设计指南CX -适用于大型公共网络的无线产品

目录

简介

本文档介绍大型公共Wi-Fi网络的设计和配置指南。

《 CX设计指南》

CX设计指南由思科技术支持中心(TAC)和思科专业服务(PS)的专家撰写，并由思科内部的专家进行同行评审；这些指南基于思科领先的操作规范，以及多年来从无数客户实施中获得的知识和经验。根据本文档中的建议设计和配置网络有助于避免常见缺陷并改善网络运行。

范围和定义

本文档提供大型公共无线网络的设计和配置指南。

定义：大型公共网络-通常以高密度进行无线部署，为数以千计的未知和/或非受管客户端设备提供网络连接。

本文档通常假定目标网络为大型和/或临时事件提供服务。它还适用于接待大量访客的场所的静态永久网络。例如，商场或机场与体育场或音乐会场的Wi-Fi网络有相似之处，因为对最终用户没有控制，而且它们通常只在网络中存在几个小时，或者最多只存在于一天中。

大型活动或场馆的无线覆盖有其自身的一组要求，这些要求往往不同于企业、制造业，甚至不同于大型教育网络。大型公共网络可能只有数千人，集中在一栋或几栋建筑中。此类设备可以非常频繁地发生客户端漫游（经常或处于高峰期），此外，网络必须尽可能与任何无线客户端设备兼容，且无需控制客户端设备配置或安全。

本指南介绍高密度的一般RF概念和实施细节。本指南中的许多无线电概念适用于所有高密度网络，包括Cisco Meraki。但是，实施细节和配置侧重于使用Catalyst 9800无线控制器的Catalyst无线，因为这是目前为大型公共网络部署的最常见解决方案。

本文档互换使用术语无线控制器和无线LAN控制器(WLC)。

大型公共网络

大型公共网络和活动网络在很多方面都独树一帜，本文档就以下几个关键方面进行了探讨并提供指导。

- 大型公共网络非常密集；无线射频(RF)空间减少后，会有成千上万台设备在人们四处走动时进行大规模漫游，一些活动和场所可能会更加静态，在非常特定的时间出现带宽峰值。基础设施需要尽可能平稳地处理所有这些状态更改，以便客户端进入该区域并在该区域内移动。
- 首要任务是简化入职流程。相关联的客户是满意的客户。这意味着您希望使客户端尽可能快地关联到网络。未连接到Wi-Fi的客户端会扫描可用接入点，这会生成不需要的射频能量，进而导致空中出现额外拥塞和容量损失。
- RF部署需要尽可能小心地设计。如果需要非常高的密度，或者场地有大的开放空间和/或高高的天花板，则必须使用使用定向天线的适当RF设计。
- 另一个关键设计驱动因素是兼容性。某些功能是802.11规范中的标准功能，而其他功能是专有功能，不会给客户端带来任何问题。但是，现实情况有所不同，当看到不理解的复杂信标或功能/设置时，许多编程不当的客户端驱动程序会出现不正常行为。
- 由于规模和时间限制，故障排除颇具挑战性。如果某个产品无法与特定客户端配合使用，您将无法与该最终用户配合来了解问题。用户可能很难找到，但也可能因为他们在场所中访问的临时性而不合作。
- 安全是一个重要因素。由于访客数量庞大且受攻击面更大，因此控制较少。

外部引用

文档名称	来源	位置
Cisco Catalyst 9800系列配置最佳实践	思科	链接
排除无线局域网控制器CPU故障	思科	链接
验证Wi-Fi吞吐量：测试和监控指南	思科	链接
思科Catalyst CW9166D1接入点部署指南	思科	链接
Catalyst 9104体育场天线(C-ANT9104)部署指南	思科	链接
监控Catalyst 9800 KPI（关键绩效指标）	思科	链接

文档名称	来源	位置
Catalyst 9800客户端连接问题故障排除流程	思科	链接
Cisco Catalyst 9800系列无线控制器软件配置指南(17.12)	思科	链接
Wi-Fi 6E：Wi-Fi下一重要章节（白皮书）	思科	链接

免责声明

本文档根据特定的场景、假设以及从大量部署中获得的知识提供建议。但是，读者负责确定网络设计、业务、合规性、安全性、隐私和其他要求，包括是否遵循本指南中提供的指导或建议。

设计网络

RF注意事项

场所类型

本指南侧重于大型访客网络，通常对公众开放，对最终用户和客户端设备类型的控制有限。这些类型的网络可以部署在不同的位置，可以是临时的或永久的。主要使用案例通常是为访客提供互联网接入，尽管这很少是唯一的使用案例。

典型位置：

- 体育场馆
- 会议场所
- 大型礼堂

从RF的角度来看，每种位置类型都有自己的一组细微差别。这些示例中大多数通常是永久安装（除会议场所外），因为它们可以是永久安装，也可以临时为特定贸易展览而设置。

其它位置：

- 邮轮
- 机场
- 购物中心/购物中心

机场和邮轮也是适合大型公共网络类别的部署示例；但是，这些示例具有特定于每个情况的额外考虑因素，并且通常使用内部全向AP。

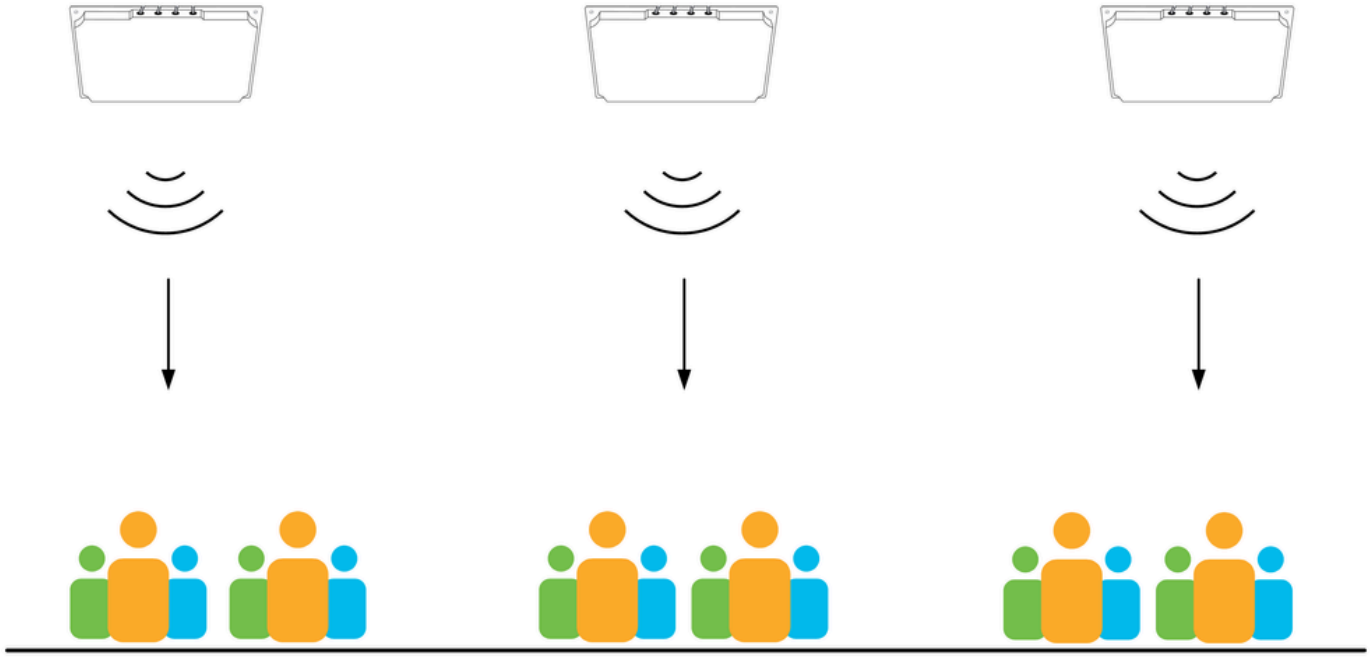
覆盖战略

覆盖策略主要取决于场所类型、使用的天线以及可用的天线安装位置。

开销

只要可能，开销覆盖总是首选。

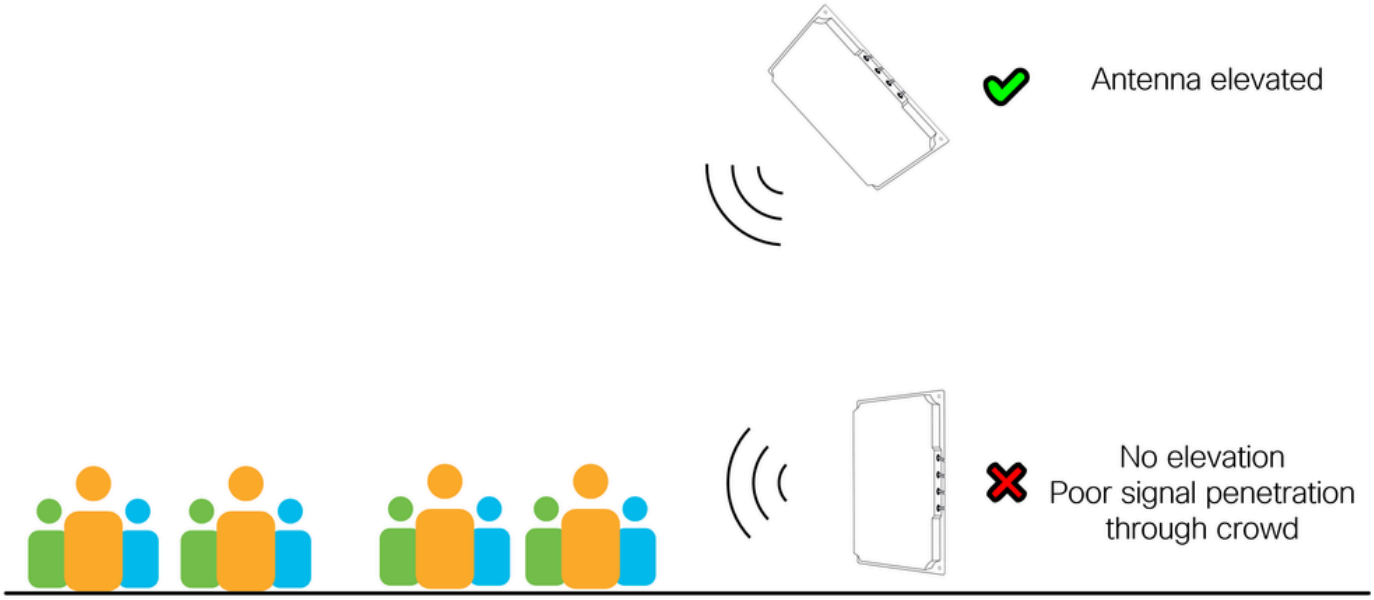
开销解决方案有一个明显的优势：即使在拥挤的情况下，所有客户端设备通常都能够直接看到天线的开销。使用定向天线的开销解决方案提供更可控且定义更明确的覆盖区域，从无线电调谐的角度来说，可以减少其复杂性，同时提供卓越的负载均衡和客户端漫游特性。有关其他信息，请参阅功率平衡部分。



客户端上方的AP

侧面

侧装式定向天线是常见选择，在各种情况下都能良好工作，特别是当由于高度或安装限制而无法进行架空安装时。使用侧装时，了解天线所覆盖区域的类型非常重要，例如，它是开放的室外区域还是密集的室内区域？如果覆盖区域是人口众多的高密度区域，则天线必须尽可能提高，因为信号在人群中的传播始终很差。请记住，大多数移动设备用于腰部以下位置，而不是使用者头部上方！如果覆盖区域密度较低，则天线高度不太重要。



天线仰角始终更好

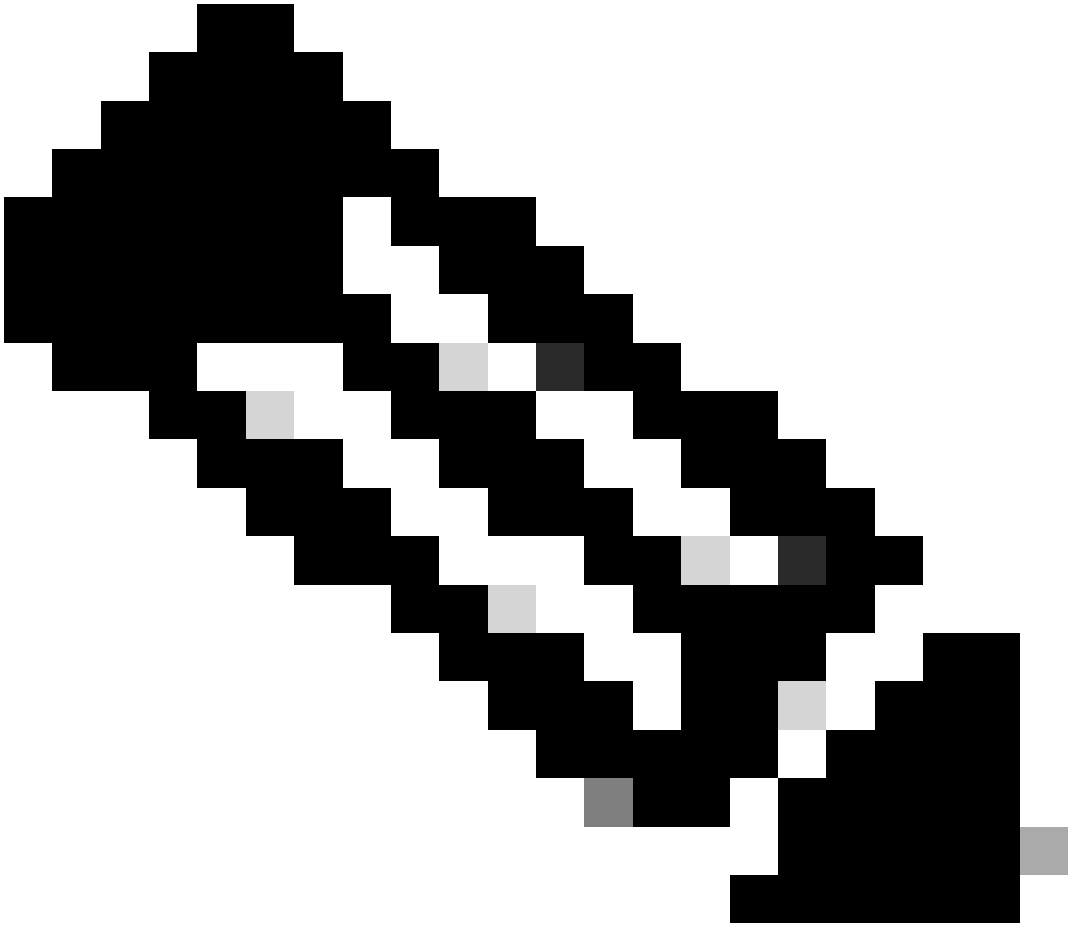
全向

通常必须在非常高密度的情况下避免使用全向天线（内部或外部），这是因为同信道干扰的潜在影响区域较大。不得在6米以上的高度使用全向天线（不适用于高增益室外设备）。

座位下

在某些体育场和体育场中，可能会出现没有合适天线安装位置的情况。最后剩下的备选方案是通过将AP放置在用户坐下的座位下来提供覆盖范围。此类解决方案更难正确部署，成本通常更高，需要的AP和安装步骤也更多。

席位不足部署的主要挑战在于全场与空场覆盖范围之间的巨大差异。人体在衰减无线电信号方面非常有效，这意味着当无线接入点周围有一群人时，与那些人不在场时相比，产生的覆盖范围要小得多。这种人群衰减系数允许部署更多AP，从而提高整体容量。但是，当场所空置时，人体不会产生衰减和明显干扰，当场所部分满时会导致并发症。



注意：席位不足部署是一个有效但不常见的解决方案，必须逐个进行评估。本文档不进一步讨论席位下部署。

美学

在一些部署中，美学问题开始发挥作用。这些区域可以是具有特定架构设计、历史价值的区域，也可以是广告和/或品牌规定设备可以（或不能）安装的区域。可能需要使用特定的解决方案来解决任何放置限制。其中一些解决方法包括隐藏AP/天线、涂刷AP/天线、将设备安装在外壳中或只使用其他位置。涂抹天线会使保修失效，如果您选择涂抹天线，则始终使用非金属涂料。思科一般不销售天线外壳，但许多产品可通过不同的提供商轻松获得。

