设计指南CX — 适用于大型公共网络的无线

目录

- 简介
  - CX设计指南
  - 范围和定义
  - 大型公共网络
  - 外部引用
  - 免责声明
- 设计网络
  - RF注意事项
    - 场所类型
    - 覆盖战略
    - 美学
    - 非法网络
    - 单5GHz与双5GHz
    - 天线
    - 高密度和6GHz
    - 无线电资源管理
  - RF配置
    - 通道
    - 数据传输速度
    - 传输功率
    - 功率平衡
    - RxSOP
  - 扩展网络
    - AP数量
    - WLC平台
    - WLC高可用性
    - 外部系统
    - DNS/DHCP
- 运行网络
  - 正确的配置
  - SSID
    - 多少个SSID?
    - WPA2/3个人
    - WPA2/3企业版
    - 访客SSID
    - 关于SSID数量的结论
    - 传统SSID与主要SSID的概念
    - SSID功能
  - 站点标签
  - 策略配置文件
  - AP 加入配置文件
  - 监控网络
    - 你监视得越严你越能造成你自己的问题

- 大型网络特有的问题
- 第2天监控：关注用户满意度
- 针对可扩展性配置
  - 9800上的SVI和接口
  - 聚合探测响应
  - IPv6
  - mDNS
- 强化网络
  - 安全
  - 流氓接入点
  - WiPS
  - 速率限制客户端
  - 限制客户端访问
  - 防御流量风暴

结论

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)的专家编写，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实践，以及多年来从无数客户实施中获得的知识和经验。按照本文档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，为数千台未知和/或非受管客户端设备提供网络连接。

本文档通常假设目标网络为大型和/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，购物中心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，或最多一天存在。

大型活动或场馆的无线覆盖有其自身的要求，往往不同于企业、制造甚至大型教育网络。大型公共网络可以容纳数千人，集中在一栋或几栋建筑中。它们可以经常或高峰期进行客户端漫游，而且网络必须尽可能兼容无线客户端设备方面的任何设备，而不控制客户端设备配置或安全。

本指南介绍了高密度的RF概念以及实施细节。本指南中的许多无线电概念适用于所有高密度网络，无论硬件平台如何。但是，实施详细信息和配置都侧重于使用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的解决方案。

本文档使用术语“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有其独特性，本文档对这些关键领域进行了探讨并提供相关指导。

- 大型公共网络非常密集；在减少的射频(RF)空间和大量漫游中，有成千上万台设备可供人们四处走动，某些活动和场所可能会更加静态，在特定时间出现带宽峰值。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。
- 轻松自注册是重中之重。关联的客户是快乐的客户。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，这会产生不需要的射频能量，进而导致额外拥塞和空中的容量损失。
- RF部署需要尽可能仔细设计。如果需要非常高的密度，或者场地有大的开放空间和/或高天花板，必须使用方向性天线进行适当的RF设计。
- 另一个关键设计驱动器是兼容性。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，两者都不会给客户端带来任何问题。但是，现实情况有所不同，许多编程不当的客户端驱动程序在面对复杂的信标或它们不了解的功能/设置时会出现不正常的情况。
- 由于规模和时间限制，故障排除非常困难。如果某些功能无法与特定客户端配合使用，则您无法与该最终用户配合来了解问题。用户可能很难找到，但也可能不合作，因为他们访问场所的短暂性。
- 安全是一个重要因素。由于访客数量非常多，并且攻击面更大，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	链路
排除无线局域网控制器CPU故障	思科	链路

文档名称	来源	位置
验证Wi-Fi吞吐量：测试和监控指南	思科	链路
Cisco Catalyst CW9166D1接入点部署指南	思科	链路
Cisco 9179F部署指南	思科	链路
Catalyst 9104体育场天线(C-ANT9104)部署指南	思科	链路
监控Catalyst 9800 KPI（关键绩效指标）	思科	链路
Catalyst 9800客户端连接问题故障排除流程	思科	链路
Cisco Catalyst 9800系列无线控制器软件配置指南	思科	链路
Wi-Fi 6E:Wi-Fi白皮书中的下一个重要章节	思科	链路

免责声明

本文档根据特定场景、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、隐私性和其他要求，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问者提供互联网接入，虽然这很少是唯一的使用案例。

典型位置：

- 体育场馆
- 会议地点
- 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都是永久性的安装，除了会议/音乐会场所，因为这些场所可以是永久性的，也可以临时为特定展览而设置。

其它位置：

- 游轮
- 机场
- 购物中心/购物中心

机场和游轮也是适合大型公共网络类别的部署示例；但是，这些设备具有特定于每种情况的额外注意事项，并且通常使用内部全向AP。

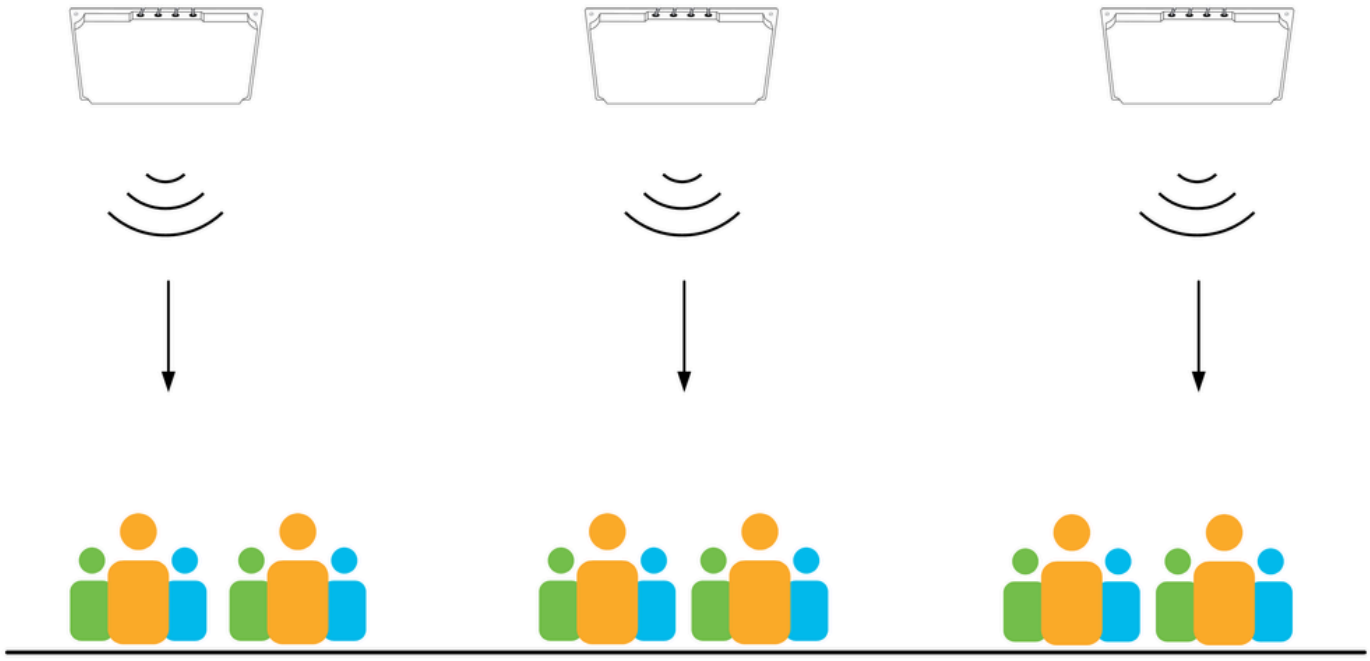
覆盖战略

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

尽可能优先使用开销覆盖。

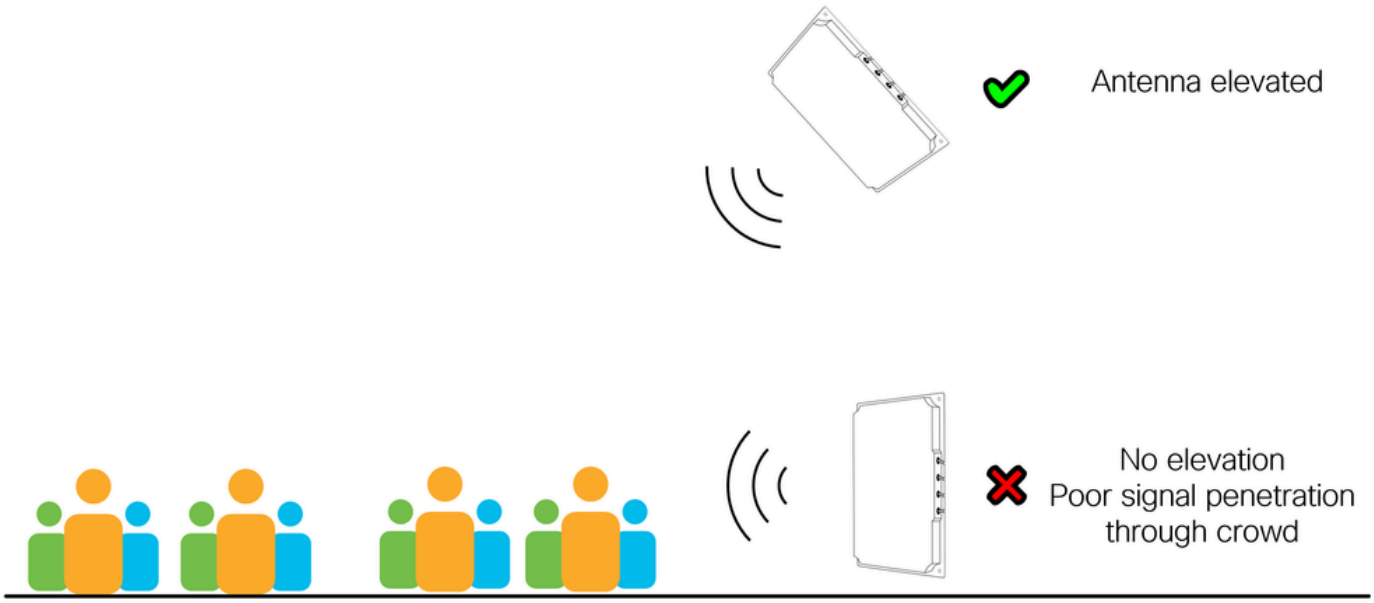
架空解决方案的明显优势是，即使是在拥挤的情况下，所有客户端设备通常都能够直接到达天线架空。使用定向天线的开销解决方案可提供更加受控和定义明确的覆盖区域，从无线电调谐的角度而言，使覆盖区域更加简单，同时提供卓越的负载均衡和客户端漫游特性。有关其他信息，请参阅功率平衡部分。



