思科验证设计

园区局域网和无线局域网设计摘要

2015 年 10 月

目录

园区设计简介

有一种倾向是，将网络简化成如同水管一样，这样可以认为您只需考虑管道的尺寸和长度，或者链路的速度和流量，而其它东西并不重要，也不再考虑。正如大型体育馆或高楼大厦水管设施的设计必须考虑规模、用途、冗余、防范擅动或拒绝操作，以及应对峰值负荷的能力一样，对网络也需要类似的考虑。因为用户依赖网络来访问工作所需的大多数信息，同时可靠地传输语音或视频数据，网络必须能够提供弹性和智能化的传输。

网络设计应着眼于考虑组织的网络趋势和未来需求。

- 随着时间的推移，为了满足所支持的组织需求，网络必须随时可以进行适当扩展。
- 随着对采用最新 802.11ac 技术的无线接入点 (AP) 的需求超过 1 Gbps，您应当部署一个随时可以满足该需求的网络，而无需升级现有的铜质以太网布线方案。您可以通过部署具有 mGig 能力的网络平台来满足这些最新需求。
- 随着您部署具有更高功率要求的设备，例如照明、远程接入交换机和接入点，您的设计应当具备支持每个端口 60W 的以太网供电能力。接入思科通用型以太网供电 (UPOE) 可实现这一目标。
- 合规性问题推动您作出在支持标准认证和 MACsec 时所需的平台选择。在这种情况下，您还应当使用 NetFlow 等技术随时准备提供分析数据。
- 物联网和万物互联影响着当今的网络设计。您的网络应当支持 TrustSec 及其它分段和虚拟化技术，以便能够扩展使用受这些趋势推动的网络。
- 在网络的整个使用寿命期间，带宽需求正在翻倍、甚至可能翻数倍，因此，随着时间推移，当今部署的网络需要做好准备，以利用 10 Gbps 以太网汇聚为 40 Gbps 到 100 Gbps 的容量。
- 当今部署的网络平台应当面向未来提供最长的使用寿命，而不是选择仅满足眼下需求的设备。
- 对于不同的场地面积和网络密度，您应当以满足部署要求的最佳方式，融合有线和无线网络平台。

园区局域网 (LAN) 是支持一个场所的人们使用设备连接信息的网络。园区局域网可以是小型远程站点的单台交换机，也可以是大型的多个建筑基础设施，支持教室、铺好地毯的办公区域及人们使用设备的类似地方。园区设计兼具有线和无线连接，实现完整的网络接入解决方案。本文档阐述了以下内容：

- 园区有线局域网设计的基础知识。
- 无线局域网 (WLAN) 如何扩展安全网络接入，惠及您的移动员工队伍。
- WLAN 可以如何为承包商和访客提供访客接入。

如需相关的设计指南、部署指南和白皮书，请点击以下链接：

http://www.cisco.com/go/designzone

园区局域网和无线局域网设计指南

为园区用例设计一个局域网并不存在放之四海而皆准的设计。园区局域网的规模可以小至单台交换机和小型远程站点的无线接入点，也可以是一个大型、分布式、多个建筑综合体，具有高密度的有线端口和集中化的无线需求。其部署可能要求网络所提供的服务高度可用，而对风险的容忍度很低，或者可能对于出故障再修复方法有一定的容忍度，同时数量有限的用户遭受较长时间的服务中断被认为是可接受的。使用精益的云管理方法对于一些场所可能是可接受的，而对于网络设备密度更加集中的较大总部场所来说，则现场 IT 员工更受青睐。这些部署的平台选择的驱动因素通常是网络容量的需求、所提供的设备和网络功能，以及满足对于组织来说很重要的任何合规要求这一需求。

大多数园区有线局域网设计的复杂度是在与接入层和分布层互连时才暴露出来。如果连接至接入层的设备在第二层有邻接需求，而囿于网络的规模，连线需要覆盖连接至一个分布层的多个配线间，则您可以调整传统的多层园区设计来满足这些需求。然而，存在一些更受青睐的替代方案，可让部署变得更加易于管理且更不易出错。这类替代方案包括在分布层使用交换机堆叠或虚拟交换系统 (VSS) 来简化分布层选项，这使得 IT 人员可以更加轻松地进行部署和故障排除。通过部署思科 Catalyst 即时接入解决方案，将接入层和分布层合并至一个设备管理域中，您可以使这种简化更进一步。尽管传统的多层园区设计是得到广泛部署的有效解决方案，但鉴于有更好的替代方法，它并非我们通常推荐的方案。

推荐的设计选择并非仅有的选择，但是考虑到要求范围，它们是重点强调的首选选择。

高密度大型园区设计

高密度大型园区设计具有连接至一个核心的多个分布层，并在有线端口和 WLAN 设备的接入层具有密度要求。首选的设计具有支持超过 1000 个有线及无线用户和设备的容量，而且高度可用，能够实现关键业务的连续性，同时具有支持诸如 NetFlow 及网络虚拟化和分段等高级功能的能力。您可能选择这种设计用于密度低于所支持密度的情况；然而，其要求会提出对关键业务连续性或高级功能的需求。

园区核心

如果存在三个及以上互相连接的分布层，或者需要在一个共同位置的连接性，则您需要使用一个第三层局域网，从而简化连接和管理。您从两种核心选项中选择使用其中一种，以满足高密度大型园区设计的核心需求。

- **Catalyst 6800 系列和配备了管理引擎 2T 的 Catalyst 6500 系列**——Catalyst 系列中的成员能够适应各种核心密度，从而涵盖园区核心中普遍使用的功能。您可以将设备合并至 VSS 模式中，各成员交换机具有冗余管理引擎选项，从而提供高度可用的配置，作为一个设备进行管理。这是实现轻松配置和管理的首选选项，使用了部署最广泛的核心园区平台。

- **思科 Nexus 7000 系列**——思科 Nexus 系列中的成员拥有各种密度选项，并可以分成多个虚拟设备环境，允许同样的设备用于一个园区核心和一个数据中心核心。当需要独立管理核心交换机，并在交换机之间具有虚拟 PortChannel 功能，或者需要 100 千兆位的高密度以太网时，这些交换机便是首选选项。

园区有线分布、有线接入和无线

在高密度大型园区中，您对有线分布和接入的选择是基于对此用途最可用的平台、最高的密度和最广泛的接口选项、冗余电源和模块化控制平面，具有最先进的软件功能。

在高密度大型园区设计中，集中化无线是首选选项，使用具备 802.11ac 和 CleanAir 功能的接入点。

表 1　　高密度大型园区建议的部署平台

	同类最佳——综合领先高级网络功能	任务关键型——基础另加额外网络功能	企业级——基础网络功能
分布/汇聚交换机	思科 Catalyst 6807-XL 模块化机箱对，采用管理引擎 2T VSS 四管理引擎状态切换配置	思科 Catalyst 6880-X 可扩展固定机箱对 VSS 配置	思科 Catalyst 3850 系列 SSO 堆叠
接入交换机	思科 Catalyst 4500E 系列，采用双管理引擎 8-E SSO 和 6800IA	思科 Catalyst 3850 和 3650 系列以及 6800IA 可堆叠交换机	思科 2960-X 系列，采用堆叠模块
无线局域网控制器	高可用性状态切换 (HA SSO) 模式的集中化思科 8500 或 5500 系列 (AireOS)	HA SSO 模式的集中化思科 8500 或 5500 系列 (AireOS)	HA SSO 模式的集中化思科 8500 或 5500 系列 (AireOS)
接入点	思科 3700 系列	思科 2700 系列	思科 1700 系列
关键功能——有线	最高可用性 1/10/40/100 千兆位以太网服务、MACsec、TrustSec MPLS（分布/即时接入）、NetFlow、UPoE（通用型以太网供电）	1/10/40 千兆位以太网服务、MACsec、TrustSec MPLS（分布/即时接入）、NetFlow、UPoE（通用型以太网供电）	1 千兆位以太网接入、PoE+
关键功能——无线	超过 1 Gbps 的 802.11ac、4x4 MIMO:3SS、HDX、CleanAir 80 MHz、ClientLink 3.0、VideoStream、用于 3G/位置准确性/第二阶段选项的模块化	超过 1 Gbps 的 802.11ac、3x4 MIMO:3SS、HDX、CleanAir 80 MHz、ClientLink 3.0、VideoStream	高达 1 Gbps 的 802.11ac、3x3 MIMO:2SS、CleanAir Express、传输波束成形

中密度园区设计

中密度园区设计是单一分布层，它可以单独使用，或者用作连接至另一个分布层或其它服务的折叠核心，或者也可能连接至远程站点（已发展到需要一个汇聚层）的广域网路由器。接入层中对有线端口和 WLAN 设备的需求量通常为数百个（而大型设计中则为数千个），需要的接入点少于 100 个。首选设计力求满足典型的业务连续性需求，这类需求不需要提供所有冗余组件和标准网络功能。

园区有线分布、有线接入和无线

您选择有线分布和接入时偏向于规模和灵活性，从而满足中等规模安装的空间和功率需求，并随着组织的发展进行弹性扩展。在对密度和高级软件功能的要求并不那么强烈的地方，显示的选项更具经济性和更常见的节约偏好。

在中密度园区设计中，融合接入和使用 FlexConnect 的集中化无线是首选选项。

表 2　　中型园区建议的部署平台

	同类最佳——综合领先高级网络功能	任务关键型——基础另加额外网络功能	企业级——基础网络功能	云管理
分布/汇聚交换机	思科 Catalyst 4500E 系列，采用管理引擎对 8-E VSS 配置	思科 Catalyst 6880-X 可扩展固定机箱对 VSS 配置	思科 Catalyst 3850 系列 SSO 堆叠	思科 Meraki MS420 系列交换机
接入交换机	思科 Catalyst 3850 系列可堆叠交换机融合接入配置	思科 Catalyst 3850/3650 系列可堆叠交换机融合接入配置	思科 2960-X 系列，采用堆叠模块	思科 Meraki MS220 系列交换机
无线控制器	集成接入交换机或 5500/2500 系列本地控制器	集成接入交换机	HA SSO 模式的 FlexConnect 搭配集中化思科 8500/7500/5500 系列 (AireOS)	云管理控制器
接入点	思科 3700 系列	思科 2700 系列	思科 1700 系列	思科 Meraki MR34 系列
关键功能——有线	1/10/40 千兆位以太网服务、MACsec、TrustSec、NetFlow、UPOE	1/10 千兆位以太网服务、MACsec、TrustSec NetFlow、UPOE	1/10 千兆位以太网服务、MACsec、TrustSec NetFlow	云管理、千兆位以太网接入、深度可视性、PoE+
关键功能——无线	超过 1 Gbps 的 802.11ac、4x4 MIMO:3SS、HDX、CleanAir80 MHz、ClientLink 3.0、VideoStream、用于 3G/ 位置准确性/第二阶段选项的模块化	超过 1 Gbps 的 802.11ac、3x4 MIMO:3SS、HDX、CleanAir 80 MHz、ClientLink 3.0、VideoStream	高达 1 Gbps 的 802.11ac、3x3 MIMO:2SS、CleanAir Express、传输波束成形	云管理、超过 1 Gbps 的 802.11ac、3x3MIMO、深度可视性、位置分析

小型站点园区设计

小型站点园区设计是单一接入交换机或者单一接入交换机堆叠。接入层中对有线端口和 WLAN 设备的需求量通常为数十个（而中型设计中则为数百个），需要的接入点少于 25 个。首选设计力求将成本最小化，同时提供最少数量的组件和功能。

园区有线接入和无线接入

在小型站点园区设计中，您选择有线接入时偏向于规模和灵活性，以便满足小型站点的空间和功率需求。对密度和高级软件功能的要求并不那么强烈，因此显示的选项最具经济性的偏好。

在小型站点园区设计中，融合接入和使用 FlexConnect 或云管理的集中化无线是首选选项。

表 3　　小型园区建议的部署平台

	同类最佳——综合领先高级网络功能	任务关键型——基础另加额外网络功能	企业级——基础网络功能	云管理
接入交换机	思科 Catalyst 3850 系列可堆叠交换机融合接入配置	思科 Catalyst 3650 系列可堆叠交换机融合接入配置	思科 2960-X 系列，采用堆叠模块	思科 Meraki MS220 系列交换机
无线控制器	集成接入交换机或思科 5500/2500 系列本地控制器	集成接入交换机	HA SSO 模式的 FlexConnect 搭配集中化思科 8500/7500/5500 系列 (AireOS)	云管理控制器
接入点	思科 3700 系列	思科 2700 系列	思科 1700 系列	思科 Meraki MR34 系列
关键功能——有线	千兆位以太网服务、MACsec、TrustSec NetFlow、UPoE（通用型以太网供电）	1 千兆位以太网服务、MACsec、TrustSec NetFlow、PoE+	千兆位以太网接入	云管理、千兆位以太网接入、深度可视性、PoE+
关键功能——无线	超过 1 Gbps 的 802.11ac、4x4 MIMO:3SS、HDX、CleanAir 80 MHz、ClientLink 3.0、VideoStream、用于 3G/ 位置准确性/第二阶段选项的模块化	超过 1 Gbps 的 802.11ac、3x4 MIMO:3SS、HDX、CleanAir 80 MHz、ClientLink 3.0、VideoStream	高达 1 Gbps 的 802.11ac、3x3 MIMO:2SS、CleanAir Express、传输波束成形	云管理、超过 1 Gbps 的 802.11ac、3x3MIMO、深度可视性、位置分析

园区有线局域网设计基础知识

局域网是为分布在单一楼层或单个建筑中的最终用户和设备提供网络通信服务和资源访问的网络基础设施。您可以通过相互连接一群散布在小型地理区域的局域网创建一个园区网络。园区网络设计概念包括使用单台 LAN 交换机的小型网络，一直到拥有成千上万个连接的大型网络。

园区有线局域网可实现一幢建筑或建筑群中设备之间的通信，以及在网络核心实现与广域网和互联网边缘的互连。

具体来讲，这种设计提供一种网络基础和服务，可实现：

- 分层局域网连接。
- 员工有线网络接入。
- 用于高效数据分布的 IP 组播。
- 随时用于多媒体服务的有线基础设施。

分层设计模式

园区有线局域网使用一种分层设计模式，将设计分成模块化的组或层。将设计分层后可允许每层实施特定的功能，这可简化网络设计，并由此简化网络部署和管理。

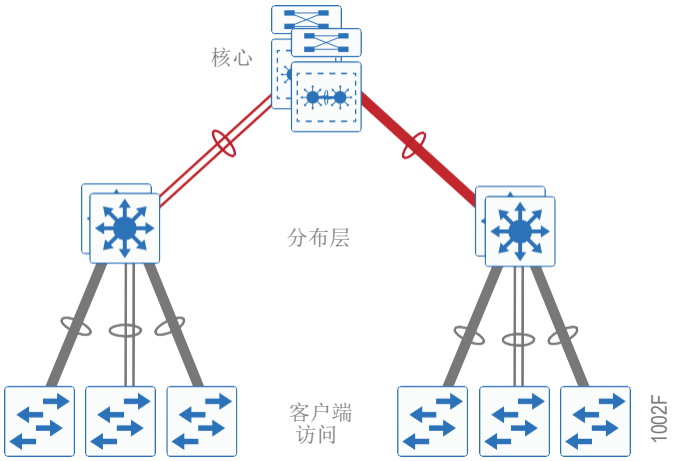
网络设计中的模块化允许您创建出可在整个网络复制的设计元素。复制可提供一种轻松的网络扩展方式，同时提供一致的部署方法。

扁平或网状网络架构中的变化常常会影响到大量系统。分层设计有助于限制对部分网络的操作性更改，这可实现轻松管理并提高恢复能力。将网络布局成为小型、容易理解的模块化元素也可通过改善故障隔离而提高恢复能力。

分层局域网设计包括以下三层：

- **接入层**——提供端点和用户对网络的直接访问
- **分布层**——汇聚接入层并提供服务连接性
- **核心层**——为大型局域网环境提供分布层之间的连接性

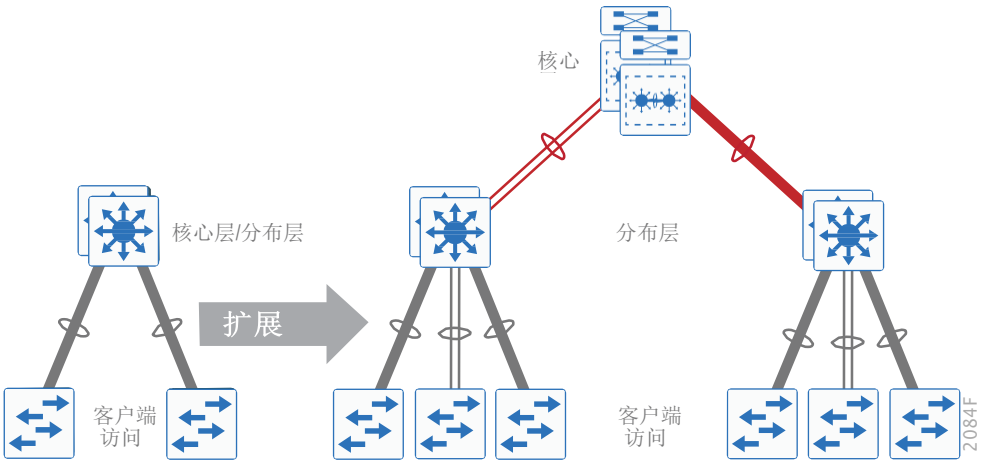
图 1　　局域网分层设计



每一层——接入层、分布层及核心层——为网络提供不同的功能。取决于部署站点的特征，您可能需要其中的一层、两层或全部三层。例如，占据单一建筑的站点可能仅需要接入层和分布层，而一个包含多幢建筑的园区将最有可能需要全部三层。

无论在一个场所实施了多少层，这种模块化设计可确保每层提供相同的服务，同时在这个架构中，将采用相同的设计方法。

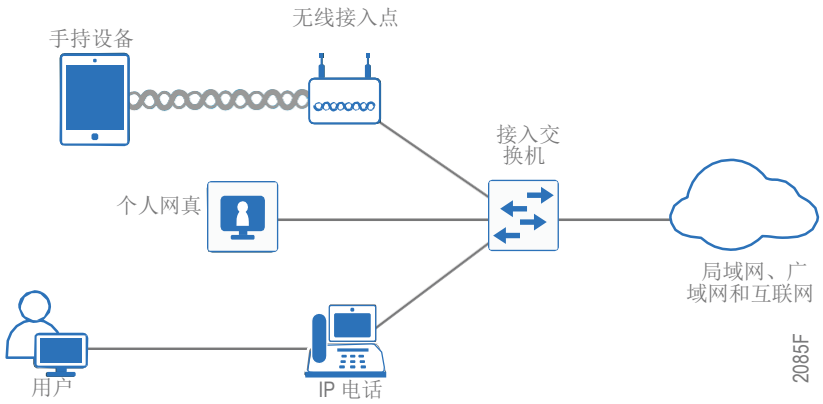
图 2　　采用模块化设计带来的可扩展性



接入层

接入层是用户控制的设备、用户可访问的设备，以及其它终端设备连接至网络的地方。接入层同时提供有线和无线连接，同时其所包含的功能和服务可确保整个网络的安全和恢复能力。

图 3　　接入层连接



- **设备连接**——接入层提供高带宽设备连接。为了帮助网络成为最终用户日常工作的一个透明部分，接入层必须在用户执行例行工作时（例如发送较大的电子邮件，或者从内部网页打开大文件）支持高带宽流量的突然爆发。

  因为众多类型的最终用户设备在接入层连接——个人电脑、IP 电话、无线接入点以及 IP 视频监控摄像头——接入层可支持众多逻辑网络，从而提升性能、管理和安全性。

- **恢复能力和安全服务**——接入层设计必须确保网络可供所有需要它的用户使用，无论他们何时需要。作为网络与客户端设备之间的连接点，接入层必须帮助网络防范人为错误和恶意攻击。这种保护包括确保用户仅可访问授权服务、防止最终用户设备在网络上接管其它设备的作用，以及只要有可能，验证每个最终用户设备被允许进入网络。

- **先进技术功能**——接入层提供一系列网络服务，可支持诸如语音和视频等先进技术。接入层必须为使用先进技术的设备提供特殊化访问，以确保来自这些设备的流量不受来自其它设备流量的影响，同时确保为网络中的众多设备高效提供所需的流量。

接入层平台

用于园区有线局域网的首选选项包括以下思科交换机，作为接入层平台：

- 思科 Catalyst 4500E 系列交换机
- 思科 Catalyst 3850 系列交换机
- 思科 Catalyst 3650 系列交换机
- 思科 Catalyst 2960-X 系列交换机

分布层

分布层支持许多重要的服务。在一个连接需要端到端地遍历局域网（无论是在不同的接入层设备之间，还是从接入层设备到广域网）的网络中，分布层可促进这种连接。

- **可扩展性**——在拥有两个或三个以上接入层设备的任何站点中，要将所有接入交换机互连是不切实际的。分布层充当多个接入层交换机的汇聚点。

  分布层可通过提高网络效率、降低内存要求、创建可分隔故障或网络更改的故障域，以及通过为网络其它地方的设备处理资源来降低运营成本。分布层还通过将故障限制在较小的域来提升网络可用性。

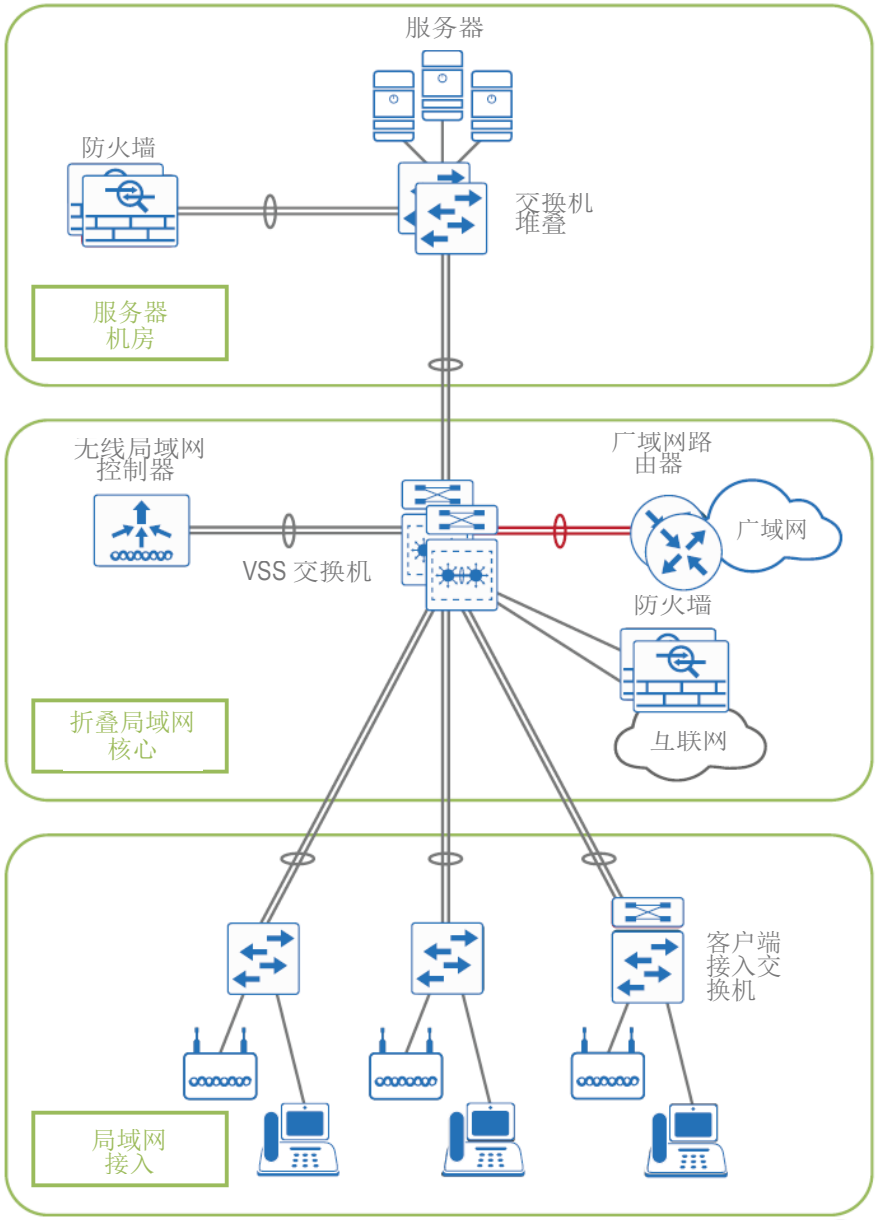
- **降低复杂度并提高恢复能力**——园区有线局域网拥有使用一个简化分布层的选项，其中一个分布层节点包含单个逻辑实体，可通过使用作为一个设备运营的一对物理分隔的交换机，或者使用作为一个设备运营的交换机物理堆栈来实施。通过物理冗余组件，如电源、管理引擎、模块以及状态切换至冗余逻辑控制平面提供恢复能力。