所有这些变通方案都会对网络的性能产生影响。无线架构师总是从提出最佳安装位置开始，以获得最佳无线电覆盖范围，而这些初始位置通常可以提供最佳性能。对这些位置的任何更改通常会导致天线偏离其最佳位置。

安装天线的地点通常是高架的，可以是天花板、猫道、屋顶结构、横梁、走道以及在预定覆盖区域提供一定高度的任何位置。这些位置通常与其他设备共享，例如：音频设备、空调、照明和各种探

测器/传感器。例如，音频和照明设备必须安装在非常特定的位置-但是为什么会这样呢？简单来说，这是因为音频和照明设备在隐藏在箱子里或墙后面时无法正常工作，并且每个人都会承认这一点。

同样适用于无线天线，当无线客户端设备有视距时，它们的工作效果最好。优先考虑美学可能会对无线性能产生负面影响（通常确实如此），从而降低基础设施投资的价值。

非法网络

非法Wi-Fi网络是共享一个公共RF空间但不由同一运营商管理的无线网络。这些设备可以是临时的或永久的，包括基础设施设备(AP)和个人设备（例如共享Wi-Fi热点的手机）。非法Wi-Fi网络是干扰源，在某些情况下还会带来安全风险。不可低估恶意程序对无线性能的影响。Wi-Fi传输仅限于在所有Wi-Fi设备之间共享的相对较小范围的无线频谱，邻近的任何行为不当的设备都有可能对许多用户的网络性能造成干扰。

在大型公共网络中，通常使用专用天线精心设计和调整。良好的RF设计只覆盖所需的区域，通常使用定向天线，并调整发送和接收特征以获得最大效率。

频谱的另一端是消费级设备，或由Internet服务提供商提供的设备。这些设备或者具有有限的RF微调选项，或者配置为提供最大范围和感知性能，通常采用高功率、低数据速率和宽信道。将此类设备引入大型事件网络有可能造成严重破坏。

我们能做些什么呢？

在个人热点方面，我们几乎无能为力，因为几乎不可能监控数万人进入一个场所。对于基础设施或半永久设备，有一些选择。可能的补救措施从简单的教育开始，包括简单的认知标牌，到签署的无线电策略文档，最后是主动实施和频谱分析。在所有情况下，都必须就指定场所内的无线电频谱保护问题作出业务决定，同时采取具体步骤执行业务决定。

当第3方控制的设备通告与受管网络相同的SSID时，非法网络的安全方面就会发挥作用。这相当于蜜罐攻击，可用作窃取用户凭证的方法。始终建议创建恶意规则，以就检测由非托管设备通告的基础设施SSID发出警报。“安全”一节更详细地讨论了恶意程序。

单5GHz与双5GHz

双5GHz是指在支持的AP上使用两个5GHz无线电。使用外部天线的双5GHz与使用内部天线的双5GHz（全向AP上的微/宏信元）之间存在一个关键区别。对于外接天线，双5GHz通常是一种非常有用的机制，可在减少总AP计数的同时提供额外的覆盖范围和容量。

微型/宏型/中型

内部AP将两个天线紧密相连（在AP内部），在使用双5GHz时，存在与最大发射功率相关的限制。第二个无线电被限制为低Tx功率（由无线控制器执行）导致无线电之间的Tx功率大幅失衡。这会导致主（高功率的）无线电吸引许多客户端，而辅助（低功率的）无线电利用不足。在这种情况下，第二个无线电会为环境增加能量，而不会为客户端带来好处。如果出现这种情况，最好禁用第二个无线电，在需要额外容量时再添加一个（单个5GHz）AP。

不同AP型号具有不同的配置选项。第二个5GHz无线电可以在较新的宏/中型 AP（如9130和

9136）中以较高的功率水平运行，并且某些内部Wi-Fi 6E AP（如9160系列）甚至可以在某些情况下以宏/宏模式运行。始终验证您的准确AP型号的功能。第二个5GHz插槽的信道使用也受到限制，当一个插槽在一个UNII频段中运行时，另一个插槽被限制到不同的UNII频段，这会影响信道规划和随后的可用传输功率。请始终考虑双5GHz无线电之间的发射功率差异，所有情况下都是如此，包括内部AP。

FRA

灵活无线电分配(FRA)作为一种技术被引入，通过将额外的2.4GHz无线电切换到5GHz模式，或将潜在未使用的5GHz无线电切换到监控模式（适用于支持它的AP），来改进5GHz覆盖范围。由于本文档涵盖大型公共网络，因此假定使用定向天线可以很好地定义覆盖范围和无线电设计，因此确定性配置优先于动态配置。不建议大型公共网络使用FRA。

或者，在设置网络以帮助确定要转换为5GHz的无线电时可以使用FRA，但如果您对转换结果满意，建议冻结FRA。

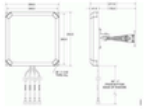
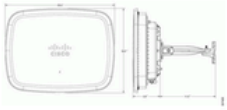
法规

每个管制范围定义了可供使用的通道及其最大功率水平，同时限制哪些通道可在室内与室外使用。根据管制范围，有时可能无法有效利用双5GHz解决方案。例如，ETSI域在UNII-2e信道上允许30dBm，但在UNII1/2信道上仅允许23dBm。在本例中，如果设计要求使用30dBm（通常由于到天线的距离较远），则使用单个5GHz无线电可能是唯一可行的解决方案。

天线

大型公共网络可以使用任何类型的天线，并且通常选择最适合工作的天线。在相同的覆盖区域内混合天线使无线电设计过程更具挑战性，如果可能必须避免。但是，大型公共网络通常具有较大的覆盖区域，即使在同一区域内也具有不同的安装选项，因此在某些情况下需要混合使用天线。全向天线易于理解，功能与任何其他天线相同。本指南将讨论外部定向天线。

下表列出了最常用的外部天线。

	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°

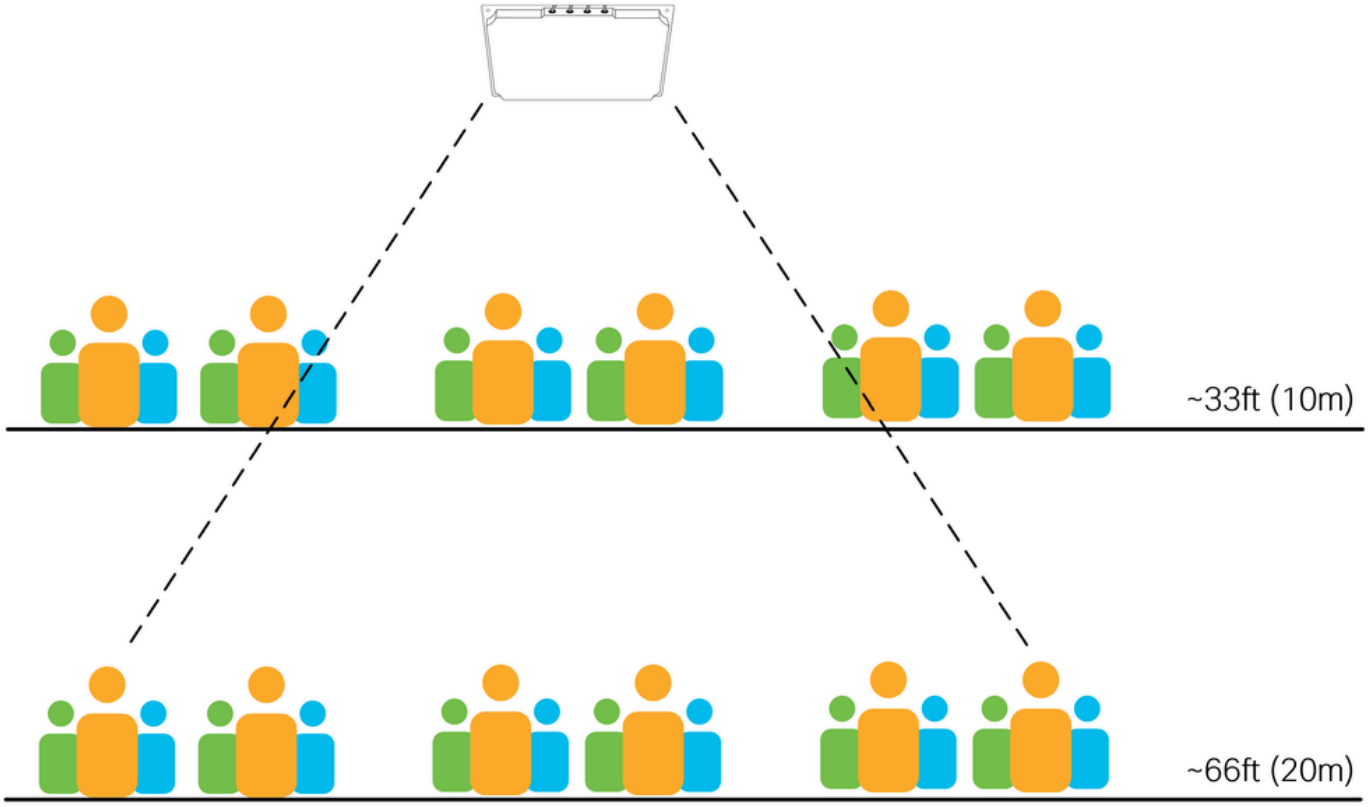
天线列表

选择天线时需要考虑的主要因素是天线波束宽度和天线安装距离/高度。下表显示了每个天线的5GHz波束宽度，括号中的数字表示圆整值（更易于记忆）。

表中建议的距离不是硬性规则，只是基于经验的指南。无线电波以光速移动，到达任意距离后不会简单地停止。天线的工作距离均超出建议的距离，但是，性能会随着距离的增加而下降。安装高度是规划过程中的关键因素。

下图显示了同一天线在高密度区域约33英尺（10米）和约66英尺（20米）处的两个可能安装高度。请注意，天线可以看到（和接受来自）的客户端数量会随着距离的增加而增加。随着距离变长，维持更小的蜂窝尺寸变得更具挑战性。

一般说来，用户密度越高，在给定的距离内使用正确的天线就显得越重要。



体育场天线

C9104体育场天线非常适合覆盖高距离高密度区域，请参阅Catalyst 9104体育场天线(C-ANT9104)部署指南了解相关信息。

随时间推移的变化

随着时间推移，物理环境变化在几乎所有无线安装中都很常见（例如内墙移动）。定期现场视察和目视检查始终是推荐的做法。对于事件网络，处理音频和照明系统，以及在很多情况下处理其他通信系统（例如5G）会更加复杂。所有这些系统通常安装在用户上方的高架位置，有时会导致对同一空间的争用。无线体育场天线的理想位置通常也是5G天线的理想位置！此外，随着这些系统的不断升级，它们可能会被重新部署到妨碍和/或主动干扰您的无线系统的位置。务必跟踪其他安装，并与安装团队进行沟通，以确保所有系统都安装在适当的位置，互不干扰（物理或电磁干扰）。

高密度和6GHz

在撰写本文档时，支持6GHz的外部天线选择有限。只有CW9166D1集成AP/天线可在6GHz的频率下工作，Cisco Catalyst CW9166D1接入点部署指南中提供了详细的天线规格。CW9166D1提供6GHz的覆盖范围，波束宽度为60°x60°，可有效用于满足此类天线条件的任何部署。例如，听众和仓库是CW9166D1部署的理想选择，因为集成设备提供定向天线功能供室内使用。

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

9166D1

在大型公共网络环境中，这些网络通常具有各种大型区域，并且需要在各种高度上组合使用天线。由于距离限制，仅使用60°x60°天线来端到端部署大型公共网络颇具挑战性。因此，仅使用CW9166D1为大型公共网络提供6GHz的端到端覆盖也极具挑战性。

一种可行的方法是使用5GHz作为主覆盖频段，同时仅在特定区域使用6GHz将支持的客户端设备卸载到更干净的6GHz频段。这种方法在更大的区域内使用5GHz专用天线，同时在可能且需要额外容量的情况下使用6GHz天线。

例如，假设在贸易会议中有一个大型活动厅，主厅使用体育场天线来提供主频为5GHz的覆盖，由于安装的高度要求使用体育场天线。在本例中，由于距离限制，CW9166D1无法用于主大厅，但可有效用于需要更高密度的相邻VIP大厅或印刷区。本文档后面将讨论5GHz和6GHz频段之间的客户端漫游。

法规

与5GHz一样，6GHz的可用功率和信道在管制范围之间也有很大差异。特别要注意的是，FCC和ETSI域之间的可用频谱有很大差异，并且分别针对室内和室外使用的可用发射功率、室内低功率(LPI)和标准功率(SP)制定了严格的准则。对于6 GHz，其他限制包括客户端功率限制、使用外部天线和天线向下倾斜，以及（目前仅在美国）对SP部署的自动频率协调(AFC)要求。

有关Wi-Fi 6E的详细信息，请参阅Wi-Fi白皮书中的Wi-Fi 6E：“The Next Great Chapter”（Wi-Fi 6E：Wi-Fi的下一重要章节）。

无线电资源管理

无线电资源管理(RRM)是一组用于控制无线电操作的算法。本指南参考了两种关键的RRM算法，即动态信道分配(DCA)和传输功率控制(TPC)。RRM是静态信道和电源配置的替代方案。

- DCA按可配置的计划运行（默认值为10分钟）。
- TPC自动运行（默认值为10分钟）。

思科事件驱动RRM (ED-RRM)是一种DCA选项，允许在标准DCA计划之外做出信道更改决策，通常是为了响应严重的射频条件。ED-RRM可以在检测到过多的干扰水平时立即更改信道。在嘈杂和/或不稳定的环境中，启用ED-RRM会带来信道更改过多的风险，这对客户端设备有潜在的负面影响。

我们鼓励使用RRM，并且通常优先于静态配置-但是，存在某些警告和例外情况。

- TPC必须根据需要使用TPC最小值/最大值设置限制为有限的值范围，并始终与RF设计保持一致。
    - 在高密度环境中启用TPC信道感知。

- DCA周期必须从默认设置10分钟更改。
    - 请勿在HD环境中使用ED-RRM。
    - 禁用避免Cisco AP加载。
    - 如果有多个恶意程序，诸如Avoid Foreign AP Interference这样的恶意AP避免选项可能会导致不稳定的环境。删除恶意程序总是比尝试对其进行响应更好。
- RRM决策可能受到无法正确侦听彼此的AP/天线的影响，例如定向天线相互背离的情况。
- 某些天线（例如C9104）不支持RRM，并且始终需要静态配置。
- RRM无法修复较差的RF设计。

在所有情况下，部署RRM时必须了解预期结果，并调整为在适合给定射频环境的范围内运行。本文档的后续部分将详细探讨这些要点。

RF配置

渠道

一般来说，渠道越多越好。在高密度部署中，部署的无线接入点和无线电数量可能会比可用信道多几个数量级，这意味着较大的信道重复使用率，以及更高的同信道干扰水平。必须使用所有可用信道，一般不建议限制可用信道列表。

在某些情况下，特定（和单独的）无线系统需要共存于同一物理空间，并且必须为其分配专用信道，同时从主系统的DCA列表中删除已分配的信道。必须非常仔细地评估这些类型的信道排除，并且仅在必要时使用。例如，在与主网络相邻的开放区域内工作的点对点链路，或者体育场内的记者区域。如果从DCA列表中排除了一个或两个以上的信道，则会导致重新评估建议的解决方案。在某些情况下，例如密度非常高的体育场，甚至连一条通道都排除在外有时可能不是可行的选择。