客户端上方的AP

侧面

侧装式定向天线是常用的选择，在各种情况下都能良好工作，尤其是当由于高度或安装限制而无法进行架空安装时。当使用侧部安装时，了解天线所覆盖的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，则天线必须尽可能地高级，因为信号在人群中的传播总是很差。请记住，大多数移动设备用于腰部下部，而不是用户头顶上方！当覆盖区域为较低密度区域时，天线的高度不太重要。



天线高度总是更好

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。全向天线不得使用在6米以上的高度（不适用于高增益室外设备）。

坐下式

在某些体育场馆或体育场馆中，可能存在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置于用户坐下的座位下来提供覆盖范围。此类解决方案更难以正确部署，并且通常成本更高，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之间的覆盖范围存在巨大差异。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人群时，与没有人群的人相比，产生的覆盖范围明显更小。此人为人群衰减系数允许部署更多无线接入点，从而提高整体容量。然而，当场地空置时，人体没有衰减，并且受到显着干扰，这会导致场地部分空置时的复杂。



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/或品牌规定可以安装设备（或不能安装）的空间。可能需要特定的解决方案来应对任何放置限制。其中一些解决方法包括隐藏AP/天线、覆盖AP/天线、将设备安装在外壳中，或仅使用不同的位置。但涂漆天线会使保修失效。思科一般不销售天线外壳，但许多产品很容易通过不同的提供商获得，这些提供商也销售各种盖板以及使接入点符合各种美观的方法。

所有此类变通方案都会对网络性能产生影响。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，而这些初始位置通常可提供最佳性能。对这些位置的任何更改通常会导致天线远离其最佳位置。

天线安装位置通常为高架部分，可以是天花板、猫道、屋顶结构、横梁、走道以及在预期覆盖区域提供一定高度的任何位置。这些位置通常与其他安装共享，例如：音频设备、空调、照明、摄像头和各种探测器/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盒子中或墙壁后面时无法正常工作。

无线天线也是如此，当无线客户端设备有视线时，它们的工作效果最佳。优先考虑美观可能会对无

线性能产生负面影响，从而降低基础设施投资的价值（这种情况经常发生）。

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，在某些情况下也是安全风险。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设备之间共享相对较小的无线电频段，邻近的任何行为不检的设备都有可能干扰许多用户的网络性能。

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，通常使用具有调谐发送和接收特性的定向天线，以实现最高效率。

频谱的另一端是消费级设备或互联网服务提供商提供的设备。它们要么具有有限的精细RF调整选项，要么配置为实现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混乱。

我们能做些什么呢？

就个人热点而言，能做的事情很少，因为要监控数万人进入一个场所几乎是不可能的。对于基础设施或半永久性设备，有一些选择。可能的补救措施从简单的教育、用于宣传的标牌开始，通过已签名的无线电策略文档，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做出业务决策，同时采取具体步骤执行业务决策。

当受第三方控制的设备通告与受管网络相同SSID时，流氓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。始终建议创建欺诈规则，以针对检测非托管设备通告的基础设施SSID发出警报。安全部分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（例如，全向AP上的微/宏信元）之间存在一个关键差异。 在外置天线的情况下，双5GHz通常是一种有用的机制，可在减少总AP数量的同时提供额外的覆盖范围和容量。

微型/宏型/中型

内部AP的两根天线都紧密相连（在AP内部），在使用双5GHz时，受与最大Tx功率相关的限制约束。第二个无线电被限制为低Tx功率（这由无线控制器实施）导致无线电之间的发射功率严重失衡。这会导致主（更高功率）无线电吸引许多客户端，而辅助（较低功率）无线电利用不足。在这种情况下，第二个无线电设备会为环境增加能量，而不会为客户端带来好处。如果观察到这种情况，最

好禁用第二个无线电，在需要额外容量时只需添加另一个（单个5GHz）AP。

不同的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AP（如9130和9136）中以较高的功率水平运行，一些内部Wi-Fi 6E AP（如9160系列）甚至可以在宏/宏中运行。请始终验证确切的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，这会影响信道规划以及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，所有情况都是如此，包括带内置天线的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monitor模式（适用于支持它的AP），来提高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。建议不要在大型公共网络中使用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，但一旦您对转换结果满意，建议冻结FRA。

监管

每个管制范围定义了可供使用的信道及其最大功率水平，对室内和室外可使用哪些信道也有限制。根据管制范围，有时无法有效利用双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。在本示例中，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。

有时，在更高软件版本中会向某些管制域添加额外的信道，但是这些信道也有可能具有不同的最大传输功率：验证您的客户端是否支持这些信道，并且仅在传输功率不会出现问题的AP上使用它们。如果您想使用所有可用信道，最好创建RF配置文件，其中需要最高发射功率的AP（例如安装在非常高的天花板上的AP）仅使用功率较高的信道，并且保留功率较低的信道到在密集区域靠近地面的AP。

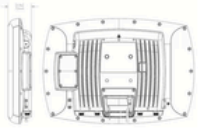
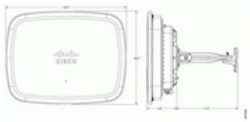
天线

大型公共网络可以使用任何类型的天线，并且通常部署最适合工作的天线。在同一覆盖区域内混合天线使无线电设计过程更具挑战性，如果可能必须加以避免。但是，大型公共网络通常覆盖范围较大，即使在同一区域内，安装选项也有所不同，因此在某些情况下，需要混合天线。

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)

下表列出了最常用的集成定向天线：

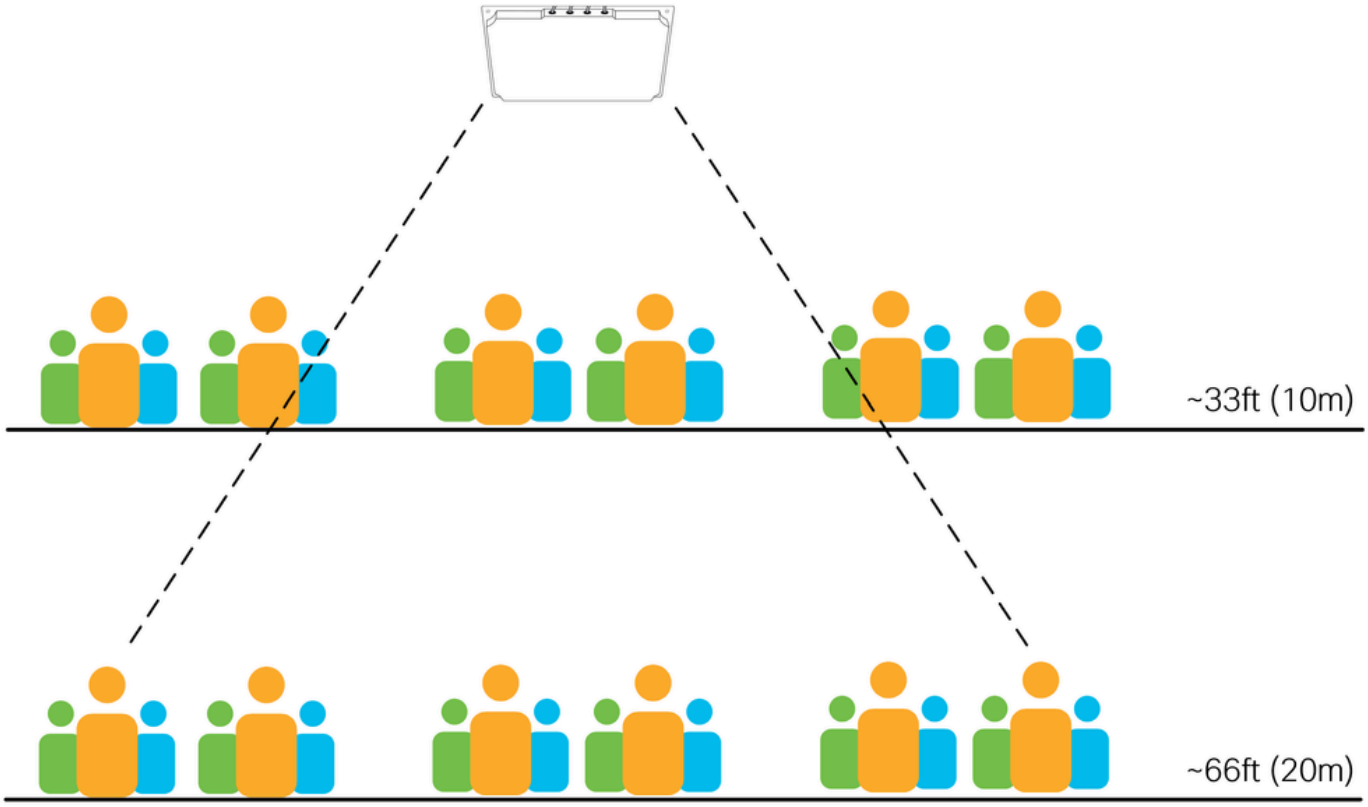
	CW9179F Integrated directional ~100ft (30m) *See data sheet for gain info.*	5GHz Narrow 35°x 35° Wide *See data sheet*	6GHz Narrow 35°x 35° Wide 70° x 35°
	C-ANT9104 Integrated directional ~66ft (20m)	5GHz Narrow 25°x 25° : 10dBi Wide 80°x 25° : 7dBi	
	CW9166D1 Integrated directional ~33ft (10m) *See data sheets for XOR info.*	6GHz 60°x 60° 8 dBi	5GHz 70°x 70° 6 dBi
	CW9176D1 Integrated directional ~33ft (10m) *See data sheets for XOR info.*	6GHz 70°x 70° 8 dBi	5GHz 70°x 70° 8 dBi

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时的距离/高度。下表显示常用天线的波束宽度，括号中的数字显示圆角（更易于记忆）值。

表中建议的距离不是硬性规则，而只是基于经验的指南。无线电波以光速传播，到达任意距离后不会简单地停止。这些天线的工作距离都超过了建议的距离，但是随着距离的增加，性能会下降。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）处的两个可能的安装高度。请注意，天线可以看到(并接受来自的)的客户端数量会随着距离增加而增加。随着距离变长，维持更小蜂窝尺寸变得更具挑战性。