  由于所需的协议更少，该方案降低了配置和运营分布层的复杂度。围绕故障或破坏提供近秒级或次秒级融合所需的调整很少或没有。

双层设计

分布层为连接至基于网络的服务、广域网和互联网边缘提供连接。基于网络的服务包括但不限于宽域应用服务（WAAS）和无线局域网控制器。取决于局域网的大小，这些服务以及与广域网和互联网边缘的互连可能位于一个分布层交换机，它同样汇聚了局域网接入层连接。这也称为折叠核心设计，因为分布层充当所有设备的第三层汇聚层。

图 4　　双层设计：分布层充当折叠核心



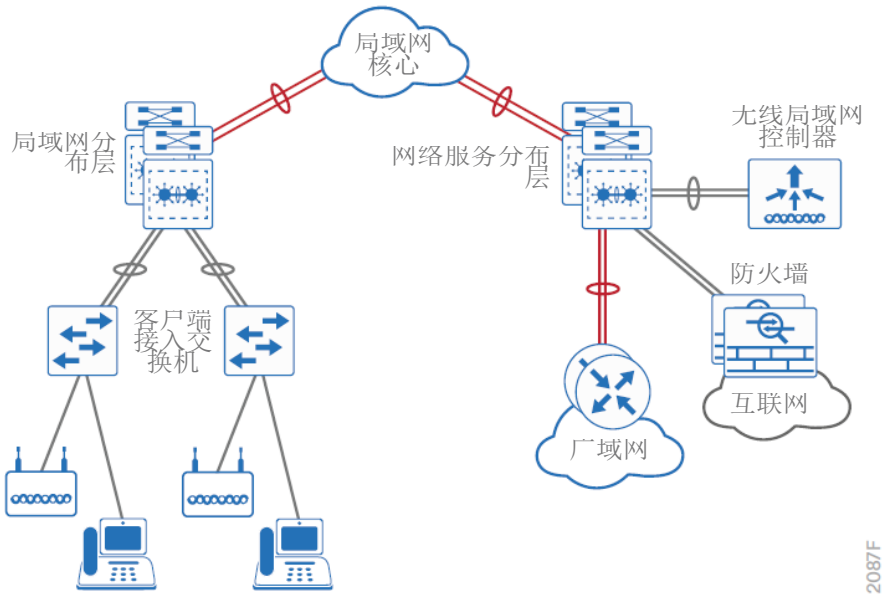
三层设计

更大型的局域网设计需要一个专属分布层，用于基于网络的服务，而不是与接入层设备共用连接。随着广域网路由器、WAAS 控制器、互联网边缘设备和无线局域网控制器密度的增长，连接至单一分布层交换机的能力变得难以管理。一系列因素推动着局域网设计包含多个分布层模块：

- 分布层平台能够提供的端口数量以及端口带宽影响网络性能和吞吐量。
- 当所有局域网和基于网络的服务依赖于单一平台时，网络恢复力便是一个因素，无论该平台的设计如何，它可以呈现出单一故障点或者一个不可接受的大型故障域。
- 改变控制和频率会影响恢复能力。当合并所有局域网、广域网和其它网络服务到单一分布层时，运营或配置错误会影响全部网络运营。
- 大型园区设施中跨越许多建筑的局域网接入交换机的地理分散性将要求有更多光纤互连至单一折叠核心。

与接入层一样，分布层也为应用程序流提供服务质量 (QoS)，以保证关键应用程序和多媒体应用的性能符合设计。

图 5　　含有网络服务分布层的三层设计



分布层平台

用于部署园区有线局域网分布层的首选思科交换机包括：

- 思科 Catalyst 6807-XL 系列交换机，采用管理引擎 2T
- 思科 Catalyst 6500 系列交换机，采用管理引擎 2T
- 思科 Catalyst 6880-X 系列交换机
- 思科 Catalyst 4500-X 系列交换机
- 思科 Catalyst 4500E 系列交换机
- 思科 Catalyst 3850 系列交换机

核心层

在大型局域网环境中，常常需要有多台分布层交换机。其中一个原因是，当接入层交换机位于多个地理分散的建筑时，通过在每幢建筑布置一台分布层交换机，您可以节省建筑之间铺设的昂贵光纤成本。随着网络在单一场所的增长超过三个分布层，组织应当使用一个核心层来优化其设计。

使用多台分布层交换机的另一个原因是，当连接至单一分布层的接入层交换机数量超过了网络设计师的性能目标时。在一个模块化和可扩展的设计中，您可以将多个分布层布置在一个机房，用于数据中心、WAN 连接或者互联网边缘服务。

在多个分布层交换机紧密相邻以及光纤提供高带宽互连能力的环境中，核心层可降低网络复杂度，N 个分布层的链接数从 N * (N-1) 减少到 N 个，如下列两图所示。

图 6　　含核心层的局域网拓扑图

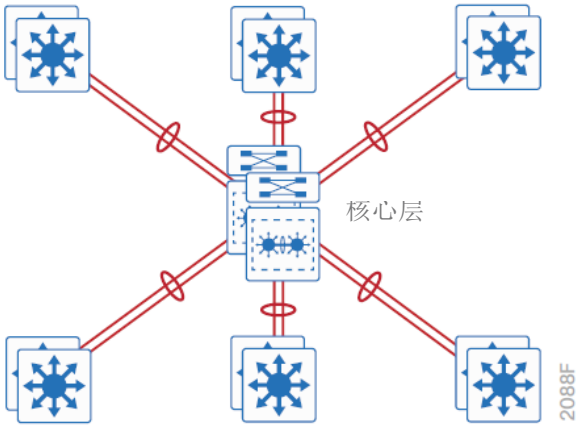
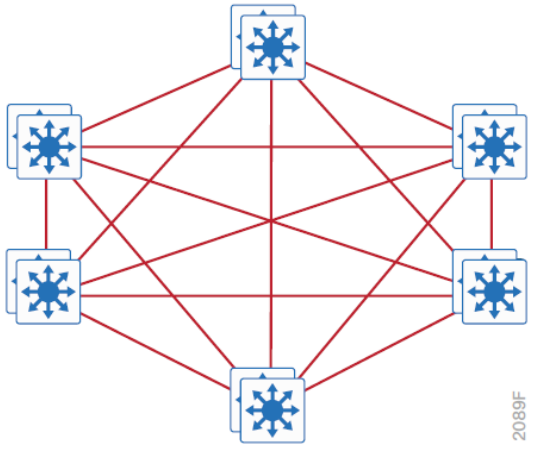


图7　　不含核心层的局域网拓扑图



局域网的核心层是可扩展网络的一个关键部分，然而它却是最简单的设计之一。分布层提供故障和控制域，而核心代表它们之间 24x7x365 的不间断连接性，这是现代商业环境中组织必备的，其中与资源的连接性对开展业务至关重要。

当使用了思科 Catalyst 6800 或 6500 系列交换机时，Catalyst VSS 第三层核心设计是传统设计的首选替代选项，传统设计通常使用两个独立配置和管理的平台。通往和来自核心的连接仅在第三层，它提升了恢复能力和稳定性。

核心层平台

用作园区核心层平台的首选思科交换机为：

- 思科 Catalyst 6807-XL 交换机，采用思科 Catalyst 6500 管理引擎 2T
- 思科 Catalyst 6500 系列交换机，采用思科 Catalyst 6500 管理引擎 2T

园区有线局域网核心另有一个选项可供选择，提供替代的密度和功能：

- 思科 Nexus 7000 系列交换机

园区有线网络设计选项

当您在园区局域网中从单一交换机扩展至一个完整的三层园区网络时，网络可靠性就显得愈发重要，因为网络中断可能会影响到更多的用户人群，涉及到更大的工作场所且具有更大的经济重要性。为了缓解对于网络资源不可用的担忧，园区设计包含额外的恢复能力选项，例如冗余链路、交换机和交换机组件。在传统的多层园区设计中，新增的恢复能力会以配置复杂性为代价，其中大部分复杂性产生于园区局域网的接入层与汇聚层的交汇处。

分布层的主要功能在于汇聚给定建筑或园区中的接入层交换机。分布层在接入层的第二层域和第三层域之间提供一个边界，它可提供通往网络其余地方的路径。

这一边界为局域网提供两大关键功能。在第二层一侧，分布层为生成树协议 (STP) 创建一个边界，从而限制第二层故障的传播。在第三层一侧，分布层提供一个逻辑点，在它进入网络时汇总 IP 路由信息。该汇总减少了 IP 路由表，可实现更轻松的故障排除，同时减少了协议开支，实现更快的故障恢复。

传统多层园区分布层设计

传统局域网设计使用一个多层方案，其中第二层从接入层到分布层，那里存在着第三层边界。从接入层到分布层的连接可形成一个无环路或者环路设计。

在传统网络设计中，分布层有两台独立交换机用于恢复能力。推荐您将第二层虚拟 LAN (VLAN) 限制在单一配线间或接入上行链路对中，以减少或消除拓扑环路，这是 STP 必定会拦截的，也是局域网中常见的故障点。将 VLAN 限制到单一交换机可提供一个无环路设计，但这确实限制了网络灵活性。

为了给传统设计中的 VLAN 创建一个弹性 IP 网关，您必须使用第一跳冗余协议，它可为 VLAN 提供具有一致的 MAC 地址和网关 IP 的主机。热待机路由协议 (HSRP) 和虚拟路由器冗余协议 (VRRP) 是最常见的网关冗余协议，但它们仅允许主机从其中一个接入上行链路向外发送数据至分布层，同时需要为每台汇聚交换机另行配置，才能允许您在上行链路分配 VLAN。网关负载均衡协议 (GLBP) 通过平衡来自多个上行链路主机的负载，确实为退出接入层的流量提供更大的上行链路利用率，但是您只能在无环路拓扑中使用它。

所有这些冗余协议均要求您微调默认的时间设置，以允许次秒级网络融合，这会影响交换机 CPU 资源。

有些组织要求同一第二层 VLAN 延伸到多个接入层配线间，以支持一个应用程序或服务。环路设计导致生成树阻塞链路，这减少了网络其余部分的带宽，并可引起网络融合变慢。其效率低下和潜在错误配置的增加促使网络工程师寻找更具吸引力的替代方案。

图 8　　每台接入交换机拥有一个 VLAN 的传统无环路设计

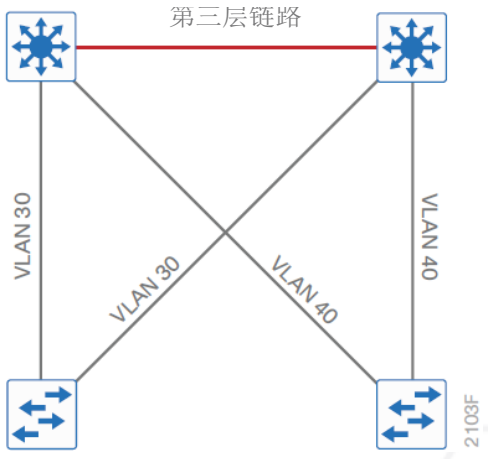
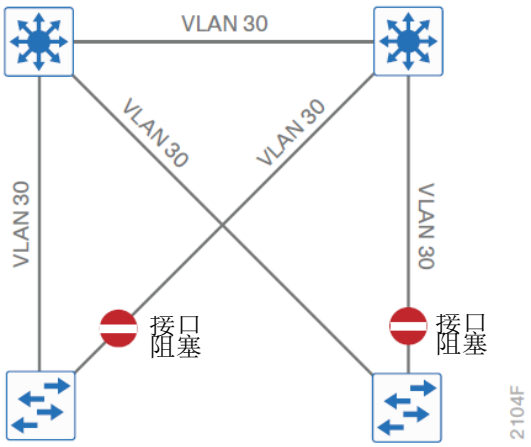


图 9　　具有横跨接入交换机的 VLAN 的传统环路设计



路由访问分布层设计

在接入层和分布层设计的另一个方案中，您可以使用第三层一直到接入层。这种设计的好处是，您消除了生成树环路并减少了协议，因为 IP 网关现在成了接入交换机。因为没有了生成树阻塞链路，您可以使用通往接入层的两个上行链路，同时为用户增加有效的带宽。

路由接入层设计的挑战在于，第二层域被局限在单一接入配线间，这限制了需要第二层连接（延伸到多个接入配线间）的应用程序灵活性。

简化型分布层设计

可以应对第二层接入需求并避免传统多层园区复杂性的一个替代方案叫做*简化型分布层设计*。该设计使用多个物理交换机充当单一逻辑交换机，例如交换机堆叠或者一个 VSS，或者次优选的单一、高冗余物理交换机。这种设计的一项优势在于将对生成树的依赖降至最低，同时从接入层至分布层的所有上行链路都是激活且通行的流量。即便在分布式 VLAN 设计中，您也因为环路拓扑而消除了生成树阻塞的链路。通过使用 EtherChannel 到双宿上行链路接入层，您将减少对生成树的依赖。这是这种设计的一个关键特征，同时如需获得额外的带宽，您可以平衡多达 8 个链路的负载。与此同时，EtherChannel 中的多个链路较之于单一的独立链路拥有更出色的性能特征。

图 10　　每台接入交换机有一个配 VLAN 的简化型分布层设计

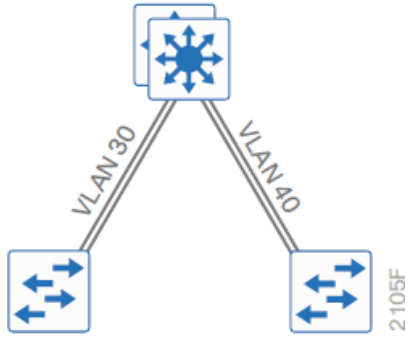
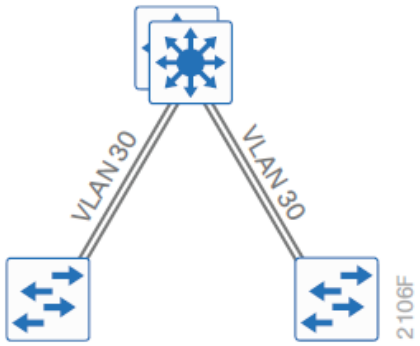


图 11　　VLAN 横跨接入交换机的简化型分布层设计



EtherChannel 是可以使用一个控制平面协议来管理捆绑包物理成员的逻辑接口。运行一个信道协议要优于使用强制开机模式，因为信道协议对编入信道的接口执行一致性检查，并可保护系统，防范配置不一致。思科 Catalyst 交换机同时提供端口汇聚协议 (PAgP) 和链路汇聚协议 (LACP)，前者是一种广泛部署的思科设计的协议，后者基于 IEEE 802.3ad。

简化型分布层设计还有其它若干优势。您不再需要 IP 网关冗余协议，例如 HSRP、VRRP 和 GLBP，因为默认 IP 网关现在在单一逻辑接口上，同时分布层交换机提供了恢复能力。另外，当发生故障时，既然网络不再依赖于生成树来疏通链路，它将更快地融合，因为 EtherChannel 在上行捆绑中的链路之间提供快速的次秒级故障转移。

从分布层至接入层的网络拓扑从逻辑上讲，属于中心辐射型拓扑，它降低了设计和故障排除的复杂性。这种中心辐射型拓扑设计为分布层中的 IP 组播提供更高的运营效率，因为现在有了单一逻辑指定路由器，从而将 IP 组播数据包转发至接入层中的一个给定 VLAN。

最后，通过使用单一逻辑分布层设计，需要管理的盒子更少了，这减少了耗费在持续调配和维护上的时间。

即时接入设计

当您使用思科 Catalyst 6500 或 6800 系列交换机并将之配置成分布层中的一个 VSS，或者作为一个折叠核心和分布层时，则有另一种设计选项可进一步简化网络部署和管理。以太网接入交换机可供部署实现即时接入功能并连接至 VSS 对。即时接入交换机发起通信，这允许它们与 VSS 分布层关联及合并，从而被当作远程线卡。

在即时接入设计中，所有配置，甚至包括软件升级都是由即时接入分布层来调用，而无需将接入端口配置为单独的交换实体。这种选项的配置属于最简单的之一，因为无需在接入交换机设备和分布层之间进行通常很复杂的手动配置。它还将以前为分布层中设备所独有的功能提供给接入层端口。

用于有线局域网的 Meraki 云网络

思科 Meraki 为部署有线局域网提供了一个云计算型的选项。在这种云计算型架构中，交换机通过互联网连接并通过云计算型管理系统进行管理。Meraki 控制器位于公共云中，同时每个企业自行管理其 Meraki 私有云。这种集中化的云计算型管理使网络管理员在有互联网接入时可以随时随地更轻松管理他们的网络。

思科 Meraki 有线网络基础设施包括下列组件：

- MS220 第二层和 320 第三层接入交换机
- MS420 汇聚交换机
- Meraki 云管理

类似的设计方法适用于使用思科 Meraki 交换机的有线局域网。其关键区别在于将思科 Meraki 云计算型管理系统，而不是传统的现场型管理系统用于日常配置和管理。其功能特性并非与现场型产品完全一致，因此请参考在线产品文档，以便理解哪些交换机具备适合您的部署的功能特性。

园区无线局域网设计基础知识

园区 WLAN 为员工提供无所不在的数据和语音连接、为访客提供无线互联网接入，同时为物联网设备提供连接。无线用户无论位于组织内的任何位置（大型园区或远程站点），都将能够在连接到语音、视频和数据服务时获得相同的体验。

园区 WLAN 的优势包括：

- **通过安全、不受位置限制的网络接入提高工作效率**——切实提高工作效率并改善通信。
- **提供额外的网络灵活性**——对难以布线的位置实施无线连接，且无需高昂的构建成本。
- **提供具有成本效益的部署**——在整个无线架构内采用虚拟化技术。
- **易于管理和运营**——从单一管理平台集中控制分布式无线环境。
- **支持即插即用部署**——当接入点连接至提供支持的有线网络时，可实现自动调配。
- **弹性、容错设计**——任务关键型环境中的可靠无线连接，包括完整的射频 (RF) 频谱管理。
- **支持无线用户**——自带设备 (BYOD) 设计模型。
- **能够高效传输组播流量**——支持多种群组通信应用，如视频和一键通功能。

基础设施

园区 WLAN 是围绕这些主要组件而建立的：

- 思科 WLAN 控制器
- 思科轻量级接入点
- 思科 Prime 基础设施 (PI)
- 思科移动服务引擎 (MSE)/思科互联移动体验 (CMX)

思科 WLAN 控制器

园区 WLAN 是一种基于控制器的无线设计，它通过使用思科 WLAN 控制器简化了网络管理，从而对无线接入点的配置和控制实现集中化。此方法使无线局域网 (WLAN) 能够成为一个智能的信息网络，并支持各种高级服务。以下是基于控制器设计的一些优势：

- **降低运营支出**——实现适合轻量级接入点的零接触配置；帮助轻松设计信道和功率设置以及实时管理（包括确定任何 RF 覆盖盲区，以优化 RF 环境）；提供跨移动组内不同接入点的无缝移动性；以及显示网络的整体视图，以便支持有关扩展、安全和整体运营的决策。
- **优化结果**——通过在初步 WLC 配置期间实施最佳实践，实现 WLAN 控制器和总体无线网络的简化配置。
- **提高投资回报**——实现无线局域网控制器的虚拟化实例（仅限于虚拟无线 LAN 控制器），从而充分利用虚拟化投资来降低总体拥有成本。
- **利用优化设计简化扩展**——通过支持适合于园区环境的集中化（本地模式）设计，以及适合于精益远程站点的思科 FlexConnect 或融合接入设计，使网络实现良性扩展。
- **支持高可用性状态切换**——在无线局域网控制器出现故障时，确保无线客户端设备的连接不会中断。

思科无线局域网控制器负责控制整个系统范围的 WLAN 功能，例如安全策略、入侵防御、RF 管理、服务质量 (QoS) 和移动性。它们与思科轻量级接入点配合使用，从而支持业务关键型无线应用。从语音和数据服务到位置跟踪，思科无线局域网控制器都能为网络经理构建可扩展的安全无线网络提供所需的可控性、可扩展性、安全性和可靠性。

下表汇总了本指南内提到的思科无线局域网控制器。

表 4　　WLAN 控制器平台

平台	部署模式	首选拓扑	最大接入点数	最大客户端数	控制器吞吐量
思科 8540[1]	集中化或者 FlexConnect	大型单个或多个站点	6,000	64,000	40 Gbps
思科 5520	集中化或者 FlexConnect	大型单个或多个站点	1,500	20,000	20 Gbps
思科 2504	集中化	小型本地控制器站点	75	1,000	1 Gbps
思科 Flex 7510[2]	FlexConnect	大量小型站点	6,000	64,000	1 Gbps
Catalyst 3850[3]	融合接入	小型站点	每个堆栈 100	每个堆栈 2,000	每台交换机 40 Gbps
Catalyst 3650	融合接入	小型站点	每个堆栈 50	每个堆栈 1,000	每台交换机 40 Gbps
Catalyst 4500-E，采用管理引擎 8-E	融合接入	小型站点	每个管理引擎 100	每台交换机 2,000	40 Gbps (20 Gbps 背板)
思科 vWLC	FlexConnect	中等数量的小型站点	200	2,000	500 Mbps