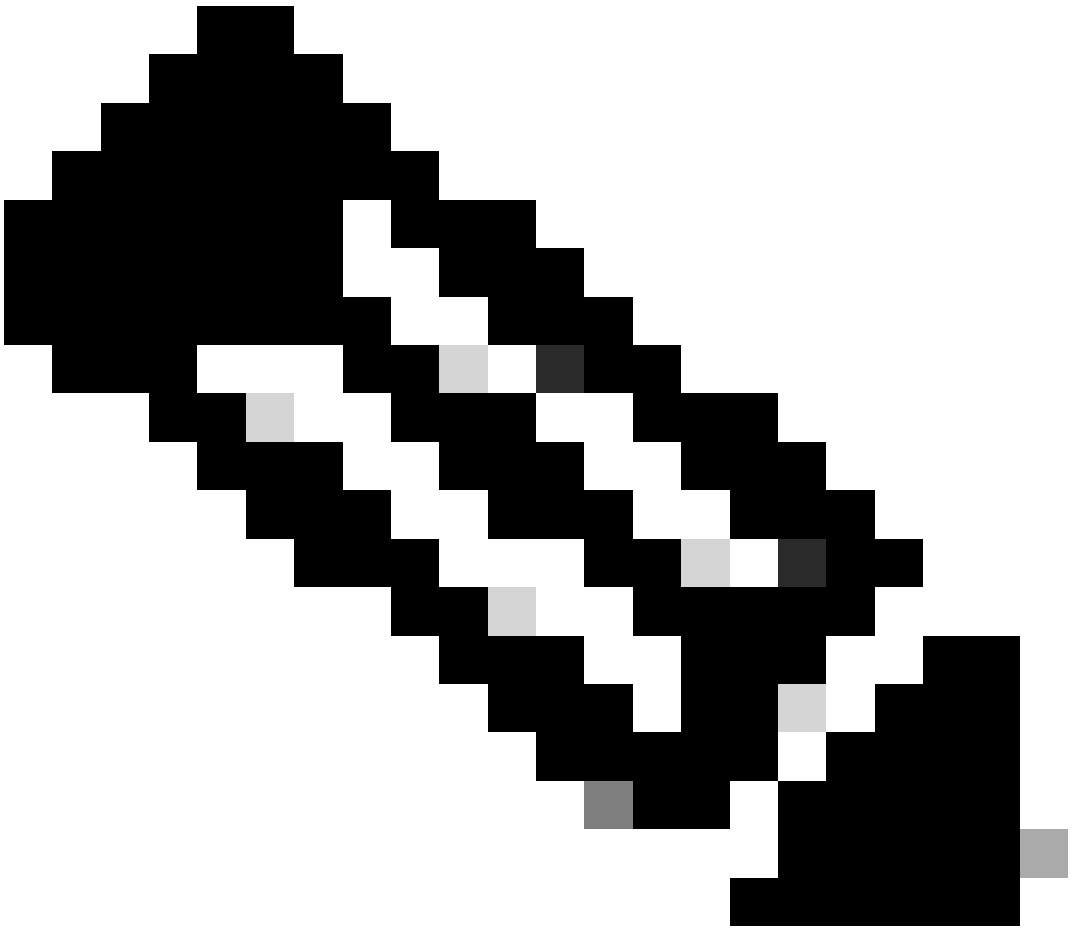
动态信道分配(DCA)可以与基于WLC的RRM或AI增强的RRM一起使用。

默认DCA间隔为10分钟，这可能会导致在不稳定的RF环境中频繁发生信道更改。在所有情况下，默认DCA计时器都必须从默认的10分钟增加，特定DCA间隔必须与所讨论网络的运行要求保持一致。示例配置可以是：DCA间隔4小时，锚点时间8。这样可将信道更改限制为每隔4小时一次，从上午8点开始。

由于干扰是必然的，因此每个DCA循环都适应这些干扰并不一定有价值，因为这些干扰中有很多是暂时的。一个好的方法是在最初几个小时内使用自动DCA，并在您有自己满意的稳定对象时冻结算法和信道计划。

重新启动WLC后，DCA在主动模式下运行100分钟，以查找合适的信道计划。在对RF设计做出重大更改（例如添加或删除大量AP或更改信道宽度）时，最好手动重新启动该过程。要手动启动此过程，请使用此命令。

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



注意：信道更改可能会对客户端设备造成干扰。

2.4 GHz

2.4GHz频段经常受到批评。它只有三个非重叠信道和除Wi-Fi以外的许多其他技术使用它，从而产

生不希望的干扰。一些组织坚持要提供这方面的服务，那么什么是合理的结论呢？事实上，2.4GHz频段不能为最终用户提供令人满意的体验。更糟的是，如果尝试提供2.4GHz服务，则会影响其他2.4GHz技术，例如蓝牙。在大型场所或活动中，许多人仍然期望在拨打电话时无线耳机能够正常工作，或者智能可穿戴式设备能够保持正常工作状态。如果您的密集型Wi-Fi以2.4GHz的频率运行，您将会影响那些甚至还未使用2.4GHz Wi-Fi的设备。

有一点是肯定的，如果您确实必须提供2.4GHz Wi-Fi服务，最好在单独的SSID上执行此操作（专用于IoT设备或将其称为“传统”）。这意味着双频段设备不会非自愿连接到2.4GHz，并且只有单频2.4GHz设备连接到该设备。

思科不建议或不支持在2.4GHz中使用40MHz信道。

5 GHz

高密度无线的典型部署。尽可能使用所有可用信道。

通道数量根据管制范围而异。考虑雷达在特定位置的影响，尽可能使用DFS信道（包括TDWR信道）。

对于所有高密度部署，高度建议使用20MHz信道宽度。

40MHz可用于2.4GHz的相同基础，即仅在绝对需要时（和位置）使用。

评估特定环境中40MHz信道的需求和实际优势。40MHz信道需要更高的信噪比(SNR)才能实现吞吐量的任何可能的改善，如果不可能有更高的SNR，那么40MHz信道就无用武之地。高密度网络为所有用户的平均吞吐量优先于任何单个用户的潜在更高吞吐量。在20MHz信道上放置更多AP比让使用40MHz作为辅助信道的AP仅用于数据帧更好，因此使用效率比让两个不同的无线信元分别以20MHz运行（就总容量而言，而不是就单个客户端吞吐量而言）要低得多。

6GHz

6GHz频段尚未在所有国家推出。此外，有些设备具有支持6GHz的Wi-Fi适配器，但需要BIOS更新才能在运行设备的特定国家/地区启用该适配器。客户现在发现6GHz无线电最常用的方式是通过5GHz无线电上的RNR通告。这意味着6GHz不能在同一AP上单独运行，没有5GHz无线电。6GHz用于卸载客户端和来自5GHz无线电的流量，并为有能力的客户端提供通常更好的体验。6GHz信道允许使用更大的信道带宽，但这在很大程度上取决于管制范围中的可用信道数量。欧洲有24个6GHz信道，因此，与5GHz信道中可能使用的20MHz信道相比，使用40MHz信道提供更好的最大吞吐量并非不合理。在美国，信道数量几乎翻倍，使用40MHz是无需费心费力的，即使使用80MHz对于密度较大的事件也并非不合理。在高密度活动或场所中不得使用更大的带宽。

数据传输速度

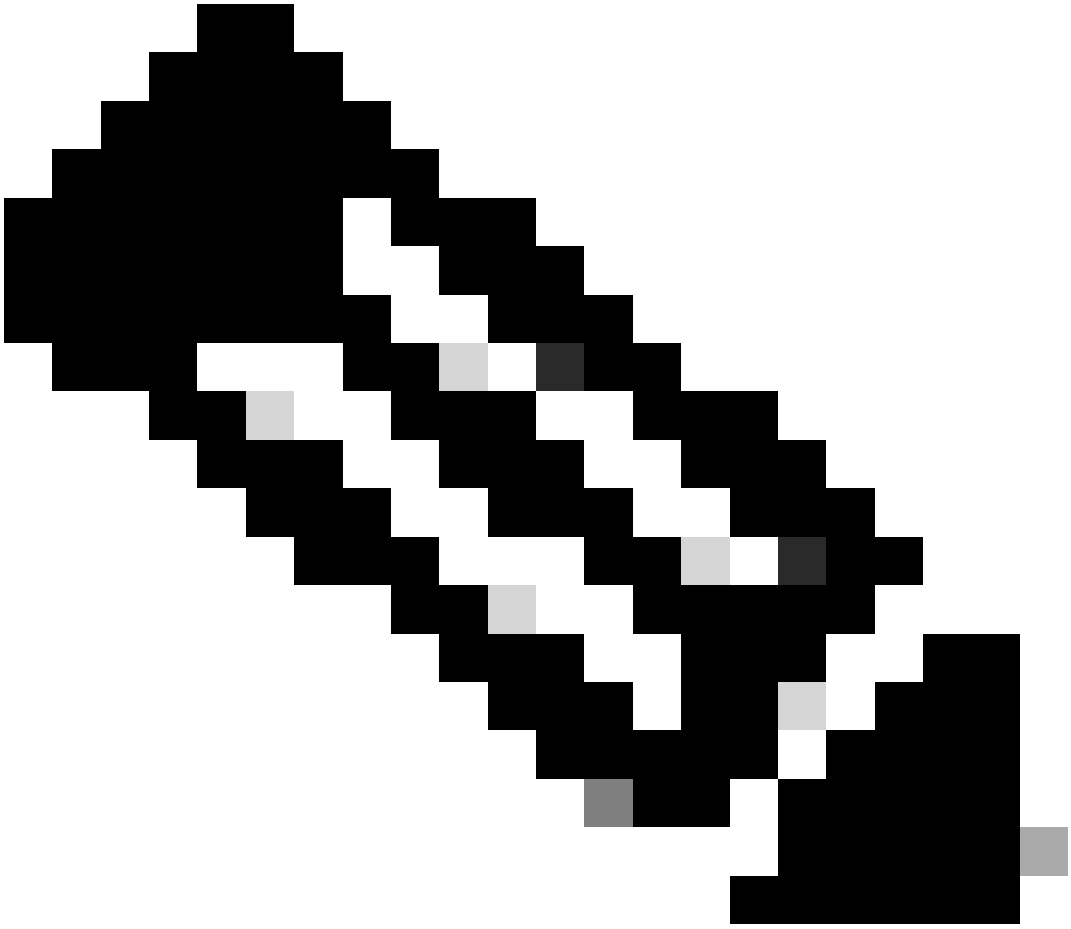
客户端与AP协商的数据速率主要是该连接的信噪比(SNR)的函数，相反的情况也成立，即更高的数据速率需要更高的SNR。事实上，决定最大可能链路速度的最主要是SNR，但为什么在配置数据速率时这一点如此重要呢？这是因为一些数据速率具有特殊的意义。

传统OFDM (802.11a)数据速率可以配置为以下三种设置之一：禁用、支持或强制。OFDM速率是（以Mbps为单位）：6、9、12、18、24、36、48、54，客户端和AP必须同时支持一个速率才能使用。

支持- AP将使用速率

强制- AP将使用速率，并将使用此速率发送管理流量

已禁用- AP将不使用该速率，强制客户端使用其他速率



注：强制性费率也称为基本费率

强制速率的意义在于，使用此速率以及广播和组播帧发送所有管理帧。如果配置了多个强制性速率，则管理帧使用最低配置的强制性速率，而广播和组播使用最高配置的强制性速率。

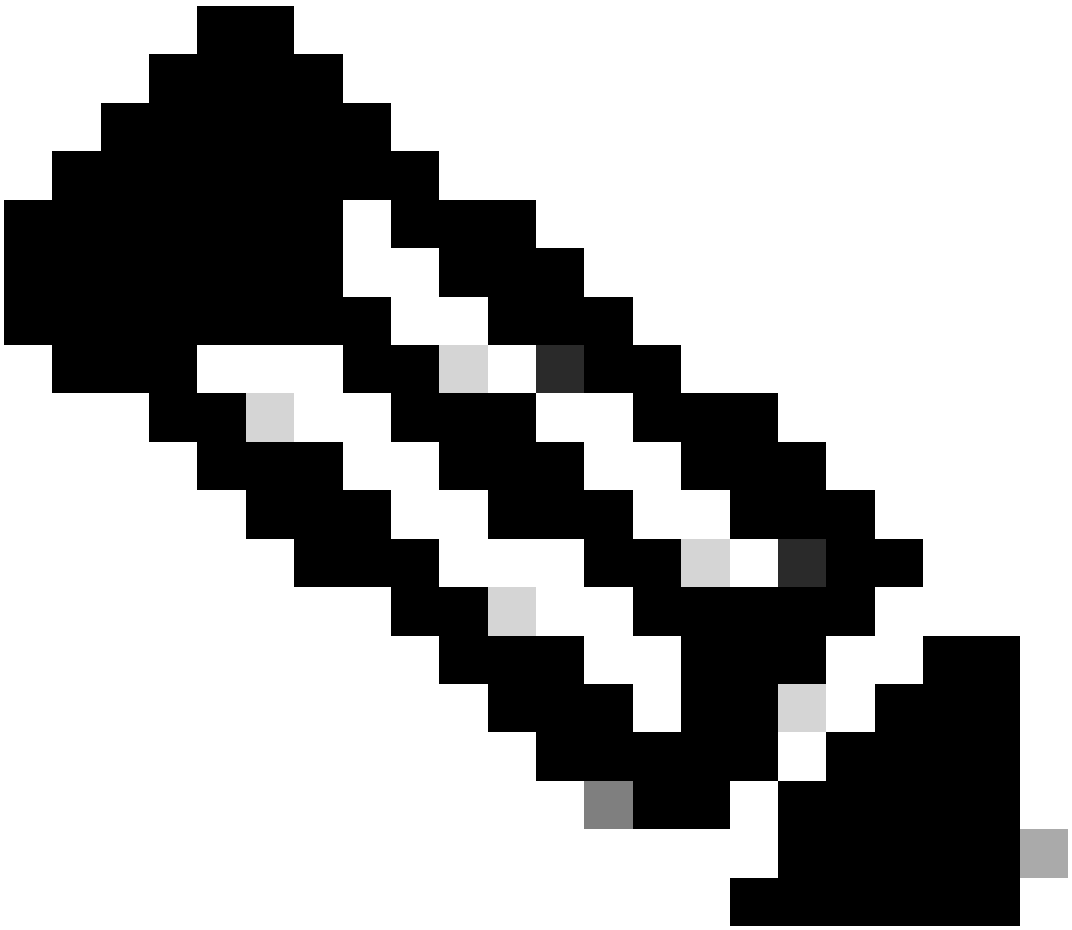
管理帧包括客户端必须侦听到才能与AP关联的信标。增加强制速率还会增加该传输的SNR要求，请回想一下，更高的数据速率需要更高的SNR，这通常意味着客户端需要更靠近AP才能解码信标并进行关联。因此，通过操纵强制性数据速率，我们还可以操控AP的有效关联范围，强制客户端靠近AP或做出潜在的漫游决策。接近AP的客户端使用更高的数据速率，而更高的数据速率使用更少的通话时间-预期效果是更高效的信元。请务必记住，提高数据速率仅影响特定帧的传输速率，它不会影响天线的RF传播或干扰范围。仍然需要良好的RF设计实践来最小化同信道干扰和噪声。

相反，将较低速率保留为必需速率通常意味着客户端可以从更远的距离进行关联，这在较低的AP密度情况下很有用，但在较高密度情况下可能会造成漫游混乱。任何试图定位正在广播6Mbps的恶意AP的人都知道，您可以检测到远离其物理位置的AP！

在广播和组播主题上，在某些情况下，配置第二个（较高）强制速率以增加组播流量的交付速率。这很少会成功，因为组播永远不会被确认，并且一旦帧丢失就不会重新传输。由于某些丢失是所有无线系统中固有的，因此无论配置的速率如何，某些组播帧都不可避免地会丢失。实现可靠组播传输的更好方法是组播到单播的转换技术，该技术将组播作为单播流传输，具有更高的数据速率和可靠（确认）传输的优势。

首选仅使用单一强制性费率，禁用低于强制性费率的所有费率，并将高于强制性费率的所有费率保留为受支持。具体使用速率取决于使用案例，如前所述，较低的速率适用于密度较低、AP间距离较大的室外场景。对于高密度和事件网络，必须禁用低速率。

如果您不确定从何处开始，请对低密度部署使用12Mbps的强制性速率，对高密度部署使用24Mbps。事实证明，许多大型活动、体育场甚至高密度企业办公室部署都能够可靠地运行，并采用24Mbps的强制性速率设置。建议对需要低于12Mbps或高于24Mbps速率的特定使用案例进行适当的测试。