一般规则是用户密度越高，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

CW9179F非常适合用于覆盖高距离的高密度区域，有关信息，请参阅Cisco Wireless 9179F接入点部署指南。

随时间推移发生的变化

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，移动内墙或改造场所座位）。 经常现场视察和目视检查一向是推荐的做法。对于事件网络来说，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，随着时间推移，这些系统升级后，可能会被重新定位到阻碍和/或主动干扰无线系统的位置。必须跟踪其他安装，并与安装这些系统的团队进行沟通，以确保所有系统都安装在合适的位置，互不干扰（物理或电磁干扰）。

高密度和6GHz

更清洁且拥塞更少的6GHz频段提供比5GHz更出色的体验，同时由于更多的客户端设备采用6GHz，具有减少5GHz通话时间的额外优势。现代网络应同时适用于5GHz和6GHz覆盖范围，包括大型公共网络。
思科产品组合包括几个支持6 GHz的设备，可用于高密度部署；9179F用于覆盖范围更广和焦点更集中，91x6D1型号用于覆盖范围更广的更短距离 — 这些产品的组合使您可以在各种位置选择充分的6GHz设计选项。

设计6GHz覆盖范围的方法通常与5GHz相同。关于选择数据速率、信道宽度和Rx-Sop值的准则保持不变，尽管必须对6GHz所需的安全配置以及信道规划和主扫描(PSC)信道的使用给予一些额外的考虑。

在大型公共网络中，这些网络通常具有各种大型区域，并且需要组合使用各种高度的天线。由于距离模拟问题，仅使用60°x60°天线部署大型公共网络端到端可能颇具挑战性。因此，对于大型公共网络而言，仅使用CW9166D1提供6GHz的端到端覆盖也极具挑战性。

一种可能的方法是使用5GHz作为主覆盖频段，同时仅在特定区域使用6GHz将支持客户端设备卸载到更干净的6GHz频段。此类方法在大区域内使用5GHz专用天线，同时尽可能在需要额外容量的情况下使用6GHz天线。

本文档稍后将讨论5GHz和6GHz频段之间的客户端漫游。

监管

与5GHz一样，6GHz的可用功率和信道在管制范围之间有很大差异。值得注意的是，FCC和ETSI域之间的可用频谱有很大差异，以及针对室内和室外可用发射功率、低功率室内(LPI)和标准功率(SP)的严格规定。对于6GHz，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部署自动频率协调(AFC)的要求。

有关Wi-Fi 6E的详细信息，请参阅Wi-Fi 6E:Wi-Fi白皮书的下一个重要章节。

无线电资源管理

无线电资源管理(RRM)是一组算法，负责控制无线电操作。本指南参考两个关键的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（默认时间为10分钟）。
- TPC自动运行（默认时间为10分钟）。

Cisco Event Driven RRM(ED-RRM)是一个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RF条件。当检测到过多的干扰水平时，ED-RRM可以立即更改信道。在噪声和/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。

建议使用RRM，并且通常优先于静态配置，但存在某些警告和例外。

- 必须根据需要使用TPC最小/最大设置将TPC限制到适当的值范围，并始终与RF设计保持一致。
    - 在高密度环境中启用TPC Channel Aware。

- DCA周期必须从默认设置10分钟更改。
  - 请勿在繁忙、嘈杂和高密度环境中使用ED-RRM。
  - 禁用Avoid Cisco AP Load。
  - 如果存在许多欺诈，诸如避免外部AP干扰之类的欺诈AP规避选项可能会导致环境不稳定。删除欺诈总是比尝试响应更好。
- RRM决策可能受到不能正确侦听的AP/天线的影响，例如定向天线相互背对的情况。
- 某些天线（例如C9104）不支持RRM，始终需要静态配置。
- RRM不能修复不良的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边界内运行。本文档的后续部分将更加详细地探讨这些要点。

RF配置

通道

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比可用信道多几个数量级，这意味着更大的信道重复使用率，以及更高的同信道干扰。必须使用所有可用信道，并且一般不建议限制可用信道列表。

在某些情况下，特定（和独立的）无线系统需要共存于同一物理空间中，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，在邻近主网络的开放区域中运行的点对点链路，或者体育场内的按压区域。如果从DCA列表中排除超过一个或两个信道，则会导致重新评估建议的解决方案。在某些情况下，例如密度极高的体育场馆，甚至连一条通道都不行，有时候也不是可行的选择。

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，这可能会导致不稳定射频环境中的频段更改。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，锚定时间8。这样，从上午8点开始，信道更改将限制为每4小时一次。

由于干扰势必发生，因此对每个DCA循环进行适应不一定能带来价值，因为许多干扰是暂时的。一个好的技术是在最初几个小时使用自动DCA，并在您有满意的稳定对象时冻结算法和通道计划。

当WLC重新启动时，DCA在主动模式下运行100分钟，以查找适当的信道计划。在对RF设计进行重大更改（例如添加或删除多个AP或更改通道宽度）时，最好手动重新启动该流程。 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，而且除Wi-Fi外，还有许多其他技术使用它，这会产生不需要的干扰。一些组织坚持要提供这方面的服务，那么合理的结论是什么？事实上，2.4GHz频段无法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，许多人在拨打电话或智能可穿戴设备时仍期望无线耳机能够正常工作。如果您的密集型Wi-Fi以2.4GHz运行，您将会影响那些甚至不使用您的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”）。 这意味着双频设备不会非自愿连接到2.4GHz，只有单频2.4GHz设备连接到该设备。

思科不建议或支持在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。

通道数量因管制范围而异。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,强烈建议使用20MHz信道宽度。

40MHz可以和2.4GHz一样使用，即仅在绝对需要时（和位置）。

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进，如果不可能有更高的SNR，那么40MHz信道就无用武之地。高密度网络将所有用户的平均吞吐量优先于任何单个用户的潜在较高吞吐量。在20MHz信道上放置更多无线接入点比使用40MHz作为辅助信道的AP只用于数据帧，因此其使用效率比使用两个不同的无线信元要低得多，每个无线信元以20MHz的速度运行（就总容量而言，而不是单个客户端吞吐量）。

最关键的细节是保持给定区域内相同的通道宽度。实际上，如果配置不同的信道宽度，客户端会倾向于粘接到信道宽度最大的AP，即使有另一个AP更接近更强的信号强度。

6GHz

6GHz频段尚未在所有国家/地区可用。此外，有些设备具有支持6GHz的Wi-Fi适配器，但需要BIOS更新才能为特定国家/地区启用。客户端现在发现6GHz无线电最常用的方式是通过减少邻居报告(RNR)通告，这会向使用其他AP无线电的客户端通告6GHz网络的存在。这意味着6GHz不能在没有同一AP上的其他无线电的情况下单独运行。

当配置双频SSID（5GHz和6GHz）时，5GHz通告将包含6GHz SSID的RNR，使客户端可以快速查找6GHz SSID，而无需扫描频段。

另一种方法是在2.4GHz上配置一个虚构（和/或隐藏）SSID，这里的目的是使用2.4GHz无线电通告6GHz RNR，而不提供2.4GHz SSID。此方法适用于需要添加6GHz容量而不向环境中添加5GHz无线电的情况。

6GHz允许使用更大的信道带宽，但这在很大程度上取决于监管域中可用的信道数量。由于欧洲有24个6GHz信道，考虑40MHz信道以提供比5GHz时可能使用的20MHz更好的最大吞吐量并非不合理。在美国，信道数量几乎是美国的两倍，使用40MHz是理所当然之事，甚至使用80MHz也不无道理。在高密度活动或场所中不得使用更大的带宽。

6GHz信道宽度较大的警告是，在5GHz中并非总是可以使用相同的信道宽度，这将影响某些客户端设备的漫游行为。最关键的细节是保持给定区域内相同的通道宽度。实际上，如果配置不同的信道宽度，客户端会倾向于粘接到信道宽度最大的AP，即使有另一个信号强度更强的AP更接近，这也适用于5GHz和6GHz频段之间的漫游。

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，反之，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必须都支持一个速率才能使用。

支持 — AP使用速率

强制 — AP使用速率，并使用此速率发送管理流量

已禁用 — AP不使用速率，强制客户端使用其他速率

注意：强制利率也称为基本利率

强制速率的意义在于使用此速率发送所有管理帧以及广播和组播帧。如果配置了多个强制速率，则管理帧使用配置的最低强制速率，广播和组播使用其中一个强制速率（此点在RF配置文件中可配置）。

管理帧包括客户端必须侦听才能与AP关联的信标。增加强制速率也会增加该传输的SNR要求，请回想一下，较高的数据速率需要更高的SNR，这通常意味着客户端需要更接近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，我们还可以操纵AP的有效关联范围，迫使客户端更接近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填项，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密度场景中很有用，但在较高密度场景中漫游可能会造成混乱。任何试图定位以6Mbps速度广播的恶意AP的人都知道，您可以在远离其物理位置的地方检测到AP!

