aruba
a Hewlett Packard Enterprise company

ArubaOS 8 基本原理

作者:

Syed Ahmed
Jerrod Howard
Kevin Marshall
Mak Moussa
Andrew Tanguay

供稿人:

Shiv Mehra
Dipen Vardhe

基本原理指南

版权信息

开源代码

本产品包含获得 GNU 通用公共许可、GNU 宽通用公共许可和/或某些其他开源许可授权的代码。根据请求，可提供与此类代码相应的源代码的完整机器可读副本。这项服务对收到此信息的任何人都有效，其有效期为自由 Hewlett Packard Enterprise Company 最终发布此产品版本的日期之后三年。要获得此类源代码，请将金额为 10.00 美元的支票或汇票发送至：

Hewlett Packard Enterprise Company
收件人：法律总顾问 (General Counsel)
3000 Hanover Street
Palo Alto, CA 94304
USA

www.arubanetworks.com

3333 Scott Blvd

Santa Clara, CA 95054

电话：1-800-WIFI-LAN (+800-943-4526)

传真：408.227.4550

修订历史记录

下表列出了本文档的修订版本：

版本	日期	变更说明
1.1.0	2018/6/1	对“控制器模式比较”、“授权更改”和“许可概念”进行了编辑
1.0.0	2018/5/28	最初发布

表 1 *修订历史记录*

关于本指南

概述

Aruba 部署指南是最佳实践建议文档，其中专门概述 Aruba 技术的工作方式，以及使部署 Aruba 解决方案的客户能够获得最佳效果。本文不仅旨在介绍部署指南，而且还提供 Aruba 技术的说明、产品选择建议、网络设计决策、配置程序和最佳实践。此外，ArubaOS 8 的 Aruba 文档套件还包含一个参考模型，其有助于了解针对常见客户部署方案的 Aruba 技术和设计。客户可依赖这些久经考验的设计以在其生产环境中迅速部署 Aruba 解决方案，并且不必担心解决方案的性能和扩展能力达不到预期水平。

目标受众和假设

本指南面向负责在客户现场部署和配置 AOS 8 解决方案的管理员。读者应至少对 WLAN 概念有基本的了解。这是 ArubaOS 的基本设计指南，其假设读者至少对基本无线概念以及 Aruba 技术有一定了解。

相关文档

以下文档可作为本指南的补充参考资料：
ArubaOS 8 用户指南
ArubaOS 8 CLI 参考指南
Aruba 解决方案交换

范围

“已验证参考设计”(VRD) 系列文档侧重于 Aruba 技术和部署模式的特定方面。这些指南共同提供了一个用于理解和部署 Aruba 无线局域网 (WLAN) 的结构化框架。VRD 系列有四个文档类别：

- **基础**指南说明 Aruba WLAN 的核心技术。这些指南还描述计划、操作和故障排除部署的不同方面
- **基本设计**指南描述最常见的部署模式、建议和配置
- **应用**指南以基本设计为基础。这些指南提供与部署语音、视频或室外园区扩展等特定应用相关的具体信息。
- **专业部署**指南介绍与高密度 WLAN 部署等常见基本设计部署模式显著不同的部署。

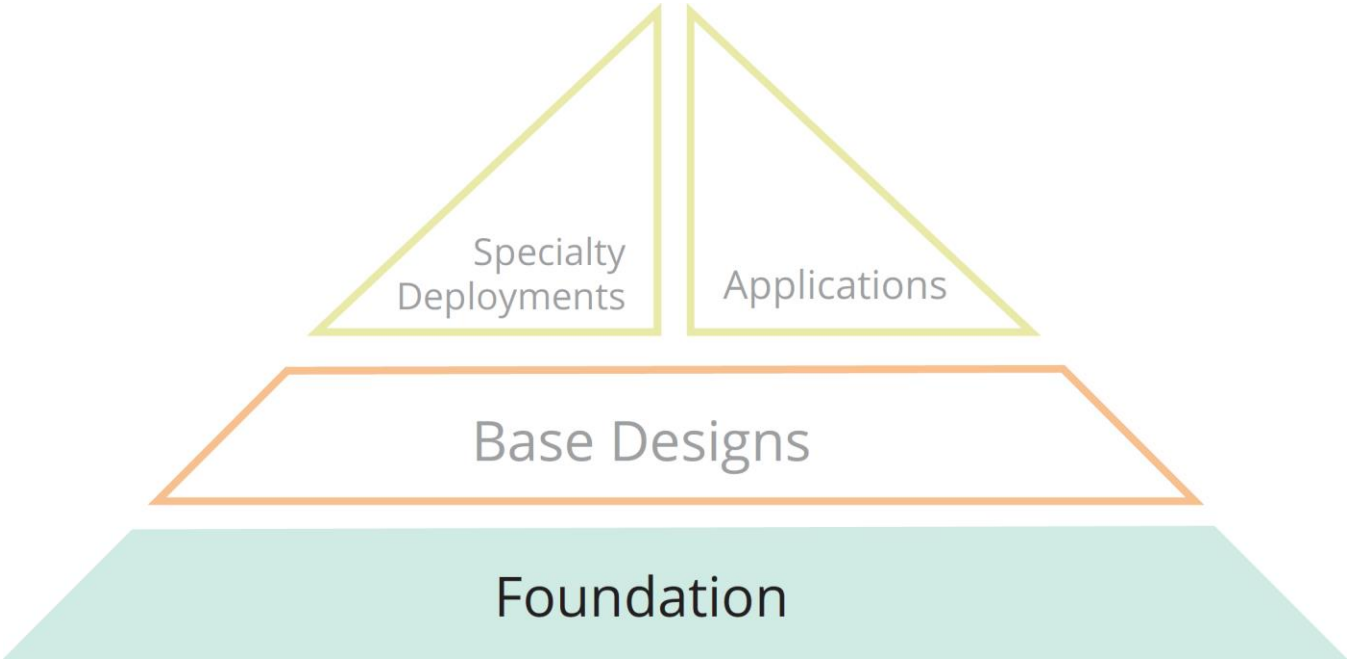


图 1 *Aruba 参考架构*

信息图标

在整个指南中使用了以下信息图标：

NOTE	表示有帮助的建议、相关信息以及需要记住的重要事项。
CAUTION	表示存在硬件损坏或数据丢失的风险。
WARNING	表示存在人员受伤或死亡的风险。

惯例

印刷惯例

在整个手册中使用以下惯例来强调重要概念：

样式类型	描述
斜体	斜体用于强调重要项以及标记文档标题。
粗体字	粗体字表示应在图形用户界面（GUI）中选择的选项。尖角括号表示选项是 GUI 中的路径的一部分。
命令文本	采用此字体中的命令文本将显示在框内，指示可输入到命令行界面（CLI）中的命令。
<变量>	在命令示例中，单尖括号中的斜体字代表应使用适合您特定情况的信息加以更换的项目。例如： `# send <text message>` 在本示例中，您需要在系统提示时完全按照所示内容键入“send”，然后键入您想要发送的消息文本。不要键入尖括号。
`[Optional]`	括号中的命令示例为可选。不要键入括号。
`{Item A | Item B}`	在该命令示例中，大括号中用竖线分开的项目代表可用选择。仅输入一个选择。不要键入括号或竖线。

表 2 *印刷惯例*

图形图标

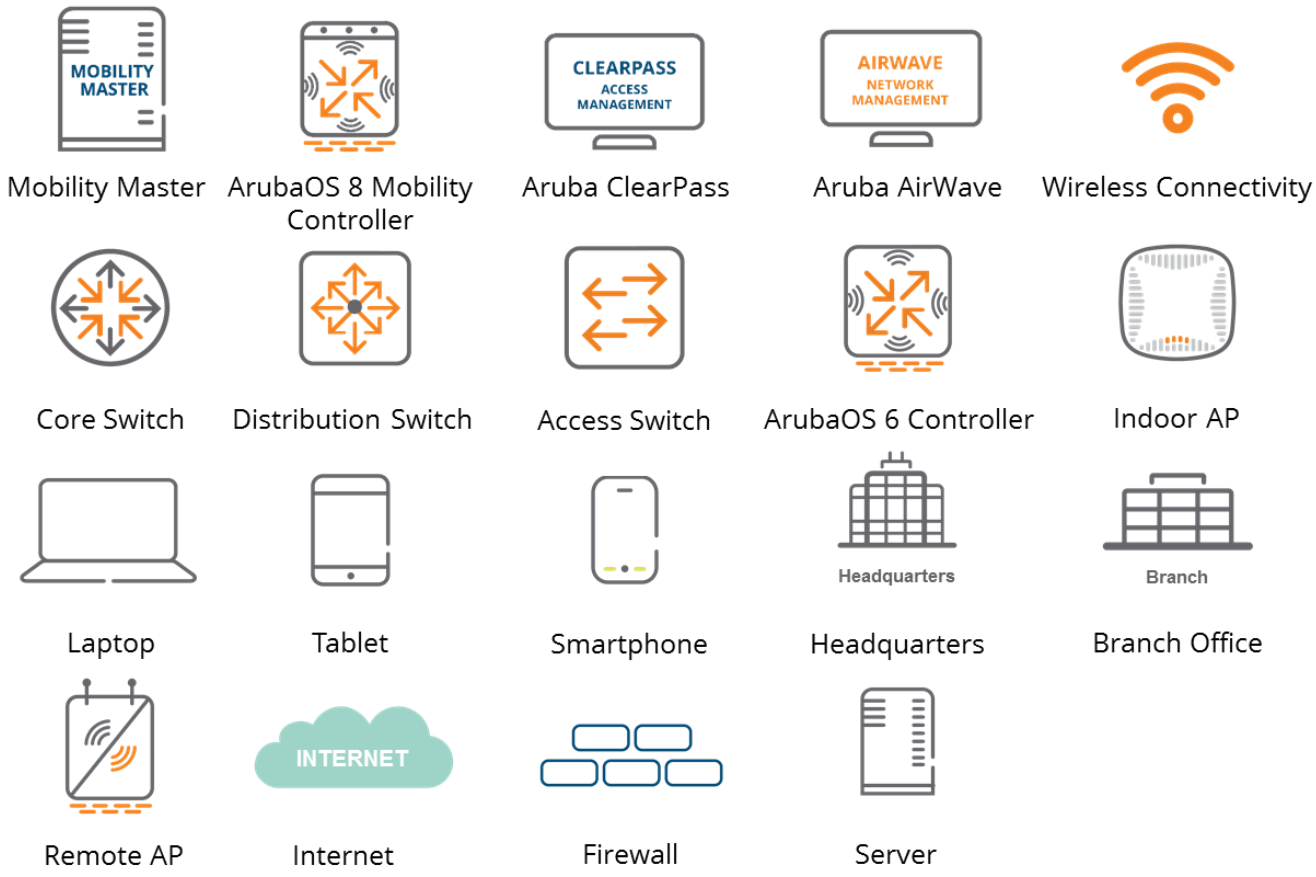


图 1 *VRD 图标集*

缩写词列表

缩写	定义
A-MPDU	聚合媒体访问控制分组数据单元
A-MSDU	聚合媒体访问控制服务数据单元
AAA	身份验证、授权和计费
AAC	AP 锚点控制器
ACL	访问控制列表
ACR	高级密码学
AM	无线监测器
AP	接入点
API	应用程序编程接口
ARM	自适应射频管理
ASP	Aruba 支持门户网站
BLMS	备用本地管理交换机
CoA	授权变更
CLI	命令行界面
CPSec	控制平面安全
CPU	中央处理器
DC	数据中心
DLNA	数字生活网络联盟
DNS	域名服务
DHCP	动态主机配置协议
DMZ	非管制区域
DPI	深度分组检测
FQDN	完全限定的域名
GRE	通用路由封装
GUI	图形用户界面
HA	高可用性
HMM	硬件 MM
HTTP	超文本传输协议
HTTPS	HTTP 安全
IAP	Instant 接入点

IDF	中间配线架
IKE	Internet 密钥交换
IP	Internet 协议
IPsec	Internet 协议安全
IPv4	Internet 协议版本 4
IPv6	Internet 协议版本 6
JSON	JavaScript 对象表示法
LACP	链接聚合控制协议
LAN	局域网
LAG	链接聚合连接
LMS	本地管理交换机
LSM	可加载服务模块
MAC	媒体访问控制
MC	移动控制器
MCM	主控制器模式
mDNS	多播域名服务
MD	托管设备
MD	移动设备
MDF	主配线架
MM	Mobility Master
MM-HW	Mobility Master - 硬件
MM-VA	Mobility Master – 虚拟设备
MN	托管节点
MNP	MyNetworking 门户网站
NAS	网络接入服务器
NAT	网络地址转换
NBAPI	北向应用程序编程接口
NVF	网络虚拟化功能
PAPI	专有访问协议接口
PAT	端口地址转换
PEF	政策强制防火墙
PSK	预共享密钥

QoS	服务质量
RADIUS	远程身份验证拨入用户服务
RAM	随机存取存储器
RAP	远程接入点
RF	射频
RFP	射频保护
S-AAC	备用 AP 锚点控制器
S-UAC	备用用户锚点控制器
SDN	软件定义网络
SfB	Skype for Business
SIP	会话初始协议
SSID	服务集标识符
SVI	交换机虚拟接口
UAC	用户锚点控制器
UCC	统一通信与协作
UCM	统一通信管理器
UDLD	单向链路检测
URL	统一资源定位符
VAP	虚拟接入点
VIA	虚拟 Internet 接入
VIP	虚拟 Internet 协议地址
VLAN	虚拟局域网
VM	虚拟机
VMC	虚拟 MC
VMM	虚拟 MM
VPN	虚拟专用网
VPNC	虚拟专用网集中器
VRRP	虚拟路由器冗余协议
VSF	虚拟交换框架
WLAN	无线局域网
XML	可扩展标记语言
ZTP	零接触配置

架构

现代化生产网络中几乎所有最终用户设备都是无线设备，包括未配备以太网端口的笔记本电脑。甚至有线电话也被 Skype for Business (SfB) 等统一通信应用程序所取代。这些趋势正迫使企业日益依赖无线局域网 (LAN) 来满足其业务需求。由于对无线 LAN 的这种极大依赖性，网络管理员必须设计复杂的网络来支持各种类型的应用程序、用户和设备，同时不影响安全性。本部署指南将概述通过 Aruba 的先进 ArubaOS 8 解决方案实现的所有功能，这些功能有助于应对现代化生产网络中遇到的这些挑战。

ArubaOS 是支持所有 Aruba 移动控制器 (MC) 和控制器托管无线接入点 (AP) 的操作系统。凭借广泛的集成技术和功能，ArubaOS 8 可提供统一的有线和无线接入、无缝漫游、企业级安全性，以及具有所需性能、用户体验和可靠性的高可用性网络，以支持高密度环境。

产品系列

下表列出了 ArubaOS 8 中支持的控制器及其功能：

控制器系列	控制器型号	AP 数目	用户数目	防火墙 (Gbps)
70xx	7005	16	1,024	2
	7008	16	1,024	2
	7010	32	2,048	4
	7024	32	2,048	4
	7030	64	4,096	8
72xx	7205	256	8000	12
	7210	512	16000	20
	7220	1,024	24000	40
	7240	2,048	32000	40
	7280	2,048	32000	100

表 3 *ArubaOS 8 产品系列*

ArubaOS 8.x 不支持 3000 或 600 系列控制器。

ArubaOS 6 控制器模式

ArubaOS 6 支持以下控制器模式：

主模式

如果在主模式下部署控制器，则管理员负责所有配置，包括 IP 地址、许可、WLAN、AP 组、用户角色等。管理员通过连接到该控制器的控制台并浏览命令行界面 (CLI) 向导来应用此配置。

图 2 *处于主模式的 ArubaOS 6 控制器*

主模式控制器可部分管理本地控制器以及完全管理分支控制器。所有 70xx 系列控制器和 72xx 系列控制器均能够在主模式下运行，但 70xx 系列主控制器无法管理其他 70xx 系列分支控制器。

本地模式

与主控制器类似，本地控制器最初需要由管理员使用串行控制台加以配置，以分配 IP 地址、虚拟局域网 (VLAN) 和其他网络相关参数。但无线局域网 (WLAN) 和 AP 组等全局配置参数是从作为用于全局配置的单一管理平台的主控制器来继承。从主控制器继承的全局配置无法通过本地控制器图形用户界面 (GUI) 进行修改，并且将显示为灰色。所有 70xx 系列控制器和 72xx 系列控制器均能够在本地模式下运行。

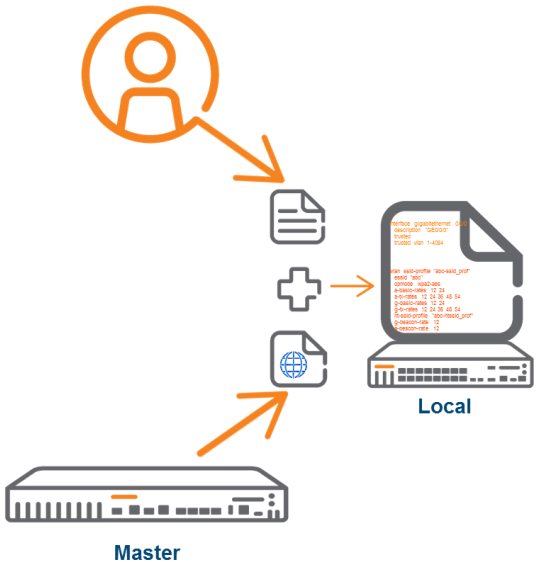


图 3 *处于本地模式的 ArubaOS 6 控制器*

分支模式

分支模式是相对较新的控制器运行模式，该模式是在 6.4.3 版本中引入的模式。该模式一般在分支机构和远程办事处位于不同地理位置的分布式企业中使用。默认情况下启用分支模式，但与主模式和本地模式不同，分支模式仅支持 70xx 系列控制器。所有 70xx 系列控制器都带有动态主机配置协议 (DHCP) 客户端功能，默认情况下启用其在 VLAN 4096 上的最后一个端口。可使用 DHCP 选项 43 将主控制器 IP 分配给分支控制器。或者，分支控制器可通过 Aruba Activate 使用零接触配置 (ZTP) 来获取主控制器 IP。

与本地控制器相比，分支控制器从其主控制器接收其整个配置。分支控制器 GUI 或 CLI 中不允许有写入权限。主控制器上启用了一个名为 Smart Config 的特殊 GUI，用于分支控制器管理和配置。在分支模式下运行的控制器具有与其他控制器完全相同的功能，但仅在 Smart Config 中显示的功能能够启用。下图展示了如何配置分支控制器。

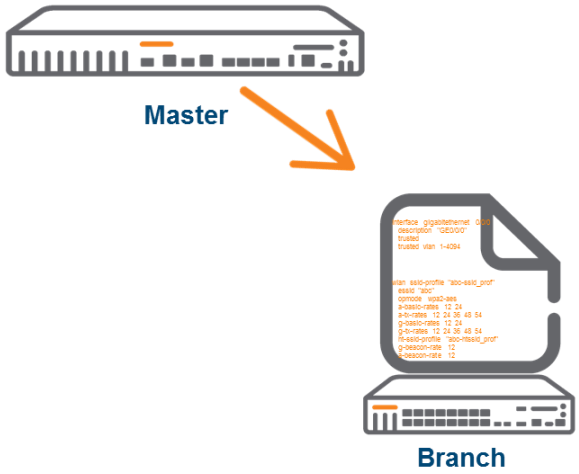


图 4 *处于分支模式的 ArubaOS 6 控制器*

独立

当架构设计需要由单个控制器组成的部署模式时使用独立控制器。独立控制器不能管理本地或分支控制器，并且由于它们本身缺乏冗余，因此在生产环境中极少使用。它们具有与主控制器完全相同的功能，一个明显的例外情况是，它们无法管理其他控制器。

图 5 *处于独立模式的 6.x 控制器*

ArubaOS 6 拓扑结构

典型 ArubaOS 6 控制器拓扑结构的特点在总部园区位置有两个采用主/备用配置的主控制器。主控制器与总部园区的多个本地控制器以及部署在远程位置的任何分支控制器相连。此外还部署了 AirWave 和 ClearPass，以用于网络管理和网络接入控制。

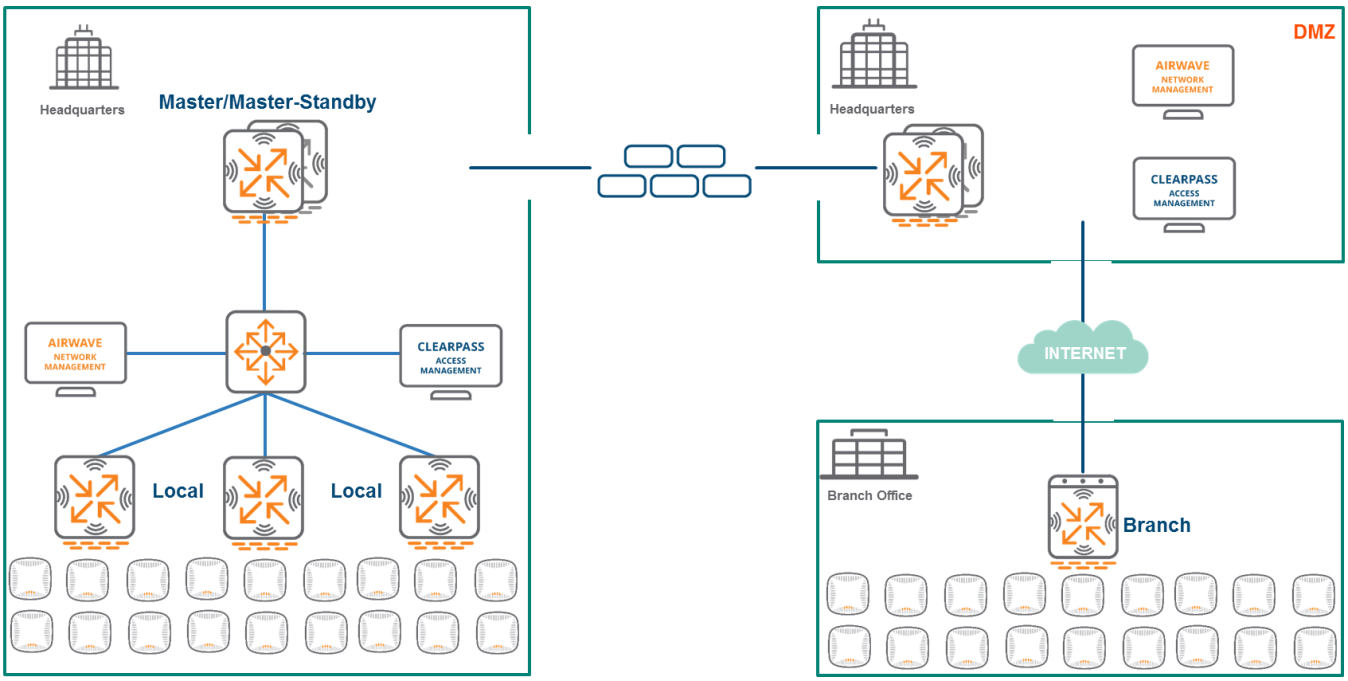


图 6 *典型 ArubaOS 6 拓扑结构*

ArubaOS 8 控制器模式

Mobility Master

ArubaOS 8 引入了 Mobility Master (MM) 的新概念。MM 有两种形式：虚拟 MM (VMM) 或硬件 MM (HMM)。MM 可在基于 x86 的平台上运行，因为 ArubaOS 8 中引入的许多功能需要随机存取存储器 (RAM)、中央处理器 (CPU) 和存储空间，这些都是物理控制器所不支持。类似于在 ArubaOS 6 中配置主控制器的方式，MM 必须由管理员完全进行配置。其主要作用是作为网络的单一配置和映像管理点。此外还可通过北向应用程序可编程接口 (NBAPI) 配置 MM。可将 VMM 安装在 VMWare、KVM 或 Hyper-V 上，这取决于哪一个更适合 VMM 的部署位置。HMM 和 VMM 也可称为 MM-HW 和 MM-VA，意思分别为 MM 硬件和 MM 虚拟设备。

NOTE

不能在 MM 上对接入点进行端接。

图 7 *ArubaOS 8 MM*

主控制器模式

此外，ArubaOS 8 还引入了主控制器模式 (MCM) 的概念，这样无需基于 x86 的设备 (HMM) 或 VMM 即可实现 ArubaOS 6 的无缝过渡。MCM 能够管理其他 MC，但只有 MM 功能的子集可用，并且 AP 无法像使用 MM 时那样进行端接。只有 7030 型号或 72xx 系列控制器支持 MCM。

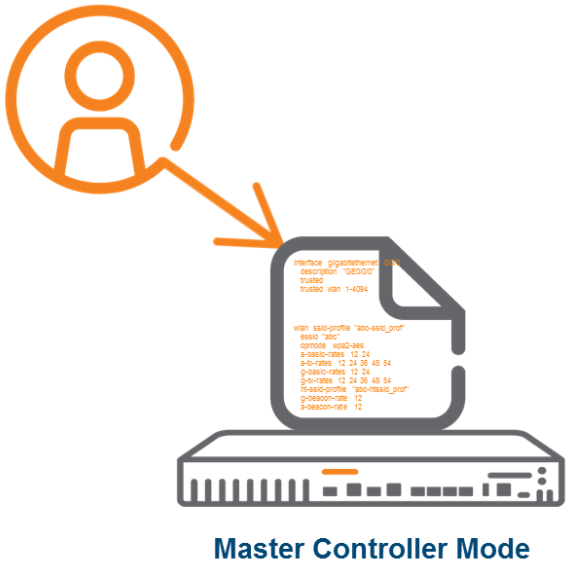


图 8 *ArubaOS 8 主控制器模式*

下表概述了 MCM 支持的并且需要 MM 的一些功能：

支持的功能	不支持的功能
新 GUI、工作流程和分层配置	群集
Multizone	AirMatch
具有自动完成功能的多线程 CLI	集中式应用支持（UCC、AppRF）
WAN 链路绑定和负载分担	实时升级
分布式 UCC、AppRF、ARM 和 AirGroup	集中可见性

表 4 *主控制器模式功能矩阵*

移动控制器

ArubaOS 8 还引入了移动控制器或 MC 的新概念。过去在某些 Aruba 文档中，MC 也称为托管节点 (MN)、托管设备 (MD) 或移动设备 (MD)。就可在 ZTP 和 Aruba Activate 中使用这个方面而言，MC 类似于 ArubaOS 6 中的分支控制器。MC 的最后一个端口在其出厂默认配置中是启用为 VLAN 4094 上的 DHCP 客户端。

NOTE

MM 和 MCM 无法使用 DHCP 选项 43 来使用 MC，因为在使用 DHCP 选项时不支持 MM 或 MCM 证书分发。

与 ArubaOS 6 本地控制器不同，MC 可由 MM 或 MCM 完全加以管理。此外，与 ArubaOS 6 分支控制器不同，管理员可配置 MC 的每个功能。所有 70xx 系列控制器和 72xx 系列控制器都是以 MC 发货。ArubaOS 8 还支持虚拟 MC (VMC)。可将 VMC 部署在 VMWare、KVM 或 Hyper-V 上。MC 可以虚拟专用网集中器 (VPNC) 来配置。

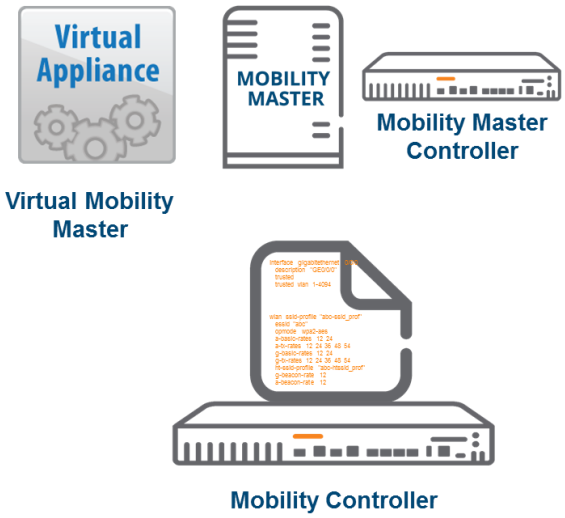


图 9 *MC 管理*

独立控制器

ArubaOS 8 包含配置独立控制器的功能。独立控制器不能由 MM 加以管理，也不能与其他独立控制器进行群集。它在功能上类似于 ArubaOS 6 中的独立控制器，并且支持 Multizone 功能。

独立控制器上未启用 AirMatch 和群集，因为这些功能只能在虚拟机 (VM) 的帮助下来部署。ARM 是唯一可用的 RF 优化方法。WebCC、AppRF、UCC、AirGroup、北向 API、UCM 和 WMS 等其他功能都将类似于在 ArubaOS 6 本地控制器上那样运行。

图 10 *ArubaOS 8 独立控制器*

ArubaOS 8 拓扑结构

从 ArubaOS 6 拓扑结构到 ArubaOS 8 拓扑结构的迁移主要包括将主控制器替换为 MM，以及将所有本地和分支控制器替换为 MC。

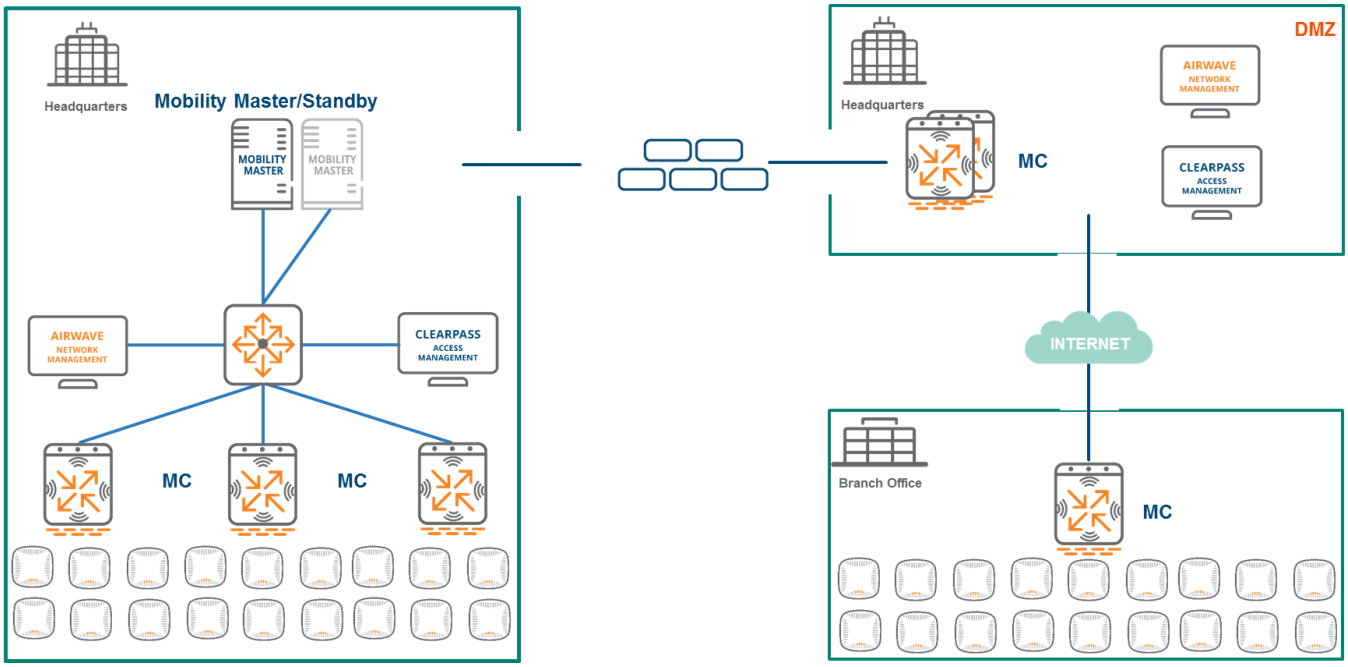


图 11 *ArubaOS 8 拓扑结构*

与 ArubaOS 6 部署相比，ArubaOS 8 代码库包括以下几点区别：

- 引入了基于 VM 的 MM 作为单一配置和映像管理点
- 引入了由 MM 使用 ZTP 完全管理的 MC
- MM 不端接任何 AP
- 所有 72xx/70xx 控制器均可被设置为 MC 或独立控制器
- 作为迁移路径引入了主控制器模式

控制器模式比较

下表概述了基于 ArubaOS 6 的架构中的先前控制器设备名称是如何变更的，并且确定了它们在基于 ArubaOS 8 的部署中相对应的名称：

ArubaOS 6	ArubaOS 8
主控制器	MM（VM 或硬件）或 MCM（仅限 72xx 和 7030）
本地控制器	MC
分支控制器	MC
独立控制器	独立控制器

表 5 *控制器模式摘要*

关于 ArubaOS 8 中的控制器模式，应注意以下要点：

1. ArubaOS 6 主控制器可部分管理本地控制器或完全管理分支控制器
2. 无论将控制器部署在哪里，ArubaOS 8 中的 MM 都可管理所有类型的控制器。
3. ArubaOS 8 中的 MM 与 ArubaOS 6 中的主控制器之间的关键区别是 MM 既不能采用 AP，也不能使 AP 指向 MC
4. MCM 是作为迁移路径引入到 ArubaOS 8，因为它不需要虚拟 MM。
5. 在 ArubaOS 8 中，独立模式以与在 ArubaOS 6 中相同的方式运行。仅在基于硬件的控制器上支持该模式
6. 基于 ArubaOS 6 的本地控制器仅从其主控制器接收部分配置，并且不支持 ZTP。所有 ArubaOS 8 硬件控制器均支持 ZTP
7. ArubaOS 6 中的分支控制器被 MC 所取代，其具有所有配置功能，这与 ArubaOS 6 中 Smart Config 的有限功能不同。

AP 模式

Campus AP

在大多数 ArubaOS 8 拓扑结构中，Campus AP 在与 MC 通信时一般在以下两种模式之一运行：

- 隧道模式
- 解密隧道模式

这两种模式的优点是用户 VLAN 位于控制器上，无需在边缘位置管理它们。必要时可将额外 VLAN 添加到 MC 上行链路已连接的核心交换机。无需将它们添加到 AP 端接所在的边缘交换机。这两种运行模式都可简化网络设计，以及在端接用户方面实现灵活性。

隧道模式

当在隧道转发模式下运行时，AP 处理所有 802.11 关联请求和响应，但通过 GRE 隧道将所有 802.11 数据包、动作帧和 EAPOL 帧发送到 MC 进行处理。然后，MC 移除或添加 GRE 报头，解密或加密 802.11 帧，以及照常将防火墙规则应用于用户流量。

由于在使用 IEEE 802.11ac 标准时引入了更高聚合，因此为在使用隧道模式时实现最大性能优势，应在有线交换机上启用端到端巨型帧支持。在隧道模式下使用控制平面安全 (CPSec) 不是强制性。大多数生产部署利用隧道模式进行 AP 转发，在这种情况下，AP 将 802.11 流量发送到控制器。AP 与 MC 之间的控制和数据平面流量始终被加密。作为最佳实践，Aruba 建议使用隧道模式，因为大多数流量适合标准 1500 字节以太网帧，并且在有线网络上无需特殊处理即可实现最大聚合性能。

当在隧道模式下使用巨型帧时，网络应支持至少 4500 字节的最大传输单元 (MTU) 大小。如果网络无法支持这种大小的 MTU，那么无线聚合效率的优势将因碎片而失去。如果有线网络上没有端到端巨型帧，则在某些情况下 802.11ac 网络可能会出现最多 30% 的性能下降。但应注意，只有在技术演示期间测量峰值网络性能时才会注意到这种对性能的不利影响。在未打开巨型帧的情况下，真实生产网络中的日常运行一般不受影响。

作为最佳实践，Aruba 建议启用端到端巨型帧。

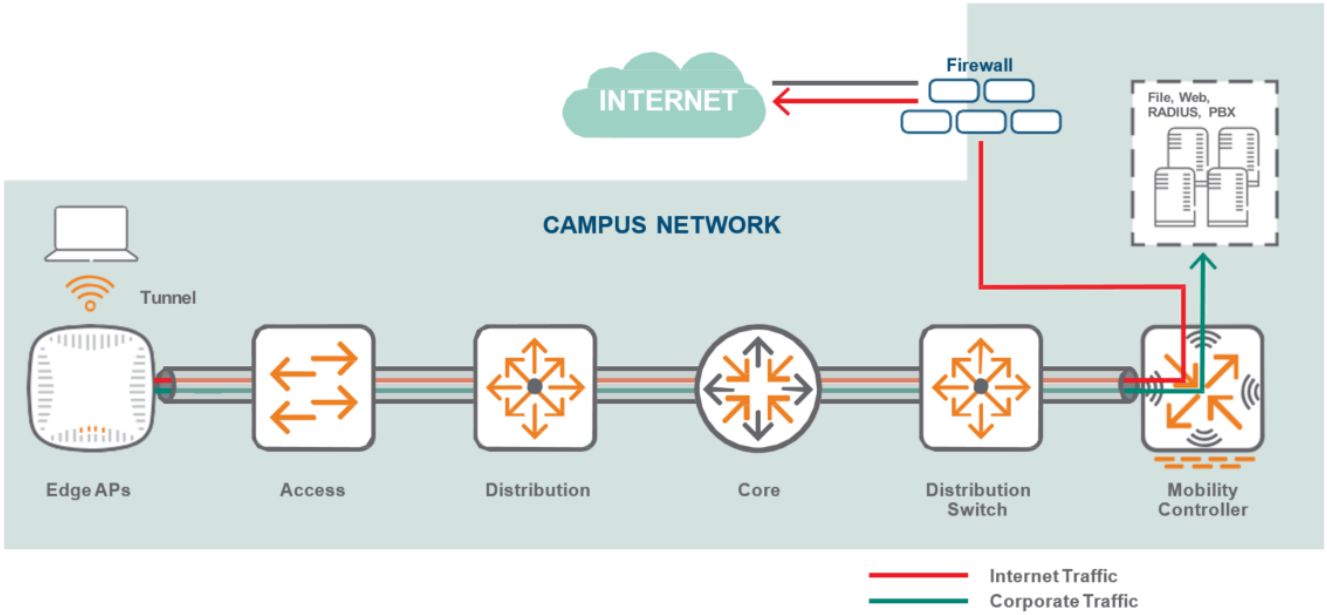


图 12 *隧道转发模式*

解密隧道模式

解密隧道模式可使 AP 客户端对充分利用聚合媒体访问控制 (MAC) 服务数据单元 (A-MSDU) 和聚合 MAC 分组数据单元 (A-MPDU)，无需通过有线网络传输巨型帧。AP 本地执行解密和解聚合。使用解密隧道模式时，必须在 AP 与控制器之间启用控制平面安全 (CPSec)。

CAUTION

解密隧道模式不提供端到端加密。在解密隧道模式下仅加密 AP 与 MC 之间的控制平面流量。

在解密隧道模式下，除执行加密和解密外，AP 还作为客户端与控制器之间的桥梁。MC 仍作为端接数据流量的聚合点。这可使 AP 客户端对利用 WLAN 射频端的 A-MSDU 和 A-MPDU，无需通过有线网络传输巨型帧，因为 AP 本地执行所有组件聚合和解聚合。然后有效负载被发送到控制器，进行防火墙处理和 L2/L3 转发。

解密隧道模式在功能上等同于启用了巨型帧的隧道模式，其一般用于技术演示。务必记住，AP 无线芯片组可为卸载到 AP 硬件的最多 50 个客户端执行加密。涉及超过 50 个客户端的方案可能会因该卸载过程而出现性能小幅下降。

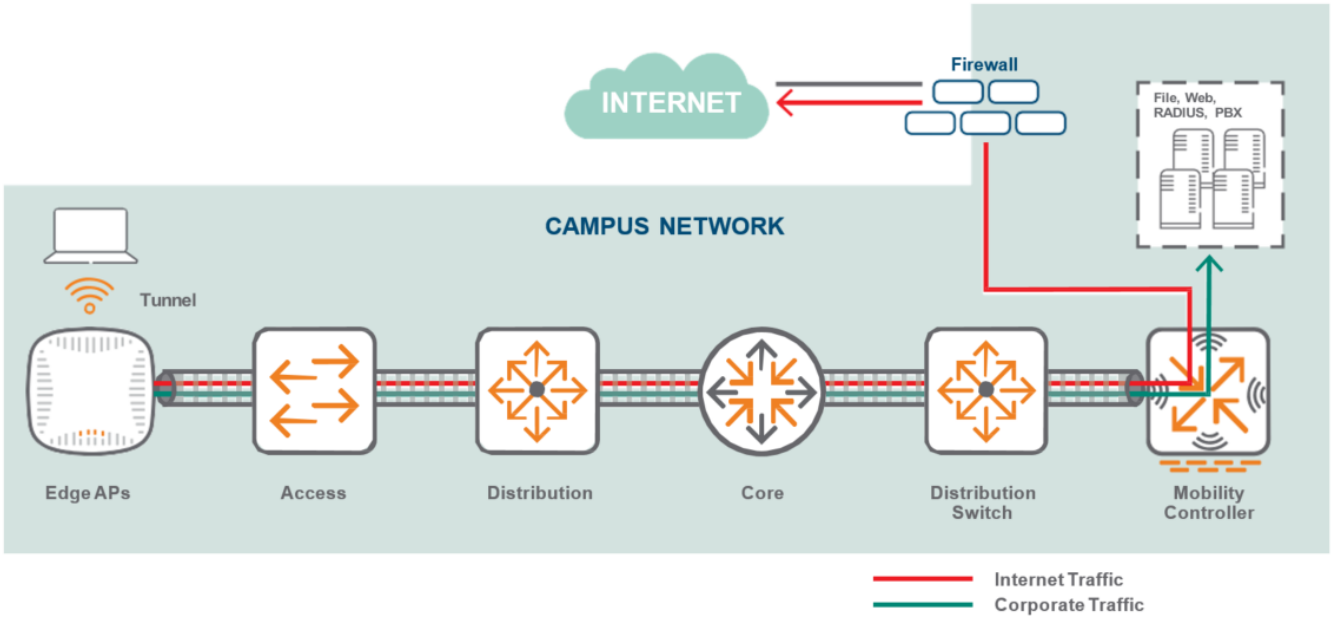


图 13 *解密隧道转发模式*

控制平面安全

CPSec 特性有两个主要功能：

1. 保护 Aruba MC 与它们连接的 AP 之间的控制通道
2. 防止未授权 AP 接入 Aruba WLAN 网络

上述目标是通过以下方式实现：

- 使用专有访问协议接口 (PAPI) 传输的控制流量在传输模式下使用基于证书的 Internet 协议安全 (IPsec) 隧道加以保护
- CPSec 白名单数据库包含已授权连接到 Aruba 控制器并接入 WLAN 网络的 AP 列表

由于在默认情况下启用了 CPSec，因此 MM 在启动后使用其生成的工厂证书对其 MC 进行认证。然后 MC 通过在其工厂默认证书上签名来证明其 AP。这些 AP 已通过 CPSec 白名单获得授权并进入 *certified-factory-cert* 状态后，它们将启动与控制器的安全 PAPI（UDP 8209 内部 IPsec）通信，同步它们的固件，以及下载它们的配置。

使用控制平面安全时的启动过程

下图说明了在使用 CPSec 时 Campus AP 启动过程涉及的步骤：

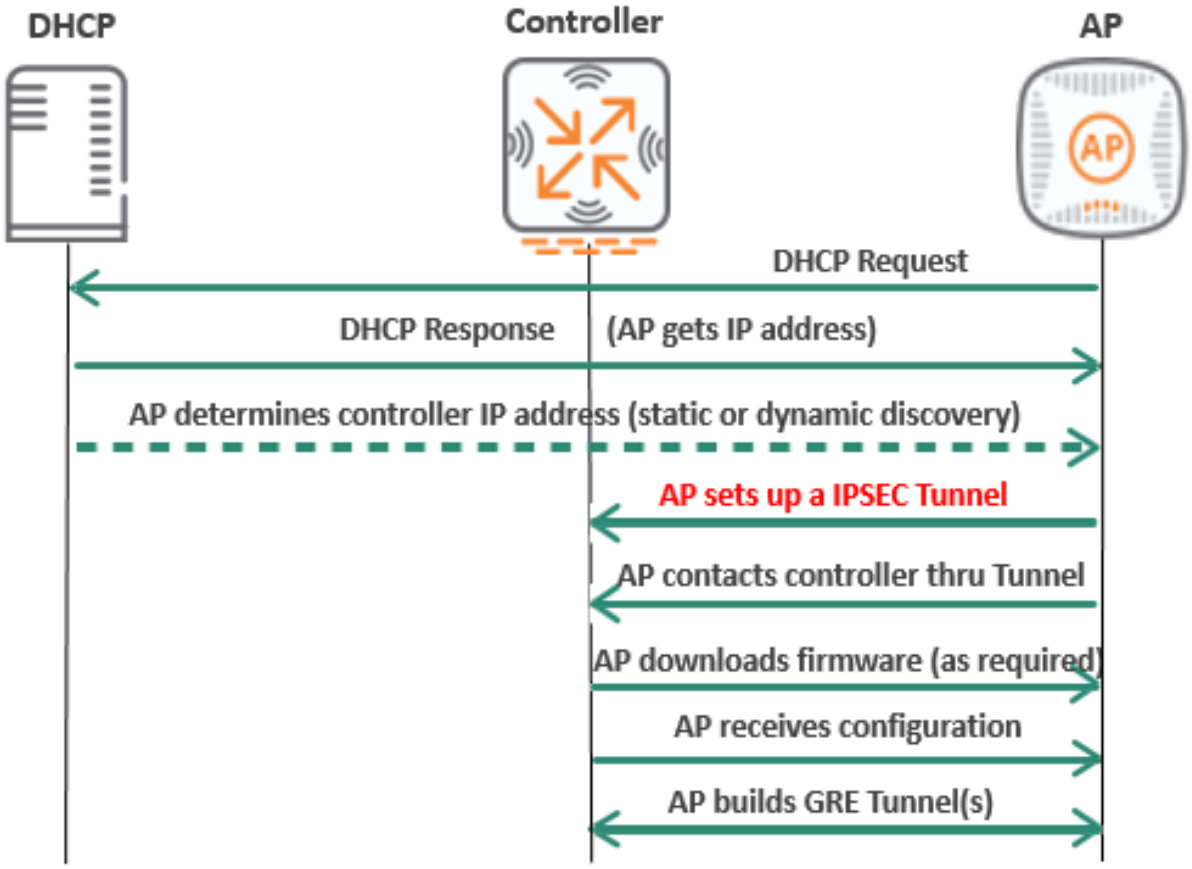


图 14 *使用 CPSec 的 AP 引导过程*

该过程包括以下步骤：

1. AP 发送 DHCP 请求
2. AP 接收 DHCP 响应中的 IP 地址
3. AP 静态或动态确定其控制器的 IP 地址
4. AP 建立与控制器之间的 IPsec 隧道
5. AP 通过 IPsec 隧道与控制器交换 PAPI (UDP 8209)
6. 如果需要，AP 从新发现的 AP 控制器下载固件，以确保版本一致性
7. AP 从控制器接收配置
8. AP 为用户流量创建通用路由封装 (GRE) 隧道

本地管理交换机

在多控制器网络中，每个控制器均通过端接来自 AP 的用户流量，处理此流量以及将此流量转发到有线网络来作为本地管理交换机 (LMS)。LMS 和备用本地管理交换机 (BLMS) 是 AP 的主要和辅助连接点。在使用 LMS 控制器时，AP 依靠心跳超时故障切换到预配置的 BLMS 控制器。

当控制器位于单独 L3 网络中时，无法使用虚拟路由器冗余协议 (VRRP) 来实现冗余。在这种情况下，应使用 LMS 和 BLMS 来实现冗余。

在两个 L3 独立控制器的最基本方案中：

- 作为配置的一部分，AP 查找 aruba-master 并获取 LMS 和 BLMS IP
- AP 在 LMS 控制器上进行端接
- 如果 LMS 控制器出现故障，则连续八次失去心跳将触发 AP 故障切换
- AP 出现在 BLMS 上

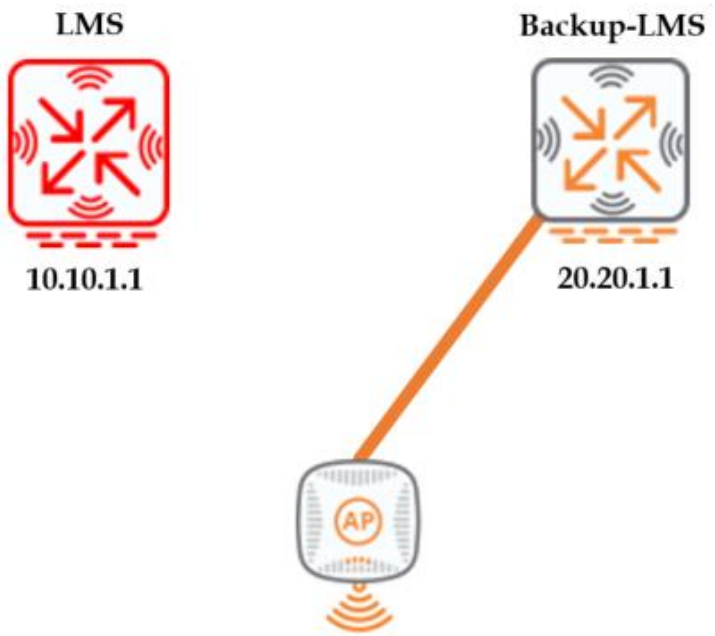


图 15 LMS 和备用 LMS

另一种方案可以是在作为控制器群集的 LMS 上端接 AP。作为配置的一部分，AP 查找 aruba-master 并获取其 LMS 和 BLMS 的 IP 地址。如果 LMS 位于控制器群集中并且 LMS 出现故障，则在该 LMS 上端接的任何 AP 均将尝试故障切换到该群集的其他成员。如果该群集中的其他所有成员均出现故障，则 AP 将仅故障切换到其 BLMS。BLMS 可以是单个控制器，也可以是群集的成员。