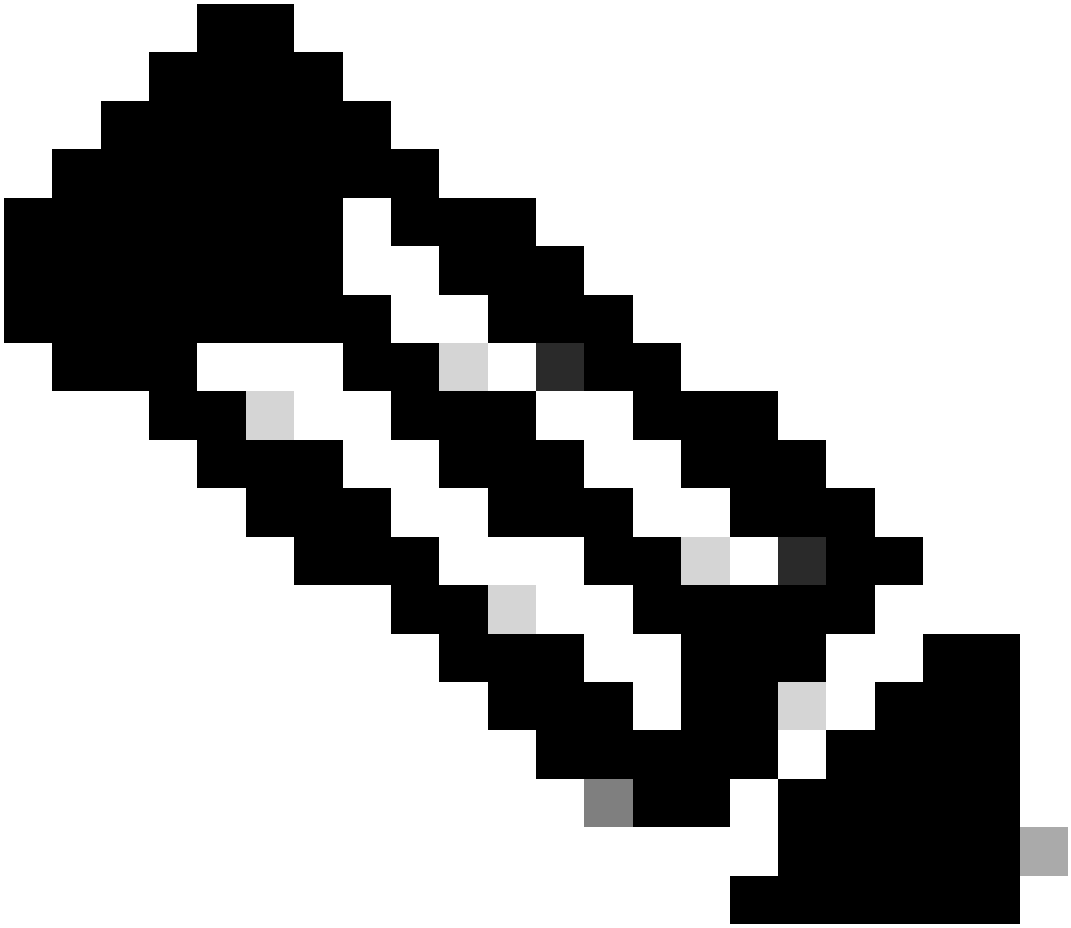


注意：最好使所有802.11n/ac/ax速率保持启用状态（WLC GUI的“高吞吐量”部分中的所有速率），无需禁用其中任何速率。

传输功率

发射功率建议因部署类型而异。在这里，我们将使用全向天线的室内部署与使用定向天线的室内部署区分开来。这两种类型的天线都可以在大型公共网络中存在，不过它们通常覆盖不同类型的区域。

对于全向部署，通常使用自动传输功率控制(TPC)，具有静态配置的最小阈值，在某些情况下，也具有静态配置的最大阈值。



注意：TPC阈值是指无线电发射功率和排除天线增益。始终确保天线增益针对所使用的天线型号正确配置，对于内置天线和自识别天线，这是自动完成的。

示例 1

TPC最小值：5dBm，TPC最大值：最大(30dBm)

这将导致TPC算法自动确定发射功率，但绝不会低于已配置的最小阈值5dBm。

示例 2

TPC最小值：2dBm，TPC最大值：11 dBm

这将导致TPC算法自动确定发射功率，但始终保持在2dBm和11dBm之间。

一种好的方法是使用不同的阈值创建多个RF配置文件，例如低功率(2-5dBm)、中等功率(5-11dbM)和高功率(11-17dBM)，然后根据需要将全向AP分配给每个RF配置文件。每个RF配置文件的值都可以调整为预期的使用案例和覆盖区域。这允许RRM算法动态运行，同时保持在预定义边界内。

定向天线的方法非常类似，唯一的区别是所需的精度级别。在部署前RF勘测期间，必须设计并验证定向天线的放置，此过程通常会得到特定的无线电配置值。

例如，如果需要安装在天花板上的贴片天线覆盖约26英尺（8米）高度内的特定区域，RF勘测必须确定达到此预期覆盖范围所需的最小发射功率（这确定RF配置文件的最小TPC值）。同样，从同一RF调查中，我们会了解此天线与下一条天线之间可能需要的重叠，甚至我们希望覆盖结束的时间点，这将为RF配置文件提供最大TPC值。

定向天线的RF配置文件通常使用相同的最小和最大TPC值，或配置范围狭窄的可能值（通常<= 3dBm）。

RF配置文件是确保配置一致性的首选，建议不要对单个AP进行静态配置。建议根据覆盖区域、天线类型和使用案例命名RF配置文件，例如RF-Auditorium-Patch-Ceiling。

正确的发射功率大小是预期覆盖区域的最弱客户端达到所需的SNR值，并且不超过该值。30dBm是真实世界条件下（即人满为患的场所中）很好的客户端SNR目标值。

CHD

覆盖空洞检测(CHD)是识别和修复覆盖空洞的独立算法。CHD是全局配置的，也是按WLAN配置的。CHD的一个可能效果是发射功率增加以补偿覆盖盲区（客户端一直检测到信号较差的区域），此效果在无线电级别上并影响所有WLAN，即使由为CHD配置的单个WLAN触发也是如此。

大型公共网络通常使用RF配置文件配置为特定功率水平，有些可能位于客户端漫游进出区域的开放区域，无需使用算法动态调整AP发射功率以响应这些客户端事件。

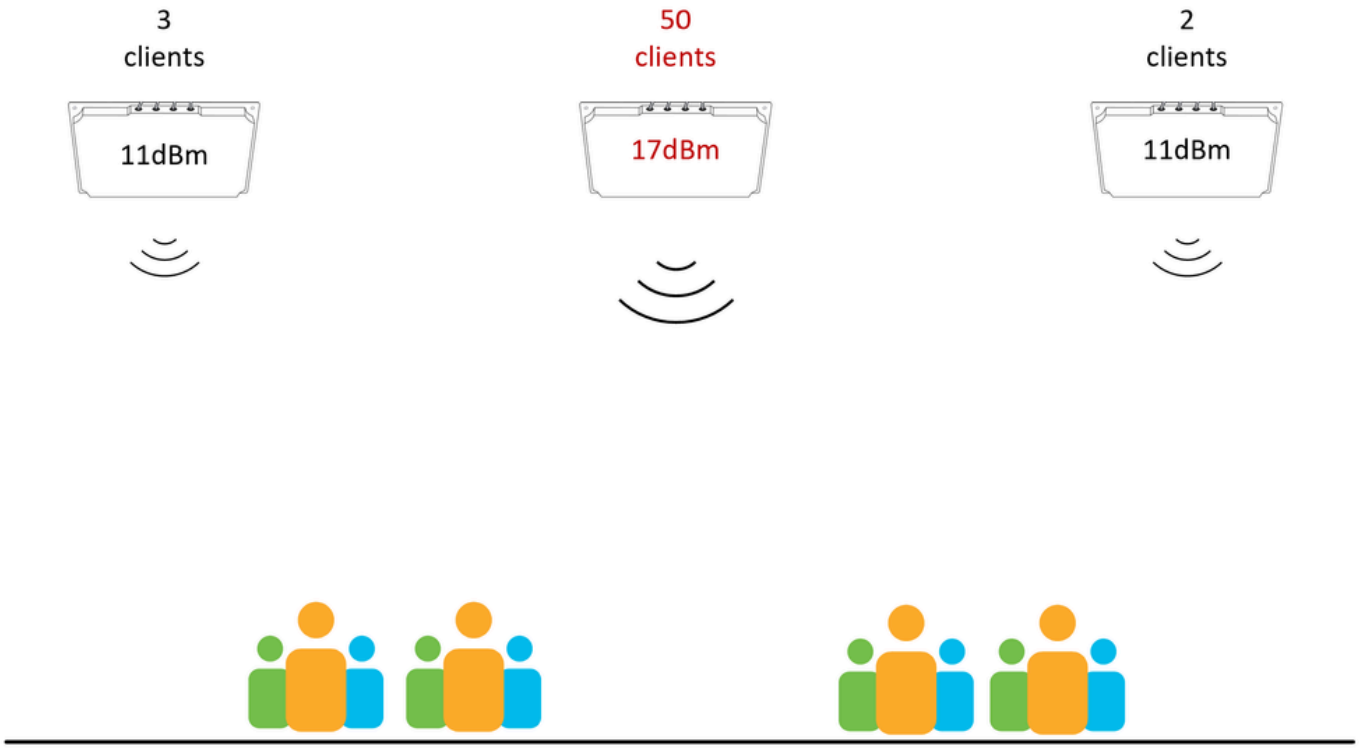
对于大型公共网络，必须全局禁用CHD。

功率平衡

大多数客户端设备在选择要与哪个AP关联时，会首选较高的接收信号。必须避免为AP配置的发射功率远远高于周围其他AP的情况。以较高发射功率运行的AP会吸引更多客户端，导致AP之间的客户端分布不均匀（例如，单个AP/无线电客户端过载，而周围AP未得到充分利用）。这种情况常见于多个天线存在较大覆盖重叠的部署，以及一个AP连接了多个天线的情况。

当选择Tx功率作为天线波束按设计重叠时，体育场天线（如C9104）需要特别注意，请参阅Catalyst 9104体育场天线(C-ANT9104)部署指南了解详细信息。

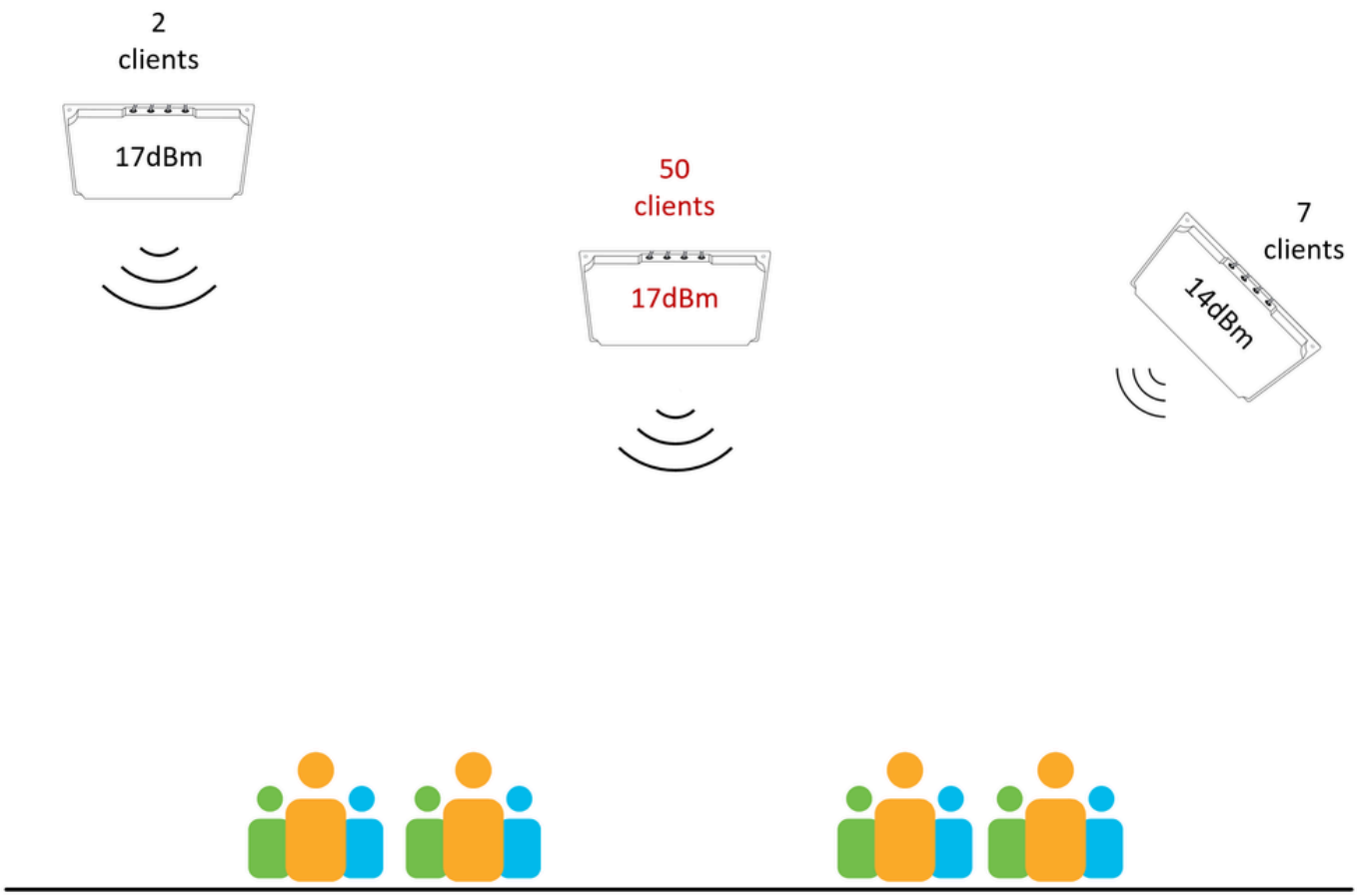
在下图中，中间的天线配置的发射功率高于周围天线的发射功率。此配置可能会导致客户端“粘滞”到中间天线。



功率高于邻居AP的AP会吸引周围的所有客户端

下图显示了一个更复杂的情况，并非所有天线都处于相同高度，并且并非所有天线都使用相同的倾斜/方向。实现功率平衡比简单地为所有无线电配置相同的Tx功率更复杂。在这种情况下，可能需要进行部署后现场勘测，这样可以从客户端设备的角度（地面）查看覆盖范围。调查数据可用于平衡配置，实现最佳覆盖范围和客户端分布。

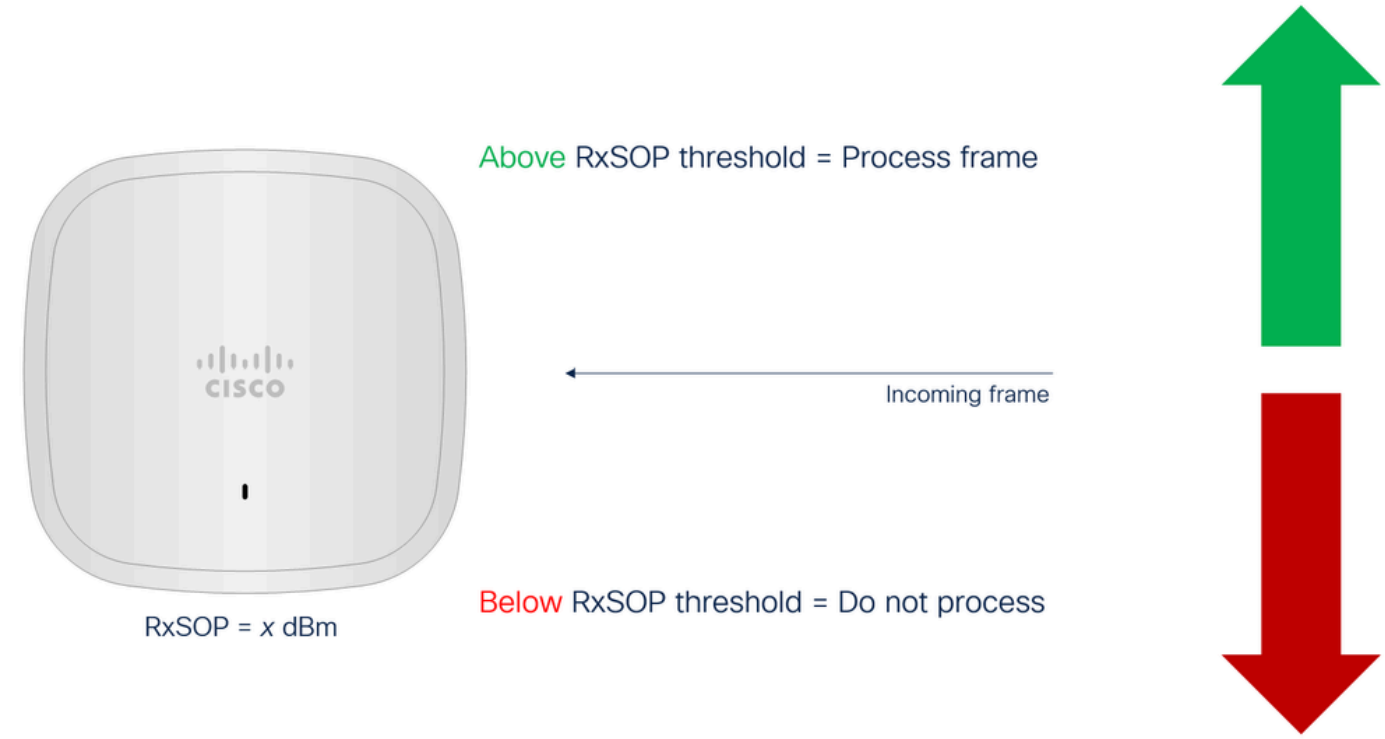
设计统一的无线接入点放置位置来避免类似这种复杂情况是防止具有挑战性的射频调整场景的最佳方法（尽管有时没有其他选择！）。



