預期的使用者端裝置數量。

每次部署都不同，並且通常需要額外的裝置來覆蓋特定或具有挑戰性的領域，這種型別的估計僅考慮客戶容量（而非覆蓋範圍），並用於概述所需投資的規模。最終AP/天線放置位置和裝置總數始終取決於經驗豐富的無線專業人員對使用案例和現場驗證的全面瞭解。

預期傳輸量

每個無線通道可提供一定量的可用容量，通常轉換為吞吐量。此容量在連線到無線電的所有裝置之間共用，這意味著每個使用者的效能都會隨著更多的使用者連線增加到無線電而下降。效能下降並非線性，還取決於連線的客戶端的準確組合。

使用者端功能會因使用者端晶片組以及使用者端支援的空間串流數目而有所不同。下表列出了每個支援空間流數的最大客戶端資料速率。

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

每種客戶端型別預期的最大實際吞吐量

列出的速率是理論上802.11標準衍生的最大MCS（調制和編碼方案）速率，假設訊雜比(SNR) >30dBm。效能良好的無線網路的主要設計目標是為所有位置的所有客戶端實現這種級別的SNR，但這種情況很少發生。無線網路本質上是動態的，並且使用未經許可的頻率，除了客戶端功能外，各種不受控制的干擾也會對客戶端SNR產生影響。

即使在達到所需的SNR水準的情況下，先前列出的速率也不考慮協定開銷，因此，不會直接對映到實際吞吐量（由各種速度測試工具測量）。實際吞吐量始終低於MCS速率。

對於所有無線網路（包括大型公共網路），客戶端吞吐量始終取決於以下因素：

- 客戶端的功能。
- 客戶端在該特定時間點的訊雜比。
- 在該特定時間點連線的其他客戶端的數量。
- 其他客戶端在該特定時間點的功能。
- 其他客戶端在該特定時間點的活動。
- 特定時間點的干擾。

根據這些因素的不同，無論裝置供應商是誰，都無法保證無線網路中每個客戶端的最低吞吐量。

有關詳細資訊，請參閱驗證Wi-Fi吞吐量：測試和監控指南。

WLC平台

選擇您的WLC平台看起來很簡單。首先要考慮的是您打算管理的預估AP計數和客戶端計數。每個WLC平台的資料表都包含平台上支援的所有最大對象：ACL、客戶端計數和站點標籤等。這些都是字面上的最大數目，而且往往很難強制執行。例如，您不能將6001 AP連線到僅支援6000個AP的9800-80。但是，在所有地方都追求最大目標是明智的嗎？

思科無線控制器已經過測試，能夠達到這些最大值，但是它們不一定會同時在所有狀況下達到所有記錄的最大值。讓我們以吞吐量為例，9800-80可以達到高達80Gbps的客戶端資料轉發，但是在這種情況下，每個客戶端資料包的最大和最佳大小均為1500位元組。混合使用資料包大小時，有效最大吞吐量較低。如果啟用DTLS加密，吞吐量會進一步降低，應用可視性也是如此。在已啟用許多功能的大型網路中，預計9800-80路由器在現實狀況下會超過40Gbps。由於這取決於使用的功能和網路活動的型別，因此要真正瞭解容量，唯一的方法就是使用此命令測量資料路徑利用率。請關注load指標，該指標是控制器可以轉發的最大吞吐量的百分比。

```
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#
```

同樣地，9800-80也能正常處理6000個AP。但是，體育場或機場等公共場所的6000個AP不算常規活動。考慮到客戶端漫遊和環境探測的量，最大規模的大型公共網路可能會增加單個WLC上的CPU使用率。如果增加每次客戶端移動時傳送的監控和SNMP陷阱，負載可能會很快變得太多。大型公共場所或大型活動的一個關鍵具體特點是，隨著人們四處移動並不斷關聯/取消關聯，客戶加入活動會顯著增加，因此這會對CPU和控制平面造成額外壓力。

許多部署都表明，單一(HA)對9800-80無線控制器可以處理擁有超過1000個AP的大型體育場部署。對於正常運行時間和可用性是首要考慮的重要事件，通常還會將AP分佈在兩個或更多控制器對上。當大型網路分佈在多個WLC上時，控制器間漫遊會更加複雜，因此必須認真考慮客戶端在體育場碗等封閉空間內的漫遊。

另請參閱本文檔中的站點標籤部分。

WLC高可用性

建議使用高可用性狀態切換(HA SSO)配對，這樣既能提供硬體備援，也能防止軟體故障。使用HA SSO，當輔助WLC無縫接管時，一台裝置上的軟體崩潰對終端使用者是透明的。HA SSO配對的另一項優勢是服務中軟體升級(ISSU)功能提供不中斷的升級。

如果網路足夠大，建議使用額外的控制器(N+1)。它可以滿足HA SSO無法滿足的多個目的。您可以在升級生產配對之前，在此WLC上測試新的軟體版本（並僅將幾個測試AP移轉至其中，以測試網路的特定區段）。某些罕見情況可能會影響HA配對中的兩個WLC（當問題複製到待命時），這裡N+1允許在主動-主動情況下使用安全的WLC，在此情況下您可以逐步在來回遷移AP。它還可以用作配置新AP的調配控制器。

9800-CL具有極高的可擴充性和強大功能。需要注意的是，它們的資料轉發容量要小得多（對於SR-IOV映像，從2 Gbps降至4 Gbps），這往往限制在FlexConnect本地交換場景（在集中交換中可能只有少量AP）。但是，在維護期間或排除故障時，當您需要額外的控制器時，它們可以作為N+1裝置提供幫助。

外部系統

雖然本文檔主要介紹大型事件網路的無線元件，但也有許多支援系統在擴展和設計階段需要考慮，其中一些將在本文中討論。

核心網路

大型無線網路通常以集中交換模式部署，並且子網很大。這意味著大量的客戶端MAC地址和ARP條目被推送到相鄰的有線基礎設施。專用於各種L2和L3功能的相鄰系統必須擁有足夠的資源來處理此負載。對於L2交換機，常見的配置是調整Switch Device Manager (SDM)模板，該模板負責分配系統資源，並根據網路中裝置的功能在L2和L3功能之間實現平衡。確保核心L2裝置能夠支援預期的MAC地址條目數量非常重要。

閘道NAT

公共網路的最常見用例是為訪問者提供網際網路接入。資料路徑上的某個位置必須有一個裝置負責NAT/PAT轉換。Internet網關必須具備處理負載所需的硬體資源和IP池配置。請記住，單個無線客戶端裝置可以負責許多NAT/PAT轉換。

DNS/DHCP

這兩個系統是確保良好使用者端體驗的關鍵。DNS和DHCP服務不僅需要適當的擴展來處理負載，還需要考慮在網路中的位置。與WLC位於同一位置的快速響應系統，可確保最佳體驗並避免客戶端登入時間過長。