NOTE

本文“群集”一章中详细介绍了群集的概念。

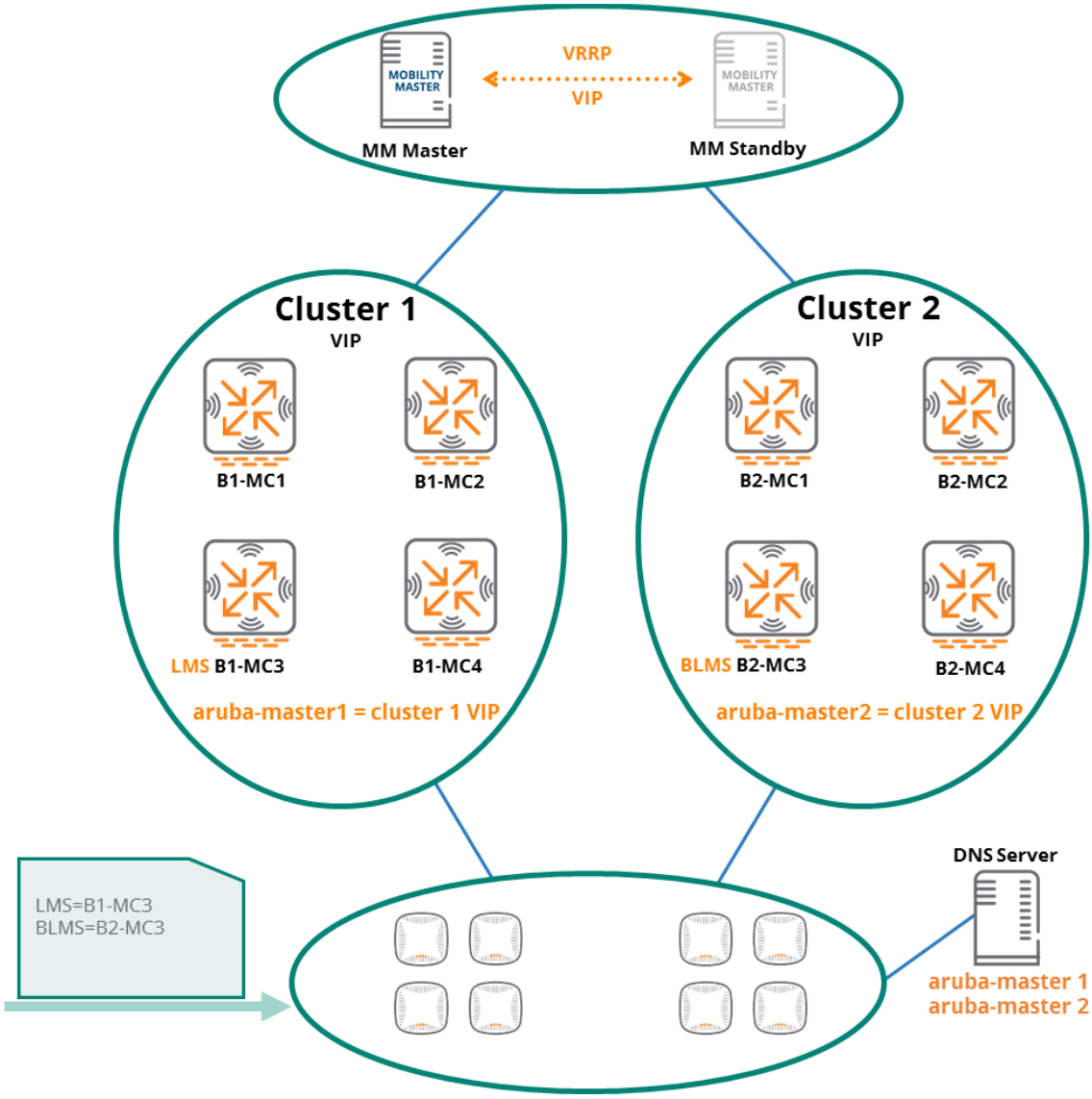


图 16 *群集中的 LMS 和 BLMS 架构*

远程 AP

远程接入点或 RAP 是用于远程接入用例的专用 AP。远程用户一般在家庭办公室、小型卫星办公室、中型分支机构工作，或者在离开酒店、热点或客户位置的路途中工作。其中每一个远程位置都具有不同的连接、容量和使用要求。

传统上，IT 组织使用不同的远程网络架构为每个类别提供服务。例如，微型分支机构使用分支机构路由器将远程站点的 IP 子网与公司网络核心进行互连，而只有一台 PC 或笔记本电脑的远程办公者可使用软件 VPN 客户端。Aruba RAP 为在家工作或在远程分支机构工作的远程企业用户提供解决方案。这些用户无论在哪里，他们都已获授权，可接入他们在主要公司办公室接入的相同无线网络。

隧道模式

当 RAP 在隧道模式下运行时，所有流量都会通过隧道传输回公司网络。客户端和控制器上使用无线加密，RAP 和控制器上使用有线加密。无法访问本地流量，例如打印机、家庭台式机等。

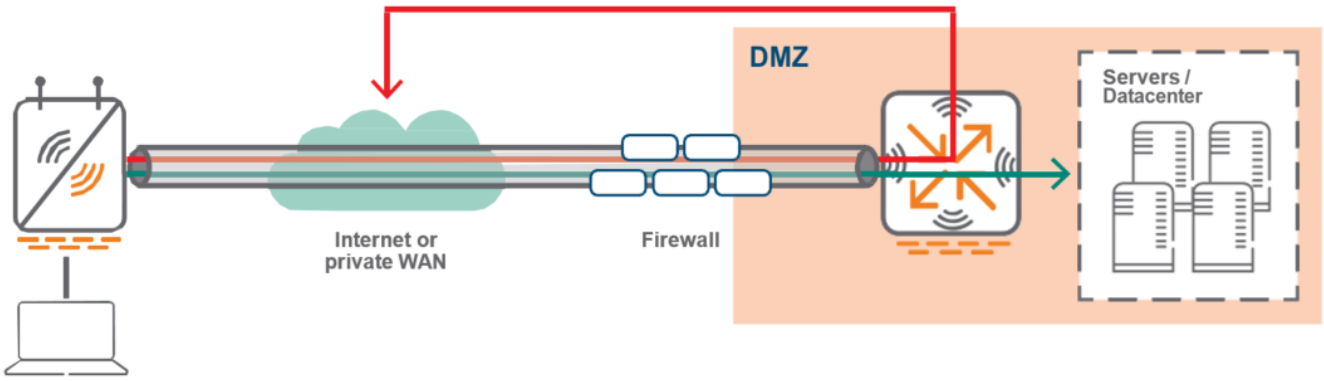


图 17 *RAP 隧道模式*

拆分隧道模式

在拆分隧道模式下允许将非公司流量本地桥接到 Internet，这可减少 RAP 与传输公司流量的控制器之间的隧道带宽。在拆分隧道模式下，客户端和 RAP 上采用无线 (L2) 加密和解密。

公司流量通过隧道传输到非管制区域 (DMZ) 和公司网络其余部分中的控制器。流量使用 GRE 进行封装，以保留 VLAN 标记。所有虚拟接入点 (VAP) 和有线端口均信任和共享此隧道。RAP 与控制器之间的流量使用 IPsec 进行加密。本地流量进行源 NAT（到 enet0 地址），并根据用户角色和会话访问控制列表 (ACL) 在上行链路和下行链路有线接口上转发。

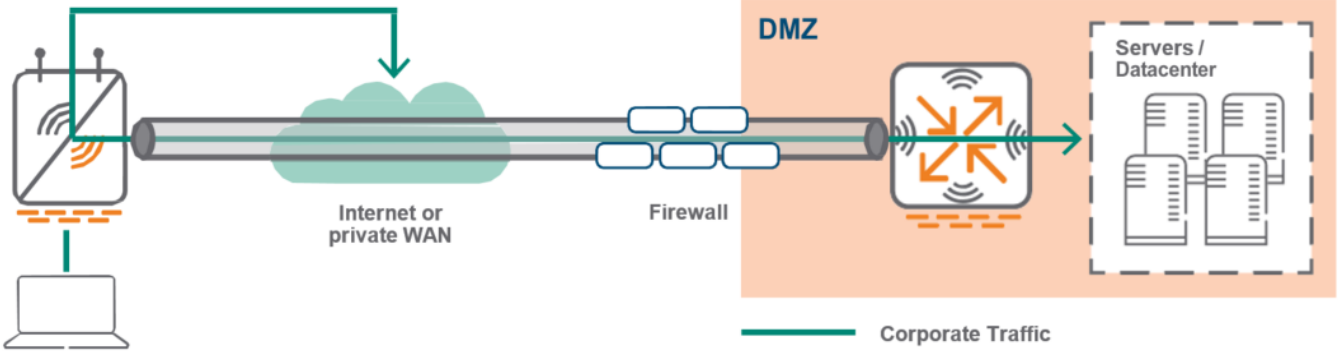


图 18 *拆分隧道模式*

桥接模式

桥接模式主要用于 RAP 和 Instant 访问点 (IAP)。在桥接模式下无法访问公司流量。AP 上行链路上存在到本地网络的用户流量桥。流量不发送到控制器。用户 VLAN 必须存在于网络边缘，而经过身份验证的流量通过隧道传输到控制器。需要使用 CPSec。DHCP、网络地址转换 (NAT) 和端口地址转换 (PAT) 由 RAP 或外部路由器提供。

一般使用桥接模式，以便使打印机或家庭拥有的设备等非公司设备可通过 RAP 上行链路直接接入 Internet（类似于家庭无线路由器操作）。建议不要将对 Campus AP 部署使用此模式，因为在桥接模式下支持较少的功能。

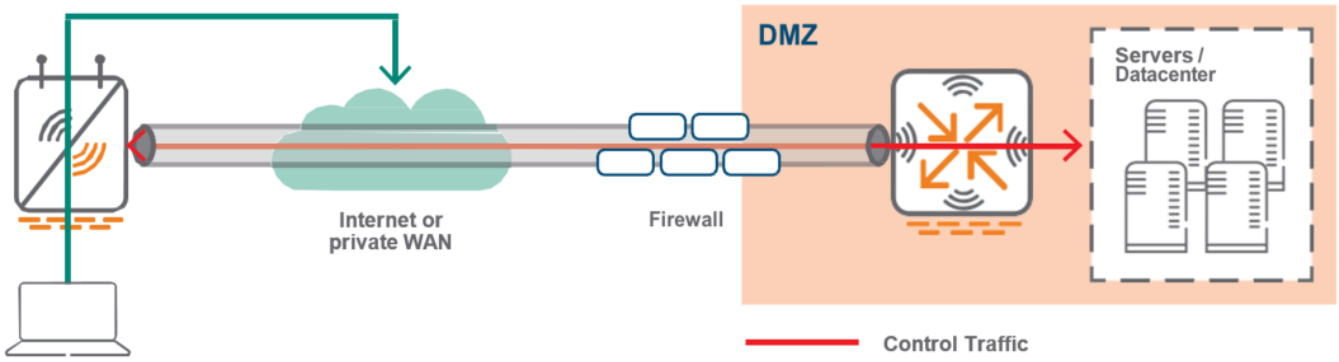


图 19 *RAP 桥接模式*

安全插孔

在提供至少两个以太网端口的任何 Aruba RAP 上均可配置额外端口，以便进行桥接或安全插孔操作。此配置可提供最大灵活性并可在远程站点实现本地有线接入。可针对类似于无线服务集标识符 (SSID) 的所有可用身份验证类型和转发模式在 RAP 上配置额外以太网端口。不能将单个 SSID 配置为同时提供 802.1X 和 MAC 身份验证，但有线端口没有此限制。

CAUTION

不应在同一 SSID 上配置 802.1X 和 MAC 身份验证，因为这样做会导致客户端连接问题。

RAP 启动过程

RAP 启动过程有几个不同阶段：

1. 通过使用 DHCP，RAP 首先在有线接口 (Eth 0) 上获得 IP 地址。在远程部署方案中，当直接连接到 Internet 时，IP 地址一般由 Internet 服务供应商提供
2. 可为 RAP 提供完全限定的域名 (FQDN) 或 MC 的静态 IP。如果使用 FQDN，则 RAP 通过使用 ISP 提供的 DNS 服务来解析主机名。
3. RAP 试图通过以太网接口形成与 MC 的 IPsec 连接。根据配置类型，RAP 的证书或 Internet 密钥交换 (IKE) 预共享密钥 (PSK) 用于完成第 1 阶段协商，XAuth（IKE 第 1 阶段的扩展）用于对 RAP 进行身份验证。
   - 如果使用 IKE PSK，则 XAuth 将使用用户名和密码对 RAP 进行身份验证。
   - 如果使用证书，则 XAuth 将对照 RAP 白名单对证书中的 MAC 地址进行身份验证。
4. 然后在 RAP 与控制器之间建立 IPsec 安全关联 (SA)。
5. MC 为 RAP 提供其进行端接所在的控制器的 IP 地址（LMS 和 BLMS IP）
6. 根据配置，在 RAP 与指定控制器之间形成了一个或多个 IPsec 加密的 GRE 隧道

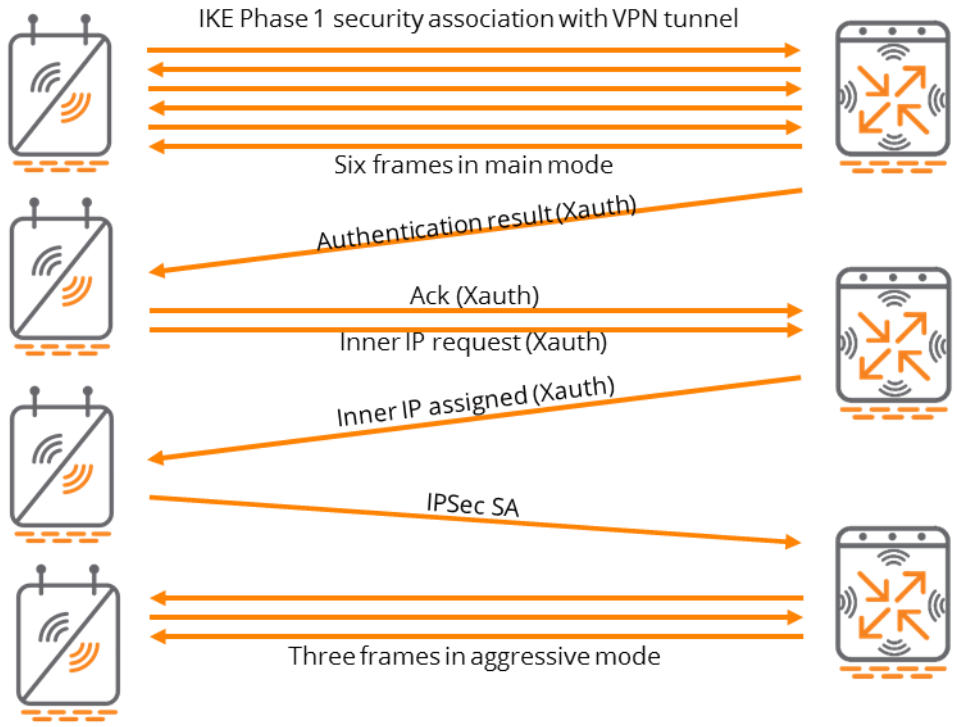


图 20 *RAP 启动*

分层配置

ArubaOS 8 中引入了分层配置，以便增强在多控制器网络中应用配置的方式。

ArubaOS 6 配置

在主控制器管理一组本地控制器的典型 ArubaOS 6 部署中，每个本地控制器首次显示时均使用各自的基本配置（接口、VLAN 和 IP 地址）。已在每个本地控制器上应用了基本配置后，主控制器将连接到本地控制器，然后推送 AP 组、SSID 和用户角色等配置。此类架构涉及具有多个控制器的架构的众多配置点，因为没有将配置完全集中在主控制器上，并且单个主控制器只能管理有限数量的本地控制器。

ArubaOS 6 中引入了 ZTP，但其仅适用于分支控制器网络，并且使用主控制器上的 Smart Config 接口只能启用部分功能。

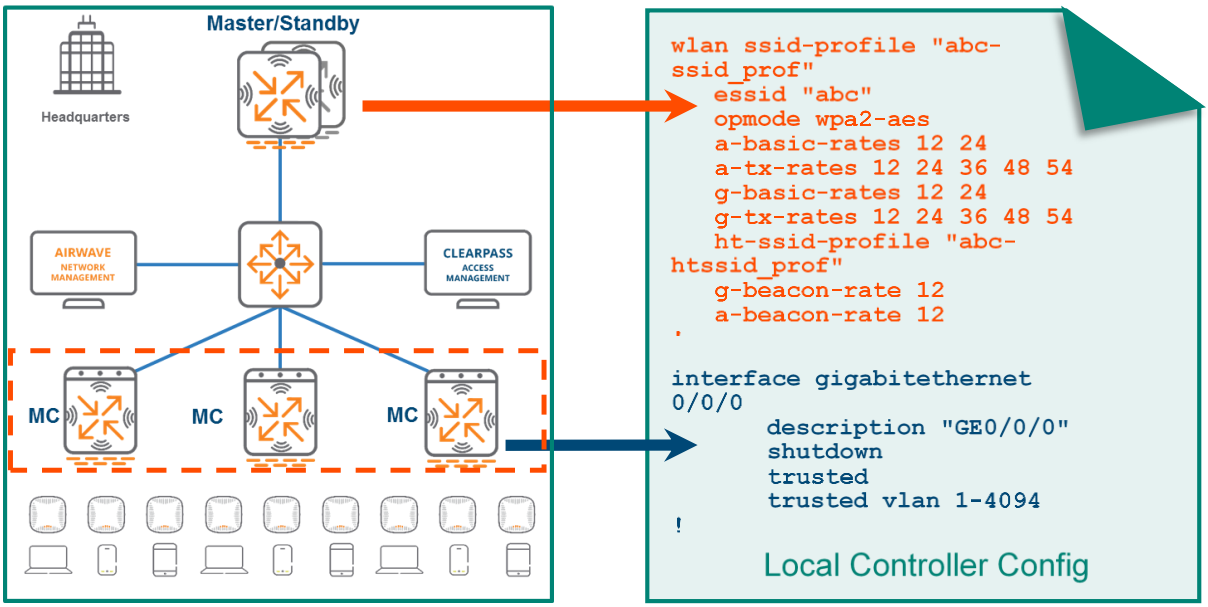


图 21 *典型 AOS 6 配置*

从主控制器向下推送的配置在所有本地控制器间均保持一致。主控制器不会有选择地为单个本地控制器推送配置。如果本地控制器分散在多个不同园区，并且每个园区均需要唯一 SSID，则推送给每个本地控制器的配置均将包含所有园区的 SSID 配置。大多数部署可能将不需要这种级别的 SSID 冗余。即使 AP 将订阅特定 AP 组以便在每个园区中广播相关 SSID，用于其他园区的配置对于未使用该 SSID 的本地控制器而言仍是不相关的。

在某些情况下，统一配置方法还可能带来运行问题，在这个意义上，整个主配置会暴露在所有区域本地控制器间。由于在更改配置时本地网络管理员将需要访问主控制器，因此他们需要格外小心，避免可能影响主控制器正在管理的其余控制器的任何错误配置。

AOS 8 配置增强

ArubaOS 8 为所有部署模式均引入了真正的 ZTP，并且引入了分层配置的概念。新园区或分支机构控制器可使用 DHCP 选项或 Aruba Activate 发现 MM，以及从 MM 接收它们的整个配置。无论正在管理的控制器规模如何，MM 均可作为整个部署的单一接触点。

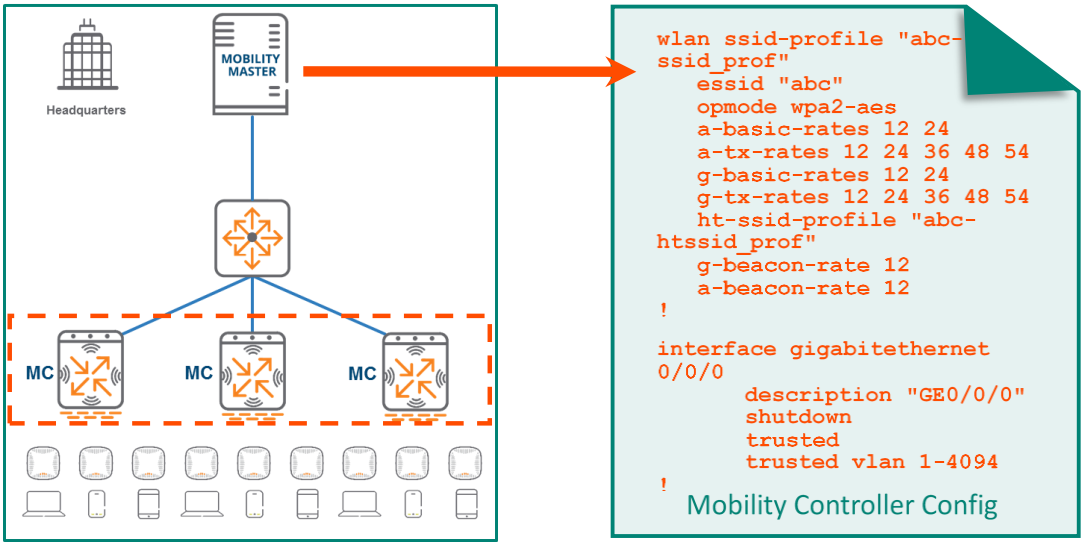


图 22 *AOS 8 配置*

通过分层配置可在 MM 上创建配置节点，这些节点包含特定区域、园区或楼宇的公共配置。在配置节点下将控制器列入白名单后，可在设备配置节点上添加设备级配置。当 MC 首次联系 MM 时，组级配置将与设备级配置进行合并，然后组级配置被向下推送到 MC。

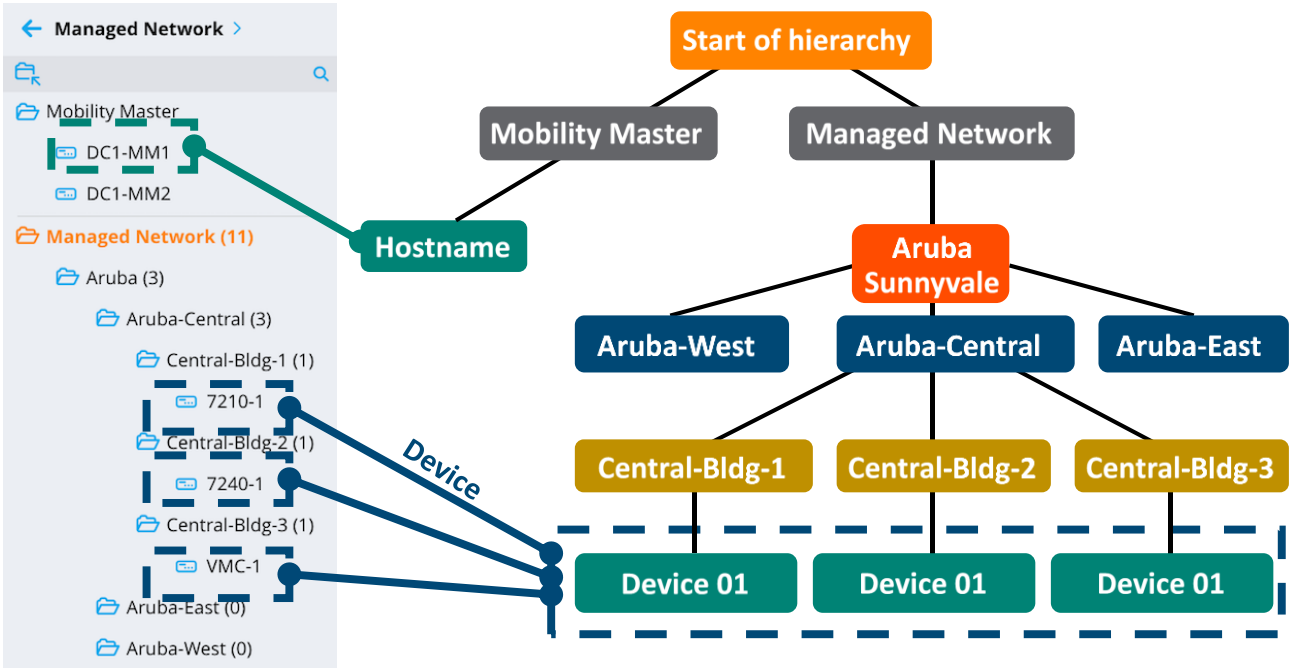


图 23 *配置层次结构*

分层配置模式具有系统定义的以及用户定义的配置节点。

系统节点

默认情况下，系统级节点存在于 MM 的 GUI 上，无法删除。系统节点如下：

- **MM** – 在冗余 MM 情况下，此节点上定义的配置对于主用和备用 MM 都是通用的
- **（MM 的）主机名** – 包含实际 MM 的配置
- **托管网络** – 创建所有用户定义的节点以及配置控制器所在的层次结构

用户节点

用户定义的节点是由管理员在**托管网络**系统节点下创建的。可在此节点下创建节点层次结构，其中上层节点包含针对所有控制器的公共配置。在层次结构的较低级别，此配置会变得更具体（基于区域、园区或楼宇）。设备节点是在最底层定义的。以下示例演示了分层组和设备节点定义：

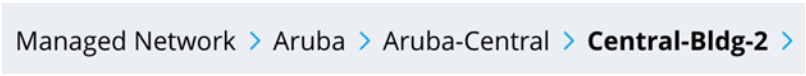


图 24 *路由器节点示例*

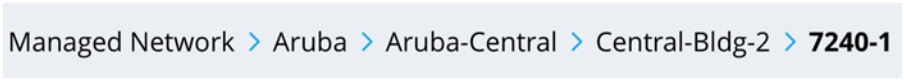


图 25 *设备节点示例*

可在**托管网络**节点下创建最多四个嵌套子节点。例如：

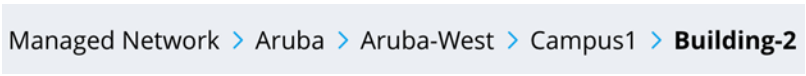


图 26 *四个嵌套子节点*

可在同一父节点下创建许多子节点。此外，可将子节点自由移动到层次结构中的其他节点，也可以从同一父节点下的其他节点克隆子节点。

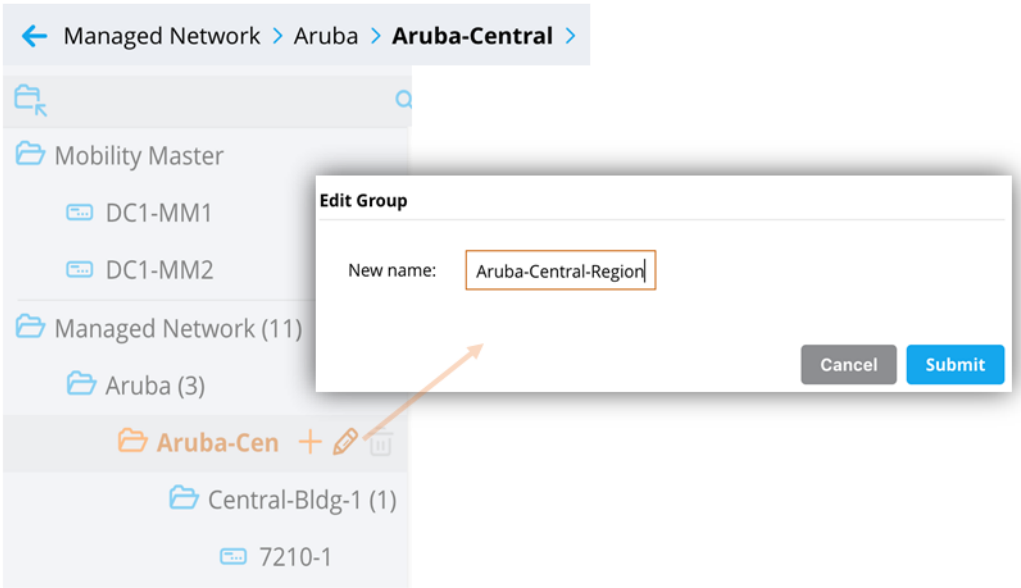


图 27 *重命名节点*

配置继承

当 MC 最初联系 MM 时，它会将设备节点上的配置与层次结构中较高层一直到**托管网络**节点上的配置进行合并。

如果任何节点上的配置存在冲突或重叠，则在向下推送最终配置时，较低节点上定义的配置将优先于较高节点上的配置。以下示例显示了控制器如何从 MM 继承其最终配置：

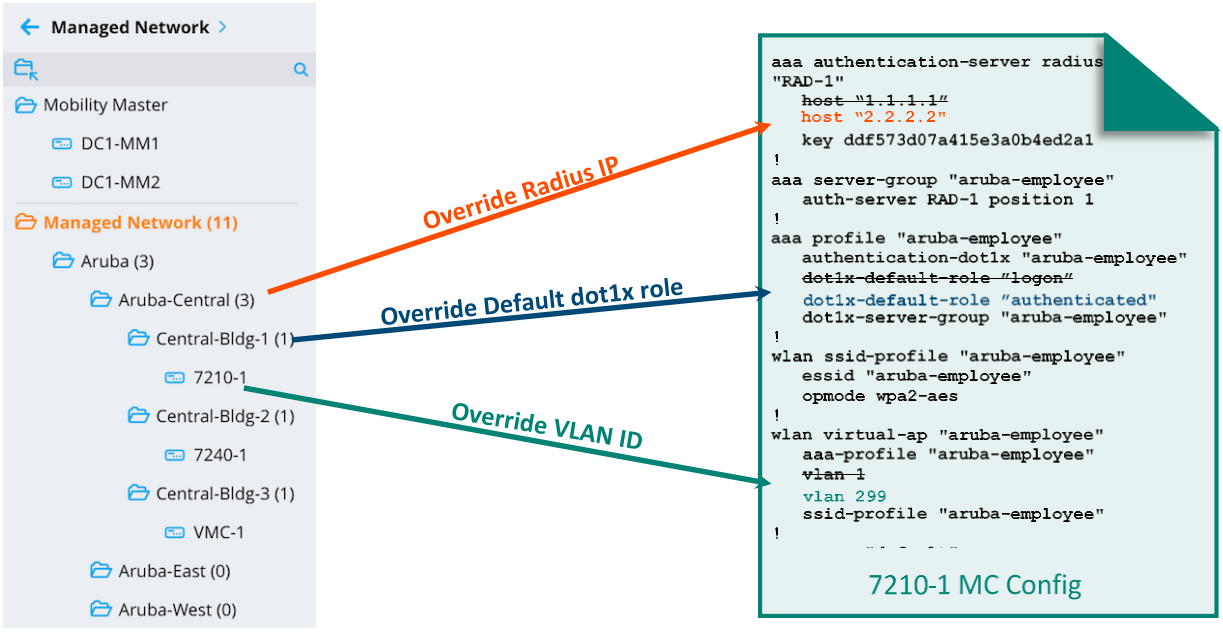


图 28 *MM 配置继承*

在以上示例中，初始配置是在用户定义的 **Aruba** 节点上创建的，该配置对于组织中的所有控制器将是通用的。由于 **Aruba-Central** 节点位于层次结构的较低层，因此它将从该 Aruba 节点接收其初始配置，然后覆盖 RADIUS IP 地址。同样，**Cenral-Bldg-1** 节点和 **7210-1** 设备节点将分别覆盖原始配置中定义的 dot1x 角色和 VLAN ID。下图显示了使用**托管网络 > Aruba** 路径配置的一些关键元素：

Server Group > aruba-employee **Servers**

NAME	TYPE	IP ADDRESS	TRIM FQDN
RAD-1	Radius	1.1.1.1	--

图 29 *RADIUS IP 为 “1.1.1.1” 的 RADIUS 服务器 RAD-1*

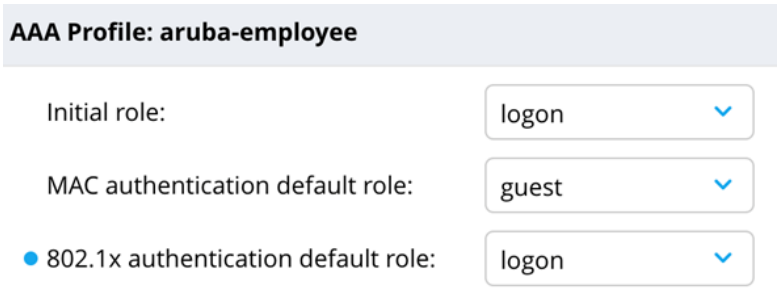


图 30 *802.1X 默认登录角色*

配置参数旁存在蓝色点表示该值被覆盖，例如在更改了从父节点继承的配置或替换了空值的情况下。单击蓝色点可显示有关此更改的其他详细信息，以及提供移除或保留此覆盖的选项。

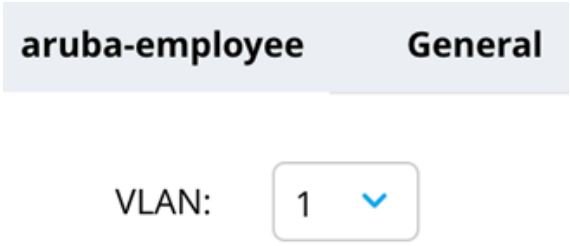


图 31 *VLAN “1”*

在下图中，**Aruba-Central** 节点继承了此配置，但 RADIUS 服务器 **RAD-1** 的 IP 已更改为“2.2.2.2”：

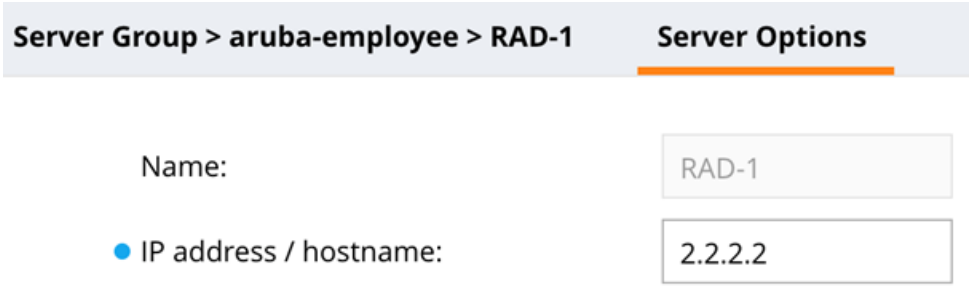


图 32 *RADIUS 服务器 IP 覆盖*

在较下层的 **Central-Bldg-1** 节点上，存在蓝色点表示身份验证、授权和计费 (AAA) 配置文件中的默认 802.1X 角色已更改为“authenticated”，并且从父节点接收的配置已被覆盖。**托管网络 > Aruba > Aruba-Central > Central-Bldg-1 > ：**

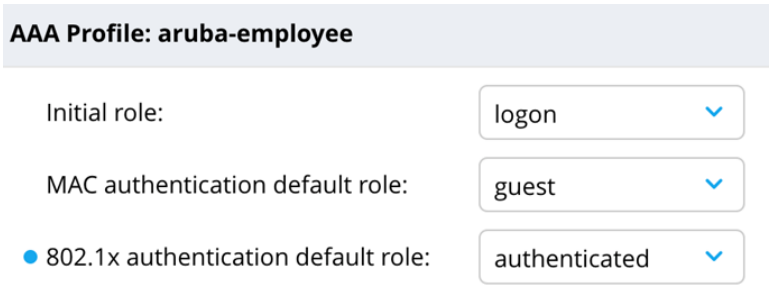


图 33 *身份验证默认角色覆盖*

最后，应用于设备节点 **7210-1** 上的虚拟 AP 配置文件“aruba-employee”的 VLAN 已更改为“299”。**托管网络 > Aruba > Aruba-Central > Central-Bldg-1 > 7210-1**：

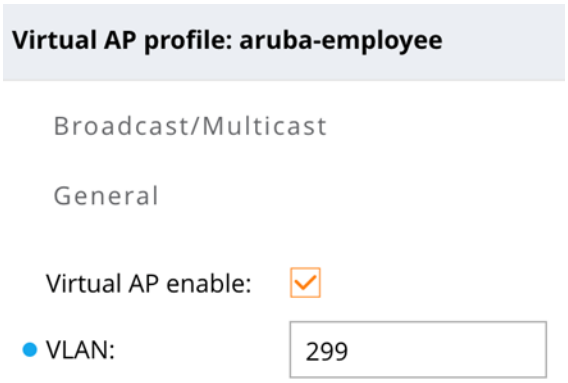


图 34 *VLAN 已更改为 299*

当分配给 **Central-Blg-1** 节点的 7210 控制器首次与 MM 联系时，其继承的配置将导致以下更改：

	原始配置	继承配置
RADIUS 服务器 IP	1.1.1.1	2.2.2.2
802.1X 默认角色	logon	authenticated
VLAN	1	299

表 6 *继承配置更改摘要*

节点级管理

通过分层配置可在 MM 上创建节点级管理帐户。对于网络管理员有必要访问权限（例如在区域、园区或楼宇层面上）的配置节点，他们可完全管理这些配置节点上及其下方的控制器的配置，同时不影响全局层次结构中其他位置的控制器。此功能可确保在本地站点上进行的任何不良配置更改受到抑制且不影响整个组织。

概念验证测试是在投产前需要对自定义 ArubaOS 内部版本和功能进行实验室测试的另一个用例。在这种情况下，可将测试配置节点与节点级管理帐户一同创建。由于这些节点是在沙箱环境中创建的，因此可自由地执行测试，不会产生在配置层次结构中的更高层所具有的任何不良影响。

许可池

ArubaOS 8 中的许可从 MM 集中加以管理，在默认情况下，全局许可池将用于其管理的所有控制器。但如果特定许可池需要专用（例如用于特定区域），则必须使用相应的分层节点和许可数定义在 MM 上创建自定义许可池。

有关其他信息，请参阅“在 MM 上创建许可池”部分。

配置最佳实践

部署控制器前，在配置层次结构上，对于网络将来是什么样子应有一个已定义的计划。以下部分提供了有关制定配置和部署计划的指导。

节点层次结构设计

实施分层设计有多种方法：

- 通常基于控制器的地理位置划分来创建配置层次结构。如果某个组织在一个国家/地区有多个办事处，那么为例如东部、中部和西部等每个区域均创建配置节点是有意义的。其中每个区域又可具有多个园区、楼宇和设备，它们各自有自己的配置节点。
- 层次结构的另一种组织方式可基于提供的服务类型，例如在树形图底部具有区域变化的园区和远程位置。

应设计分层配置，以便使对组织通用的那些配置位于更高级节点上。随着网络要求变得更加具体，层次结构的较低节点将继承配置的其余部分。例如，能够以层次结构的较高级别定义指定的 VLAN，然后以较低级别为其分配特定 VLAN ID。最后，在设备级节点配置特定于单个控制器的配置，例如 IP 地址、物理和虚拟接口，以及群集成员资格。作为最佳实践，应始终定义取决于单个节点的所有配置，例如，在公共节点中一同定义 VLAN ID 和 VLAN 接口参数。

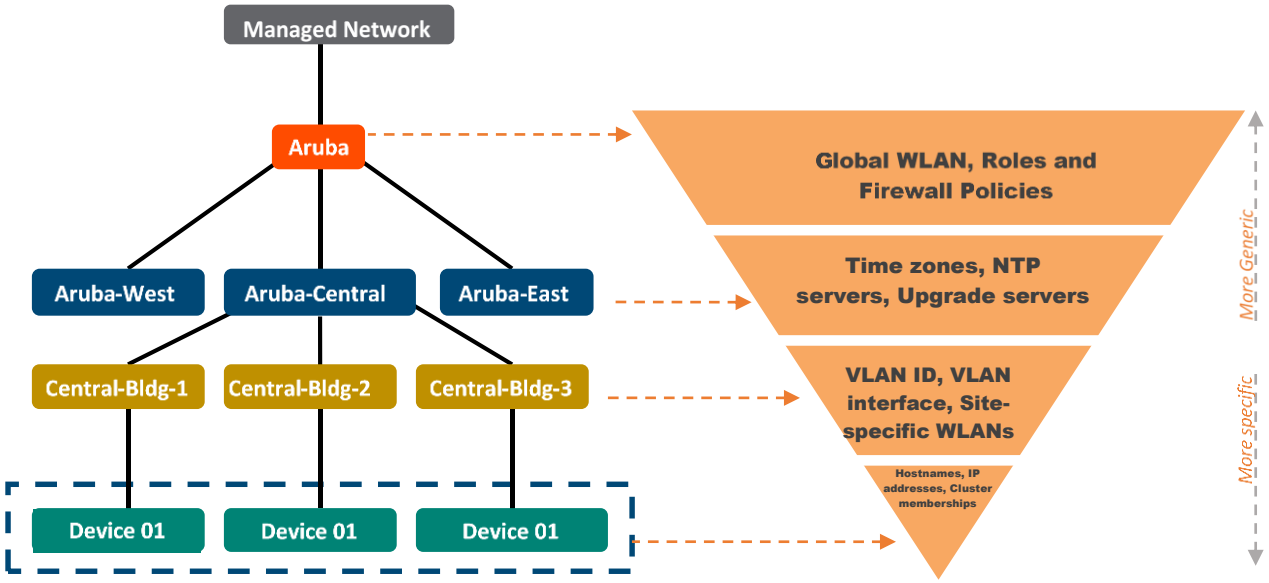


图 35 *节点层次结构设计*

配置覆盖

一般无法删除从更高级节点继承的配置，但可在更低级节点上覆盖它。但是，有些配置参数无法在较低级节点上进行覆盖。这些参数包括：

- Net 目的地
- IP 访问列表
- 用户角色
- AAA 服务器组
- AAA 用户推导规则

CAUTION

应该避免跨多个层级的过多覆盖，因为这样可能难以进行故障排除。

层次结构的深度

可在**托管网络**节点下创建最多四个嵌套子节点。但为了简化配置管理，建议仅创建所需数量的嵌套节点。

托管网络节点

作为最佳实践，Aruba 建议在**托管网络**节点以下的节点上定义配置，而不是在**托管网络**节点本身上定义。这样做可实现充分的网络增长和可扩展性，同时为新站点保持单独的配置层次结构。**托管网络**节点上的配置应尽可能保持最小，以便防止与错误配置相关的问题在层次结构中的其他每个节点上传播。

Aruba 强烈建议在任何情况下都不要在 **/md（托管网络）**节点上放置任何配置。修改此级别的配置将永久改变每个子节点的配置，并且无法确定默认设置。应始终从低于**托管网络**节点的级别开始配置。

站点可以物理方式或按类型加以区分。在以下示例中，如果组织“Aruba”收购了另一家公司“Network-Co”，则将在**托管网络**下定义一个新的配置节点，称为 **Network-Co**，该节点与 **Aruba Sunnyvale** 节点并行。

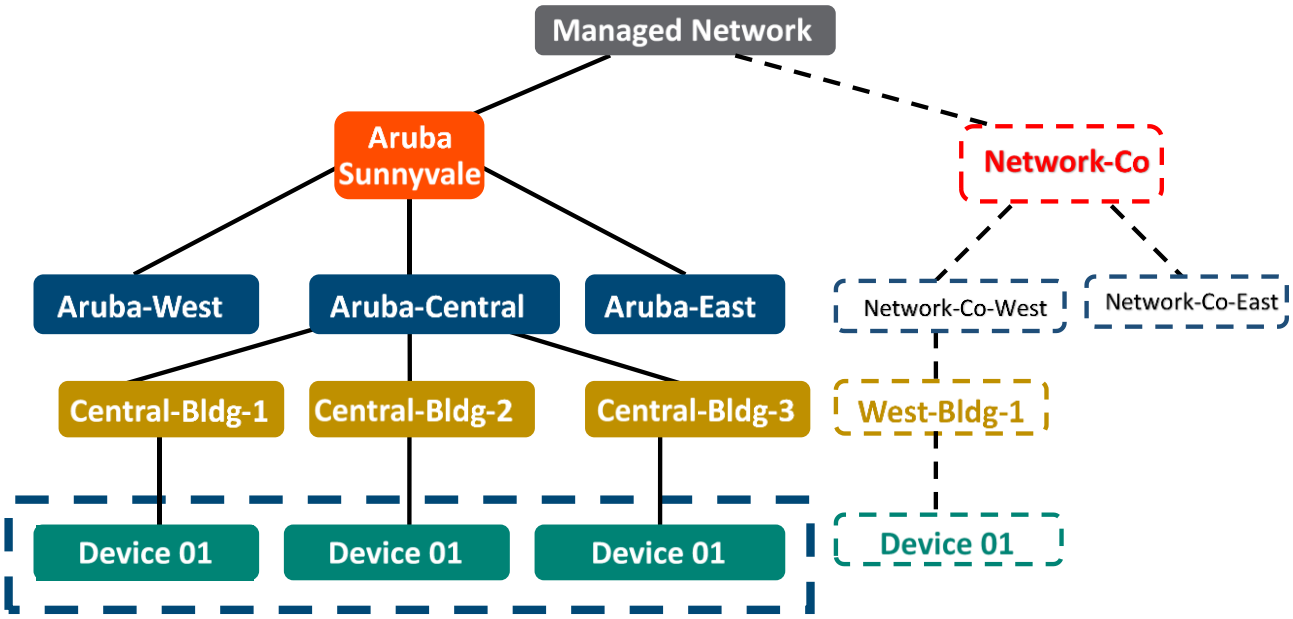


图 36 *托管网络节点层次结构*

配置注释

- 手动启动 MC 时，务必确保在相应配置节点下已在 MM 上将它们列入了白名单
- 使用 ZTP 启动 MC 时，确保在 Activate 上配置正确的配置节点和 MM MAC 地址至关重要。
- 验证 MM 是否已从 Activate 中了解了 MC，并在 Activate 配置规则中指定的配置节点下将它们列入了白名单
- 当在控制器的初始配置期间为建立 IPsec 连接而指定了 MM 的 MAC 地址时，始终确保将**管理端口硬件 MAC 地址**用于 VMM，以及将**硬件 MAC 地址**用于 HMM
- 当 MM 向 Activate 注册时，将自动填入正确的 MAC 地址。如果控制器正在使用 ZTP 来联系 Activate 以及向 MM 注册，则确定 MM 的 MAC 地址，以及在配置 Activate 上的配置规则时从下拉列表中选择该地址

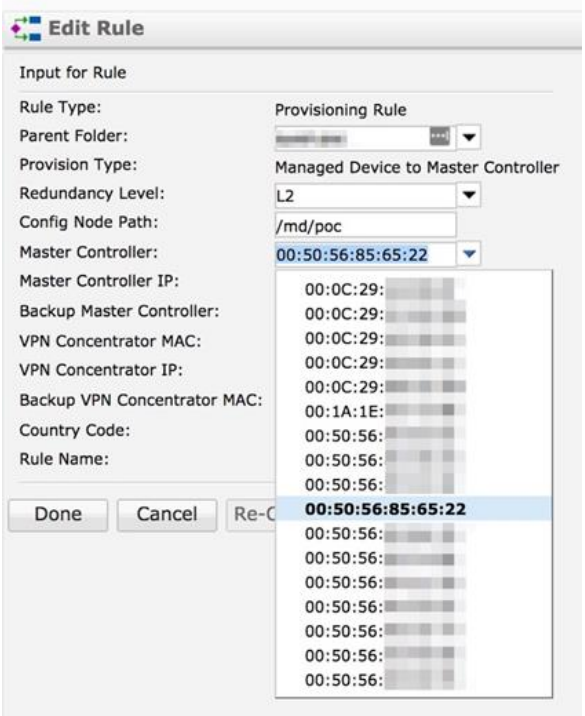


图 37 *选择 MM MAC 地址*

可加载服务模块

可加载服务模块 (LSM) 是 ArubaOS 8 的一项功能，该功能可使管理员在正在运行的系统上动态升级或降级服务模块，同时无需进行控制器固件升级或完全重启系统。每个应用程序都有自己的压缩映像，并且升级实时进行，无需重启控制器。

统一通信与协作

统一通信与协作 (UCC) 是 Aruba 用于描述实时企业通信服务集成的术语，例如即时消息、语音、视频会议、桌面共享、应用程序共享等。

在 UCC 作为 Aruba 控制器、交换机和 AP 上的一个功能的情况下，它表示企业通信和协作应用程序各个方面的统一。这些方面可大致分类为媒体检测、媒体与流量优先级排列、监控与可见性，以及媒体分类。