备注：

1. 思科 8540 和 5520 WLCs 需要思科统一无线网络 (CUWN) (AireOS) 8.1 及更高版本。

2. 所提到的吞吐量为流量终止于思科 Flex 7510 WLC 的吞吐量。

3. Catalyst 3850 和 3650 可扩展性在思科 IOS XE 3.7.1 版本中首次推出。

由于软件许可证的灵活性允许您随业务需求的变化添加额外的接入点，因此您可以选择能长期满足您的需求的控制器，仅在需要时购买增量接入点许可证。

思科轻量级接入点

在思科统一无线网络架构中，接入点是*轻量级*的。这意味着它们不能独立于 WLAN 控制器。接入点与 WLAN 控制器通信时，会下载控制器中的配置，并同步其软件或固件映像。这些接入点可转化为自主运营，但是自主运营要求对每个接入点单独管理，因此不在本指南探讨的范围之内。

思科轻量级接入点与思科无线局域网控制器协同工作，可在将无线设备连接至局域网的同时，支持同步数据转发和通风监控功能。园区 WLAN 提供稳健的无线覆盖，具有九倍于 802.11a/b/g 网络的吞吐量。

下表汇总了本指南内讨论的接入点。

表 5　　思科 Aironet 接入点

	1700 系列	2700 系列	3700 系列
最适合于	中小型网络	高密度、中型和大型网络	任务关键型、高密度、大型网络
功能	802.11ac 第一阶段射频、3x3 多输入、多输出 (MIMO)、两空间流	802.11ac 第一阶段射频、3x4 MIMO、三空间流	802.11ac 第一阶段射频、4x4 MIMO、三空间流
天线	仅内部	内部和外部	内部和外部
支持模块	无	无	无线安全模块 (WSM)
HDX 支持	否	是	是
CleanAir	是 (express)	是	是
ClientLink	否（基于标准的 TxBF）	是 (3.0)	是 (3.0)
吞吐量	867 Mbps	1.3 Gbps	1.3 Gbps

对两项关键技术的支持将选用于园区 WLAN 部署的接入点区别开来：

- **思科 CleanAir 技术**——为 IT 经理提供对无线频谱的可视性，以便管理 RF 干扰，并防止意外停机。思科 CleanAir 可为 802.11 网络提供性能保障。这种芯片级智能创建一种自修复、自优化无线网络，可缓解无线干扰的影响。
- **802.11ac**——IEEE 802.11ac 第一阶段 (Wave 1) 规格可显著增强无线网络性能。

移动服务引擎/互联移动体验

思科 MSE/思科 CMX 通过提高网络可视性、基于位置的定制移动服务和加强无线安全，是一个有助于组织提供创新型移动服务和改进业务流程的平台。

MSE/CMX 有如下外形可供选择：

- MSE 3355 或 3365 设备
- 运行 VMware ESXi 5.1 或更高版本的虚拟机

目前有两个版本的 MSE/CMX，名称略有不同。*MSE 8.0* 指的是两个 MSE 平台，运行 CMX 软件 8.0 版。采用 CMX 10.1 及更高版本，这个名称已改为 *CMX*。

下表汇总了不同版本的 MSE/CMX 提供的服务。

表 6　　MSE 8.0 和 CMX 10.1 提供的服务

服务	MSE 8.0	CMX 10.1
基于位置的服务	是	是
思科无线入侵防御系统 (wIPS)	是	否（已规划）
CMX 分析	位置和在线状态	仅位置（在线状态已规划）
CMX 互联	是	是
CMX 移动应用服务器和 SDK	是	否（已规划）
移动“管家”	是	否

无线设计模型

本指南描述了下列三种设计模型及其推荐用途：

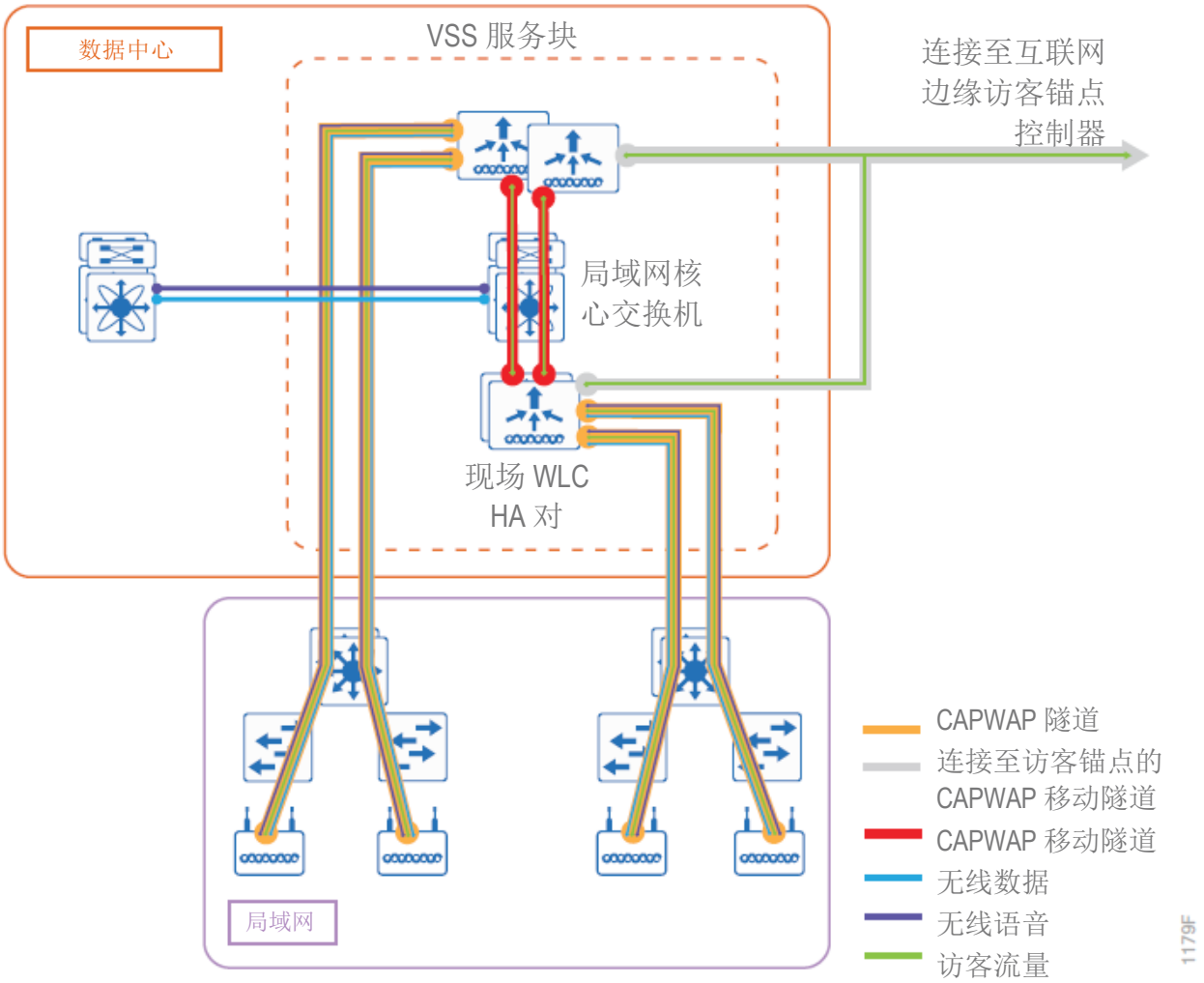
- 集中化（本地模式）设计模型
- FlexConnect 设计模型
- 融合接入设计模型

此外，另有一个思科 Meraki 云计算型选项。

集中化（本地模式）设计模型

一种集中化设计模型，也称为*本地模式设计模型*，主要推荐用于大型站点部署。集中化设计的优势包括 IP 地址管理、简化型配置和故障排除以及大规模漫游。在集中化设计模型中，WLAN 控制器和接入点均位于同一个站点内。您可以将无线局域网控制器连接到数据中心服务块、园区核心之外的独立服务块或者局域网分布层。无线局域网客户端和局域网之间的无线流量是通过使用控制器和接入点之间的无线接入点控制和调配 (CAPWAP) 协议进行传输的。

图 12　　本地模式设计模型



集中化架构使用控制器作为管理第二层安全和无线网络策略的单一点。它还支持以统一和协调的方式将服务应用于有线和无线流量。

本地模式设计模型不仅具有思科统一无线网络方法的传统优势，还满足以下客户需求：

- **无缝移动性**——支持快速漫游整个园区，以便用户能够在不同楼层和邻近建筑行走而不停更换子网时，始终连接到会话。
- **支持富媒体功能**——采用呼叫准入控制增强语音稳定性，采用思科视频流技术加强组播支持。
- **集中式策略**——通过使用防火墙以及应用检测、网络访问控制、策略实施和准确流量分类支持智能检测。

如果某站点符合以下**任何**一点，则您应在该站点考虑本地部署控制器：

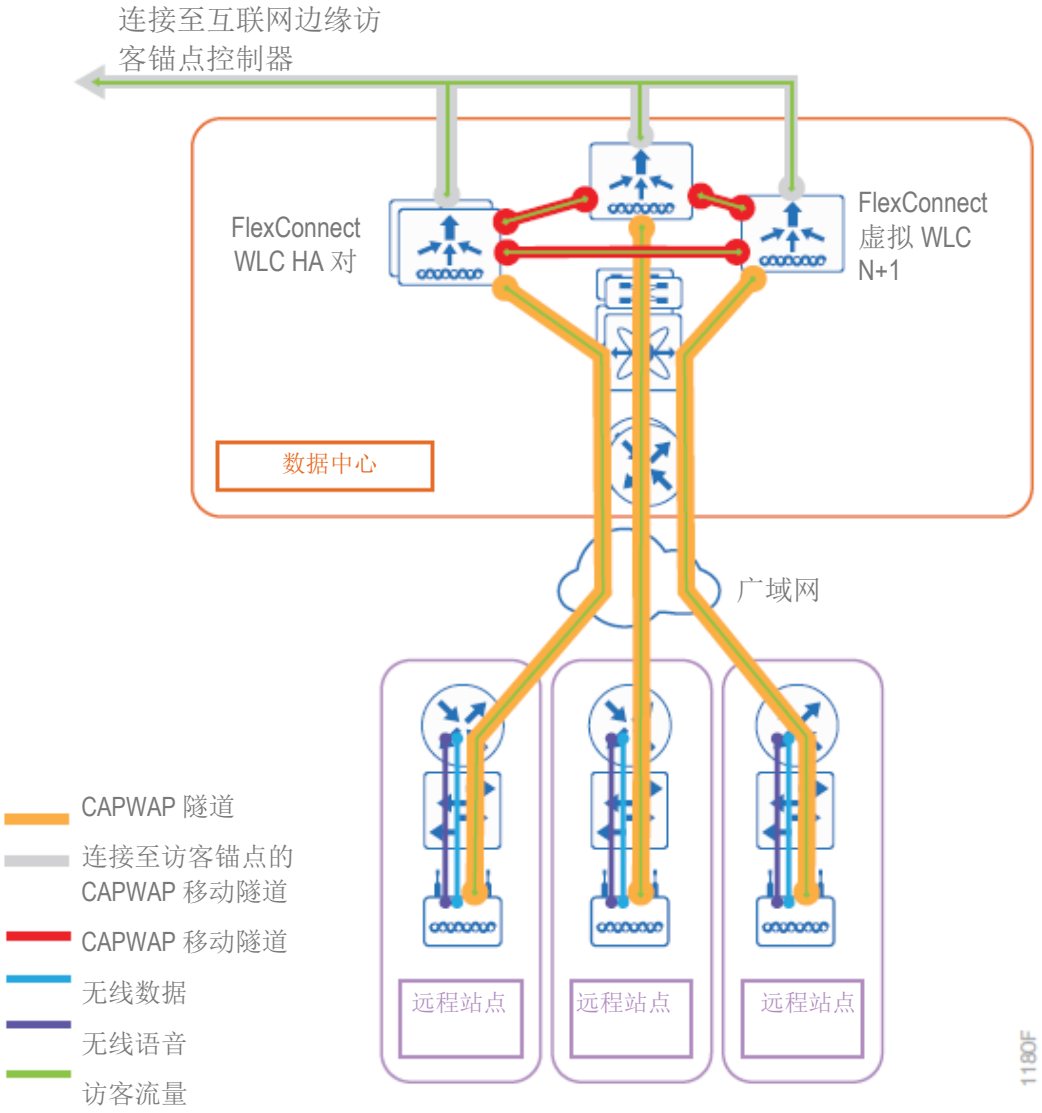
- 该站点有数据中心。
- 该站点有局域网分布层。
- 该站点有超过 100 个接入点。
- 该站点往返拟用共享控制器的广域网延迟超过 100 毫秒。

用于大型集中化（本地模式）设计的推荐平台是思科 8540 和 5520 无线局域网控制器，这是由于它们的可扩展性和所支持的功能。对于较小的站点，您可以部署思科 2504 WLAN 控制器作为站点内的一个本地控制器。

思科 FlexConnect 设计模型

思科 FlexConnect 是一种无线解决方案，主要用于包含连接至一个中央站点的多个小型远程站点（分支机构）的部署。FlexConnect 提供一个极具性价比的解决方案，使组织实现从总部通过广域网配置和控制远程站点接入点，而无需在每个远程站点部署控制器。运行于 FlexConnect 模式中的思科接入点可以切换其本地有线接口的客户端数据流量，还可以使用 802.1Q 中继分割多个 WLAN。中继的本地 VLAN 用于接入点和控制器之间的所有 CAPWAP 通信。此操作模式称为 *FlexConnect 本地交换*，也是本指南中介绍的操作模式。

图 13　　思科 FlexConnect 设计模型



思科 FlexConnect 还可将流量回传至集中式控制器，该控制器可用于无线访客接入。您可以使用共享控制器对或专用控制器对部署思科 FlexConnect。

在共享控制器模型中，本地模式和 FlexConnect 配置的接入点同时共享一个通用控制器。共享控制器架构要求无线局域网控制器同时支持 FlexConnect 本地交换和本地模式。在本指南中，同时支持两者的无线局域网控制器为思科 8500、5500 和 2500 系列无线控制器。

如果您满足下列所有要求，则您可能能够使用共享部署：

- 您在同一个站点已经有了一个本地模式控制器对作为您的 WAN 汇聚。
- 该控制器对具备足够的额外容量，可支持思科 FlexConnect 接入点。
- 所需的 FlexConnect 群组数量与控制器对的能力相匹配。

如果您不符合共享控制器的要求，则可以部署思科 Flex 7500 系列云控制器，它们是专门针对 FlexConnect 部署而设计的。另外，您也可以部署思科 8500 或思科 5500 系列无线控制器。如需最高的恢复能力，可在 HA SSO 中部署一对控制器。另外如有需要，您也可以部署 N+1 高可用性，从而提供站点间恢复能力。

您也可以通过使用思科 2500 系列 WLAN 控制器或者思科 vWLC，运用 N+1 高可用性 (HA) 模型配置的双弹性控制器。

如果在某个站点满足以下所有特点，则您应当在该站点考虑部署思科 FlexConnect：

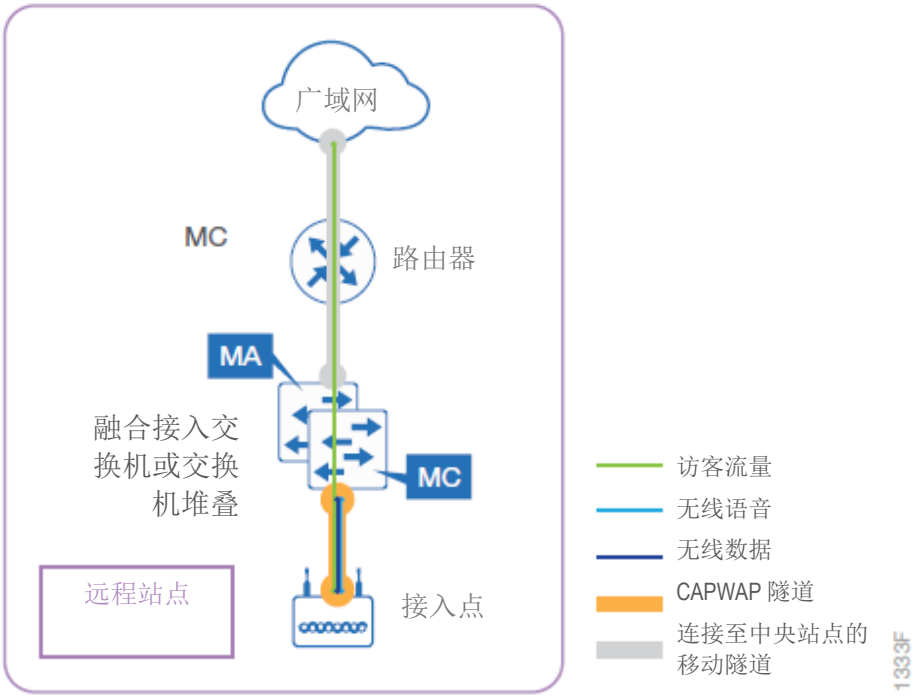
- 该站点局域网是单个接入层交换机或交换机堆栈。
- 该站点的接入点数量少于 50 个。
- 该站点是连接至一个中央位置的众多小型远程站点之一。
- 该站点往返共享控制器的广域网延迟少于 100 毫秒。

融合接入设计模型

思科融合接入是主要用于远程站点部署的无线解决方案，要么是单一小型站点，要么是连接至一个中央位置的多个小型站点。凭借融合接入解决方案，WLAN 控制器功能得以集成到思科 Catalyst 接入层交换机之内。这为在远程站点部署一个独立的本地 WLAN 控制器或部署 FlexConnect 提供了一个替代方案。

融合接入设计模型允许从通过 CAPWAP 隧道（从交换机端口延伸到接入点）直接连接到交换机的接入点终止无线流量。从本地终止无线流量可针对交换机上的这类流量提供更高的可扩展性和可视性，同时为有线和无线设备提供一个策略实施的单一点。

图 14　融合接入设计模型



对于融合接入设计模型，思科 Catalyst 3850 或 3650 系列交换机堆叠（或者思科 Catalyst 4500 管理引擎 8-E）实施如下无线控制器功能：

- 移动代理——从接入点终止 CAPWAP 隧道并保留无线客户端数据库。
- 移动控制器——在子域之内或之间管理移动性。同时还管理无线电资源管理 (RRM)、无线侵入防御系统等。

依托 Catalyst 3850 和 3650 平台，可在单一交换机堆叠中支持多达 9 台交换机。Catalyst 4500-E 模块化交换机平台支持与管理引擎 8-E 模块的无线集成。

用于 WLAN 的思科 Meraki 云网络选项

思科 Meraki 为思科统一无线网络架构提供一个云计算型的替代方案。在云计算型架构中，接入点通过互联网连接至一个云计算型控制器用于管理。思科 FlexConnect 控制器位于组织的私有数据中心，而 Meraki 控制器位于公共云，同时各企业自行管理各自的 Meraki 私有云，从这个意义上来讲，这与思科 FlexConnect 模型不同。这种集中化的云计算型管理使网络管理员在有互联网接入时可以随时随地更轻松管理他们的网络。

思科 Meraki 无线网络基础设施包括如下组件：

- MR 系列云管理无线接入点
- Meraki 云管理

思科 Meraki MR 系列接入点

思科 Meraki 提供一系列不同的接入点，它们仅与思科 Meraki 云配合使用。

技术小提示

思科 Aironet 并不与思科 Meraki 云计算型控制器配合使用。

下列室内思科 Meraki MR 系列接入点型号支持 802.11ac：

- Meraki MR34 是一种双频（5 GHz 和 2.4 GHz）802.11ac 接入点，专为要求最高性能和最高容量 WLAN，以及园区部署内最高密度的企业环境而设计。MR34 的特色是支持三空间流的 3x3 MIMO 设计，实现高达 1.75 Gbps 的最大理论数据速率。
- Meraki MR32 是一种双频（5 GHz 和 2.4 GHz）、一般用途 802.11ac 接入点，专为要求高性能和高容量 WLAN、以及园区部署内高密度的企业或零售环境而设计。MR32 的特色是支持两空间流的 2x2 多输入、MIMO 设计，实现高达 1.2 Gbps 的最大理论数据速率。

上述 Meraki MR 系列接入点拥有第三双频射频，专用于安全性 (WIDS/wIPS) 和 RF 管理。第三射频还可支持数据接收信号强度 (RSSI)，以实现更大准确度和确定性的位置跟踪。MR34 和 MR32 也支持带转向和波束成形。MR32 包含低功耗蓝牙 (BLE) Beacon 扫描功能。

无线设计考虑要点

高可用性

随着更多具有关键功能的设备采用无线介质，无线基础设施的高可用性正变得日益重要。实时音视频和文本通信依赖于企业无线网络，同时对零停机时间的预期正在成为常态。无线网络中断的负面影响与有线网络中断具有同样的冲击力。在无线基础设施之内实施高可用性牵涉到部署在整个网络基础设施中的多种组件和功能，其本身就必须针对高可用性而设计。本部分讨论对于实施无线控制器平台特定的高可用性。平台级冗余指的是当通往站点内一个及以上物理 WLAN 控制器平台的连接丢失时维持无线服务的能力。

本设计指南之内所讨论的高可用性方法如下：

- 高可用性 SSO
- N+1 高可用性
- Catalyst 交换机堆叠恢复能力
- WLAN 控制器链路汇聚

高可用性 SSO

思科 AireOS 支持接入点状态切换和客户端状态切换。这两个功能统称为高可用性 SSO *(HA SSO)*。HA SSO 对于简单性和有效性来说均是提供高可用性的首选选项。通过使用具有成本效益的 HA SSO 许可模型，思科无线部署可通过在无线局域网控制器中断期间将控制器恢复时间控制在次秒级，从而提高无线网络的可用性。此外，HA SSO 允许将弹性无线局域网控制器以具有成本效益的方式许可用作备用弹性控制器，实现自动从其配对的主无线局域网控制器继承其接入点许可证计数。为此，需要使用为思科 5500、7500 和 8500 系列无线局域网控制器提供的 HA SKU 购买备用弹性控制器。

主无线局域网控制器的配置和软件升级自动同步到弹性备用无线局域网控制器。

N+1 高可用性

您可以使用 N+1 HA 架构，以便为单一站点内或者地理上分离站点之间的无线局域网控制器提供冗余，同时总体部署成本更低。它通常与 FlexConnect 架构一同部署，以便为远程分支机构提供跨数据中心的高可用性。您可以使用单一备用 WLAN 控制器，以便为多个主 WLAN 控制器提供备份。不支持将 HA SSO 功能用于 N+1 HA。当主控制器失效时便会重启 AP CAPWAP 状态机。

凭借 N+1 HA，无线局域网控制器相互独立，且不会在它们的任何接口上共用配置或 IP 地址。每个 WLC 必须独立管理，可以运行不同的硬件，也可跨越广域网链路部署在不同的数据中心。

推荐您（但不要求）在所有 WLC 之间运行用于 N+1 HA 的相同软件版本，以便在接入点与备用控制器之间建立 CAPWAP 会话时减少停机时间。您可以凭借 N+1 HA 优先配置接入点。主控制器上的高优先级接入点始终会最先连接至备用控制器，即便它们必须挤出低优先级接入点。当主 WLC 恢复运行时，如果接入点退回选项被激活，则接入点自动从备用 WLC 退回到主 WLC。