AAA/Web門戶

沒有人喜歡速度緩慢的網頁，為外部Web身份驗證選擇適當且擴展良好的系統對於良好的客戶端註冊體驗非常重要。對於AAA，RADIUS身份驗證伺服器也必須能夠滿足無線系統的要求。請記住，在某些情況下，負載可能會在關鍵時刻突然增加，例如在足球比賽期間半小時，這可以在很短的時間內生成較高的身份驗證負載。調整系統規模以適度並行載入是關鍵。使用AAA記帳等功能時必

須特別小心。不惜一切代價避免以時間為基準的會計，並且如果您使用會計，請嘗試停用臨時會計。另一個需要考慮的重要專案是使用負載均衡器，此處必須使用會話計時機制來確保完整的身份驗證流。確保將RADIUS超時保持在5秒或更長時間。

如果使用帶有大量客戶端的802.1X SSID（例如，使用OpenRoaming），請確保啟用802.11r快速過渡(FT)，否則客戶端每次漫遊時都可能導致身份驗證風暴。

DNS/DHCP

關於DHCP的一些建議：

- 確保DHCP池至少是預期客戶端數量的三倍。即使在客戶端斷開連線後，IP仍會保持分配一段時間，因此，根據訪客的駐留時間，這會佔用更多IP地址。嘗試將租用時間與使用者訪問場館的預期持續時間相匹配，如果一般訪問持續時間為2小時，則無需為一週分配IP地址，這有助於淘汰陳舊的租約。
- 建議為客戶端使用一個大型子網，WLC具有代理ARP功能，預設情況下不轉發廣播（DHCP除外）。為客戶端使用大型（例如/16）客戶端子網不會帶來問題。與具有多個VLAN的VLAN組相比，單個大型VLAN更簡單。配置許多較小的子網（例如/24）和VLAN組不會影響廣播域，只會導致配置更加複雜，從而產生諸如髒VLAN和必須跟蹤無法平均使用的各種DHCP池等問題。
- 使用由子網的第3層網關處理的DHCP中繼功能，使無線控制器上的DHCP保持橋接模式。這樣可以實現最大的效率和簡便性。其理念是完全不將無線控制器納入DHCP過程。
- 在任何公共WLAN上使用DHCP Required，無論身份驗證方法為何。雖然這可以觸發一小部分失敗的客戶端關聯，但可以防止出現重大安全問題，無論是客戶端嘗試為自己分配靜態IP地址，還是客戶端行為不當，並且嘗試在未經允許的情況下重複使用以前的IP地址。

運行網路

正確的配置

啟用許多選項以利用現代Wi-Fi的所有最新功能是很誘人的。不過，某些功能在小型環境中效果極佳，但在大型和密集環境中卻影響巨大。同樣地，某些功能也會造成相容性問題。儘管思科裝置遵守所有標準並提供與各種經過測試的客戶端的相容性，但世界上仍有許多獨特的客戶端裝置，這些客戶端裝置有時具有帶有錯誤的驅動程式軟體版本或與某些功能不相容。

根據您對客戶端的控制級別，您必須保持保守。例如，如果您部署Wi-Fi來參加公司的大型年度聚會，您會知道大多數客戶端是公司裝置，您可以相應地規劃啟用功能集。另一方面，如果您運營的是機場Wi-Fi，您的訪客滿意度水平直接與其連線到網路的能力相關，而您對使用者可使用的客戶端裝置沒有任何控制權。

SSID

多少SSID？

建議始終儘量使用較少的SSID。在高密度網路中，由於幾乎可以保證在同一通道上擁有多個AP，這種情況會更加嚴重。通常，許多部署使用過多的SSID，承認它們有太多的SSID，但宣告它

們不能使用更少的SSID。您必須對每個SSID執行業務和技術研究，以瞭解SSID與將多個SSID摺疊為一個SSID的選項之間的相似之處。

讓我們來瞭解一下一些安全/SSID型別及其用法。

WPA2/3個人

預共用金鑰SSID因其簡單性而廣受歡迎。你可以把鑰匙印在胸卡上的某個地方，或者印在紙上，或者標語牌上，或者以某種方式把它傳達給訪客。有時候，即使訪客SSID也首選預共用金鑰SSID（假設金鑰為所有參加者所熟知）。它可以幫助防止由於連線的故意性而導致DHCP池耗盡。經過的裝置不會自動連線到網路，因此無法使用DHCP池中的IP地址。

WPA2 PSK不提供隱私保護，因為流量很容易解密，因為每個人都使用相同的金鑰。相反，WPA3 SAE確實提供私密性，即使每個人都擁有主金鑰，也無法導出其他客戶端使用的加密金鑰。

WPA3 SAE是安全的更好選擇，許多智慧型手機、筆記型電腦和作業系統都支援它。某些IoT裝置或智慧可穿戴式裝置仍然支援有限，如果較舊客戶端未收到最新的驅動程式或韌體更新，則通常容易出現問題。

考慮使用過渡模式WPA2 PSK-WPA3 SAE SSID來簡化某些情況可能很誘人，但此欄位已顯示出來會導致一些相容性問題。程式設計不良的使用者端不會預期在相同SSID上會有兩種型別的共用金鑰方法。如果要提供WPA2和WPA3選項，建議配置單獨的SSID。

WPA2/3企業

WPA3 Enterprise（使用AES 128位元加密）在技術上與WPA2 Enterprise使用相同的安全性方法（至少在SSID信標中通告），可提供最大的相容性。

對於802.1X，建議使用轉換模式SSID，因為最新裝置未出現相容性問題（Android 8或舊Apple IOS版本報告出現問題）。IOS XE 17.12及更高版本允許使用單個過渡企業SSID，其中僅在6GHz上使用和通告WPA3，而5GHz頻段上提供WPA2。我們建議儘快在企業SSID上啟用WPA3。

WPA企業SSID可用於關鍵使用者，這些使用者有一個身份提供程式資料庫，允許根據使用者身份返回AAA引數（例如VLAN或ACL）。此類型別的SSID可以包括Eduroam或OpenRoaming，它們將訪客SSID的優點（透過允許訪客輕鬆連線而無需輸入任何憑證）與企業SSID的安全性結合起來。它們大大降低了通常與802.1X關聯的登入的複雜性，因為只要客戶端在手機上有一個配置檔案（可透過事件應用輕鬆提供），客戶端就無需執行任何操作即可加入歐洲同步漫遊或OpenRoaming SSID

訪客SSID

訪客SSID通常與開放式身份驗證同義。您可以將Web門戶（或不增加）在其後面（取決於所需的友好性或本地要求），其形式多種多樣：外部、本地或中央Web身份驗證，但概念保持不變。使用訪客門戶時，可擴充性在大型環境中可能會迅速成為問題。有關此過程的詳細資訊，請檢視配置可擴充性部分。

6GHz操作要求您的訪客SSID使用增強型開放，而不僅僅是開放。這仍然允許任何人進行連線，但是提供了隱私（比WPA2-PSK更好的隱私！）和加密，所有這些都不提供任何金鑰或證書在SSID上