Aruba 控制器支持以下 UCC 应用程序：

- Skype for Business
- Cisco Jabber
- 会话初始协议 (SIP)
- Wi-Fi 通话

以上应用程序列表并不全面。有关支持的 UCC 应用程序的完整列表，请参阅 ArubaOS 用户指南。

UCC 功能与 ArubaOS 6 中的相同，UCC 不是 ArubaOS 8 的新功能。但在 ArubaOS 8 中已改变的是该功能的架构及其部署方式。

架构比较

UCC 由深度分组检测 (DPI) 引擎组成，该引擎在 ArubaOS 6 和 MC ArubaOS 8 中的本地控制器上运行。在 ArubaOS 6 中，DPI 和 UCC 进程均在本地控制器本身上运行。在 ArubaOS 8 中发生的变化是，Aruba 称为 UCC 服务或 UCC 应用程序的 UCC 进程部分已被移至 MMM。DPI 功能本身仍在 MC 上。

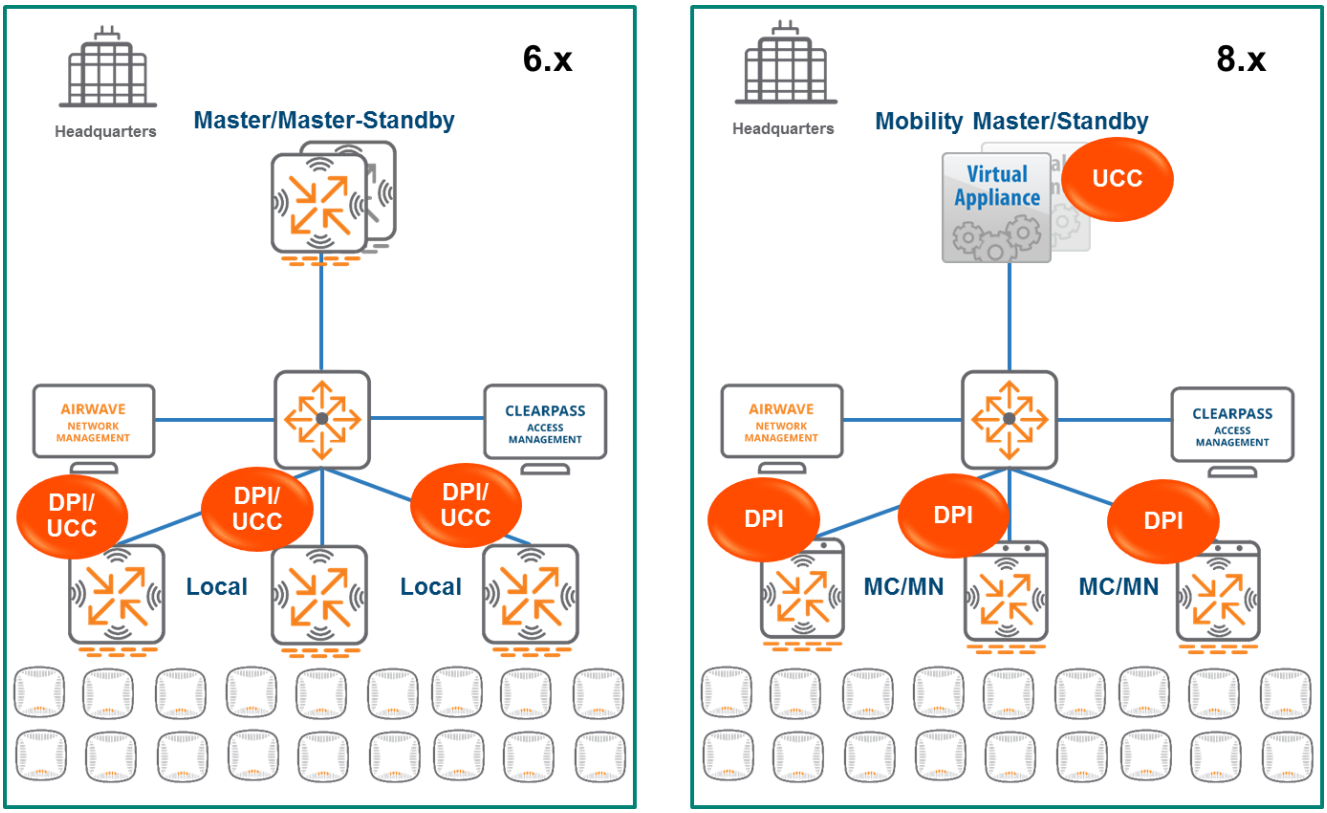


图 38 *ArubaOS 6 与 ArubaOS 8 之间的 UCC 架构比较*

ArubaOS 8 中 UCC 的新特性

尽管 ArubaOS 6 中的 UCC 表现地很好，但其设计中存在一些缺点，在 ArubaOS 8 中已改进了这些缺点，从而为考虑迁移到 ArubaOS 8 的管理员提供了优势，这些缺点如下：

- **缺乏可见性** - 在 ArubaOS 6 中，UCC 可见性未集中在主控制器上。统计数据和监控保留在本地控制器上。这种设计并不理想，因为这需要用户分别登录每个本地控制器才能监控 UCC 数据
- **极具挑战性的升级** - 在 ArubaOS 6 中添加对新应用程序的支持会涉及整个控制器升级，这可能对网络具有破坏性
- **无 SDN 聚合** - 在 ArubaOS 6 中使用 Skype for Business 软件定义网络 (SDN) API 涉及利用网络中所有订户的 IP 地址配置 SDN 管理器。这样做会对网络可扩展性产生不利影响

相比之下，ArubaOS 8 通过其出色的架构设计和 UCC 实施方法，全面改进了功能，从而克服了上述挑战。现在 UCC 在 MM 上作为应用程序（或可加载服务）运行。DPI 引擎继续在 MC 上运行，这些 MC 执行与 ArubaOS 6 中的本地控制器相同的功能。

分类和优先级决策制定功能已连同作为 UCC 应用程序一部分运行的 VoIP 应用程序层网关一起被移动到 MM。此外还可独立升级 UCC 功能，无需升级网络中的所有控制器，因为它是一个 LSM。这种无缝可升级能力可使管理员添加对更新语音和 UCC 应用程序的支持，并且不会遇到与重启控制器相关的任何不利影响。

MM 为将 SfB 作为 UCC 应用程序的企业带来重要价值主张。现在可在 MM 上为所有 MC 聚合 SfB SDN API。这样可无需利用数千个单独订户的 IP 地址配置 SfB SDN 管理器。MM 会跟踪发起了呼叫的 MC，并将从 SfB SDN 管理器接收的 SDN API 消息与呼叫流相匹配，同时对该特定 MC 上的数据路径进行编程。采用 ArubaOS 8 中引入的基于 MM 的架构可通过 MM 的 GUI 提供对 UCC 的集中可视性。

UCC 启发

在 UCC 环境中，启发是控制器用于检测和分类不同类型媒体的方法。其可被视为针对分组大小和用于流的端口等方面的高级模式匹配形式。UCC 功能本身由两个主要进程组成：DPI 和统一通信管理器 (UCM)。

UCM 为进程的名称，这些进程处理 UCC 分类，以及对控制器数据路径中已排列优先级的流进行编程。以下步骤概述了 ArubaOS 8 中的 UCC 在使用启发时如何处理呼叫流：

1. 客户端发起一个呼叫，MC 上的 DPI 引擎对流进行分析，以检测媒体流的存在
2. 媒体流的检测从 MC 传递到 MM 上的 UCC 应用程序
3. MM 上的 UCC 应用程序将这些媒体流分类为语音和视频等类别
4. MM 上的 UCC 应用程序在 MC 上触发一个操作，对数据路径进行编程，以便排列这些流的优先级
5. MC 将已排列优先级的流从客户端安装到服务器，再从服务器安装到呼叫接收者。最终对上游和下游流量进行端到端优先级排列

上列步骤假设 MM 与 MC 之间的预设信道交换与该呼叫有关的信息，例如触发流编程操作

下图展示了 ArubaOS 8 架构中的上述步骤：

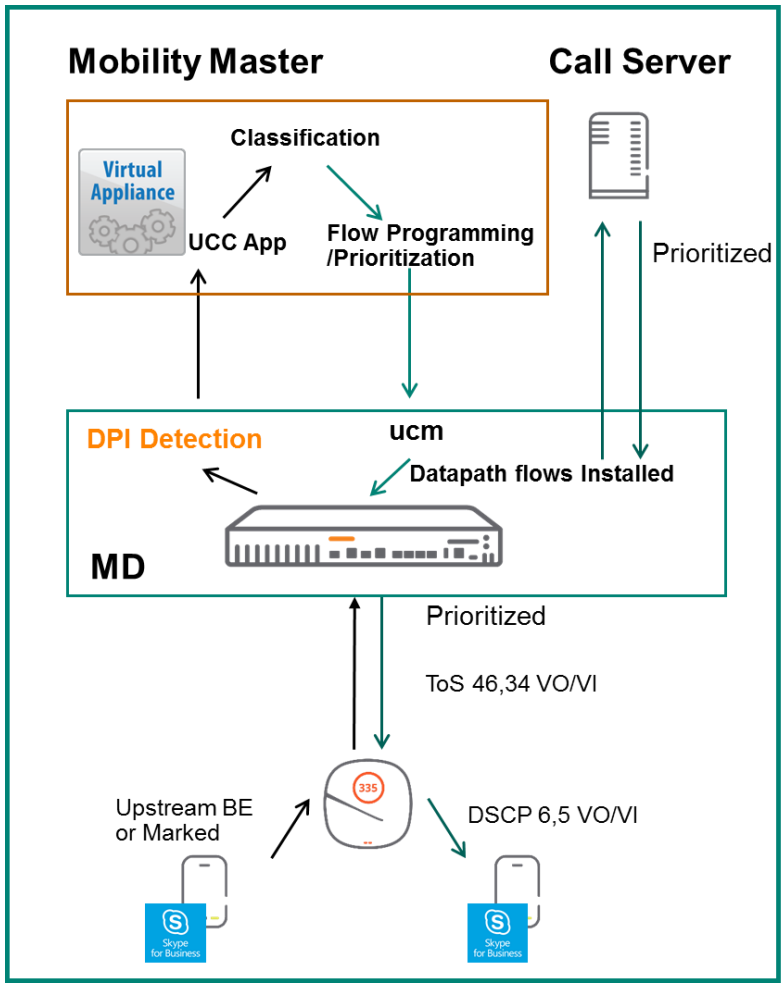


图 39 *具有启发的 ArubaOS 8 呼叫流*

Skype for Business

Microsoft 开发了一项为交换机提供详细呼叫信息的服务，他们将其称为 Skype for Business 软件定义网络应用程序编程接口。此工具先前称为 Lync SDN API。

SfB SDN API 包含 3 个组件：

- **SfB SDN 管理器** - 位于 SfB 前端服务器旁
- **SDN 对话侦听器** - 位于前端服务器上
- **订户 -** 在 Aruba 架构中，订户将是 SfB SDN API 认证的 Aruba 控制器（或交换机）

NOTE

凭借与 OpenFlow 相关的 SDN 概念，SfB SDN API 不会被误解。

订户（在这种情况下为 Aruba 控制器或交换机）订阅接收 SDN API XML 消息的 SDN API 管理器。这些消息由包含详细呼叫信息的 XML 组成，例如呼叫者、接收者、端口号、呼叫类型和端点客户端信息。

SDN API 可扩展标记语言 (XML) 消息可显著提高对以下方面的可见性：呼叫质量，以及为排列数据路径流优先级，控制器能够充分利用的信息。如果使用 SDN API XML，则无需启用启发来进行媒体分类，因为这些流为控制器提供此类详细信息。

ArubaOS 6 SfB SDN API

在 ArubaOS 6 中，SfB SDN API 用于使控制器能够基于超文本传输协议 (HTTP) 或 HTTP 安全 (HTTPS) 侦听某个端口，从而对媒体会话进行分类和优先级排列。然后将 SfB SDN 管理器配置为通过同一端口向控制器发送消息。以下步骤概述了使用 SfB SDN API 的呼叫流程：

1. 客户端发起呼叫。SfB 前端服务器触发会话信息 XML，然后将其发送到 SfB SDN 管理器
2. SfB SDN 管理器将 SDN API XML 发送到已订阅它的控制器
3. 控制器上的 DPI 检测到存在媒体流
4. 控制器接收会话信息 XML，其中包括呼叫者、接收者、端口、MAC 地址和媒体类型等详细信息
5. UCM 进程将其接收的 SDN API XML 与被识别为媒体的会话的 DPI 结果进行匹配
6. UCM 程序在数据路径中流动，以便对从客户端到呼叫服务器以及从服务器到呼叫接收者的流量进行优先级排列
7. 在呼叫终止时，SDN 管理器向控制器发送呼叫结束消息，其中包括有关呼叫质量的详细统计信息

SfB SDN API 的工作方式如下图所示：

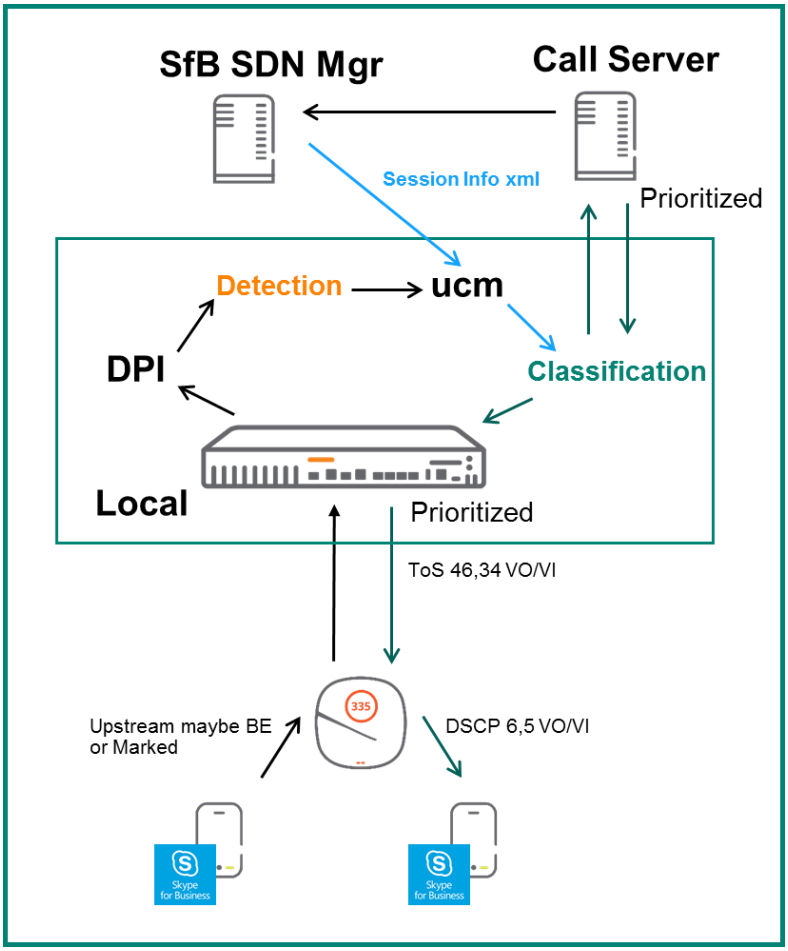


图 40 *ArubaOS 6 SfB SDN API 呼叫流*

ArubaOS 8 SfB SDN API

ArubaOS 8 中的 SfB SDN API 功能类似于 ArubaOS 6，主要区别为 SfB SDN 管理器只需要使用 MM 的订户 IP 地址加以配置。默认情况下，MM 被配置为侦听端口 32000 上的 SfB SDN API 消息。然后，SfB SDN 管理器使用相同端口基于 http 或 https 向 MM 发送消息。

在 Aruba OS 8 中使用 SfB SDN API 时，SfB 呼叫的流程如下：

1. 客户端发起呼叫。MC 的 DPI 引擎检测到存在媒体流后，其触发到 MM 上 UCC 应用程序的通知
2. 同时，SfB 前端服务器将向 SfB SDN 管理器发送呼叫会话信息 XML 消息，然后 SfB SDN 管理器将此消息转发给 MM。
3. MM 使用 XML 并将其与最初发送 DPI 元数据的 MC 相关联
4. MM 上的 UCC 应用程序使用 SDN 会话信息对数据路径流进行分类和编程
5. MM 向发起了此呼叫的客户端的 MC 发送流编程操作
6. MC 相应地对数据路径进行编程，并在上游和下游安装优先级流

在使用基于 ArubaOS 6 的架构时，所有 UCC 功能均位于本地控制器上。ArubaOS 8 在这方面有所不同，只有 DPI 位于 MC 上，而分类和优先级决策制定已移至 MM。ArubaOS 8 中 UCC 的一个关键区别是能够在 MM 上聚合 SfB SDN API 消息。下图展示了 ArubaOS 8 中的 SfB SDN API 流程：

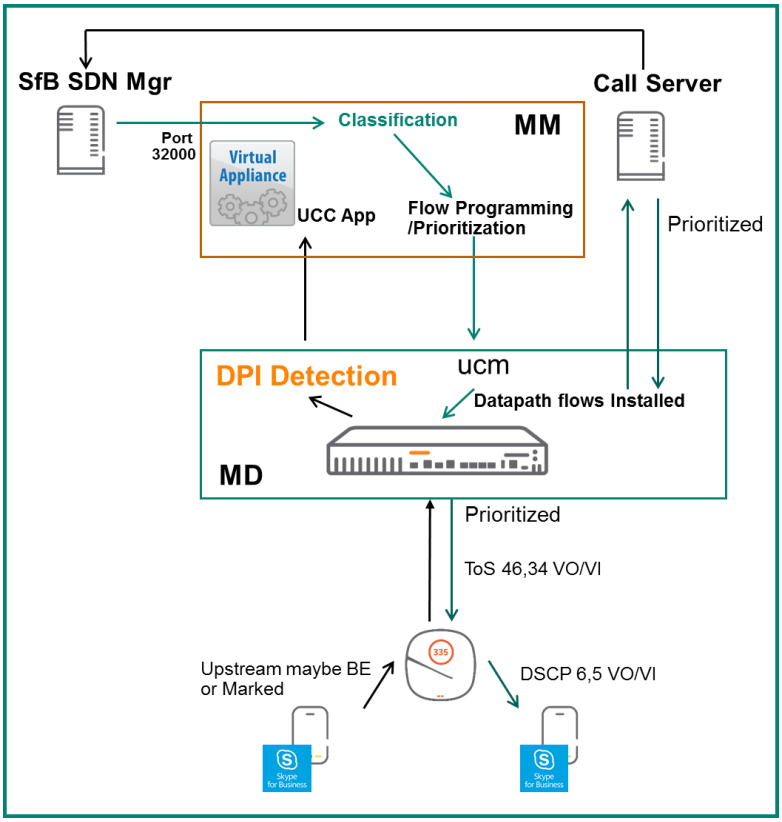


图 41 *ArubaOS 8 SfB SDN API 呼叫流*

AirMatch

ArubaOS 6 中的 ARM

自适应射频管理 (ARM) 是 ArubaOS 6 中使用的主要 RF 优化技术。尽管 ARM 在推出时是一项革命性技术，但其确实存在一些缺点。其中包括：

- 过于频繁的信道变化，这会导致客户端断连和 RF 网络不稳定，以及邻近射频之间信道计划耦合
- 可用信道的不均匀使用
- 非对称 EIRP 计划，这会对客户端漫游行为产生不利影响
- 在 EIRP 计划中缺少 2.4Ghz/5Ghz 区别
- 缺少自动带宽计划

这些缺点已导致一些客户放弃了 ARM 解决方案，他们关闭了该功能，或者通过漫长而繁琐的配置过程手动设置射频参数。ARM 在 ArubaOS 6 中具有以下特点：

1. 分散式服务；每个射频均做出自己的决定
2. ARM 本质上具有“反应性”
3. 未来频谱增强
4. 非对称 EIRP 计划，其可能不会提供最佳客户端漫游行为

当构思 ARM 时，与新式企业网络相比，这些网络的规模相对较小，并且信道结构太过基础。尽管在 RF 计划方面必须实现自动化，但在网络稳定性和性能方面，其并不像现在这样关键。那时，设计分散式算法被认为是可接受的做法，在该算法中，每个射频均基于本地信息做出各自的决定。持久收敛时间、级联效应，以及互耦或退避为自然结果，被视为小问题。在新式生产网络中，这些情况不再可接受，它们可能对更大、更密集和越来越异构的网络带来重大挑战。

创建 AirMatch 的目的是克服 ARM 无法应对的所有上述挑战。AirMatch 是一种从零开始的集中式 RF 优化服务。信息收集和配置部署路径是最新定义的。该算法旨在实现长期网络稳定性和性能，以便建模和克服整个网络面临的 RF 挑战。

ArubaOS 8 中的 AirMatch

AirMatch 为 RF 网络资源分配提供前所未有的高质量。其从过去 24 小时的 RF 网络统计中收集数据，以及主动为第二天优化网络。

最佳实践是，应在网络利用率最低时部署 RF 计划更改，以便使客户端断连对用户体验的影响最小。除每 24 小时进行的主动信道计划外，AirMatch 还会对 RF 环境中的动态变化做出反应，例如雷达和高噪声事件。AirMatch 极大减少了信道和 EIRP 更改，从而可实现稳定的网络体验。AirMatch 具有以下关键属性：

1. 集中式 RF 优化服务
2. 新定义的信息收集和配置部署路径
3. 建模并解决整个网络问题
4. 为网络实现最佳信道、带宽和 EIRP 计划

AirMatch 仅在网络由 MM 加以管理且与 MCM 架构不兼容时才起作用。在 MCM 拓扑结构中，ARM 将继续作出所有信道、带宽、EIRP 和其他 RF 优化决策，就像它们在 ArubaOS 6 架构中那样。

如果 MM 与 MC 之间的链路中断并且 MM 无法访问，这将影响性能，但 AirMatch 仍将继续运行。最值得注意的是，需要集中式 MM 协调的功能将丢失，例如可实现 RF 优化的计划更新。当前 RF 解决方案将继续运行，并且仍将发生由高噪声事件和雷达导致的变化。

AirMatch 工作流程

AirMatch 是 Aruba 的下一代自动 RF 计划服务，该服务可为整个网络中的射频分配信道、带宽和功率。AirMatch 服务在 Mobility Master 上运行，其生成为每个射频指定新信道、带宽和 EIRP 设置的 RF 解决方案。AirMatch 工作流程是通过以下步骤进行的：

1. AP 将 RF 统计信息作为 AMON 消息发送到 MC
2. MC 将这些 AMON 消息转发到其 MM
3. AirMatch 计算最佳 RF 解决方案
4. MM 将该解决方案推送回到 MC
5. MC 将 dot11 射频配置文件发送到 AP

AirMatch 和 ARM 比较

以下表和图像概述了 ArubaOS 8 中的 AirMatch 与 ArubaOS 6 中 ARM 提供的功能有何不同，以及有何改进：

功能	AirMatch	ARM
ArubaOS 8 支持	Mobility Master	独立或 MCM
计算	集中	分散
高噪声避免	是	是
雷达避免	是	是
优化范围	整个 RF 网络	每个 AP
使用的 RF 信息	过去 24 小时	瞬间快照

表 7 *AirMatch 和 ARM 功能比较*

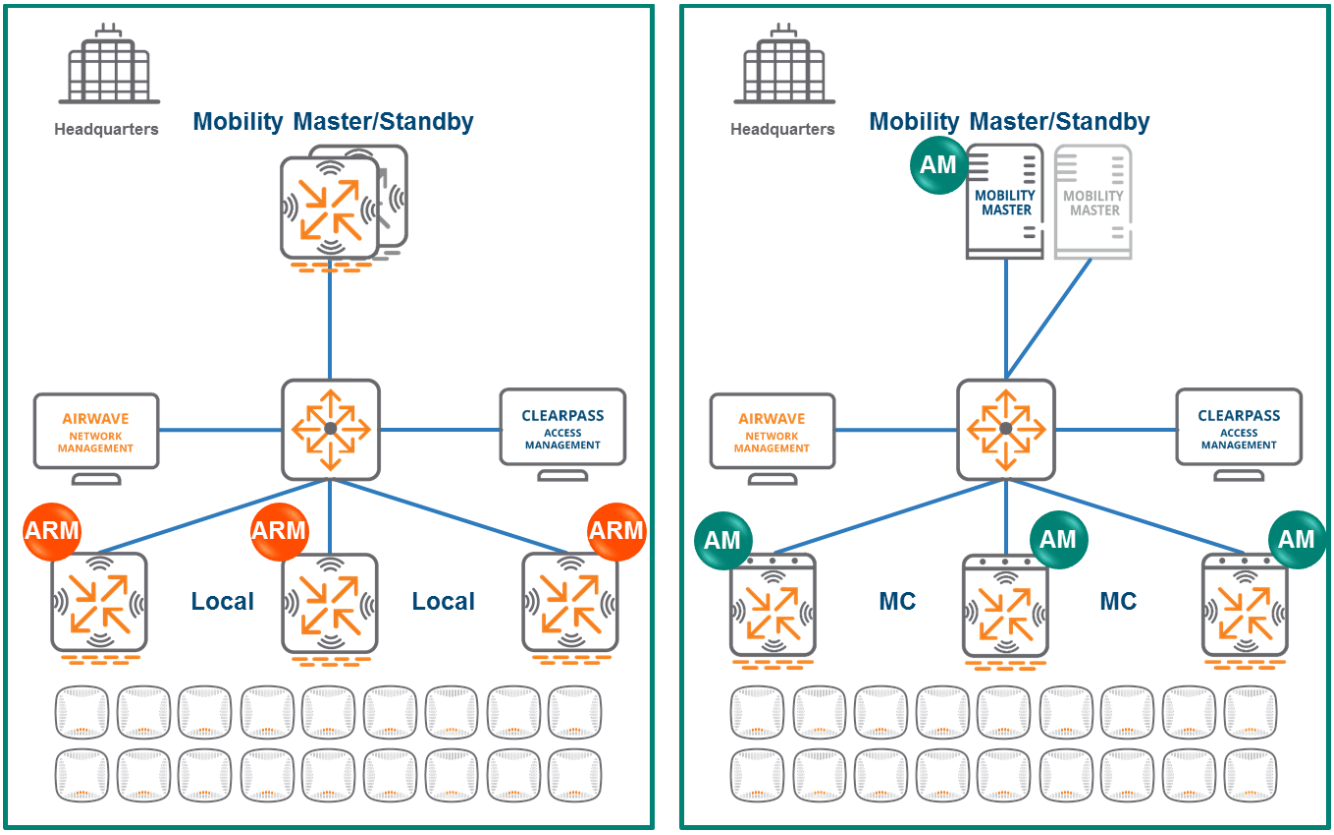


图 42 *ARM 和 AirMatch 比较*

Web 内容分类

Web 内容分类 (WebCC) 是 Aruba 控制器和 IAP 上的一项功能，在 ArubaOS 6 中最先引入了的该功能。其用途是根据类别和声誉对 http 和 https 流量进行分类。然后根据 WebCC 的分类可相应地应用防火墙规则。WebCC 能够阻止访问已知危险的站点，从而阻止间谍软件和恶意软件，通过 WebCC 还能够查看用户正在访问的 Web 内容类别和站点。

在 ArubaOS 6 部署中，WebCC 进程在本地控制器上运行。但在 ArubaOS 8 中，WebCC 进程已通过应用程序或*可加载服务*的形式被移至 MM，从而改变了底层架构。

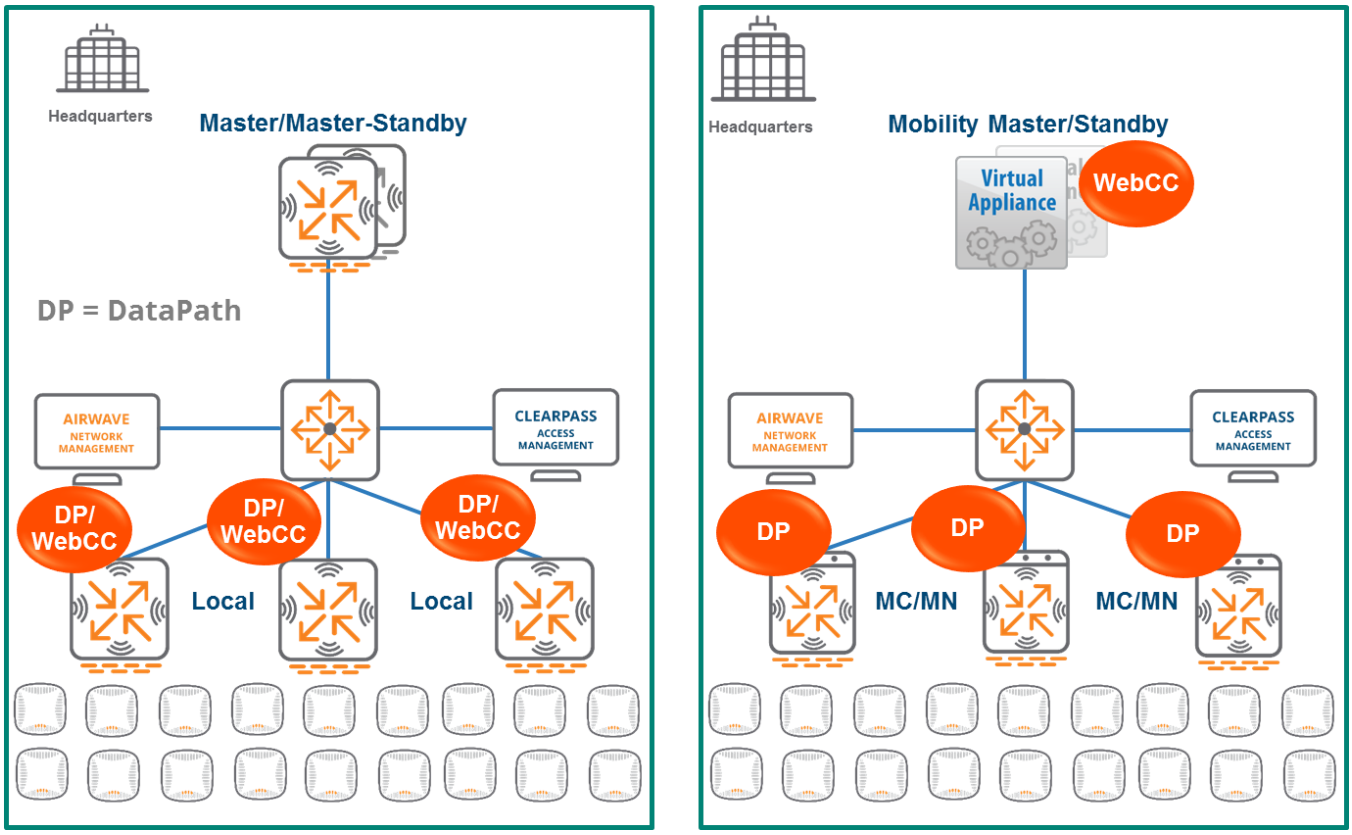


图 43 *ArubaOS 8 中的 WebCC 变化*

ArubaOS 6 中的 WebCC

WebCC 作为进程在 ArubaOS 6 中的本地控制器上运行，并与数据路径一起使用。其主要作用是搜寻数据路径中的 http/https 流量并对这些流量进行检查，以确定是否需要进一步操作。客户端具有 IP 连接并访问 URL 后，数据路径会截获来自客户端的 http/https 流量，然后对照其本地 URL 缓存检查是否有匹配项。如果数据路径找到了匹配项，则应用分类和信誉规则。防火墙访问列表中也使用 WebCC 提供的分类，该列表可根据额外信息进行操作，以便允许或拒绝访问 URL。

如果数据路径缓存未找到客户端正尝试访问的 URL 的匹配项，则会向 WebCC 发送 URL 未命中触发器。然后，WebCC 进程在控制器维护的数据库中查找此 URL。如果找到匹配项，则将对此 URL 进行分类，并将这些信息提供给数据路径。然后在 ACL 中使用这些信息来拒绝或允许访问 URL。如果 WebCC 进程在 URL 数据库中未找到匹配项，则其从 Brightcloud 存储库执行实时云查找并请求 URL 的分类。

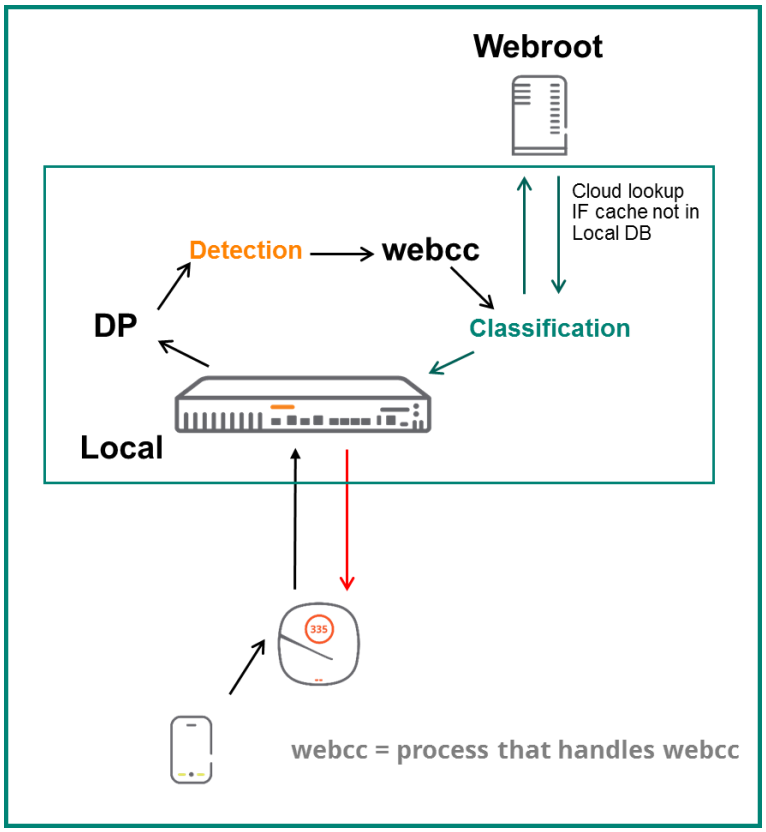


图 44 *ArubaOS 6 中的 WebCC 设计*

尽管 ArubaOS 6 中的 WebCC 具有显著优势，但其设计仍存在一些缺点。每个控制器均维护一个 URL 数据库，但控制器大小各异，它们的数据库和内存大小也不同。可在控制器上维护的 Web URL 数据库取决于该控制器的大小。在减小控制器的大小时，在本地数据库中找到 URL 的可能性会降低。这会在 URL 未命中时增加 URL 分类所需的实时云查找次数。阻止 URL 所需的时间也会增加，这会使用户能够访问本应被阻止的 URL。

ArubaOS 6 中 WebCC 的另一个缺点是每个本地控制器都必须单独联系 Brightcloud。此外，本地控制器还必须占用内存和空间来维护其 URL 数据库。

ArubaOS 8 中的 WebCC

与 ArubaOS 6 中 WebCC 设计固有的缺点相比，在 ArubaOS 8 中对 WebCC 的设计更改提供了许多优势：

- WebCC 作为可加载服务模块 MM 运行
- MC 仅维护浅层 URL 缓存，从而节约了内存
- MM 拥有更大的内存，能够维护最多有 100 万条记录的 URL 数据库
- 对未命中 URL 的云查找仅由 MM 执行

尽管 ArubaOS 8 中的 WebCC 流与 ArubaOS 6 类似，但仍有一些需要注意的关键区别。最关键的区别是 ArubaOS 8 中的 WebCC 进程在 MM 上运行，而不是在 MC 上。ArubaOS 8 中的 WebCC 功能流如下图所示：

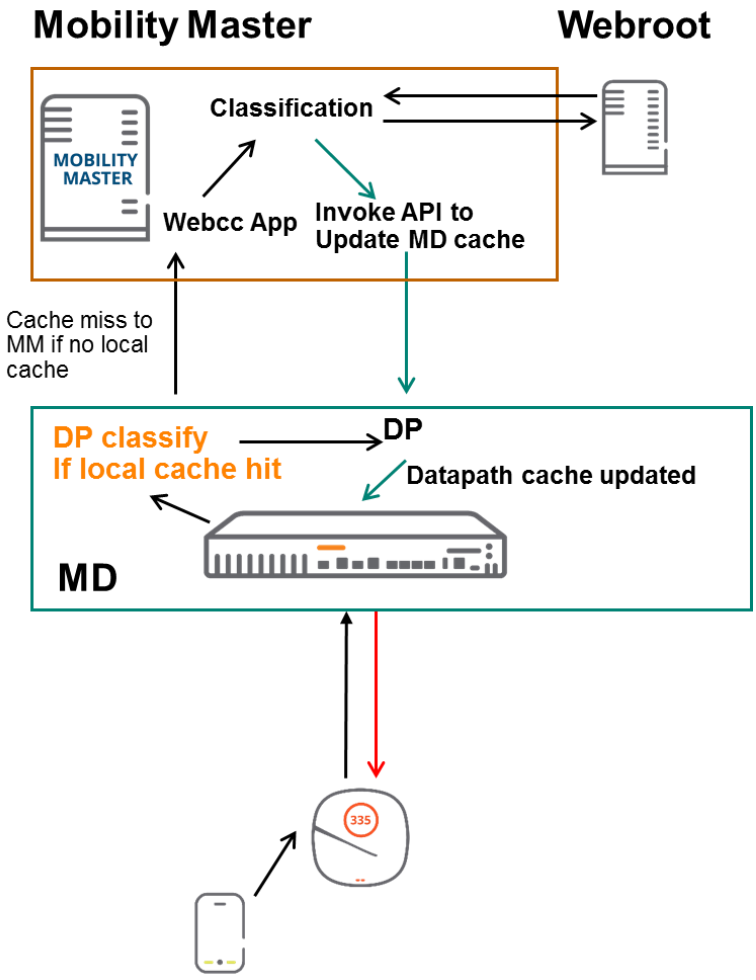


图 45 *ArubaOS 8 中的 WebCC*

当用户尝试访问 http 或 https URL 时，维护本地 URL 缓存的 MC 上的数据路径会搜寻该数据包。如果在 MC 的本地缓存中找到了该 URL，则会应用分类，并且可采取进一步操作，以便基于已配置的任何 ACL 允许或拒绝访问。

如果 MC 的数据路径未在其本地缓存中找到该 URL，则会触发 URL 未命中并将其发送到 MM。MM 在其远大于 MC 上本地缓存的数据库中查找该 URL。如果找到了匹配项，则会将分类结果发送回 MC，这将根据现有 ACL 确定是否需要进行操作来限制访问。如果 MM 在其本地数据库中未找到匹配项，则其将通过 Webroot 来执行云查找。MM 将更新其本地缓存以及发起了查找请求的 MC 的数据路径。

MM 需要配置有 DNS 服务器才能通过 Internet 访问 Webroot。

AirGroup

AirGroup 是 ArubaOS 的一个组件，其可解决与在企业和教育网络中使用多播域名系统 (mDNS) 服务相关的可用性和性能问题。Bonjour 等零配置网络服务和其他 mDNS 服务具有针对台式计算机、移动设备和网络服务的发现、地址分配和名称解析功能。它们主要用于扁平单子网 IP 网络，例如住宅部署。在大型大学和企业网络中，支持 Bonjour 的设备跨 VLAN 连接到网络的情况司空见惯。因此，特定 VLAN 上的 iPad 等用户设备无法发现位于另一个 VLAN 上的 Apple TV。为了在企业环境中的移动设备上使用 mDNS 服务，零配置网络多播需要由 AirGroup 等解决方案加以管理，以便提高网络吞吐量，简化连接到与用户和位置相关的设备的过程，以及在子网间正确加以转发。

ArubaOS 6 中的 AirGroup

mDNS 协议旨在促进多播通信，其在 L2 边界内极为有效。但这意味着在同一 VLAN 中，只有支持 mDNS 的设备才能相互通信。即，VLAN 10 中的 iPad 无法与 VLAN 20 中的 Apple TV 通信。

Aruba 创建 AirGroup 的目的是帮助促进跨 VLAN 的设备通信，以及根据 VLAN、用户角色、用户名、用户组和位置等属性提供对等多播流量的过滤。

每个控制器均通过学习和抑制无线 mDNS 或数字生活网络联盟 (DLNA) 查询及通告来构建 mDNS 缓存表。例如，每当 iPad 发送 AirPlay 查询时，控制器就会查看其 mDNS 缓存表，如果 AirPlay 服务可用，其将通过单播对该 iPad 作出响应。使用单播数据包有助于降低无线信道利用率。

AirGroup 域可用于跨不同控制器的设备间 mDNS 和 DLNA 通信。此外，控制器还能够与 ClearPass 集成来创建个人区域网。AirGroup 服务器可在 ClearPass 上加以定义，并且可选择连同用户名、用户角色、用户组、AP 组、AP 名称和 AP FQLN 一同加以共享。

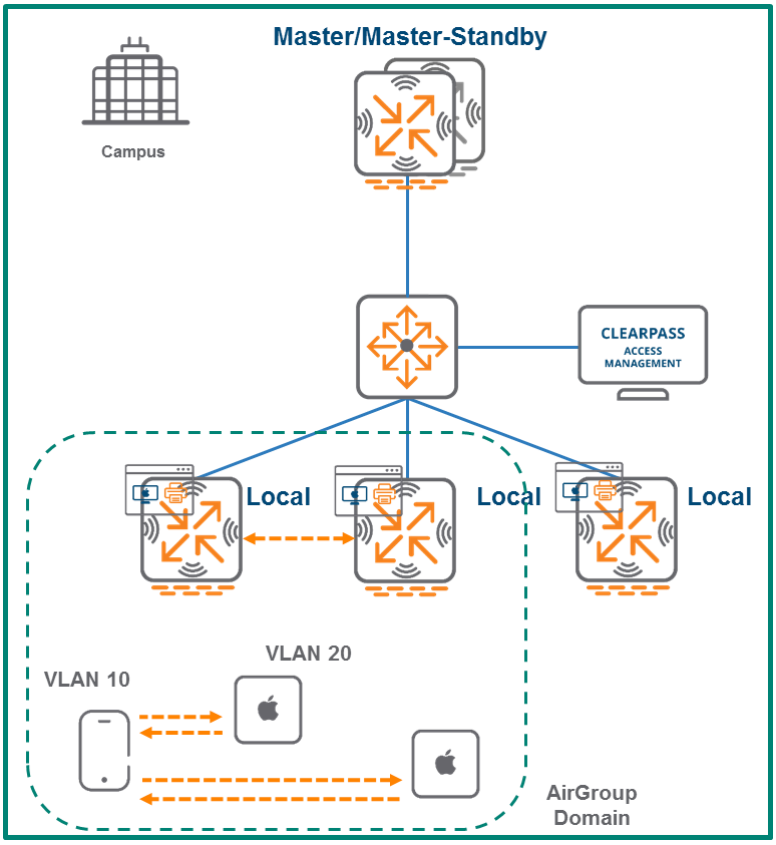


图 46 *ArubaOS 6 中的 AirGroup*

ArubaOS 8 中的 AirGroup

尽管 ArubaOS 6 中的 AirGroup 能够提供重要功能增强，但其具有可扩展性限制。ArubaOS 8 解决了 ArubaOS 6 中 AirGroup 的平台可扩展性问题，在 ArubaOS 6 中，可扩展性受控制器平台容量的限制。

在 ArubaOS 6 中，每个控制器均单独运行 AirGroup，与 ArubaOS 6 不同，在 ArubaOS 8 中，AirGroup 功能已被移至 MM，即整个 mDNS 缓存表均位于 MM 上。为传播 mDNS 和 DLNA 信息，MM 上安装了 OpenFlow 控制器，而 MC 上安装了 OpenFlow 代理。每当 MC 截获 mDNS 或 DLNA 查询或通告时，都会通过 OpenFlow 信道将其转发给 MM。

MM 根据其 AirGroup 策略创建相应的 mDNS/DLNA 流，并将这些流推送到 MC。MC 允许或拒绝 WLAN 上 AirGroup 设备的 mDNS 和 DLNA 通信。

在 ArubaOS 8 中，AirGroup 具有远远更高的可扩展性，因为与 ArubaOS 6 中基于硬件的控制器相比，MM 配备了相应的资源来处理网络上的大量 mDNS 通信。

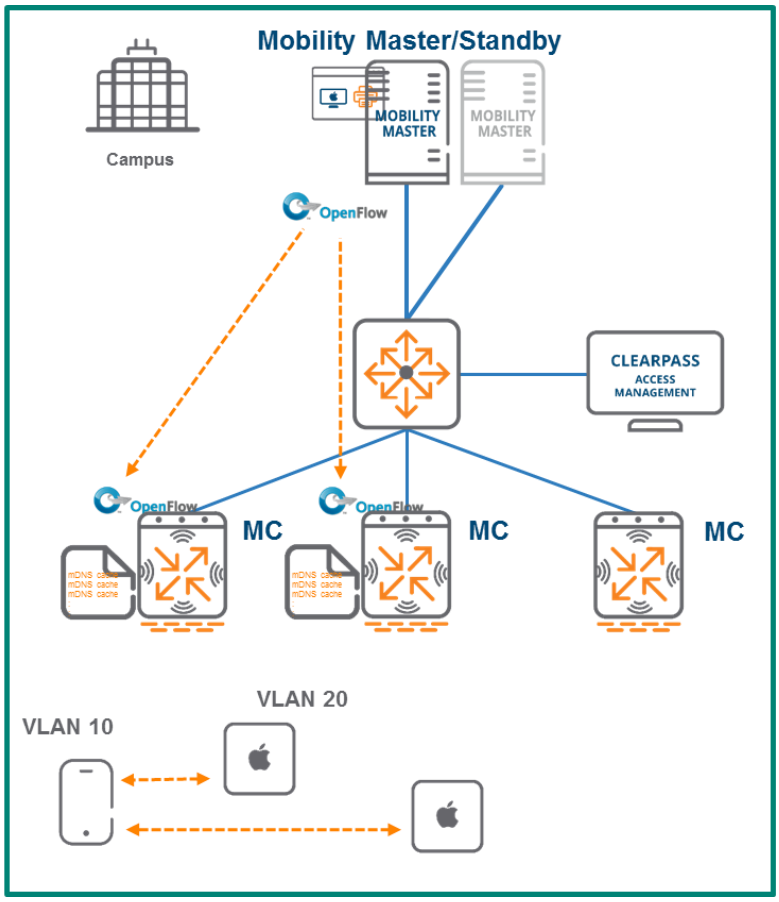


图 47 *ArubaOS 8 中的 AirGroup*

AirGroup 功能增强

功能	备注
AirGroup 支持有线用户	有线用户现在可搜索 AirGroup 服务
AirGroup 仪表板	显示 mDNS/DLNA 流量趋势、服务器分发和用户/服务器带宽
能够定义跃点数目	能够与离 AP 最多 3 个 RF 跃点的用户共享服务
不允许的指定 VLAN	允许限制跨 VLAN ID 组的 AirGroup 服务
不允许的 VLAN ID（针对用户）	除服务器外，还能为用户定义不允许的 VLAN ID
不允许的用户角色（针对服务器）	除服务器外，还能为用户定义不允许的用户角色

表 8 *AirGroup 功能增强*

AppRF

ArubaOS 6 中的 AppRF

ArubaOS 6 中的 AppRF 能够识别策略并将策略应用于约 2000 个应用程序，包括允许、阻止或速率限制。升级 AppRF 或在 ArubaOS 6 中添加新的 AppRF 签名需要进行系统范围的升级。例如，即使只需要在一个本地控制器上测试新签名，或者需要在主-本地控制器部署中修复一个错误，也需要将网络中的主控制器与所有本地控制器一同进行升级。此限制会导致网络中断，并且需要计划整个网络的停机。此外，ArubaOS 6 还无法创建自定义 AppRF 策略或自定义应用程序类别。