您可以将一个 HA-SKU 辅助控制器配置为一个备用控制器，以实现 N+1 HA。HA-SKU 唯一设备标识符可实现该硬件支持最大数量的接入点。您不能结合 HA SSO 来配置 N+1 辅助 HA-SKU。它们是相互排斥的。

Catalyst 交换机堆叠恢复能力

Catalyst 3850 和 Catalyst 3650 系列交换机与思科 IOS 软件 SSO 一起支持 StackWise 技术，从而实现在一个交换机堆叠内提供恢复能力。支持 Catalyst 交换机堆叠恢复能力，用于融合接入交换机：

- Catalyst 3850 系列交换机——IOS XE 软件 3.2.0SE 及更高版本
- Catalyst 3650 系列交换机——IOS XE 软件 3.3.0SE 及更高版本

Catalyst 3850 系列和 Catalyst 3650 系列交换机分别支持思科 StackWise-480 和 StackWise-160 堆叠端口。基于铜缆的思科 StackWise 布线连接交换机，以实现大约 480 Gbps 的堆叠带宽用于 Catalyst 3850 系列，以及 160 Gbps 用于 Catalyst 3650 系列。

凭借 StackWise 技术，数量多达 9 台的交换机堆叠相当于单一交换单元，它由一台由成员交换机选出的“活动”交换机进行管理。活动交换机自动在堆叠内选择一个备用交换机。活动交换机创建并更新所有交换/路由/无线信息并不断地与备用交换机同步该信息。如果活动交换机出现故障，则备用交换机充当活动交换机并继续让堆叠保持运行。接入点在活动至备用状态切换期间继续保持连接。无线客户端被取消关联，同时需要重新关联和重新验证。因此，恢复时间取决于有多少无线客户端需要重新关联和重新验证，以及验证的方法。为了在 Catalyst 3850 和 3650 系列交换机上激活恢复能力，并不需要配置命令——它在交换机通过堆栈电缆连接时默认激活。

WLAN 控制器链路汇聚

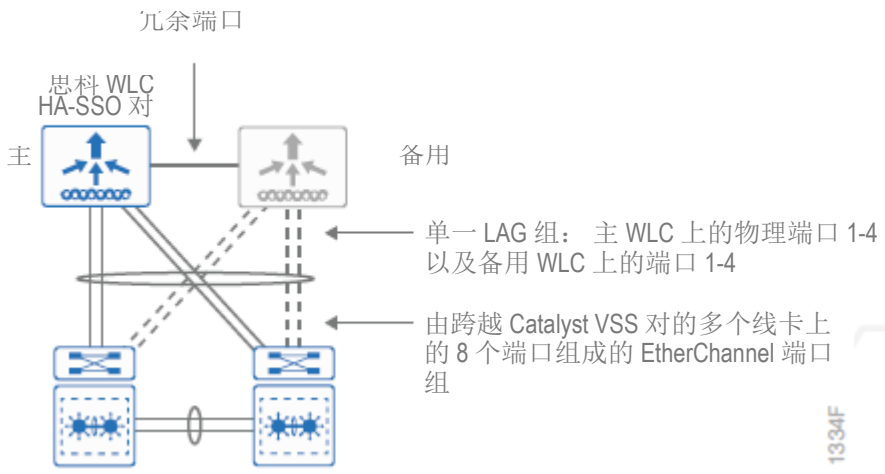
大多数思科无线控制器设备具有多个 1 千兆位或 10 千兆位物理以太网端口。在典型部署中，有一个或更多 WLAN/服务集标识符 (SSID) 映射到一个动态接口，而动态接口随后被映射到一个物理端口。在集中化设计中，无线流量在整个网络基础设施回传并在物理端口上终止。随着每个 WLAN 使用单一物理端口，每个 WLAN 的吞吐量被限制为该端口的吞吐量。因此，一种替代方法是跨越分布系统端口部署链路汇聚 (LAG)，将它们植入单一高速接口。

当激活 LAG 时，无线控制器即动态管理端口冗余并透明地平衡接入点负载。LAG 也简化了控制器配置，因为不再有必要为每个接口配置主端口和辅助端口。如有任何控制器端口出现故障，流量便自动迁移至其它端口中的一个。只要有至少一个控制器端口正常运行，无线控制器就会继续运行，接入点就会与网络保持连接，同时无线客户端继续发送和接收数据。

LAG 需要一个 EtherChannel 端口组配置到附加的 Catalyst 交换机上。EtherChannel 端口组可以跨越 Catalyst 交换机上的多个线卡，或者跨越 Catalyst 交换机 VSS 配置中的交换机进行配置，实现额外的冗余。当进行跨交换机配置时，则称之为一个*多机箱 EtherChannel*。

下图是对 Catalyst 交换机 VSS 对的高可用性配置中无线控制器链路汇聚的示例。

图 15 *链路汇聚示例*



推荐设计是将活动和备用 WLC 的端口分散在 VSS 对内两台交换机之间。这种设计可将跨越 VSS 对中 Catalyst 交换机之间的虚拟交换机链路正常（无故障）运行期间的流量降至最低，因为活动和备用 WLC 上均有端口连接至两台交换机。当 VSS 对之内出现交换故障时，这种设计还避免了从活动 WLC 至备用 WLC 的状态切换。然而，当 VSS 对内部出现交换故障时，连接至 WLC 的端口数量便会减少一半。

技术小提示

您应当无条件地将 Catalyst 设置成 LAG （开启模式），因为该无线控制器不支持 LACP 或者 PAgP。

下表汇总了各种控制器对高可用性的支持。

表 7 *高可用性功能支持*

思科 WLC 型号	HA SSO	N+1 HA	堆叠冗余	LAG
8540	是	是	—	是
5520	是	是	—	是
2504	否	是	—	是
Flex 7510	是	是	—	是
vWLC	否	是	—	通过 VMware
Catalyst 3850 及 3650	否	—	是	是（交换机上行链路）
Catalyst 4500-E，采用管理引擎 8-E	否	—	双管理引擎	是（交换机上行链路）

组播支持

随着智能手机、平板电脑和 PC 加入我们日常生活方方面面的无线网络，视频和语音应用继续发展。在每种无线设计模型中，用户习惯的有线网络中的组播支持现可通过无线获得。要支持高效交付特定的一对多应用，例如视频和一键通组通信，需要使用组播。通过将组播支持扩展到超出园区和数据中心，移动中的用户现在可以使用基于组播的应用。

这种园区无线局域网设计通过使用组播-组播模式支持现场控制器的组播传输，该模式使用组播 IP 地址，从而更有效地将组播流传输至拥有订用特定组播组的无线用户的接入点。在本指南中，通过使用思科 2500、5500 和 8500 系列无线局域网控制器，可支持组播-组播模式。

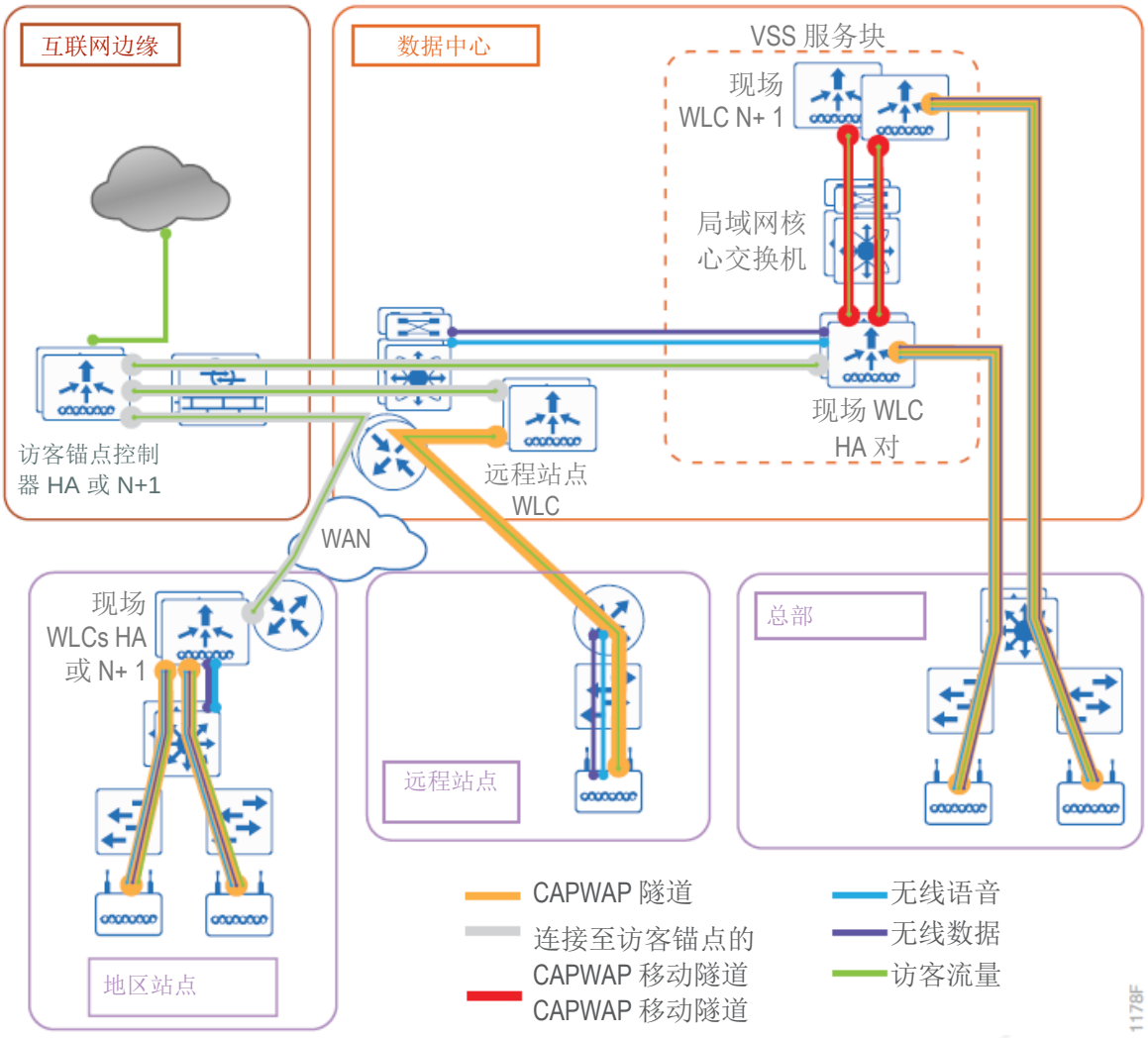
使用思科 Flex 7500 系列云控制器或思科 vWLC 的远程站点在本地交换模式下使用思科 FlexConnect，也可受益于使用基于组播的应用。远程站点组播利用基础广域网和局域网对组播流量的支持。当与使用本地交换的 FlexConnect 模式下的接入点结合时，组播流用户直接通过广域网或局域网网络获得服务，不会对无线局域网控制器带来额外开销。

无线访客

将现有园区有线和无线基础设施用于访客访问，为访客和承包商提供方便、具有成本效益的互联网接入方式。无线访客网络提供以下功能：

- 采用 Web 身份验证访问控制，通过开放式无线安全集标识符 (SSID) 为访客提供互联网接入
- 通过授权的内部用户支持为每个访客创建临时身份验证凭据
- 使访客网络上的流量与内部网络分离，以防止访客访问内部网络资源
- 支持集中化的融合接入和思科 FlexConnect 设计模型

图 16　　无线架构概述



如果您的整个组织只有单个控制器对，并且该控制器对与互联网边缘防火墙连接到同一个分布层交换机，则您可以使用共享部署。

在共享部署中，分布层交换机上会创建一个 VLAN，以将访客流量从无线局域网控制器逻辑连接至隔离区 (DMZ)。DMZ 访客 VLAN 将不具备关联的第 3 层接口或交换机虚拟接口。因此，访客网络中的每个无线客户端将使用互联网边缘防火墙作为其默认网关。

如果不满足共享部署的要求，您可以使用思科 5500 或思科 2500 系列无线局域网控制器来部署专用访客控制器。控制器直接连接至互联网边缘 DMZ，来自组织中所有其他控制器的访客流量都将传输至该控制器。其它控制器可提供所述访客锚定服务，但不在本指南探讨的范围之内。

在共享和专用访客无线设计模型中，互联网边缘防火墙会限制来自访客网络的访问。访客网络仅能连接互联网和内部 DHCP 和 DNS 服务器。

大多数组织的 IT 部门在允许访客访问互联网之前，会选择首先进行访客无线用户身份验证。有时伴随着这个步骤而来的是，访客用户在接入互联网之前必须阅读并同意一个可接受使用政策 (AUP) 或者最终用户协议 (EUA)。因为访客无线设备的硬件和软件功能通常不受组织的 IT 部门控制，身份验证和授权决定通常只是基于访客的用户 ID 和密码。换言之，在制定任何策略决定时可能不会考虑访客用来访问网络的设备。实施访客用户验证的一种典型方式是通过访客用户的网络浏览器，这种方法被称为 *Web 身份验证*，即 *WebAuth*。凭借这种身份验证，无线访客必须首先打开其网络浏览器，或者嵌入了浏览器的移动应用，连接至位于互联网某处的一个 URL。浏览器会话被重定向至一个包含登录页面、需要登录凭据的 Web 门户。成功完成身份验证后，访客用户要么获准访问互联网，要么被重定向至另一个网站。这种身份验证方式也称为一个*强制网络门户*。

在 WLAN 上对访客进行身份验证的方式有多种，例如下列方式：

- **本地 WebAuth**——借助这种方式，访客设备的网络会话由访客无线控制器重定向至访客无线控制器内一个包含登录屏幕的 Web 门户。随后对照访客无线控制器内的本地数据库对访客的凭据进行查验。此选项的优势在于对访客无线接入的整个管理都被限定在 DMZ 内部的访客无线控制器之内。此选项的短板在于，访客凭据在访客无线控制器内单独维护。
- **中央网络认证**——借助这种方式，访客设备的网络会话由访客无线控制器重定向至一个包含登录屏幕的外部 Web 门户。随后对照身份验证、授权和计费 (AAA) 服务器之内的一个外部数据库对访客凭据进行查验。思科身份服务引擎 (ISE) 可同时提供外部 Web 门户和 AAA 服务器功能。通过将网络身份验证登录门户置于一个中央服务器，网络管理员可为所有无线访客接入提供一个统一的登录页面（可选 AUP 或 EUA），而无需在每个访客无线控制器上创建一个单独的登录页面。通过把访客凭据数据库和访客发起人门户移至一个 AAA 服务器，网络管理员可提供一个中央位置用于创建和管理访客凭据，而不是必须在每个访客无线控制器上创建访客凭据。
- **基于 CMX 的访客载入**——基于 CMX 的访客接入通常由那些希望在其场所提供免费互联网接入的组织实施，以收集来自访问该站点的客户的某些信息作为交换。借助这种方式，访客通过使用其现有的社交媒体凭据登录，从而获准使用该无线网络并从该场所访问互联网。该场所的业主也可以选择允许匿名登录该无线网络。场所的业主也可选择显示一个针对这个特定场所位置定制的启动页面和注册表单。您可以通过部署思科 CMX 平台（也称为*移动服务引擎*）实现基于 CMX 的访客载入。您可以与 CMX 一起部署思科企业移动服务平台，从而不只是提供连接——通过经由一个网络浏览器或部署在移动设备上的移动应用融入访客参与。

思科 OfficeExtend

对于在家办公的远程工作人员而言，必不可少的是业务服务的访问必须可靠和一致，为其提供与园区相当的体验。但在常用的 2.4 GHz 无线频段内，住宅环境和城市环境存在许多潜在的拥塞，如无绳电话、智能手机、平板电脑、婴儿监控器。为了支持技术技能差别很大的用户，远程工作人员解决方案必须提供简化的方法来实施支持安全访问企业环境的设备。

涉及到实现远程工作解决方案时，包括从集中位置适当保护、维护和管理远程工作人员环境，IT 运营将面临一组不同的挑战。由于运营费用始终是一个考虑因素，IT 必须执行具有成本效益的解决方案，在不牺牲质量或功能的同时保护组织的投资。

思科 OfficeExtend 满足了易用性、体验质量和运营成本要求。思科 OfficeExtend 解决方案围绕以下两个主要组件构建：

- 思科 2500、5500 或 8500 系列无线 LAN 控制器
- 思科 Aironet 600 系列 OfficeExtend 无线接入点

思科 WLAN 控制器

思科无线局域网控制器与思科 OfficeExtend 接入点协同工作，从而为远程工作人员支持业务关键型无线应用。思科无线局域网控制器提供网络经理构建安全、可扩展的远程工作人员环境所需的可控性、可扩展性、安全性和可靠性。

一个独立控制器可支持多达 500 个思科 OfficeExtend 站点。对于弹性解决方案，思科建议成对部署控制器。

下列控制器是思科 OfficeExtend 的首选选项：

- 思科 2500 系列无线局域网控制器
- 思科 5500 系列无线局域网控制器

由于软件许可证灵活性支持根据业务需求更改添加额外接入点，因此您可以选择可长期支持您需要的控制器，但仅在您需要时为所需许可证付费。

为了支持用户将其终端设备连接到组织的现场无线网络或家庭远程工作无线网络，而无需进行重新配置，思科 OfficeExtend 在远程工作人员家庭使用与组织内部支持数据和语音相同的无线 SSID。

思科 OfficeExtend 接入点

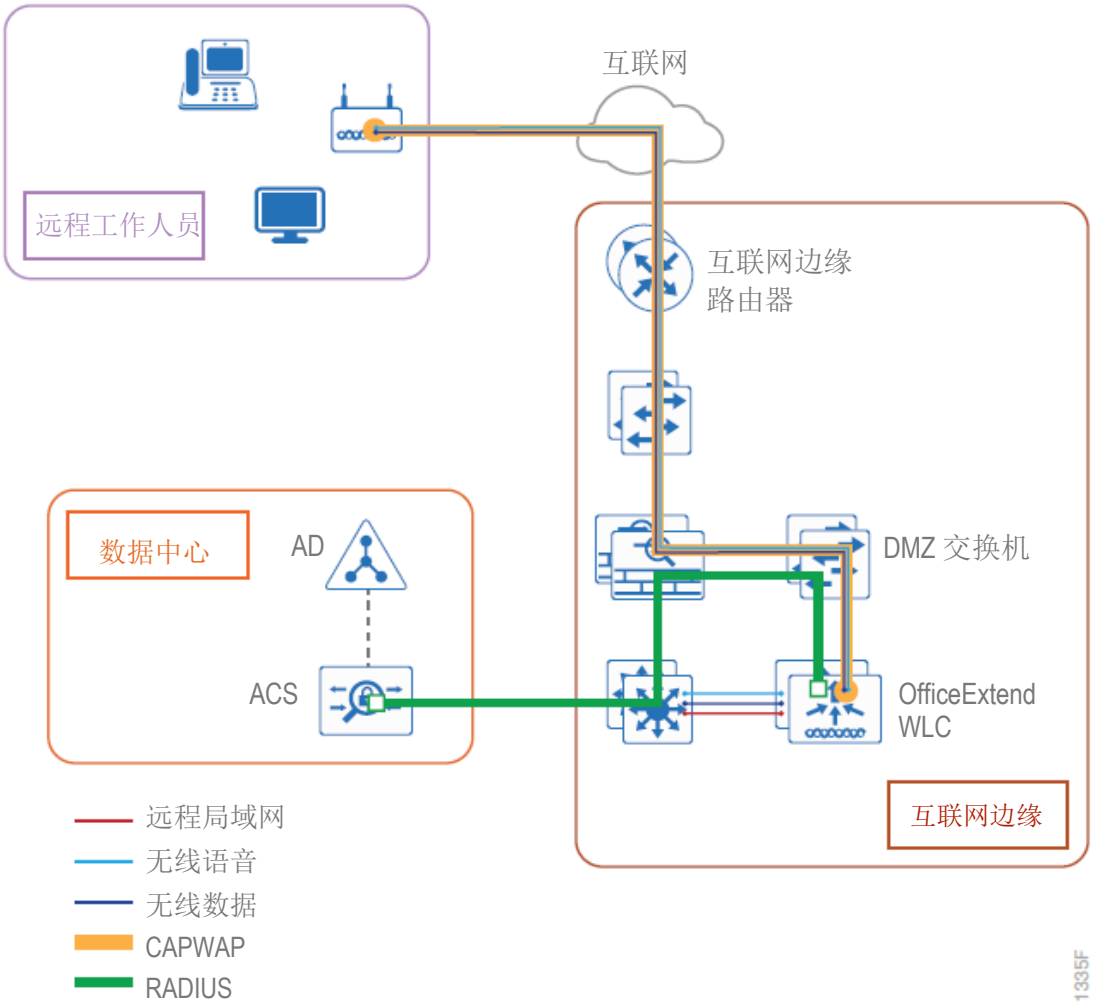
思科 Aironet 600 系列 OfficeExtend 接入点为轻量级，这意味着它无法独立于无线局域网控制器发挥作用。为了使用与企业办公室相同的配置文件提供远程 WLAN 连接，接入点将根据集中式安全策略验证所有流量。通过使用无线局域网控制器实现策略集中，思科 OfficeExtend 可最大程度地降低与基于家庭的防火墙相关的管理开销。数据报传输层安全连接可保障接入点与 WLAN 控制器之间的通信安全。

思科 OfficeExtend 提供全 802.11n 无线性能，还可避免因住宅设备同时运行 2.4GHz 和 5GHz 两种射频频段而导致的网络拥塞。接入点不仅提供无线连接，还提供有线以太网连接。思科 OfficeExtend 接入点提供家庭和企业流量的有线和无线分段，从而允许不会为企业策略引入安全风险的家庭设备连接。

OfficeExtend 设计模型

为了实现思科 OfficeExtend 的最灵活、安全的部署，可使用思科 5500 或 2500 系列无线局域网控制器为思科 OfficeExtend 部署专用控制器对。在专用设计模型中，控制器直接连接到互联网边缘 DMZ，来自互联网的流量将终止于 DMZ 中（而不是内部网络中），但是客户端流量仍直接连接到内部网络。

图 17　思科 OfficeExtend 专用设计模型



组播域名服务和 Bonjour 网关

Bonjour 是苹果的零配置协议，用于通告、发现和连接至诸如文件共享、打印共享和媒体共享等网络服务。Bonjour 协议原本是设计用于家庭网络用途并通过链路-本地组播使用组播域名服务来共享网络服务。尽管这一方案在家庭网络中运行良好，链路-本地组播的一个局限性在于，这些网络服务将只能在单一的第二层域（例如一个 VLAN 或者 WLAN）之内共享。在一个 WLAN 企业场景中，您将不同的 WLAN 和 VLAN 用于不同级别的设备，包括企业设备、员工设备、个人设备和访客设备（以及用于未批准设备的隔离 WLAN）。因此，基本的 Bonjour 操作——例如从一个无线局域网打印到一台有线打印机——可能不会得到本地支持。