的連線。主要智慧型手機供應商和作業系統現在支援增強型開放模式，但在無線客戶端群中這種支援還不是很普遍。增強型開放轉換模式提供了良好的相容性選項，其中功能強大的裝置連線到加密的訪客SSID（使用增強型開放），而功能不強的裝置仍然像以前一樣使用SSID進行簡單開放。雖然終端使用者注意到只有一個SSID，但請注意，此過渡模式會在您的信標中廣播兩個SSID（儘管只能看到一個）。

在大型活動和場所中，通常建議在訪客SSID上配置PSK，而不是將其完全保持為開放狀態（增強開放過渡模式會更好，但這樣會建立兩個SSID，並且客戶端相容性仍必須經過廣泛驗證）。雖然這會使註冊過程變得較為複雜（您必須將PSK列印在人們的胸卡或門票上，或者以某種方式將其通告），但是它可避免臨時客戶端自動連線到網路，而無需終端使用者打算使用網路。越來越多的移動作業系統供應商也取消了開放網路的優先順序，並顯示安全警告。在其他情況下，您可能希望連線最大數目的路過者，因此最好選擇打開。

關於SSID數量的結論

對於必須堅持多少SSID的問題，沒有令人滿意的答案。此效果取決於配置的最小資料速率、SSID的數量以及在同一通道上廣播的AP的數量。在思科的一次大型活動中，無線基礎設施使用了5個SSID：主WPA2 PSK、用於安全和6GHz覆蓋的WPA 3 SAE SSID、用於方便教育參與者訪問的企業Eduroam SSID、用於安全地歡迎從事件應用中配置Wi-Fi的任何人的OpenRoaming SSID，以及用於員工和管理網路訪問的單獨的802.1X SSID。 這幾乎已經太多了，但是由於大量的可用通道，並且使用定向天線來儘可能減少通道重疊，因此效果仍然合理。

舊版SSID與主要SSID概念

建議在一定時間段內將2.4GHz服務限制為僅通告為2.4GHz的「傳統」獨立SSID。隨著人們停止提供2.4GHz服務，這種情況越來越少見。然而，這個想法可以而且必須持續下去，但還有其他概念。您想要推出WPA3 SAE，但是轉換模式會造成您的使用者端發生相容性問題？具有WPA2「傳統」SSID和主WPA3 SAE SSID。透過將最低效能的SSID命名為「傳統」，它不會吸引客戶端，您可以輕鬆看到有多少客戶端仍然面臨與您的主SSID的相容性問題，並且需要此傳統客戶端。

但是為什麼停下來呢？您聽到傳言說802.11v導致某些較舊客戶端出現問題，或者某些客戶端驅動程式不希望看到SSID上啟用的裝置分析？在進階主SSID上啟用所有這些方便的功能，並在舊版/相容性SSID上將其關閉。這允許您在主SSID上測試新功能的推廣，同時仍為客戶端提供最大相容性SSID以便回退。這個系統只能這樣運作。如果您將您的相容性驅動型SSID作為主裝置使用相反的名稱，並將您的高級SSID命名為「<name>-WPA3」，您會發現人們堅持使用以前使用的舊SSID，並且在您的「新」SSID上採用多年保持小規模。推出新設定或功能後，由於連線至它的使用者端數目較少，因此不會產生任何結果。

SSID功能

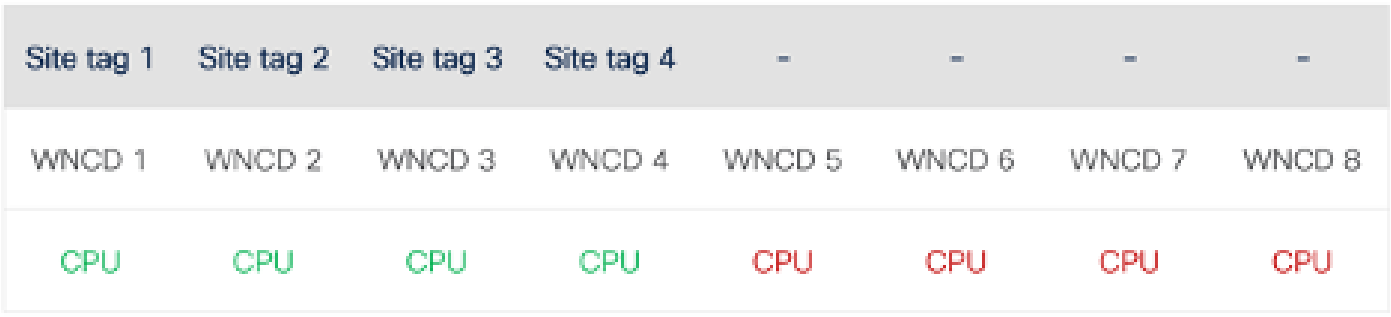
- 最好停用Aironet擴展。這些功能對於站點勘察和WGB操作特別有用，但有時會導致一些舊客戶端出現問題。Aironet IE還會通告AP主機名，這在注重安全的部署中是不需要的。
- CCKM是已被棄用的協定（支援FT），必須停用。
- 此時，最好使用AES-128加密，即使在WPA3中也如此，因為客戶端對更高加密的支援較少（除非您能夠負擔一個特定的更安全和更嚴格的SSID）
- 最好停用「覆蓋盲區檢測」（適用於所有SSID）。大型部署通常使用定向天線，需要進行全面的站點勘察。每個天線的功率電平都是RF設計過程的結果，通常配置為特定電平。

- 必須停用自適應FT，因為當FT未完全通告但存在於某些屬性中時，某些客戶端可能會出現問題。要麼完全停用FT（以實現最大相容性），要麼使用大多數客戶端（除非它們更舊或更面向IoT）支援的FT+802.1X。配置FT+802.1X時，甚至允許非FT客戶端加入SSID。唯一可能發生的問題是某些客戶端無法容忍在相同SSID上看到兩個安全選項。
- 停用802.11ac MU-MIMO。它增加了複雜性，而且在802.11ac中的優勢非常低。
- 停用BSS目標喚醒時間。目前，它在客戶端的採用率很低。
- 停用主動負載均衡和頻寬選擇。如果您未在2.4GHz中通告SSID（或者它位於專用SSID上），則無需進行頻段選擇。如果它堅持連線到已載入的AP，則主動負載均衡會在最終接受客戶端之前拒絕客戶端幾次，從而延遲客戶端關聯。您始終在繁忙環境中載入AP，這對客戶端體驗來說是不利的。
- 停用Fastlane+。
- 停用通用管理，此功能僅適用於3700 AP，並且僅適用於-UX域。如果任其發展，就會造成不必要的攻擊媒介。
- 保持啟用機會金鑰快取(OKC)。對於不支援FT的客戶端，它充當快速漫遊機制。
- 保留WMM允許。停用它會將您的網路帶回802.11g時代，而且要求它不會為9800平台帶來任何優勢。
- 啟用IP源防護。
- 停用RADIUS分析。在非常繁忙的環境中，這會傳送過多的RADIUS計量訊息（只要使用者端執行DHCP或傳送HTTP封包），而且非常有可能超載RADIUS伺服器。
- 避免使用隱藏的SSID。這不能用於任何安全目的，SSID名稱仍可透過簡單的應用程式或透過捕獲嗅探器輕鬆發現。隱藏SSID會降低所有客戶端漫遊的速度，因為它們不再受益於被動信標掃描，必須依靠主動掃描來獲取相鄰AP資訊。
- 嘗試每個無線電使用不超過4個WLAN，因為這會對RF利用率產生重大影響。使用五個WLAN並非硬性限制，但因為使用越來越多的WLAN，所以要非常注意浪費的通話時間。
- 802.11v和802.11k是常用客戶端型別越來越支援的標準。它們通常不會造成客戶端連線問題。它們帶來的好處在很大程度上取決於客戶端如何使用這些協定，有時（在802.11k的情況下）會導致CPU使用率略高。您可以將它們排除在IoT或傳統SSID之外，但必須儘可能在生產SSID上啟用它們。