在广播和组播主题上，在某些情况下，配置第二个（较高）强制速率以提高组播流量的交付速率。这很少会成功，因为组播不会得到确认，也不会在帧丢失时重新传输。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，不可避免地会丢失某些组播帧。实现可靠组播传输的更好方法是将组播作为单播流进行传输的组播到单播转换技术，这具有更高的数据速率和可靠（确认）传输的优势。

首选仅使用单个强制费率，禁用低于强制费率的所有费率，并将高于强制费率的所有费率保留为支持。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和AP之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；低密度部署使用12Mbps的强制性速率，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测试。

注意：最好使所有802.11n/ac/ax/be速率保持启用状态（WLC GUI的“高吞吐量”部分中的所有速率），很少需要禁用任何这些速率。

传输功率

发射功率建议因部署类型而异。此处我们区分了使用全向天线的室内部署和使用定向天线的室内部

署。这两种类型的天线都可以在大型公共网络中存在，尽管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)和静态配置的最小阈值，在某些情况下，也使用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。始终确保为所使用的天线型号正确配置了天线增益，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。

一个好方法是创建具有不同阈值的多个射频配置文件，例如低功率(2-5dBm)、中等功率(5-11dbM)和高功率(11-17dBM)，然后根据需要为每个射频配置文件分配全向AP。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相似，唯一的区别是所需的精度水平。在部署前RF勘测期间，必须设计和验证定向天线的放置，此过程通常会导致特定的无线电配置值。

例如，如果需要天花板安装贴片天线覆盖约26英尺（8米）高的特定区域，RF调查必须确定达到此预期覆盖范围所需的最小Tx功率（这确定RF配置文件的最小TPC值）。 同样，通过同一次RF调查，我们可以了解此天线与下一天线之间可能需要的重叠，甚至可以了解我们希望覆盖结束的位置 — 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TPC值和最大TPC值，或配置范围较窄的可能值（通常小于3dBm）。

首选射频配置文件以确保配置一致性，建议不要对单个AP进行静态配置。根据覆盖区域、天线类型和使用案例（例如RF-Auditorium-Patch-Ceiling）命名RF配置文件是比较好的做法。

正确的发射功率大小是预期覆盖区域中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）的良好客户端SNR目标值。

CHD

覆盖盲区检测(CHD)是识别和修复覆盖盲区的独立算法。CHD是全局配置的，也是根据WLAN配置的。CHD的可能影响是发射功率增加以补偿覆盖盲区（客户端始终检测到信号较差的区域），此影响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。

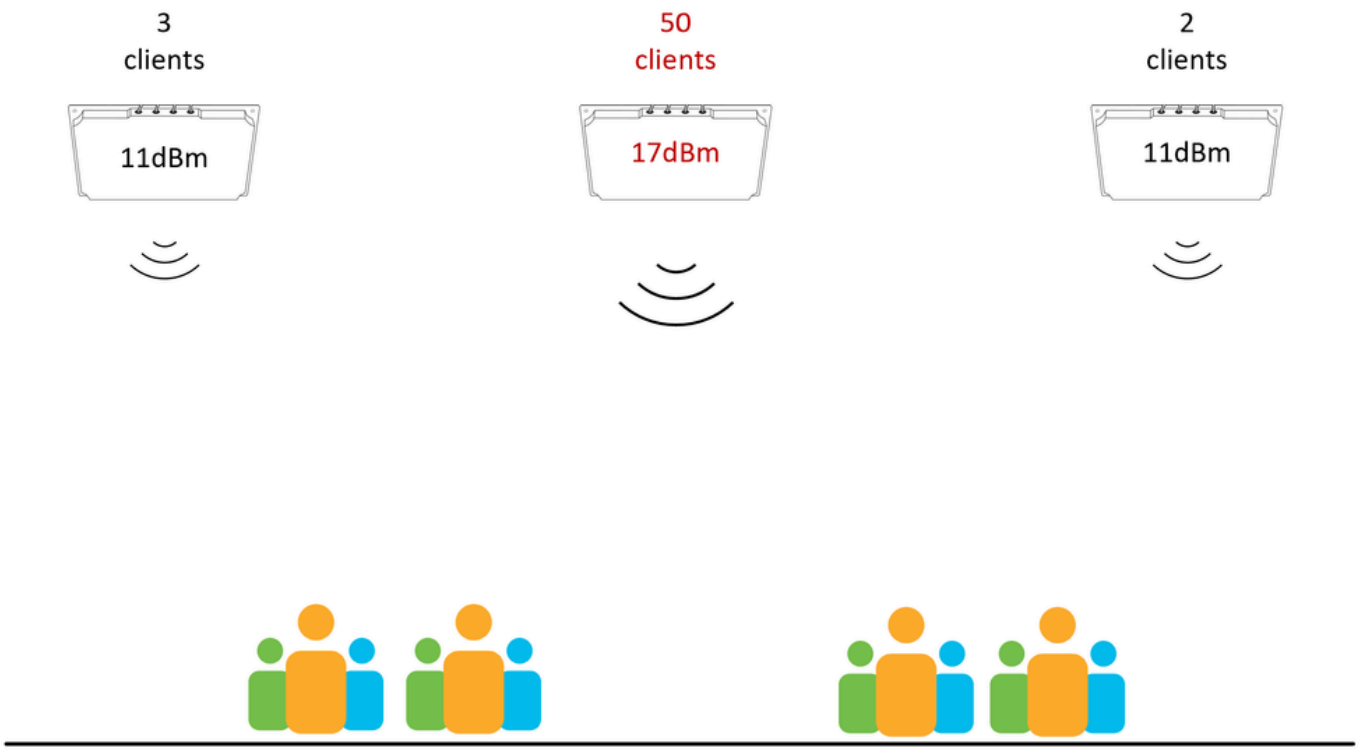
对于大型公共网络，必须全局禁用CHD。

功率平衡

大多数客户端设备在选择要与哪个AP关联时都首选较高的接收信号。必须避免为AP配置的发射功率远高于周围其他AP的情况。以更高发射功率运行的AP会吸引更多客户端，导致AP之间的客户端分布不均（例如，单个AP/无线电客户端过载，而周围的AP未得到充分利用）。 这种情况常见于多天线覆盖范围较大的部署，以及一个AP连接多个天线的情况。

当选择Tx功率时，体育场天线（例如C9104）需要特别小心，因为天线波束在设计上重叠，有关详情，请参阅相关天线部署指南。

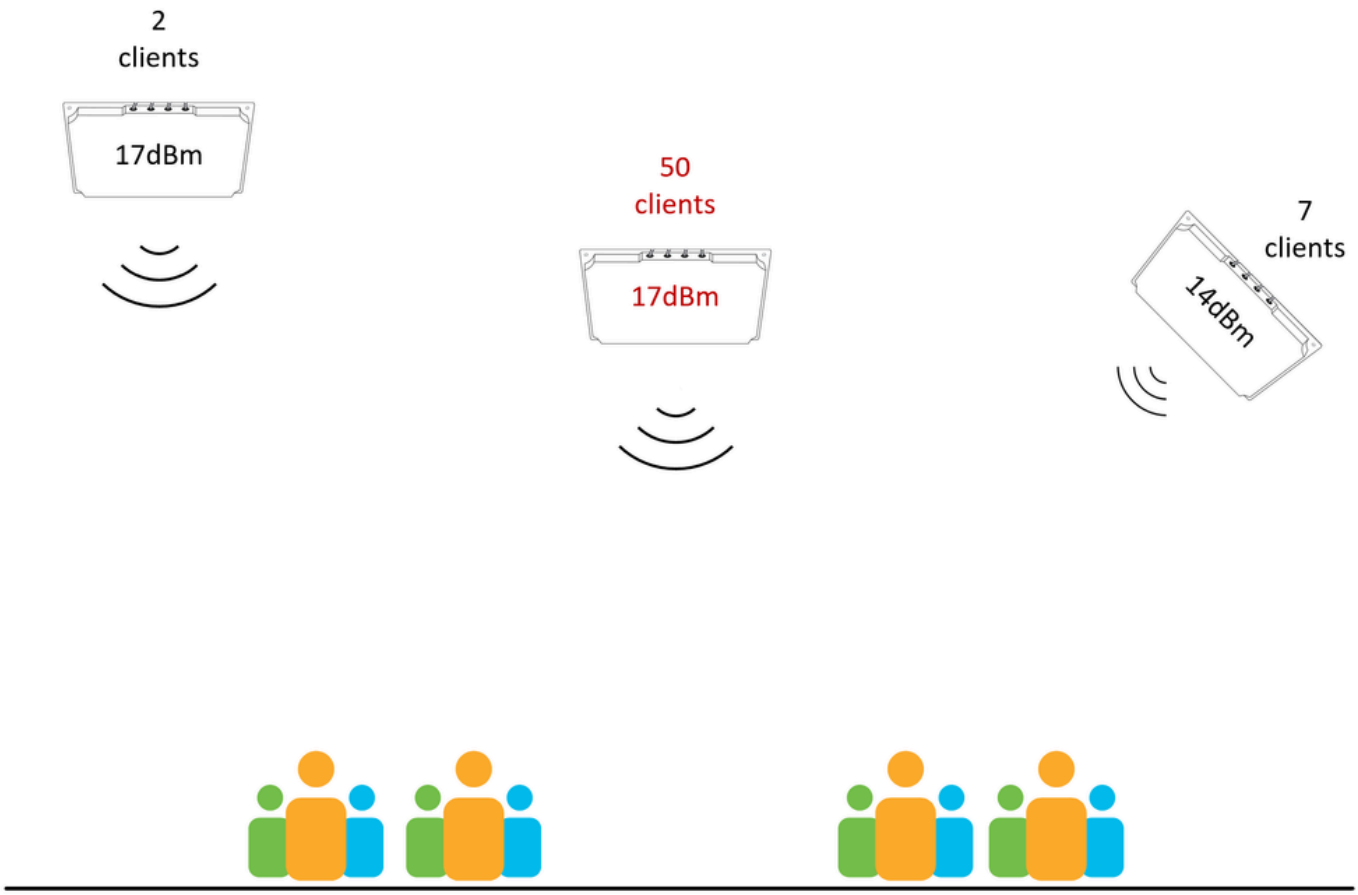
在下图中，中间天线配置的发射功率高于周围天线。此配置可能会导致客户端“粘滞”到中间天线。



功率高于其邻居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的高度，并且并非所有天线都使用相同的倾斜/方向。与简单地为所有无线电设备配置相同的Tx功率相比，实现功率平衡更为复杂。在诸如此类的场景中，可能需要部署后现场勘测，这样可以从客户端设备的角度（在地面上）查看覆盖范围。 调查数据可用于平衡配置，以实现最佳覆盖范围和客户端分布。