为了解决这一局限性，从而满足企业内部用户对于苹果自带设备的需求，思科为其无线局域网控制器开发了 Bonjour 网关功能。该功能通过允许 WLC 监听、缓存和代理响应可能位于不同的第二层域中的 Bonjour 服务请求，为 Bonjour 解决了第二层域限制。此外，这些响应可能受到管理策略有选择的控制，因此仅在特定的第二层域中允许某些 Bonjour 服务。

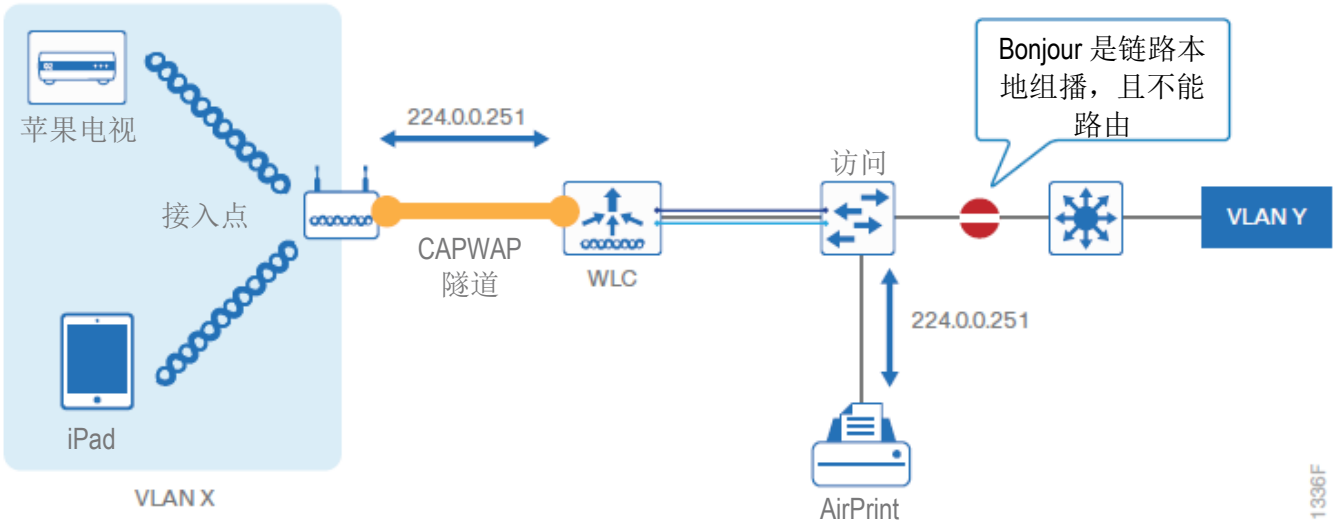
Bonjour 协议使用 mDNS 查询。这些查询从 UDP 端口 5353 发送至这些保留的组地址：

- IPv4 组地址：224.0.0.251
- IPv6 组地址：FF02::FB

需要重点强调的是，Bonjour 使用的 mDNS 地址是链路-本地组播地址，并仅在本地第二层域内部转发，因为链路-本地组播根据设计本来就是要保留在本地。另外，路由器甚至不能使用组播路由来重定向 mDNS 查询，因为这些数据包的生存时间 (TTL) 被设置为 1。

Bonjour 原本是为典型家庭网络而开发的，带有单一的第二层域，在那里 mDNS 的链路-本地限制很少会形成任何实际的部署约束。然而，在企业园区部署中（那里存在着大量有线和无线第二层域），该限制严重地限制了 Bonjour 的功能，因为 Bonjour 客户端仅能看到本地托管的服务，而不能看到或连接至其它子网上托管的服务。Bonjour mDNS 的这种链路-本地组播限制如下图所示。

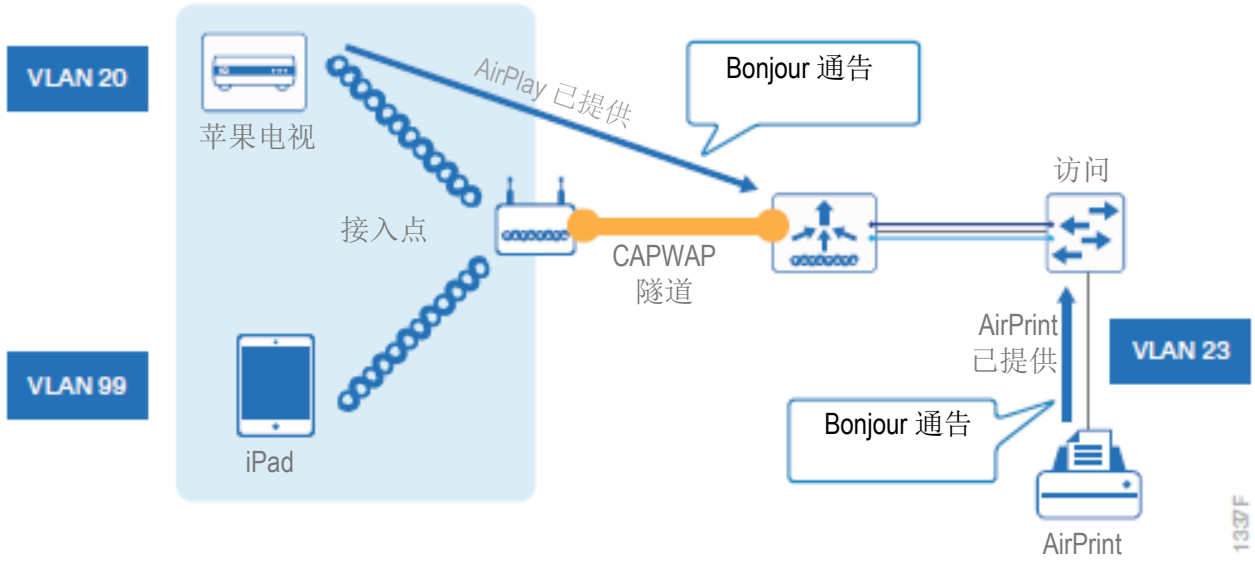
图 18　　企业网络中 Bonjour 的部署限制



为了解决这种限制并支持企业园区网络上的自带设备功能，思科发布了一个 Bonjour 网关功能。Bonjour 网关功能（mDNS 网关功能大多数情况下已激活用于 Bonjour）跨越多个 VLAN 监听并缓存所有 Bonjour 服务通告，并可配置成选择性地回复 Bonjour 查询。

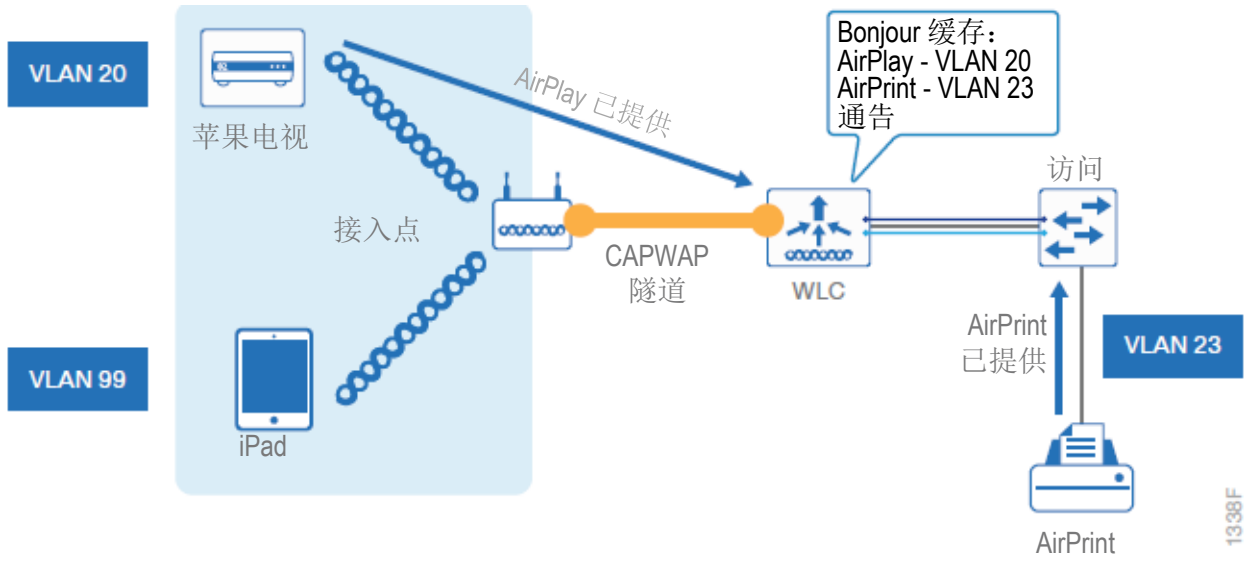
下列数据展示了 Bonjour 网关的操作。首先，Bonjour 网关监听所有 Bonjour 通告。

表 19　　思科无线局域网控制器 Bonjour 网关操作，步骤 1：Bonjour 服务通告监听



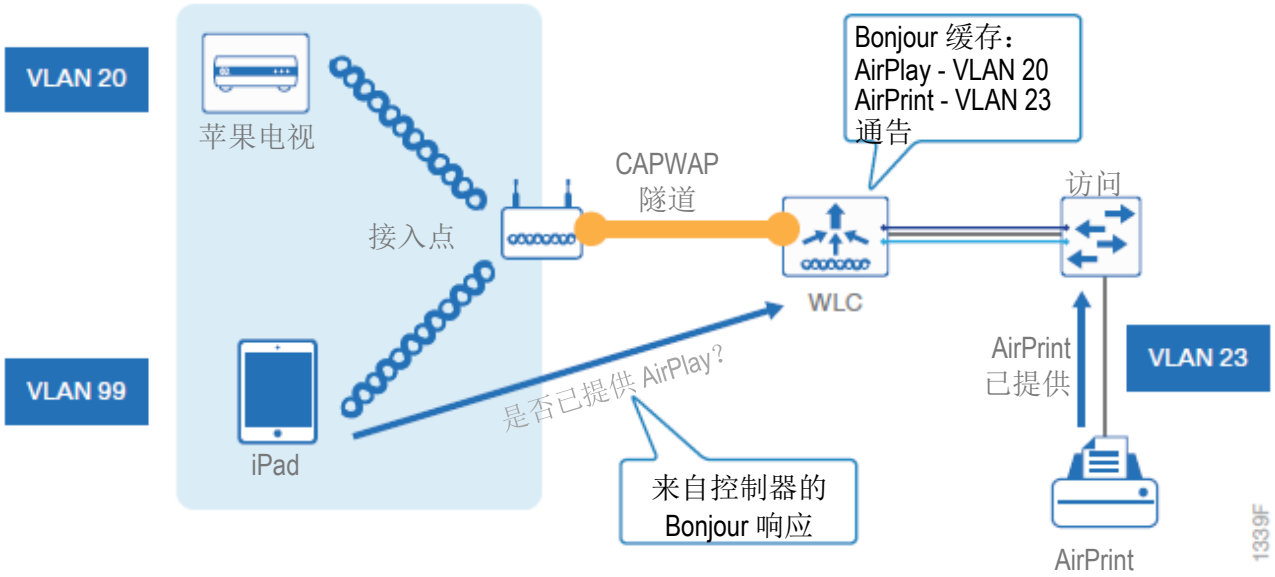
接下来，Bonjour 网关缓存服务通告，如下所示。每个运营商以其域名注册到 WLC 中。此外，每个 Bonjour 服务都有一个通告 TTL（与数据包的 TTL 不同），同时控制器在这个 TTL 85% 的时候要求该设备更新。

表 20　　思科 WLC Bonjour 网关操作，步骤 2：服务通告缓存



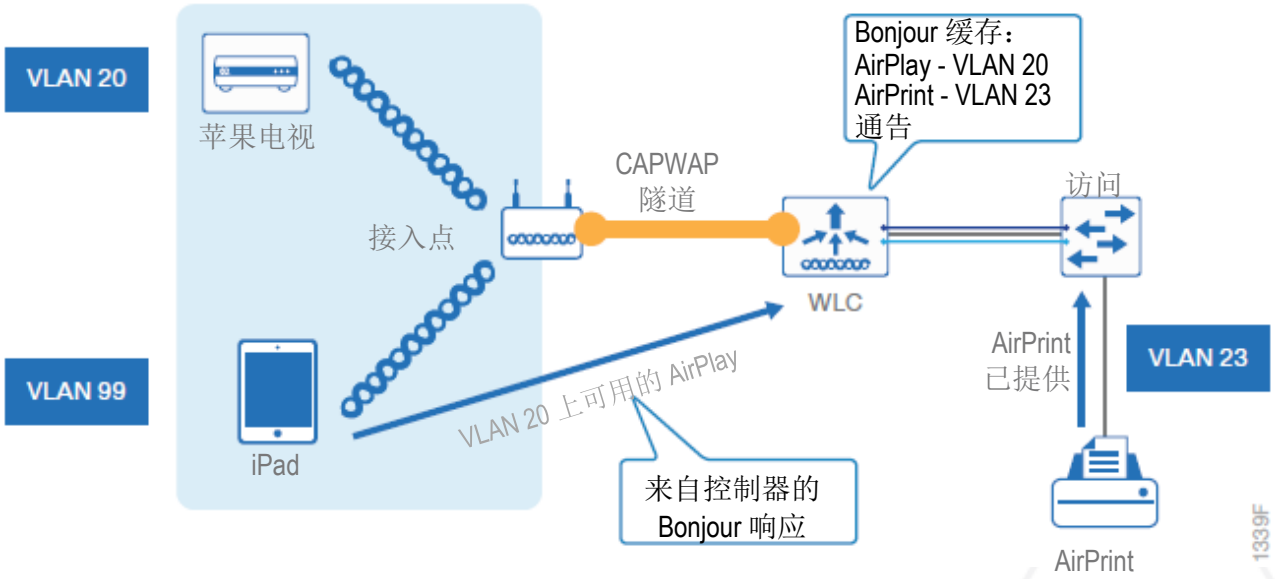
除了侦听服务通告以外，WLC 还始终侦听客户端对于服务的查询，如下所示。

表 21　　思科无线局域网控制器 Bonjour 网关操作，步骤 3：Bonjour 查询监听



需要本地托管服务的客户端会收到来自运营商的单播回复，然而，需要可能托管于其它 VLAN 服务的客户端会收到来自 WLC 的单播回复，如下所示。

表 22　　思科无线局域网控制器 Bonjour 网关操作，步骤 4：Bonjour 查询响应（来自缓存）



最后，Bonjour 网关服务可通过对客户端请求给定服务直接进行单播回复（而不是组播回复），进一步优化 Bonjour 流量，从而更高效地使用网络资源。

Bonjour 网关服务策略部署选项

Bonjour 网关的一项关键功能性优势在于，它可以配置成选择性回复 Bonjour 服务请求，从而允许在企业内对 Bonjour 服务进行管控。Bonjour 策略可按照如下方式应用：

- 每 WLAN
- 每 VLAN
- 每接口/接口组

思科应用可视性与可控性

WLC 平台可提供思科应用可视性与可控性 (AVC) 解决方案——早已得到诸如思科 ASR 1000 和思科 ISR 等思科路由平台的支持——包括思科 2500、5500、7500 和集中交换模式中的 8500 WLC。

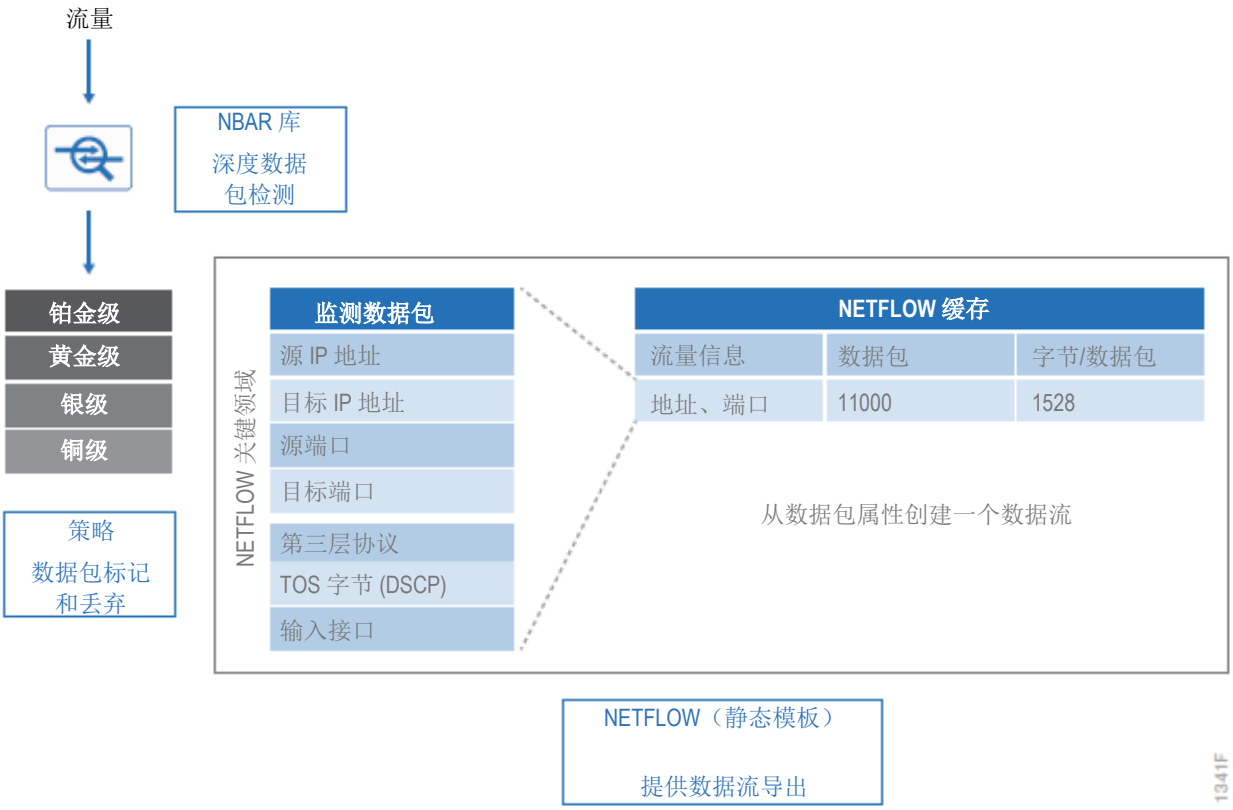
思科 AVC 功能集提高了无线网络的效率、生产率和可管理性。此外，嵌入到 WLAN 基础设施内的 AVC 支持端到端地扩展了思科基于应用的 QoS 解决方案。

AVC 包括这些组件：

- 称为 *下一代基于网络的应用识别* (NBAR2) 的下一代深度数据包检测（DPI）技术，它可实现对应用的识别和分类。思科 IOS 型平台上提供的 NBAR2 是一种深度数据包检测技术，它包含对 L4-L7 状态分类的支持。
- 通过使用 DiffServ 备注应用的能力，您随后还可使用它来设置或取消设置应用的优先级，以便在有线和无线网络上进行 QoS 处理。
- 一个用于思科 NetFlow v9 的模板，用来选择和导出感兴趣的数据到思科 PI 或第三方 NetFlow 收集器，以收集、分析和保存报表，用于故障排除、容量规划和合规目的。

这些 AVC 组件如下表所示。

表 23　　思科 AVC 组件



无线局域网上的思科 AVC 继承了来自思科 IOS 的 NBAR2，它可提供 DPI 技术，从而对 L4-L7 应用进行状态分类。这是用于应用管理的关键技术，因为要基于 TCP 或 UDP 端口号配置一个访问列表以便主动识别一个应用，这已不再是一个直接明了的问题。事实上，随着应用已经成熟——特别是在过去十年间——日益增多的应用已使这种识别捉摸不定。例如，HTTP 协议（TCP 端口 80）可在里面承载数以千计的应用，同时在当今网络中似乎更多的是充当一种传输协议，而不是它原本设计成的 OSI 应用层协议。因此，为了准确识别应用，诸如 NBAR2 等 DPI 技术至关重要。

在 NBAR 引擎通过其分立式协议签名识别出应用后，它会在一个共同数据流表中注册该信息，这样其他 WLC 功能就能利用这一分类结果。这些功能包括 QoS、NetFlow 和防火墙功能，它们全部可以基于这一详细分类采取行动。

思科 AVC：

- 通过对任何配置好的 WLAN 启用应用可视性，在思科 WLC 上提供应用可视性。一旦您开启应用可视性，NBAR 引擎便在那个特定 WLAN 上进行应用分类。您可以按 WLAN 或者客户端，在 WLC 上在整体网络层面查看应用可视性。
- 通过创建一个 AVC 配置文件（或策略）并附加到 WLAN，在思科 WLC 上提供应用可控性。AVC 配置文件可按照应用支持 QoS 规则并对每个已分类的应用提供下列可采取的行动：备注（与 DSCP）、许可（并不加改变地传输）或丢弃。

思科 AVC 的关键使用案例包括：

- **分类和备注无线移动设备应用**——识别实时语音、视频或业务关键型应用并将之从那些不那么重要（但可能属于带宽密集型）的应用中区别开来，以便设置或取消优先级，或者丢弃特定的应用流量。
- **流量规划和趋势预测**——设置网络基线，从而对于哪些应用正在消耗带宽获得一个更加清晰的理解，同时预测应用使用趋势，以便帮助网络管理员规划基础设施升级。

无线入侵防御系统

为了满足客户的需求，思科无线侵入防御系统解决方案提供一个灵活和可扩展的、24x7x365 的全天候无线安全解决方案。安全性是当今 WLAN 部署中的一项重大考量，而思科无线侵入防御系统是为满足 WLAN 部署中所有第一、第二、第三层的安全挑战而设计的。通过使用 WLC、PI 和 MSE 及其情景感知位置服务的思科解决方案，无线侵入防御系统可以在园区环境中锁定、缓解并遏制攻击。无线侵入防御系统可以支持的各种攻击如表所示。

表 8　　无线侵入防御系统攻击和思科解决方案

无线侵入防御系统攻击和威胁	思科解决方案
有线攻击 流氓无线接入点 自组网无线网桥	WLC、PI 和带情景感知的 MSE 可检测、定位、缓解并遏制这些攻击。
无线攻击 双面恶魔/蜜罐接入点 拒绝服务 侦测 破解工具	WLC、PI 和带无线侵入防御系统的 MSE 可检测这些活动并针对它们发出警报。
非 802.11 威胁 已篡改的流氓接入点 蓝牙、微波 RF 干扰器	CleanAir 接入点、WLC、PI 和带情景感知的 MSE 可检测、定位这些攻击并针对它们发出警报。

有线攻击

无线侵入防御系统优化模式中的接入点将使用与当前已实施的思科统一无线网络相同的逻辑，来执行欺诈威胁评估和缓解。这允许无线侵入防御系统接入点扫描、检测并遏制流氓接入点和临时网络。一旦发现后，有关流氓无线设备的该信息随即报告至思科 PI，流氓设备警报汇聚发生的地方。然而，对于该功能需要注意的一点是，如果一个遏制攻击是使用无线侵入防御系统模式接入点发起的，则其执行系统的、专注于攻击的信道扫描的能力在遏制期间会中断。