尽管发射功率相似，但一个AP仍然吸引着所有客户端，但高度和角度在其中发挥了作用

RxSOP

与影响发射信元特性的发射功率或数据速率等机制不同，RxSOP（接收方开始数据包检测）旨在影响接收信元的大小。实质上，RxSOP可以视为噪声阈值，因为它定义了接收信号电平，AP在该电平下不会尝试解码传输。到达时信号电平低于所配置的RxSOP阈值的所有传输都不会被AP处理，而是被有效视为噪声。



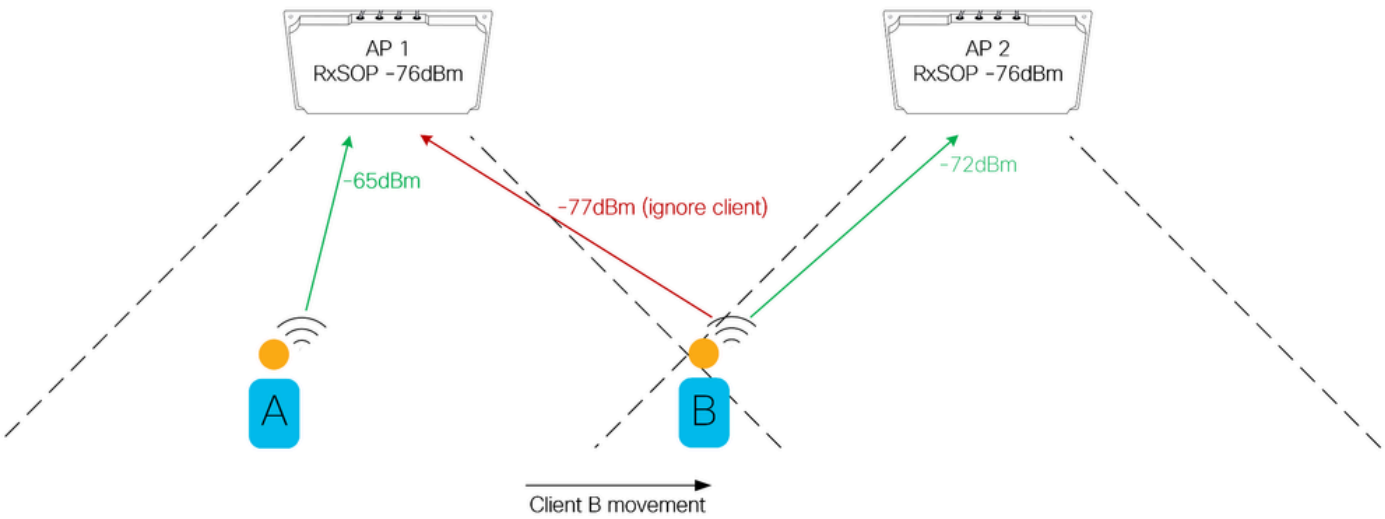
RxSOP概念介绍

RxSOP的重要性

RxSOP具有多种用途。它可用于提高AP在嘈杂环境中的传输能力，控制客户端在天线之间的分配，以及优化较弱和粘滞客户端。

在嘈杂的环境中，请回想一下，在发送802.11帧之前，发送站（本例中为AP）首先需要评估介质的可用性，此过程的部分内容是首先侦听已发生的传输。在密集型Wi-Fi环境中，通常会有许多AP在相对有限的空间中共存，并且通常使用相同的信道。在如此繁忙的环境中，AP可以报告来自周围AP的信道利用率（包括反射），并延迟其自身的传输。通过设置适当的RxSOP阈值，AP可以忽略那些较弱传输（感知信道利用率降低），从而导致更频繁的传输机会和更高的性能。AP报告没有任何客户端负载的情况下信道利用率很高（例如> 10%）的环境（例如空场地）非常适合进行RxSOP调整。

对于使用RxSOP的客户端优化，请考虑下图。



受rxsop影响的客户端漫游

在本例中，有两台AP/天线具有明确定义的覆盖区域。客户端B正在从AP1的覆盖区域移动到AP2的覆盖区域。AP2比AP1能更好地侦听客户端，但客户端尚未漫游到AP2的交叉点。这是设置RxSOP阈值如何实施覆盖区域边界的一个很好的示例。确保客户端始终连接到最近的AP，通过消除以较低数据速率提供服务的远程和/或弱客户端连接来提高性能。以这种方式配置RxSOP阈值需要透彻了解每个AP的预期覆盖区域的开始和结束位置。

RxSOP的危险。

过于积极地设置RxSOP阈值会导致覆盖盲区，因为AP无法解码来自有效客户端设备的有效传输。这会对客户端产生不良后果，因为AP没有响应；毕竟，如果没有侦听到客户端传输，就没有理由做出响应。必须谨慎调整RxSOP阈值，始终确保配置的值不会排除覆盖区域内的有效客户端。请注意，一些客户端无法通过这种方式很好地响应被忽略，过于激进的RxSOP设置不会给客户端一个自然漫游的机会，从而实际上会迫使客户端查找另一个AP。能够解码来自AP的信标的客户端假定它能够传输给该AP，因此，RxSOP调整的意图是将接收信元的大小与AP的信标范围相匹配。请记住，（有效的）客户端设备并不总是能够直接到达AP，用户面对天线或将其设备放在袋子或口袋中时，信号通常会衰减。

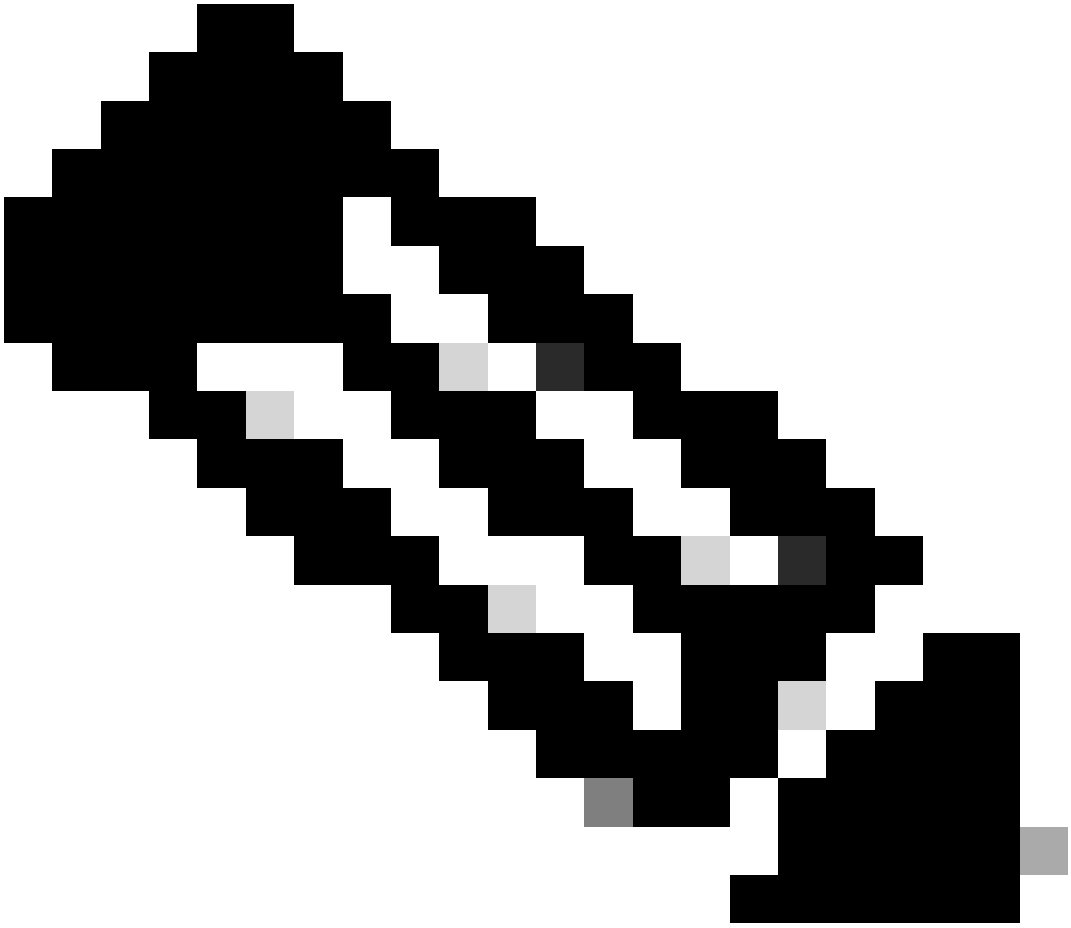
配置RxSOP

RxSOP是按射频配置文件配置的。

对于每个频段，预设阈值（低/中/高）会设置预定义的dBm值。此处建议始终使用自定义值，即使预期值为可用预设，这样也可使配置更易读。

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

RxSop设置表



注意：RxSOP更改不需要无线电重置，并且可以动态完成。

扩展网络

一般来说，最大限度地使用设备已编档的功能是不明智的。数据表报告真实情况，但所提及的数字可能处于特定活动条件下。无线控制器经过测试和认证，可支持一定数量的客户端和AP以及特定的吞吐量，但这不是假设客户端每秒漫游一次、可以为每个客户端配置极长的唯一ACL或者启用所有可用的监听功能。因此，必须仔细考虑所有方面，以确保网络在高峰时段扩展，并为未来增长保持安全裕度。

AP数量

部署任何网络的首要任务之一就是预算并订购适当数量的设备，而最大的可变因素则是接入点和天线的数量和类型。无线解决方案必须始终基于射频设计，但是（不幸的是），这通常是项目生命周期中的第二步。在简单的室内企业部署中，有许多估计技术可以在无线架构师查看平面图之前，以合理的确定性水平预测可能需要多少个AP。在这种情况下，预测模型也非常有用。

对于更具挑战性的安装（例如工业、室外、大型公共网络或需要外部天线的任何地方），简单的估算技术通常是不够的。在以前的类似安装中，需要具备一定级别的经验才能充分估计所需设备的类型和数量。无线架构师的现场探访是了解复杂场所或设施布局的最低要求。

本部分提供有关如何确定给定部署的AP和天线的最小数量的指南。最终数量和特定安装位置始终将通过需求分析和无线电设计流程确定。

初始物料清单必须基于两个因素：天线类型和天线数量。

天线类型

这里没有快捷方式。天线类型由需要覆盖的区域以及该区域中的可用安装选项决定。如果不了解物理空间，则不可能确定此项，这意味着了解天线及其覆盖模式的人需要进行现场探访。

天线数量

所需设备的数量可以通过了解客户端连接的预期数量来确定。

每人的设备

用户数量可以通过场所的座位容量、售出的门票数量或基于历史统计数据的预期游客数量来确定。每个人类用户可携带多个设备，通常假设每个用户拥有多个设备，但人类用户同时主动使用多个设备的能力值得怀疑。主动连接到网络的访客数量也取决于事件类型和/或部署。

示例1：拥有80,000个座位的体育场没有连接80,000台设备是很正常的，这个百分比通常要低很多。在体育赛事中，20%的连接用户比率并不罕见，这意味着对于拥有80,000个席位的体育场而言，预计连接设备的数量可以是16,000 (80,000 x 20% = 16,000)。此数字还取决于使用的自注册机制，如果要求用户执行某些操作（例如点击Web门户），则数字低于设备自动自注册时的值。自动登录可以简单到像以前事件中记住的PSK，或者更高级的操作（如使用OpenRoaming），无需用户交互即可登录设备。OpenRoaming网络可以将用户的使用率大幅提高到50%以上，从而对容量规划产生重大影响。

示例2：有理由期待技术会议具有高用户连接率。会议参与者需要花费更长的时间连接到网络，并希望能够访问其电子邮件并在全天内执行日常任务。此外，这类用户很可能将多台设备连接到网络，尽管同时使用多台设备的能力仍存在疑问。对于技术会议，假设100%的访客连接到网络，此数字可能更低，具体取决于会议类型。

在这两种情况下，关键都是要了解预计的已连接设备数量，而且没有针对每个大型公共网络的单一解决方案。无论哪种情况，天线都会连接到无线电，而连接到该无线电的是客户端设备（非人类用户）。因此，每个无线电的客户端设备是一个可用度量。

每无线电设备数

对于Wi-Fi 6个AP，思科AP的最大客户端计数为每无线电200个连接设备；对于Wi-Fi 6E AP，每无线电400个连接设备。但是，不建议设计最大客户端计数。出于规划目的，建议将每个无线电的客户端数量保持在最大AP容量的50%以下。此外，无线电数量取决于所用的AP和天线的类型，关于单、双5GHz的部分对此进行了更详细的探讨。

在此阶段，最好将网络划分为不同的区域，每个区域都有预期的设备数量。回想一下，本部分旨在

估计AP和天线的最低数量。

以三个不同覆盖区域的示例为例，为每个区域提供预期客户端计数，并使用每个无线电75个客户端的（正常）值来估计所需的无线电数量。

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

每个区域的预期无线电/客户端数量

这些初始数字现在需要结合了解每个区域中部署的AP和天线类型，以及是否使用单或双5GHz。6GHz计算遵循的逻辑与5GHz相同。本例中不考虑2.4GHz。

我们假设这三个区域分别使用2566P贴片天线和9104体育场天线，以及单频和双5GHz的组合-此场景用于说明目的。

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)

每区域天线数

每个区域列出所需的天线和AP的类型。请注意，在双5GHz的情况下，比值为两个天线对一个AP。

本节介绍如何估计部署所需的天线和AP的初始数量。估算时需要了解物理区域、每个区域中可能的

安装选项、每个区域中要使用的天线类型以及预期的客户端设备数量。

每次部署都各不相同，并且通常需要额外的设备来覆盖特定或具有挑战性的领域，这种类型的评估仅考虑客户容量（未覆盖），并用于概述所需投资的规模。最终AP/天线放置位置和设备总数始终取决于经验丰富的无线专家对使用案例的透彻了解以及现场验证。

预期吞吐量

每个无线信道可提供一定数量的可用容量，通常转换为吞吐量。此容量在连接到无线电的所有设备之间共享，这意味着随着更多用户连接添加到无线电中，每个用户的性能都会下降。性能下降并非线性，并且还取决于所连接的客户端的确切组合。

客户端功能因客户端芯片集和客户端支持的空间流数量而异。下表列出了每个支持的空间流数的最大客户端数据速率。

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

每种客户端类型的预期最大实际吞吐量

所列速率是理论最大MCS（调制和编码方案）速率，源自802.11标准，假设信噪比(SNR) >30dBm。性能良好的无线网络的主要设计目标是使所有位置的所有客户端都达到这一级别的SNR，但这种情况很少发生。无线网络在本质上是动态的，并且使用未经许可的频率，除了客户端功能外，各种不受控制的干扰也会对客户端SNR产生影响。

即使在达到所需的SNR水平的情况下，以前列出的速率也不考虑协议开销，因此，不会直接映射到实际吞吐量（由各种速度测试工具测量）。实际吞吐量始终低于MCS速率。

对于所有无线网络（包括大型公共网络），客户端吞吐量始终取决于：

- 客户端的功能。
- 客户端在该特定时间点的信噪比。
- 在该特定时间点连接的其他客户端的数量。
- 其他客户端在该特定时间点的功能。
- 特定时间点上其他客户端的活动。
- 特定时间点的干扰。