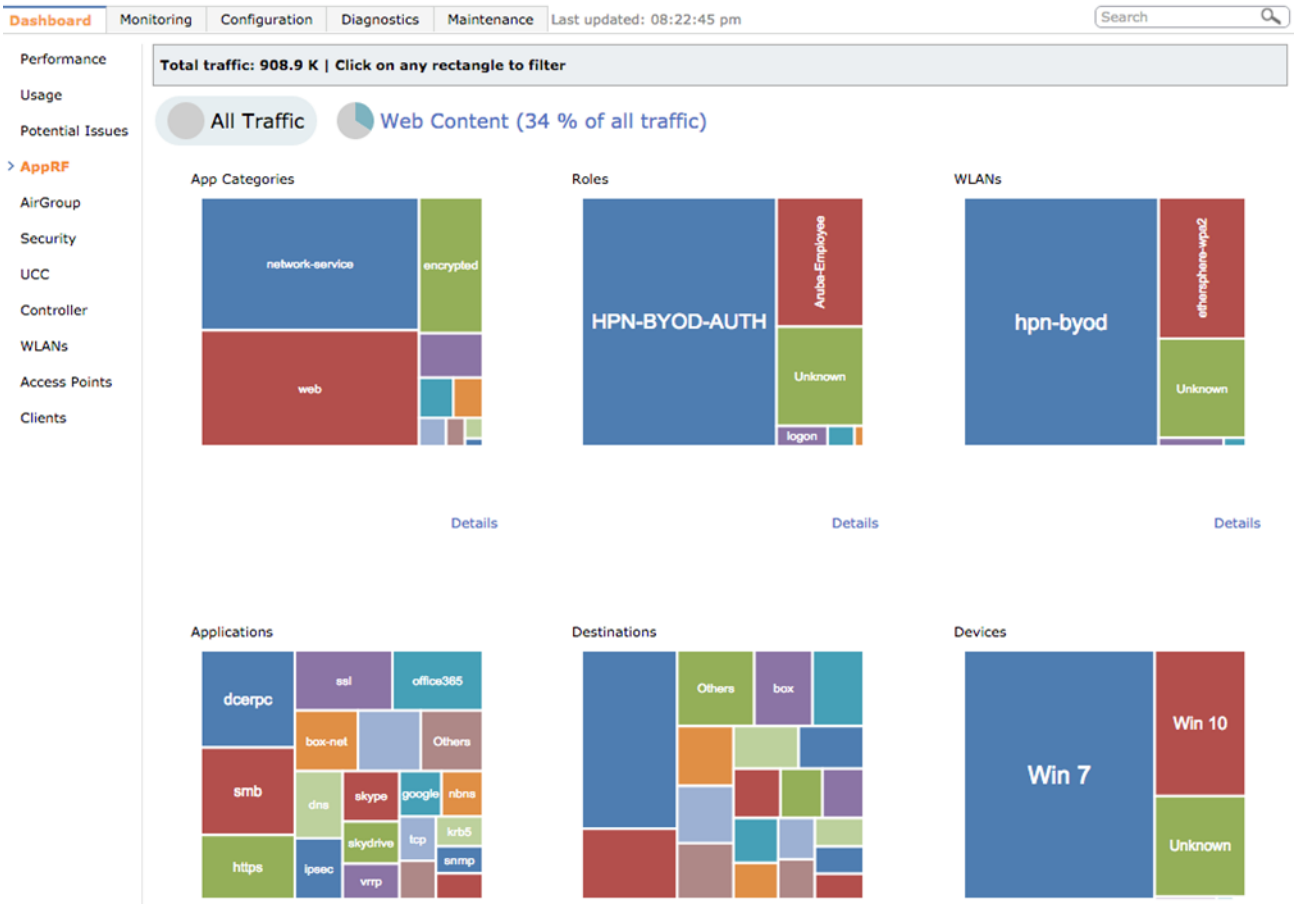


图 48 *ArubaOS 6 中的 AppRF*

ArubaOS 8 中的 AppRF

ArubaOS 8 支持在不必执行升级的情况下向控制器添加新应用程序。可在运行时下载并激活原型捆绑包，以便添加对新应用程序的支持。DPI 当前支持约 2,000 个可对它们应用规则的应用程序。在 ArubaOS 6 中无法分类自定义应用程序，例如组织内部的应用程序。ArubaOS 8 支持可根据需要推送到 MC 的自定义应用程序。

在 MM 上定义的新应用程序将以二进制格式存储为应用程序签名，并且在向下推送配置时，这些应用程序会被传输到 MC。然后应用程序签名被添加到 MC 上的活动签名集，从而提供根据需要支持和定义新应用程序的功能。MM 可配置最多 64 个自定义应用程序，每个应用程序有 16 个规则。此外还可创建自定义应用程序类别，以及对它们应用策略。即使 MC 失去与其 MM 和备用 MM 的连接，MC 也不会失去应用程序分类功能。

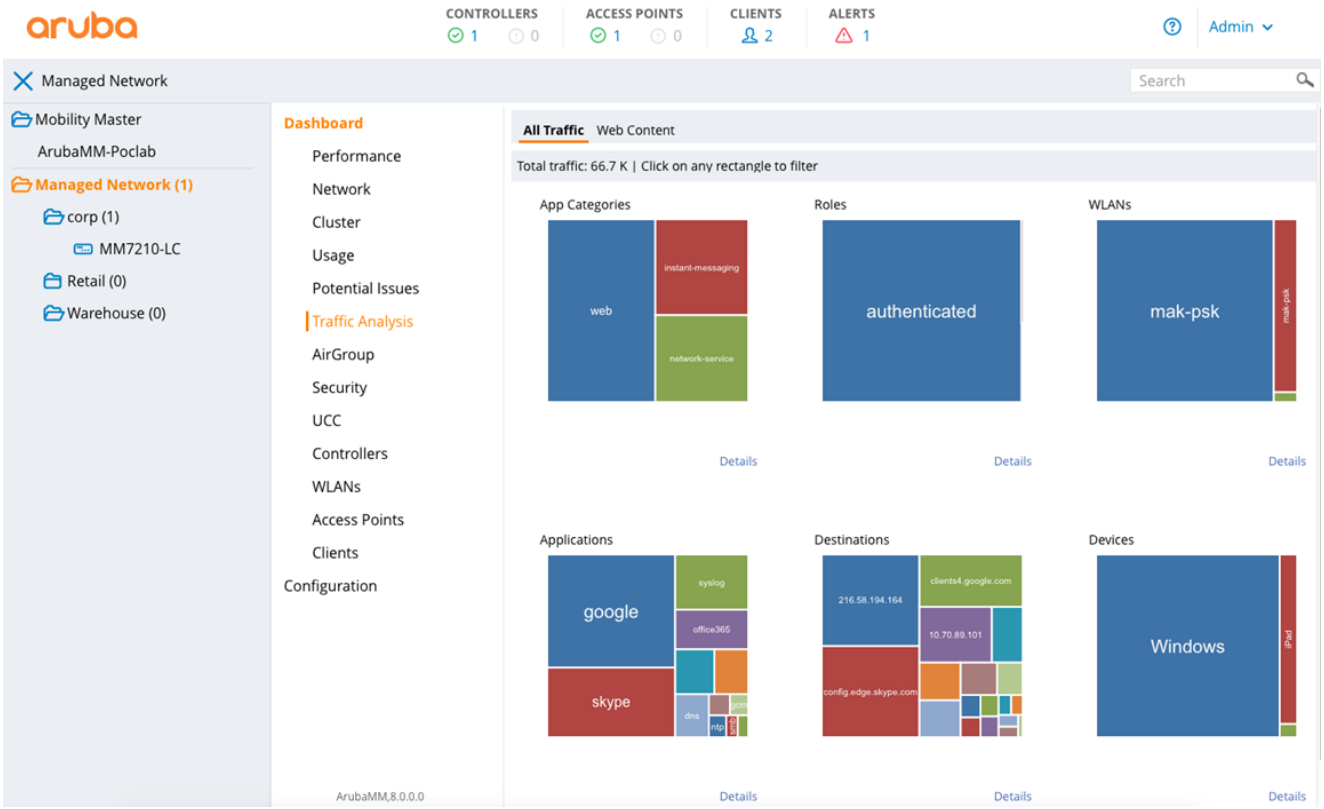


图 49 *ArubaOS 8 中的 AppRF*

应用程序编程接口

在 ArubaOS 8 中可使用三种方法来自动进行配置：

- 命令行界面
- 图形用户界面
- 应用程序编程接口

ArubaOS 6 仅可通过 CLI 和 GUI 实现配置自动化。不幸的是，局限于这些方法意味着如果 CLI 输出随时间而改变，那么脚本也需要更改，因为并非所有输出均使用结构化数据生成。每次有新的代码发布就修改脚本很快会变得乏味。同样，GUI 基于 CLI，而一些 GUI 页进行了硬编码。

ArubaOS 8 引入了基于 JavaScript 对象表示法 (JSON) 模型的结构化 API，该模型使用结构化格式的 GET 和 SET 消息来进行所有配置。结构化数据意味着所有数据均以特定格式加以组织，其中属于某一数据类型的所有元素均遵循相同数据模型。这是通过将架构与数据分离实现的。架构（也称为元数据）是一种 JSON 格式的数据模型表示，其告诉用户如何解释数据。

ArubaOS 8 环境中的数据以 JSON 格式表示 MM 的配置状态。MM 按照与架构相同的顺序排列数据，以便能够根据架构指令对其进行解释。

配置 API

配置 API 使用 HTTPS 对 MM 进行 GET 和 POST 调用。GET API 用于了解 MC 的配置状态并提供类似输出以显示命令，区别之处在于它们采用 JSON 格式。POST API 用于配置 MC。例如，可通过 POST API 创建新的 VLAN。

配置 API 可能会吸引面向服务提供商的客户，或者使用 Elk Stack 等工具构建自己大型数据系统的客户，在这些系统中，他们可使用第三方 API 从单一配置点与整个网络进行交互。可在 **https://x.x.x.x/api** 上获得完整 API 列表，其中 x.x.x.x 表示控制器的 IP 地址。

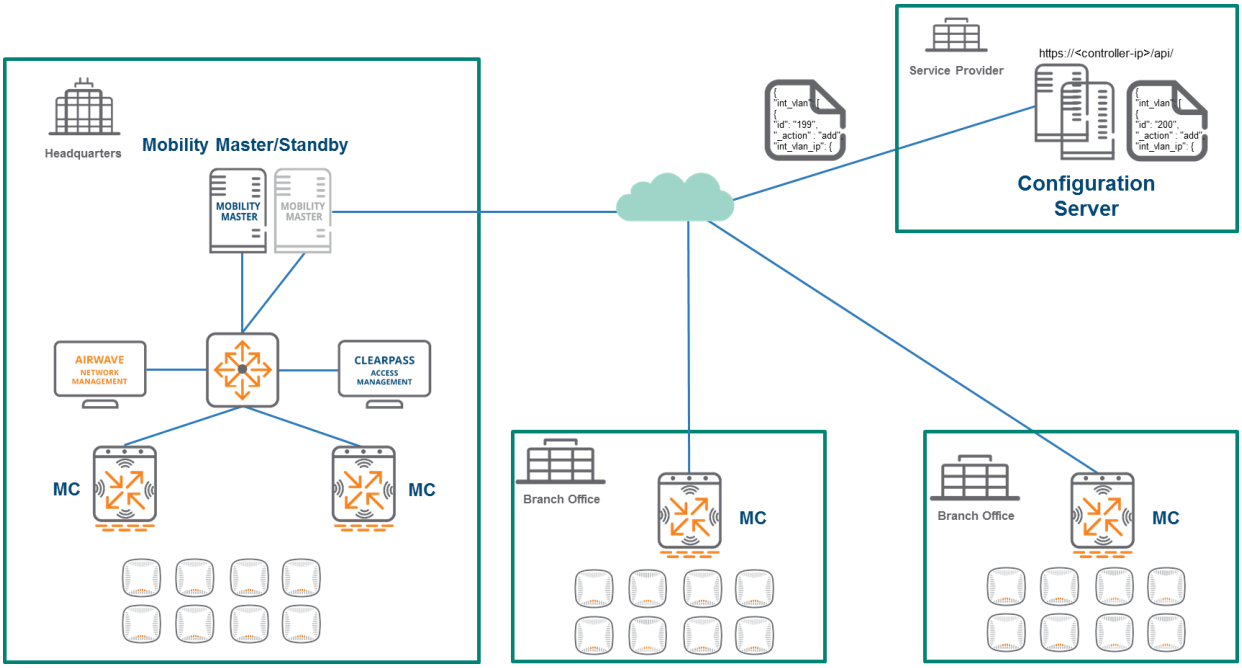


图 50 *ArubaOS 8 中的配置 API*

上下文 API

上下文 API 类似于 Aruba 的分析与定位引擎 (ALE) 中的北向 API。其主要用途是网络分析。以下列出了 ArubaOS 8 中的预定义 API：

上下文 API

- 园区
- 楼宇
- 楼层
- 接入点
- VAP
- 站
- 无线
- 目的地
- 应用程序

来自 ALE

- 存在
- 位置
- 地理围栏

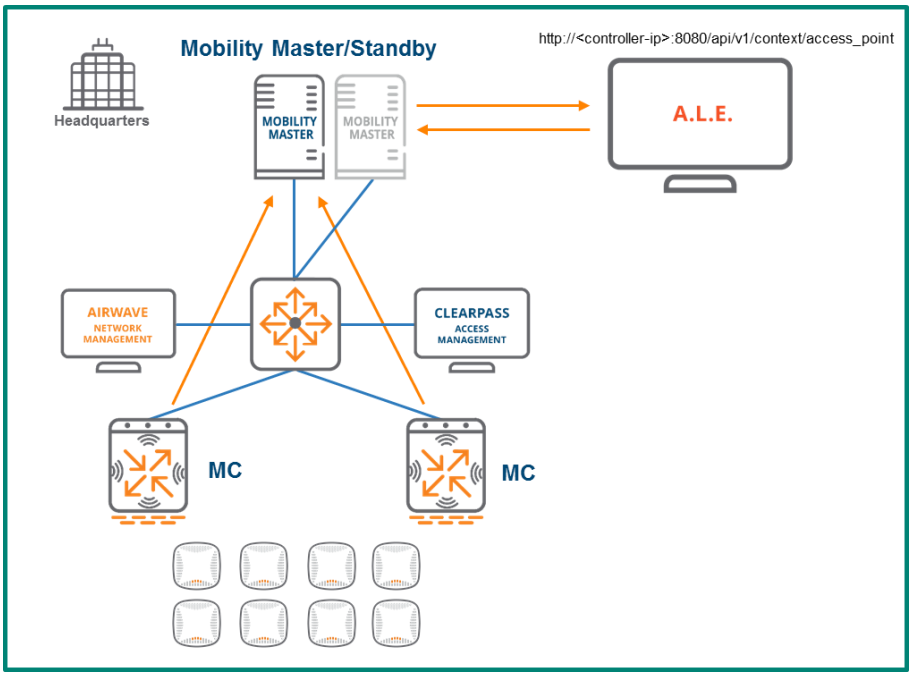


图 51 *ArubaOS 8 中的上下文 API*

Multizone

Multizone 是 ArubaOS 8 中的一项功能，其可使 IT 组织具有使用相同 AP 的多个独立且安全的网络。先前在一个物理位置创建 2 个安全网络需要使用单独 AP。Multizone 可使一个 AP 在两个不同的控制器上端接两个不同的 SSID。从客户端一直到控制器都会对数据进行加密，包括在其流经 AP 时。ArubaOS 8 中的 Multizone 可实现完全安全的网络隔离和安全性，即使同一 AP 正在服务于来自多个网络的流量也是如此。

*区域*是单个管理域下 MC 的集合。区域可包含独立控制器或 MM 及其关联的 MC。*Multizone AP* 是一个 Aruba AP，能够在位于不同区域的 MC 上端接其隧道。AP 在单个控制器上端接其隧道的 ArubaOS 6 部署将被视为单区域部署。

架构

在 Multizone 部署中，AP 与主区域之间存在一个主隧道。在以下示例的情况下，主区域是一个具有 MC 的 3 节点群集的 MM。Multizone 配置文件从主区域下载到 AP。凭借获取的 Multizone 配置文件，AP 了解数据区域控制器（独立）的 IP 地址，然后建立一个数据隧道。

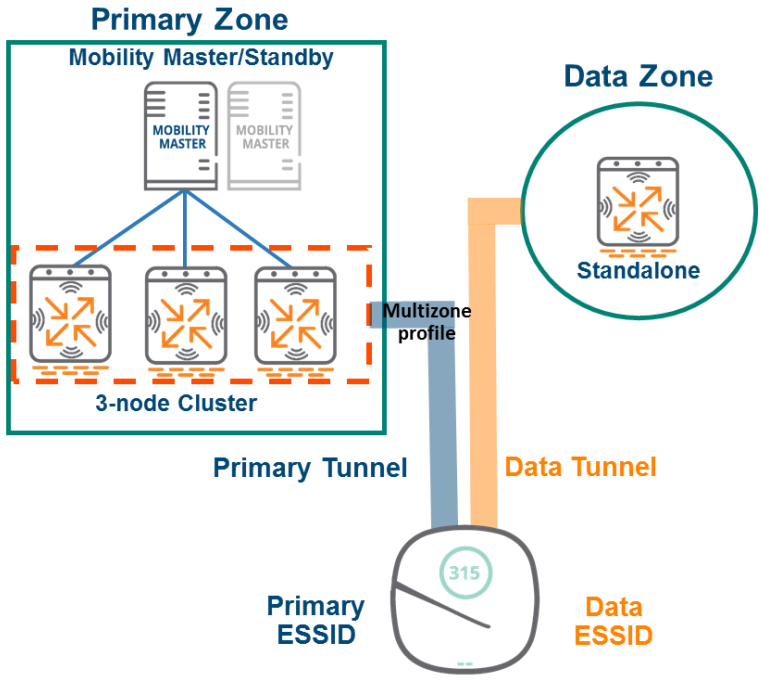


图 52 *Multizone 架构*

区域角色

Multizone 具有几个关键目标和功能：

- 能够充分利用现有 AP 部署广播来自不同控制器域或区域的 SSID
- 为属于不同组织的不同基本服务集 (BSS) 创建安全容器
- 在不同区域之间竖立一道墙，其中每个管理域只能查看和管理各自的 SSID

主区域

- 启动时 AP 连接到的区域
- 保留对 AP 管理和配置（AP、WLAN 和 RF 配置文件）的完全控制
- 将 Multizone 配置文件配置为启用该功能的区域

数据区域

- 从主区域接收到 Multizone 配置后 AP 连接到的辅助区域
- 无法重新启动、升级或配置 Multizone AP
- 允许的唯一配置是隧道模式下的虚拟 AP 配置

必须在主区域上启用 RFP 许可才能启用 Multizone 功能。在数据区域控制器上不需要许可。

主要考虑因素

1. 所有区域中的 MC 都需要运行相同 ArubaOS 版本
2. 数据区域应使用主区域使用的相同 AP 组和 AP 名称
3. 无法从同一 MM 管理主区域 MC 和数据区域 MC
4. 最多只能有 5 个区域：1 个主要区域和 4 个数据区域
5. 所有区域最多只能有 12 个组合控制器
6. 每个射频 16 个 VAP 的限制仍适用于所有区域
7. 不支持远程 AP
8. 支持除 AP-9x 外的所有 AP 类型

MM 冗余

在设计关键任务网络时，不仅要为数据平面提供冗余，还要为管理和控制平面提供冗余，这非常重要。在没有 MM 的情况下，除无法推送配置之外，还有一些服务可能会受到不利影响。拥有冗余 MM 可确保配置和服务相关任务受到保护并将始终根据需要继续执行。

以下是在 MM 无法访问时受影响的服务列表：

- AirGroup 操作（仅限集中模式）和仪表板可见性
- UCC 仪表板可见性
- 未缓存的 WebCC 查找
- AirMatch 重新校准
- ClientMatch
- 配置 API
- 无线入侵检测和预防

ArubaOS 8 中可为 MM 配置两种类型的冗余。第 2 层冗余涉及数据中心 (DC) 内的冗余。主用 MM 负责管理网络中的所有 MC，以及任何关联的配置和服务相关任务。主用 MM 由备用 MM 使用 VRRP 进行备份。如果主用 MM 出现故障，关联的控制器将在检测到该故障后立即故障切换到备用 MM。然后备用 MM 承担主用 MM 的角色。

第 3 层冗余涉及第 3 层单独网络中的灾难恢复，其一般应用于 DC。在 ArubaOS 8 架构中，这涉及每个 DC 中的一个或一对 MM，以及 DC 中的第 2 层冗余（如果使用一对）。在第 3 层冗余的情况下，一个 DC 被称为*主 DC*，另一个 DC 被称为*辅助 DC*。

无论正在使用哪种类型的冗余，许可均在主用 MM 上进行配置。这些许可将自动同步到 L2 和 L3 冗余 MM。

第 2 层冗余

Aruba MM 依赖作为其第 2 层冗余机制的 VRRP。除主用 MM 的设备配置节点下的任何配置外，整个配置层次结构将自动从主用 MM 同步到备用 MM。

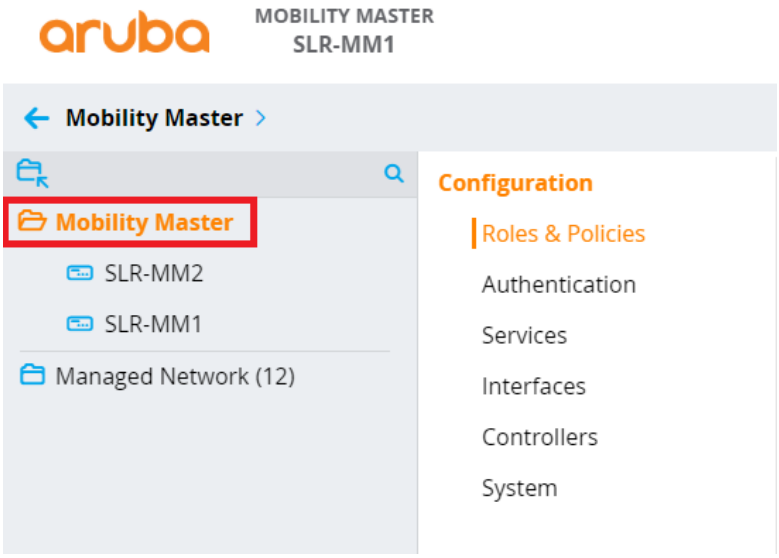


图 53 *针对所有 MM 的配置*

主用和备用 MM 通用的配置放在 **MM** 节点下，以便将同步它们。必须将特定于主用 MM 的配置（例如，IP 地址和 VRRP）单独放置在各自的特定设备节点上。无法从备用 MM 配置 MM 服务和托管设备。

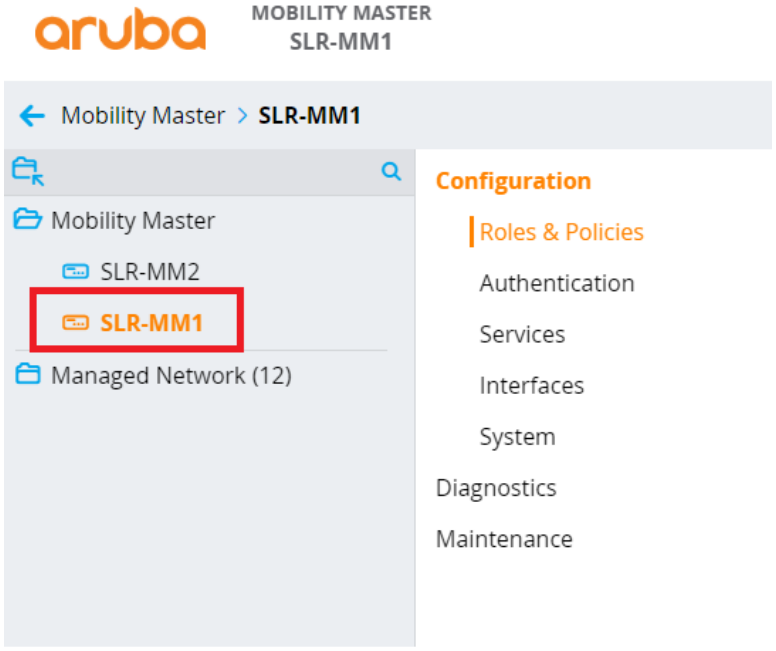


图 54 *特定于主用 MM 的配置*

拓扑结构

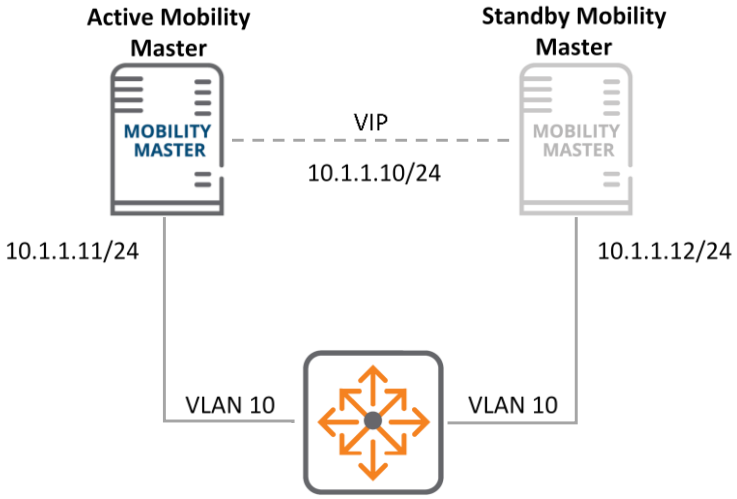


图 55 *第 2 层 MM 冗余*

同步

在主用与备用 MM 之间一配置 VRRP 和主冗余，就会同步整个配置层次结构。以下列出了在主用 MM 上配置数据库同步时定期同步到备用 MM 的一些数据库：

- WMS 数据库
- 本地用户数据库
- 全局 AP 数据库
- AirGroup 数据库
- 许可数据库
- CPSec 数据库

同步间隔被指定为数据库同步配置的一部分。数据库同步间隔是可配置的。Aruba 建议的最佳做法是将间隔配置为不小于 20 分钟。配置更频繁的间隔可能会增加大量网络开销。

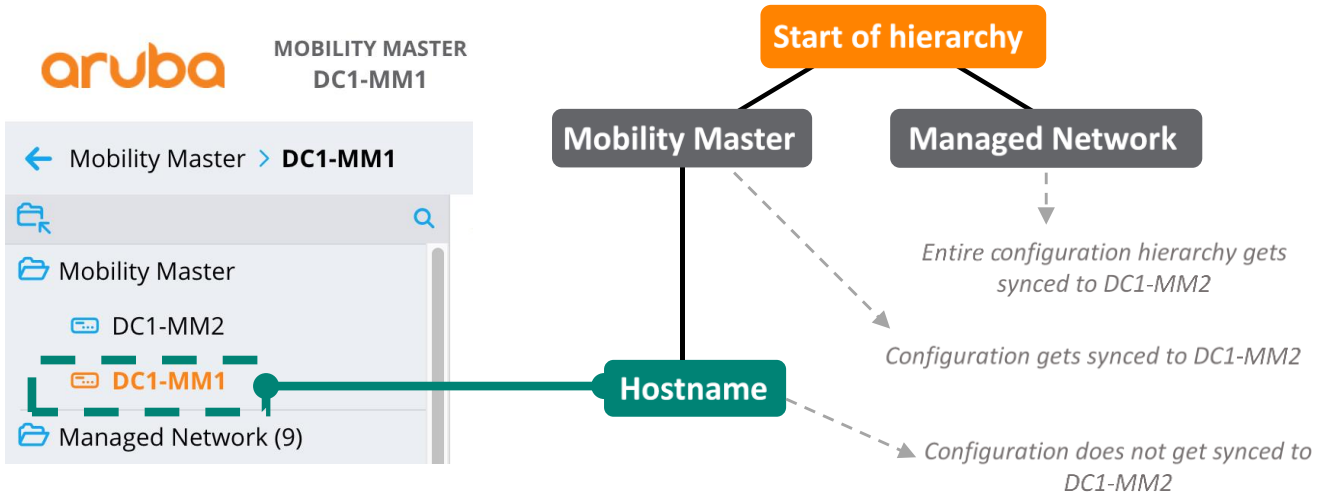


图 56 *数据库同步*

在主用和备用 MM 执行了初始同步并达到稳定状态后，已提交并保存在主用 MM 上的任何增量配置更改都会导致与备用 MM 进行配置同步。

此行为的例外情况是在主用 MM（即 /mynode）的设备配置节点上进行的任何更改。这些更改不会同步到备用 MM。备用 MM 包含自己的设备配置版本，因此任何所需的更改都必须直接在相对应的设备配置节点（即备用 MM 上的 /mynode）上进行。在备用 MM 上不允许对层次结构中的其他节点进行配置更改。

MC 故障切换

MC 使用 MM 对共享的 VRRP 实例的虚拟 Internet 协议 (VIP) 地址与其主用 MM 进行通信。主用 MM 是 VRRP 实例的主控制器，在默认情况下其每秒都会发出 VRRP 通告。备用 MM 监控这些通告，以便确保 VRRP 实例主控制器仍能正常运行。如果备用 MM 无法接收来自主控制器的 VRRP 通告，例如在控制器故障或重启的情况下，则备用 MM 将一直等待连续错过三个通告，之后其将自己提升为该 VRRP 实例的主控制器。MC 继续与其 MM 的虚拟 IP 通信。将影响 MC 的唯一因素是在因 VIP 所有权变更备用 MM 已变为活动状态时，它们与备用 MM 建立 IPsec 会话所用的时间。MC 继续与不同 MM 间 VRRP 实例的 VIP 所有者相对应。在任何特定时刻拥有该 VIP 并因此作为主用 MM 的实际设备与这些 MC 无关。

第 3 层冗余

第 2 层 MM 冗余非常适用于备用 MM 支持主用 MM 的单个数据中心拓扑结构。但如果数据中心断电或网络中断，则 MC 可能会失去与两个 MM 的连接，这将导致功能丧失。第 3 层 MM 冗余的引入可防止发生此类情况。其涉及在第 3 层连接上由辅助 MM 或 MM 对备份主 MM 或 MM 对，以便在主 DC 出现故障时使控制器实现服务连续性。尽管第 2 层冗余可被视为数据中心内 MM 之间的冗余，但第 3 层冗余可被视为数据中心之间的冗余。

拓扑结构

以下是在 MM 之间已配置有第 3 层冗余的两个常见拓扑结构示例。

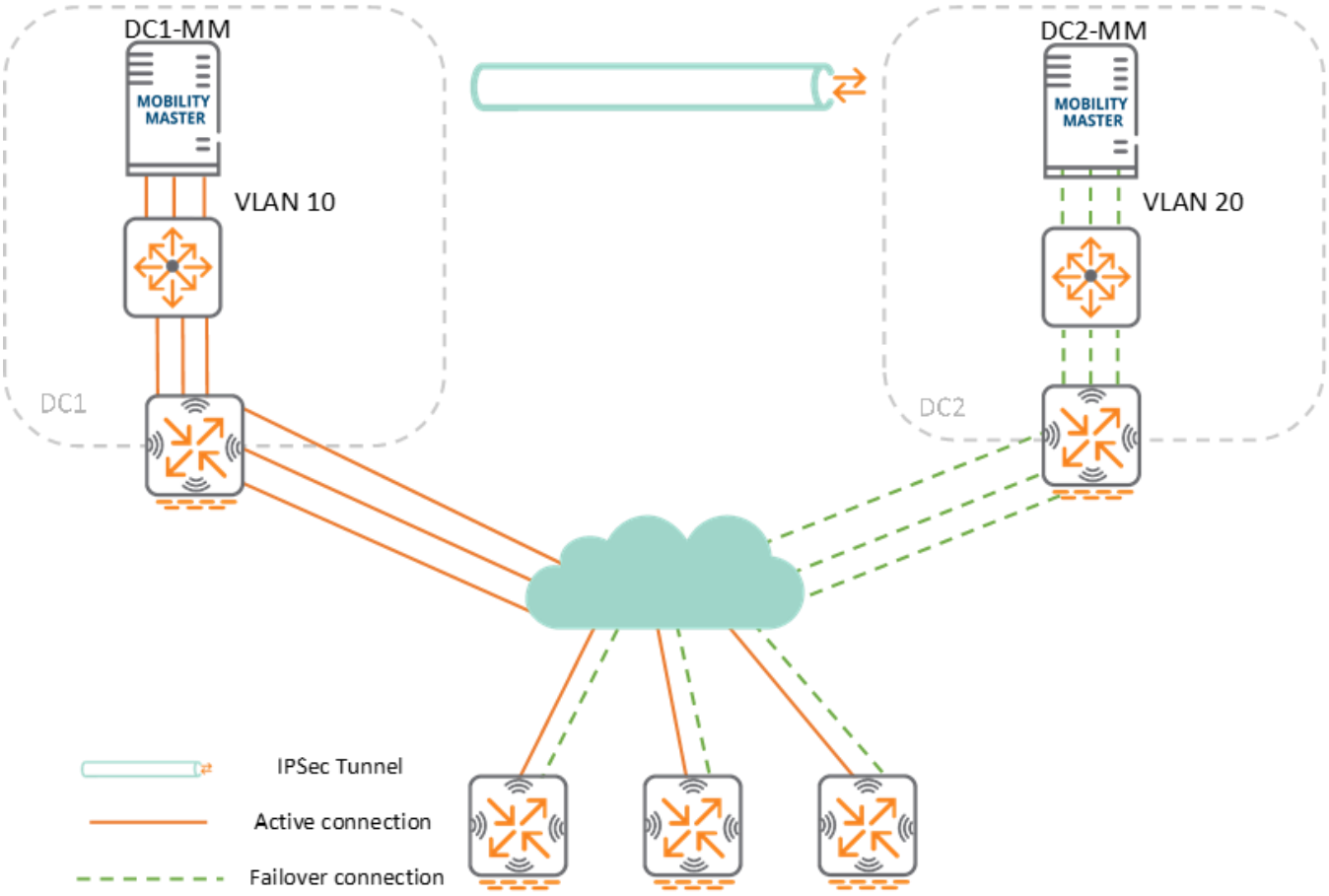


图 57 *两个 MM 之间的第 3 层冗余*

在上述拓扑结构中，DC1 作为具有 DC1-MM 的主 DC，而 DC2 是具有 DC2-MM 的辅助 DC。在主 DC 与辅助 DC 之间已配置了第 3 层冗余。由于 MC 能够检测并启动故障切换，因此它们还需要配置有辅助 MM 的 IP 地址。

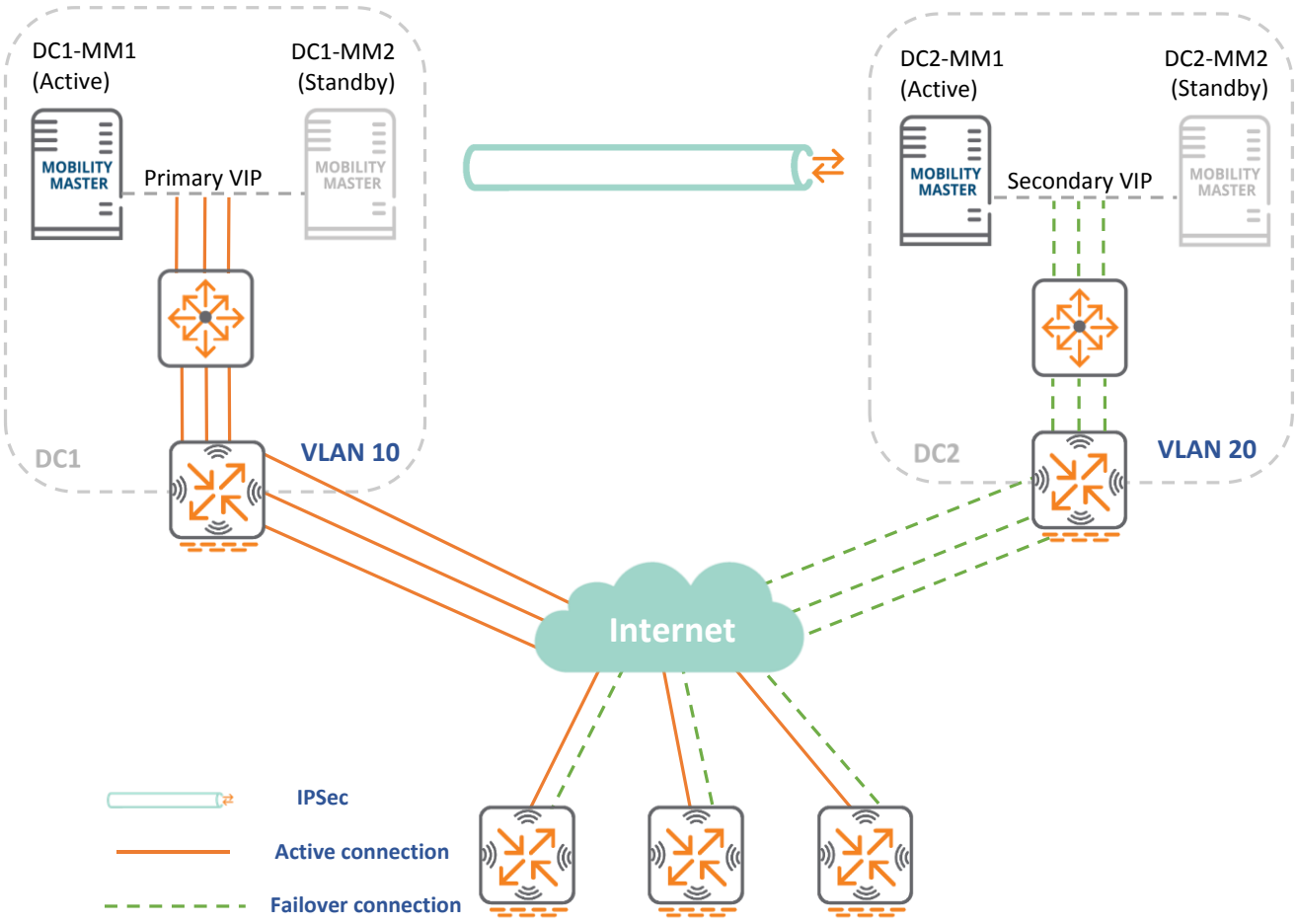


图 58 *两个 MM 对之间的冗余*

在图 58 中，DC1 是主 DC，DC1-MM1 作为主用 MM，DC1-MM2 作为备用 DC。在每个 DC 内的 MM 之间配置了第 2 层冗余。如果 DC1-MM1 出现故障，则 DC1-MM2 会作为新的主用 MM 接管 VIP。MC 将在 DC1-MM1 与 DC1-MM2 之间针对 VRRP 实例的 VIP 上进行端接。

DC2 是辅助 DC，DC2-MM1 作为主用 MM，DC2-MM2 作为备用 MM。在它们之间按照与在 DC1 中相同的方式配置第 2 层冗余。如果 DC2-MM1 出现故障，则 DC2-MM2 将承担针对其共享 VRRP 实例的 VIP 的所有权，并成为 DC2 中的新主用 MM。

从 MC 的角度讲，DC1 中的 VIP 是主 MM IP，而 DC2 中的 VIP 是辅助 MM IP 地址。与第一个第 3 层拓扑结构一样，MC 将需要配置有针对两个数据中心的虚拟 IP 地址。

同步

DC1 中主用 MM 上的整个配置层次结构、数据库和关联配置与 DC2 中的主用 MM 同步。如果在 DC 中配置了第 2 层冗余，则 DC2 中的主用 MM 也会将配置层次结构、数据库和关联配置与其备用 MM 同步。

MM 之间的配置同步不包括 MM 和设备节点下的同步。

故障切换

MC 使用 IP 运行状况检查 (ping) 主动监控与主 DC 和辅助 DC 的连接，但仅与主 DC 建立活动连接。仅在与主 DC 中所有可用 MM 的连接均丢失时，才建立与辅助 DC 的连接。

如果与主 DC 的连接丢失，则 MC 将等待 15 分钟，然后再故障切换到辅助 DC。15 分钟的窗口期使主 DC 有机会恢复并保护 MM，使它们免受不必要故障切换情况的影响，例如在重新启动它们时。在这种情况下，MM 将停机，而不打算将 MC 故障切换到辅助 DC。

如果 15 分钟后与主 MM 的连接仍然存在，则 MC 将故障切换到辅助 MM，辅助 MM 仅在检测到自己与主 MM 的 IPsec 隧道已关闭时才会接受它们。如果稍后主 MM 重新启动，则 MC 将立即断开与辅助 MM 的连接并重新与主 MM 连接。

在默认情况下，即使故障切换后，辅助 MM 仍保持辅助角色。在此期间，不能在 MC 上执行任何配置更改。这是为了防止*裂脑状态*，在该状态下，在辅助 MM 将配置更改已推送到 MC 后，主 MM 会重新启动，从而导致每个 DC 中的配置不同。即使在辅助角色中，所有 MM 服务仍将照常运行。故障切换事件的唯一影响是对 MM 配置功能的影响：运行能力将完全不受影响。

如果主 MM 无法恢复，则可将辅助 MM 转换为主角色，这将使其能够将配置更改推送到 MC。将辅助 MM 提升为主角色的过程可能只能手动执行。这会迫使人们确认他们绝对确定主 DC 将保持停机，以及确认需要此更改并且此更改也是必要的。如果辅助 MM 被提升为主 MM 的角色，则必须将出现故障的主 MM 重新配置为新的辅助 MM，以便其继承新主 MM 的配置和数据库。这样做可防止出现故障的主 MM 在恢复时承担其旧角色，以及在此过程中因主角色中有两个 MM 而产生冲突。

群集

目标

群集是 ArubaOS 8 中引入的关键功能之一，其专门用于利用 MM 架构为关键任务网络提供最大价值。开发群集是为了实现以下目标：

- **无缝园区漫游** - 单个大型第 2 层域中的客户端在漫游时将关联并保持锚定到单个 MC。用户将保持相同的子网和 IP 地址，即使它们在锚定到不同控制器的 AP 间漫游也是如此。这样可在不影响或牺牲性能的情况下实现移动性
- **有状态客户端故障切换** - 用户流量将保持不间断，并且在群集成员出现故障时将保护高价值会话。无需对客户端重新进行身份验证，也不会对性能产生不利影响。对性能的影响微乎其微，以致于无论用户当前正在使用哪些应用程序，他们都不会注意到任何性能下降，甚至不知道发生了故障
- **接入点和客户端负载分担** - AP 和用户在作为群集成员的控制器间自动进行负载分担。此过程可确保均匀分配，以便提供和保持最佳网络性能，以及在所有群集成员间保持容量，以实现新的客户端关联
- **实时升级** - Aruba 允许客户执行服务中群集升级，这可在不影响性能的情况下实施改进，同时网络保持完全运行。实时升级功能可实现完全自动化升级。对于拥有必须保持全天候运行的关键任务网络的客户而言，这是一项关键功能

NOTE

只能在群集中的 MC 以及与它们关联的 AP 上执行实时升级。

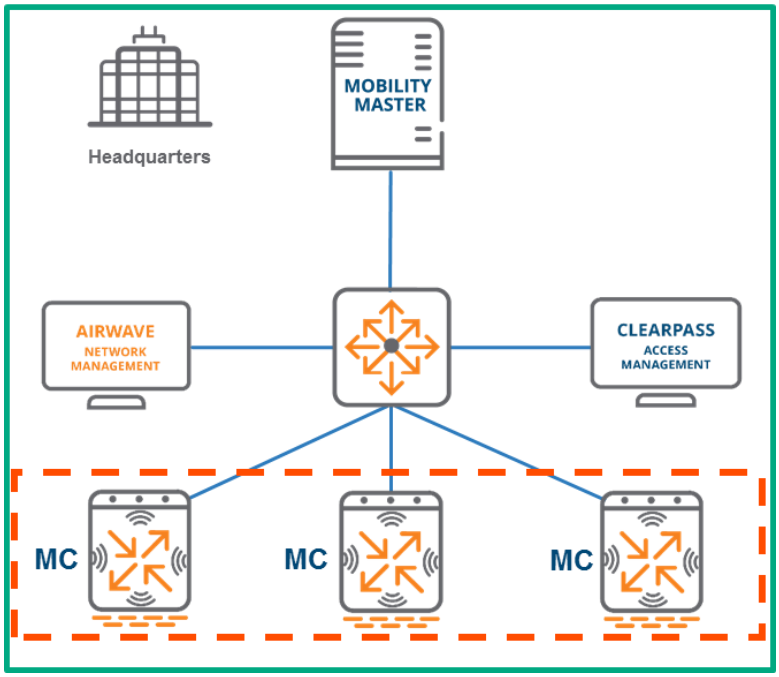


图 59 *典型 MC 群集架构*

要点和考虑因素

群集是 ArubaOS 8 的一个关键功能，但并非对所有设备都能够启用它。只有受 MM 管理的 MC 才能形成群集。但在具有另一个 MM 或具有 MC 的群集中，MM 本身不能成为该群集的成员。MM 严格作为群集中 MC 的管理设备。尽管针对 MM 环境的冗余选项包括群集以及具有 AP 快速故障切换的高可用性 (HA)，但这些是互相排斥的功能。必须选择其中一个，因为它们不能同时运行。

群集中的所有 MC 都需要运行相同软件版本，以便使故障切换到新控制器的 AP 不会无意中升级到新版本。

应注意，独立控制器不支持群集。如果必须使用独立控制器，则它们的主要冗余机制为 HA。园区接入点、远程接入点和网状接入点均支持群集及其所有组成功能，无需任何额外许可。支持群集的控制器型号包括 72xx 系列、70xx 系列和 VMC。

下表详细列出了每个产品系列的群集容量：

产品系列	每个群集的设备数
72xx	12
70xx	4
虚拟	4

表 9 *按产品系列划分的群集容量*

尽管在技术上可将 72xx 和 70xx 设备结合在同一个群集中，但作为长期部署选择，强烈建议不要这样做。此类情况作为临时迁移策略是可接受的，但作为最佳实践，群集设备应始终是同类的。如果将不同型号的控制器群集在一起，则所有控制器可扩展性限制将被降级到最低控制器型号的功能。例如，如果使用两个 7240 控制器和一个 7210 控制器创建群集，则该群集的可扩展性容量将被限制为三个 7210 控制器的可扩展性容量。

在任何情况下，虚拟控制器和硬件控制器都不能结合在一个群集中。

如果在群集中的任何 MC 上端接 RAP，则该群集中允许的设备数量被限制为 4 个。下图描绘了群集的仪表板视图：

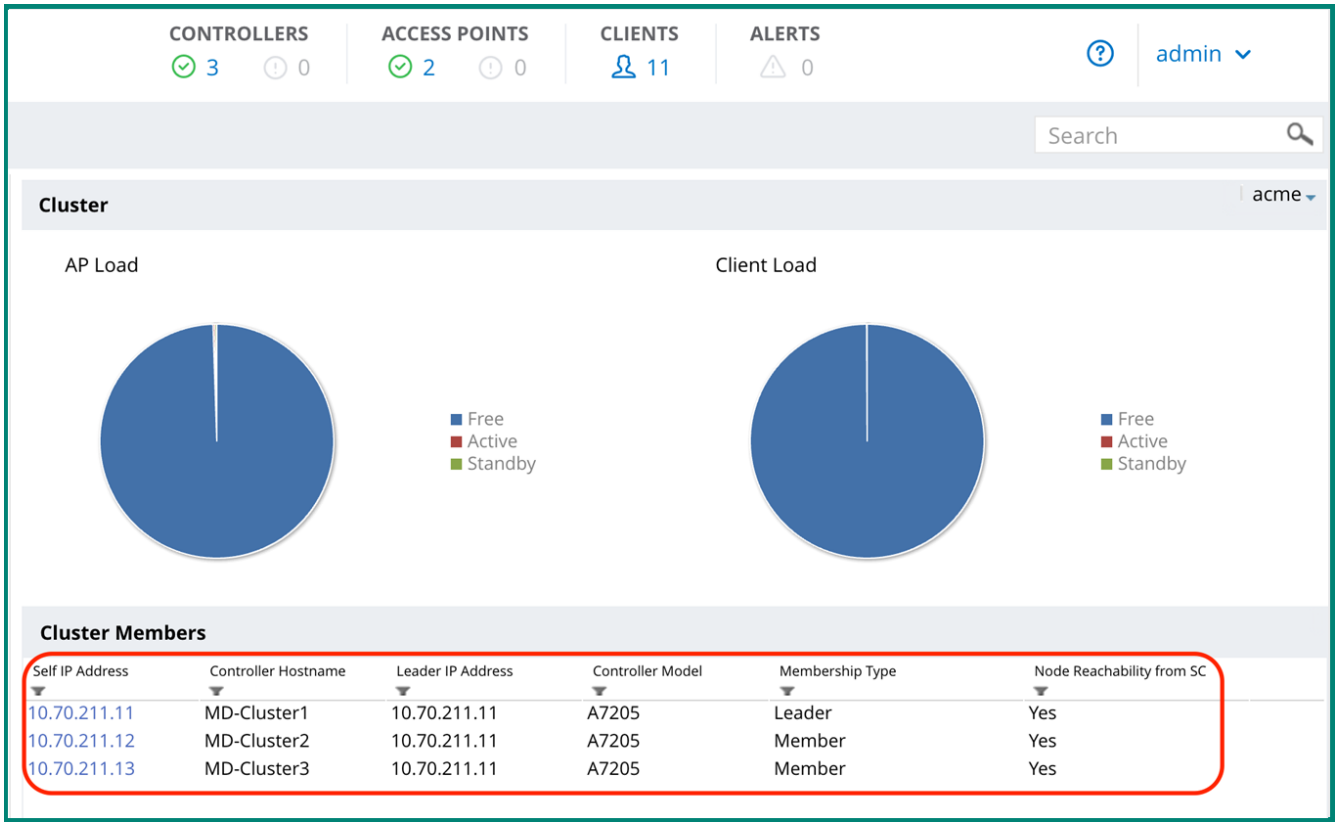


图 60 *MM 群集仪表板*

通过导航到主仪表板的**群集**选项卡可通过 GUI 访问以上视图。可在此选项卡下看到有关群集的关键统计信息，包括 MM 管理的群集中的控制器、AP 和客户端的数量，以及群集成员的当前 AP 和客户端负载。底部的**群集成员**部分显示与作为群集成员的 MC 相关的关键统计信息，包括其 IP 地址、型号，以及哪个设备正在作为当前群集领导者。

群集形成

握手过程

群集形成的第一步涉及握手过程，其中消息在所有潜在群集成员之间进行交换。握手过程使用呼叫消息进行，交换这些消息是为了验证所有群集成员之间的第 3 层可访问性。通过这些消息交换与群集相关的信息，包括内部版本、群集名称，以及有关发送此消息的 MC 的信息。在所有成员已交换了这些消息后，它们将在全网状配置中建立相互之间的第 3 层 IPsec 连接。下图描绘了在群集形成前作为握手的一部分参与呼叫消息交换过程的群集成员：