網站標籤

站點標籤是一項配置專案，允許對共用相同FlexConnect設定以及AP加入配置檔案設定（如憑據、SSH詳細資訊和國家代碼）的存取點進行分組。為什麼站點標籤很重要？站點標籤還定義了Catalyst 9800中的WNCD進程如何處理AP。讓我們舉幾個例子說明：

- 如果您在具有八個WNCD進程的9800-80上配置四個站點標籤，則每個站點標籤會被分配到不同的WNCD進程（在單獨的CPU核心上運行每個進程），而四個WNCD進程不執行任何操作。這表示您並未使用9800-80的所有CPU，因此不建議使用最多支援6000個AP來載入它。



站點標籤平衡的第一個示例

- 如果您在具有八個WNCD進程的9800-80上配置了10個側標籤，則兩個WNCD進程會分別處理兩個站點標籤，而其餘六個進程則處理每個站點標籤。

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

站點標籤平衡的第二個示例

對於具有許多站點和許多站點標籤的地理上大型部署，站點標籤的數量建議為所用平台上WNCD進程數量的倍數。

但是，對於通常位於同一屋頂下的活動網路或位於同一場所的多個建築物，建議是將站點標籤數量與給定平台上WNCD的確切數量相匹配。最終目標是每個WNCD進程（以及分配給無線任務的每個CPU核心）處理大約相似數量的客戶端漫遊事件，從而平衡所有CPU核心的負載。

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

每種平台型別的WNCD進程數

在核心層，真正重要的是將位於同一物理鄰居中的AP分組到同一站點標籤中，以便這些AP之間頻繁發生的客戶端漫遊事件保持在同一個CPU進程中。這意味著，即使您有一個大型場地，建議將該場地分為幾個場地標籤（與處理場地的WNCD流程數量相當），並將AP儘可能按邏輯分組，以形成邏輯RF鄰居組，這些鄰居組也均勻分佈在場地標籤中。

從IOS XE 17.12開始，可以啟用負載均衡演算法，以便WLC根據RF接近度對AP進行分組。這將減輕您的負擔，並在WNCD流程中平衡地分配AP。如果您無法輕鬆繪製要放置到正確數量的站點標籤中的鄰居AP組，這將很有幫助。此演算法的一個特點是，它將AP分配給WNCD進程，而不考慮其站點標籤分配，這意味著它不會更改AP的站點標籤分配。然後，您可以完全根據配置邏輯分配基本站點標籤，並讓演算法以最佳方式在CPU之間平衡AP。

基於RF的自動AP負載均衡功能在Cisco Catalyst 9800系列無線控制器軟體配置指南（Cisco IOS

XE都柏林17.12.x）中進行了介紹。

在大型事件期間，必須監控WNCD進程的CPU使用情況。如果一個或多個WNCD進程顯示高利用率，則可能是WNCD處理過多的AP或客戶端，或者它處理的AP或客戶端比平均值繁忙（如果所有進程經常漫遊，例如在機場）。

策略配置檔案

- 啟用ARP和重複位址偵測(DAD)代理，這允許WLC在裝置嘗試學習無線裝置的MAC位址時，代表無線使用者端回覆。這也會節省無線使用者端的電池。
- 除非有需要，否則請勿啟用WGB功能。
- 啟用所需的DHCP以避免具有靜態IP地址的客戶端。
- 縮短空閒超時（300秒）。有些管理員會花很長的時間來避免使用者端必須重新進行驗證，但長時間的閒置逾時會導致使用者端計數因即時延遲而產生Ghost使用者端專案（影響報告）。最好將閒置-timeout保持在低於組金鑰輪換計時器的水準，以避免在刪除客戶端時泛洪記帳。可以在Web UI中的Configuration > Security > Advanced EAP下將組金鑰輪換間隔配置為「EAP-Broadcast Key Interval」
- 將會話超時設定為86400秒，以避免不必要的斷開和重新身份驗證。

AP加入配置檔案

- 確保啟用TCP adjust MSS。
- 啟用信任DSCP上游。很遺憾，許多無線客戶端不執行802.11e WMM UP標籤，信任DSCP欄位是為語音應用提供正確優先順序的可靠方法。
- 為您的存取點啟用Syslog。配置Syslog伺服器IP可以使AP向其單播其控制檯日誌。它不僅有助於排除AP故障，而且對網路也比預設設定（使AP在本地VLAN中廣播其系統日誌）更有效。AP日誌記錄可能會生成大量消息負載，即使在AP系統日誌未受監控的情況下，設定適當的消息嚴重性和/或配置一個虛擬Syslog IP地址（例如0.0.0.0）以防止廣播消息來限制事件數量仍然是非常好的做法。
- 最大化CAPWAP重試和超時。問題檢測速度較慢，但網路對輕微的瞬時資料包丟棄具有更強的抵抗力。
- 啟用SSH並配置憑證。停用AP控制檯。
- 視需要啟用AP監視器，但不啟用無線電監視器。
- 啟用惡意程式檢測並配置-70 dBm的RSSI閾值。

監控網路

一旦網路啟動並正常運行，您就必須密切監控網路是否存在問題。在標準的辦公環境中，使用者瞭解網路，可以在出現問題時互相幫助，也可以打開內部幫助台故障單。在接待眾多訪客的較大型場所中，您希望重點關注最大問題，而不是那些可能只是配置錯誤的特定人員，因此您需要制定正確的監控策略。