根据这些因素的可变性，无论设备供应商是谁，都无法保证无线网络的每客户端流量最低。

有关详细信息，请参阅验证Wi-Fi吞吐量：测试和监控指南。

WLC平台

选择您的WLC平台似乎很简单。首先，您可以考虑您要管理的估计AP数量和客户端数量。每个WLC平台的数据表包含平台上支持的所有最大对象：ACL、客户端计数、站点标记等。这些都是字面上的最大数目，而且往往很难执行。例如，您不能将6001个AP连接到仅支持6000个AP的9800-80。但是，在任何地方追求最大目标是明智的吗？

思科无线控制器经过测试，能够达到这些最大值，但是它们不一定能同时达到所有条件中记录的所有最大值。以吞吐量为例，9800-80可以达到最高80 Gbps的客户端数据转发，但每个客户端数据包的最大和最佳大小均为1500字节时就是这种情况。混合数据包大小时，有效最大吞吐量较低。如果启用DTLS加密，吞吐量会进一步降低，应用可视性也是如此。在具有启用许多功能的大型网络中，现实状况下，预计9800-80的吞吐量将超过40 Gbps，这相当乐观。由于这取决于正在使用的功能和网络活动的类型，因此了解实际容量的唯一方法是使用此命令测量数据路径利用率。重点关注load指标，该指标是控制器可以转发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#
```

同样，9800-80也可以通过正常活动完美地处理6000个AP。但是，体育场或机场等公共场所的6000个AP不算作常规活动。考虑到客户端漫游和周围探测的规模，最大规模的大型公共网络会导致单个WLC上的CPU使用率增加。如果添加监控和SNMP陷阱，每次客户端移动时发送它们，负载可能会很快变得过大。大型公共场所或大型活动的其中一个主要特点是，随着人们四处走动并不断关联/取消关联，客户端入网事件明显增多，因此这会对CPU和控制平面造成额外压力。

大量部署表明，一对9800-80无线控制器可以处理超过1000个接入点的大型体育场部署。对于正常运行时间和可用性成为主要关注点的关键事件，将AP分配到两个或更多控制器对上也很常见。当大型网络分布在多个WLC上时，控制器间漫游会更加复杂，在体育场馆等封闭空间内必须仔细考虑客户端漫游。

另请参阅本文档中的站点标签部分。

WLC高可用性

建议使用高可用性状态切换(HA SSO)对，这样既可提供硬件冗余，又可防止软件故障。使用HA SSO，一台设备上的软件崩溃对最终用户是透明的，因为辅助WLC会无缝接管。HA SSO对的另一项优势是服务中软件升级(ISSU)功能提供的无中断升级。

如果网络足够大，建议使用额外的控制器(N+1)。它可以满足HA SSO无法实现的几个目的。您可以在升级生产对之前在此WLC上测试新的软件版本（并且仅将几个测试AP迁移到此WLC上以测试网络的特定部分）。某些罕见情况可能会影响HA对中的两个WLC（当问题复制到备用时），此处N+1允许在主用-主用情况下拥有安全的WLC，在此情况下可以逐步将AP迁入和迁出。它还可以用作配置新AP的调配控制器。

9800-CL具有很强的扩展性和功能。需要注意的是，它们的数据转发容量要小得多（对于SR-IOV映像，从2 Gbps到4 Gbps），这往往会限制它们只能使用FlexConnect本地交换方案（在中心交换中可能只有少量的AP）。但是，在维护时段或排除故障期间，当您需要额外控制器时，它们可以作为N+1设备提供帮助。

外部系统

虽然本文档主要介绍大型事件网络的无线组件，但在扩展和设计阶段还需要考虑许多支持系统，其中一些将在本文中讨论。

核心网络

大型无线网络通常以集中交换模式部署，并且包含大型子网。这意味着大量客户端MAC地址和ARP条目被推送到相邻的有线基础设施。专用于各种L2和L3功能的相邻系统必须拥有足够的资源来处理此负载。对于L2交换机，常见的配置是调整交换机设备管理器(SDM)模板，SDM负责分配系统资源，并根据网络中设备的功能在L2和L3功能之间实现平衡。确保核心L2设备能够支持预期的MAC地址条目数量非常重要。

网关NAT

公共网络最常见的使用案例是为访客提供Internet接入。数据路径中一定有负责NAT/PAT转换的设备。Internet网关必须具备所需的硬件资源和IP池配置才能处理负载。请记住，单个无线客户端设备可以负责大量NAT/PAT转换。

DNS/DHCP

这两个系统是确保良好客户端体验的关键。DNS和DHCP服务不仅需要适当的扩展来处理负载，还需要考虑在网络中的位置。与WLC位于同一位置的快速响应系统可确保最佳体验并避免客户端登录时间过长。

AAA/Web门户

没有人喜欢速度缓慢的网页，因此，为外部Web身份验证选择适当且扩展良好的系统对于良好的客户端登录体验非常重要。对于AAA，RADIUS身份验证服务器也必须能够满足无线系统的要求。请记住，在某些情况下，负载会在关键时刻达到高峰，例如在足球比赛期间达到半小时，这会在短时间内生成较高的身份验证负载。扩展系统以实现并发足够负载是关键。使用AAA记帐等功能时，必

须特别小心。不惜一切代价避免基于时间的记帐，如果使用记帐，请设法禁用临时记帐。另一个需要考虑的重要项目是使用负载均衡器，此处必须使用会话计时机制来确保完整的身份验证流程。确保将RADIUS超时保持在5秒或更长。

如果使用带有大量客户端的802.1X SSID（例如使用OpenRoaming），请确保启用802.11r快速过渡(FT)，否则客户端每次漫游时都可能引发身份验证风暴。

DNS/DHCP

关于DHCP的一些建议：

- 确保DHCP地址池至少是预期客户端数量的三倍。即使在客户端断开连接后，IP仍会保持分配一段时间，因此，根据访客的停留时间，这会消耗更多的IP地址。尝试将租用时间与用户访问场所的预期持续时间相匹配，如果通常访问持续时间为两个小时，则分配一周的IP地址没有意义，这有助于淘汰陈旧的租约。
- 建议为客户端使用一个大型子网，WLC具有代理ARP功能，并且默认情况下不转发广播（DHCP除外）。为客户端使用大型（例如/16）客户端子网不会带来问题。单个大型VLAN比具有多个VLAN的VLAN组简单。配置许多较小的子网（例如/24）和VLAN组不会影响广播域，只会导致配置更加复杂，从而产生诸如脏VLAN和必须跟踪无法均匀使用的各种DHCP池等问题。
- 使用子网的第3层网关处理的DHCP中继功能，在无线控制器上保持DHCP处于桥接模式。这样可以实现最大的效率和简便性。其理念是根本不需要在DHCP过程中使用无线控制器。
- 在任何公共WLAN上使用DHCP Required，无论身份验证方法如何。虽然这可以触发一小部分失败的客户端关联，但是如果客户端尝试为自己分配静态IP地址，或者客户端行为不端并试图未经允许重复使用以前的IP地址，则可能会阻止出现严重的安全问题。

运行网络

正确的配置

启用大量选项以从现代Wi-Fi的所有最新功能中获益颇具诱惑力。但是，某些功能在小型环境中运行良好，但在大型和密集环境中影响巨大。同样，某些功能也会带来兼容性问题。尽管思科设备符合所有标准，并且与各种经过测试的客户端兼容，但世界上充斥着独特的客户端设备，这些客户端设备有时具有带有错误或不兼容某些功能的驱动程序软件版本。

根据您对客户端的控制级别，您必须保持保守。例如，如果您部署了Wi-Fi用于公司的大型年度聚会，您知道大多数客户端是公司设备，您可以相应地规划启用该功能集。另一方面，如果您运营的是机场Wi-Fi，那么您的访客满意度水平直接与他们连接到您的网络的能力相关，而您对人们可以使用的客户端设备没有任何控制。

SSID

多少个SSID？

建议始终尽可能少用SSID。在高密度网络中，由于几乎可以保证在同一个信道上有多个AP，因此这种情况会更加严重。通常，许多部署使用的SSID太多，它们承认拥有的SSID太多，但声明不能

使用更少的SSID。您必须对每个SSID进行业务和技术研究，以了解SSID和将多个SSID合并为一个SSID的选项之间的相似之处。

让我们来看看安全/SSID的几种类型及其用法。

WPA2/3个人

预共享密钥SSID由于其简单性而广受欢迎。你可以把钥匙印在徽章上的某个地方、纸上或标语上，或者以某种方式把它传达给来访者。有时，甚至访客SSID也首选预共享密钥SSID（前提是密钥为所有参与者所熟知）。它有助于防止由于连接的有意为而导致DHCP池耗尽。经过的设备不会自动连接到网络，因此无法使用DHCP池中的IP地址。

WPA2 PSK不提供隐私保护，因为每个人都使用相同的密钥，所以可以轻松解密流量。相反，WPA3 SAE提供私密性，即使每个人都拥有主密钥，也无法派生其他客户端使用的加密密钥。

WPA3 SAE是更好的安全选择，许多智能手机、笔记本电脑和操作系统都支持它。某些IoT设备或智能可穿戴式设备仍然具有有限的支持，并且如果较旧的客户端没有收到最新的驱动程序或固件更新，则它们通常容易出现问题。

为了简化操作，人们可能会忍不住考虑使用过渡模式WPA2 PSK-WPA3 SAE SSID，但此字段已在字段中显示会导致一些兼容性问题。编程不当的客户端不希望同一SSID上存在两种类型的共享密钥方法。如果要同时提供WPA2和WPA3选项，建议配置单独的SSID。

WPA2/3企业

WPA3 Enterprise（使用AES 128位加密）在技术上与WPA2 Enterprise相同，安全方法（至少与SSID信标中通告的方法相同），因此具有最大的兼容性。

对于802.1X，建议使用过渡模式SSID，因为最近使用的设备没有出现兼容性问题（Android 8或旧版Apple IOS报告了问题）。IOS XE 17.12及更高版本允许使用单个过渡企业SSID，其中仅在6GHz上使用和通告WPA3，而5GHz频段上提供WPA2选项。我们建议尽快在企业SSID上启用WPA3。

WPA企业SSID可用于具有身份提供者数据库的密钥用户，该数据库允许根据用户身份返回AAA参数（例如VLAN或ACL）。此类类型的SSID可以包括eduroam或OpenRoaming，将访客SSID的优点（允许访客轻松连接，而无需输入任何凭证）与企业SSID的安全性结合在一起。它们显著降低了通常与802.1X关联的登录的复杂性，因为客户端只要在其电话上拥有配置文件（可通过事件应用轻松提供），就无需执行任何操作即可加入欧洲漫游或OpenRoaming SSID

访客SSID

访客SSID通常与开放式身份验证同义。您可以在其后面添加（或不添加）Web门户（取决于所需的友好性或本地要求），其形式多种多样：外部、本地或中心Web身份验证，但概念保持不变。使用访客门户时，可扩展性在大型环境中可能会迅速成为问题。有关此内容的详细信息，请查看配置可扩展性部分。

6GHz操作要求您的访客SSID使用增强型开放式而非仅开放式。这仍允许任何人进行连接，但提供了隐私（甚至比WPA2-PSK更好的隐私！）和加密，在连接SSID时无需提供任何密钥或凭证。主要

的智能手机供应商和操作系统现在都支持增强型开放式，但这种支持尚未在无线客户端群中广泛普及。增强型开放过渡模式提供良好的兼容性选项，支持该模式的设备连接到加密的访客SSID（使用增强型开放），不支持该模式的设备仍然使用SSID，就像之前一样只是简单地打开即可。虽然最终用户注意到只有一个SSID，但请注意，此过渡模式会在您的信标中广播两个SSID（尽管只能看到一个）。

在大型活动和场所中，通常建议在访客SSID上配置PSK，而不是将其完全保持为打开状态（增强开放过渡模式会更好，但这样会创建两个SSID，并且客户端兼容性仍必须得到广泛验证）。尽管这会使注册过程更加复杂（您必须在人们的胸卡或门票上打印PSK，或者以某种方式将其通告），但是它可避免临时客户端自动连接到网络，而最终用户却无意使用网络。越来越多的移动操作系统供应商也取消了开放式网络的优先级，并显示安全警告。在其他情况下，您可能希望连接最大数量的路人，因此最好选择“打开”。

关于SSID数量的结论

对于您必须坚持多少个SSID这一问题，没有令人满意的答案。其影响取决于最小配置的数据速率、SSID数量以及在同一信道上广播的AP数量。在思科的一次大型活动中，无线基础设施使用了5个SSID：主WPA2 PSK、用于安全和6GHz覆盖范围的WPA 3 SAE SSID、用于方便教育参与者访问的企业教育SSID、用于安全地欢迎任何从活动应用配置Wi-Fi的人员的OpenRoaming SSID以及用于员工和管理网络访问的单独的802.1X SSID。 这几乎已经太多了，但是由于可用的信道数量庞大，并且使用定向天线来尽可能减少信道重叠，所以效果还是保持合理的。

传统SSID与主要SSID的概念

在一定期限内，建议将2.4GHz服务限制为仅通告给2.4GHz的“传统”独立SSID。随着人们完全停止提供2.4GHz服务，这种方案越来越不流行。然而，这个想法可以而且必须持续下去，但与其他概念无关。您想实施WPA3 SAE，但过渡模式是否给您带来了与客户端的兼容性问题？具有WPA2“传统”SSID和主WPA3 SAE SSID。通过将性能最低的SSID命名为“legacy”，它不会吸引客户端，您可以轻松看到有多少客户端仍然面临与您的主SSID的兼容性问题，并且需要此传统SSID。

但是为什么停在那里呢？您听到传言说802.11v导致某些较旧客户端出现问题，或者某些客户端驱动程序不希望看到SSID上启用的设备分析？在高级主SSID上启用所有这些方便的功能，并在旧版/兼容SSID上禁用这些功能。这允许您在主SSID上测试新功能的推出，同时仍为客户端提供最大兼容性SSID以便回退。这个系统只能这样运作。如果您将您的兼容性驱动的SSID作为主设备使用相反的名称，并将您的高级SSID命名为“<name>-WPA3”之类的名称，您会发现人们固守着以前使用过的旧SSID，并且您的“新”SSID的采用率多年来一直很小。由于连接新设置或功能的客户端数量较少，因此推广新设置或功能会产生不确定的结果。