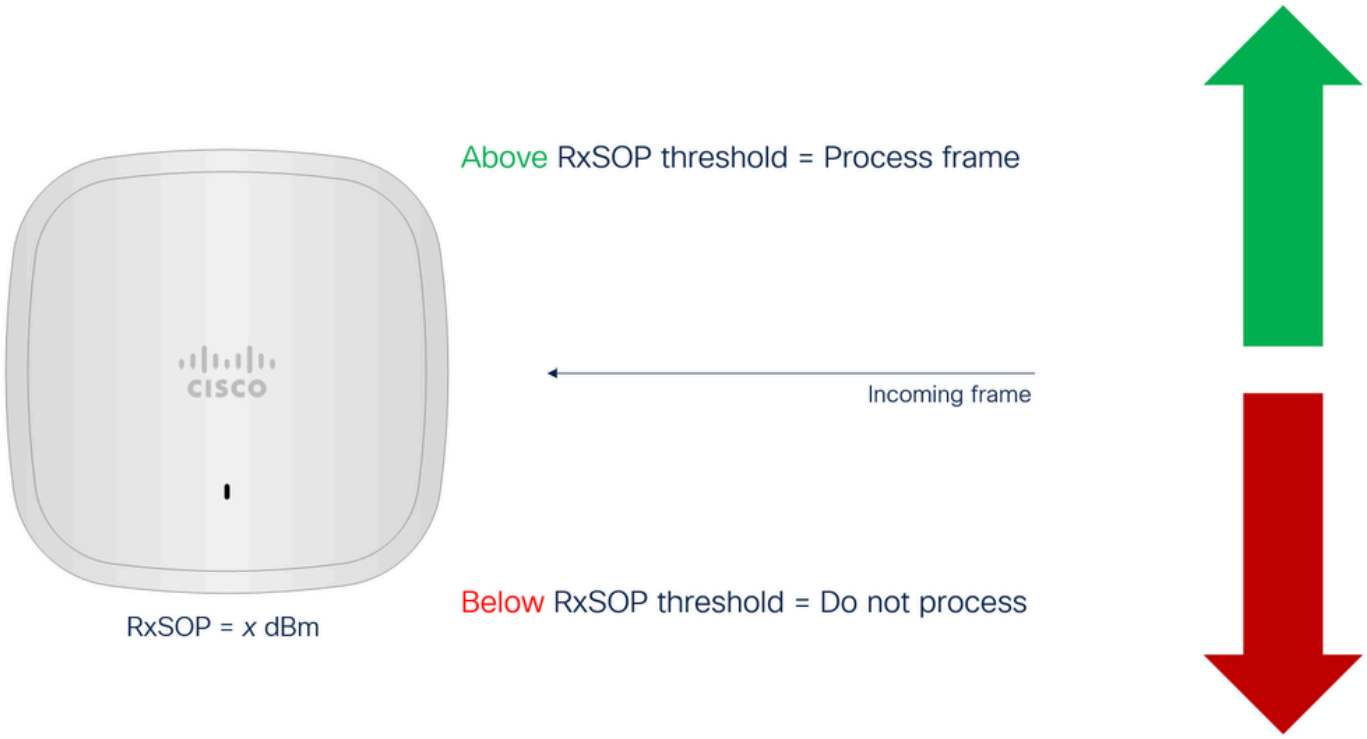
设计统一AP放置位置来避免类似复杂情况是防止挑战性RF调整场景的最佳方法（虽然有时没有其他选择！）。



尽管发射功率相似，但一个AP正在吸引所有客户端，但高度和角度在其中起着作用

RxSOP

与发射功率或数据速率等影响发射信元特性的机制不同，RxSOP（接收方数据包起始检测）旨在影响接收信元的大小。本质上，RxSOP可以视为噪声阈值，因为它定义了接收信号电平，AP在该电平以下不会尝试解码传输。到达时信号电平低于配置的RxSOP阈值的所有传输均不会由AP处理，而是被有效视为噪声。



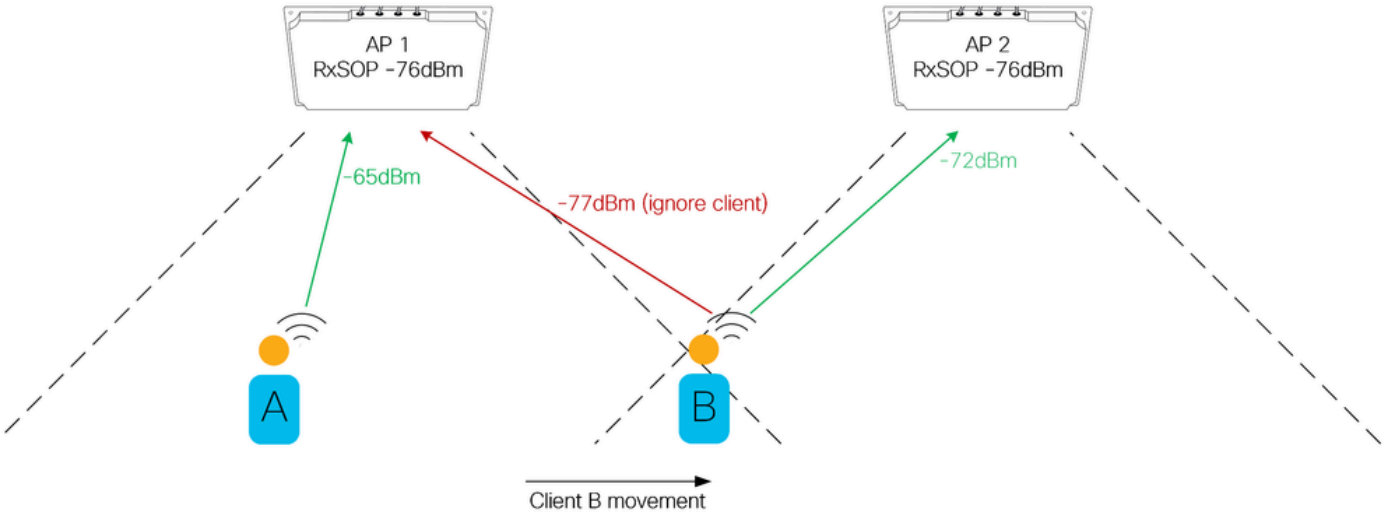
RxSOP概念说明

RxSOP的意义

RxSOP具有多种用途。它可用于提高AP在噪声环境中传输的能力，控制客户端在天线之间的分配，以及针对较弱和粘滞客户端进行优化。

在有噪声的环境中，请记住，在传输802.11帧之前，传输站（本例中为AP）首先需要评估介质的可用性，此过程的一部分是首先侦听已发生的传输。在密集Wi-Fi环境中，许多AP通常在相对有限的空间中共存，通常使用相同的信道。在如此繁忙的环境中，AP可以报告周围的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可以忽略那些较弱的传输（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报告显着通道利用率(例如>10%)而没有任何客户端负载(例如，空场)的环境是RxSOP调整的良好候选者。

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

在本示例中，有两个具有明确覆盖区域的AP/天线。客户端B正在从AP1的覆盖区域进入AP2的覆盖区域。AP2比AP1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阈值如何强制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。

过度设置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。这会对客户端产生负面影响，因为AP不响应；毕竟，如果没有听到客户端传输信息，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排除覆盖区域内的有效客户端。请注意，某些客户端可能无法很好地响应被忽略的情况，过于激进的RxSOP设置不会给客户端一个自然漫游的机会，从而有效地迫使客户端查找另一个AP。可以解码来自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直接到达AP，信号通常因用户背对天线或将其设备放在袋子或口袋中而衰减。

配置RxSOP

根据RF配置文件配置RxSOP。

每个频段都有预置阈值（低/中/高），该值为预定义的dBm值。每个频段的这些预设值不同（例如，“低”在2.4GHz和5GHz之间的dBm中有不同的值）此处的建议是始终使用自定义值，即使预期值是可用的预设值之一，这也使配置更易读。“Auto”设置有效禁用RxSOP，因为AP会尝试像往常一样解码任何数据包。

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，可以动态完成。

扩展网络

一般而言，最大限度地利用设备已编档的功能是不明智的。数据表报告了真实情况，但提及的数字可能处于特定的活动状态。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，以及一定的吞吐量，但这并不假设客户端每秒都在漫游、您可以为每个客户端配置超长的唯一ACL或者启用所有可用的监听功能。因此，必须认真考虑所有方面，以确保网络在高峰时段能够扩展，并为未来发展保持安全裕度。

AP数量

部署任何网络的首要任务之一是编制预算和订购正确的设备数量，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（很不幸），这通常是项目生命周期的第二步。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，以合理程度的确定性预测可能需要多少个AP。预测模型在这种情况下也非常有用。

对于更具挑战性的安装（例如工业、户外、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。之前类似的安装需要一定程度的经验，才能充分估计所需设备的类型和数量。无线架构师进行现场探访是了解复杂场所或设施布局的最低要求。

本节提供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

这里没有捷径。天线类型取决于需要覆盖的区域，以及该区域中可用的安装选项。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

所需设备的数量可通过了解预期客户端连接数量而得出。

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的预期访客数量来确定。每个人类用户可携带多个设备，通常每个用户可携带多个设备，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问者数量也取决于事件和/或部署的类型。

示例 1：一个80,000个座位的体育场通常没有80,000个连接的设备，这一比例通常要低得多。20%的互联用户比率在体育赛事中并不罕见，这意味着对于拥有80,000个席位的体育场而言，预期的连接设备数量可以是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从以前的事件中记住的PSK，也可以简单到使用OpenRoaming等更高级的功能，无需用户交互即可登录设备。OpenRoaming网络可以将用户连接率提高至50%以上，这对容量规划有重大影响。

示例 2：期望技术会议具有高用户连接率是合理的。会议参与者需要较长的时间才能连接到网络，并希望能够访问其电子邮件并在全天执行日常任务。这种类型的用户也更可能将多个设备连接到网络 — 尽管他们一次可能仍只使用一台设备。对于技术会议，假设所有访客都连接到网络，此数字可能较低，具体取决于会议类型。

在这两个示例中，关键是要了解预期连接的设备数量，并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，并且连接到该无线电的是客户端设备（不是用户设备）。因此，每个无线电的客户端设备都是可用度量。

每个无线电的设备

对于Wi-Fi 6个AP，思科AP的最大客户端计数为每无线电200个连接的设备，而对于Wi-Fi 6E AP，每个无线电400个连接的设备。但是，不建议设计最大客户端数量。出于规划目的，建议将每个无线电的客户端计数保持在远远低于最大AP容量的50%。此外，无线电数量取决于所使用的AP和天线的类型，关于单频和双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，本部分旨在估计最小AP和天线数量。

以三个不同覆盖区域的示例为例，系统为每个区域提供预期客户端计数，并且每个无线电75个客户端的（正常）值用于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

现在，这些初始数字需要与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结合使用。6GHz计算遵循与5GHz相同的逻辑。本示例未考虑2.4GHz。

假设这三个区域都使用2566P贴片天线和9104体育场天线的组合，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)

每个区域的天线

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，比值为两根天线对一个AP。

本部分演示用于估计部署所需的天线和AP初始数量的方法。此估算需要了解物理区域、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客户端设备的数量。

每次部署都各不相同，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（而非覆盖范围），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业人员对使用案例的透彻了解以及现场验证情况。

预期吞吐量

每个无线信道都可以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，这意味着当无线电中添加更多用户连接时，每个用户的性能都会下降。性能下降并非线性，还取决于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。请注意，大多数客户端设备最多支持2个空间流。