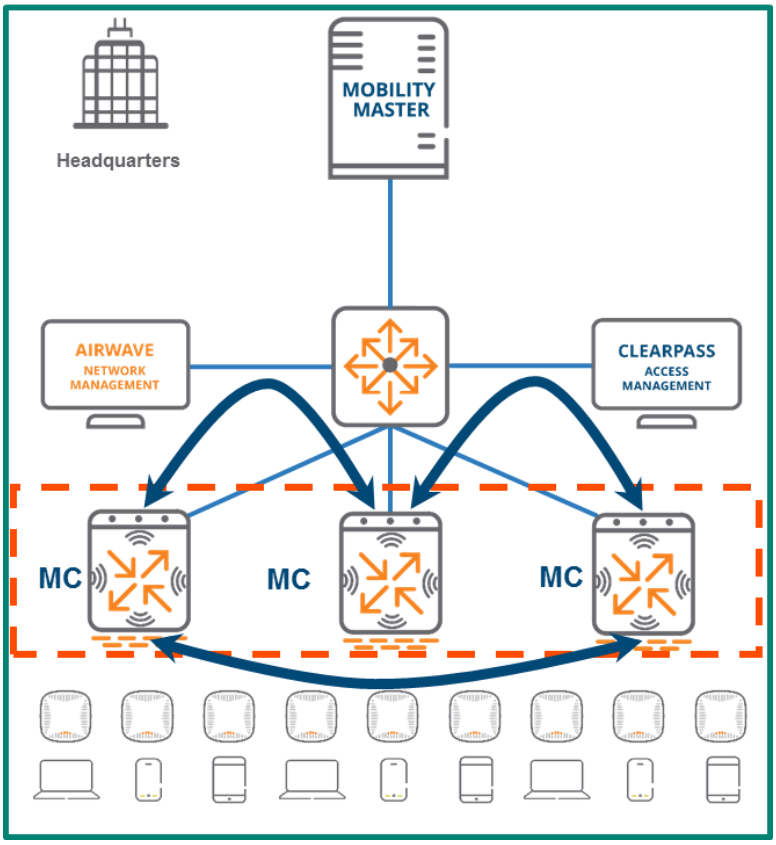


图 61 *握手过程/呼叫消息*

VLAN 探测

在群集已进入“L3 已连接”状态并且群集成员已完全形成 IPsec 连接后，每个成员都将在其每个 VLAN 上将第 2 层探测单播到其他每个群集成员。如果探测过程成功，则群集将从“L3 已连接”状态转变为“L2 已连接”状态，这意味着所有群集成员都在共享相同 VLAN。

NOTE 可在第 2 层或第 3 层网络上形成群集。Aruba 强烈建议将具有第 2 层连接的群集配置为启用 VRRP。这样做可为群集提供 CoA 支持，以及促进控制器发现。

在讨论 Aruba MC 群集时，*“L2 已连接”*和*“L3 已连接”*为特定术语，它们指的是群集的状态，以及表示所有群集成员是否共享相同 VLAN。它们不是传统网络术语*第 2 层*和*第 3 层*的缩写。下表提供了有关该主题的额外说明：

术语	定义
第 2 层连接	MC 已连接并共享相同管理 VLAN
第 3 层连接	MC 可相互访问，但不共享相同管理 VLAN
L2 已连接	所有成员都共享所有相同 VLAN 的群集状态
L3 已连接	成员不共享所有相同 VLAN 的群集状态

表 10 *群集连接区别*

NOTE 可在“L2 已连接”状态下配置群集中的 MC，即使它们不共享所有相同的 VLAN 也是如此。此操作是通过输入一个强制 MC 将某些 VLAN 从探测过程中排除的命令来完成的。

领导者选举

在每个群集中都将选择一个 MC 作为群集领导者。群集领导者有多个责任，包括：

- 确定向每个群集成员映射哪些客户端
- 对客户端进行动态负载分担，以确保在群集成员负担过重时均匀分配资源。在将新成员添加到群集时，群集领导者将在所有成员间均匀地重新分配负载。这是一个完全无缝的过程，用户不会遇到任何性能下降问题
- 识别每个 AP 和客户端的备用 MC，以确保在控制器出现故障时进行有状态故障切换

群集选举在初始握手之后发生，其作为 VLAN 探测和心跳过程的一个并行线程。选举群集领导者是因为每个群集成员均交换包括它们的已配置优先级、平台值和 MAC 地址的消息。

心跳

在初始握手后，所有群集成员都将开始以并行于领导者选举和 VLAN 探测线程的定期间隔互相发送心跳消息。这些心跳消息作为群集成员故障的主要检测机制。心跳是群集领导者用于确定每个群集成员角色的过程不可分割的一部分。

连接性和验证

通过导航到**仪表板 > 群集 > 群集成员**，然后选择任何群集成员的 IP 地址，可在 MM 的 GUI 中查看群集的连接状态。下图显示了该视图：

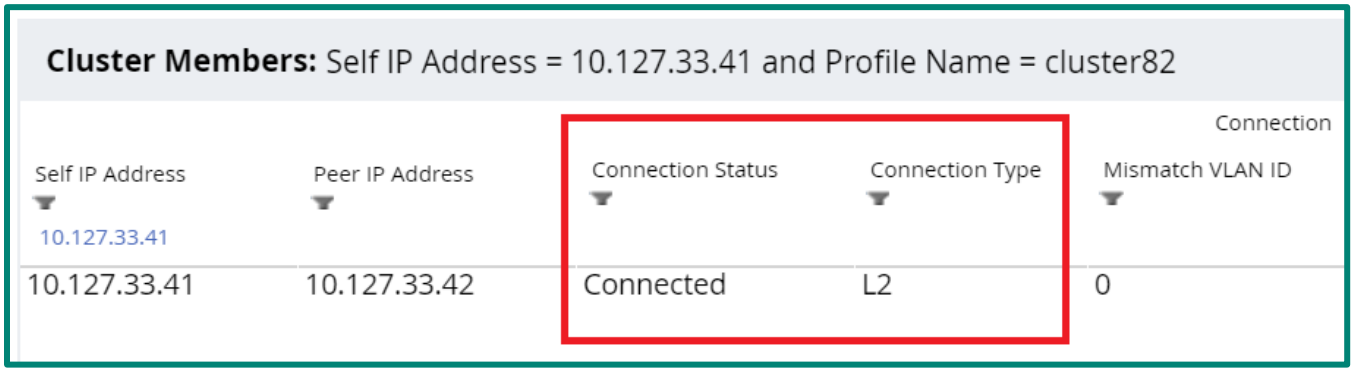


图 62 *查看群集连接状态*

群集角色

除作为群集领导者外，MC 可在群集中具有以下四种角色的任何组合：

1. AP 锚点控制器 (AAC)
2. 用户锚点控制器 (UAC)
3. 备用 AAC (S-AAC)
4. 备用 UAC (S-UAC)

AP 锚点控制器

AAC 分配

锚定是在 ArubaOS 8 中作为群集功能集一部分引入的概念。锚定和群集旨在实现以下目标：

- 通过无缝园区漫游提高用户移动性
- 确保在群集中均匀分配资源，以便保持可实现的最高性能级别
- 启用冗余方案，从而为群集创建容错并最大程度降低 MC 故障的影响

AP 锚点控制器 (AAC) 可被视为锚定到它的任何 AP 的 LMS。每个 AP 均接收 LMS 的 IP 地址，在已端接了它们后，它们将保持锚定状态，直到群集领导者确定应将它们移至其他群集成员为止。可通过三个步骤将 AP 锚定到其 AAC：

1. AP 建立与其 AAC 的主用隧道
2. 群集领导者从其他一个群集成员为 AP 动态分配备用 AP 锚点控制器 (S-AAC)
3. 指定后，AP 建立到 S-AAC 的备用隧道

AAC 和 S-AAC 分配过程与配置 HA 的方式类似，但不必手动配置，该过程完全是动态的。为 AP 指定了 AAC 后，后续步骤就会自动进行。下图为 AAC 分配的直观表示：

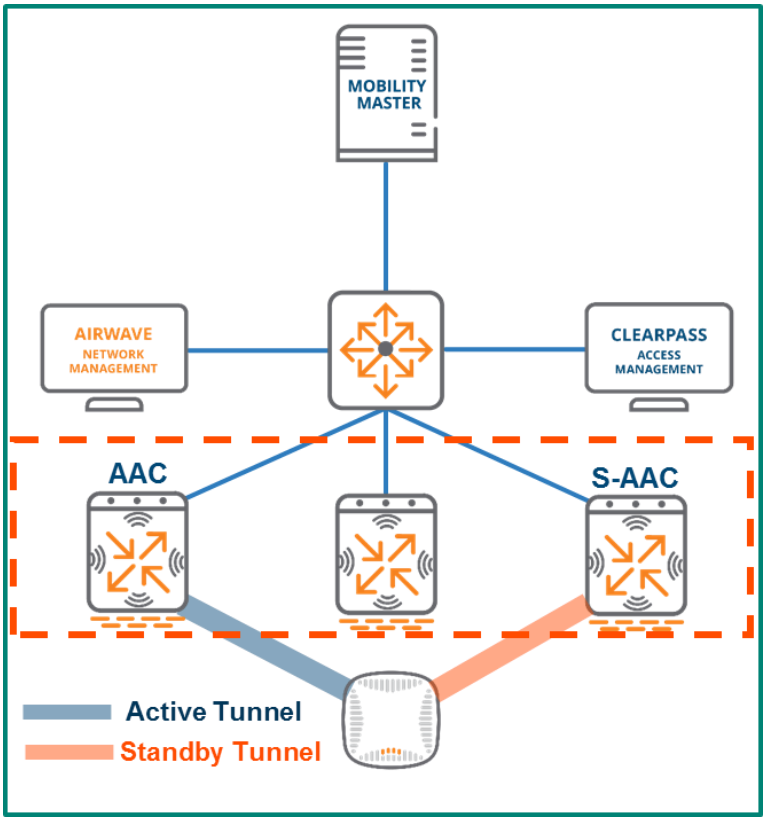


图 63 *AAC 分配*

通过导航到**仪表板 > 接入点**，可在 MM 的 GUI 中识别 AP 的 AAC 和 S-AAC：

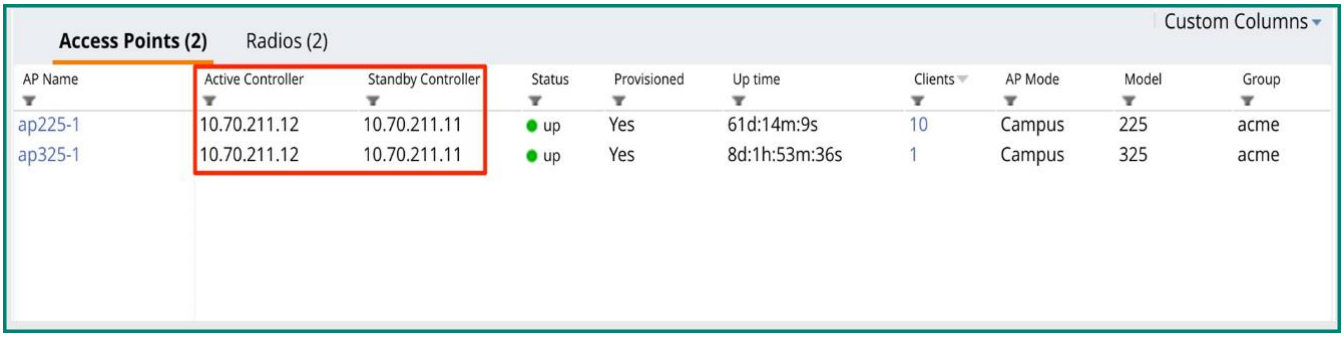


图 64 *AAC 和 S-AAC 状态*

尽管以上视图表明两个 AP 的 S-AAC 是同一设备 (10.70.211.11)，但应注意，此 S-AAC 由群集领导者分配，并且在 AAC 上端接的所有 AP 并非都具有相同 S-AAC。其可轻松成为不同群集成员，这取决于群集领导者根据分配时群集环境中的条件所做出的决定。

AAC 故障切换

从群集成员为每个 AP 均分配 AAC 和 S-AAC。AP 将提前创建到两个 MC 的隧道，以便促进故障切换过程。到 S-AAC 的冗余隧道可确保在群集成员出现故障时 AP 将无缝转换。凭借群集，配置的故障切换事件对网络性能的影响可忽略不计，用户也不会意识到发生了故障。以下步骤概述了故障切换的发生过程：

1. AAC 出现故障。由于心跳，S-AAC 立即检测到此故障
2. 在检测到此故障时，S-AAC 将指示 AP 进行故障切换
3. AP 断开其与故障 AAC 的隧道，并故障切换到 S-AAC
4. 现有 AP 备用隧道变为活动状态，S-AAC 承担针对该 AP 的 AAC 的角色
5. 从剩余群集成员为该 AP 动态分配新的 S-AAC
6. AP 建立到新 S-AAC 的备用隧道

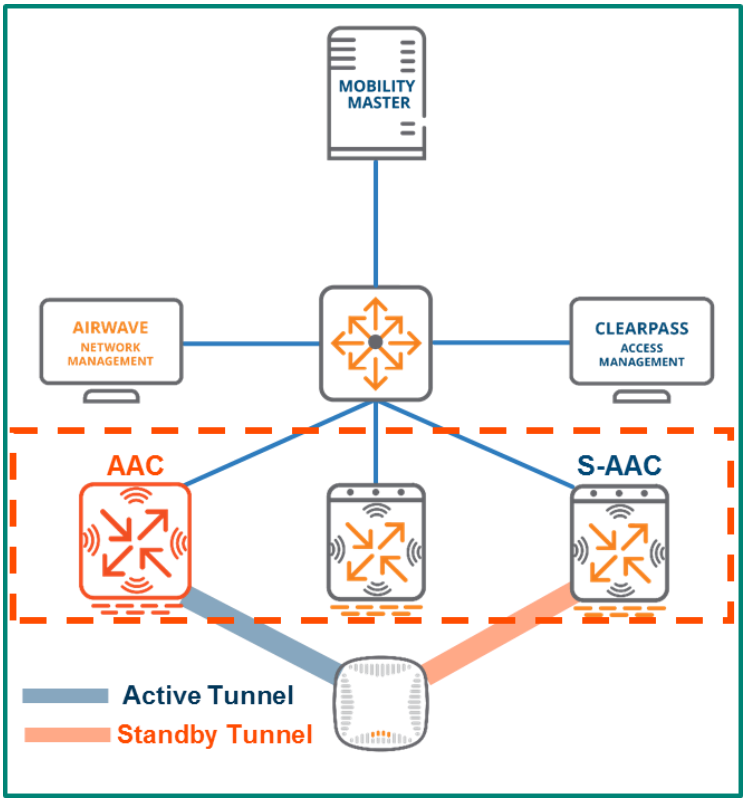


图 65 *AAC 出现故障*

上图显示了先前将 AP 连接到的 AAC 已出现故障。此时，S-AAC 将指示 AP 进行故障切换并断开其到故障 AAC 的主用隧道。

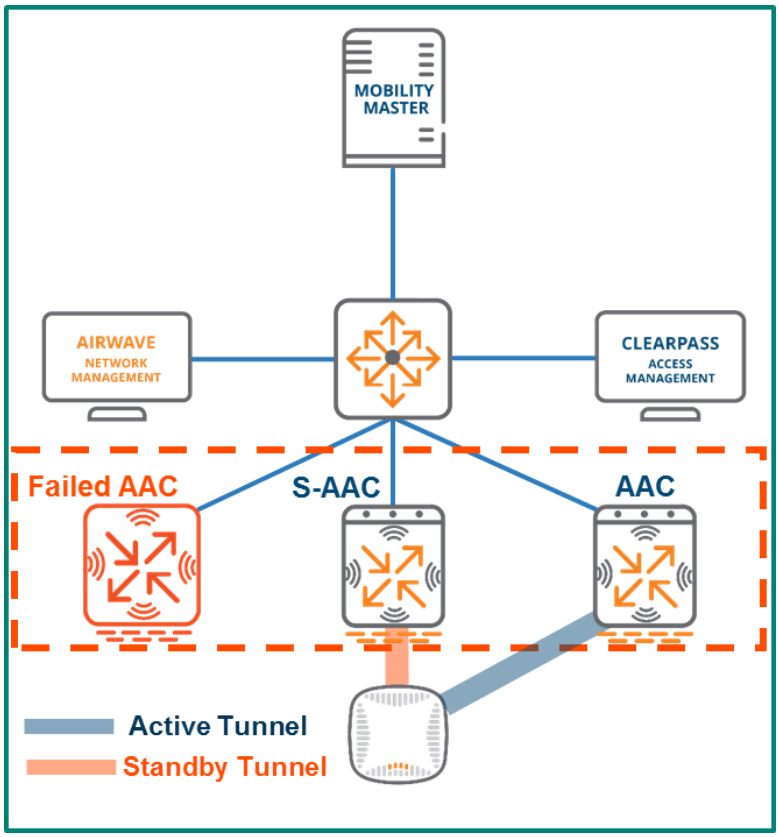


图 66 *AP 故障切换和分配的新 S-AAC*

旧 S-AAC 现在承担了 AAC 的角色。AP 与 S-AAC 之间的旧备用隧道现在已成为主用隧道。群集领导者动态选择了群集的另一个成员作为新的 S-AAC，并且 AP 已相应地构建了一个备用隧道。此故障切换过程现在完成，用户完全觉察不到所有步骤。

用户锚点控制器

使用*用户锚点控制器 (UAC)* 将用户锚定到控制器的概念是 ArubaOS 8 中的全新概念，其主要用于增强用户漫游体验。当用户关联到一个 AP 时，如果已存在到他们 UAC 的现有隧道，他们将使用此隧道。如果该 AP 没有建立到其 UAC 的隧道，则会创建一个动态隧道。当客户端漫游到新 AP 时，他们正在漫游离开的 AP 会断开其动态隧道。无论在用户漫游时客户端与哪个 AP 关联，始终都会通过隧道将用户流量传输回到其 UAC，即使该 AP 具有不同 AAC 也是如此。

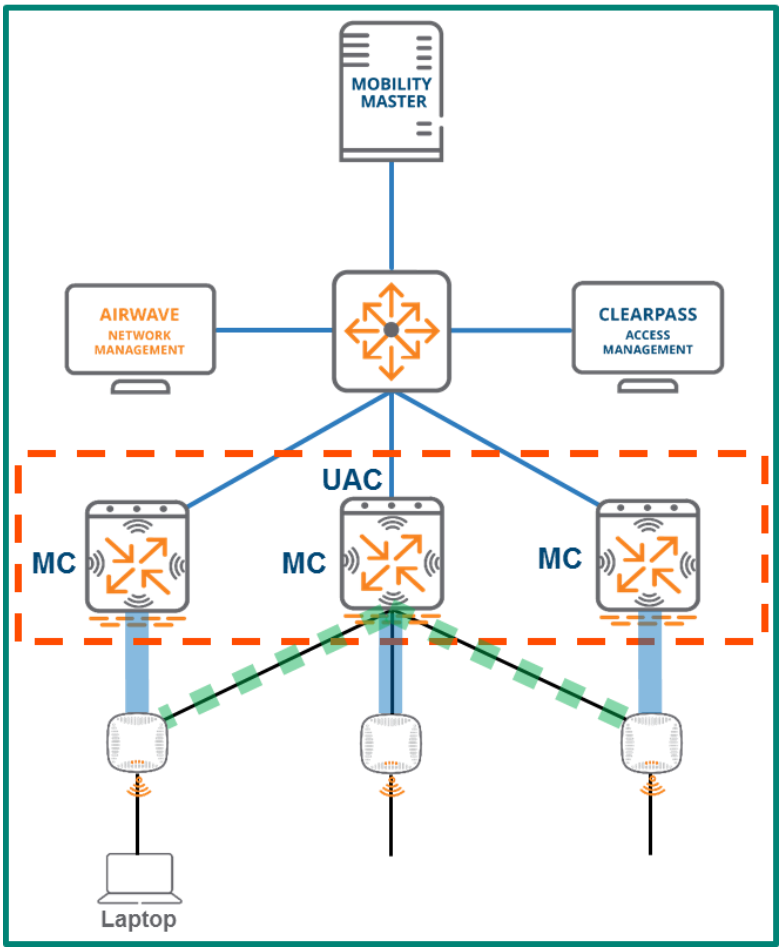


图 67 *到客户端 UAC 的动态隧道*

为保持锚定，必须首先通过 AP 级别的哈希算法将用户映射到 UAC。检查客户端的 MAC 地址，哈希算法会创建一个索引，然后将该索引与映射表进行比较。群集领导者将相同映射表推送到所有 AP，以确保群集中的 UAC 映射一致性。此外，出于冗余目的，群集领导者将基于每个用户动态选择备用 UAC (S-UAC)。下图显示了哈希算法和 UAC 分配过程的示例：

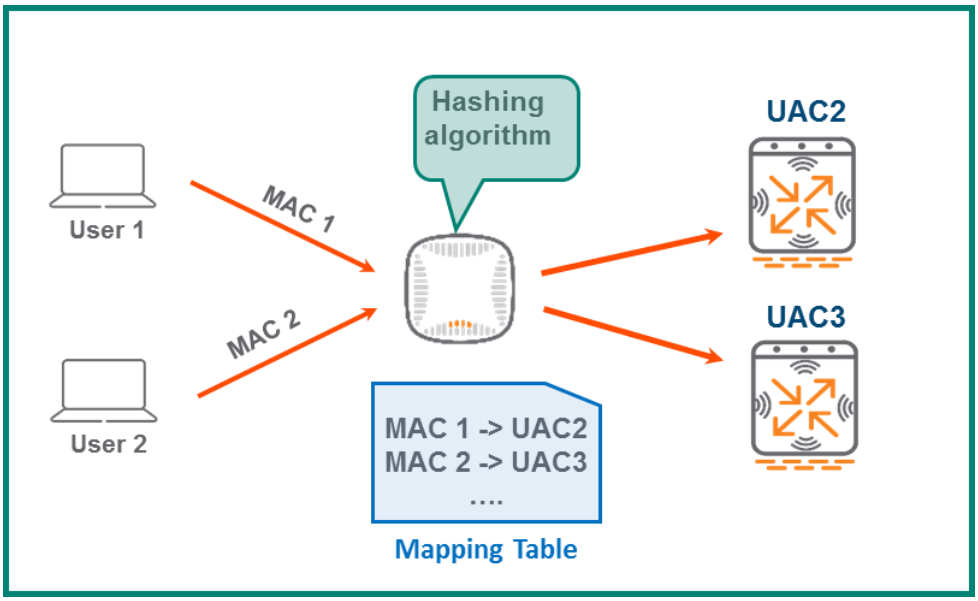
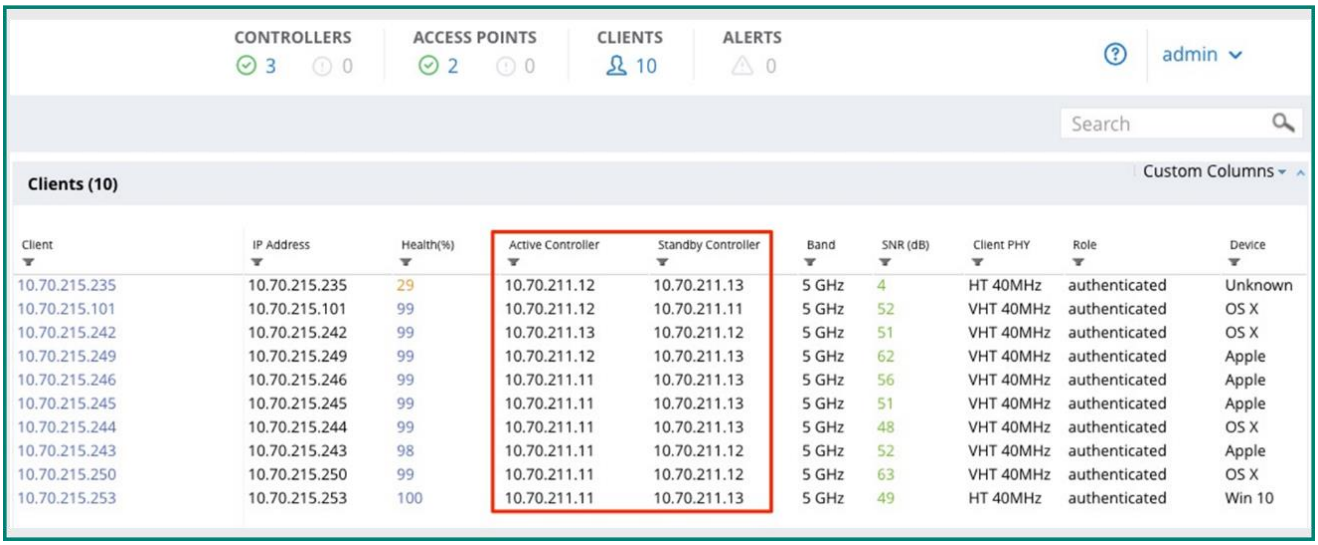


图 68 *UAC 分配过程*

通过导航到**仪表板 > 客户端**，可在 MM 的 GUI 中识别所有关联客户端的 UAC 和 S-UAC 分配：



Client	IP Address	Health(%)	Active Controller	Standby Controller	Band	SNR (dB)	Client PHY	Role	Device
10.70.215.235	10.70.215.235	29	10.70.211.12	10.70.211.13	5 GHz	4	HT 40MHz	authenticated	Unknown
10.70.215.101	10.70.215.101	99	10.70.211.12	10.70.211.11	5 GHz	52	VHT 40MHz	authenticated	OS X
10.70.215.242	10.70.215.242	99	10.70.211.13	10.70.211.12	5 GHz	51	VHT 40MHz	authenticated	OS X
10.70.215.249	10.70.215.249	99	10.70.211.12	10.70.211.13	5 GHz	62	VHT 40MHz	authenticated	Apple
10.70.215.246	10.70.215.246	99	10.70.211.11	10.70.211.13	5 GHz	56	VHT 40MHz	authenticated	Apple
10.70.215.245	10.70.215.245	99	10.70.211.11	10.70.211.13	5 GHz	51	VHT 40MHz	authenticated	Apple
10.70.215.244	10.70.215.244	99	10.70.211.11	10.70.211.13	5 GHz	48	VHT 40MHz	authenticated	OS X
10.70.215.243	10.70.215.243	98	10.70.211.11	10.70.211.12	5 GHz	52	VHT 40MHz	authenticated	Apple
10.70.215.250	10.70.215.250	99	10.70.211.11	10.70.211.12	5 GHz	63	VHT 40MHz	authenticated	OS X
10.70.215.253	10.70.215.253	100	10.70.211.11	10.70.211.13	5 GHz	49	HT 40MHz	authenticated	Win 10

图 69 *客户端 UAC 和 S-UAC 分配*

NOTE

GUI 的“客户端”页标准视图中不包括“主用控制器”和“备用控制器”列。可通过向该页面视图添加自定义来显示它们。

群集功能

无缝漫游

引入 UAC 概念的优势是，其显著增强了在群集中漫游的用户的体验。用户关联到 AP 后，该 AP 会对客户端的 MAC 地址进行哈希处理，并为其分配 UAC。从这一刻开始，来自该用户的流量将始终通过隧道传输到其 UAC。无论用户在漫游时与关联到哪个 AP 都是如此，即使该 AP 在其他控制器上进行端接也是如此。用户漫游到的任何 AP 都会自动将流量转发到在关联时分配给用户的 UAC。如果在用户漫游所在的 AP 与 UAC 之间尚不存在主用或备用隧道，则将创建一个动态隧道。下图为群集中漫游过程的直观表示：

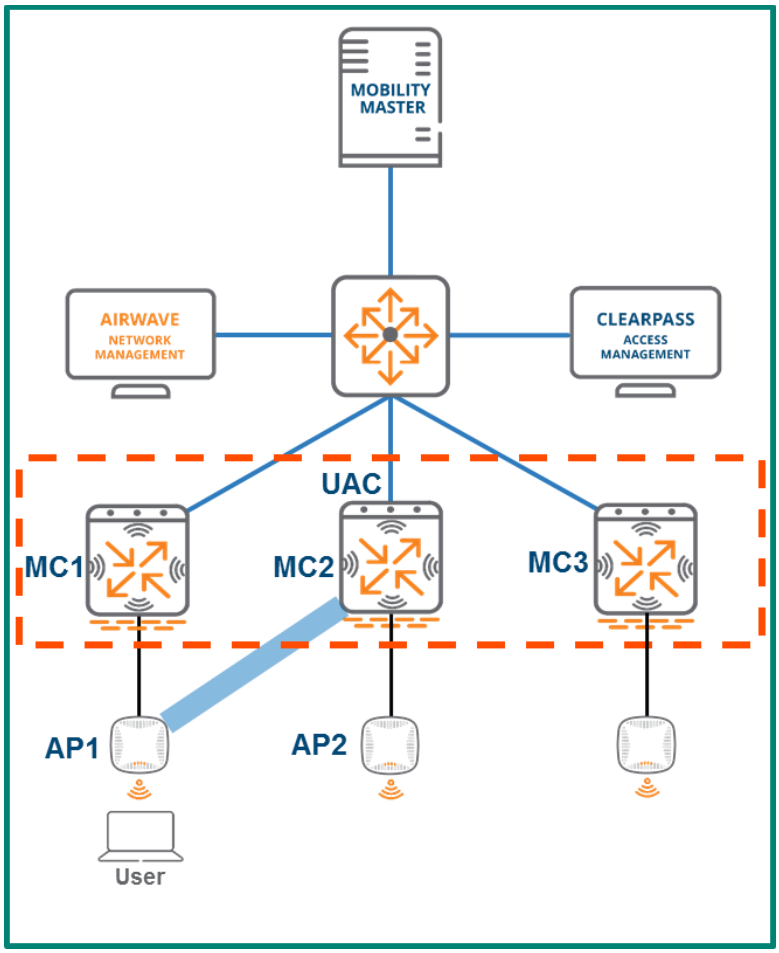


图 70 *群集无缝漫游*

在上图中，用户已关联到 AP1，AP1 在 MC1 上进行端接，但流量正在通过隧道传输到 MC2。在这种情况下，针对该用户已经为 MC2 指定了 UAC，因此在用户漫游到 AP2 或群集中的其他任何 AP 时，将继续通过隧道将流量传输到 MC2。

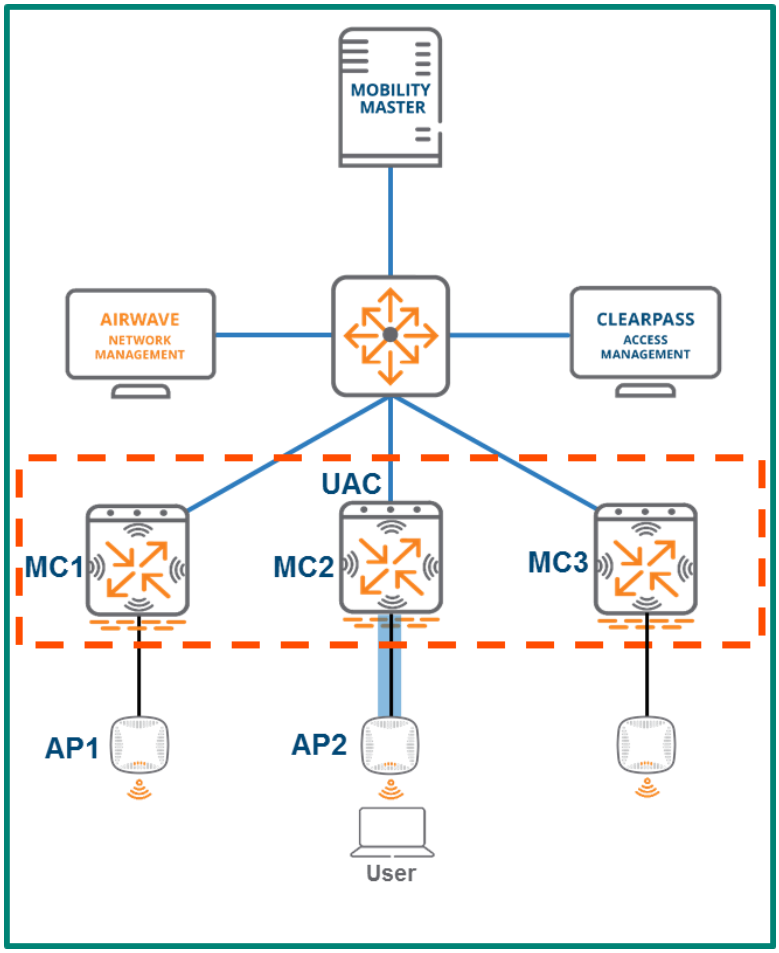


图 71 *群集无缝漫游（续）*

有状态故障切换

有状态故障切换是群集操作的一个关键方面，其可防止用户受到与控制器故障事件相关的任何影响。为群集启用有状态故障切换功能必须符合两个关键条件：

1. 必须启用了冗余模式。可禁用该模式，但在默认情况下，该模式已启用
2. 所有群集成员之间必须存在“L2 已连接”状态

如果符合了这两个条件，则将在 UAC 与 S-UAC 之间完全同步该客户端状态，这意味着站点表、用户表、第 2 层用户状态、第 3 层用户状态、密钥缓存和 PMK 缓存等信息都将在这两个设备之间共享。此外，还会将 FTP、Telnet、SSH 和 DPI 限定会话等高价值会话同步到 S-UAC。同步所有客户端状态和高价值会话信息可使 S-UAC 在客户端的当前 UAC 出现故障时无缝承担客户端的新 UAC 角色。以这种方式建立群集冗余可确保在它们从 UAC 迁移到 S-UAC 时进行有状态故障切换，并且不存在客户端取消身份验证。与在使用 HA 配置时启用的冗余相比，无缝群集故障切换可提供显著优势，这将需要在控制器出现故障时对客户端取消身份验证。下表概述了“L2 已连接”与“L3 已连接”群集状态相比的优势，特别是在它们与冗余、故障切换和性能有关时：

L2 已连接	L3 已连接
完全复制 AP 和客户端	仅完全复制 AP
在节点之间完全同步用户	不同步用户
同步高价值会话	不同步高价值会话
用户故障切换，并且不取消身份验证	在故障切换时对用户取消身份验证
完全冗余	不完全冗余

表 11 *“L2 已连接”与“L3 已连接”*

客户端负载分担

MC 间的客户端负载分担是另一项有助于保持群集性能的功能。尽管对关联到 AP 以进行 UAC 分配的客户端应用的哈希算法非常适用于其预期用途，但其可能导致群集成员间的客户端分配不成比例。这可能会降低系统资源的使用效率。负载分担使群集领导者能够在群集中以最佳方式分配用户，以及确保保持最高性能级别。群集领导者通过执行多步骤计算过程在群集中对客户端进行负载分担，在该过程中，其确定群集的每个控制器的型号，对关联客户端数量进行计数，以及将该客户端计数与每个设备的最大容量进行对照，以便计算其负载率。

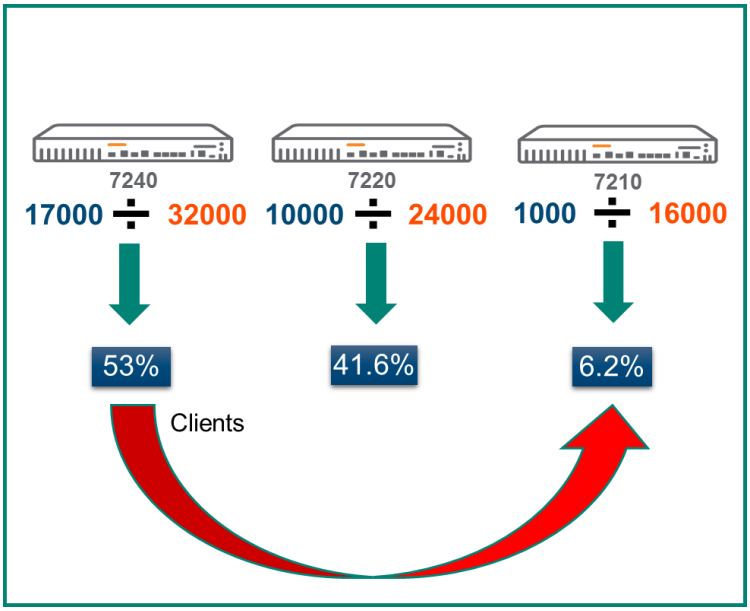


图 72 *群集负载计算过程*

上图展示了群集领导者将为每个成员执行的负载计算过程。在该情况下有三个群集成员，其中每个成员都具有不同的控制器型号：7240、7220 和 7210。每个群集成员下方的蓝色数字表示关联客户端的数量，而橙色数字表示每个特定型号的最大容量。群集领导者比较客户端计数，以及对照每个设备型号的容量检查该计数，然后为每个设备生成一个比率，并以总容量的百分比形式表示。下表显示了已就绪的特定触发器，这些触发器将导致群集领导者在群集中对客户端进行负载分担：

类别	阈值
活动客户端负载	50%
备用客户端负载	75%
不平衡阈值	5%

表 12 *负载分担触发器*

该表展示了当活动客户端负载超过 50%，或者备用客户端负载在群集的任何成员上超过 75%，同时*不平衡阈值*也超过 5% 时将触发重新平衡事件。不平衡阈值是指具有最高负载百分比的群集成员与具有最低负载百分比的群集成员之间的增量，其已就绪，以确保无论群集成员多么接近容量触发器，它们都将始终保持大致均匀的客户端分配。

AP 负载分担

正如群集领导者将对客户端进行负载分担以确保在群集成员间均匀分配一样，其还将为 AP 执行相同功能。动态群集 AP 负载分担是 ArubaOS 8 中的一个可配置功能。只要在将 MC 添加到群集时需要实现轻松可扩展性或者需要消除手动 AP 分配时，就应启用该功能。

在 AP 可参与群集负载分担前，必须首先为它们分配一个 AP 主控制器。AP 主控制器是拥有在 DHCP 选项 43 和 *aruba-master.yourdomain* 的 DNS 记录中使用的 IP 地址的设备。有两个群集互连级别会影响新 AP 在尝试加入群集时查找其 AP 主控制器的方式：

1. **第 2 层连接** - 所有群集节点的控制器 IP 都在同一 VLAN 中
2. **第 3 层连接** - 群集节点的控制器 IP 在不同 VLAN 中

如果群集成员共享第 2 层连接，这意味着它们属于同一广播域。应在群集成员之间创建一个 VRRP 实例，以便其 VIP 可作为加入群集的 AP 的 AP 主控制器。在具有第 3 层连接的群集中，成员不在同一广播域中，因此无法创建 VRRP 实例。可通过 DHCP 选项 43 指定其中一个控制器的 IP 地址，以用于发现，但这样做不会提供冗余，并且会产生单点故障。L3 已连接群集的首选 AP 主控制器发现选项是将 DNS 发现与两个主 Aruba 记录结合使用，从而充分利用从群集成员中选择的两个控制器 IP 地址。

某个 AP 加入群集后，下载的节点列表将具有比发现的 AP 主控制器更高的优先级

在群集成员之间有两种 AP 分配方法：

1. **计划分配** - 这是 ArubaOS 6.x 和 ArubaOS 8 中使用的传统方法，该方法充分利用 AP 系统配置文件中的 LMS-IP 在群集中分配主用 AAC。这是一种确定性方法，需要管理员每 AP 组均预先计划 AP 分配，并将相应群集成员控制器 IP 地址配置为每个 AP 组中的 LMS-IP。
2. **自动分配** - 此方法充分利用 ArubaOS 8.1 中引入的 AP 负载分担功能。AP 端接分配自动进行，群集领导者根据每个群集成员上的现有 AP 负载为 AP 分配主用 AAC。

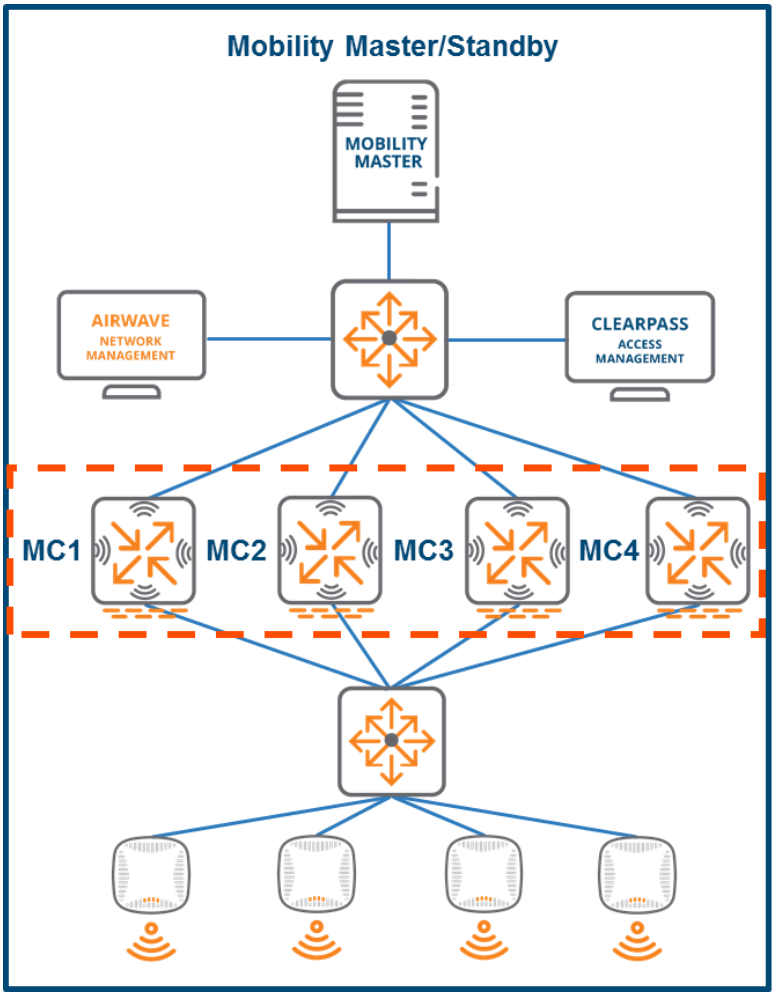


图 73 *群集架构*

计划分配

预先为 AP 选择 AAC 可使管理员对 AP 负载分配具有确定性控制。在 AOS 8.3 中默认启用 AP 负载分担，如果管理员选择计划 AAC 分配，则必须禁用 AP 负载分担。每个 AP 系统配置文件中属于每个 AP 组的 LMS-IP 需要设置为其中一个群集成员的控制器 IP 地址。使用计划分配方法时，加入群集的 AP 使用以下步骤连接到其 AAC：

1. AP 从发现的 AP 主控制器下载其配置，包括 LMS-IP 地址分配
2. AP 采用指定的 LMS 控制器作为其主用 AAC，并且端接 GRE 隧道
3. AP 接收由群集领导者确定的备用 AAC 分配

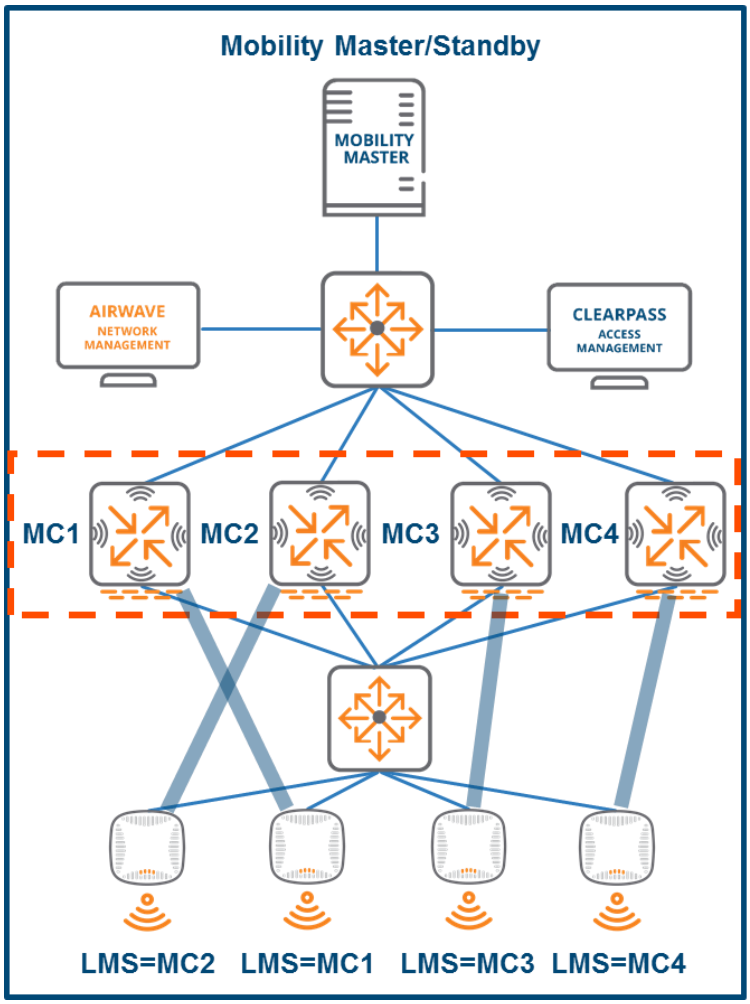


图 74 *AAC 隧道建立*

自动分配

为了对加入群集的 AP 使用自动 AAC 分配方法，必须启用群集中的 AP 负载分担选项。将执行以下步骤：

1. 如果群集成员是在第 2 层连接的，则加入群集的新 AP 利用 VRRP 实例的 VIP 联系其 AP 主控制器，如果群集成员是在第 3 层连接的，则其联系指定群集成员
2. AP 主控制器在内部检查由群集领导者分配的 AP 是否有 AAC
3. 该 AP 的 AAC 分配可用于 AP 主控制器后，其响应该 AP 的 PAPI 呼叫/握手，并在几毫秒内为其提供 AAC。
4. AP 建立了其 GRE 隧道并在其主用 AAC 上端接后，群集领导者会为其提供备用 AAC 分配
5. AP 使用其指定 S-AAC 来建立其备用隧道，从而完成该过程

NOTE

AAC 和 S-AAC 分配基于群集成员之间的现有 AP 负载分配。

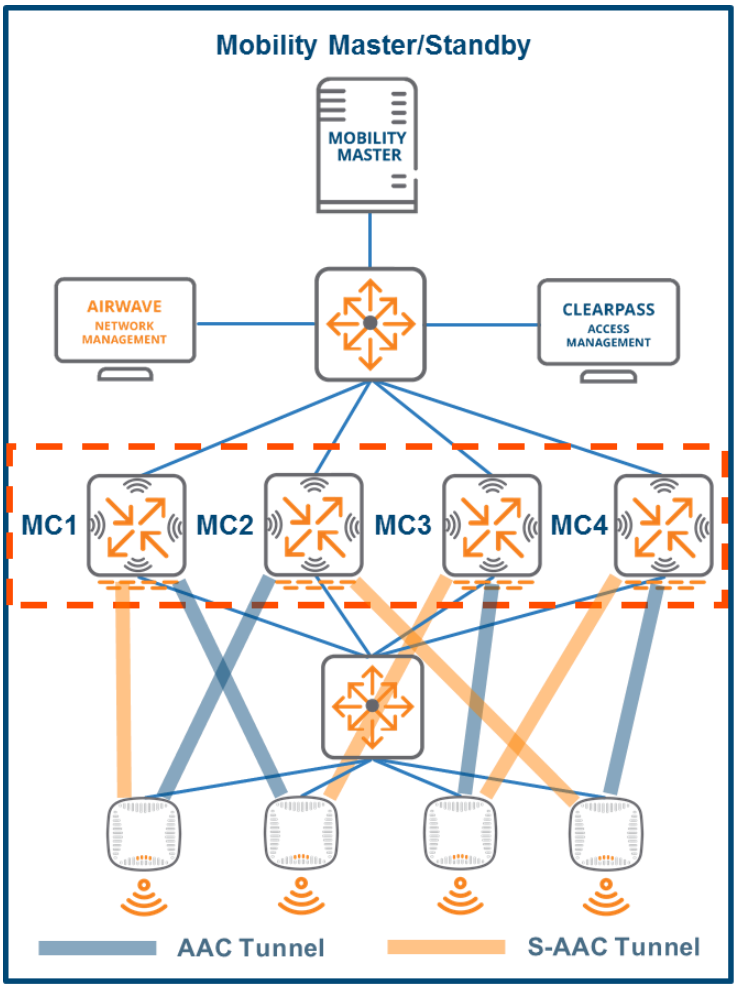


图 75 *S-AAC 隧道建立*

负载分担指标

为了解负载分担过程，熟悉与群集节点上的 AP 负载相关的各种指标及其定义至关重要：

- **AP 负载百分比** - 控制器上的 AP 数量与该控制器平台 AP 容量的比率。例如，如果 AP 容量为 1000 的控制器上有 500 个 AP，则负载为 50%。这相同的 500 个 AP 如果在 AP 容量为 2000 的控制器上，则负载为 25%
- **主用 AP 负载百分比** - 控制器上仅具有主用隧道的 AP 数量与该控制器平台容量的比率
- **总 AP 负载百分比** - 控制器上的 AP（包括具有主用和备用隧道的 AP）数量与该控制器平台容量的比率