SSID功能

- 最好禁用Aironet扩展功能。这些功能对于现场勘测和WGB操作特别有用，但有时会导致一些传统客户端出现问题。Aironet IE还会通告AP主机名，这在注重安全的部署中是不必要的。
- CCKM是已弃用的协议（支持FT），必须禁用。
- 此时，最好使用AES-128加密，即使在WPA3中也是如此，因为客户端对更高加密的支持较低（除非您可以负担一个特定的更安全且更严格的SSID）
- 最好禁用覆盖盲区检测（适用于所有SSID）。大型部署通常使用定向天线，需要进行全面的现场勘测。每个天线的功率电平都是RF设计流程的结果，通常配置为特定电平。

- 必须禁用自适应FT，因为当FT未完全通告但存在于某些属性中时，某些客户端可能会出现问题。要么完全禁用FT（以实现最大兼容性），要么选择大多数客户端都支持FT+802.1X（除非它们更旧或更面向IoT）。配置FT+802.1X时，甚至允许非FT客户端加入SSID。唯一可能的问题是某些客户端不允许在同一SSID上看到两个安全选项。
- 禁用802.11ac MU-MIMO。它增加了复杂性，在802.11ac中的优势非常低。
- 禁用BSS目标唤醒时间。目前客户端的采用率较低。
- 禁用主动负载均衡和频段选择。如果您未在2.4GHz中通告SSID（或者它位于专用SSID上），则无需选择Band Select（频段选择），并且如果客户端坚持连接到已加载的AP，则主动负载均衡会在最终接受客户端之前拒绝该客户端几次，从而延迟客户端关联。您仍然在一个繁忙的环境中加载了AP，这对客户端体验是负面的。
- 禁用Fastlane+。
- 禁用通用管理，此功能用于3700 AP，并且仅用于-UX域。任其发展会导致不必要的攻击媒介。
- 保持启用机会密钥缓存(OKC)。对于不支持FT的客户端，它充当快速漫游机制。
- 保留WMM允许。禁用它会将您的网络带回802.11g时代，而且要求它不会为9800平台带来任何优势。
- 启用IP源防护。
- 禁用RADIUS分析。在非常繁忙的环境中，这会发送过多的RADIUS记账消息（只要客户端执行DHCP或发送HTTP数据包），并且非常有可能使RADIUS服务器过载。
- 避免使用隐藏的SSID。这没有任何安全目的，SSID名称仍可通过简单应用程序或采用嗅探器捕获轻松发现。隐藏SSID会减慢所有客户端漫游速度，因为它们不再受益于被动信标扫描，必须依靠主动扫描来获取相邻AP信息。
- 尝试每个无线电使用不超过四个WLAN，因为它对RF利用率有重大影响。这并不是一个硬性限制，使用五个WLAN可以正常工作，但是由于使用越来越多的WLAN，因此会非常注意浪费的通话时间。
- 802.11v和802.11k是越来越受常见客户端类型支持的标准。它们通常不会造成客户端连接问题。它们带来的好处在很大程度上取决于客户端如何使用这些协议，并且有时（在802.11k的情况下）会导致CPU使用率略高。您可以将它们排除在IoT或传统SSID之外，但必须尽可能在生产SSID上启用它们。

站点标签

站点标签是一个配置项目，允许对共享相同FlexConnect设置以及AP加入配置文件设置（例如凭证、SSH详情和国家代码）的接入点进行分组。为什么站点标签很重要？站点标签还定义了Catalyst 9800中的WNCD进程如何处理AP。让我们举几个例子来说明：

- 如果您在具有八个WNCD进程的9800-80上配置四个站点标记，则每个站点标记将被分配到不同的WNCD进程（在单独的CPU内核上运行每个站点），四个WNCD进程不执行任何操作。这意味着您未使用9800-80的所有CPU，因此不建议将其加载到最多支持6000个AP。

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

站点标记平衡的第一个示例

- 如果在具有八个WNCD进程的9800-80上配置10个侧标记，则两个WNCD进程分别处理两个站点标记，而其余六个进程分别处理一个站点标记。

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

站点标记平衡的第二个示例

对于具有许多站点和许多站点标记的地理位置较大的部署，站点标记的数量建议为您使用的平台上WNCD进程数量的倍数。

但是，对于通常在一个屋顶下或在同一场所有多个建筑的活动网络，建议是将站点标签数量与给定平台上WNCD的确切数量相匹配。最终目标是每个WNCD进程（以及分配给无线任务的每个CPU内核）处理大致相似数量的客户端漫游事件，以便在所有CPU内核之间均衡负载。

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

每种平台类型的WNCD进程数

在核心层，真正重要的是将处于同一物理邻居中的AP分组到同一站点标签中，以便这些AP之间频繁的客户端漫游事件保持在同一CPU进程中。这意味着，即使您有一个大型场所，仍建议将该场所分成多个站点标签（与处理场所的WNCD进程数量相同），并尽可能将AP按逻辑分组到这些标签中

，以形成逻辑射频邻居组，这些邻居组也在站点标签之间均匀分布。

从IOS XE 17.12开始，可以启用负载均衡算法，以便WLC根据AP的RF接近程度对AP进行分组。这样可以减轻负担，并使AP在WNCD过程中均衡分布。如果您无法轻松地将邻居AP的组放入正确的站点标签数量中，这会很有帮助。此算法的一个特点是，它将AP分配到WNCD进程，而不管它们的站点标签分配如何，这意味着它不会更改AP的站点标签分配。然后，您可以完全根据配置逻辑分配站点标记，让算法以最佳方式在CPU之间平衡AP。

基于RF的自动AP负载均衡功能在Cisco Catalyst 9800系列无线控制器软件配置指南、Cisco IOS XE Dublin 17.12.x中都有介绍。

在大事件期间，必须监控WNCD进程的CPU使用情况。如果一个或多个WNCD进程显示高利用率，则可能是WNCD处理了太多的AP或客户端，或者它处理的AP或客户端比平均值繁忙（如果所有进程持续漫游，例如在机场）。

策略配置文件

- 启用ARP和重复地址检测(DAD)代理，这样，当设备尝试获取无线设备的MAC地址时，WLC可以代表无线客户端进行回复。这还可以节省无线客户端电池。
- 除非需要，否则请勿启用WGB功能。
- 启用所需的DHCP以避免使用静态IP地址的客户端。
- 缩短空闲超时（300秒）。有些管理员会花很长时间来避免客户端必须重新进行身份验证，但过长的空闲超时会导致客户端计数因实时延迟而出现Ghost客户端条目（影响报告）。最好将idle -timeout保持低于组密钥轮换计时器，以避免删除客户端时的记帐泛洪。组密钥交替间隔可以在Web UI中的Configuration > Security > Advanced EAP下配置为“EAP-Broadcast Key Interval”
- 将会话超时设置为86400秒，以避免不必要的断开和重新身份验证。

AP加入配置文件

- 确保启用TCP调整MSS。
- 启用Trust DSCP upstream。很遗憾，许多无线客户端不执行802.11e WMM UP标记，信任DSCP字段是为语音应用提供正确优先级的可靠方法。
- 为您的接入点启用系统日志。配置Syslog服务器IP会使AP向其单播其控制台日志。这不仅有助于对AP进行故障排除，而且与使AP在本地VLAN中广播其系统日志的默认设置相比，它对网络也更好。AP日志记录可能会生成大量消息负载，即使在AP Syslog未被监控的情况下，通过设置适当的消息严重性和/或配置虚拟Syslog IP地址（例如0.0.0.0）以防止广播消息来限制事件数量仍是一个好主意。
- 最大化CAPWAP重试次数和超时。检测问题的速度较慢，但网络对轻微的瞬时数据包丢弃的抵抗力较强。
- 启用SSH并配置凭证。禁用AP控制台
- 根据需要启用AP监控，但不启用无线电监控。
- 启用欺诈检测并将RSSI阈值配置为-70 dBm。

监控网络

网络启动并运行后，您必须密切监控其是否存在问题。在标准的办公环境中，用户了解网络，可以

在出现问题时互相帮助，也可以打开内部帮助台故障单。在接待了大量来访者的大型场所中，您希望重点关注最大的问题，而不是那些可能只是配置错误的特定人员，因此，您需要制定正确的监控策略。

从Catalyst 9800 CLI或GUI监控网络是可能的，但它不是日常监控的最佳工具。当您已经对问题产生怀疑和/或数据并希望实时运行特定命令时，它是最直接的。主要监控选项包括Cisco Catalyst Center或自定义遥测控制面板。可以使用第三方监控工具，但是当使用SNMP作为协议时，数据远非实时，通常的第三方监控工具对于所有无线供应商的特定要求也不够精细。如果选择SNMP协议，请确保使用SNMPv3，因为SNMPv2的安全性已过时。

Cisco Catalyst Center是最佳选择，因为它允许您在监控网络的基础上管理网络。除了监控，它还允许实时故障排除和修复许多情况。

如果您希望以永远在线的方式在屏幕上显示非常具体的指标和构件，以供NOC或SOC使用，自定义遥测控制面板会很有用。如果您需要关注网络的特定区域，您可以构建专用小部件，以您选择的方式显示这些区域的网络指标。

对于事件网络，最好监控系统范围内的RF统计信息，尤其是每个AP的信道利用率和客户端数量。这可以从CLI完成，但仅提供特定时间点的快照，信道利用率往往是动态的，更适合于随时间推移进行监控。对于此类监控，自定义控制面板通常是一个不错的方法。随着时间的推移进行监控时更有价值的其他指标包括WNCD利用率、客户端数量及其状态，以及场所特定指标。场所特定指标的一个示例是监控特定区域或位置的使用和/或负载，例如，会议中心为X 号大厅，活动场所为休息区Y。

对于自定义监控，NETCONF RPC (pull)和NETCONF流传输遥测(push)都是有效的方法，尽管将自定义流传输遥测与Catalyst Center结合使用需要一些调查，因为在WLC上配置的遥测订用数量有限，并且Catalyst Center预填充（并利用）其中许多遥测订用。

使用NETCONF RPC时，需要进行一些测试以确保WLC不因NETCONF请求而过载，尤其重要的是要记住某些数据点的刷新率以及返回数据所需的时间。例如，AP信道利用率每60秒刷新一次（从AP刷新到WLC），1000个AP的RF指标收集（从WLC）可能需要几秒钟，在此示例中，每5秒轮询WLC将没有用，更好的方法是每3分钟收集一次系统范围的RF指标。

NETCONF始终优先于SNMP。

不能忽视对核心网络组件的持续监控，包括DHCP池利用率、核心路由器上的NAT条目数量等等。因为其中任何一种设备的故障都很容易导致无线中断。

大型网络特有的问题

如果您有一个使用Web身份验证的SSID，一个问题可能是客户端连接到该SSID并获得IP地址，但是由于最终用户没有主动尝试连接（自动连接的设备），因此从不进行身份验证。控制器必须拦截处于称为Web authentication pending的状态、且使用WLC资源的那些客户端发送的每个HTTP数据包。网络运行后，请定期监视给定时间处于Web身份验证挂起状态的客户端数量，以查看它如何与基线数量进行比较。处于IP Learn状态的客户端也是如此。当客户端执行DHCP过程时，您始终会看到处于该状态的客户端，但了解适合您的网络的正确工作编号有助于设置基线并确定此编号可能过高以及指示更大问题的时刻。

对于大型场所，看到约10%的客户端处于Web Auth Pending状态并不罕见。

第2天监控：关注用户满意度

网络启动并运行后，有两种典型的最终用户抱怨类型：无法连接或难以连接（断开连接），或者Wi-Fi的运行速度比预期慢。后者很难识别，因为它首先取决于对给定区域的速度和实时密度的期望。我们来了解一些有助于您日常监控大型公共场所网络的资源。

验证Wi-Fi吞吐量：测试和监控指南。本cisco.com文档介绍如何监控网络以发现吞吐量问题。它通过计算客户端在安静时能够在您的网络中合理期望的吞吐量，并估算随着客户端数量和负载的增加这些估计值会下降多少。这是评估最终用户对吞吐量的投诉是否合法的关键，也是评估您是否需要重新设计该区域以应对其潜在负载的关键。

当客户端报告连接问题后，请查看Catalyst 9800客户端连接问题故障排除流程，在此连接问题被隔离并用Catalyst Center进行澄清之后。

最后，作为一种通用的好的做法，请借助监控Catalyst 9800 KPI（关键绩效指标）来关注WLC的整体关键指标。

针对可扩展性进行配置

9800上的SVI和接口

避免在WLC上为客户端VLAN创建SVI。习惯于使用较旧AireOS WLC的管理员往往会反射以为每个客户端VLAN创建一个第3层接口，但很少需要这样做。接口会增加控制平面攻击媒介，而且可能需要更多ACL和更为复杂的条目。默认情况下，可以访问WLC的任何接口，需要做更多的工作来保护具有更多接口的WLC。它还会使路由变得复杂，因此最好避免它。

从IOS XE 17.9开始，mDNS监听或DHCP中继方案不再需要SVI接口。因此，在客户端VLAN中配置SVI接口的原因很少。

聚合探测响应

对于大型公共网络，建议修改接入点发送的默认汇聚探测间隔。默认情况下，AP每500毫秒更新一次WLC有关客户端发送的探测的信息。此信息用于负载均衡、频段选择、位置和802.11k功能。如果有多个客户端和接入点，建议修改更新间隔，以防止WLC中出现控制平面性能问题。建议的设置是每64秒有50个汇聚探测响应。此外，请确保您的AP未报告来自本地管理的MAC地址的探测功能，因为如果认为单个客户端可能在扫描时使用多个本地管理的MAC地址，从而避免故意跟踪，则没有跟踪点。