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

列出的速率是理论最大MCS（调制和编码方案）速率，从802.11标准派生，并假设信噪比(SNR)>30dBm。性能良好的无线网络的主要设计目标是为所有位置的所有客户端达到这一级别的SNR，但这种情况很少发生。无线网络本质上是动态的，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影响客户端SNR。

即使达到所需的SNR级别，之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。
- 其他客户端在该特定时间点的活动。
- 特定时间点的干扰。

根据这些因素的变化性，无论设备供应商是谁，都不能保证无线网络的每客户端最低吞吐量。

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平台看起来很简单。首先您可以考虑的是您打算管理的预估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 AP加入仅支持6000 AP的9800-80。但在任何地方都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可以达到高达80 Gbps的客户端数据转发，但这种情况发生在每个客户端数据包的大小为1500字节的最大、最佳的情况下。混合数据包大小后，有效最大吞吐量会降低。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。在启用了许多功能的大型网络中，现实状况下的9800-80交换机有望达到40 Gbps以上，这一点很乐观。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度量，该度量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也能通过正常活动完美处理6000个AP。但是，体育场或机场等公共场所的6000个AP不算常规活动。考虑到客户端漫游量和环境探测量，最大规模的大型公共网络可能会增加单个WLC上的CPU利用率。如果添加监控和SNMP陷阱，客户端每次移动时都会发送，负载可能会很快变得过大。大型公共场所或大型活动的关键特点之一是，随着人们四处移动并不断关联/取消关联，客户端入职活动显着增加，因此这会对CPU和控制平面造成额外压力。

许多部署都表明，一对9800-80无线控制器可以处理拥有超过1000个AP的大型体育场部署。对于正常运行时间和可用性是主要问题的关键事件，通常还会将AP分布到两个或多个控制器对上。当大型网络分布在多个WLC上时，控制器间漫游会更加复杂，因此必须在体育场碗等封闭空间仔细考虑客户端漫游。

另请参阅本文档中的Site Tag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于最终用户是透明的，因为辅助WLC可以无缝接管。HA SSO对的另一个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。升级生产对之前，您可以在此WLC上测试新的软件版本（并仅将几个测试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），此时N+1允许在主动 — 主动场景中拥有安全的WLC，在该场景中，您可以逐渐将AP迁移到和从中迁移AP。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），这往往限制它们只能使用FlexConnect本地交换方案（可能在中央交换中只有少量的AP）。 但是，在维护时段或排除故障时，当您需要额外的控制器时，它们可以作为N+1设备提供帮助。

外部系统

尽管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众多支持系统，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，而且子网很大。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Switch Device Manager(SDM)模板，该模板负责分配系统资源，并根据网络中设备的功能在L2和L3功能之间进行平衡。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问者提供互联网访问。数据路径上的某个位置必须有一个设备负责NAT/PAT转换。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多种NAT/PAT转换。

DNS/DHCP

这两个系统是确保良好的客户体验的关键。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，因此选择适当且扩展良好的外部Web身份验证系统对于良好的客户端入网体验非常重要。对于AAA，RADIUS身份验证服务器必须能够处理无线系统的需求。请记住，在某些情况下，负载会在关键时刻突然增加，例如在足球比赛期间的半小时内，这可以在很短的时间内生成较高的身份验证负载。扩展系统以获得足够的并发负载是关键。使用AAA记账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，如果您使用记帐，请尝试禁用临时记帐。另一个需要考虑的重要事项是使用负载均衡器，此处必须使用会话触发机制来确保完整的身份验证流程。确保将RADIUS超时保持在5秒或以上。

如果将802.1X SSID与较大的客户端计数（例如使用OpenRoaming）配合使用，请确保启用802.11r快速转换(FT)，否则客户端每次漫游时都可能导致身份验证风暴。

DNS/DHCP

DHCP的一些建议：

- 确保DHCP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仍将保持分配一段时间，因此，根据访客的驻留时间，这会消耗更多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，如果一般访问持续时间为两个小时，则无需分配一周的IP地址，这有助于淘汰陈旧租约。
- 建议为客户端使用单个大型子网，WLC具有代理ARP功能，并且在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。与具有多个VLAN的VLAN组相比，单个大型VLAN更简单。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，从而导致VLAN脏乱，并且必须跟踪无法平均使用的各种DHCP池等问题。此建议适用于本地模式AP和集中交换的流量。在使用本地交换的FlexConnect的情况下，由于受到大量广播传输的影响，不支持将100多个（或17.9之后的300个）AP置于同一子网中。Flexconnect要求AP为同一个VLAN提供服务以支持无缝漫游，因此不建议在此场景中支持大型子网。
- 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。这样可以最大限度地提高效率和简化操作。其理念是根本无需在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，但是它可以防止客户端尝试为自己分配静态IP地址，或者客户端行为不当，尝试未经允许重复使用先前IP地址时出现严重的安全问题。

运行网络

正确的配置

启用许多选项以从现代Wi-Fi的所有最新功能中获益非常诱人。但是，某些功能在小型环境中工作良

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。尽管思科设备遵守所有标准并提供与各种经过测试的客户端的兼容性，但世界上仍有许多独特的客户端设备，这些客户端设备有时具有驱动程序软件版本，这些版本存在缺陷或无法与某些功能兼容。

根据您对客户端的控制级别，您必须保持谨慎。例如，如果您为公司的大型年度聚会部署Wi-Fi，您知道大多数客户端是公司设备，您可以相应地计划启用功能集。另一方面，如果您运营的是机场Wi-Fi，您的访客满意度水平将直接与其连接到网络的能力相关，而您对用户可使用的客户端设备没有任何控制权。

SSID

多少个SSID?

建议始终使用尽可能少的SSID。在高密度网络中，由于几乎可以保证在同一信道上有多个AP，这种情况会更加严重。通常，许多部署使用过多的SSID，承认其SSID过多，但声明不能使用更少的SSID。您必须对每个SSID执行业务和技术研究，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。

让我们来了解一些安全/SSID类型及其用途。

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，或者印在纸上，或者标语上，或者以某种方式把它传达给参观者。有时候，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DHCP池因连接的有意为而耗尽。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可能具有有限的支持，如果较旧的客户端没有收到最近的驱动程序或固件更新，则通常容易出现问题。

考虑使用过渡模式WPA2 PSK-WPA3 SAE SSID来简化操作可能很有吸引力，但此字段显示会导致一些兼容性问题。编程不当的客户端不需要在同一SSID上使用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。

Wi-Fi 7需要在WPA3 SSID上配置两个新的AKM（SAE-EXT和SAE-EXT-FT）以及GCMP256加密

，这加强了选择需求（如果您要保持WPA2兼容性，最好不要考虑Wi-Fi 7功能）。 目前并非所有AP型号或客户端都支持GCMP256。

WPA2/3企业版

WPA3 Enterprise（使用AES 128位加密）在技术上与WPA2 Enterprise安全方法相同（至少与SSID信标中通告的安全方法相同），因此可提供最大的兼容性。

对于802.1X，建议使用转换模式SSID，因为未发现最新设备的兼容性问题（Android 8或旧Apple IOS版本报告出现问题）。IOS XE 17.12及更高版本允许使用单个过渡企业SSID，其中在6GHz频段上仅使用WPA3并进行通告，而在5GHz频段上提供WPA2作为选项。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程序数据库的密钥用户，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可以包括结合访客SSID的优点（通过允许访客轻松连接而无需输入任何凭证）和企业SSID安全性的路由器或开放式漫游。它们显着降低了通常与802.1X关联的自注册复杂性，因为只要客户端在电话上有一个配置文件（可通过事件应用轻松提供），客户端就无需执行任何操作来加入教育或OpenRoaming SSID

Wi-Fi 7支持要求（使用最严格的客户端）AP也提供GCMP256加密，这需要IOS-XE 17.18.3及更高版本的软件。

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、本地或集中式Web身份验证，但概念保持不变。使用访客门户时，可扩展性会迅速成为大型环境中的问题。有关这方面的详细信息，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。这仍然允许任何人进行连接，但提供了隐私（甚至比WPA2-PSK更佳的隐私！）和加密，在连接SSID时无需提供任何密钥或凭证。主要智能手机供应商和操作系统现在支持增强型开放性，但在无线客户端群中尚未得到广泛支持。Wi-Fi 7和6GHz操作禁止增强型开放式过渡模式。因此，正确的方法可能是只在6GHz频段上运行增强型开放式SSID，并在5GHz频段上保持完全开放式SSID以实现兼容性。您需要为SSID指定不同的名称，因为它们具有不同的安全方法。这会在客户端扫描列表中添加SSID，但不会在空中添加额外的SSID，因为它们存在于不同的频段。

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，但创建两个SSID且客户端兼容性仍须经过广泛验证）。 虽然这会使注册过程变得更为复杂（您必须在人们的胸卡或门票上打印PSK，或以某种方式将其通告），但这样做可以避免临时客户端自动连接到网络，而最终用户没有任何使用网络的意图。越来越多的移动操作系统

供应商也取消了开放网络的优先级，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的问题，没有令人满意的答案。影响取决于最小配置的数据速率、SSID数量和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:主要WPA2 PSK、用于安全和6GHz覆盖的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事件应用配置Wi-Fi的人员的OpenRoaming SSID，以及用于员工和管理网络访问的独立802.1X SSID。 这几乎已经太多了，但效果仍然合理，因为有大量的可用信道，并且定向天线用于尽可能减少信道重叠。

传统SSID与主要SSID的概念

建议将2.4GHz服务限制为仅在2.4GHz中通告的“传统”独立SSID。随着人们完全停止提供2.4GHz服务，这种情况越来越少了。然而，这个想法可以而且必须坚持下去，但其它概念除外。您想推广WPA3 SAE，但是过渡模式是否给您带来了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，您可以轻松查看有多少客户端仍然面临与您的主SSID的兼容问题，并且需要此旧的SSID。