在 ArubaOS 8.3 之前，负载分担算法使用总 AP 负载率。但在 ArubaOS 8.3 中增强了该算法，现在仅在做出负载分担决策时才考虑主用 AP 负载百分比。

负载分担算法

ArubaOS 8.3 之前的负载分担

在 8.3 之前的 ArubaOS 版本中，负载分担算法的工作方式是确定具有最高和最低总 AP 负载百分比的 MC 成员。当同时超出了两个阈值时，将进行负载分担：

- **主用 AP 重新平衡阈值**（总 AP 负载百分比）超过 50%
- **主用 AP 不平衡阈值**（具有最高和最低总 AP 百分比的控制器之间的增量）超过 5%

当该算法启动时，首先重新分配备用 AP 负载，以恢复总平衡。如果对具有备用隧道的 AP 进行负载分担不足以重新平衡群集，则重新分配主用 AP 负载，直至达到正确的平衡为止。

负载分担 ArubaOS 8.3 及更高版本

ArubaOS 8.3 中引入了一项增强功能，可指导群集领导者在制定负载分担决策时主要考虑群集成员上的主用 AP 负载百分比。8.3 之前的 ArubaOS 8 版本中使用了总 AP 负载百分比指标，其包括备用以及从 AP 到群集成员的主用隧道。

ArubaOS 8.3 及更高版本中的定期负载分担算法按照以下过程进行工作：

1. 确定具有最高和最低主用 AP 负载百分比的群集成员
2. 确定具有最高和最低总 AP 负载百分比的群集成员
3. 当同时超出了两个阈值时，将触发负载分担机制：
   - 主用 AP 重新平衡阈值（主用 AP 负载百分比）超过 50%（默认）
   - 主用 AP 不平衡阈值（具有最高和最低主用 AP 百分比的群集成员之间的增量）超过 5%
4. 从具有最高负载的群集成员将主用 AP 重新分配到具有最低负载的群集成员
5. 如果无法移动主用 AP 来恢复平衡，则从具有最高负载的群集成员将备用 AP 重新分配到具有最低负载的群集成员

负载分担阈值可配置，其使用以下额外指标加以控制：

- **主用 AP 重新平衡计时器** - 控制负载分担评估间隔
- **主用 AP 重新平衡 AP 计数** - 确定在主用 AP 重新平衡计时器已触发负载分担时将移动的 AP 数量

指标	在 ArubaOS 8.3 之前为默认	自 ArubaOS 8.3 起为默认
主用 AP 重新平衡计时器	1 分钟	5 分钟
主用 AP 重新平衡 AP 计数	10 个 AP	30 个 AP

表 13 *主用 AP 重新平衡默认值*

群集分组

ArubaOS 8 中引入了群集功能，这是一种比 ArubaOS 6 中的高可用性 AP 快速故障切换功能更强大的冗余机制。尽管 HA 配置要求配置控制器模式，例如“主用”、“备用”或“双”，但通过引入群集领导者动态选择备用 AP 锚点控制器和备用用户锚点控制器 (S-UAC) 的功能，群集实现了故障切换过程的自动化。

尽管群集提供的动态备用选择是一个强大的工具，但在生产环境中存在需要影响 S-AAC 和 S-UAC 选择的情况。以下示例说明了在以更确定的方式选择备用控制器时可能非常有利：

1. 群集中的 MC 在具有冗余电源的同一数据中心的不同机架之间分开
2. 确保在同一大型园区内的两个数据中心之间将 AAC 和 UAC 冗余分开是非常可取的做法

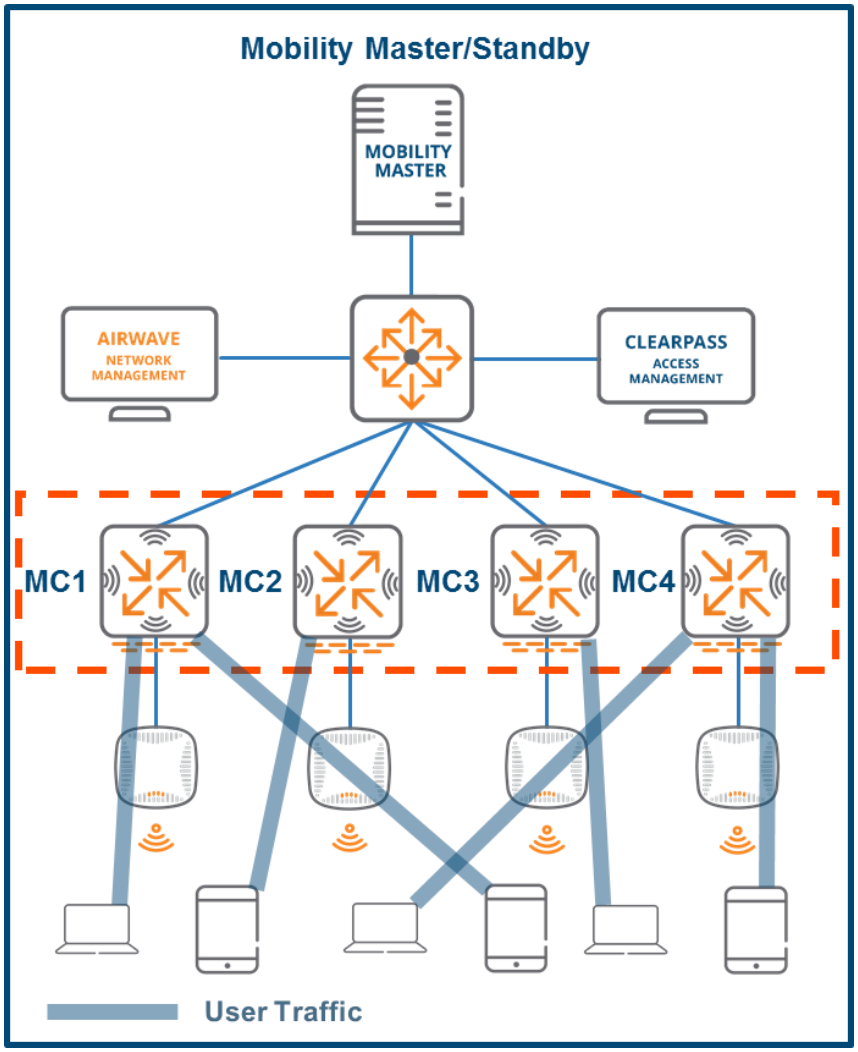


图 76 *典型 ArubaOS 8 群集架构*

为满足此需求，Aruba 创建了分组选项，用于将群集中的 MC 分为 2 个或更多组。当群集领导者正在为 AP 或用户选择备用控制器时，其将优先选择属于与主用控制器不同的组的控制器。

在以下示例中，MC1 和 MC2 在组 1 中进行配置，而 MC3 和 MC4 在组 2 中进行配置。如果 AP 将 MC1 作为其 AAC，则群集领导者将选择组 2 中的 MC3 或 MC4 作为该 AP 的 S-AAC。此选择标准适用于在组 2 的一个 MC 上进行端接的 AP；将选择 MC1 或 MC2 作为其 S-AAC。

在使用组时，对于备用用户锚点控制器 (S-UAC)，群集领导者遵循与 S-AAC 相同的选择过程。

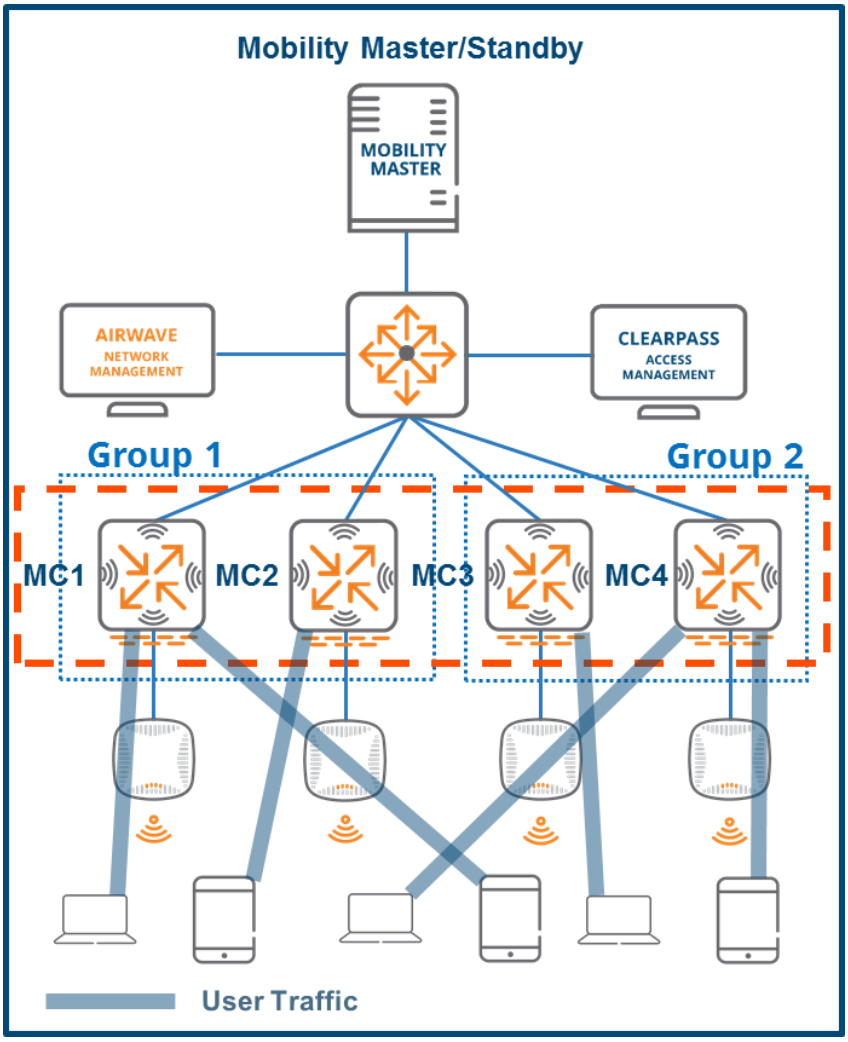


图 77 *ArubaOS 8 中的群集组*

NOTE

分组功能对 AAC 或 UAC 选择没有影响。应始终在组之间平分群集成员。

AP 节点列表

AP *节点列表*是每个 AP 维护的各群集成员 IP 地址的存储库。连接到群集后，AP 将获知所有群集成员的 IP 地址。然后这些地址被存储为 AP 的节点列表并另存为环境变量。启动后，AP 将联系其节点列表中的第一个 IP 地址。如果没有收到响应，其将尝试联系该列表中的下一个 IP 地址，以确保 AP 始终能够在群集中找到可访问的控制器。

授权变更

授权变更 (CoA) 功能可扩展远程身份验证拨入用户服务 (RADIUS) 协议的功能，其在 RFC 5176 中进行了定义。CoA 请求消息通常由 RADIUS 服务器发送到网络接入服务器 (NAS) 设备，以便对现有会话的授权属性进行动态修改。如果 NAS 设备能够成功对用户会话实施所请求的授权变更，则其将使用 CoA 确认（也称为 CoA-ACK）来响应 RADIUS 服务器。相反，如果该变更不成功，则 NAS 将使用 CoA 否定确认或 CoA-NAK 来进行响应。

在 ArubaOS 8 群集环境中，对于具有正在进行的活动会话的用户，主动提出的 CoA 请求被发送到该用户的锚点控制器。然后，在成功实施该更改后，UAC 向 RADIUS 服务器返回确认，或者如果此实施不成功，则返回 NAK。但由于 MC 故障或用户负载分担事件等原因，在正常群集操作过程中用户的 UAC 可能发生变更。这种情况将导致 CoA 请求被丢弃，因为目标用户将不再关联到从 RADIUS 服务器接收请求的 MC。为防止出现此类情况，Aruba 已实施了群集冗余功能。

群集 CoA 支持

Aruba 为 ArubaOS 8 中的 MC 群集提供 CoA 支持所使用的主要机制是 VRRP。在每个群集中，节点有多少，VRRP 实例就有多少，并且每个 MC 均作为实例的主控制器。例如，具有 5 个 MC 的群集将具有 5 个 VRRP 实例和 5 个虚拟 IP 地址 (VIP)。主 MC 接收针对其实例的 VIP 的消息，而群集中的其余 MC 是其他所有实例的备份，在这些实例中，它们不是主控制器。此配置可确保每个群集均受容错和完全冗余设计的保护。

该部分描述对 RFC-5176 中所述的 RADIUS 进行动态授权的过程，以及 RADIUS 如何与群集中的 Aruba 控制器通信。选择了授权变更过程来表示该通信顺序。

ArubaOS 预留了 220-255 范围内的 VRRP 实例 ID。当每个实例的主控制器向 RADIUS 服务器发送 RADIUS 请求时，该主控制器默认将其实例的 VIP 注入到作为 NAS-IP 的消息中。这可确保始终正确转发来自 RADIUS 服务器的 CoA 请求，无论哪个 MC 是该实例的活动主控制器。即，RADIUS 服务器将 CoA 请求发送到 VRRP 实例的当前主控制器，而不是单独站点。从服务器的角度讲，其正在将此请求发送到该实例的 VIP 地址的当前持有者。下图描绘了将在 CoA 部分的持续时间内使用的示例架构：

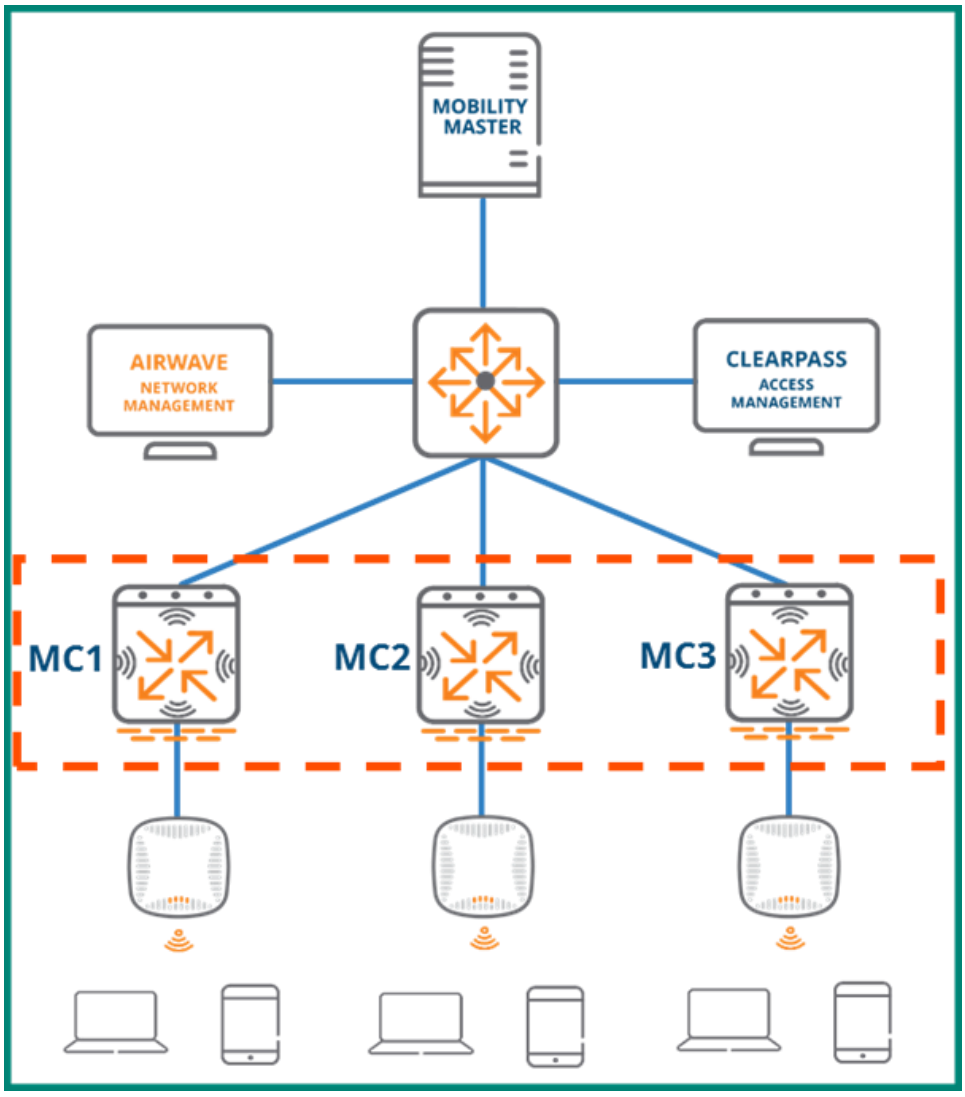


图 78 *用于 CoA 演示的示例架构*

此示例网络由具有三个 VRRP 实例的三节点群集组成。AOS 分配的 VRRP ID 范围介于 220 与 255 之间，因此为该群集中的三个实例分配的 VRRP ID 为 220、221 和 222。动态分配每个实例中 MC 的优先级，以便为实例的主控制器分配优先级 255，为第一个备份分配优先级 235，为第二个备份分配优先级 215。下表概述了示例网络中每个 MC 和每个实例的优先级分配：

VRRP 实例	虚拟 IP	MC1 优先级	MC2 优先级	MC3 优先级
ID 220	VIP1	**255**	235	215
ID 221	VIP2	215	**255**	235
ID 222	VIP3	235	215	**255**

表 14 *每个 VRRP 实例的 MC 优先级和 VIP*

如该表所示，优先级为 255 的 MC1 是实例 220 的主控制器，优先级为 235 的 MC2 是第一个备份，优先级为 215 的 MC3 是第二个备份。同样，MC2 是实例 221 的主控制器，因为其优先级最高，为 255，优先级为 235 的 MC3 是第一个备份，优先级为 215 的 MC1 是第二个备份。实例 222 遵循与实例 220 和 221 相同的模式。

MC 出现故障时的 CoA

如果网络没有相应的容错级别，则群集节点的故障是可能对 CoA 操作产生不利影响的事件。如果用户的锚点控制器出现故障，则 RADIUS 服务器会照常将 CoA 请求推送到其 UAC，同时假设其将执行此变更并使用 ACK 进行响应。但如果尚未实施 VRRP 等冗余机制，则该请求将不会得到应答，并且不会实现成功变更。在这种情况下，与故障节点关联的用户将照常故障切换到其备用 UAC。但 UAC 不会收到来自 RADIUS 服务器的变更请求，因为该服务器不知道群集操作。必须为每个节点实施 VRRP 实例，以防止出现此类情况，以及保持群集中的 CoA 操作。

在下图中，MC1 为实例 220 的主控制器，MC2 作为第一备份，MC3 作为第二备份。与 MC1 关联的客户端已使用 802.1X 进行了完全身份验证，MC3 作为该客户端的备用 UAC。当与 ClearPass 相对应时，MC1 自动插入实例 220 的 VIP，以作为 NAS-IP。从 ClearPass 的角度讲，其正在将 CoA 请求发送到实例 220 的当前主控制器。

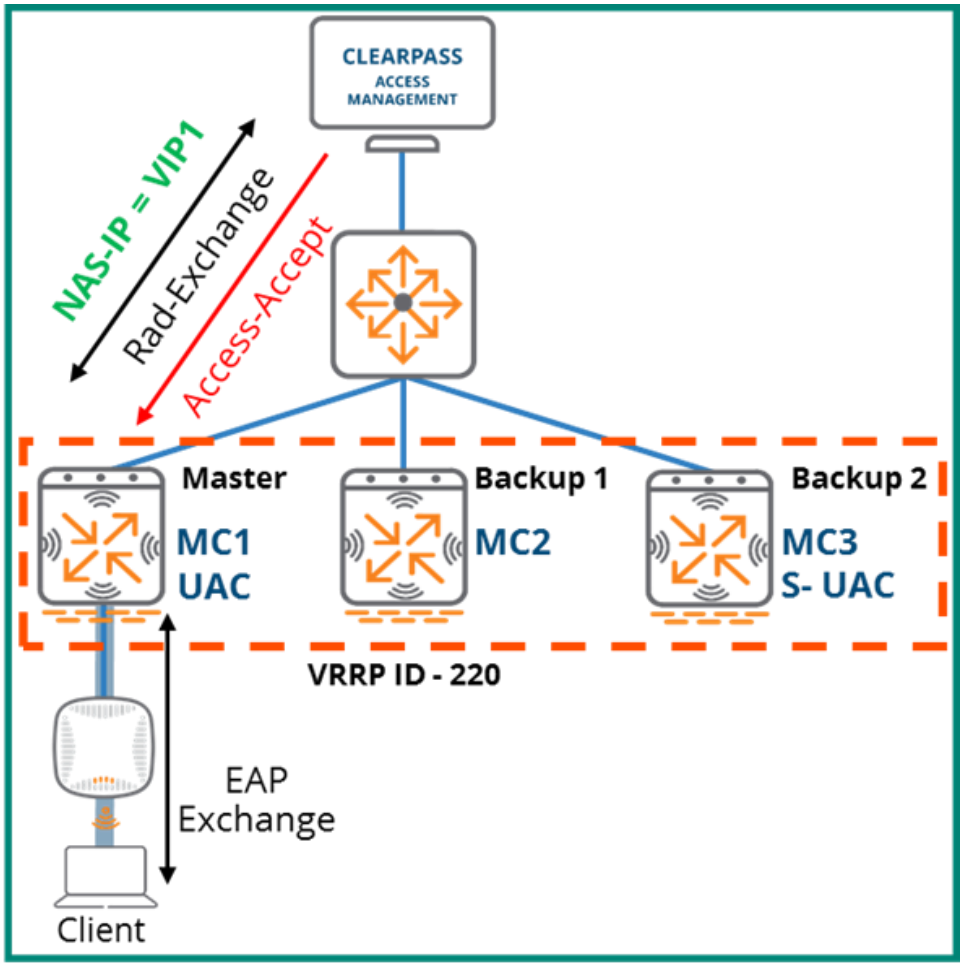


图 79 *用户对照 ClearPass 进行身份验证*

如果在客户端处于会话中时 MC1 出现故障，则关联该客户端所在的 AP 将故障切换到 MC2。该客户端的会话将转移到 MC3，因为这是备用 UAC。然后 MC3 承担该客户端的 UAC 角色。由于 MC2 在实例 220 中具有比 MC3 更高的优先级，因此其将承担主控制器的角色并获得 VIP 的所有权。

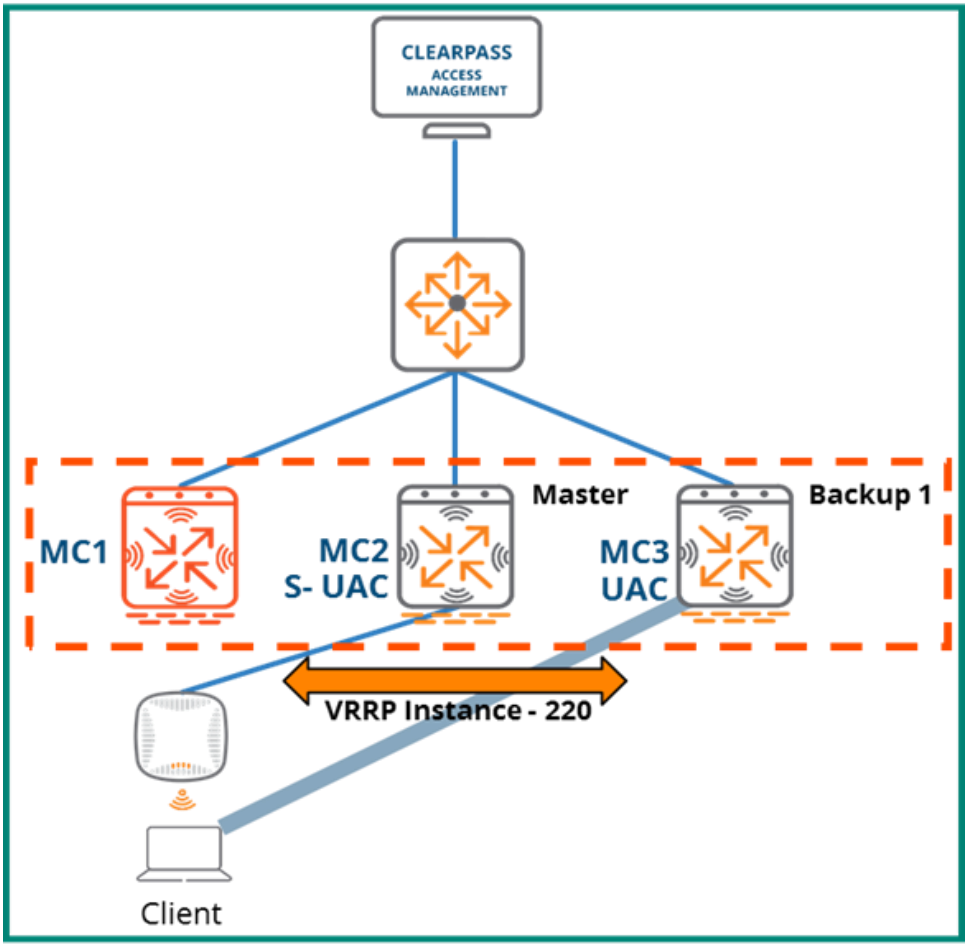


图 80 *MC1 故障*

ClearPass 为客户端发送的任何 CoA 请求将被发送到实例 220 的 VIP。从 ClearPass 角度讲，在该示例中，对于计划向该客户端发送的任何 CoA 请求，实例 220 的 VIP 均为正确地址。由于 MC1 已出现故障，MC2 现在是 VRRP 实例 200 的主控制器，并且拥有其虚拟 IP。当 ClearPass 向该客户端发送 CoA 请求时，MC2 将接收该请求，然后将其转发到群集中的所有节点。由于我们的群集只有三个节点，因此在这种情况下，MC2 将该请求转发到 MC3。

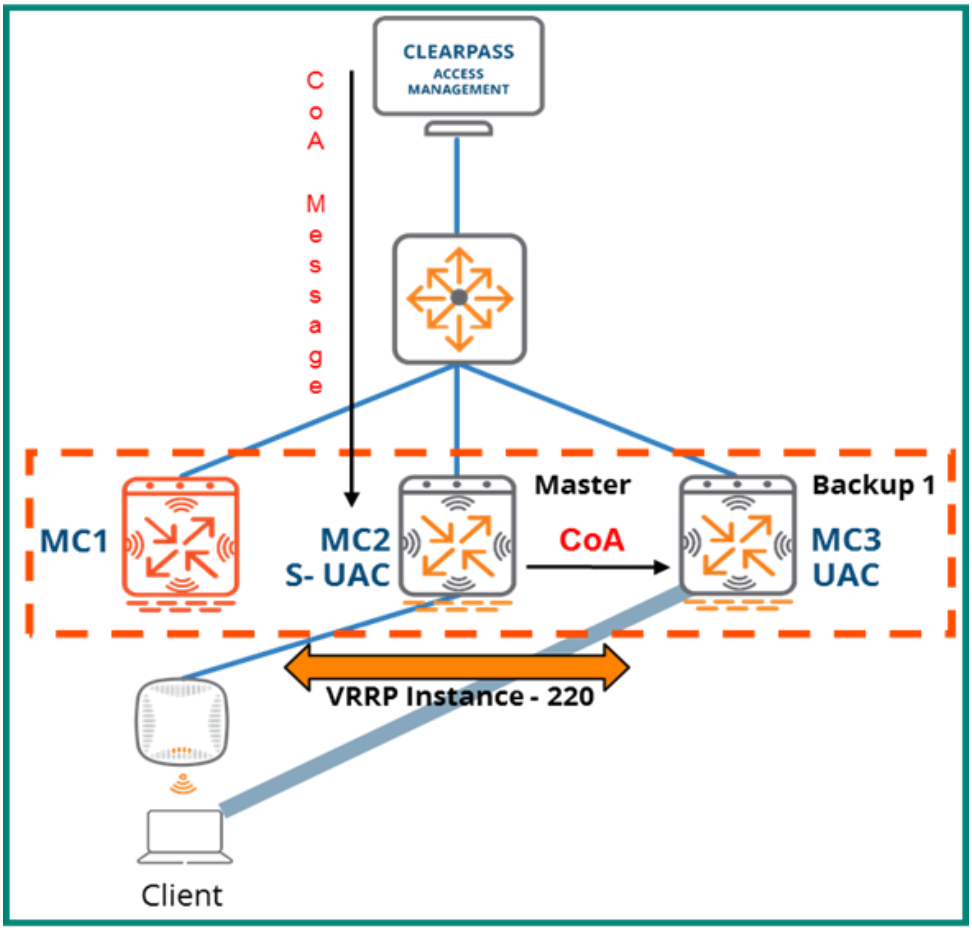


图 81 *转发到 MC3 的 CoA 消息*

在已成功实施 CoA 请求的更改后，MC3 将把 CoRe-ACK 发送会 ClearPass。

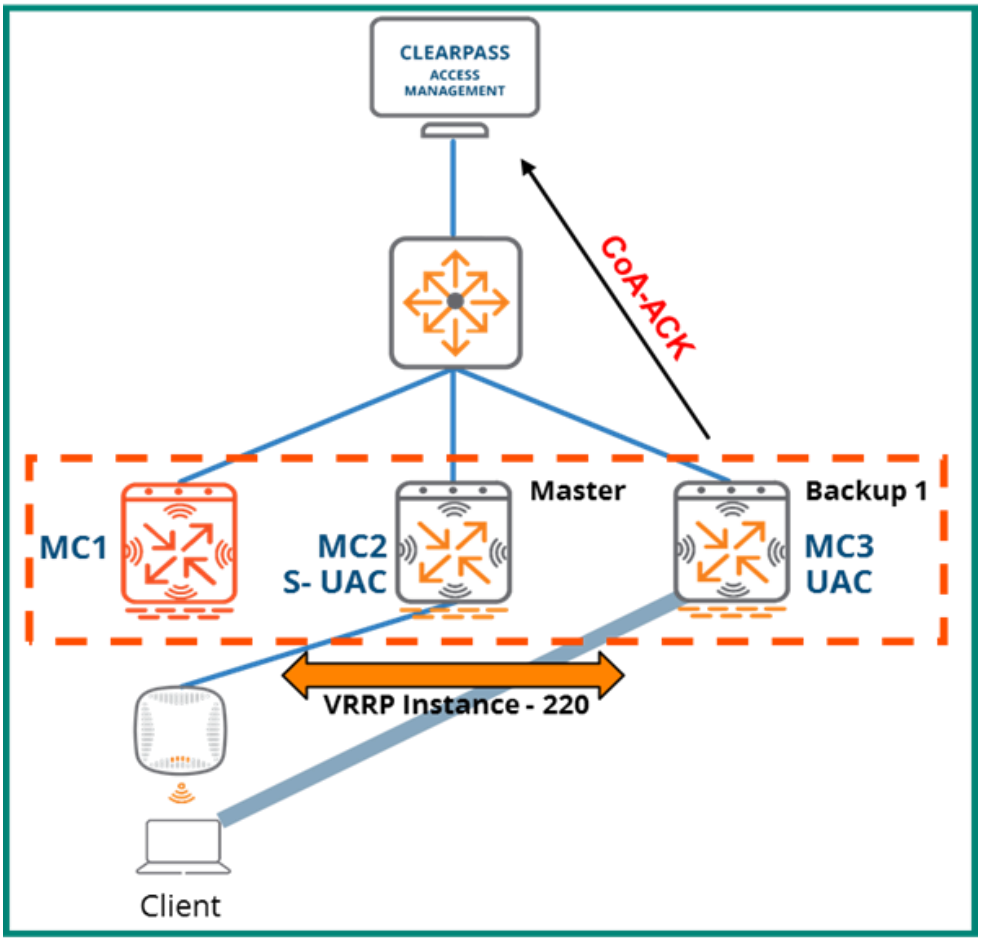


图 82 *转发到 MC 的 CoA 消息*

具有负载分担的 CoA

尽管不像设备故障那样严重，但如果尚未实施适当的设计，群集内的负载分担事件可能给 CoA 操作带来挑战。为演示可防止负载分担事件阻止 CoA 功能的 Aruba 解决方案，将使用相同架构作为 MC 故障示例。该示例将模拟与 MC1 关联的客户端仍在会话中时其被负载分担到 MC3 的事件。

MC1 可运行，是 VRRP 实例 220 的主控制以及 VIP 的所有者。与先前示例一样，MC1 在 RADIUS 请求中插入了 VIP1，以作为 NAS-IP，该请求启动了客户端身份认证，因此 ClearPass 将把针对该客户端的任何 CoA 请求均发送到 VRRP 实例 220 的 VIP 地址。

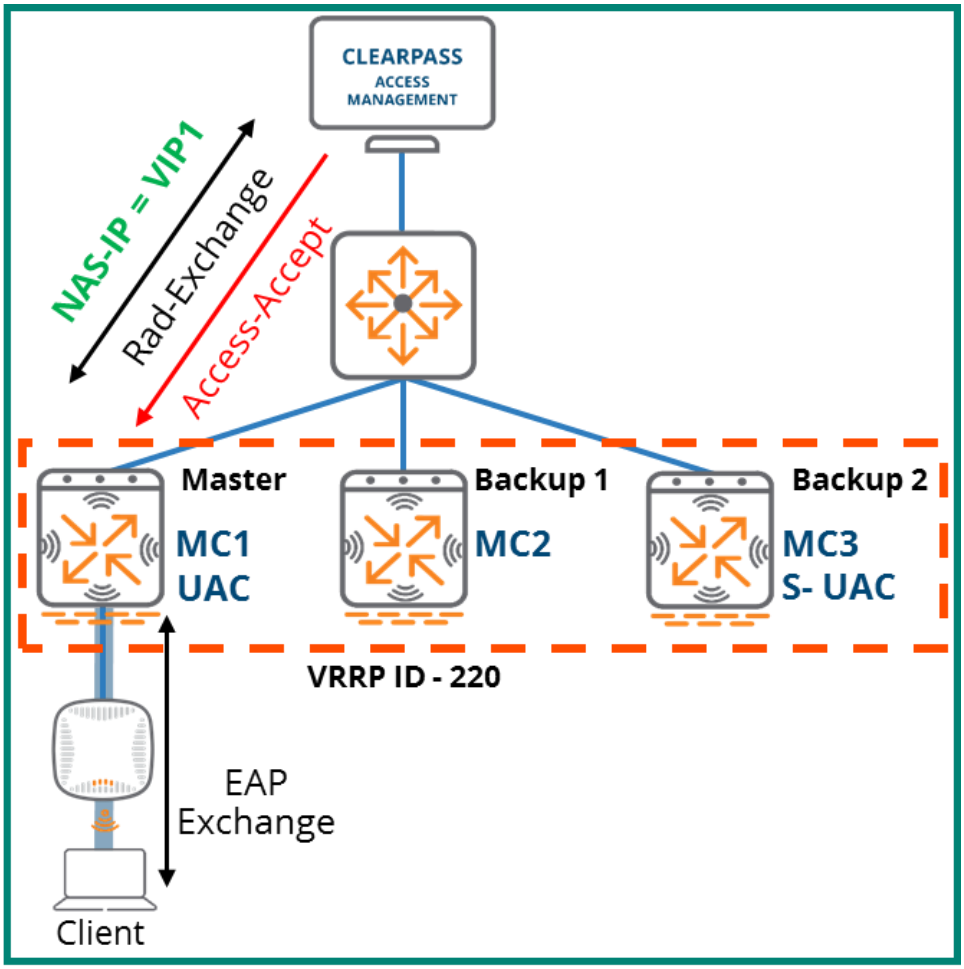


图 83 *客户端对照 ClearPass 进行身份验证*

下一步将该客户端负载分担到成为其 UAC 的 MC3。MC1 成为该客户端的 S-UAC，但仍为 VRRP 实例 220 的主控制器。

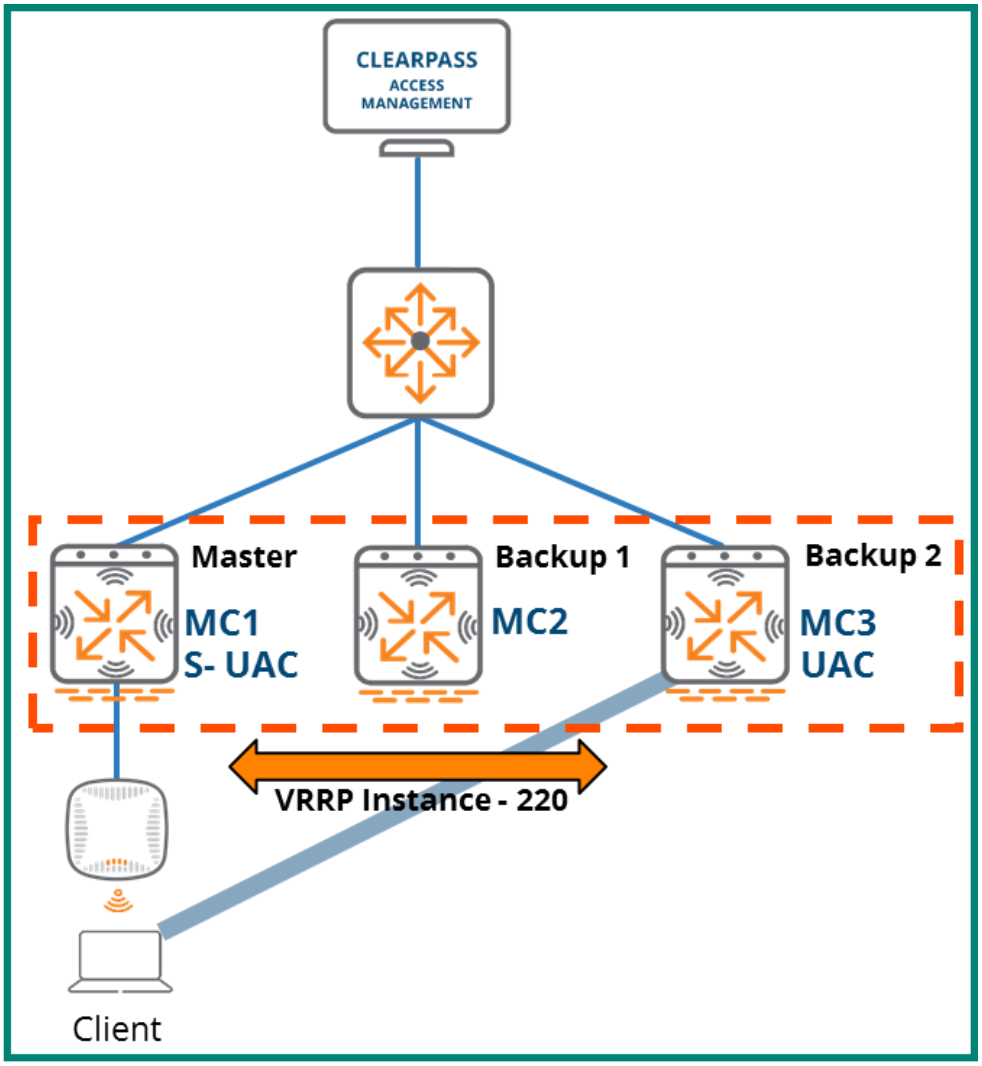


图 84 *客户端 UAC 更改*

ClearPass 向 VRRP ID 220 的 VIP 的所有者发送 CoA 消息：

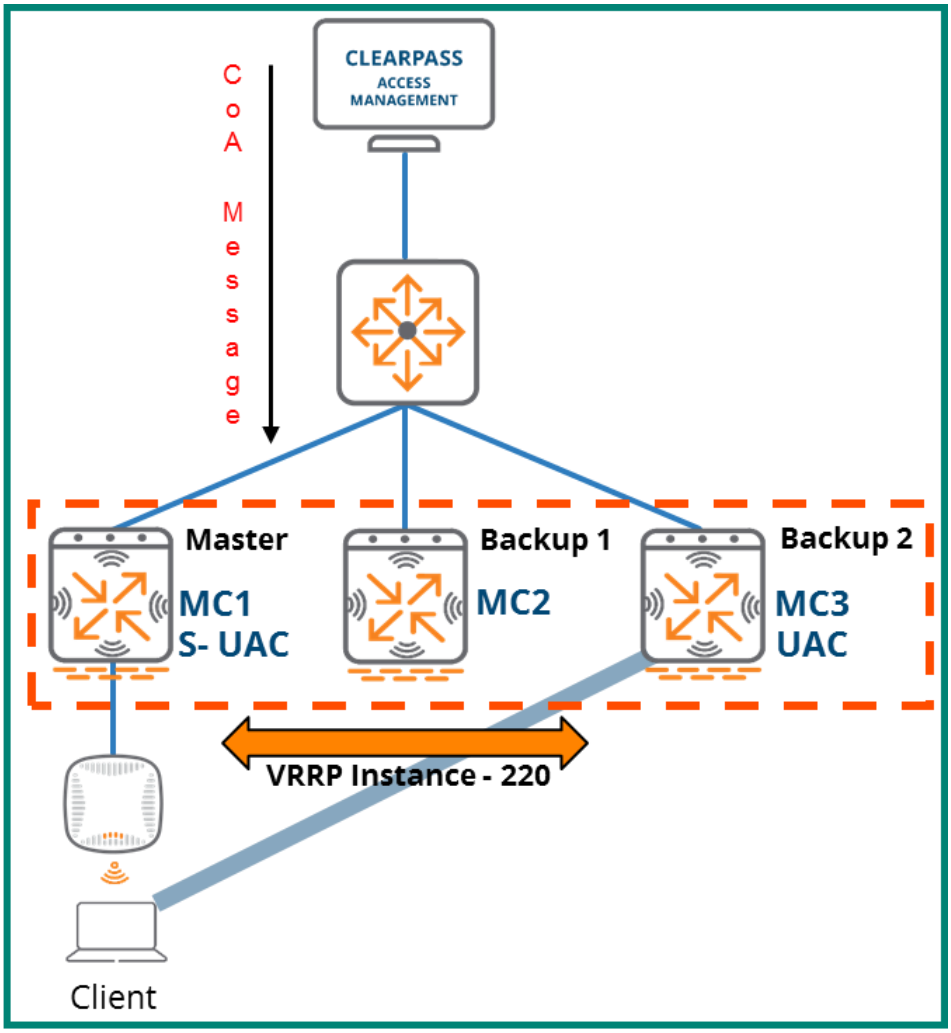


图 85 *发送到 VIP1 的 CoA 消息*

MC1 接收 CoA 请求，因为其为 VRRP 实例的主控制器。然后其将该请求单播到其他群集成员。

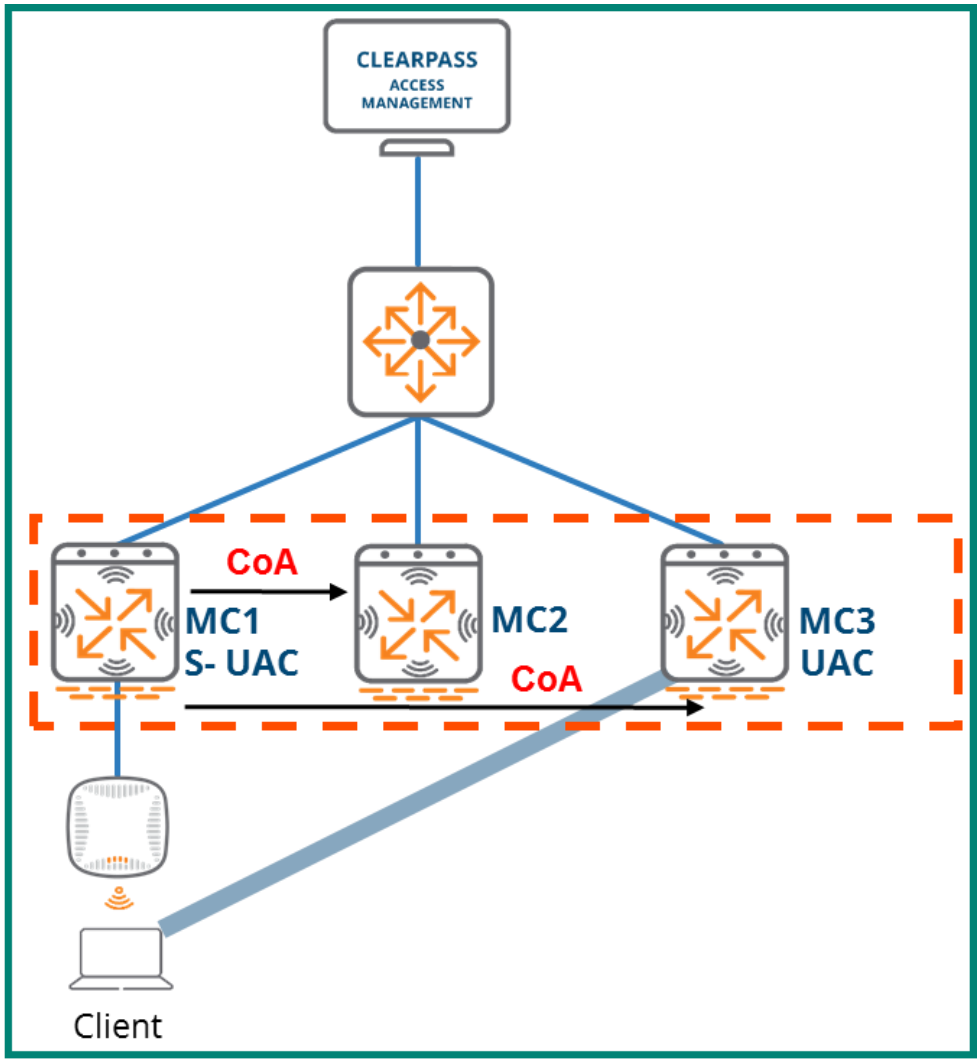


图 86 *MC1 转发请求*

MC3 收到从 MC1 转发的 CoA 请求并成功实施更改后，它将使用 CoA-ACK 响应 ClearPass。实施此更改的 UAC 始终是负责将 CoA-ACK 或 CoA-NAK 返回到 ClearPass 的 MC。

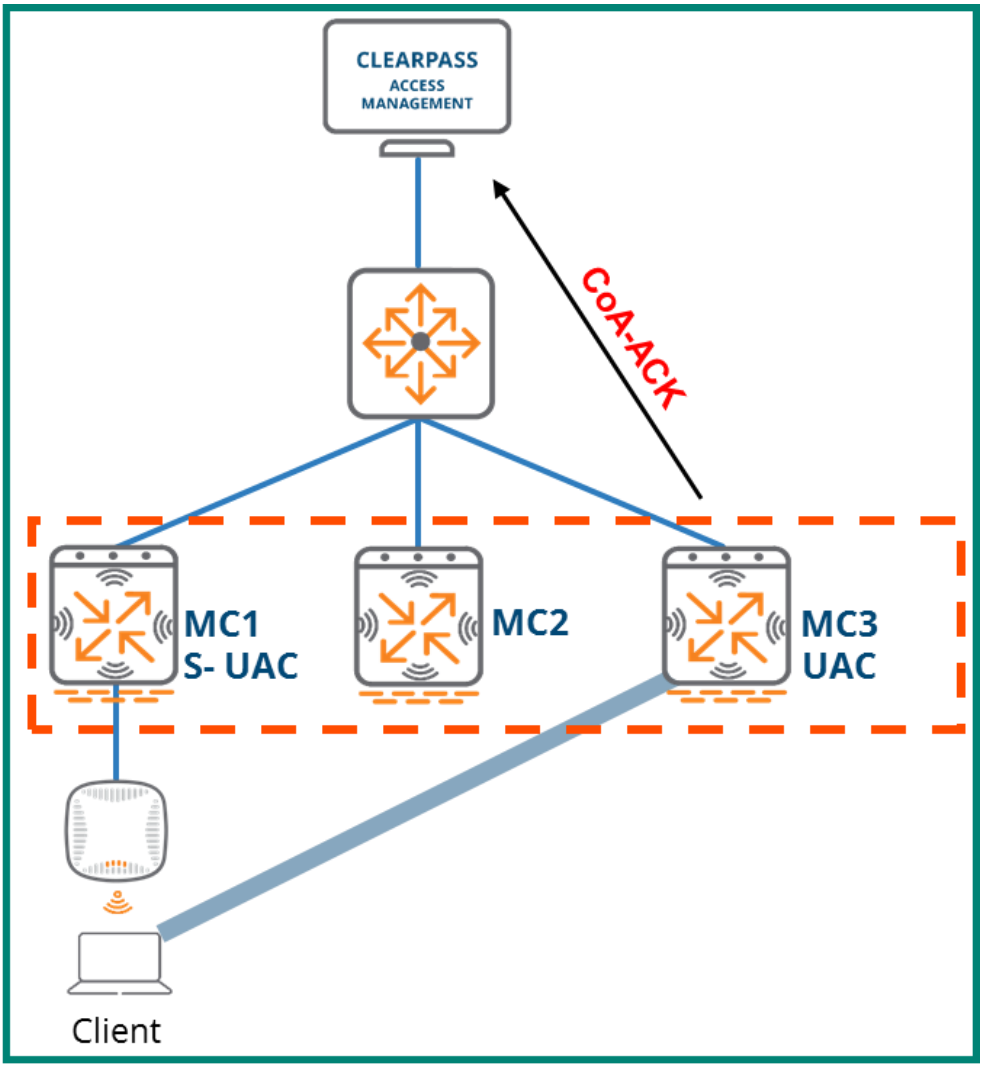


图 87 *MC3 将 CoA-ACK 返回到 ClearPass*

实时升级

实时升级功能可使群集中的 MC 和 AP 自动将其软件升级到更高的 ArubaOS 版本。群集中的 MC 可无缝升级，不会对客户端连接和性能产生任何不利影响。以下几点概述了实时升级的主要详情：