從Catalyst 9800 CLI或GUI監控網路是可能的，但它不是日常監控的最佳工具。如果您已經對問題有懷疑和/或資料，並且希望即時運行特定命令，則這是最直接的方法。主要監控選項包括Cisco Catalyst Center或自定義遙測控制台。可以使用第三方監控工具，但是當使用SNMP作為協定時，資料遠非即時，並且通常的第三方監控工具對於所有無線供應商的特定要求不夠細分。如果選擇SNMP協定，請確保使用SNMPv3，因為SNMPv2的安全性已過期。

Cisco Catalyst Center是最佳選擇，因為它允許您在監控網路的基礎上管理網路。除了監控之外，它還允許即時故障排除和修復許多情況。

如果您希望以永遠線上的方式在螢幕上顯示NOC或SOC的非常特定的指標和構件，自定義遙測控制台會非常有用。如果您想要關注網路的特定領域，您可以構建專用小部件，以您選擇的方式顯示這些領域的網路指標。

對於事件網路，最好監控系統範圍內的RF統計資訊，尤其是通道利用率和每個AP的客戶端數量。這可以從CLI完成，但僅提供特定時間點的快照，通道利用率往往是動態的，更適合隨著時間的推移進行監控。對於這種型別的監控，自定義控制台通常是一種很好的方法。隨時間推移進行監控時更有價值的其他指標包括WNCD利用率、客戶端數量及其狀態，以及特定場所的指標。場所特定指標的一個示例是監控特定區域或位置的使用情況和/或負載，例如會議中心為X 號大廳，或者活動場所為Y 號休息區。

對於自定義監控，NETCONF RPC (pull)和NETCONF流遙測(push)都是有效的方法，儘管將自定義流遙測與Catalyst Center結合使用需要一些調查，因為在WLC上可以配置的遙測訂閱數量有限，並且Catalyst Center預填充（和使用）其中許多遙測訂閱。

使用NETCONF RPC時，需要進行一些測試以確保WLC不會因NETCONF請求而超載，尤其重要的是要記住某些資料點的刷新率以及返回資料所用的時間。例如，AP通道利用率每60秒刷新一次（從AP刷新到WLC），收集1000個AP（從WLC）的RF度量可能需要幾秒鐘，在此示例中，每5秒輪詢WLC沒有幫助，更好的方法是每3分鐘收集一次系統範圍的RF度量。

與SNMP相比，NETCONF始終是首選方案。

不能忽視對核心網路元件的持續監控，包括DHCP池利用率、核心路由器上的NAT條目數量等等。因為其中任何一項的故障都很容易成為無線服務中斷的原因。

大型網路特有的問題

如果您有使用Web驗證的SSID，其中一個問題可能是連線到該SSID並獲得IP地址的客戶端無法進行驗證，因為終端使用者沒有主動嘗試連線（裝置自動連線）。控制器必須攔截處於稱為Web身份驗證掛起且使用WLC資源的狀態的那些客戶端傳送的每個HTTP資料包。網路運行後，請定期檢視在給定時間處於Web身份驗證掛起狀態的客戶端的數量，以檢視其與基線數量的比較。處於IP Learn狀態的客戶端也是如此。當客戶端執行DHCP過程時，您總是讓客戶端處於該狀態，但瞭解網路適當的工作編號有助於設定基線並確定此編號可能過高並指示較大問題的時刻。

對於大型場所，約10%的客戶端處於Web Auth Pending狀態並不罕見。

第2天監控：關注使用者滿意度

一旦網路啟動並正常運行，通常有兩種型別的終端使用者抱怨：他們無法連線，或難以連線（斷開連線），或者Wi-Fi的運行速度比預期慢。後者很難辨識，因為它首先取決於對給定區域的速度和即時密度的預期。讓我們介紹一些有助於您日常監控大型公共場所網路的資源。

驗證Wi-Fi傳輸量：測試和監控指南。本cisco.com文檔說明如何監控網路以發現吞吐量問題。它透過計算客戶端在靜默情況下可以在您的網路中合理預期的吞吐量，並估計隨著客戶端數量和負載增加，這些估計值會下降多少。從技術角度評估終端使用者對吞吐量的投訴是否合法，以及是否需要

重新設計該區域以應對其可能面臨的負載，這一點至關重要。

當客戶端報告連線問題後，透過Catalyst Center進行隔離和說明，檢視Catalyst 9800客戶端連線問題故障排除流程。

最後，作為一種一般良好做法，藉助監控Catalyst 9800 KPI（關鍵效能指標），關注WLC的總體關鍵指標。

配置以實現可擴充性

9800上的SVI和介面

避免在WLC上為客戶端VLAN建立SVI。習慣於較舊的AireOS WLC的管理員往往會反射為每台客戶端VLAN建立第3層介面，但很少需要這樣做。介面會增加控制平面攻擊媒介，並且可能需要更多ACL以及更複雜的條目。預設情況下，可以訪問WLC的任意介面，要保護具有更多介面的WLC還需要做更多的工作。它還會使路由複雜化，因此最好避免這種情況。

從IOS XE 17.9開始，mDNS監聽或DHCP中繼場景不再需要SVI介面。因此，在客戶端VLAN中配置SVI介面的原因很少。

彙總探測響應

對於大型公共網路，建議修改存取點傳送的預設聚合探測間隔。預設情況下，AP每500毫秒更新一次有關客戶端傳送的探測的WLC。此資訊用於負載均衡、頻帶選擇、位置和802.11k功能。如果有多個客戶端和存取點，建議修改更新間隔，以防止WLC中出現控制平面效能問題。建議的設定是每64秒有50個聚合探測響應。此外，請確保您的AP未報告來自本地管理的MAC地址的探查，因為考慮到單個客戶端可能在掃描時使用許多本地管理的MAC來避免故意跟蹤，所以沒有跟蹤的必要。

```
wireless probe limit 50 64000

no wireless probe localy-administered-mac
```

IPv6

許多網路管理員仍然拒絕IPv6。對於IPv6，只有兩種可接受的選項：要麼您支援該協定，而且必須在任何位置部署足夠的配置；要麼您不支援該協定，而且必須阻止它。不關注IPV6並在某些位置啟用而不進行正確配置是不能接受的。這將導致整個IP世界被您的網路安全所忽視。

如果啟用IPv6，則必須在2001：DB8：：/32範圍內配置虛擬IPv6地址（這經常被人遺忘）。

必須注意的是，儘管IPv6的基本操作在很大程度上依賴於組播，但如果您在WLC上停用組播轉發，IPv6仍可以運行。組播轉發是指客戶端組播資料轉發，而不是鄰居發現、路由器請求和運行IPv6的其他必需協定。

如果您的網際網路連線或網際網路服務供應商提供IPv6位址，您可以決定為您的使用者端允許

IPv6。這與在您的基礎設施中啟用IPv6是不同的。您的AP只能在IPv4中運行，但仍能在CAPWAP資料包中傳輸IPv6客戶端資料流量。要在您的基礎設施上啟用IPv6，您還需要考慮保護對AP、WLC和管理子網的客戶端訪問。