但是为什么停下来呢？您听到传言说802.11v导致一些较旧的客户端出现问题，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，同时仍然为客户端提供最大兼容性SSID以便回退到。这个系统只能这样工作。如果您将您的兼容性驱动的SSID作为您的主要名称，并将您的高级SSID命名为“<name>-WPA3”，您会发现人们固守了他们以前使用过的旧SSID，而且在您的“新”SSID上采用率在多年内保持较小。由于连接新设置或功能的客户端数量较少，因此推行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。这些功能对于站点调查和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（除非您能提供更加安全且更严格的特定SSID）
- 最好禁用覆盖盲区检测（对于所有SSID）。 大型部署通常使用定向天线，需要进行彻底的现场勘测。每个天线的功率电平是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（以获得最大兼容性），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，而且在802.11ac中的优势非常低。
- 禁用BSS目标唤醒时间。目前客户端对它的采用率很低。
- 禁用主动负载均衡和带选择。如果不在2.4GHz中通告SSID（或者它位于专用SSID上），并且主动负载均衡在客户端坚持连接到已加载的AP时通过拒绝客户端几次，最后接受客户端来延迟客户端关联，则无需使用频段选择。您仍然是在繁忙环境中加载AP，这对于客户端体验是不利的。
- 禁用Fastlane+。
- 禁用通用管理，此功能用于3700 AP，并且仅用于 — UX域。如果任其发展，将会造成不必要的攻击媒介。
- 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。
- 保持WMM允许。禁用它会将您的网络带回802.11g时代，而且要求它不会在9800平台上带来任何优势。
- 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），并且极有可能使您的RADIUS服务器过载。
- 避免使用隐藏的SSID。这不能用于任何安全目的，SSID名称仍可以通过简单应用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的AP信息。
- 尝试每个无线电不要使用四个以上的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，但是使用越来越多的WLAN会浪费大量通话时间。
- 802.11v和802.11k是常见客户端类型越来越支持的标准。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，有时（对于802.11k），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（如凭证、SSH详细信息和国家/地区代码）的接入点进行分组。 为什么站点标签很重要？站点标记还定义了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核心上运行每个进程），四个WNCD进程不执行任何操作。这意味着您没有使用9800-80的所有CPU，因此不建议使用最多支持6000个AP来加载它。

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

- 如果您在具有八个WNCD进程的9800-80上配置了10个站点标记，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

对于包含多个站点和多个站点标记的地理位置较大的部署，建议将站点标记数量设为所使用平台上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的多栋建筑的活动网络，建议将站点标签数量与给定平台上的精确WNCD数量相匹配。最终目标是每个WNCD进程（以及因此分配给无线任务的每个CPU核心）处理大致相似数量的客户端漫游事件，以便在所有CPU核心之间均衡负载。

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，真正重要的是将位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之间的频繁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记（与处理场所的WNCD进程数相同），并将AP按逻辑尽可能划分到这些标记中，以形成逻辑射频邻居组，这些组也均匀分布在站点标记之间。

从IOS XE 17.12开始，可以启用负载均衡算法，以便WLC根据RF接近程度对AP进行分组。这样可以减轻您的负担，并使AP在WNCD过程中均衡分布。如果无法轻松绘制要放置在正确数量的站点标签中的邻居AP组，这将非常有用。此算法的一个特殊性是它将AP分配到WNCD过程，而不考虑它们的站点标签分配，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，并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，可能是WNCD处理了过多的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，例如在机场内）。

策略配置文件

- 启用ARP和重复地址检测(DAD)代理，这允许WLC在设备尝试获取无线设备的MAC地址时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DHCP以避免客户端使用静态IP地址。
- 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，但是由于客户端计数从实时开始延迟，过长的空闲超时会导致生成虚拟客户端条目（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发生的记帐泛洪。组密钥轮换间隔可以在Web UI中的Configuration > Security > Advanced EAP下配置为“EAP-Broadcast Key Interval”
- 使会话超时为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

- 确保已启用TCP adjust MSS。
- 启用信任DSCP上游。不幸的是，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Syslog。配置Syslog服务器IP会使AP向其单播控制台日志。它不仅对AP进行故障排除很有用，而且它比默认设置（使AP在本地VLAN中广播其系统日志）对网络更有利。AP日志记录会生成大量消息负载，即使在AP系统日志未受监控的情况下，通过设置适当的消息严重性和/或配置虚构Syslog IP地址（例如0.0.0.0）来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。问题检测速度较慢，但网络对轻微的暂时性丢包具有更强的抵抗力。
- 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通知单。在接待了许多访客的较大场所中，您希望重点关注最大的问题，而不是那些可能仅仅存在配置错误的特定个人，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。如果您已经对问题

有怀疑和/或数据，并且希望实时运行特定命令，则它是最直接的。主要监控选项为Cisco Catalyst Center或可能的自定义遥测控制面板。使用第三方监控工具是可能的，但是当使用SNMP作为协议时，数据远非实时，而通常的第三方监控工具未对所有无线供应商的特定功能进行足够细细化。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，它还可用于实时故障排除和修复许多情况。

如果要以始终在线的方式在屏幕上显示NOC或SOC的非常具体的指标和构件，自定义遥测控制面板非常有用。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中的网络指标。

对于事件网络，最好监控系统范围的RF统计信息，尤其是每个AP的信道利用率和客户端数量。这可以通过CLI完成，但只在特定时间点提供快照，信道利用率往往是动态的，更适合长期监控。对于这种类型的监控，自定义控制面板通常是一种很好的方法。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，例如会议中心的房间为X，活动场所的房间为Y。

对于自定义监控，NETCONF RPC(pull)和NETCONF流传输遥测(push)都是有效方法，尽管将自定义流传输遥测与Catalyst Center结合使用需要一些注意，因为在WLC上配置的遥测订用数量有限，并且Catalyst Center预填充（和使用）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和返回数据所用的时间。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，在本示例中，每5秒轮询WLC没有用处，更好的方法是每3分钟收集系统范围的RF指标。

NETCONF始终是优先于SNMP的协议。

对核心网络组件的长期监控不容忽视，包括DHCP池利用率、核心路由器上的NAT条目数量等等。因为其中任何一个故障都很容易导致无线故障。

你监视得越严你越能造成你自己的问题

过多的监控会产生问题的几种典型场景：

- 充当客户端的无线传感器可以很好地测量网络中特定位置的吞吐量和连通性，但请记住，设置高测试频率意味着传感器将花费大量时间进行大型数据传输，因此即使没有进行其他测试，信道和网络实际上也很繁忙。这是“你监控的越严厉，你的指标看上去越糟糕”的最好例子。
- 如前所述，SNMP是一种对CPU影响较大的传统协议。当您频繁监控所有无线客户端或AP（当您拥有大量无线客户端或AP时）时，执行大量SNMP轮询会很容易使您的无线网络

CPU被请求淹没。在设置主动轮询间隔之前，请始终考虑要轮询的对象数量。SNMP守护程序在IOS-XE中的IOSd进程内，因此当它位于高CPU时，可能会影响其他IOS功能。

- 即使遥测比SNMP更有效，大型无线网络的客户端、AP数量可能非常多，但也会存在干扰和欺诈设备。如果您的遥测配置设置过于集中，并且WLC必须持续报告任何欺诈设备的信号变化，这也会轻易使任何控制器设备饱和。请务必关注您负责遥测的“pubd”进程，并确保该进程未处于高CPU使用率状态。如果是，请重新考虑您的阈值并确保遵循9800最佳实践。

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，但从不进行身份验证，因为最终用户没有主动尝试连接（自动连接的设备）。 控制器必须拦截那些处于称为Web身份验证挂起且使用WLC资源的状态的客户端发送的每个HTTP数据包。网络运行后，请定期监视在给定时间处于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（IP学习）状态的客户端也同样如此。客户端执行DHCP过程时，您始终处于该状态，但了解适合您的网络的正常工作数量有助于设置基准并确定此数量可能过高并表明出现较大问题的时间。

对于大型场所，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：他们无法连接，或者难以连接（断开连接），或者Wi-Fi的运行速度低于预期。后者很难识别，因为它首先取决于对速度的期望以及给定区域的实时密度。让我们讨论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。此cisco.com文档介绍如何监控网络以发现吞吐量问题。通过计算客户端在安静状态下可以合理期望在网络上出现多少吞吐量，并估计随着客户端数量和负载增加，这些估计值会下降多少。从技术角度评估最终用户对吞吐量的投诉是否合法，以及您是否需要重新设计该区域以满足其可能面临的负载，这是非常关键的。

当客户端报告连接问题时，在隔离并与Catalyst Center进行澄清后，请查看Catalyst 9800客户端连接问题故障排除流程。

最后，作为一般良好的做法，请借助Monitor Catalyst 9800 KPI（关键性能指标）来关注WLC的总体关键指标。

针对可扩展性配置

9800上的SVI和接口

避免在WLC上为客户端VLAN创建SVI。习惯于旧版AireOS WLC的管理员倾向于反射为每个客户端VLAN创建第3层接口，但很少需要这样做。接口会增加控制平面攻击向量，并且可能需要更多ACL以及更复杂的条目。默认情况下，WLC可以在其任何接口上访问，需要做更多的工作来保护具有更多接口的WLC。它也会使路由复杂化，因此最好避免它。

从IOS XE 17.9开始，mDNS监听或DHCP中继场景不再需要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聚合探测间隔。默认情况下，AP每500毫秒更新一次WLC以了解客户端发送的探测功能。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中的控制平面性能问题。建议设置为每64秒有50个聚合探测响应。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，因为如果认为在扫描时单个客户端可能使用许多本地管理的MAC来避免故意跟踪，则跟踪没有意义。

```
wireless probe limit 50 64000

no wireless probe locally-administered-mac
```

IPv6

许多网络管理员仍然拒绝IPv6。IPv6只有两个可接受的选项：您要么支持该协议，并且必须在任何位置部署足够的配置，要么不部署该协议，并且必须阻止该协议。不关心IPV6，而将其保留在某些地方，没有正确配置，这是不可接受的。这会使整个IP世界对您的网络安全一无所知。

如果启用IPv6，则必须在2001:DB8::/32范围内配置虚拟IPv6地址（这是常被遗忘的步骤）。

需要注意的是，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，IPv6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、路由器请求和其他运行IPv6所需的协议转发。

如果您的Internet连接或Internet服务提供商提供IPv6地址，您可以决定允许客户端使用IPv6。这与在您的基础设施中启用IPv6是不同的决策。您的AP只能在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发生通信。

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层组播发送（因此发送到整个客户端子网）的概念。mDNS在家庭和小型办公室场景中非常流行，在这种场景中，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网关是指使用WLC作为网络中所有服务的目录这一概念。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，打印机通过带有相同子网第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。这样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，并且只有在他们询问存在哪些服务时才会收到应答。虽然它极大地提高了流量效率，但由于mDNS流量的监听，它确实会导致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。