- 无缝的服务中群集升级
- 无人工干预，对 RF 的影响最小
- 自 ArubaOS 8.1 起提供此功能
- 适用于 MM 环境中的群集

先决条件

为启用实时升级功能，同时将 RF 影响和客户端中断降至最低，需要以下 ArubaOS 功能：

- 在启用了冗余时通过“L2 已连接”群集进行的有状态故障切换
- 集中式图像升级
- AirMatch（已启用计划）

NOTE

有关如何配置上列先决条件的其他信息，请参阅 ArubaOS 8 用户指南。

为获得积极结果，应始终遵循有关 AP 部署和 RF 覆盖范围的 Aruba 最佳实践，但在执行实时升级时，它们是防止客户端失去连接的必要条件。应在基于容量的设计中部署 AP，以保证重叠 RF 覆盖范围。这样可确保在升级过程中，客户端将始终能够在先前将它们关联到的 AP 需要重新启动时漫游到其他 AP。至少应设计一个部署，以便客户端无论在哪里漫游都能够看到两个 AP。

CAUTION

在没有足够覆盖范围的区域中，如果在实时升级过程中将客户端连接到的 AP 重新启动，则在重新启动完成并且该 AP 恢复运行前，它们将失去连接。

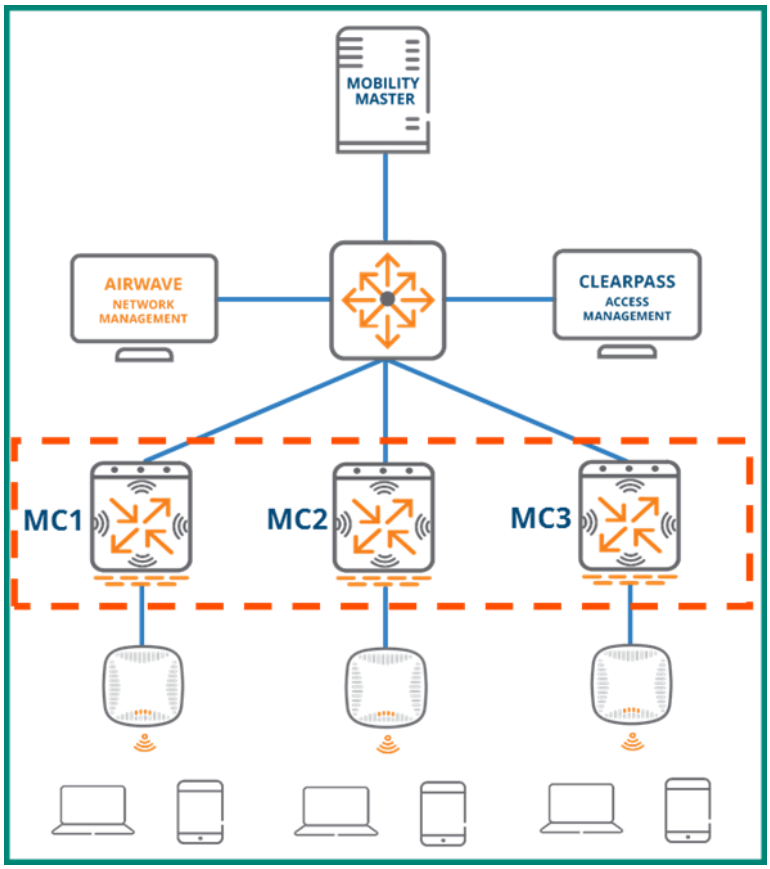


图 88 *参考实时升级架构*

实时升级流程

实时升级过程涉及多个步骤，旨在确保正确应用升级，以及在整个持续时间内继续为客户端服务。升级过程所需的高级步骤如下所示，在后续章节中将详细介绍每个步骤：

1. **AP 分区** - 在群集中端接的 AP 根据各自 RF 信道被逻辑分组到多个分区中
2. **目标控制器分配** - 每个 AP 分区均被分配了群集中的一个 MC，此 MC 作为该分区中 AP 的升级后端接目标。所有群集成员均作为 AP 分区目标，有一个除外
3. **推送到 MC 的新固件 -** 所有群集成员均使用预先配置的升级配置文件，通过集中式映像升级功能下载新的 ArubaOS 固件
4. **群集成员升级** - 实际升级过程首先将一个群集成员重新引导至新固件。接受升级的第一个控制器在加载了其新固件重新启动后，以该控制器为目标的分区中的 AP 将被预加载新固件。这些 AP 一次重新启动一个分区，然后在它们升级后的目标控制器上启动

在为第一个目标控制器重新启动了所有 AP 后，重新启动群集中的第二个控制器，然后按照上述相同方式重新启动以该控制器为目标的 AP 分区。

升级了所有 AP 并在它们升级后的目标控制器上对它们进行了端接后，已不再作为目标的最后一个控制器将重新启动并加入升级群集。

初始实验 AP 分配

下图描绘了在本节期间将用于演示实时升级功能的关键概念的方案。所选架构为标准 ArubaOS 8 设计，由部署在虚拟设备上的完全冗余 MM 对组成。该方案在单个群集中有三个 MC，这些 MC 已在“L2 已连接”状态下进行了配置，并且已按照先决条件所指定的那样在它们之间启用了完全冗余。七个 AP 连接到了三个 MC，这些 AP 在各种不同的信道上运行。

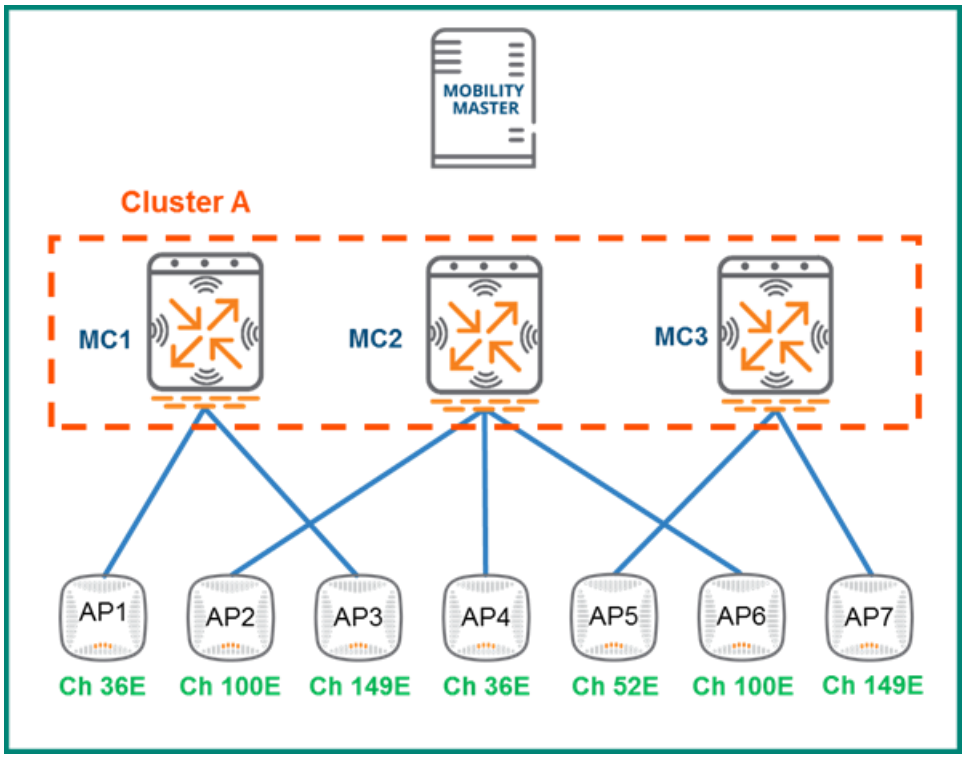


图 89 *实时升级的示例网络*

NOTE

为演示实时升级操作，已严格地随机选择了 AP 的信道分配。它们不代表生产网络中信道分配的最佳实践建议。

AP 分区

当群集的升级管理器将有关连接到群集的所有 AP 的信息发送到 AirMatch 时，实时升级过程开始。这就是为什么先决条件是在执行实时升级时使启用 AirMatch 计划的这一默认设置保持完整的原因。从升级管理器收到 AP 信息后，AirMatch 会将 AP 隔离到逻辑组中，并使用分区到 AP 映射分配来更新升级管理器。

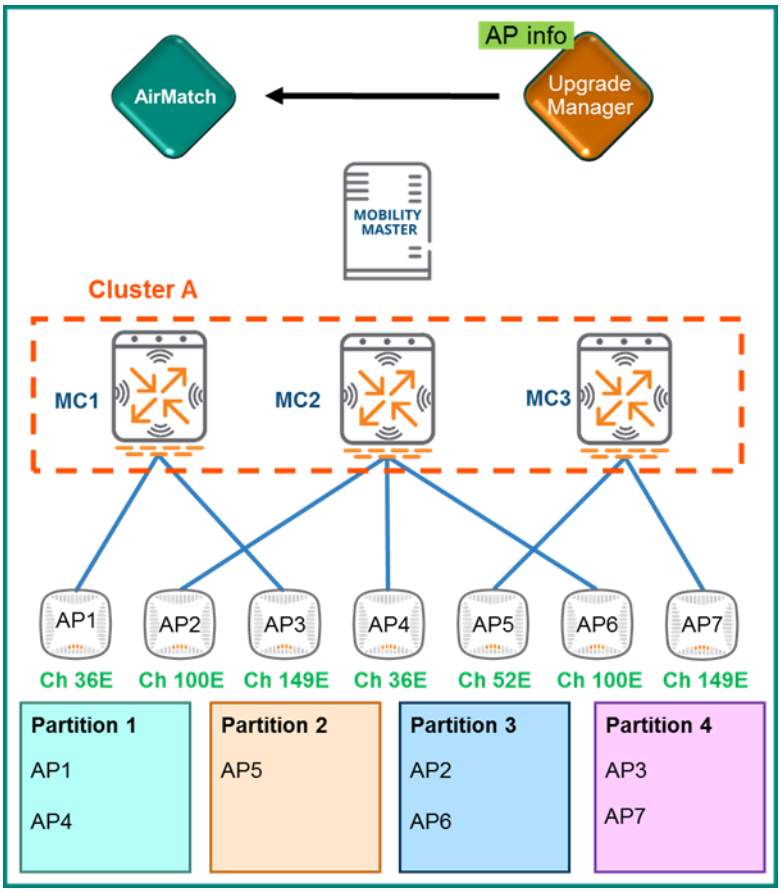


图 90 *AP 分区*

目标分配和固件下载

在 AirMatch 根据所有 AP 的信息对这些 AP 进行了逻辑分区，并且已使用这些分配更新了升级管理器后，每个分区都将被分配一个“目标”MC。此目标代表在这些 AP 利用新固件重新启动后管理它们每个分区的 MC。如下图所示，已为分区 1、2 和 3 中的 AP 分配了 MC3 作为它们的目标，而分区 4 中的 AP 已被分配了 MC1：

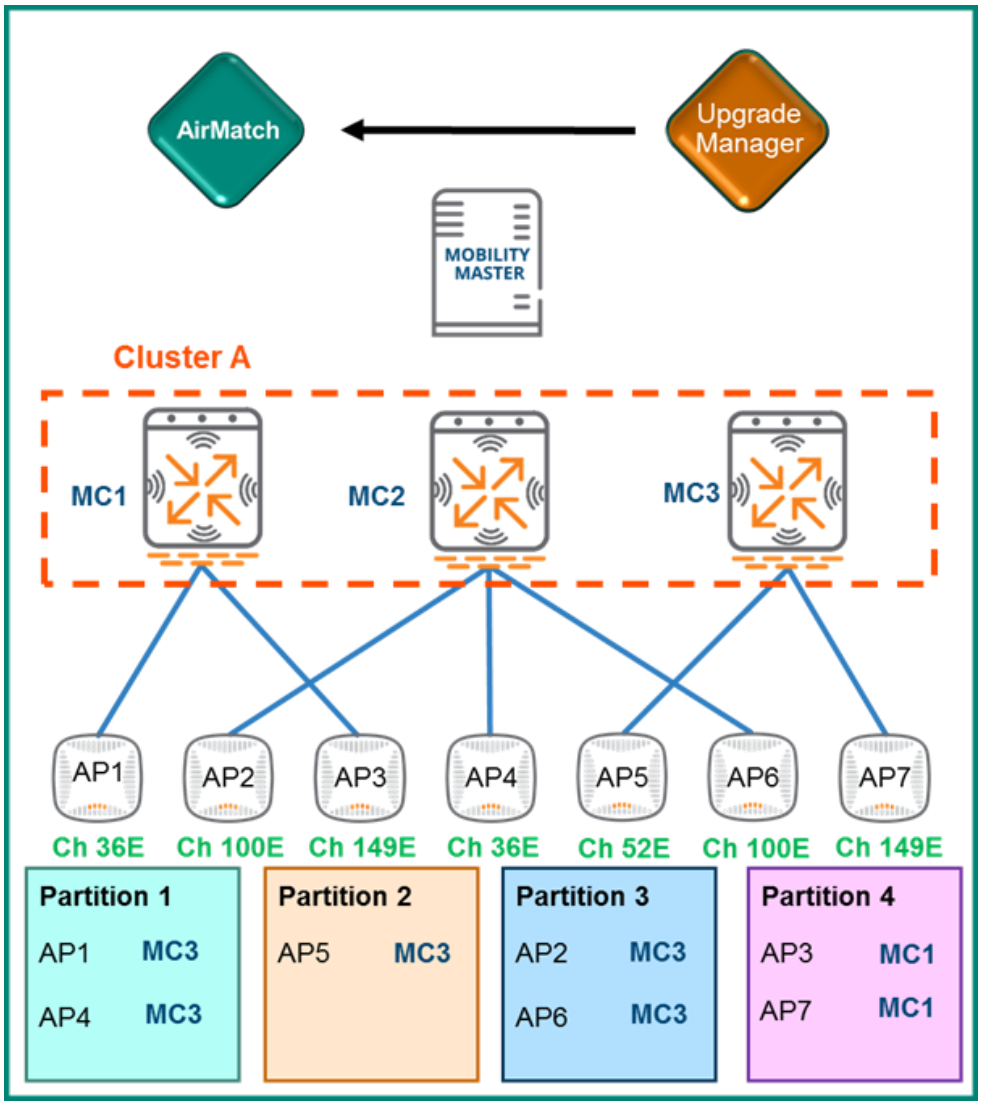


图 91 *目标分配*

NOTE

MC2 尚未被指定为任何分区或 AP 的目标。其被故意排除，原因将在以下章节中讨论。

所有分区都有各自的目标分配后，MC 将一次下载一个新的 ArubaOS 固件。在进行各自下载的同时，它们将继续正常运行。

群集成员升级

已对所有 AP 均进行了分区，为它们分配了目标 MC，并且 MC 已预先下载了它们的新固件后，它们准备开始实际的升级过程。该示例群集有三个成员，但无论群集中有多少个 MC，该过程都将相同。每个群集成员逐个重新启动，未被指定为任何 AP 的目标的最后一个群集成员最后一个重新启动。

第一个成员升级

在 MC3 重新启动时，升级过程开始，这样其预先下载的固件升级便可生效。在重新启动过程中，MC3 将关闭并且无法继续作为 AP 5 和 7 的 AAC，因此它们将需要分别故障切换到 MC1 和 MC2。同样，已分配了 MC3 作为 UAC 的任何客户端都将需要故障切换到 MC1 和 MC2。

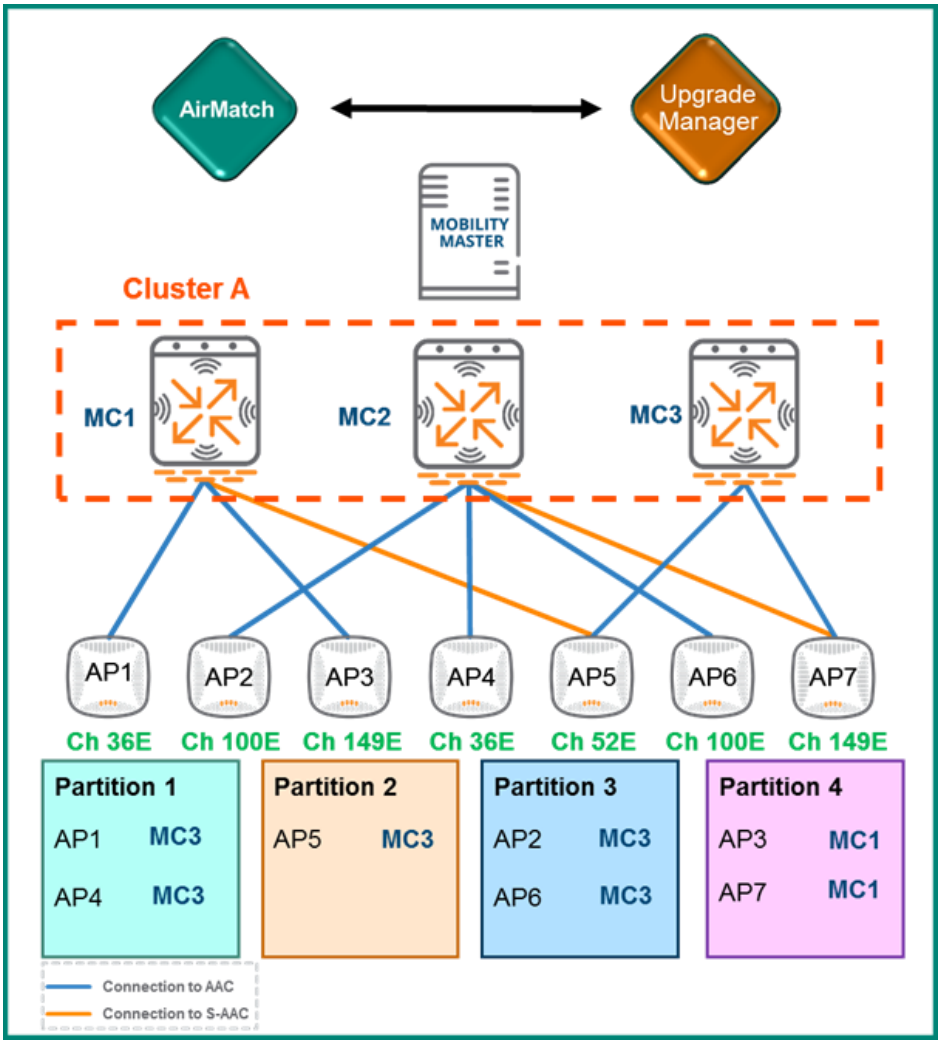


图 92 *MC3 开始重新启动，并且 AP 和客户端进行故障切换*

在 MC3 完成重新启动并重新联机运行其新固件后，其将形成一个单独群集，因为同一群集中的 MC 必须运行相同的固件版本。下图以绿色边框表示 MC3 已形成的新群集，该群集称为群集 B。此时，MC1 和 MC2 以及所有关联的 AP 和客户端仍在运行先前固件版本的群集 A 中。

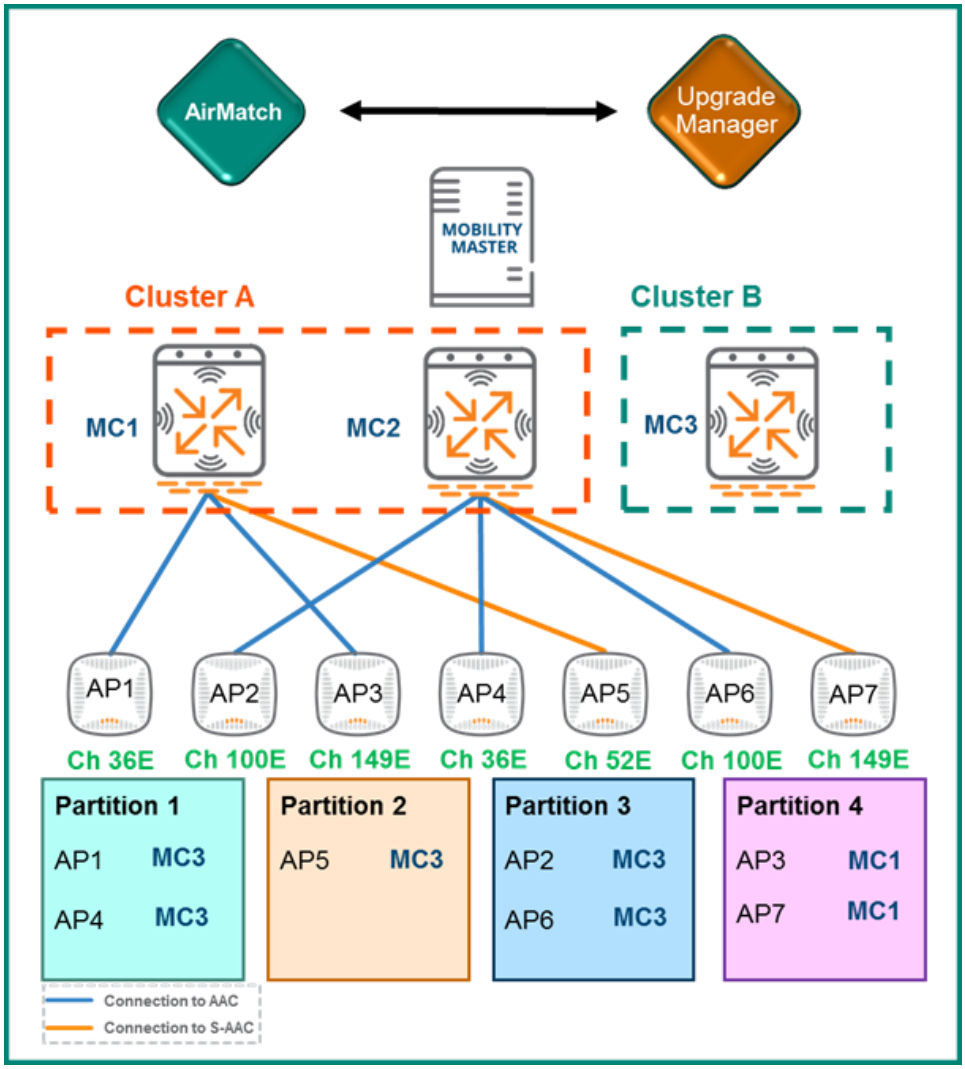


图 93 *MC3 重新启动*

MC3 重新联机后，对于已分配了 MC3 作为目标 MC 的 AP，MC3 将作为这些 AP 的 AAC 运行。这些 AP 将首先预加载它们的新固件，然后重新启动。将一次重新启动一个分区，以确保不会剥夺客户端用于保持连接的 AP 选项。如果所有 AP 都将立即重新启动，ARM 的覆盖空洞检测机制将无法充分补偿所有间隙。这可能导致客户端被迫离开网络，直到 AP 完成重新启动为止。与重新启动 AP 相关联的客户端将漫游到与红色群集 A 相连的 AP。这些客户端将仅需要完成 4 路 802.1X 握手，而不是完整的身份验证过程，因为它们将保留其 UAC 并且其已经是该群集的成员。

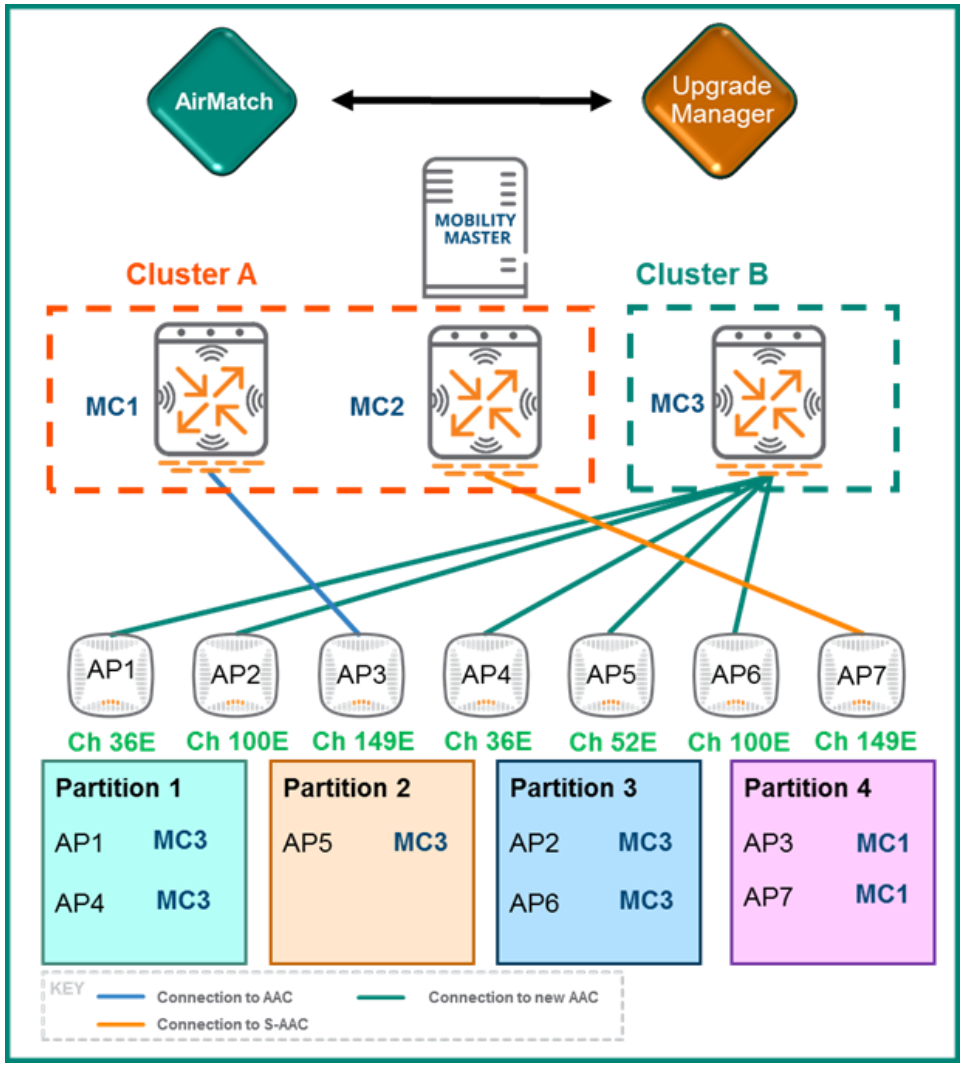


图 94 *AP 1-2 和 4-6 连接到群集 B*

第二个成员升级

现在 MC3 使用其新固件运行，并且其指定的 AP 已重新启动，MC1 能够使用相同过程开始升级。MC1 将重新启动，并且使群集 A 将 MC2 作为原始群集的最后一个成员。MC1 重新启动后，作为 AAC 的任何 AP 都将故障切换到它们的 S-AAC (MC2)，并且任何客户端都将故障切换到它们的 S-UAC（也为 MC2）。在我们的示例中，这意味着 AP3 将与 UAC 为 MC1 的任何客户端一起故障切换到 MC2。

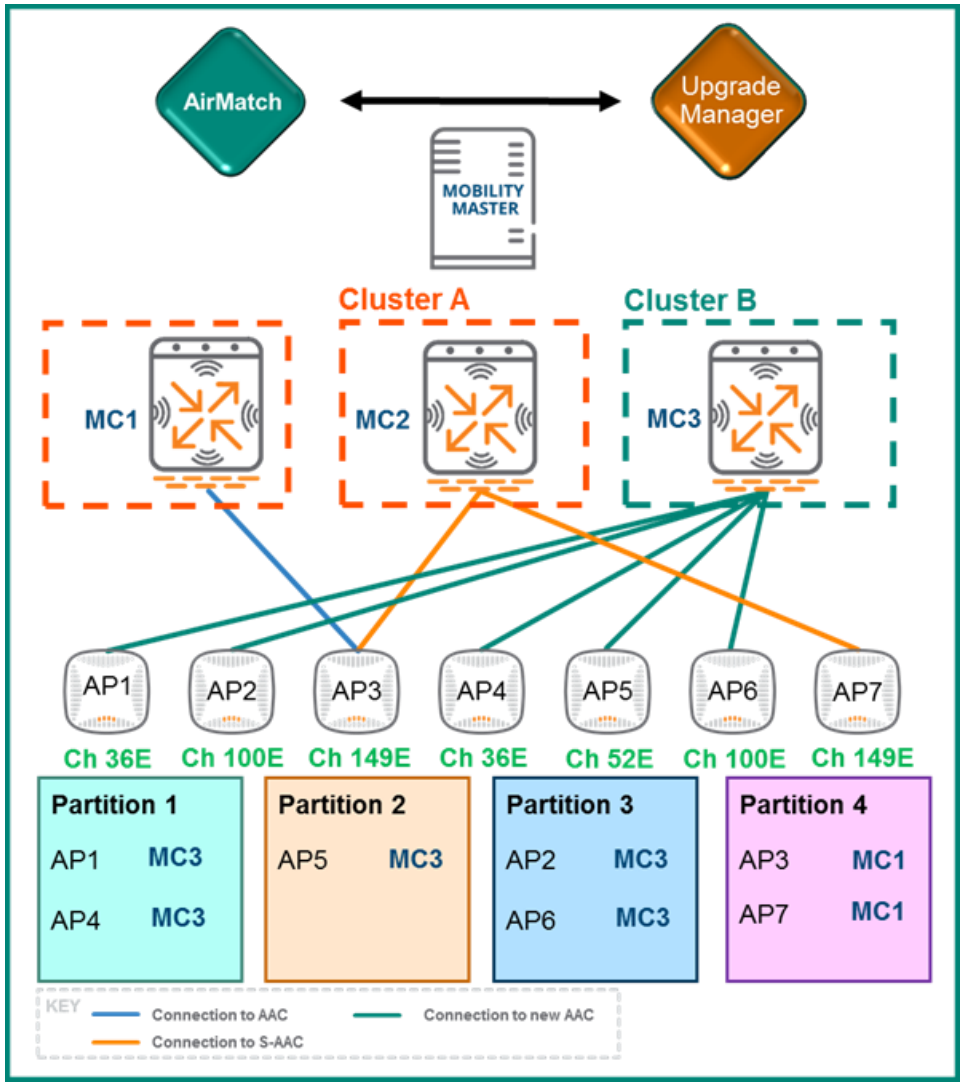


图 95 *MC1 重新启动时，AP 和客户端故障切换到 MC2*

MC1 重新联机后，其将立即加入群集 B 中的 MC3。分区 4 中的 AP3 和 AP7 被分配了 MC1 作为它们的目标，并且将预先下载新固件，以便它们能够重新启动并加入新群集。已预先下载了固件后，这些 AP 会重新启动，从而导致其关联的客户端立即漫游到与绿色群集 B 相连的 AP。即使先前将这些客户端连接到了 MC1 和 MC3，从客户端的角度讲，这些控制器也被视为新设备，因为它们升级了固件并形成了新的群集。这将要求任何 802.1X 客户端都进行完全授权过程，就像它们在关联到新设备时那样。AP3 和 AP7 在使用新固件重新启动后，它们将连接到作为它们 AAC 的 MC1。

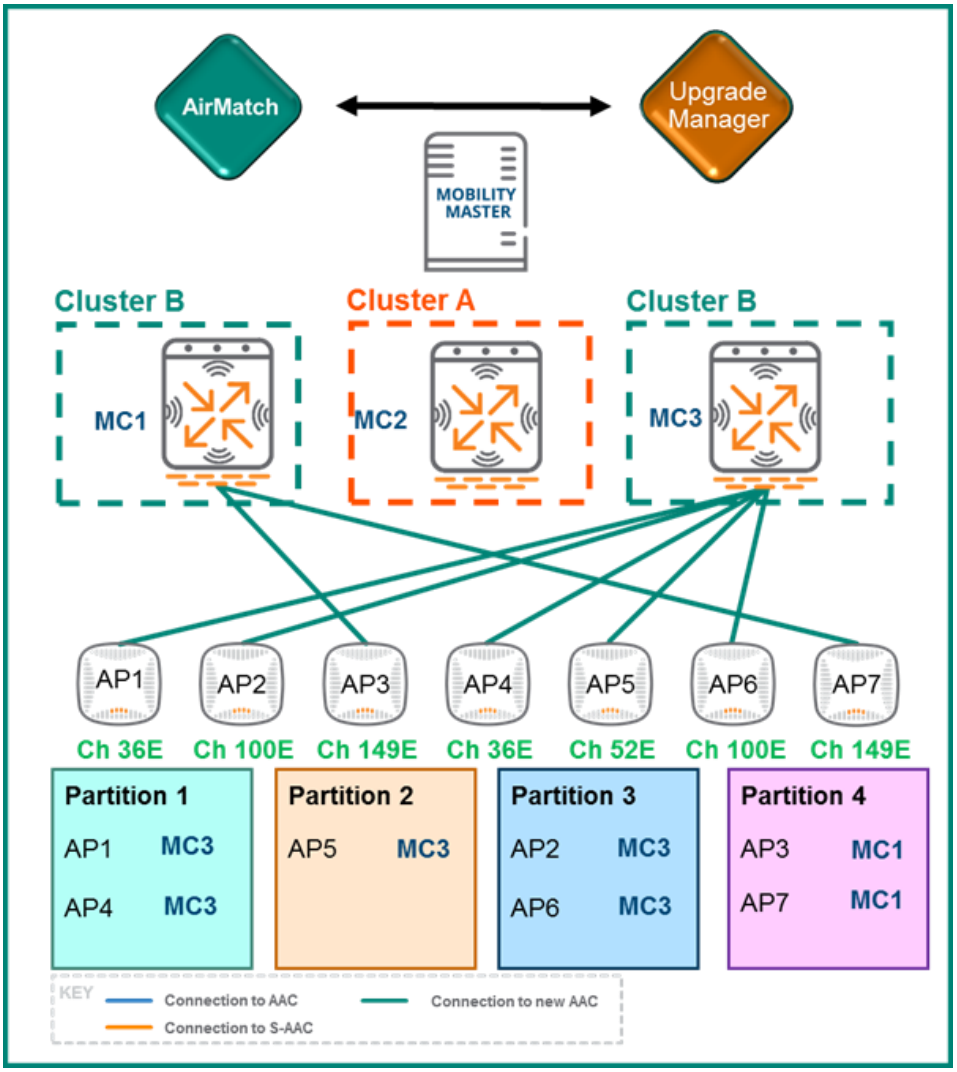


图 96 *AP 3 和 7 连接到 MC1*

最后一个成员升级

在所有群集成员均接受了升级并重新启动后，最后一个成员 (MC2) 也能够开始升级。MC2 没有任何关联的客户端或 AP，因为其已被故意排除，不作为这些分区的目标控制器，因此不需要重新分配 AP 或客户端。这意味着 MC2 可重新启动，使用其新固件重新联机，以及重新加入群集 B 中的其他两个 MC。重新加入群集后，MC2 将可用于群集领导者确定的 AP 和客户端负载分担。

NOTE

有关群集负载分担的其他信息，请参阅客户端负载分担和 AP 负载分担部分。

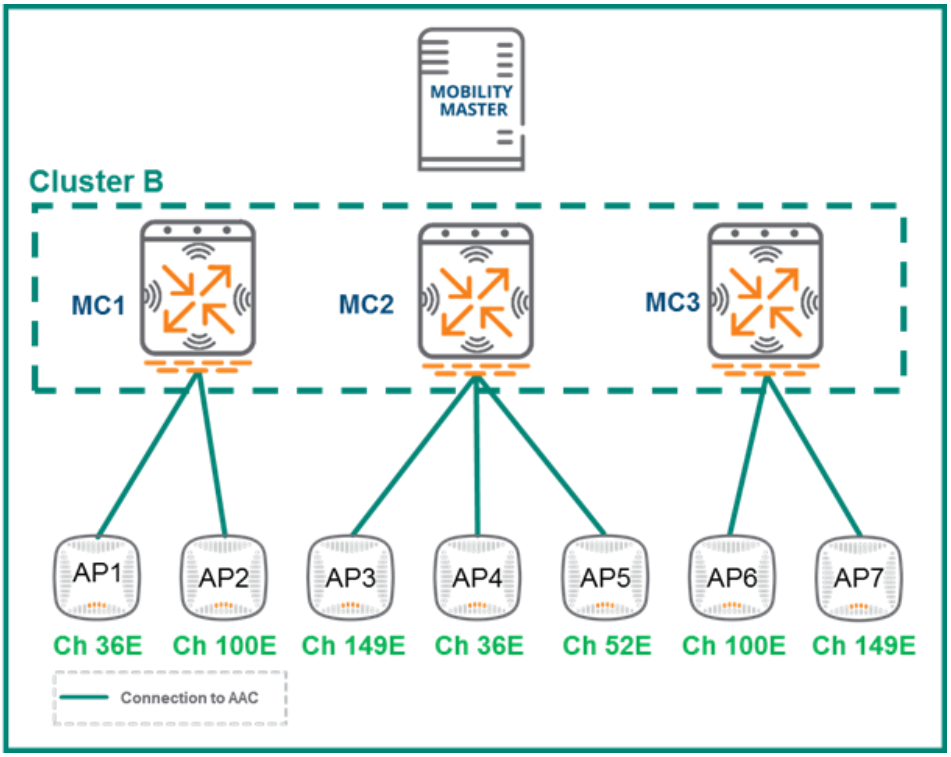


图 97 *实时升级完成*

集中式许可

自 ArubaOS 6 推出以来，ArubaOS 便已支持集中式许可模式。这种模式以往的工作方式是可将许可安装在一个控制器上，其他控制器将“订阅”，以便在需要时从全局许可池中撤销许可。但此模式的一个重要限制是，在某些客户部署中无法控制一个控制器能够从池中撤销多少许可。此限制导致了在某些情况下，当一个站点部署的 AP 多于许可池中可用的许可数时，许可池将被耗尽。

随着 ArubaOS 8 的推出，MM 现在支持在全局池中创建更小的许可池。通过这种分段方法可限制或预留允许特定控制器或控制器组从全局池中撤销的许可。

许可概念

许可类型

在使用许可时可实现 ArubaOS 8 平台的许多关键功能和特性。这些许可通常安装在 MM 上，但如果需要，也可安装在 MCM 或独立控制器上。此外，集中式许可能够使受 MM 或 MCM 管理的 MC 根据需要“订阅”和撤销它们所需数量的许可。

ArubaOS 8 许可分为三个不同的许可类或类别：

设备许可	功能许可	会话许可
MM-VA	LIC-PEF	LIC-VIA
MM-HW*	LIC-RFP	LIC-ACR
MC-VA	LIC-PEFV	
LIC-AP	SUBX-WebCC**	
LIC-ENT		

表 15 *ArubaOS 8 中的许可*

* MM-HW 许可集成在硬件 MM 中。

** WebCC 是基于订阅的许可，“X”等于 1、3、5、7 或 10 年订阅。

- **基于设备的许可** - 可实现设备功能的许可
  - **MM-VA/MM-HW*** - 使控制器和 AP 能够在 MM 上进行端接。MM-HW 许可预安装在 MM 硬件设备上
  - **MC-VA** - 使 VMC 能够端接 AP。可将这些安装在 MM 上，或者直接安装在未在 MM 上进行端接的任何 VMC 上
  - **LIC-AP** - 安装在 MM、MCM 或独立控制器上以实现 AP 端接的许可
- **基于功能的许可** - 可实现特定软件功能的许可

- **LIC-PEF -** 可实现策略执行防火墙 (PEF) 功能
- **LIC-RFP -** 这些可实现射频保护 (RFP) 功能，从而提供 WIDS/WIPS 和频谱分析支持
- **LIC-PEFV -** 作为应用于每个控制器的平台许可，在虚拟 Internet 接入 (VIA) 客户端角色上实现 PEF 支持。正在逐步被 LIC-VIA 会话许可所淘汰
- **SUBX-WebCC -** 这种基于订阅的许可在 1、2、3、5 和 7 年订阅中实现 Web 筛选支持
- **LIC-ENT -** 这是 AP、PEF、RFP 和 LIC-AW (AirWave) 许可的捆绑组合

- **基于会话的许可** - 根据控制器中允许的并发会话数定义功能
  - **LIC-VIA -** 使虚拟 Internet 接入 (VIA) 客户端能够连接并建立到控制器的隧道
  - **LIC-ACR -** 高级加密 (ACR) 许可能够使 Suite B 许可在控制器上使用

MM 许可

ArubaOS 8 中的 MM 可作为受其管理的任何 MC 的集中式许可服务器。当 MM 作为许可主控制器时，AP 和控制器将从集中式 MM 许可池中提取许可。以下表 16 描述了 MM 上的许可使用过程。

VMM 许可使用采用略微不同的方法，因为这些计算机为虚拟设备。即使部署了多个 VMM 来实现冗余，也只需要购买一个 MM-VA-XX 许可。如果正在使用 VMM 来支持多达 5,000 个设备，则只需要一个 MM-VA-5K 许可，并且可配置多个 VMM 来管理 WLAN。此外，可堆叠较小的 MM-VA 许可，以支持 MM 上的大量设备。但堆叠较小的许可在达到某一点时，其成本可能高于单个较大的 MM-VA 许可。

因为硬件 MM 是硬件设备，并且无法堆叠许可，因此在它们上预装了许可，这会导致许可成本增加。例如，如果某个部署必须支持多达 5,000 个设备，则将需要两个 MM-HW-5K 设备，即使它们一起仍将仅支持最多 5,000 个设备。

对于其他所有许可（AP、PEF、RFP 等），只需购买必要数量的许可即可，在 MM 之间将共享许可数据库。

许可类型	使用方法
MM-VA/MM-HW	每个控制器或 AP 都将使用 1 个许可
MC-VA	在 VMC 上端接的每个 AP 都将使用 1 个许可
AP、PEF、RFP	在控制器上端接的每个 AP 都将使用 1 个许可
LIC-PEFV	将每个 LIC-PEFV 许可应用于每个控制器
SUBX-WebCC	在控制器上端接的每个 AP 都将使用 1 个许可
LIC-VIA	控制器上的每个“VIA 用户会话”均将使用 1 个许可
LIC-ACR	每个“SuiteB”客户端或隧道均将使用 (1) 个许可

表 16 *ArubaOS 8 中的许可使用*

许可模式示例

- **示例部署 1 -** 由硬件 MC (MC) 和虚拟 MM (VMM) 管理的具有 AP、PEF、RFP 许可的 800 个 AP。通过此示例部署，800 个 AP 中的每一个均需要 AP、PEF 和 RFP 许可。拥有 VMM 需要有足够的 MM-VA 许可才能涵盖其管理下的每个 AP 和 MC。MM-VA-1K 许可提供具有 1000 个许可的许可池。该池 1000 个许可中有 800 个由 AP 使用，这意味着剩下 200 个许可用于 MC 以及将来添加的任何设备。

许可类型	数量
MM-VA-1K	1
LIC-AP	800
LIC-PEF	800
LIC-RFP	800

表 17 *许可示例模式 1*

- **示例部署 2 -** 使用 VMC 和 VMM 的具有 AP 和 PEF 许可的 250 个 AP。在这种情况下，MM-VA-500 许可提供了一个可在 MM 上用于最多 500 个设备的许可池。MC-VA-250 许可将使最多 250 个 AP 能够在 MM 下任何数量的 VMC（可以是一个 VMC，也可以是多个 VMC）上进行端接。

许可类型	数量
MM-VA-500	1
MC-VA-250	1
LIC-AP	250
LIC-PEF	250

表 18 *许可示例模式 2*

- **示例部署 3** - 具有 AP、PEF 和 RFP 许可的 6,000 个 AP，它们使用具有冗余的硬件 MC 和硬件 MM (HMM) 来进行群集。以下尺寸规格显示了两个 10k MM 设备、支持群集中所有 6,000 个 AP 的六个 7240XM 控制器，以及分别用于 AP、PEF 和 RFP 的 6000 个 AP 许可。

许可类型	数量
MM-HW-10K	2
7240XM MC	6
LIC-AP	6000
LIC-PEF	6000
LIC-RFP	6000

表 19 *许可示例模式 3*

- **示例部署 4** - 具有 AP、PEF 和 RFP 许可的 2000 个 AP，支持需要 VIA 和 Suite B 加密的 1,500 个客户端，使用硬件 MC 和硬件 MM。MM-HW-5k 许可提供了一个可在 MM 上用于最多 5,000 个设备的许可池。

许可类型	数量
MM-HW-5K	2
7240XM MC	2
LIC-AP	2000
LIC-PEF	2000
LIC-RFP	2000
LIC-VIA	1500
LIC-ACR	1500

表 20 *许可示例模式 4*

- **示例部署 5 -** 具有 AP 和 PEF 许可的 2000 个 AP，使用硬件 MC 和 HMM，每 AP 最多支持 50 个客户端，最多共支持 10,000 个客户端。客户端数远高于平均值，因此即使总 AP 数量仅为 2,000，最大 HMM 也必须能够容纳所有客户端。

许可类型	数量
MM-HW-10K	2
7240XM MC	2
LIC-AP	2000
LIC-PEF	2000

表 21 *许可示例模式 5*

MCM 许可

MC Master (MCM) 类似于 Aruba OS 6 中的“主-本地”控制器架构，其中专用硬件控制器作为所有托管本地控制器的中心许可服务器以及中心配置点。

仅在 7030 和 7200 系列控制器上支持 MCM 模式。7024 及更小以及 VMC 不能作为 MCM 设备。

可在 MCM 控制器上配置和安装许可。基于设备（MM-VA 许可除外）、功能和会话的许可应根据其使用要求进行扩展并使用相同的考虑因素（类似于 MM）。

但针对将由 MCM 管理的 VMC 控制器的 MC-VA 许可将安装在单独 VMC 上。即，MCM 下的 VMC 不能像在 MM 下那样共享许可。此外 MC-VA 许可还必须整个安装，并且必须与平台匹配。例如，不能购买单个 MC-VA-250 许可，然后在 5 个 VMC 间进行拆分，每个 50 个许可。MC-VA-250 将需要安装在 MC-VA-250（或更小）非 MM 托管的 VMC 上。

独立许可

当许可独立控制器时，所有基于设备、功能和会话的相同许可都可安装在独立控制器上，并以相同方式加以使用。

独立控制器上的 MC-VA 许可必须整个安装，并且必须与平台匹配。例如，不能购买单个 MC-VA-250 许可，然后在 5 个 VMC 间进行拆分，每个 50 个许可。MC-VA-250 将需要安装在 MC-VA-250（或更小）非 MM 托管的 VMC 上。