驗證客戶端網關的RA頻率。WLC提供RA限制策略，用於限制轉發到客戶端的RA數量，因為這些流量有時會變得不穩定。

mDNS

一般而言，在大型場所部署中最好完全停用mDNS。

mDNS橋接是指允許mDNS資料包作為第2層組播傳送（從而傳送到整個客戶端子網）的概念。mDNS在家庭及小型辦公室中非常流行，在這種情況下發現子網中的服務非常實用。但是，在大型網路中，這意味著將資料包傳送到子網中的所有客戶端，這在大型公共網路中從流量的角度來看是有問題的。另一方面，橋接不會對AP或WLC CPU造成任何開銷，因為它被視為常規資料流量。mDNS代理或mDNS網關是指將WLC用作網路中所有服務的目錄的概念。這允許在第2層邊界上有效提供mDNS服務，同時減少整體流量。例如，使用mDNS閘道時，印表機會透過具有相同子網路第2層多點傳送的mDNS傳送定期服務宣告，但WLC不會將其轉送到所有其他無線使用者端。相反，它會記錄提供的服務，並在其服務目錄中註冊。每當任何客戶端請求給定型別的可用服務時，WLC都會代表印表機回覆通知。這樣可避免其他所有無線客戶端聽到不必要的請求和服務產品，並且只有在他們詢問存在哪些服務時才會收到回覆。雖然可大幅提升流量效率，但由於mDNS流量窺探，WLC（或AP，如果您在FlexConnect案例中依賴AP mDNS）確實會產生額外負荷。如果使用mDNS閘道，請務必留意CPU使用狀況。

橋接會導致大型子網中的組播風暴，而偵聽它（使用mDNS網關功能）會導致大量CPU使用率。在全局和每個WLAN上停用該功能。

有些管理員啟用mDNS是因為一些服務在特定位置需要它，但瞭解這會增加多少不需要的流量非常重要。Apple裝置經常自我宣傳，並不斷尋找服務，從而導致mDNS查詢的背景噪音，即使沒有人對任何服務進行特殊使用。如果您出於特定業務要求需要允許mDNS，請全局啟用它，然後僅在需要它的WLAN上啟用它，並嘗試限制允許mDNS的作用域。

強化網路

安全性

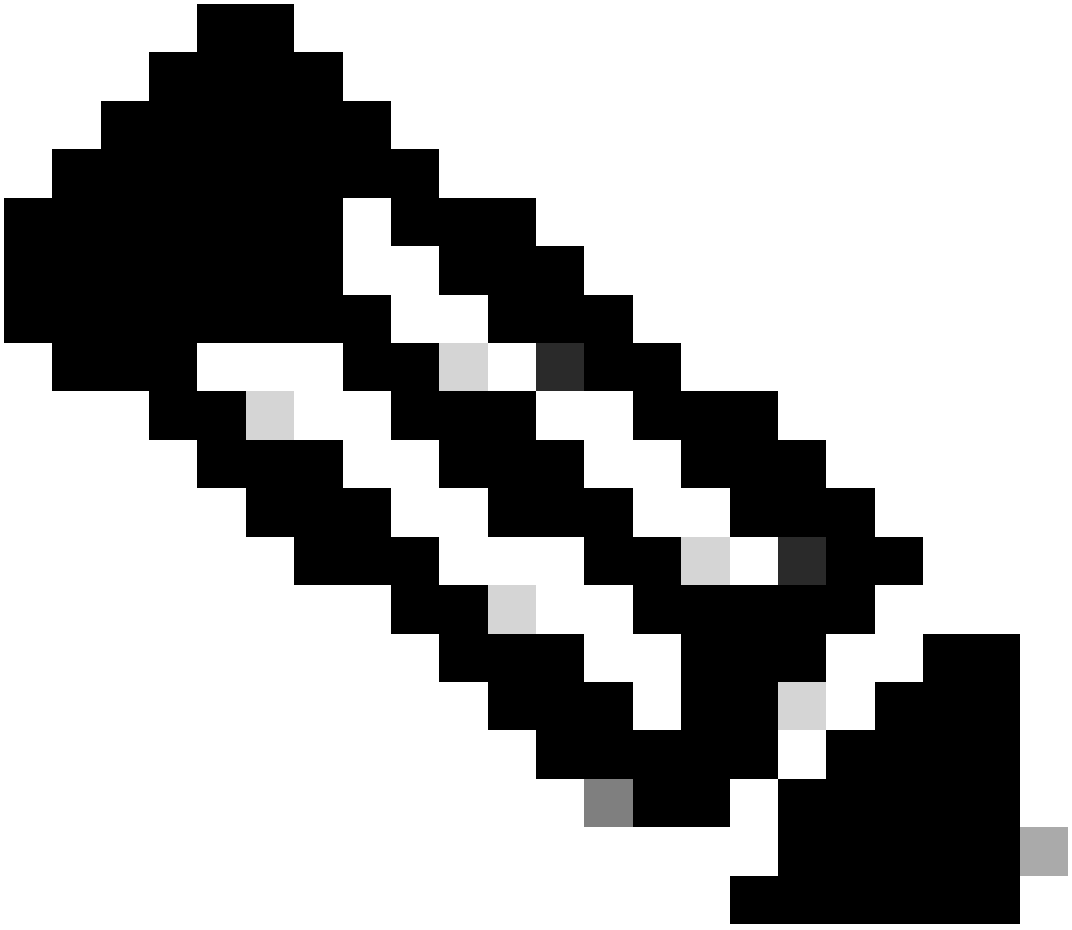
在大型公共網路中，許多事情可能是在管理員不知道的情況下發生的。人們會在隨機地點要求電纜掉落，或在某個地點插入家用交換機，為自己的小把戲設定更多交換機埠……他們通常不事先請求允許就嘗試這些裝置。這意味著，即使沒有不良行為者的參與，安全性也可能會被心甘情願的客戶和/或員工破壞。這樣一來，惡意攻擊者就很容易四處尋找，找到一條電纜，然後檢視他們從那裡獲得哪些網路接入。在所有交換機埠上配置802.1X身份驗證是在大型網路中保持適當安全性的近乎必要條件。Catalyst Center可以幫助您自動完成此部署，並且可以為不支援802.1X身份驗證的特定裝置設定例外，但儘量少依賴基於MAC的身份驗證，因為這樣並不是真正的安全性。

Rogue存取點

你對付流氓的戰略取決於幾個因素。許多管理員本能地遵循非常嚴格的規則，但主要問題是：

- 當收到數百個（如果不是數千個）惡意警報時，您是否擁有人力資源來檢視所有這些警報，並對所有這些警報採取行動？
- 您的目標是物理移除惡意單元，以保持清晰的射頻頻譜？如果是，您需要許多人員來執行此操作。或者，你的目標只是盯著安全因素，確保這些流氓不構成任何危險？這樣的人類工作成本就更容易控制了。
- 啟用惡意檢測可能會對您的通話時間產生影響，而惡意遏制通常會產生更大的影響。您是否分析了這種影響並將其考慮在內？