无线攻击

思科自适应无线 IPS 将完整的无线威胁检测和缓解功能嵌入到了无线网络基础设施中，从而提供业内最全面、精确和最经济高效的无线安全解决方案。

非 802.11 威胁

思科 CleanAir 技术可检测非 802.11 威胁。CleanAir 技术是监控和管理您的网络 RF 状况的一个有效工具。思科 MSE 扩展了这些功能。

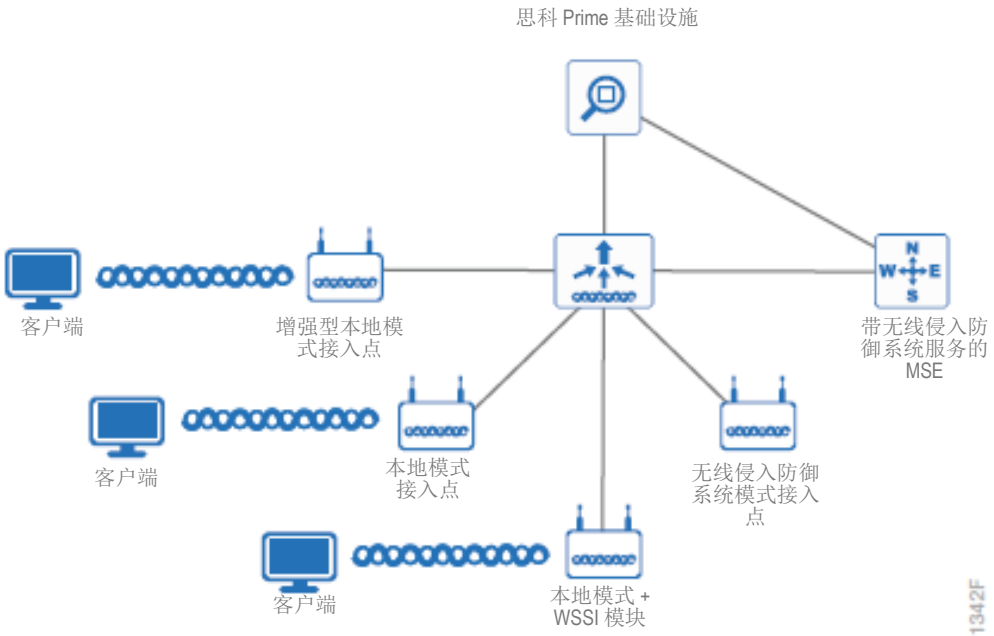
思科自适应 WiPS 系统

思科自适应 WiPS 系统的基本系统组件包括：

- 思科无线侵入防御系统监控模式、增强型本地模式或带思科 WSM 的接入点
- WLAN 控制器
- 正在运行思科无线侵入防御系统服务的思科 MSE
- 思科 Prime 基础设施

集成式无线侵入防御系统部署是一种系统设计，其中非无线侵入防御系统模式接入点和无线侵入防御系统模式接入点交互混合在相同的控制器上，并由相同的 Prime 基础设施进行管理。这可以是本地模式、FlexConnect 模式、增强型本地模式、监控模式以及带 WSM 的 3600 或 3700 系列接入点的任意组合。通过使用接入点上的 WSM 来叠加无线侵入防御系统保护和数据共享，您可以降低基础设施成本。

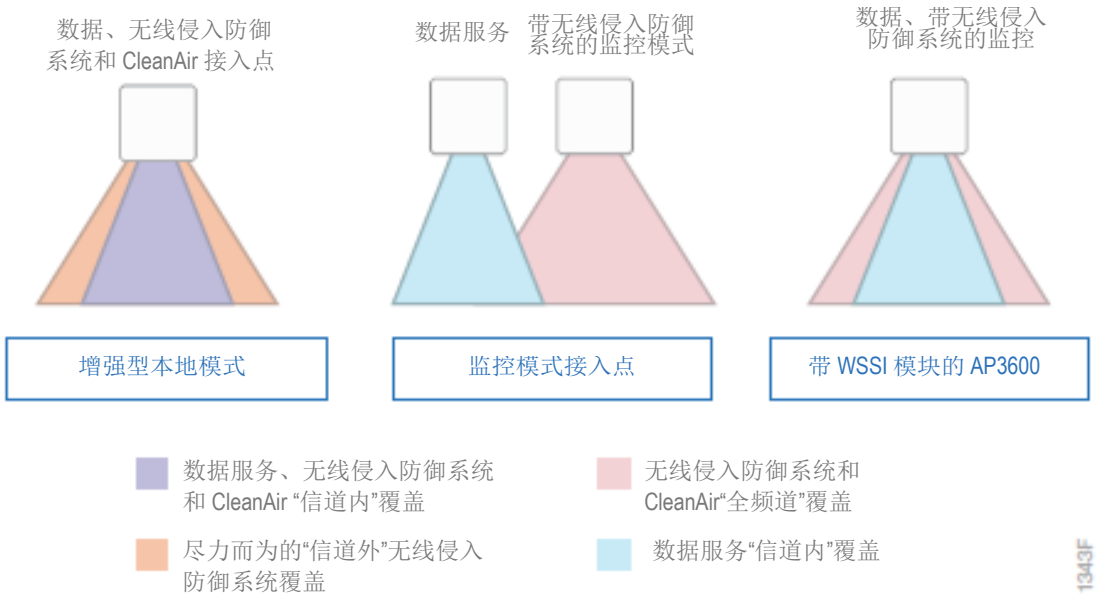
表 24　　无线侵入防御系统协同思科 MSE 运营



无线侵入防御系统部署模式

思科自适应无线 IPS 拥有三种选项用于无线侵入防御系统模式接入点。为了更好地阐述无线侵入防御系统模式接入点之间的区别，本部分对每个模式进行了描述。

表 25　无线侵入防御系统运营模式



增强型本地模式

增强型本地模式提供*信道内*无线侵入防御系统检测，这意味着正在服务客户端的信道检测到攻击者。对于其它所有信道，增强型本地模式提供尽力而为的无线侵入防御系统检测。这意味着每一帧射频将偏离信道一段较短的时间。当射频偏离信道时，如果攻击发生在信道被扫描时，则该攻击将被检测到。

对于 3700 系列接入点上的增强型本地模式，举例来说，假设 2.4 GHz 射频运行于信道 6。该接入点将不间断地监控信道 6，同时将会检测并报告信道 6 上的任何攻击。如果攻击发生于信道 11，而接入点正在信道外扫描信道 11，则该攻击将被检测到。

增强型本地模式功能包括：

- 无线侵入防御系统安全扫描用于 7x24 信道内扫描（2.4 GHz 和 5 GHz），同时提供尽力而为的信道外支持。
- 接入点额外服务客户端，同时借助思科 Aironet 第二代 (G2) 系列接入点，CleanAir 频谱分析在信道内 (2.4 GHz and 5 GHz) 启用。
- 服务本地及 FlexConnect 接入点的数据信道中的自适应无线侵入防御系统扫描。
- 无需单独重叠网络的保护。
- 为 WLAN 提供 PCI 兼容。
- 全 802.11 和非 802.11 攻击检测。
- 调查分析和报告功能。

- 设置集成和专用监控模式接入点的灵活性。
- 在接入点预处理，这将数据回程降至最低（即运行于非常低的带宽链路上）。
- 对服务于客户端数据的接入点影响很低。

监控模式

监控模式提供信道外无线侵入防御系统检测，这意味着接入点停留于每个信道上的时间将会延长，从而使接入点能够检测到所有信道上的攻击。2.4 GHz 射频扫描所有 2.4 GHz 信道，而 5 GHz 射频扫描所有 5 GHz 信道。将需要安装一个额外的接入点用于客户端访问。

监控模式的一些功能：

- 监控模式接入点 (MMAP) 专用于在监控模式下运行，并且可以选择添加所有信道（2.4 GHz 和 5 GHz）的无线侵入防御系统安全扫描。
- 对于思科 Aironet 第二代系列接入点，APS 频谱分析在所有信道上（2.4 GHz 和 5 GHz）均被激活。
- MMAP 不服务于客户端。
- 带 WSM 模块的思科 3700 或 3600 系列接入点组合使用信道内和信道外运营。这意味着接入点 2.4 GHz 和 5 GHz 内部射频将扫描它们借以服务于客户端的信道，同时 WSM 模块将额外运行于监控模式下并扫描所有信道。

流氓设备检测

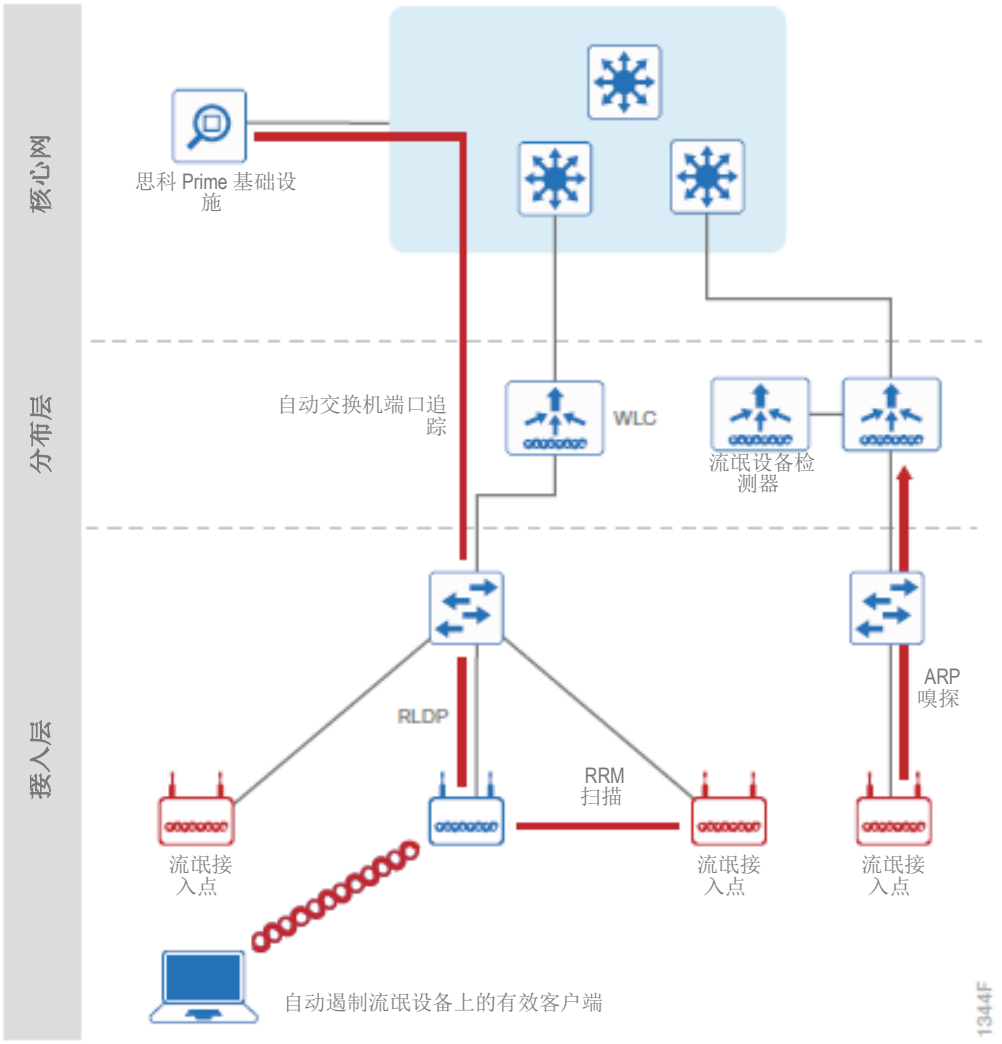
您可以将任何共享您的频谱却不受您管理的设备视作*流氓设备*。流氓设备在如下场景中会变得危险：

- 使用与您的网络相同的 SSID 的流氓接入点（蜜罐）
- 同处于有线网络的流氓接入点
- 临时流氓设备
- 由外部人员设置的具有恶意意图的流氓设备

CUWN 解决方案中对于流氓设备管理有三个主要阶段：

- **检测**——该解决方案使用射频资源管理 (RRM) 扫描，从而检测流氓设备的存在。
- **分类**——该解决方案采用流氓设备定位发现协议、流氓设备检测器和交换机端口追踪，从而识别流氓设备是否已连接至有线网络。流氓设备分类规则在基于流氓设备特性将它们划分为特定类别的过程中也可起到辅助作用。
- **缓解**——该解决方案使用交换机端口追踪和关闭、流氓设备位置和流氓设备遏制，从而跟踪流氓设备的物理位置并解除其威胁。

表 26　　思科流氓设备管理



如需更多信息，请参阅下列网站：

http://www.cisco.com/c/en/us/td/docs/wireless/technology/roguedetection_deploy/Rogue_Detection.html

射频资源管理

嵌入到思科无线 LAN 控制器中的 RRM 软件充当内置 RF 工程师，从而对您的无线网络不间断地提供实时 RF 管理。RRM 使思科 WLC 得以连续监控与其关联的轻量级接入点的下列信息：

- **流量负载**——用于发射和接收流量的总带宽，它使 WLAN 管理者得以领先客户端需求跟踪并规划网络增长
- **干扰**——来自于其它 802.11 源的流量
- **噪音**——干扰当前指定信道的非 802.11 流量
- **覆盖**——所有已连接客户端的 RSSI 和信噪比
- **其它**——附近接入点的数量

通过使用该信息，RRM 可以定期重新配置 802.11 RF 网络实现最高效率。为此，RRM 执行这些功能：

- 射频资源监控
- 发射功率控制
- 动态信道分配
- 覆盖空洞检测和校正

RRM 在新的思科 WLC 和轻量级接入点添加至网络时对它们进行自动检测和配置。它随后自动调整附近关联的轻量级接入点，以优化覆盖和容量。

轻量级接入点可同时扫描运营国所有有效的 802.11a/b/g/n/ac 信道以及其它位置的可用信道。接入点偏离信道不超过 60 毫秒，从而监控这些信道的噪音和干扰。对这个时间内收集的数据包会做分析，从而检测流氓接入点、流氓客户端、临时客户端和干扰接入点。

技术小提示

当出现语音流量（在最后 100 毫秒）时，接入点会推迟信道外测量。

每个接入点在信道外仅花费 0.2% 的时间。此活动分布于所有接入点，这样邻近的接入点不会在同时扫描，否则会影响 WLAN 性能。

技术小提示

当网络中有众多流氓接入点时，FlexConnect 或本地模式接入点检测到信道 157 或 161 上流氓设备的几率很小。在这种情况下，您可以使用监控模式接入点用于流氓设备检测。

发射功率控制

思科 WLC 基于 WLAN 的实时状况动态控制接入点的发射功率。您可以在两个版本的发射功率控制之间进行选择：TPCv1 和 TPCv2。借助 TPCv1，通常可以保持低功率以获得额外的容量并减少干扰。借助 TPCv2，发射功率可动态调整，以实现干扰最小化。TPCv2 适用于密集网络。在这种模式中，可能会出现更高的漫游延迟和覆盖空洞事故。

发射功率控制 (TPC) 算法可响应 RF 环境的变化升高和降低接入点的功率。在大多数情况下，TPC 寻求降低接入点功率以减少干扰，但是当 RF 覆盖出现突然变化时——例如，假设一个接入点出现故障或被禁用——TPC 也可以升高周围接入点的功率。这个功能与覆盖空洞检测不同，后者主要涉及客户端。TPC 为实现所需的覆盖水平提供足够的 RF 功率，同时避免接入点之间的信道干扰。

下表显示了控制器功率水平设置和每个频段中接入点射频发射功率之间的关系。

表 9　　控制器功率设置

控制器功率水平设置	2.4 GHz 频段中的功率	5 GHz 频段中的功率
1	23 dBm (200mW) 仅 CCK	20 dBm (100 mW)
2	20 dBm (100 mW)	17 dBm (50 mW)
3	17 dBm (50 mW)	14 dBm (25 mW)
4	14 dBm (25 mW)	11 dBm (12.5 mW)
5	11 dBm (12.5 mW)	8 dBm (6.25 mW)
6	8 dBm (6.25 mW)	5 dBm (3.13 mW)
7	5 dBm (3.13 mW)	2 dBm (1.56 mW)
8	2 dBm (1.56 mW)	-1 dBm (0.78 mW)

用最大和最小发射功率设置替代 TPC 算法

TPC 算法可平衡许多形形色色 RF 环境中的 RF 功率。然而，自动功率控制将有可能无法解决一些由于建筑限制或场地限制而无法实施适当的 RF 设计的场景——例如，当所有接入点必须安装在中央过道里，从而将接入点紧密布置在一起，但又要求向外覆盖到建筑边缘时。

在这些场景中，您可以配置最大和最小发射功率限制，以替代 TPC 建议值。在一个 RF 网络中，最大和最小 TPC 功率设置通过 RF 配置文件应用到所有接入点。

如果您配置一个最大发射功率，RRM 不允许任何附加在控制器上的接入点超过这个发射功率水平（无论该功率是由 RRM TPC 还是覆盖空洞检测设置）。例如，如果您配置一个 11 dBm 的最大发射功率，则接入点的发射功率不会超过 11 dBm，除非手动配置接入点。

动态信道分配

同一信道上的两个邻近接入点要么会导致信号争用，要么会导致信号冲突。在信号冲突中，接入点不接收数据。这个功能可能会成为一个问题——例如，当有人在咖啡馆阅读电子邮件时，这会影响邻近商店接入点的性能。即便这些完全是单独的网络，有人发送流量到信道 1 上的咖啡馆，也可以扰乱使用同一信道的企业中的通信。控制器可以动态进行接入点信道分配，从而避免冲突并提高容量和性能。信道得到重复利用，从而避免浪费稀缺的 RF 资源。换言之，信道 1 被分配给一个远离咖啡馆的不同接入点，这比完全不使用信道 1 更加有效。

控制器的动态信道分配 (DCA) 功能也有助于将接入点之间的邻近信道干扰降至最低。例如，802.11b/g 频段中的两个重叠信道，例如信道 1 和 2，两者不能同时使用 11/54 Mbps。通过有效地重新分配信道，控制器使邻近信道保持分开。您应当仅使用非重叠信道，例如信道 1、6 和 11 用于 2.4 GHz。

控制器检查各种实时的 RF 特征，从而按照下列方式高效处理信道分配：

- **接入点接收能量**——每个接入点及其附近相邻接入点之间测量到的接收信号强度。信道得到优化以实现最高的网络容量。
- **噪音**——噪音可在客户端和接入点限制信号质量。噪音的增加可降低有效的蜂窝尺寸并降低用户体验的等级。通过优化信道以避开噪音源，控制器可在优化覆盖的同时保持系统容量。如果一个信道由于过多的噪音而无法使用，则可避开该信道。
- **802.11 干扰**——干扰即任何不属于您的 WLAN 的流量，包括流氓接入点和相邻无线网络。轻量级接入点不间断地扫描所有信道，从而寻找干扰源。如果 802.11 干扰量超过了预先定义的可配置阈值（默认为 10%），则接入点向控制器发出警报。通过使用 RRM 算法，控制器随后可能会动态地重新安排信道分配，以在出现干扰时提升系统性能。这种调整可能会导致邻近的轻量级接入点在同一信道上，但相比使接入点保持在由于外来接入点干扰而无法使用的信道上，这种设置更可取。此外，如果出现其它无线网络，控制器便切换信道使用以补充其它网络。例如，如果一个网络位于信道 6，则将信道 1 或 11 分配给邻近 WLAN。这种安排通过限制频率的共享而提升了网络容量。如果一个信道实际上没有剩余容量了，则控制器可能会选择避开该信道。在非常密集的部署中，所有非重叠信道都被占用，控制器会尽力而为，但是您在设立预期的时候必须考虑 RF 密度。
- **负载和利用率**——当启用利用率监测时，容量计算可以考虑某些接入点的部署需承载比其它接入点更多的流量（例如，大堂对比工程区）。控制器随后可以分配信道以改善报告性能最差的接入点。当改变信道结构以将对当前处于 WLAN 中的客户端的影响降至最低时会考虑负载。这项指标保持跟踪所有接入点的发射和接收数据包计数，以判定接入点的繁忙程度。新的客户端会避开超负荷接入点，并关联到一个新的接入点。该参数默认为禁用。

控制器将这一 RF 特征信息与 RRM 算法结合起来，以制定整个系统范围的决策。通过使用可为最小化网络干扰而保证最佳选择的软决策指标，冲突需求得以解决。最终结果是在一个三维空间中的优化信道配置，其中楼层上下的接入点在总体 WLAN 配置中充当主要因素。

技术小提示

使用 2.4-GHz 频段中 40-MHz 信道或 DCA 不支持的射频是不能配置的。

下列条件下会调用 RRM 启动模式：

- 在单一控制器环境中，控制器重启后调用 RRM 启动模式。
- 在多控制器环境中，选出 RF 组领导后调用 RRM 启动模式。

您可以从 CLI 触发 RRM 启动模式。

RRM 启动模式运行时间为 100 分钟（10 次迭代，每次间隔为 10 分钟）。RRM 启动模式的持续时间并不取决于 DCA 间隔、敏感度和网络大小。启动模式由 10 轮高敏感度 DCA 组成（使改变信道变得简便并使其对环境敏感），以融合到一个稳态信道计划中。启动模式完成后，DCA 继续以特定间隔和敏感度运行。

覆盖空洞检测和校正

RRM 覆盖空洞检测算法可以检测一个 WLAN 中低于稳健无线性能所需水平的无线覆盖区域。该功能可提醒您需要额外的（或者重新安置的）轻量级接入点。

如果检测到轻量级接入点上的客户端处于低于 RRM 配置中确定的阈值水平，则接入点会发送一个“覆盖空洞”警报到控制器。该阈值包括 RSSI、失败客户端计数、失败数据包百分比以及失败数据包数。该警报表明存在一个区域，那里的客户端正在连续经历糟糕的信号覆盖，而没有可行的漫游接入点。控制器会辨别可以校正和不可校正的覆盖空洞。对于那些可以校正的覆盖空洞，控制器通过对该特定接入点增加发射功率水平来缓解覆盖空洞。控制器并不缓解那些由客户端引起的（无法增加其发射功率或被静态设置为一个功率水平）覆盖空洞，因为增加其下游发射功率可能会增加网络中的干扰。

RRM 的优势

RRM 产生一个容量、性能和可靠性最优化的网络。它将您解放出来，从而不必连续监控网络噪音和干扰问题，这些可能是短暂的且难以排除故障。RRM 可确保客户端在整个思科统一无线网络内享受无缝、无故障的连接。

RRM 将独立的监测和控制用于所部署的每个网络：802.11an/ac 和 802.11bgn。RRM 算法可单独运行，用于各种无线电类型 802.11an/ac 和 802.11b/g)。RRM 同时使用测量和算法。RRM 测量可通过使用监测间隔时间进行调整，但不能禁用它们。RRM 算法是自动启用的，但是可以通过静态配置信道和功率分配来禁用。RRM 算法以一个特定的更新间隔时间运行，默认为 600 秒。

频段选择

随着消费设备越来越多地在 2.4 GHz 工业、科学与医学 (ISM) 频段运行，对该频段造成干扰的噪音已显著增加。同样，现在提供的许多无线设备都支持双频段，可在 2.4 GHz 或 5 GHz 频段运行。