```
wireless probe limit 50 64000

no wireless probe localy-administered-mac
```

IPv6

许多网络管理员仍在拒绝IPv6。对于IPv6，只有两个可接受的选项：要么您支持它并且必须在任何位置部署足够的配置，要么您不这样做，并且必须阻止它。如果不关心IPV6，并且在一些没有正确配置的情况下将其保持启用状态是不可接受的。这会让整个IP世界成为您的网络安全所无法察觉的。

如果启用IPv6，则必须在2001：DB8：：/32范围内配置虚拟IPv6地址（这通常是忘记的步骤）。

请注意，尽管IPv6的基本操作在很大程度上依赖于组播，但如果您在WLC上禁用组播转发，它仍然可以运行。组播转发是指客户端组播数据转发，而不是向邻居发现、路由器请求和运行IPv6所需的其他协议转发。

如果您的Internet连接或Internet服务提供商提供IPv6地址，您可以决定为您的客户端允许IPv6。这与在基础设施中启用IPv6是不同的决策。您的AP可以只在IPv4中运行，但仍在其CAPWAP数据包中传输IPv6客户端数据流量。在基础设施上启用IPv6也需要考虑保护对AP、WLC和管理子网的客户端访问。

验证您的客户端网关的RA频率。WLC提供RA限制策略，限制转发到客户端的RA数量，因为这些客户端有时可能会出现频繁通信。

mDNS

一般来说，最好在大型场所部署中完全禁用mDNS。

mDNS桥接是指允许mDNS数据包作为第2层组播（因此发送到整个客户端子网）发送的概念。mDNS在家庭和小型办公室场景中很流行，在这些场景中，发现子网中的服务非常实用。但是，在大型网络中，这意味着将数据包发送到子网中的所有客户端，这在大型公共网络中从流量的角度来看是有问题的。另一方面，桥接不会对AP或WLC CPU造成任何开销，因为它被视为常规数据流量。mDNS代理或mDNS网关是指将WLC用作网络中所有服务的目录的概念。这样可以高效地跨第2层边界提供mDNS服务，同时减少整体流量。例如，使用mDNS网关时，打印机会通过具有相同子网第2层组播的mDNS发送其定期服务通告，但WLC不会将其转发到所有其他无线客户端。相反，它会记录提供的服务，并将其注册到其服务目录中。每当任何客户端请求特定类型的可用服务时，WLC都会代表打印机回复通知。这可以避免所有其他无线客户端听到不必要的请求和服务产品，并且只有当它们询问存在哪些服务时，才会收到回复。虽然它极大地提高了流量效率，但由于mDNS流量监听，确实会导致WLC（或AP，如果您在FlexConnect场景中依赖AP mDNS）的开销。如果使用mDNS网关，请密切关注CPU使用率至关重要。

将其桥接会导致大型子网中的组播风暴，而对其进行监听（使用mDNS网关功能）会导致大量CPU使用率。在全局以及每个WLAN上禁用它。

有些管理员启用mDNS是因为一些服务在特定位置需要它，但了解这会增加多少不需要的流量非常重要。Apple设备经常在不断寻找服务时也会自我广告，这会导致mDNS查询的背景噪音，即使没有人特别使用任何服务。如果您由于特定业务需求而需要允许mDNS，请全局启用它，然后仅在需要它的WLAN上启用它，并尝试限制允许mDNS的作用域。

强化网络

安全

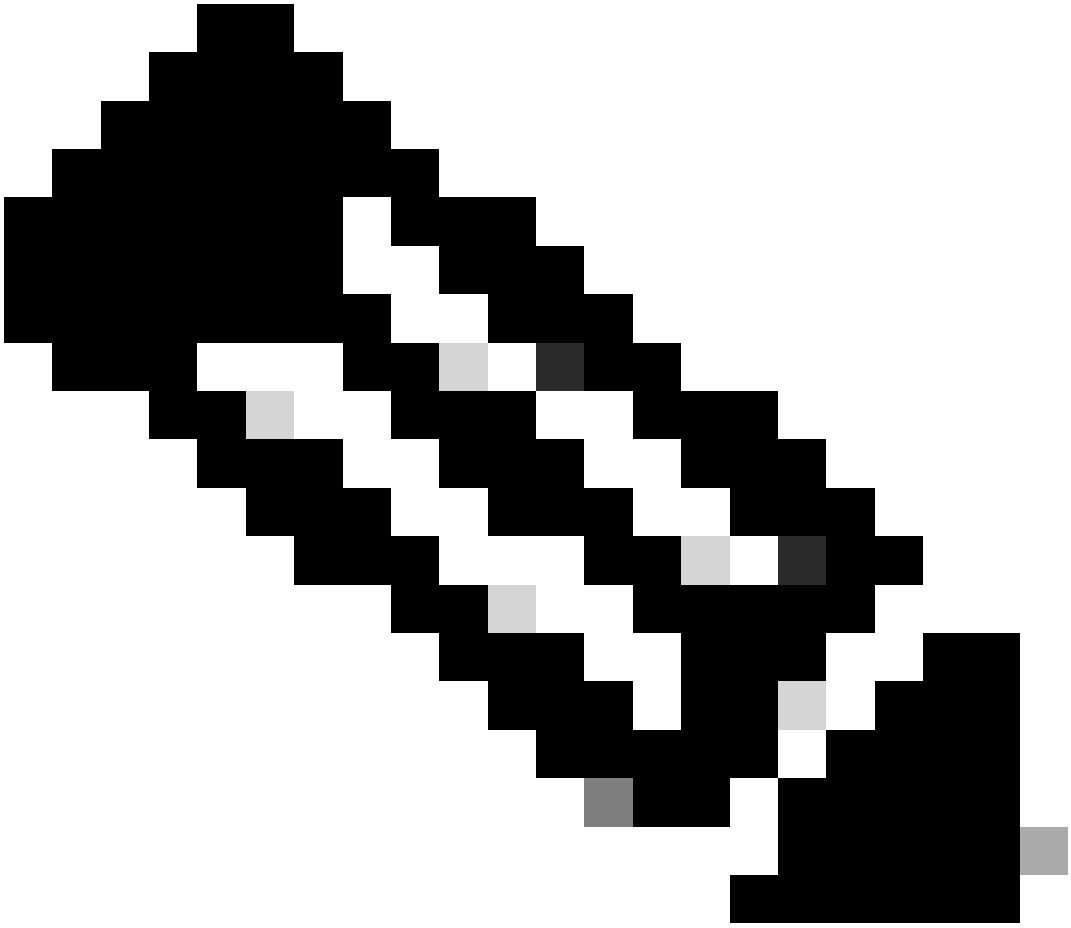
在大型公共网络中，许多事情都可能在管理员不知道的情况下发生。人们会随机要求电缆掉落，或在某个位置插入家庭级交换机，为恶作剧设置更多交换机端口……他们通常会先尝试这些操作，而不需要事先获得许可。这意味着，即使没有恶意行为者参与，安全也会被积极配合的客户和/或员工破坏。这样一来，恶意攻击实施者只需四处走动，查找电缆并查看他们从那里获得哪些网络访问权就变得非常容易。在所有交换机端口上配置802.1X身份验证是在大型网络中保持良好安全性的近乎必备要求。Catalyst Center可以帮助您自动执行此部署，并且可以为不支持802.1X身份验证的特定设备设置例外情况，但尽量少依赖基于MAC的身份验证，因为这样并不是真正的安全。

流氓接入点

你们打击流氓的战略取决于几个因素。许多管理员本能地追求非常严格的规则，但主要问题是：

- 当您收到数百个（如果不是数千个）恶意警报时，您是否拥有人力资源来查看所有这些警报并对它们采取行动？
- 您的目标是物理移除恶意程序以保持射频频谱清洁吗？如果是，您需要很多人来执行此操作。或者，您的目标可能只是关注安全因素，确保这些流氓不构成任何危险？这样的人力成本要可控得多。
- 启用恶意程序检测可能会影响您的通话时间，而恶意程序遏制通常会产生更大的影响，您是否已分析此影响并将其考虑在内？

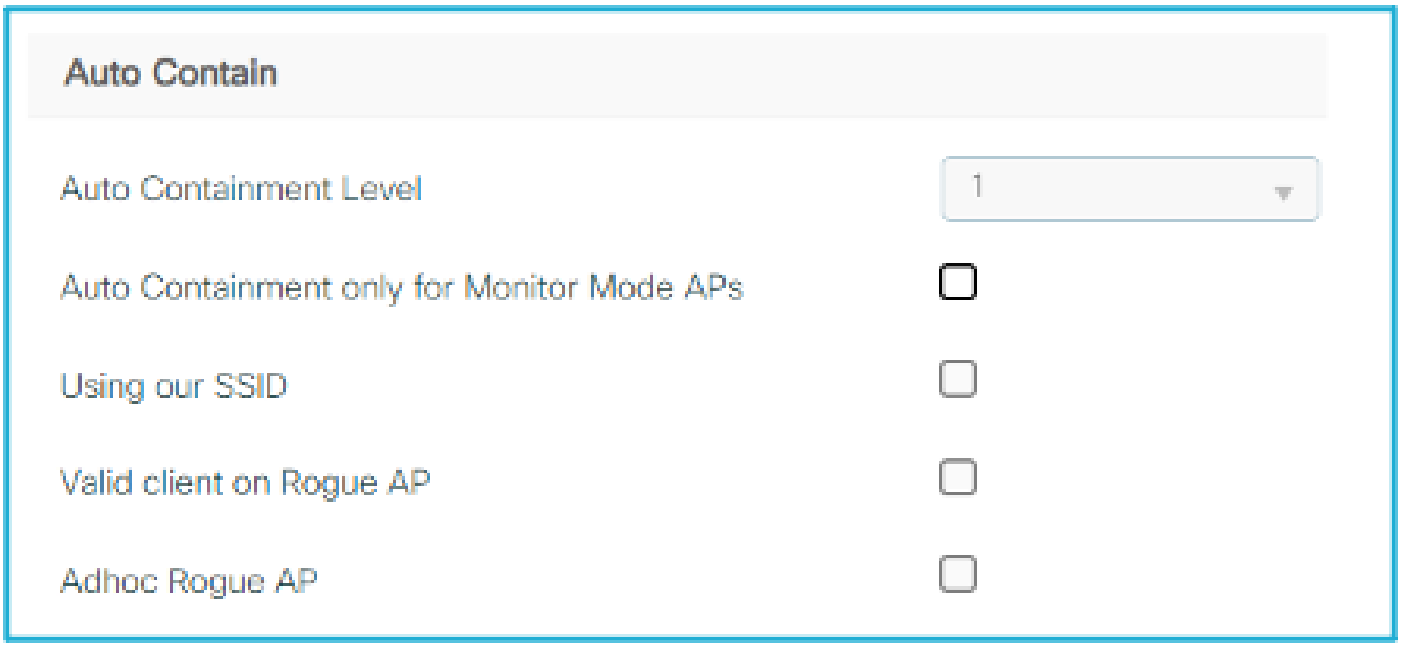
至于欺诈检测的影响，9120和9130具有专门的CleanAir芯片，负责信道外扫描（以及欺诈检测），使对客户端服务无线电的影响几乎为零。带有CleanAir Pro芯片的9160系列AP具有类似的无影响扫描功能，但没有CleanAir芯片的AP需要将客户端服务无线射频带离信道，以扫描恶意程序或执行遏制。因此，您使用的AP型号在决定是否使用专用监控模式AP进行欺诈检测和遏制时发挥了作用。



注意：共享Wi-Fi热点的移动电话在“基础设施”模式下运行与传统AP一样，“对等”模式是指移动设备之间的直接连接，不太常见。

非法遏制通常受到监管规则的禁止，因此，在启用它之前，您必须先向您的当地管理机构核实。遏制恶意程序并不意味着远程关闭恶意程序，而是使用解除身份验证帧对尝试连接到恶意接入点的客户端进行垃圾邮件发送，使其无法连接。由于您的接入点无法对取消身份验证帧正确签名，因此只能对旧版安全SSID执行此操作（在WPA3中或者在WPA2中启用PMF时，它不起作用）。遏制会对目标信道上的RF性能产生负面影响，因为AP会使用解除身份验证帧填充通话时间。因此，它只能被视为一种安全措施，以防止您自己的合法客户端错误地关联到恶意接入点。鉴于上述所有原因，建议不要进行任何遏制，因为它不能完全解决非法问题并导致更多射频问题。如果需要使用遏制，则仅对欺骗其中一个托管SSID的恶意程序启用该遏制才有意义，因为它是明显的蜜罐攻击。

您可以使用“使用我们的SSID”选项配置自动遏制：



自动包含设置

您还可以配置恶意规则，以便根据您自己的标准将其分类为恶意恶意恶意接入点。不要忘记将您的相邻和已批准的SSID的名称作为友好恶意程序输入，以从警报列表中删除这些SSID。

启用AP身份验证或PMF以保护AP免受模拟。

有线非法接入点是连接到有线网络的非法接入点，这显然会增加安全威胁。有线恶意程序的检测更为复杂，因为恶意程序的以太网MAC地址通常与其无线电MAC地址不同。Cisco Catalyst Center的算法仍会尝试检测是否有线欺诈，并搜索通过无线侦听并在有线基础设施上看到的欺诈客户端MAC。防止有线欺诈，最佳解决方案是使用802.1X身份验证保护您的所有交换机端口。

如果您要对恶意接入点进行物理操作，利用Cisco Spaces是获得恶意接入点准确位置的关键。您很可能仍然需要现场搜索一次，因为人们有时会隐藏恶意AP，但将搜索范围缩小到几米就非常可行了。如果没有空间，欺诈无线接入点将在地图上显示，检测到该无线接入点声音最大，搜索区域也相当大。许多无线工具和设备可以实时显示恶意接入点的信号，帮助您实际定位恶意接入点。

与恶意程序不完全相关，但由于CleanAir刚刚被覆盖，因此必须注意，启用CleanAir不会对性能产生明显的负面影响（BLE信标检测除外），因为这会影响2.4GHz性能。您可以将无线配置为完全忽略蓝牙干扰源，因为它们在当今世界上无处不在，并且您无法阻止客户端启用其蓝牙。

WiPS

WiPS涵盖更高级的攻击媒介，而不只是检测是否存在未经授权的非法设备。除了这些攻击，它还有时会提供事件的PCAP以供调查分析使用。

虽然这对企业来说是一个非常有用的安全功能，但面向公众的网络必须面对一个永恒的问题：如何应对它？

由于难以管理许多您无法控制的客户端，因此可以将警报分为两类。如果您发现来自Cisco Catalyst Center的警报过多，则可以决定忽略这些警报：

- 10001：DoS：身份验证泛洪警报
- 10002：DoS：关联请求警报
- 10003：DoS：广播探测功能泛洪警报
- 10004：DoS：取消关联泛洪警报
- 10005：DoS：广播解除关联警报
- 10006：DoS：取消身份验证泛洪警报
- 10007： DOS：广播取消身份验证警报
- 10008： DOS： EAPOL-Logoff Attack Alarm
- 10009：CTS泛洪警报
- 10010：RTS关联请求警报
- 10011：按对取消身份验证泛洪
- 10021：Airdrop会话（此会话通常在任何网络中经常发生，并且只描述Apple设备之间的常规对等活动）
- 10022：关联请求格式不正确
- 10023：按签名泛洪身份验证失败
- 10024：签名的MAC OUI无效
- 10025：身份验证格式不正确

这些警报可能由行为不当的客户端引起。无法自动阻止拒绝服务攻击，因为从本质上讲，您无法阻止有故障的客户端让通话时间保持忙碌。即使基础设施忽略客户端，它仍然能够使用介质和通话时间进行传输，因此会影响周围客户端的性能。

其他警报是如此具体，以至于它们最有可能描绘实际的恶意攻击，而且由于客户端驱动程序故障很难发生。最好持续监控以下警报：

- 10012：模糊信标
- 10013：模糊化探测请求
- 10014：模糊探测响应
- 10015：按签名的PS轮询泛洪
- 10016：EAPOL启动V1泛洪（按签名）
- 10017：按目标重新关联请求泛洪(Reassociation Request Flood by Destination)
- 10018：按签名划分的信标泛洪
- 10019：按目标划分的探测响应泛洪
- 10020：通过签名阻止Ack泛洪
- 10026/10027：RTS和CTS虚拟载波侦听攻击

无线基础设施有时可以采取缓解措施，例如阻止列出违规设备，但摆脱此类攻击的唯一实际行动就是以物理方式访问并删除违规设备。

建议启用所有形式的客户端排除，以节省与故障客户端交互所浪费的通话时间。

限制客户端访问

建议在所有WLAN上启用点对点阻止（除非您对客户端到客户端通信有硬性要求，但需要仔细考虑并可能加以限制）。此功能可防止同一WLAN上的客户端相互联系。这不是一个完美的解决方案，因为不同WLAN上的客户端仍能相互联系，并且属于移动组中不同WLC的客户端也可以绕过此限制。但是，它还是一个简单高效的第一层安全和优化。这种对等阻塞功能的另一个优点是还可以阻

止客户端到客户端ARP，阻止应用发现本地网络上的其他设备。如果不进行对等阻塞，在客户端上安装简单的应用程序可能会显示子网中连接的所有其他客户端，并显示它们的IP地址和主机名。

此外，建议在WLAN上同时应用IPv4和IPv6（如果在网络中使用IPv6） ACL以防止客户端之间的通信。无论您是否具有客户端SVI，应用阻止客户端与WLAN级别客户端通信的ACL都能发挥作用。

另一个强制步骤是防止无线客户端访问您的无线控制器的任何管理形式。

示例：

```
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可应用于管理接口SVI：

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

这在WLC上完成，WLC具有在第2层VLAN数据库中创建的客户端VLAN 131到137，但没有对应的SVI，并且VLAN 130仅存在一个SVI，即管理WLC的方式。此ACL可完全阻止所有无线客户端向

WLC管理和控制平面发送任何流量。不要忘记，SSH或Web UI管理不是您需要允许通过的唯一操作，因为还需要允许与所有AP之间的CAPWAP连接。这就是此ACL具有默认允许但阻止无线客户端范围的原因，而不是依靠默认deny all操作来指定所有允许的AP子网范围和管理范围。

同样，您可以创建指定所有可能管理子网的另一个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
```

然后，可以应用此ACL进行CLI访问：

```
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
```

同一ACL也可以应用于Web管理员访问。

防御流量风暴

组播和广播在某些应用中的使用率高于其他应用。当考虑纯有线网络时，防范广播风暴通常是唯一的防范措施。但是，当通过空中发送时，组播与广播一样痛苦，了解其原因非常重要。首先，假设一个数据包（无论通过广播还是组播）发送到您的所有无线客户端，该数据包可以快速累加到多个目的地。然后，每个AP都需要以尽可能最可靠的方式（虽然不能保证可靠）通过空中传输此帧，而这是通过使用强制数据速率（有时最低，有时可配置）实现的。通俗地说，这意味着帧是使用OFDM (802.11a/g)数据速率发送的，这显然不是很理想。

在大型公共网络中，不建议依靠组播来保持通话时间。但是，在大型企业网络中，您可能需要保持为特定应用启用组播，不过您必须尽可能控制组播以限制其影响。最好记录应用详情、组播IP并确保阻止其他形式的组播。如前所述，启用组播转发不是启用IPv6的必要条件。最好完全禁用广播转发。应用程序有时使用广播来发现同一子网中的其他设备，这在大型网络中显然是一个安全问题。

如果启用全局组播转发，请确保使用组播-组播AP CAPWAP设置。启用此功能后，当WLC收到来自有线基础设施的组播数据包时，它会将该数据包通过单个组播数据包发送到所有感兴趣的AP，从而节省大量的数据包复制工作。确保为每个WLC设置不同的CAPWAP组播IP，否则AP会从其他WLC接收不需要的组播流量。

如果AP位于WLC的无线管理接口（可能在大型网络中）的其他子网中，则必须在有线基础设施上启用组播路由。您可以使用以下命令验证所有AP是否正确接收组播流量：

```
show ap multicast mom
```

如果需要依靠组播，建议在所有情况下启用IGMP（用于IPv4组播）和MLD（用于IPv6）组播。它们仅允许感兴趣的无线客户端（因此仅允许具有感兴趣的客户端的AP）接收组播流量。WLC将注册代理到组播流量，并负责保持注册处于活动状态，从而卸载客户端。

结论

大型公共网络非常复杂，每个网络都有其独特的要求和结果。

遵守本文档中的指南是一个很好的起点，有助于在避免最常见问题的同时成功完成部署。但是，这些指南只是指南，可能需要在特定场所的上下文中进行解释或调整。

Cisco CX拥有一支专门从事大型无线部署的无线专业团队，在众多大型活动（包括体育赛事和会议）中拥有丰富的经验。请与您的客户团队联系以获取进一步帮助。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。