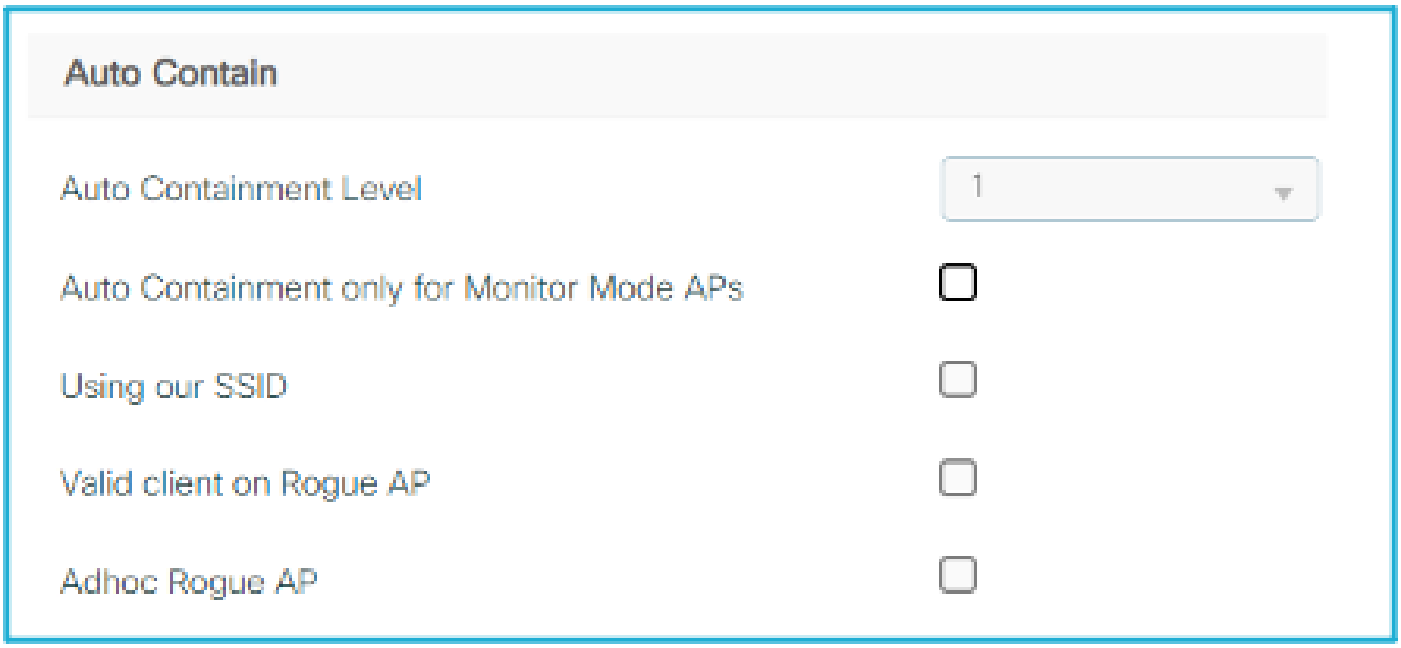
關於欺詐檢測的影響，9120和9130具有專屬CleanAir晶片，負責通道外掃描（以及欺詐檢測），從而使得對客戶端服務的無線電的影響幾乎為零。帶有CleanAir Pro晶片的9160系列AP具有類似的無影響掃描功能，但其他沒有CleanAir晶片的AP需要將客戶端服務的無線電「離通道」以掃描惡意程式或執行遏制。因此，您使用的AP型號在決定是否使用專用的監控模式AP進行惡意程式檢測和遏制時發揮了作用。



注意：共用Wi-Fi熱點的行動電話以「基礎架構」模式運行，就像傳統AP一樣，「ad-hoc」模式是指流動裝置之間的直接連線，因此不太常見。

非法遏制通常被監管規則禁止，因此啟用前務必先向您的在地主管部門核實。包含惡意程式並不意味著遠端關閉該惡意程式，而是使用去身份驗證幀向嘗試連線到惡意存取點的客戶端傳送垃圾郵件，使其無法連線。這只能用於舊版安全SSID（在WPA3中或在WPA2中啟用PMF時不起作用），因為您的存取點無法正確簽署解除驗證架構。由於AP使用去身份驗證幀填充空時，遏制會對目標通道上的RF效能產生負面影響。因此，只能將其視為一種安全措施，以防止您自己的合法客戶端錯誤地關聯到惡意存取點。由於上述所有原因，建議不要進行任何遏制，因為它不能完全解決惡意問題，並且會導致更多的RF問題。如果需要使用遏制，則僅對欺騙某個受管SSID的惡意程式啟用該遏制才有意義，因為這是一種明顯的蜜罐攻擊。

您可以使用「使用我們的SSID」選項來配置自動包含：



自動包含設定

您也可以根據自己的標準配置惡意規則，將其歸類為惡意惡意惡意的惡意存取點。不要忘記將您的鄰近和已批准的SSID名稱輸入為友好惡意程式，以便將其從警報清單中刪除。

啟用AP驗證或PMF以保護AP免於模擬。

有線非法存取點是連線到有線網路的非法存取點，這顯然會增加安全威脅。有線惡意程式的檢測更為複雜，因為惡意程式的乙太網MAC地址通常與其無線電MAC地址不同。Cisco Catalyst Center的演算法仍會嘗試檢測惡意程式是否處於有線狀態，並搜尋無線偵聽的惡意客戶端MAC並在有線基礎設施上可見。防止有線非法接入的最佳解決方案是使用802.1X身份驗證保護所有交換機埠。

如果您要在惡意存取點上進行物理操作，則利用Cisco Spaces是獲得惡意存取點準確位置的關鍵。您很可能仍然需要在現場搜尋一次，因為有時人們會隱藏惡意AP，但是將搜尋範圍縮小到幾公尺就非常可行了。如果沒有空間，惡意程式會顯示在檢測到它的最響亮搜尋區域的AP旁邊的地圖上。許多無線工具和裝置可以即時顯示惡意存取點的訊號，幫助您實際定位惡意存取點。

與惡意程式不完全相關，但由於CleanAir剛剛被覆蓋，因此必須注意，啟用CleanAir不會對BLE信標檢測以外的效能產生明顯的負面影響，因為這會影響2.4GHz的效能。您可以將無線設定為完全忽略藍芽干擾器，因為它們在當今的世界中無處不在，而且您無法阻止您的使用者端啟用其藍芽。