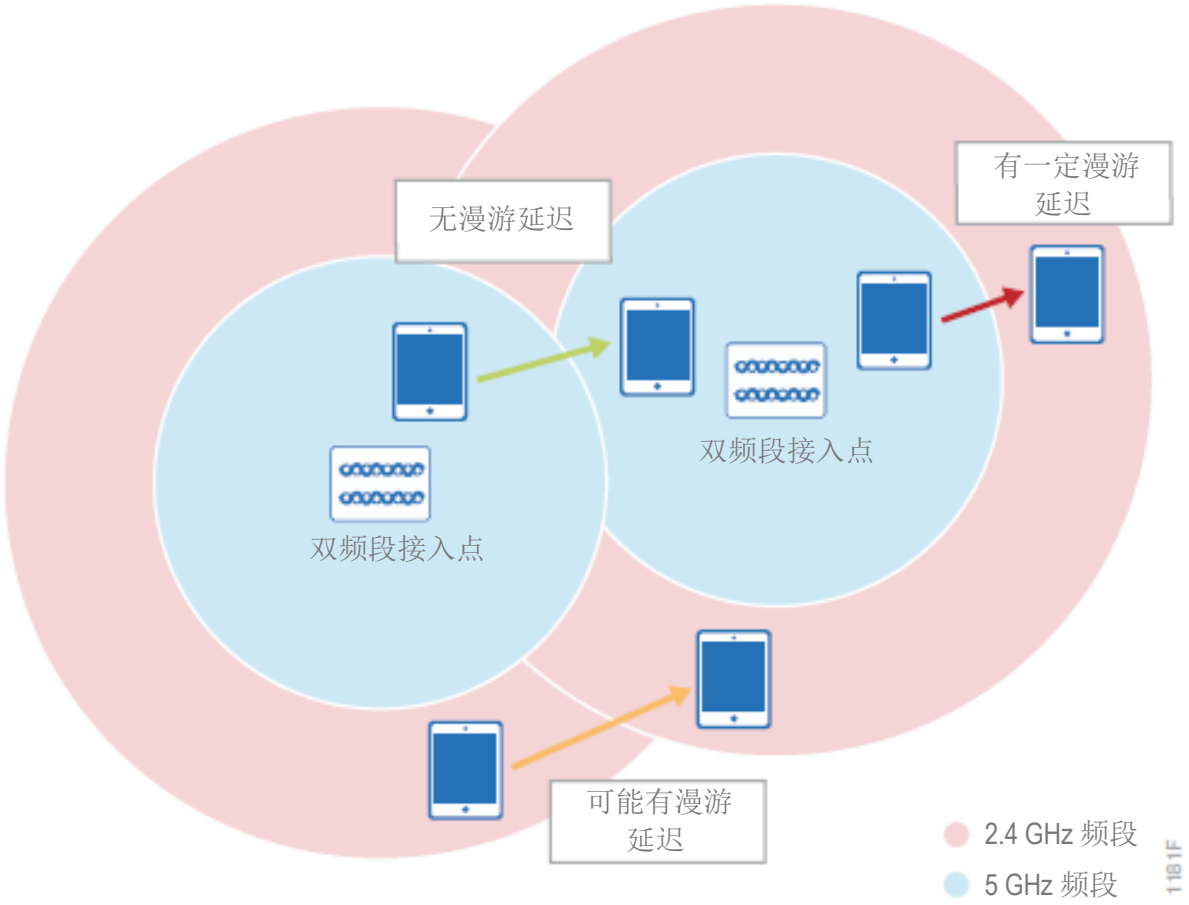
对于关键业务类设备，如果能够对这些设备施加影响，从而使用 5 GHz 频段来降低干扰，提供更好的用户体验，这将会十分有利。

当双频段无线设备寻找接入点时，它们往往先在 2.4 GHz 频段发送探测请求，几毫秒后在 5 GHz 频段发送探测请求。因为 2.4 GHz 探测响应通常先接收到，所以许多设备在即使 5 GHz 接入点可用时仍会使用 2.4 GHz 频段连接。

“频段选择”将 2.4 GHz 探测的探测响应延迟数百毫秒，使接入点确定无线设备是否为双频段设备。当从同一设备接收到 2.4 GHz 和 5 GHz 探测时，则检测到双频段无线设备。通过延迟 2.4 GHz 探测响应，可在提供 2.4 GHz 探测响应之前提供 5 GHz 探测响应，对无线客户端施加影响，将其连接到首选的 5 GHz 频段。

不推荐对语音和视频设备使用频段选择，因为它会延迟 2.4 GHz 频段对探测请求的响应。对于从 5 GHz 区域移动到 2.4 GHz 覆盖区域的实时流设备，或在 2.4 GHz 接入点之间漫游的客户端，此延迟会导致短暂的连接中断。对于仅有数据的流量传输，该延迟可以忽略，通常不会影响应用访问。

图 27　　频段选择 - 对实时应用的影响



CLIENTLINK

思科 ClientLink 无线网络技术使用波束成形改善所有无线客户端的信噪比，而不限于支持 802.11n 标准的无线客户端。ClientLink 通过减少重新传输和提高数据速率，实现从接入点到客户端的更佳吞吐量。此外，通过减少任何给定无线客户端使用 RF 信道的时间，您便提升了无线网络的整体性能。

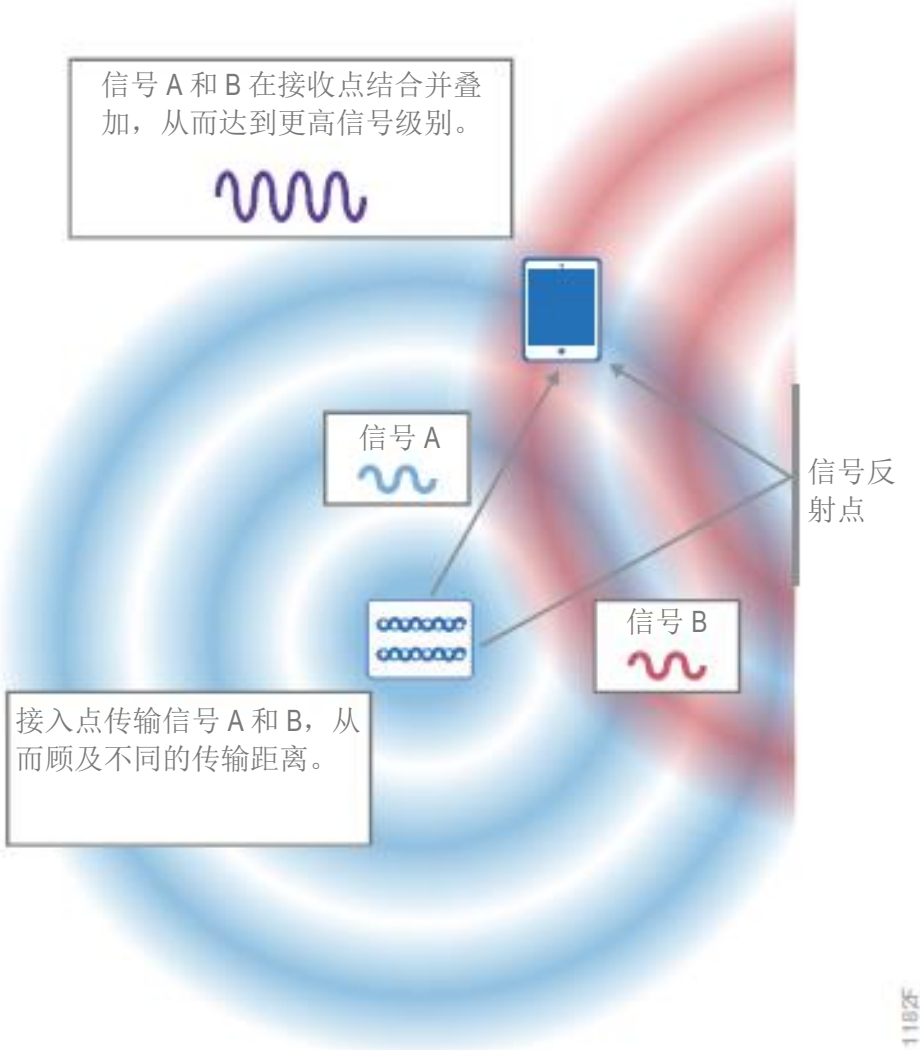
在给定无线局域网控制器上，ClientLink 在整个射频频段（802.11b/g/n 或 802.11a/n/ac）启用或针对具体接入点启用。

表 10　ClientLink 支持和默认配置

ClientLink 版本	支持接入点系列	默认 ClientLink 设置
3.0	思科 Aironet 3700 和 2700 系列	启用
2.0	思科 Aironet 1600、2600 和 3600 系列	启用
1.0	思科 Aironet 1140、3500、1250 和 1260 系列	禁用

思科 1700 系列接入点支持基于标准的传输波束成形 (TxBF)。

图 28　ClientLink 优化



802.11AC 带宽性能

在基于 Wi-Fi 的无线技术的发展过程中，802.11ac 的引入带来前所未有的巨大性能提升。最初的 802.11 标准开始于 1997 年，实现了 2 Mbps 的理论物理层 (PHY) 性能。现在，通过引入配备三空间流 (3SS) 的 802.11ac 第一阶段，理论最大 PHY 性能飙升至 1.3 Gbps。

表 11　　802.11ac 带宽性能

年份	技术	频段	理论最大 PHY 性能	理论最大用户性能
1997	802.11	2.4 GHz	2 Mbps	1 Mbps
1999	802.11b	2.4 GHz	11 Mbps	6 Mbps
1999	802.11a	5 GHz	54 Mbps	25 Mbps
2003	802.11g	2.4 GHz	54 Mbps	25 Mbps
2003	802.11a/g	2.4 GHz/5 GHz	54 Mbps	13—25 Mbps
2007	802.11n	2.4 GHz/5 GHz	450 Mbps w/3SS	180—220 Mbps
2013	802.11ac 第一阶段	5 GHz	1.3 Gbps w/3SS	最高 750 Mbps
未来	802.11ac 第二阶段	5 GHz	2.5—3.5 Gbps	待定

实际无线性能涉及到距离、无线适配器以及整体 RF 环境等许多变量。此外，使用 802.11a 的相邻混合蜂窝可能因为传输速度较低而导致较长时间的信道使用。如果采用非对齐的主信道部署使用固定 40 MHz 的相邻 802.11a/n，则 Clear Carrier Assessment 机制的优势将无法实现。

802.11ac 第一阶段规格包括许多技术，它们均有助于显著提高性能。

- 802.11ac 只能在较为安静和空闲的 5 GHz 频段实施。
- 802.11ac 使用高达 256 个正交调幅 (QAM)，支持每个符号使用 8 个位，性能提升四倍。简单来说，QAM 是一种使用波形阶段和振幅编码数据的调制技术。256 个 QAM 带来 256 个符号，这大大提高了吞吐量。
- 802.11ac 扩展了信道宽度，可在第一阶段支持 20、40 和 80 MHz 带宽，在第二阶段支持 20、40、80、80+80 和 160 MHz 带宽。
- 波束成形在 802.11ac 第一阶段得到增强并包含在思科 ClientLink 无线网络技术中，它支持接入点*波束转向*或将集中信号导入接收器，该种结合能够提高接收器处的质量和信号级别。

802.11AC 信道规划

使用射频资源管理 (RRM) 和动态信道分配 (DCA) 时，信道分配要比 802.11 的早期阶段更为简单。即使如此，决定绑定信道前仍需考虑一些因素。尽管园区无线局域网采用全新部署，现有无线环境的网络管理员可能希望更谨慎地行动，并解决信道规划考虑事项。

如果您的环境实施 20 MHz 宽信道，思科推荐您采用一个分阶段的方法，并考虑转到更宽的（40 或 80 MHz 宽）信道。80 MHz 宽信道在大型组织中的使用非常罕见，因为其可用的信道数量有限。第一步是启用动态频率选择 (DFS) 信道集。使用 DFS 信道需要接入点扫描是否使用雷达。如果检测到雷达，则接入点移动到另一信道或降低传输功率。DFS 信道支持范围更广泛的 RF 频谱，具体取决于您的监管域。这反过来使 DCA 支持更大的信道绑定选择。

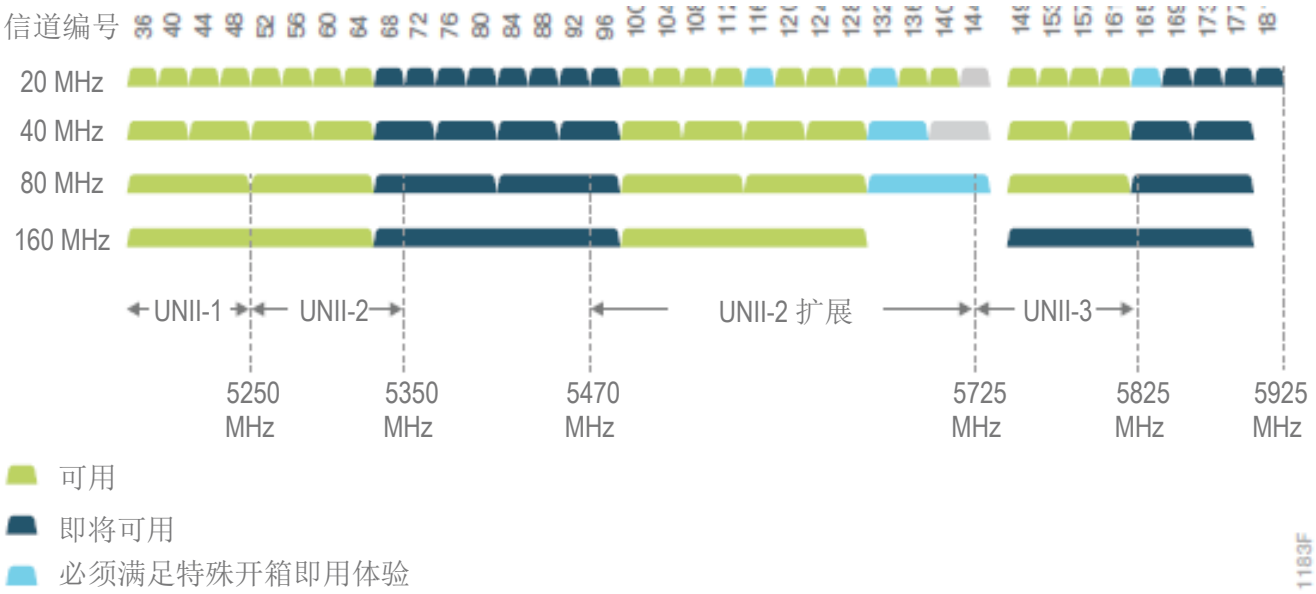
由于启用了 DFS 信道，美国可提供四个 80 MHz 信道和九个 40 MHz 信道，除信道 120-128 和 144 例外。

表 12　　全球 5 GHz 信道可用性

可用信道数量	美国	欧盟	中国	印度	日本	俄罗斯
20 MHz 信道	21	16	5	13	19	15
40MHz 信道	9	7	2	6	9	7
80MHz 信道	4	3	1	3	4	4

随着 802.11ac 第一阶段引入 80 MHz 宽信道，第二阶段即将引入 160 MHz 宽信道，出现一些与信道规划相关的考虑事项。5 GHz 频段中的 20 MHz 信道数量充足，但随着企业部署 80 MHz 和 160 MHz (第二阶段)，这种情况将迅速改变。下图阐述了 40 MHz 和 80 MHz 信道选择的影响。

图 29　　美国的信道使用



借助 RRM、TPC 和 DCA，您可以同时对信道选择的过程实现自动化和优化。

园区无线 CLEANAIR

思科 CleanAir 是一个频谱智能解决方案，其设计旨在主动管理共享无线频谱的挑战。它允许您看到共享频谱的所有用户（同时包括本地设备和外来干扰者）。它还使您或您的网络得以基于该信息采取行动。例如，您可以手动移除干扰设备，或者系统可以自动改变信道远离干扰。CleanAir 提供频谱管理和射频可视性。

思科 CleanAir 系统由 CleanAir 启用的计入点、思科无线局域网控制器和思科 Prime 基础设施组成。这些接入点收集有关运行于 ISM 频段的所有设备的信息、作为潜在的干扰源识别并评估这些信息，并把它转发给思科 WLC。思科 WLC 控制接入点、收集频谱数据，并根据请求向思科 Prime 基础设施或思科 MSE 转发信息。

对于运行于未授权频段中的所有设备，思科 CleanAir 无线网络告诉您它是什么，它在哪里，它正在如何影响您的无线网络，以及您或者您的网络应当采取什么行动。它简化了射频，因此您不必成为一个射频专家。

WLAN 系统运行于未授权的 2.4 和 5 GHz ISM 频段中。许多设备，例如微波炉、无绳电话和蓝牙设备也运行于这些频段中，并可对 Wi-Fi 运行产生负面影响。

某些最高级的 WLAN 服务，例如无线和 IEEE 802.11n 射频上的语音通信，可能会由于 ISM 频段中的其它合法用户引起的干扰而被大幅削弱。将思科 CleanAir 功能集成到思科统一无线网络解决了这个射频干扰的问题。

在 5 GHz 射频网格的网状接入点回程上支持 CleanAir。您可以在回程射频上启用 CleanAir 并可以提供报告干扰详情和空气质量。

思科 CleanAir 部署中思科 WLC 的作用

在思科 CleanAir 系统中，思科 WLC：

- 配置思科 CleanAir 在接入点上的功能
- 为配置思科 CleanAir 功能和检索数据提供接口 (GUI、CLI 和 SNMP)。
- 显示频谱数据。
- 从接入点收集并处理空气质量报告并将它们存储到空气质量数据库中。空气质量报告包含有关来自空气质量指数所代表的所有已识别源的总干扰，以及对最严重干扰类型的汇总信息。CleanAir 系统还可以根据干扰类型报告包含未分类的干扰信息，这使您在由于未分类干扰设备而干扰更多的情况下得以采取行动。
- 从接入点收集并处理干扰设备报告并将它们存储到干扰设备数据库中。
- 将频谱数据转发给思科 Prime 基础设施和思科 MSE。

思科 CleanAir 可以检测到的干扰类型

思科 CleanAir 可以检测干扰、报告干扰的位置和严重性，同时推荐不同的缓解策略。这类缓解策略的其中两种分别是永久设备避免和频谱事件驱动 RRM。

基于 Wi-Fi 芯片的 RF 管理有这些共同特征：

- 对任何不能识别为 Wi-Fi 信号的 RF 能量报告为噪音。
- 用于分配信道规划的噪音测量在一段时间内倾向于平均化，从而避免可对某些客户端设备造成破坏的不稳定性和剧烈变化。
- 平均化测量可降低测量分辨率。因此，一个破坏客户端的信号可能似乎不需要在平均化后进行缓解。
- 当今可用的所有 RF 管理系统都是被动性质的。

思科 CleanAir 有所不同，不但可以主动识别噪音源，而且还可识别其位置和对 WLAN 的潜在影响。拥有了这个信息，您便可以在网络环境下考虑该噪音，并且只要有可能，可以做出明智、积极主动的决策。对于 CleanAir，一般有两种类型的干扰事件：

持久干扰

自发干扰

持久干扰事件由具有固定性质的设备引起，并具有断断续续但可大范围重复的干扰模式。例如，考虑一下位于休息室的微波炉的情形。这种设备的每次活动时间可能只有一两分钟。然而，当它运行时，它可能会扰乱无线网络及其关联客户端的性能。通过使用思科 CleanAir，您可以主动识别该设备为一台微波炉，而不是不加区别地对待噪音。您还可以准确判定该设备影响了频段的哪个部分，同时因为您可以定位它，您还可以了解到哪些接入点受影响最严重。您随后可以使用该信息来指导 RRM 选择信道规划，从而使干扰范围内的接入点避免受到该干扰源的影响。因为这种干扰在一天中的活动时间比例并不大，现有的 RF 管理应用可能会尝试再次改变受影响的接入点信道。然而，永久设备避免是独特的，即只要定期检测到干扰源以刷新持久状态，它就保持有效。思科 CleanAir 系统知道微波炉的存在，并将它纳入未来的所有规划中。如果您移动微波炉或附近的接入点，该算法便会自动更新 RRM。

> ***技术小提示***
>
> 频谱事件驱动 RRM 只能由本地模式中已启用思科 CleanAir 的接入点触发。

*自发干扰*是突然出现在网络上的干扰，可能在干扰一个信道或一个完整范围的信道。思科 CleanAir 频谱事件驱动 RRM 功能允许您为空气质量设置一个阈值，如果超出，则立即为受影响的接入点触发信道改变。大多数 RF 管理系统可以避免干扰，但是该信息需要花时间在整个系统中传播。思科 CleanAir 依赖 AQ 测量结果，从而持续评估该频谱并可在 30 秒内触发一个行动。例如，如果一个接入点检测到来自摄像机的干扰，它可以通过在摄像机激活后 30 秒内改变信道进行恢复。思科 CleanAir 还可识别并定位干扰源，因此可以在晚些时候对该设备采取更永久性的缓解措施。

对于蓝牙设备，已启用思科 CleanAir 的接入点可以仅当设备正在传输时检测并报告干扰。蓝牙设备拥有广泛的省电模式。例如，当数据或语音正在已连接设备之间进行流式传输时可检测到干扰。

永久设备

某些干扰设备（例如室外网桥和微波炉）仅在需要时才进行传输。由于持续时间短以及正常的 RF 管理指标仍然无法检测到大多数定期运行，这些设备可对本地 WLAN 产生严重的干扰。借助 CleanAir，RRM DCA 算法可检测、测量、注册并记住其影响并调整 DCA 算法。对于受属于干扰源本地的信道规划中永久设备影响的信道，这将其使用减至最低。思科 CleanAir 检测永久设备信息并把它存储到思科 WLC 中，同时该信息被用来缓解干扰信道。

永久设备检测

已启用 CleanAir 的监控模式接入点收集所有已配置信道上关于永久设备的信息，并将该信息存储到思科 WLC 中。本地/网桥模式接入点仅在服务信道上检测干扰设备。

永久设备传播

由本地或监控模式接入点检测到的永久设备信息被传播到连接至同一个思科 WLC 的相邻接入点，从而提供更好的机会来应对和避开永久设备。由已启用 CleanAir 的接入点检测到的永久设备被传播到相邻的非 CleanAir 接入点，从而增强信道选择质量。

通过接入点检测干扰

当一个启用了 CleanAir 的接入点检测到干扰设备时，来自多个检测器对这个相同设备的检测会合并到一起，以创建集群。每个集群会获得一个独特的 ID。有些设备通过限制传输时间直到真正需要的时候以省电，这导致频谱检测器暂停检测设备。随后该设备会被正确地标记为停机。停机设备会被正确地从频谱数据库中移除。假如报告了对于某特定设备的所有干扰检测，则将延长集群 ID 的活动时间，从而防止可能的设备检测弹跳。如果再次检测到同一台设备，则将它与原始集群 ID 合并起来并保存该设备的检测历史。