桥接它会导致大型子网中的组播风暴，而监听它（使用mDNS网关功能）会导致大量CPU利用率。在全局和每个WLAN上禁用它。

有些管理员启用mDNS是因为一些服务需要特定位置的mDNS，但了解这会增加多少不需要的流量非常重要。Apple设备经常自我宣传，并不断寻找服务，即使没有人专门使用任何服务，也会导致mDNS查询的背景噪音。如果您由于特定业务需求而需要允许mDNS，请全局启用它，然后仅在需要的WLAN上启用它，并尝试限制允许mDNS的范围。

强化网络

安全

在大型公共网络中，许多事情可能是在管理员不知道的情况下发生的。人们会随机要求电缆掉落，或在某个位置插入家用交换机，为他们的恶作剧设置更多交换机端口……他们经常在没有事先获得允许的情况下尝试这些事情。这意味着，即使没有恶意攻击者介入，安全也可能会被有意愿的客户和/或员工破坏。这样一来，恶意攻击者就很容易四处走动，找到一条电缆，然后查看从那里获得的网络访问。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条件。Catalyst Center可以帮助您自动执行此部署，并且可以为不支持802.1X身份验证但尽量少依赖基于MAC的身份验证的特定设备设置例外，因为这是（真诚的）并非真正的安全性。

流氓接入点

你对付流氓的策略取决于几个因素。许多管理员本能地追求非常严格的规则，但主要问题是：

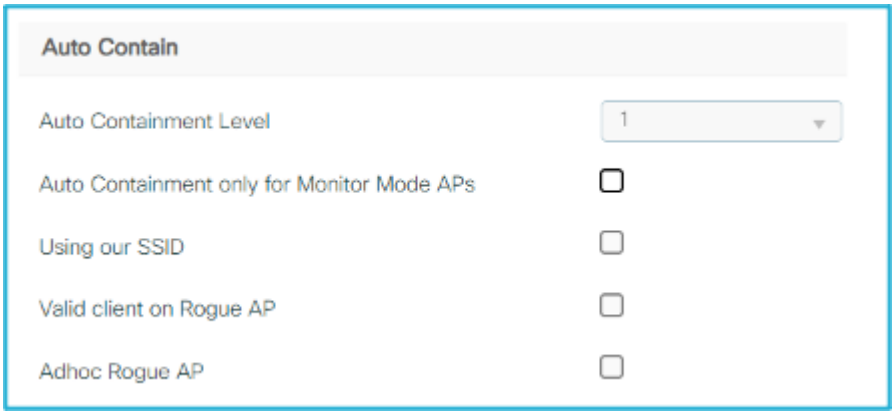
- 当您收到数百个（如果不是数千个）恶意警报时，您是否拥有人力资源来查看所有这些警报并对它们执行操作？
- 您的目标是物理移除恶意程序以保持干净的射频频谱吗？如果是，您需要很多人来执行此操作。或者，您的目标可能只是关注安全因素，确保恶意软件不会带来任何危险？这会产生更易于管理的人类工作成本。
- 启用欺诈检测可能会对您的通话时间产生影响，而欺诈遏制通常会产生更大的影响。您是否分析了这种影响并将其考虑在内？

关于欺诈检测的影响，9120和9130配有专门的CleanAir芯片，负责信道外扫描（因此欺诈检测），使对客户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，但其他没有CleanAir芯片的AP需要将其客户端服务无线电（非信道）置于非信道状态以扫描恶意程序或进行遏制。因此，您使用的AP型号在是否使用专用监控模式AP进行欺诈检测和遏制决策中发挥了作用。

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

非法遏制经常被法规禁止，因此您在启用前必须与您的当地权威机构进行核实。控制欺诈并不意味着远程关闭欺诈，而是使用取消身份验证帧对尝试连接到欺诈接入点的客户端进行垃圾邮件处理，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，因此只能使用旧版安全SSID（在WPA3中或在WPA2中启用PMF时不起作用）。遏制会对目标信道上的RF性能产生负面影响，因为您的AP会使用取消身份验证帧来填充通话时间。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。出于上述所有原因，建议不要进行任何遏制，因为它不能完全解决欺诈问题并导致更多RF问题。如果需要使用遏制功能，则只需为欺骗某个托管SSID的恶意程序启用该功能即可，因为这是一种明显的蜜罐攻击。

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

您还可以配置欺诈规则，根据自己的标准将其分类为恶意欺诈接入点。不要忘记输入相邻和已批准的SSID的名称作为友好欺诈，以便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，并搜索在无线和有线基础设施上都能侦听的欺诈客户端MAC。要完全防止有线欺诈，最好的解决方案是使用802.1X身份验证保护您的所有交换机端口。

如果您要对欺诈接入点进行物理操作，则利用Cisco Spaces是获得欺诈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，但是将搜索范围缩小到几米就非常可行了。如果没有空间，恶意程序将显示在地图上，旁边的AP检测到它声音最响，这会导致搜索区域相当大。许多无线工具和设备可以实时显示恶意接入点的信号，帮助您在物理上定位恶意接入点。

与恶意程序不完全相关，但因为CleanAir刚刚被覆盖，所以必须注意，启用CleanAir不会带来明显的负面影响，除了BLE信标检测，因为这会影响2.4GHz的性能。您可以将无线配置为完全忽略蓝牙干扰源，因为蓝牙干扰源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。

您的欺诈检测列表中没有显示另一类欺诈。某些客户端可以在彼此之间使用Wi-Fi直接连接，因此不使用任何接入点。这并不是真正的安全问题，而是使用RF广播时间。
例如Apple AirDrop，两台设备通过蓝牙相互检测，然后可以同意使用Wi-Fi通道传输文件。用户仍然希望传输此文件，因此最好让用户尽快传输该文件，以便干扰尽快停止。但是，请注意，如果VPN应用无法正确处理AWDL接口状态更改，空投检测有时会导致VPN隧道抖动；对于最终用户而言，当实际是其VPN应用与空投协议的组合导致抖动时，它感觉您的基础设施Wi-Fi质量较差。如果在客户端上禁用蓝牙可以解决问题，则在Wi-Fi端不是问题。
另一个众所周知的例子是Apple SideCar，您可以使用iPad将计算机屏幕扩展到另一个显示器。这会导致显着的RF利用率，因为流是连续的，并且可以使用较大的信道宽度。

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。除了这些攻击以外，它有时还会提供事件的PCAP以供调查分析。

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：要怎么做才能对抗它？

由于难以管理许多不受您控制的客户端，因此可以将警报分为两类。如果您看到过多的警报，您可以决定从Cisco Catalyst Center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:广播探测泛洪警报
- 10004：DoS:取消关联泛洪警报
- 10005：DoS:广播取消关联警报
- 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攻击警报
- 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都会发生，仅描述Apple设备之间的常规点对点活动）
- 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

这些警报可能是由行为不端的客户端引起的。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使通话时间处于繁忙状态。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，因此会影响其周围的客户端性能。

其他警报非常具体，最可能描述实际的恶意攻击，并且由于客户端驱动程序不正确几乎不可能发生。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 Start V1 Flood by Signature
- 10017：按目标重新关联请求泛洪
- 10018：按签名的Beacon泛洪
- 10019：按目标划分的探测响应泛洪
- 10020：按签名阻止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，但消除此类攻击的唯一实际操作是实际前往该位置并删除违规设备。

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。

速率限制客户端

管理层和管理员会忍不住考虑对用户进行速率限制，以防止一个用户占用特定位置的带宽。然而，在实地已经多次证明，从总飞行时间的角度来看，不进行任何速率限制更有效率。用户访问网络和进行活动的速度越快，离开网络的速度也越快。速率限制传输速度不会阻止用户进行大型文件传输，它只会使传输速度变慢，并在传输过程中丢弃数据包，这意味着浪费的总传输时间比没有任何限制的情况更常见。无线速率限制通过在AP在特定时间段转发来自客户端的一定数量的数据包后丢弃数据包来完成，如果您不按应用执行此操作，可能会丢弃来自客户端的重要流量。但是，如果按应用程序执行此操作，可能会产生与所需不同的效果，因为某些应用程序使用多个连接，这可能会使此应用程序的吞吐量计算复杂化。思科CX专家建议彻底删除您不想要的某些应用，而不是使用速率限制。思科无线Meraki云文档也涵盖此内容：https://documentation.meraki.com/Wireless/Operate_and_Maintain/How_Tos/Firewall_and_Traffic_Shap

以及Cisco Wireless Catalyst文档https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215441-configure-qos-rate-limiting-on-catalyst.html

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上的客户端仍然能够相互联系，并且属于移动组中不同WLC的客户端也可以绕过此限制。但它可以充当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势是它还能防止客户端到客户端ARP，防止应用程序发现本地网络上的其他设备。如果不进行点对点阻塞，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，可能还显示其IP地址和主机名。

除此之外，建议在WLAN上同时应用IPv4和IPv6（如果在网络中使用IPv6）ACL来防止客户端到客户端通信。无论您是否有客户端SVI，在WLAN级别应用阻止客户端与客户端通信的ACL都可以工作。

另一个强制步骤是防止无线客户端访问任何形式的无线控制器管理。

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
```

这在第2层VLAN数据库中创建的具有客户端VLAN 131到137的WLC上完成，但没有对应的SVI，并且只有一个SVI存在于VLAN 130（即WLC的管理方式）。此ACL可完全防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管理并不是您唯一需要允许通过的事情，因为还需要允许到所有AP的CAPWAP连接。这就是此ACL具有默认permit但阻止无线客户端范围的原因，而不是依赖默认deny all操作来指定所有允许的AP子网范围和管理范围。

同样，您可以创建另一个指定所有可能管理子网的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量比其他应用要多。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，这些数据包会迅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（虽然不能保证其可靠）通过空中传输此帧，这可通过使用强制数据速率（可以使用强制速率之一进行配置）来实现。 用通俗易懂的术语来说，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，可能需要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。最好记录应用详细信息、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的要求。最好完全禁用广播转发。应用程序有时会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。通过启用此功能，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，从而节省大量数据包重复工作。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
```

如果需要依赖组播，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，每个网络都具有独特的要求和结果。

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，准则只是准则，可能需要在特定场所的范围内进行解释或调整。

思科CX拥有专用于大型无线部署的无线专业团队，并在包括体育赛事和会议在内的众多大型活动中拥有丰富的经验。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）。