WiPS

WiPS涵蓋更高級的攻擊媒介，而不只是檢測是否存在未經授權的欺詐裝置。除了這些攻擊之外，它有時還會提供事件的PCAP以供取證分析使用。

雖然這對企業來說是一個非常有用的安全功能，但面向公眾的網路必須面對一個永恆的問題：如何應對它？

由於難以管理許多不受您控制的客戶端，因此可以將警報分為兩類。如果您看到過多的警報，可以決定從Cisco Catalyst Center忽略這些警報：

- 10001： DoS：身份驗證泛洪警報
- 10002： DoS：關聯請求警報
- 10003： DoS：廣播探測泛洪警報
- 10004： DoS：取消關聯泛洪警報
- 10005： DoS：廣播解除關聯警報
- 10006： DoS：解除驗證泛洪警報
- 10007： DOS：廣播解除驗證警報
- 10008： DOS： EAPOL-Logoff攻擊警報
- 10009： CTS泛洪警報
- 10010： RTS關聯請求警報
- 10011：按對取消身份驗證泛洪
- 10021：Airdrop會話（此會話通常在所有網路中大量發生，並且僅描述Apple裝置之間的常規點對點活動）
- 10022：關聯請求格式錯誤
- 10023：透過簽名泛洪身份驗證失敗
- 10024：簽名的MAC OUI無效
- 10025：身份驗證格式不正確

這些警報可能由行為不當的客戶端引起。不可能自動阻止拒絕服務攻擊，因為從本質上講，您無法阻止有故障的客戶端讓通話時間保持忙碌。即使基礎架構忽略了客戶端，它仍然能夠使用介質和廣播時間進行傳輸，從而影響其周圍客戶端的效能。

其他警報非常具體，因此極有可能描述實際的惡意攻擊，並且由於客戶端驅動程式錯誤而很難發生。最好持續監控這些警報：

- 10012：模糊化信標
- 10013：模糊化探測請求
- 10014：模糊化探測響應
- 10015：按簽名的PS輪詢泛洪
- 10016：按簽名的EAPOL開始V1泛洪
- 10017：按目標重新關聯請求泛洪
- 10018：依簽名的信標泛洪
- 10019：按目標分類的探測響應泛洪
- 10020：透過簽名阻止Ack泛洪
- 10026/10027：RTS和CTS虛擬載波偵聽攻擊

無線基礎設施有時可以採取緩解措施，例如阻止列出違規裝置，但消除此類攻擊的唯一實際措施是實際前往並刪除違規裝置。

建議啟用所有形式的客戶端排除，以節省與故障客戶端互動所浪費的通話時間。

限制客戶端訪問

建議您在所有的WLAN上啟用點對點封鎖（除非您對使用者端對使用者端通訊有硬性需求，但需要仔細考慮並可能加以限制）。此功能可防止同一WLAN上的客戶端相互聯絡。這不是一個完美的解決方案，因為不同WLAN上的客戶端仍然能夠相互聯絡，並且移動組中屬於不同WLC的客戶端也可以繞過此限制。但它可以充當簡單而高效的第一層安全和最佳化。這種對等阻塞功能的另一個優點是它還能防止客戶端到客戶端ARP，從而防止應用程式發現本地網路上的其他裝置。如果不進行對等阻塞，在客戶端上安裝簡單的應用程式可能會顯示子網中連線的所有其他客戶端，並可能顯示其IP地址和主機名。

除此之外，建議在WLAN上同時應用IPv4和IPv6（如果您在網路中使用IPv6） ACL，以防止客戶端之間的通訊。無論您是否具有客戶端SVI，在WLAN級別應用阻止客戶端與客戶端通訊的ACL都可以正常工作。

另一個必要步驟是防止無線使用者端存取任何形式的無線控制器管理。

範例：

```
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
```

此ACL可以應用於管理介面SVI：

```
interface Vlan130
 ip access-group ACL_DENY_CLIENT_VLANS in
```

這會在具有建立在第2層VLAN資料庫中的使用者端VLAN 131到137的WLC上完成，但沒有對應的SVI，而且VLAN 130隻有一個SVI，這就是管理WLC的方式。此ACL可防止所有無線客戶端完全向WLC管理和控制平面傳送任何流量。不要忘記，SSH或Web UI管理並不是您唯一需要允許的事情，因為還需要允許到所有AP的CAPWAP連線。這就是此ACL具有預設允許但阻止無線客戶端範圍的原因，而不是依賴預設deny all操作，該操作需要指定所有允許的AP子網範圍和管理範圍。

同樣，您可以建立指定所有可能管理子網的另一個ACL：

```
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
```

然後，可以應用以下ACL進行CLI訪問：

```
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
```

相同的ACL也可以應用於Web管理員訪問。

防禦流量風暴

組播和廣播在一些應用程式中的使用率高於其他應用程式。當考慮僅使用有線網路時，防禦廣播風暴通常是唯一的預防措施。但是，組播在空中傳送時與廣播一樣痛苦，瞭解其原因非常重要。首先，假設一個資料包（無論是透過廣播還是組播）傳送到您的所有無線客戶端，該資料包可以快速加入多個目的地。然後，每個AP需要以儘可能最可靠的方式透過空中傳輸此幀（儘管不能保證其可靠），而這是透過使用強制性資料速率（有時最低，有時是可配置的）來實現的。用一般術語來說，這意味著幀是使用OFDM (802.11a/g)資料速率傳送的，這顯然不是很好。

在大型公共網路中，不建議依靠組播來保持通話時間。但是，在大型企業網路中，可能需要為特定應用啟用組播，不過您必須儘可能控制它以限制其影響。最好記錄應用詳情、組播IP並確保阻止其他形式的組播。如前所述，啟用組播轉發不是啟用IPv6的必要條件。最好完全停用廣播轉發。廣播有時被應用程式用於發現同一子網上的其他裝置，這在大型網路中顯然是一個安全問題。

如果啟用全局組播轉發，請確保使用組播-組播AP CAPWAP設定。啟用此功能後，WLC從有線基礎架構接收多點傳送封包時，會以單一多點傳送封包將其傳送至所有相關的AP，從而大幅減少封包複製。確保為每個WLC設定不同的CAPWAP組播IP，否則AP會從其他WLC接收不需要的組播流量。

如果AP位於WLC的無線管理介面（可能位於大型網路中）的其他子網中，則必須在有線基礎架構上啟用組播路由。您可以使用命令驗證所有AP是否正確接收組播流量：

```
show ap multicast mom
```

如果需要依賴組播，也建議在所有情況下啟用IGMP（用於IPv4組播）和MLD（用於IPv6）組播。它們僅允許感興趣的無線客戶端（因此僅允許具有感興趣客戶端的AP）接收組播流量。WLC將註冊代理到組播流量，並負責保持註冊處於活動狀態，從而解除安裝客戶端。

結論

大型公共網路非常複雜，每個網路都有其獨特的要求和結果。

遵守本文檔中的準則是一個很好的起點，有助於在避免最常見問題的同時成功完成部署。但是，這些指南只是指南，可能需要在特定地點的背景下進行解釋或調整。

思科CX擁有專門從事大型無線部署的無線專業團隊，在包括體育賽事和會議在內的眾多大型活動中擁有豐富的經驗。請與您的客戶團隊聯絡以獲取進一步幫助。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。