例如，有些蓝牙耳机通过电池供电工作。这些设备采用一些方法来降低功耗，例如在实际并不需要时关闭发射器。这类设备在分类中看上去可能会进进出出。为了管理这些设备，CleanAir 会把集群 ID 保留更长时间，同时只要检测到，它们便会重新合并到一条单一记录中。这个过程理顺了用户记录并准确地反映了设备历史。

保障 WLAN 的安全

只要有可能，无线设备应当安全地连接至网络基础设施。在企业环境中，您应当对 WLAN 进行配置，以支持 AES-CCMP 加密的 WPA2 和对设备的 802.1X 身份验证。有时这叫做无线设备上的 WPA 企业版。大多数现代无线设备支持 WPA2。由于已知的安全性漏洞，不推荐使用老式安全方法，例如 WEP 或 WPA。802.1X 身份验证需要一个 AAA 服务器（例如思科 ISE 或思科访问控制服务器 (ACS)），这为访问无线网络的最终用户提供基于策略的集中化管理和控制。

通常，AAA 服务器会在其本身和 WLC 之间实施远程验证拨入用户服务协议。对最终用户的身份验证是通过无线设备和 AAA 服务器之间的一个可扩展身份验证协议 (EAP) 会话完成的。EAP 会话通过 WLC 和 AAA 服务器之间的远程验证拨入用户服务传输。根据无线设备的功能、AAA 服务器的功能，以及组织的安全要求，可能会实施 EAP 的多种变体，例如 PEAP 和 EAP-TLS。PEAP 采用标准用户凭据（用户 ID 和密码）用于身份验证。EAP-TLS 采用数字证书用于身份验证。

强烈推荐您部署冗余 AAA 服务器来实现高可用性，以防一台或多台服务器临时变为不可用。通常，AAA 服务器会配置成参考一个外部目录或数据存储库，例如微软的 Active Directory (AD)。这允许网络管理员利用现有的 AD 凭据，而不是在 AAA 服务器内复制它们。通过使用 AD 组，这还可进行扩展，从而为最终用户提供基于角色的访问控制 (RBAC)。例如，为长期承包商而不是获准访问的员工提供受限制的网络接入，这可能是可取的。使用外部目录或数据存储库也可为授予或撤销凭据提供单一点，不仅用于访问网络基础设施，而且还用于访问组织内的其它资源。AAA 服务器自身还可将更多用于授权的策略型规则应用到网络，例如设备类型、当前时间、位置等，取决于该 AAA 服务器的功能。AAA 日志和计费可以用来为每个员工对无线网络基础设施的访问提供审计追踪。

WLAN 上对 AES-CCMP 加密型 WPA2 的使用并不扩展到管理帧。因此，只要有可能，建议将受保护的管理帧 (PMF) 的可选使用用于 WLAN。PMF 是 IEEE 802.11 标准的一部分，它为稳健的管理帧（例如解除身份验证和解除关联帧）提供一定等级的加密保护，从而防止它们被欺骗。应当注意的是，PMF 的优势确实要求无线客户端支持 PMF。思科还提供一个早期版本的管理帧保护 (MFP)，兼具基础设施和客户端组件。

在一个家庭办公环境中，可能有必要配置一个 WLAN 以支持带预共享密钥 (PSK) 的 WPA2。有时这叫做无线设备上的 *WPA 个人版*。这可能有必要，因为 AAA 服务器的实施对于访问 WLAN 的最终用户数量来说并不具成本效益。这在其它环境中可能也有必要，如果那里没有与无线设备关联的最终用户、该无线设备并不支持配置用户 ID 和密码的功能，或者该无线设备无法支持数字证书。因为 PSK 是在所有访问无线基础设施的设备之间共享，如果一名知道 PSK 的员工离职，则可能有必要修改 PSK。另外，有了 WPA PSK，便无法轻松审计追踪每个员工对网络的访问。

专用开放式 WLAN 的使用仍然很普遍，但对于无线访客接入并不理想。因此，在网络基础设施上配置一个未加密的 WLAN 可能仍有必要。通常，实施开放式接入访客 WLAN 是为了将接入仅需临时连接无线网络的访客的复杂度降至最低。通常，访客 WLAN 终止于企业防火墙外，它不允许对企业资源的入站访问，因此可能仅允许访客访问互联网。

取决于组织的要求，可能会要求访客在获准访问互联网之前先行验证身份。通常，一个强制网络门户会与 WebAuth 一起使用，其中访客网络会话被重定向至一个门户，该门户在允许访客访问互联网之前会先行验证访客身份。

管理访问控制

推荐您将安全管理访问控制实施到无线基础设施组件，从而缓解未经授权的访问。通常，您可以通过每个基础设施设备中的本地用户数据库，或者通过一个集中化的 AAA 服务器（例如思科 ISE 或者思科 Secure ACS）来实施管理访问控制。

对于少量网络基础设施设备来说，在每个基础设施设备上配置单独的本地管理员帐号是可以接受的。推荐限制管理员的数量，同时为每个管理员设置一个独特的帐号。共享管理员帐号限制了对谁访问了一个特定网络设备以及可能进行了配置更改的审核能力。当员工离职或者调入其它部门时，则应当立即撤销他们的管理访问。有了单独的管理员帐号，就只需撤销该特定员工的帐号。

随着网络内基础设施设备数量的增长，在每个基础设施设备上配置单独的本地管理员帐号的管理负担可能会变得难以应付。因此，建议您通过一个 AAA 服务器来控制管理访问，它可提供基于策略的集中化管理和控制。推荐您部署冗余 AAA 服务器实现高可用性，以防一个或多个服务器临时变为不可用。假如对基础设施设备的所有网络接入全部丢失，网络管理员可能仍然会通过控制台端口，在每个基础设施设备上为本地接入配置一个单独的本地管理员帐号。

AAA 服务器本身可能会参考一个外部目录或数据存储库，例如 AD。这允许网络管理员利用现有的 AD 凭据，而不是在 AAA 服务器内复制它们。通过使用 AD 组，这还可进行扩展，从而为管理员提供基于角色的访问控制 (RBAC)。使用外部目录或数据存储库也可为授予或撤销凭据提供单一点，不仅用于多个基础设施设备的管理访问控制，而且还用于访问组织内的其它资源。

只要有可能，应当选择一个强密码——由最小长度的字母、数字和/或特殊字符组合而成。只要有可能，在禁用帐号一段时间之前，还应当执行不成功尝试访问设备的最大次数。成功和不成功的尝试应当在本地或一个中央登录服务器进行记录。这有助于缓解通过暴力尝试获得对基础设施设备的访问权限这种情况，和/或向有关网络运营人员发出相关警报。只要是支持多个级别的管理访问的地方，就推荐您采取这些措施，其中管理员拥有执行各自相应任务所需的最低访问级别。同时还推荐您限制单一用户名的并行登录次数。

限制对无线基础设施设备发起访问的地点以及所允许的协议也可能是有益的。您可以通过多种方式实现此目的。例如，您可以从无线客户端流量将无线局域网控制器的管理界面部署在一个单独的 VLAN （因此在一个单独的 IP 子网）上。在这种部署中，部署在邻近 WLAN 控制器的第三层交换机上的访问控制列表 (ACL) 可限制对管理界面的访问。这将 ACL 的 CPU 负担从 WLAN 控制器转移到了第三层交换机上。另外，您也可以在 WLAN 控制器上配置一个 CPU ACL 以过滤管理协议。您还可以通过一个无线设备驳回对 WLAN 控制器的管理，如果其意图是从一个中央网络运营中心来管理无线基础设施，这种方法也可能会提供额外的安全性。

只要有可能，对无线基础设施设备的访问应当是通过安全的协议，例如 HTTPS 和 SSHv2。只要有可能，应当禁止通过非加密协议（例如 HTTP 和 Telnet）的访问。这可在管理会话内保护信息的机密性。当使用 SNMP 时，推荐您只要有可能就启用 SNMPv3（简易网络管理协议第 3 版）。SNMPv2c 依赖于在整个网络中以明文发送的一个共享社区字符串。使用 SNMPv2c 时请小心谨慎，特别是将 SNMP 用于读/写访问时。SNMPv3 使用独特的凭据（用户 ID/密码），同时也可以向 SNMP 流量提供加密和数据验证服务。

本地特征分析

思科 ISE 目前提供一组丰富的功能，可提供设备识别、接入、姿态和策略。作为替代选项，WLC 上的本地特征分析基于 HTTP 和 DHCP 等协议对设备进行特征分析，从而识别出网络上的终端设备。用户可以配置基于设备的策略，并根据用户或设备策略在网络上执行。WLC 还将基于按用户或按设备的端点以及按设备的适用策略显示统计数据。借助本地特征分析，您可以在 WLC 本身内部小规模地实施自带设备 (BYOD)。

特征分析和策略实施被配置成两个单独的组件。WLC 上的配置是基于针对加入网络的特定客户端所定义的参数。值得注意的策略属性包括：

- **角色**——定义用户类型或用户所属的用户组（例如：学生或员工）
- **设备**——定义设备类型（例如：Windows 设备、智能手机或苹果设备）
- **当日时间**——允许在端点获准进入网络的当日时间定义配置
- **EAP 类型**——校验客户端使用的 EAP 方法

只要策略与属性相符，上述参数是可配置的。WLC 有了一个与上述按端点的参数相对应的匹配后，策略实施便进入视野。策略实施将基于一些会话属性，例如：

- VLAN
- ACL
- 会话超时
- QoS
- 休眠客户端
- Flexconnect ACL
- AVC 配置文件（已添加至 8.0 版本）
- mDNS 配置文件（已添加至 8.0 版本）

用户可以配置这些策略并在端点实施特定策略。对无线客户端会基于 MAC、OUI、DHCP 和 HTTP 用户代理进行特征分析（为实现成功的 HTTP 特征分析，需要有效的互联网）。WLC 使用这些属性和预先定义的分类配置文件来识别设备。

用于核对 CUWN (AIREOS) 8.1 最佳实践的工具

为了方便网络部署工程师，从 CUWN (AireOS) 软件 8.1 版本开始，无线局域网控制器控制面板内提供一份最佳实践核对表。这份核对表是用于微调 WLC 配置，以匹配思科建议的最佳实践。核对表对控制器上的本地配置与推荐的最佳实践进行比较，并突出所有不同的功能。核对还提供一个简单的配置面板，以启用最佳实践。强烈推荐将最佳实践用于涉及 WLC 的 WLAN 部署。

最佳实践工具可核对这些功能并提供有关对其遵守的反馈。

- AVC 可视性
- 最小流氓设备 RSSI 阈值

- 负载均衡
- 本地特征分析
- 控制器高可用性
- NTP
- 快速 SSID
- mDNS 网关
- 无线管理
- 用于管理的 HTTPs
- Aironet IE
- 组播转发
- 组播移动性
- 802.1x 无线局域网
- 流氓设备策略
- SSH/telnet 接入
- 客户端排除
- 传统 IDS
- 本地管理密码策略
- 用户登录策略
- CPU ACL
- 高 SSID 计数
- 客户端频段选择
- 自动动态信道分配
- 自动发射功率控制
- 自动覆盖空洞检测
- CleanAir 检测
- 事件驱动 RRM

园区设计中的常用组件

使用思科 SECURE ACS 的设备管理

随着网络设备和管理员数量的增加，如果没有一个集中化的访问和身份策略实施点，则很难确保网络的可靠性。

思科 ACS 作为一个集中化的 AAA 服务器运行，在单一解决方案中结合了用户验证、用户和管理员访问控制以及策略控制。思科 Secure ACS 运用一个基于规则的策略模型，除用户身份以外，它还允许安全策略基于许多不同的属性和条件来授予访问权限。

思科 Secure ACS 的功能搭配网络设备上的 AAA 配置减少了将静态的本地帐户信息置于每个设备上所带来的问题。思科 Secure ACS 对身份验证提供集中化的控制，这使组织可以快速为用户授予或撤销对任何网络设备的访问权限。

将用户以基于规则的方式映射到身份群组，可以基于外部目录提供的信息或诸如 Microsoft Active Directory 等身份存储库。网络设备可被分类为多个设备群组，这可以基于位置、制造商或者在网络中的角色等属性充当一种层次结构。身份和设备群组的结合使您能够轻松创建授权规则，它可以定义哪些网络管理员可以对照哪些设备进行身份验证。

这些相同的授权规则允许特权级授权，它可用于授予访问设备上的命令的有限权限。例如，一个规则可以授予网络管理员完全访问所有命令的权限，或者将帮助台用户限定为监控命令。

使用思科 PRIME 基础设施的园区部署

随着网络及其所支持的服务数量持续演变，网络管理员保持并改进效率和生产力的责任也随之增长。使用网络管理解决方案可以实现并提升网络管理员的运营效率。

思科 Prime 基础设施是一个复杂的网络管理工具，它有助于支持对您组织的运营至关重要的网络技术和服务的端到端管理；它使网络管理功能与网络管理员履行职责的方式协调一致。思科 Prime 基础设施提供一个直观的、基于 web 的 GUI，它可从网络内的任何地方访问，并使您可以完整地查看网络使用和性能。

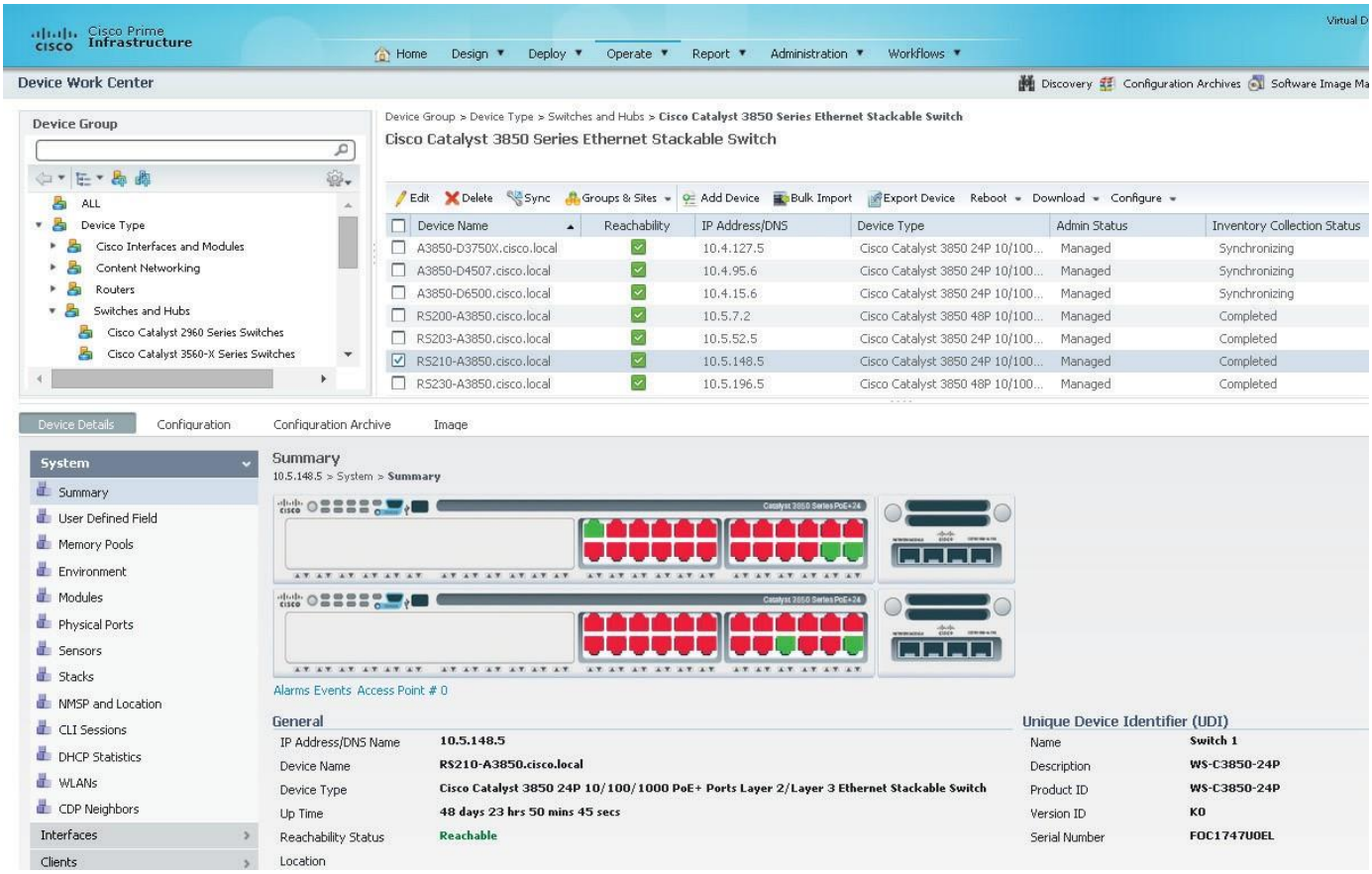
借助一个园区网络及其所支持的服务，思科 Prime 基础设施可在日常网络运行中发挥至关重要的作用。

设备工作中心

思科 Prime 基础设施包含设备工作中心。可在设备工作中心找到的一些功能包括：

- **发现**——建立并维护一个最新的受管设备清单，包括软件映像信息和设备详细配置信息。
- **配置存档**——为所有受管设备维护配置文件多次迭代的活动档案。
- **软件映像管理**——使网络管理员可以从 Cisco.com、受管设备、URL 或文件系统导入软件映像，然后将它们分配到单一设备或一组设备上。

图 30　　设备工作中心



配置模板和任务

通过使用配置任务功能将配置模板应用到许多设备上，管理员可节省大量的工作时间。思科 Prime 基础设施可提供一系列模板，您可以利用它们创建一个配置任务，从而根据需要提供针对设备的特定值。对于其它配置需求，思科 Prime 基础设施使您可以定义您自己的模板。

警报、事件和 Syslog 报文

思科 Prime 基础设施提供警报和事件功能，它可统一显示详细的调查分析。该功能提供可执行的信息，并可借助思科技术支持中心自动提交服务请求。

报告

思科 Prime 基础设施针对您可以配置、安排时间和查看的所有报告为您提供单一的发送点。报告发送台页面 (Report Launch Pad page) 提供对 100 多个报告的访问，您可以根据需要自定义每个报告。

CleanAir 支持

思科 Prime 基础设施支持对已启用 CleanAir 的无线接入点的管理，从而使管理员可以看到干扰事件。

网络分析模块支持

为了增加对您网络的可视性，思科 Prime 基础设施支持对思科网络分析模块产品的管理和报告。

MERAKI 云管理

Meraki 的云计算型管理对 Meraki 的有线和无线网络硬件提供集中化的可视性和可控性，而没有无线控制器或重叠管理系统的成本和复杂度。

园区服务质量

因为实时通信流量对延迟和丢弃非常敏感，所以网络必须确保这种类型的流量获得优先处理，从而不中断音视频的流式传输。QoS 是对这种需求给出答案的技术。

在富媒体园区网络中 QoS 的职责在于管理丢包，在那里高带宽链路出现近乎毫秒级的瞬时拥塞即可导致缓冲溢出和糟糕的用户体验。园区 QoS 的另一个目标是将策略应用到边缘，从而允许对流量的一致处理，以在整个企业网中实现可预测的用户体验。

QoS 允许组织定义不同的流量类型并对实时流量实现更有确定性的处理。QoS 在拥塞处理中尤其有用，其中一个完整的通信信道可能会防止语音或视频流在接收侧易于识别。拥塞常见于链路被来自众多设备的汇聚流量超额订用，以及当链路至设备的流量来自于具有更高带宽的上行链路时。QoS 并不是创建带宽，而是从一个类中获取带宽然后把它给另一个类。

在园区有线局域网内，思科将 QoS 配置文件尽可能保持简单，同时确保支持需要特别交付的应用。这种方法为在整个网络中实施 QoS 建立了一个牢固、可扩和模块化的框架。

在网络内实施 QoS 的主要目标包括：

- 为获得支持的实施应用加快通信服务交付。
- 为业务关键型应用提供业务连续性。
- 当出现拥塞时确保所有其它应用之间的公平性。
- 降低后台应用和以娱乐为主的非业务应用的优先级，因此这些应用不会延迟交互式或业务关键型应用。
- 在网络周围提供一个受信任的边缘，从而保证用户不会随意注入他们自己的优先级值，并允许组织在整个网络中信任已标记流量。

为了实现这些目标，这种设计在整个网络中按如下方式实施 QoS：

- 在网络内为需要特殊处理的流量（例如，实时语音、实时视频、高优先级数据、交互式流量、批流量，以及默认类）建立有限数量的类（即 1 至 8 个类）。
- 将应用划分为不同的流量类。
- 将特殊处理应用到流量类，从而实现预期网络行为。

附录—术语表

3SS 三空间流

AAA server 身份验证、授权和计费 (AAA) 服务器

ACL 访问控制列表

ACS 思科访问控制服务器

AP 接入点

AQ 空气质量

AUP 可接受的使用策略

AVC 思科应用可视性和可控性

BYOD 自带设备

CAPWAP 无线接入点控制和分配协议

Cisco ACS 思科访问控制服务器

Cisco AVC 思科应用可视性和可控性

Cisco CMX 思科互联移动体验

Cisco ISE 思科身份服务引擎

Cisco MSE 思科移动服务引擎

Cisco PI 思科 Prime 基础设施

Cisco UPOE 思科通用型以太网供电

Cisco wIPS 思科无线侵入防御系统

CMX 思科互联移动体验

CUWN 思科统一无线网络

DCA 动态信道分配

DFS 动态频率选择

DMZ 隔离区

DPI 深度数据包检测

EAP 可扩展身份验证协议

EUA 最终用户协议

G2 第二代

GLBP 网关负载均衡协议

HA 高可用性

HA SSO 高可用性状态切换

HSRP 热待机路由协议

ISE 思科身份服务引擎

ISM 工业、科学与医学频段

LACP 链路汇聚协议

LAG 链路汇聚

LAN 局域网

mDNS 组播域名服务

MFP 管理帧保护

MIMO 多输入、多输出设计

MMAP 监控模式接入点

MSE 思科移动服务引擎

NBAR2 下一代基于网络的应用识别

PAgP 端口汇聚协议

PHY 物理层

PI 思科 Prime 基础设施

PMF 受保护的管理帧

PSK 预共享密钥

QAM 正交调幅

QoS 服务质量

RBAC 角色型访问控制

RF 射频

RRM 射频资源管理

RSSI 接收信号强度

SSID 服务集标识符

SSO 状态切换

STP 生成树协议

TPC 发射功率控制

TTL 生存时间

TxBF 基于标准的传输波束成形

UPOE 思科通用型以太网供电

VLAN 虚拟局域网

VRRP 虚拟路由冗余协议

VSS 虚拟交换系统

vWLC 虚拟无线局域网控制器

WAAS 宽域应用服务

WAN 无线局域网

WIDS 无线入侵检测系统

wIPS 思科无线侵入防御系统

WLAN 无线局域网

WLC 无线局域网控制器

WSM 无线安全模块

请使用反馈表提交有关本指南的意见和建议。

美洲总部
Cisco Systems, Inc.
加州圣荷西

亚太总部
Cisco Systems (USA) Pte. Ltd.
新加坡

欧洲总部
Cisco Systems International BV Amsterdam,
荷兰

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 中列出了各办事处的地址、电话和传真。