许可激活和迁移

MyNetworking 门户网站

MyNetworkingPortal (MNP) 是 HPE 的许可门户，用于各种支持活动，其中包括：

- 通过购买激活新许可
- 激活演示和评估许可
- 许可管理（迁移、更改所有权等）
- 软件和用户指南

MNP 包含在登录将用户引导到他们正在尝试查找的相应资源后显示的主登陆页面。

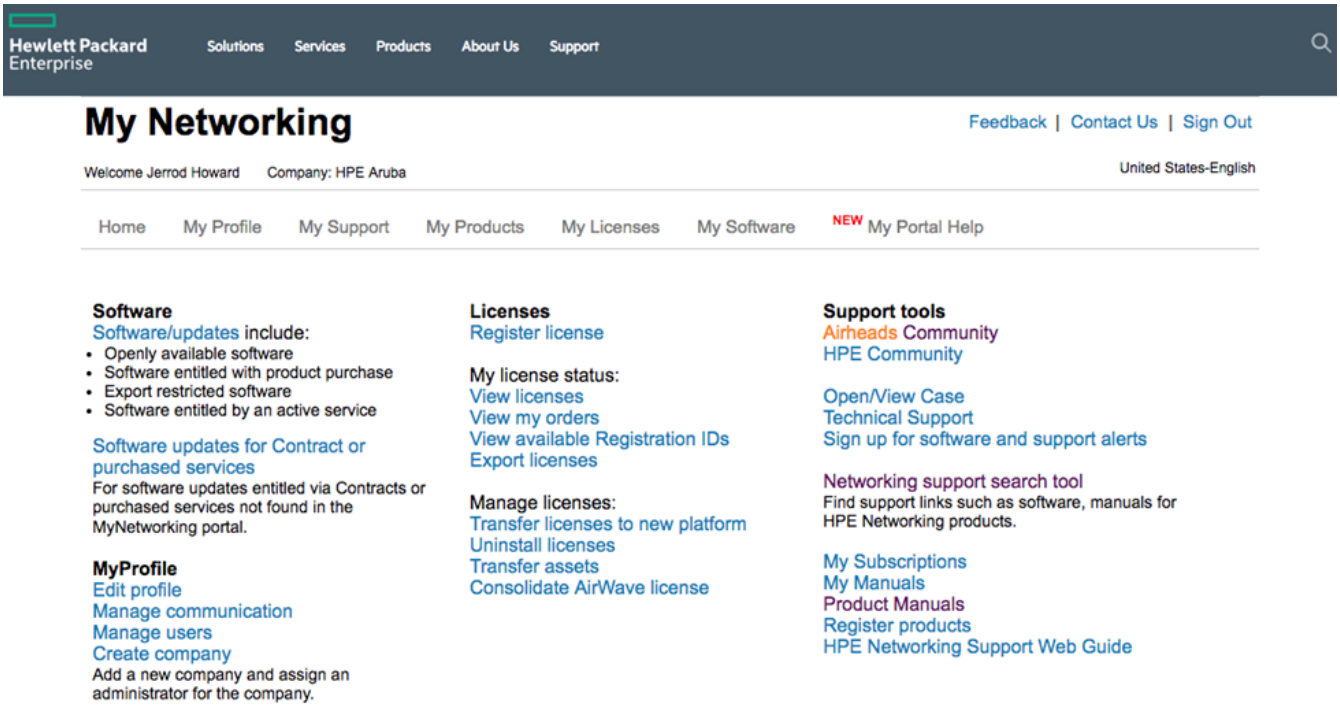


图 98 *MyNetworkingPortal 仪表板*

下新订单时，将生成包含关联*注册 ID* 或*证书 ID* 的销售订单。登录 MNP 后，单击**注册许可**，输入销售订单中的相同注册 ID 或证书 ID。然后将显示一个提示，要求输入与该订单相对应的电子邮件地址。根据创建该订单的方式，此电子邮件地址可能属于个人或组织，但在任何一种情况下，在销售发票上都会显示相应的地址。输入后将列出准备激活的所有许可的列表。将列出许可的总数量以及等待激活的许可数量。在从新的销售订单激活许可时，可用许可的数量将减少。可通过以下 URL 访问 MNP：

https://hpe.com/networking/mynetworking/

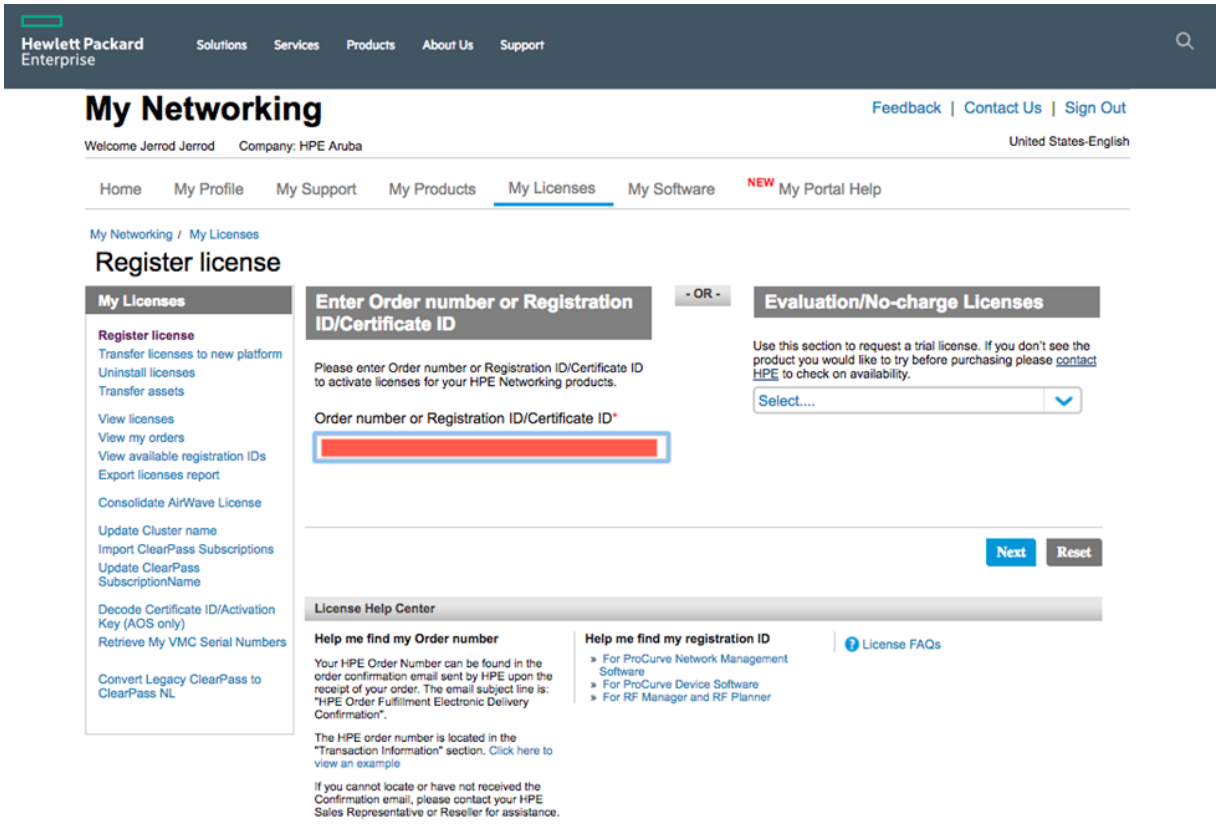


图 99 *MNP 中的许可注册*

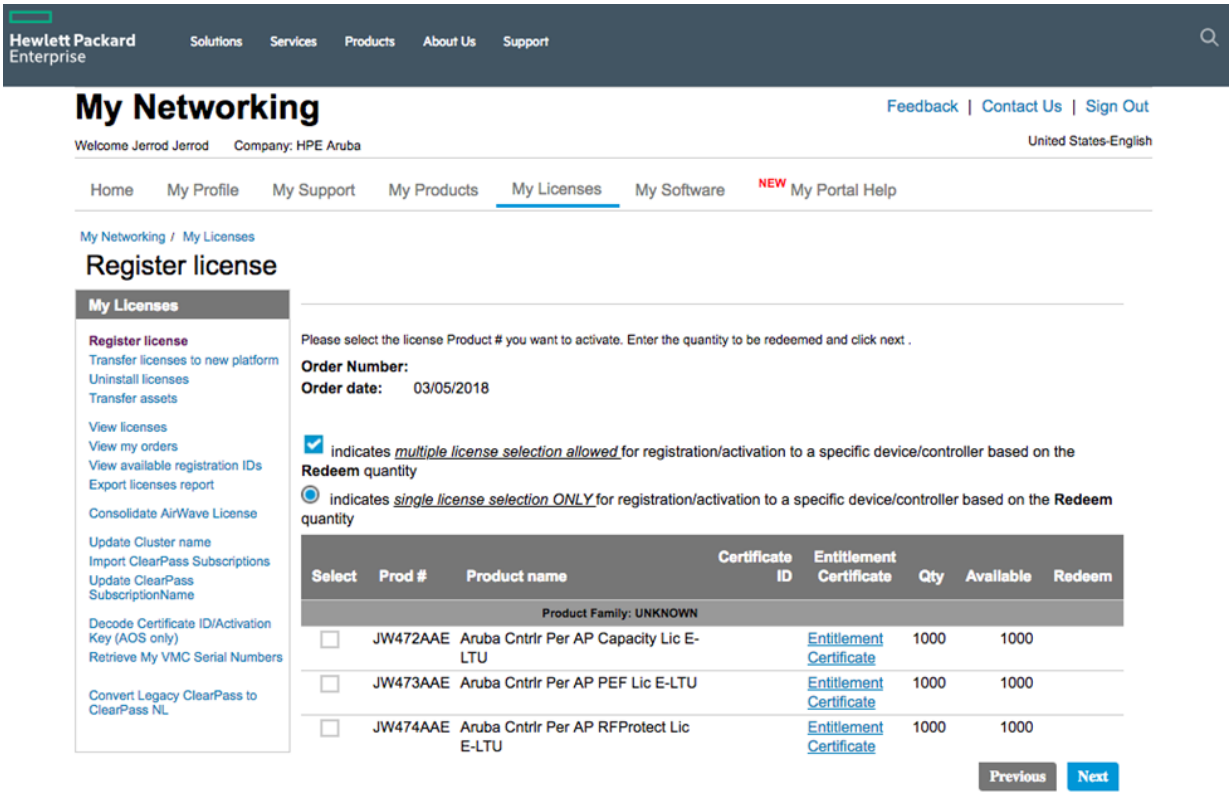


图 100 *MNP 中的许可注册*

在硬件 MC 和 MM 情况下，许可激活只需要控制器序列号，在任何虚拟设备或控制器情况下，只需要许可密码。此序列号或许可密码位于控制器 GUI 的**系统 > 许可 > MM/控制器许可**下，单击蓝色 + 号，或者对于硬件序列号，在 CLI 中使用命令 `show inventory`，或者对于虚拟设备或控制器，使用命令 `show licenses passphrase`。

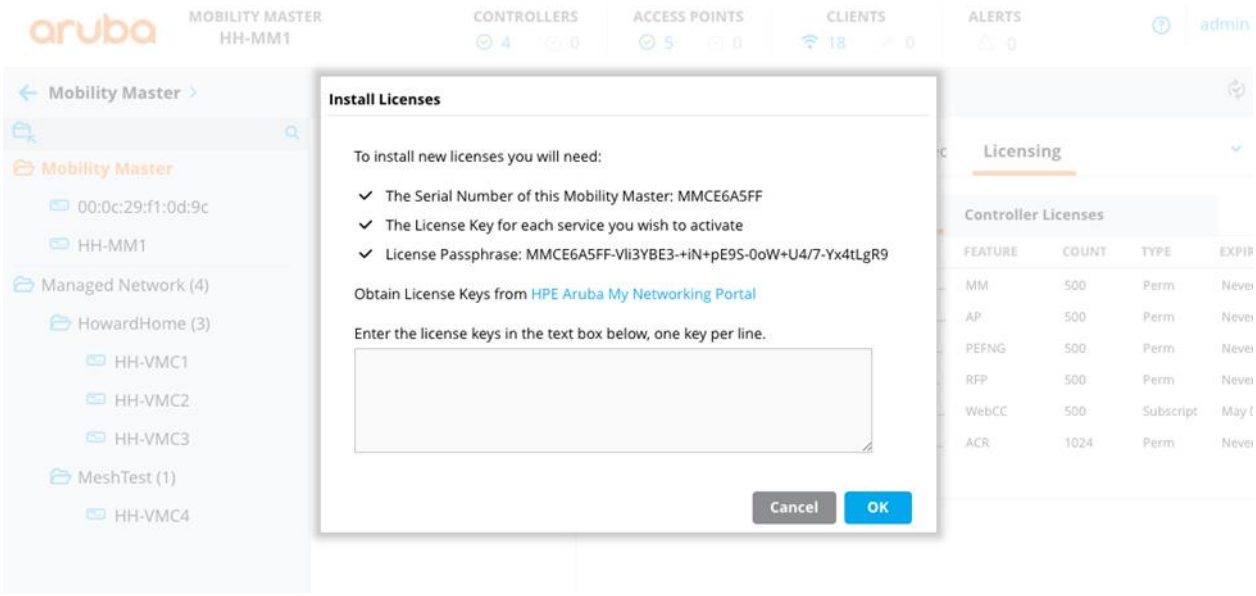


图 101 *MNP 中的许可激活*

通过 MNP 将许可从 ArubaOS 6 迁移到 ArubaOS 8：

1. 导航到 MNP 门户页面，然后选择**将许可转移到新平台**。MNP 将显示该帐户拥有的所有序列号
2. 找到当前持有这些许可的设备的序列号，然后单击**下一步**
3. 从下拉列表中选择将迁移许可的新控制器，以及新的 ArubaOS 8 序列号或密码
4. 单击**转移**

MNP 将提供新的许可密钥，以及使用新的许可激活密钥更新 MNP 中的序列号数据库。这些新的许可密钥将被粘贴到新的 MM、MCM 或独立 8.x 控制器中。

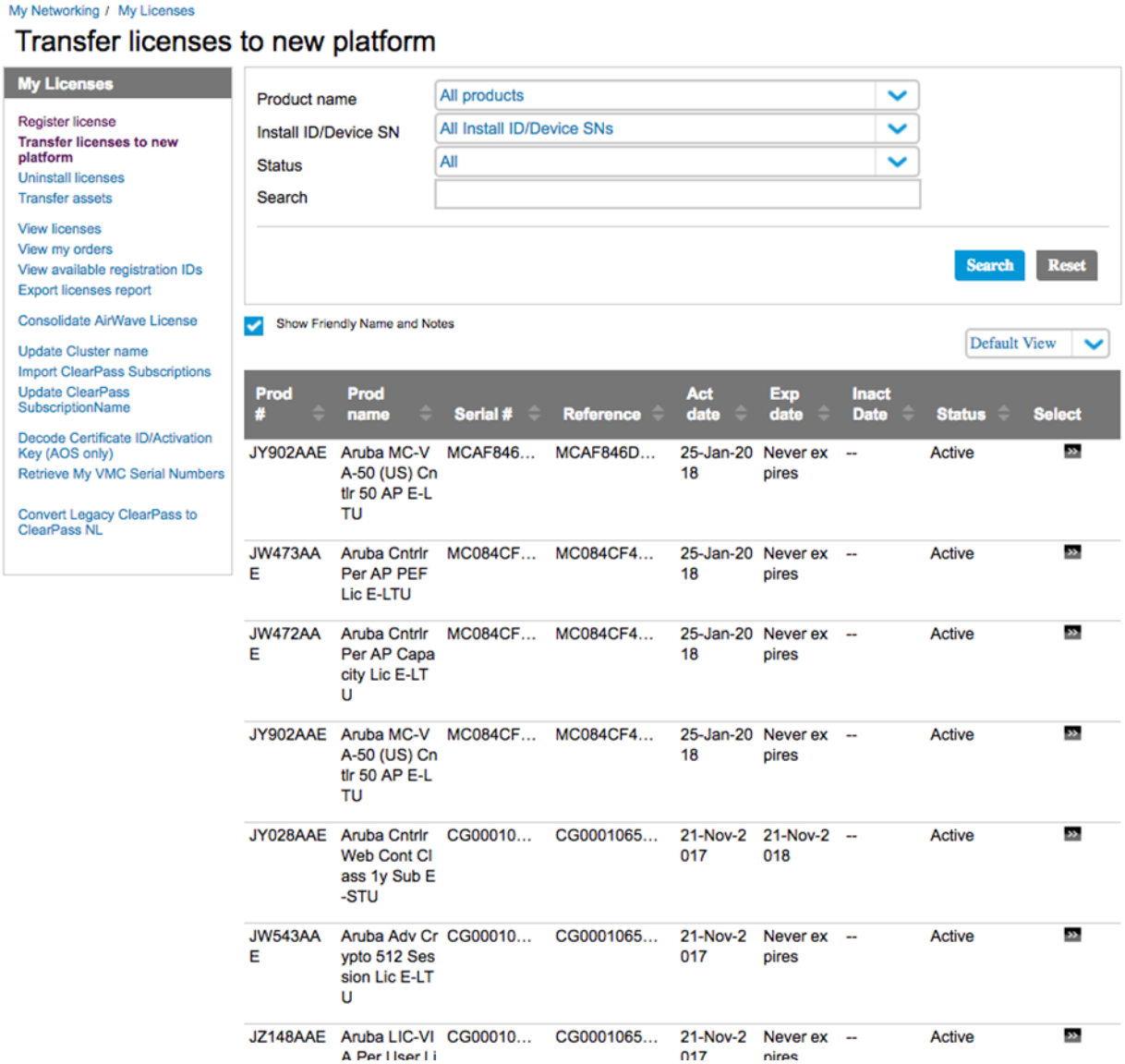


图 102 *将许可转移到 MNP 中的新平台*

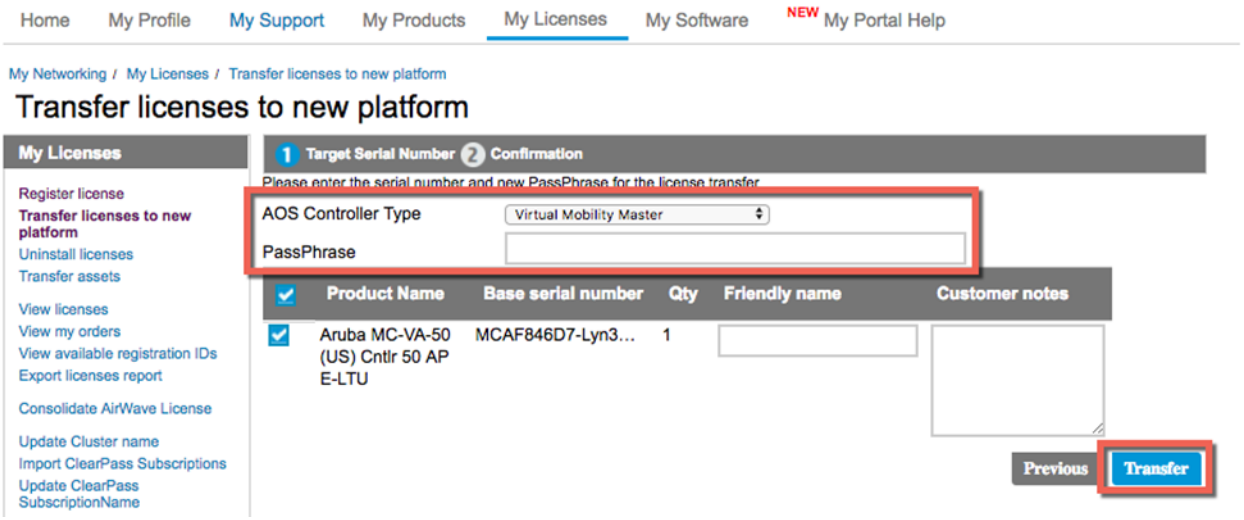


图 103 *将许可转移到 MNP 中的新平台*

Aruba 支持门户网站

Aruba 支持门户 (ASP) 是 Aruba 的新许可支持机制，旨在通过购买方式来激活新许可，激活演示和评估许可，管理许可（迁移、更改所有权等）以及访问支持文档。ASP 是一个更简化的支持门户，其更易于使用，具有更高级的额外能，并且将成为面向所有 Aruba 产品的 Aruba 主要许可支持门户。

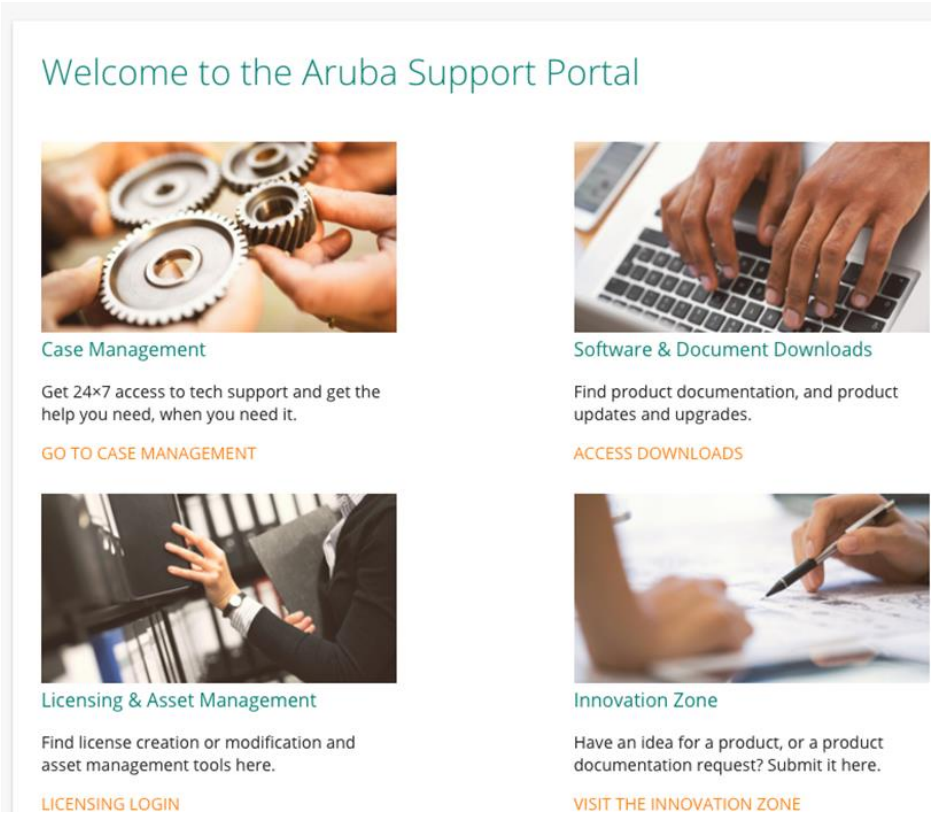


图 104 *Aruba 支持门户*

许可激活

就新订单将具有与它们关联的*订单号*或*证书 ID* 以用于许可激活而言，ASP 的工作方式与 MNP 类似。在**许可登录**页面中，可将订单号或证书 ID 输入到正确的字段中。下一步，将输入控制器序列号或密码以及需要激活的许可数量。将所有必需的信息输入该门户后，单击**激活证书**按钮将生成新的许可密钥。可通过以下 URL 访问 ASP：

https://asp.arubanetworks.com

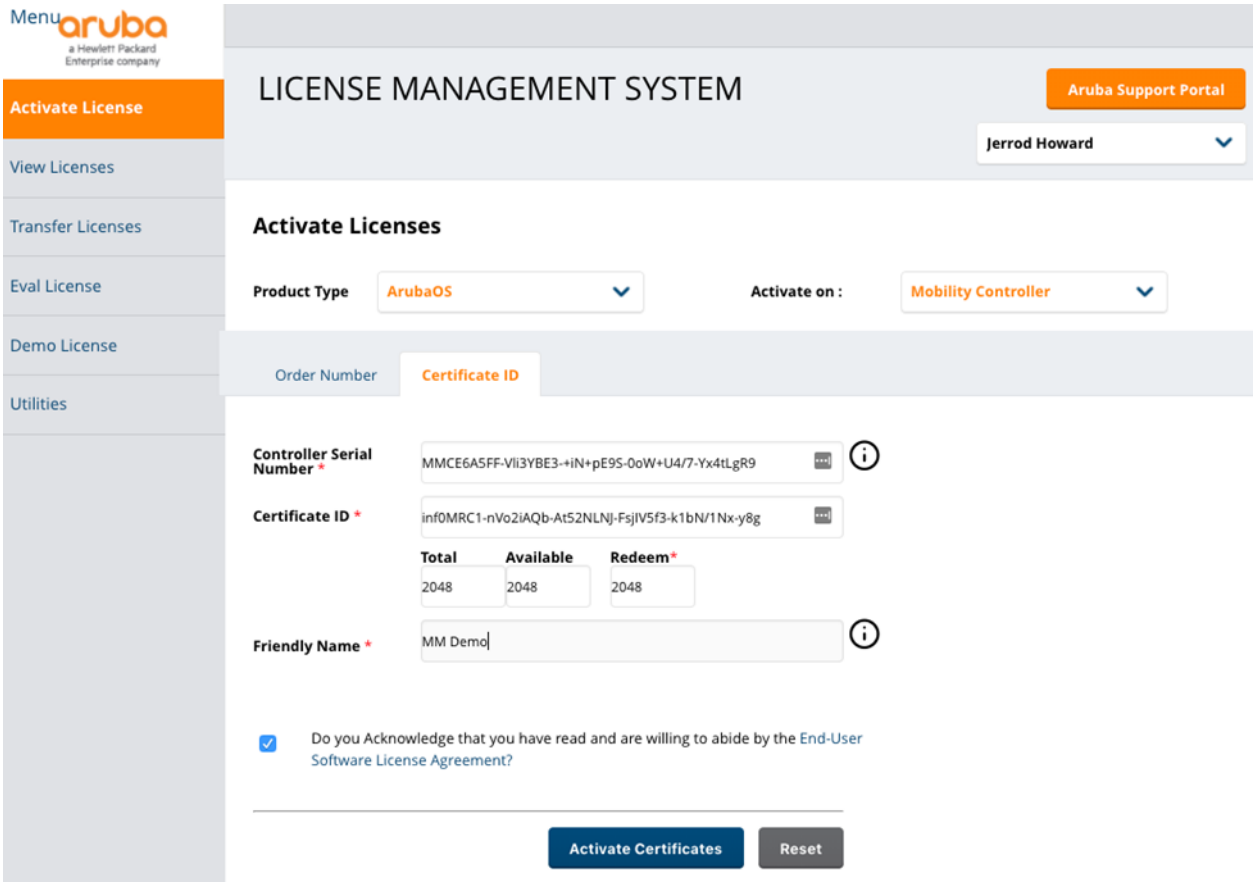


图 105 *ASP 中的许可激活*

许可迁移

ASP 还可用于在设备之间迁移许可。该门户包含一个专门用于许可迁移的部分，称为**转移许可**，其将显示当前持有许可的不同类型的设备，例如 MC、硬件 MM、虚拟 MM 等。导航到此部分后，将显示一个页面，用于输入将迁移的许可当前所在设备的序列号。输入序列号后，将显示另一个带有提示的窗口，询问新迁移许可的目标。已将所有必需的信息输入到该工具中后，ASP 将相应地更新其数据库，以显示与新设备的序列号或密码关联的新 ArubaOS 8 许可密钥。

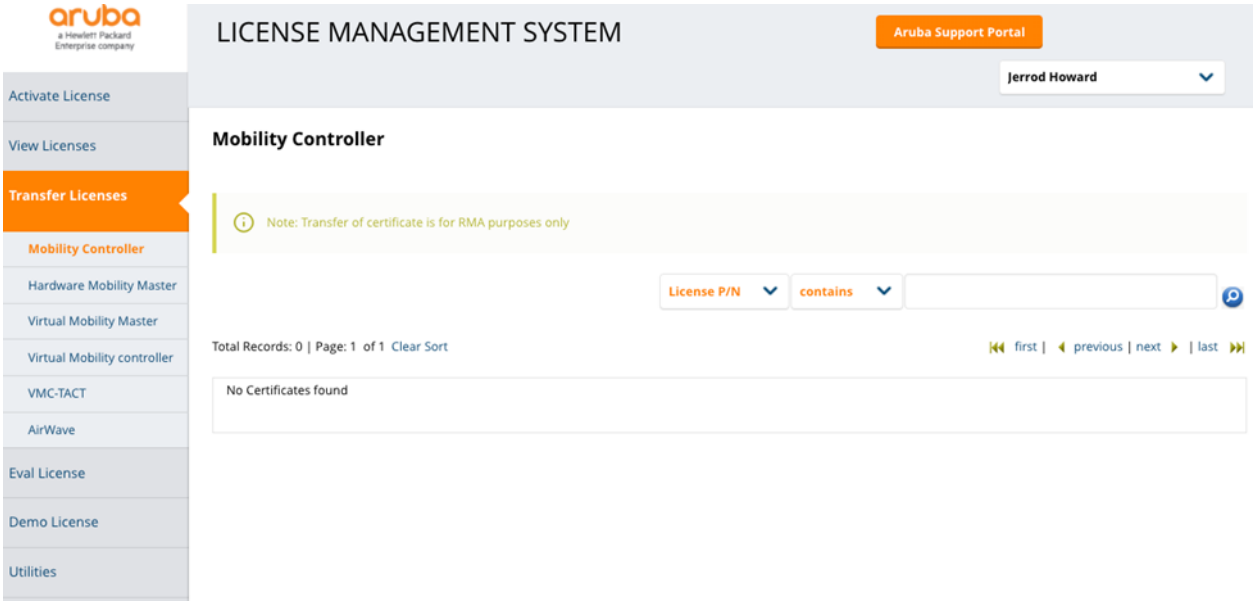


图 106 *在 ASP 中转移许可*

许可迁移工具

ArubaOS 8 迁移工具能够与 MNP 或 ASP 进行通信，以便与控制器进行通信，并在升级过程中自动迁移其关联的许可。

务必注意，此迁移工具专门用于涉及从 ArubaOS 6 升级到 ArubaOS 8 的情况。此迁移工具不能用于独立于升级的许可迁移。如果没有使用此迁移工具来进行升级，则必须通过 MNP 或 ASP 手动迁移现有许可，否则作为迁移的一部分将需要购买新许可。

在迁移工具设置过程中将显示一条提示，要求迁移许可。如果选择**是**，则会显示一个字段，要求输入 MNP 或 ASP 用户名。此外在迁移过程设置结束时还将需要输入密码。

已将正在迁移到 ArubaOS 8 的控制器的序列号和 MM 密码（如果适用）输入到该迁移工具中后，可开始升级过程。该迁移工具将登录到 MNP 或 ASP，搜索关联的序列号，然后相应地迁移许可。所有许可都将迁移到 MM，或者它们将根据其控制器序列号进行迁移。

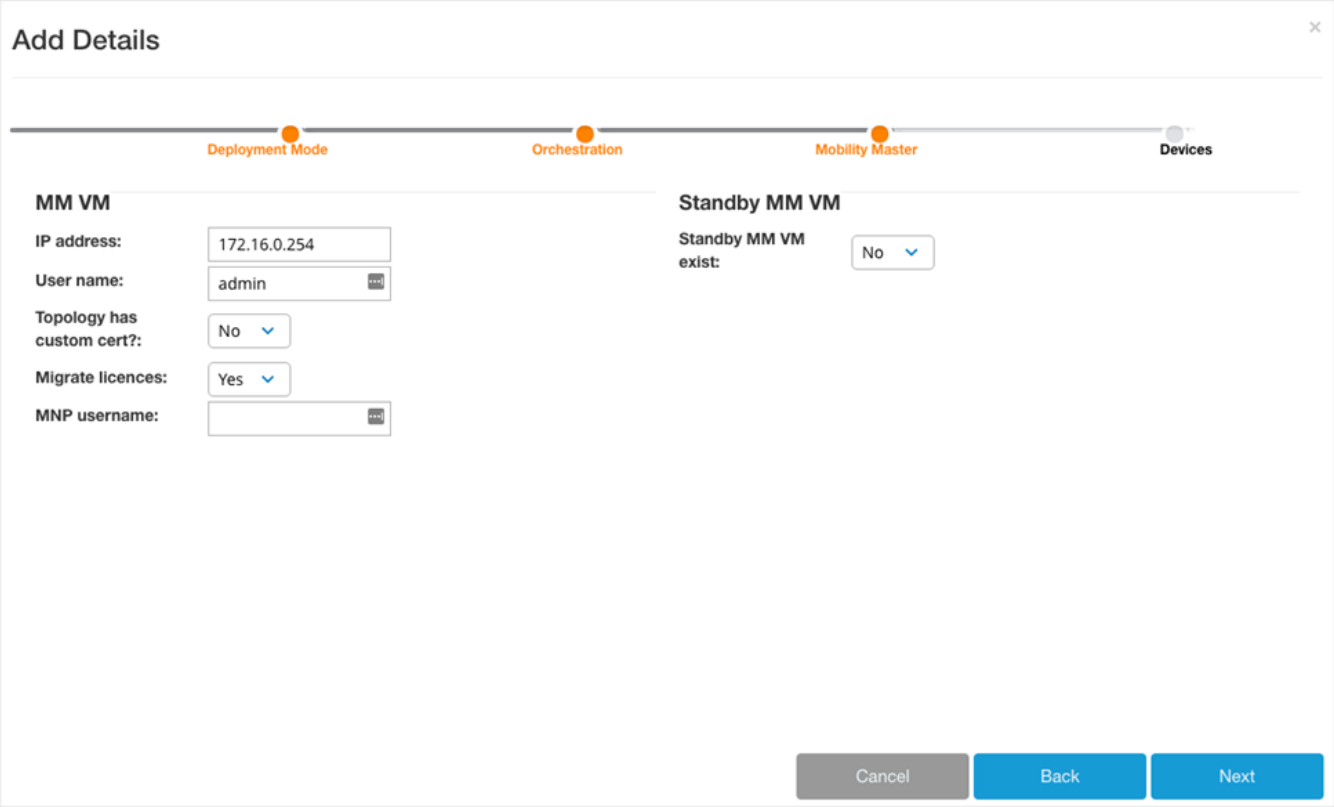


图 107 *在 ASP 中添加许可迁移的详细信息*

许可安装

许可组件

为了在控制器或 MM 上安装许可，需要输入通过 MNP 或 ASP 激活生成的*许可密钥*。该密钥将生成一个字母数字字符串，该字符串可启用特定的许可类型、功能或订阅。可通过 GUI 或 CLI 将许可安装在 MM (MM)、MM 控制器 (MCM) 或独立 MC (MC) 上。

通过 GUI 安装许可

MM 作为所有控制器和服务的主许可服务器。对于特定 MM 下的设备，其许可是以 MM 级别进行安装。要在 MM 上安装许可，则访问 GUI，导航到 **MM > 系统 > 许可选项卡**，单击 **MM 许可**，然后单击蓝色 **+** 号，添加新许可。

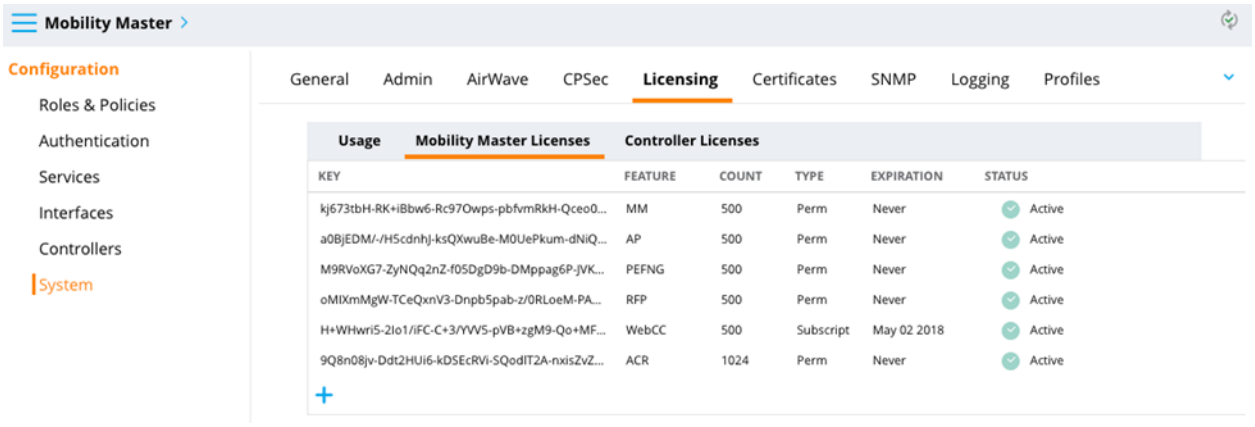


图 108 *使用 GUI 安装 MM 许可*

从该页面可看到所有已安装的许可及其数量。此外，必要时还可删除许可。MM 许可服务能够管理所有许可，包括 MC-VA 许可的动态配置。此功能为 MM 所特有，通过该功能可根据需要在该 MM 下的多个 VMC 之间拆分单个安装的 MC-VA 许可池。例如，只要所有控制器间端接的 AP 总数不超过 250 个 AP，便可将单个 MC-VA-250 许可池分布在同一个 MM 下的 2 个 MC 或 20 个 VMC 上。MM 下的许可分配完全灵活，可根据给定部署的需要轻松进行调整。

对于 MCM 和独立控制器，GUI 中的许可安装位置和过程与 MC 和 VMC 相同。主要区别是，不应选择 MM 部分，而应选择 **MC > 配置 > 系统 > 许可**。下一步，选择**库存**下拉屏幕，然后单击蓝色 **+** 号，添加新许可。

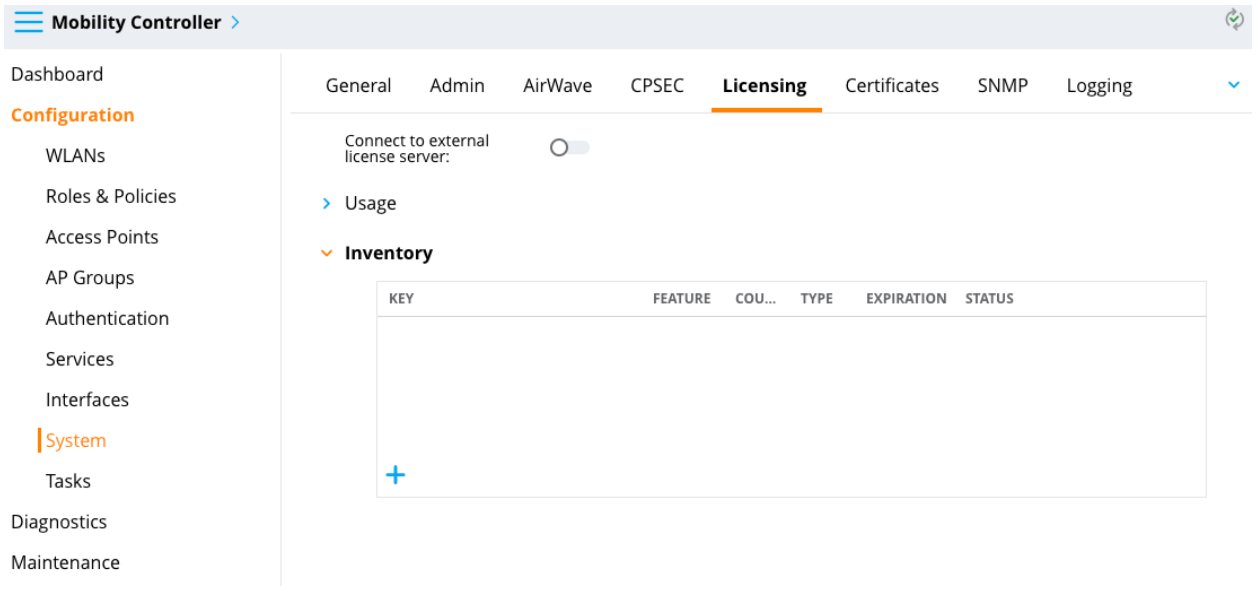


图 109 *使用 GUI 安装 MCM 和独立控制器许可*

在这两种情况下均会显示一条带有序列号、许可密码（在虚拟设备或 VMC 的情况下）的提示，以及一个窗口，可在该窗口中粘贴一个或多个许可，以应用于所需控制器。

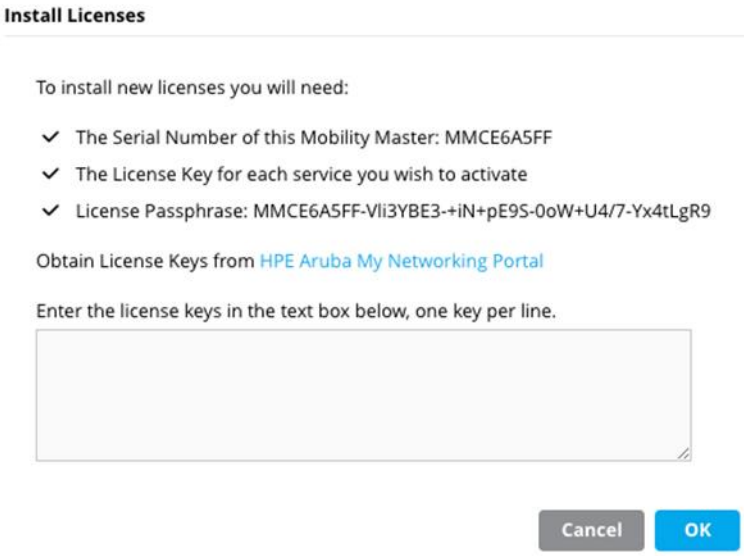


图 110 *许可安装对话窗口*

添加了许可密钥后，选择蓝色的**确定**按钮，完成此安装过程。在大多数情况下，如果控制器第一次安装了许可，则需要重新启动它们才能使许可生效。对于未来安装更多数量现有许可的许可添加情况，一般不需要重新启动。一般该页面指示控制器是否需要重新启动。标记有“R”的许可表示需要重新启动。

通过 CLI 安装许可

要通过 CLI 安装许可，可通过 SSH 登录 MM、MCM 或独立控制器，然后输入以下命令：

```
#License add <insert-license-key-here>
```

可使用以下命令显示许可清单：

```
#show licensing
```

Mobility Master 许可池

MM (MM) 特有的另一个功能是能够创建*许可池*。*许可池*可使 MM 管理较大全局许可池的较小池，以及将许可应用于该 MM 下的控制器或控制器组。以这种方式分配许可能够更细致地控制允许每个控制器或控制器组使用的许可数量。此功能的用例包括全局网络管理员想要限制某个位置可部署多少 AP 的情况，以便使它们的许可供应不会耗尽，从而避免在其他站点产生问题。

NOTE

许可池在 MCM 和独立控制器模式下不可用。

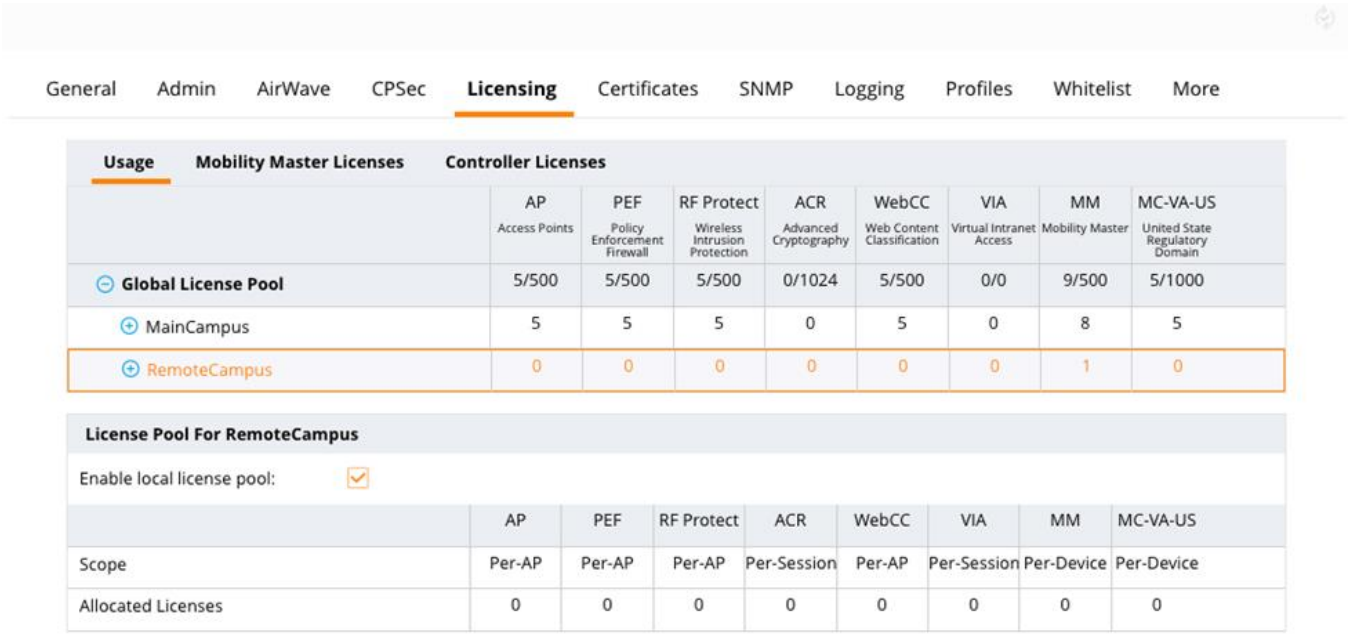


图 111 *创建许可池*

*许可池*由 MM 的节点加以定义。在以下示例中有一个“主园区”以及一个“远程园区”控制器组。全局许可池由用于 AP、PEF、射频保护等的 500 个许可组成。此示例情况的网络管理员想要在远程园区将 AP 数量限制为 50 个。

要设置此所需限制，他们将单击所需节点，然后选中**启用本地许可池**框。下一步，他们将单击每个许可类型，以便分配允许用于远程园区节点的许可数量。对于该节点所需的每个许可类型，均将需要重复此过程。在该示例中，有 50 个 AP 需要许可，这意味着将从全局许可池中扣除每个类型的 50 个许可。在我们的示例中，“远程园区”节点不能从 MM 全局池中使用超过 50 个 AP 许可。其余 450 个许可在全局许可池中可用于分配给其他节点。

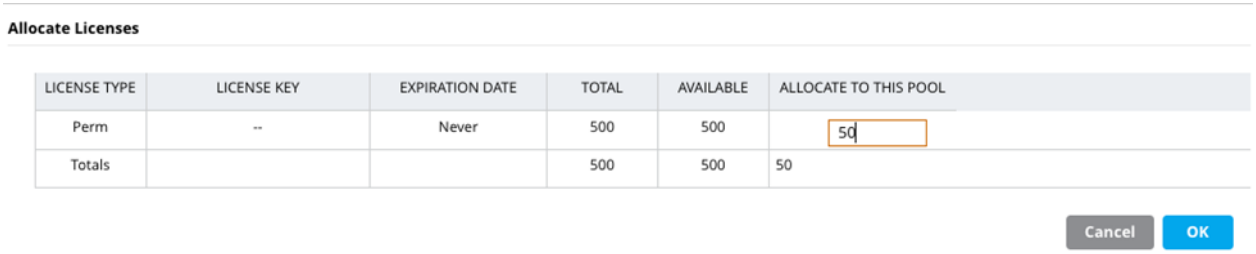


图 112 *将许可分配到许可池*

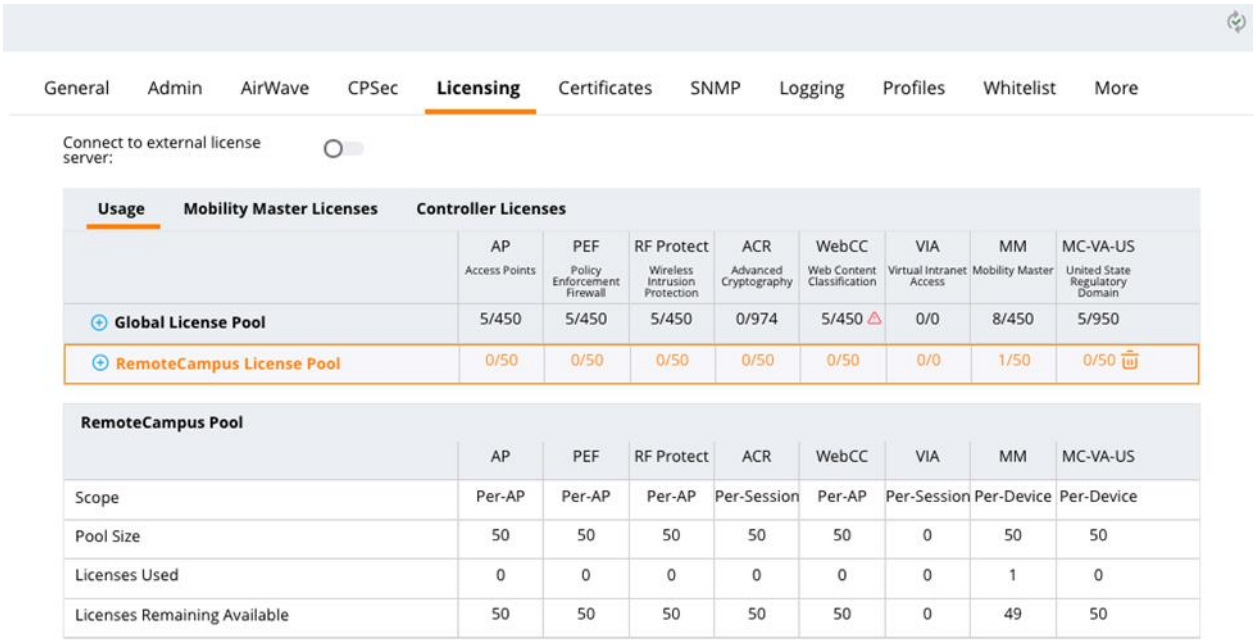

General
Admin
AirWave
CPSec
Licensing
Certificates
SNMP
Logging
Profiles
Whitelist
More
Connect to external license server:
Usage
Mobility Master Licenses
Controller Licenses
AP
Access Points
PEF
Policy Enforcement Firewall
RF Protect
Wireless Intrusion Protection
ACR
Advanced Cryptography
WebCC
Web Content Classification
VIA
Virtual Intranet Access
MM
Mobility Master
MC-VA-US
United State Regulatory Domain
Global License Pool
5/450
5/450
5/450
0/974
5/450
0/0
8/450
5/950
RemoteCampus License Pool
0/50
0/50
0/50
0/50
0/50
0/0
1/50
0/50
RemoteCampus Pool
AP
PEF
RF Protect
ACR
WebCC
VIA
MM
MC-VA-US
Scope
Per-AP
Per-AP
Per-AP
Per-Session
Per-AP
Per-Session
Per-Device
Per-Device
Pool Size
50
50
50
50
50
0
50
50
Licenses Used
0
0
0
0
0
0
1
0
Licenses Remaining Available
50
50
50
50
50
0
49
50

图 113 *许可池仪表板*

控制器参考架构

介绍

本章探讨为典型企业网络实施端到端 Aruba 移动优先架构的设计决策和最佳实践选择。该讨论侧重于架构设计建议，以及解释构建每个架构所需的各种配置和注意事项。参考架构用于小型、中型和大型楼宇以及大型园区。对于每个架构模式，将讨论以下主题：

- 推荐的模块化局域网 (LAN) 设计
- MC 群集布局
- 设计注意事项和最佳实践
- 建议的交换机和无线平台

本章提供的信息非常适用于负责绿地设计的网络架构师、负责优化现有网络的网络管理员，以及需要在网络增长时可遵循的模板的网络规划人员。本章适用的环境范围包括从少于 32 个 AP 的小型办事处，到最多支持 10,000 个 AP 的大型园区。

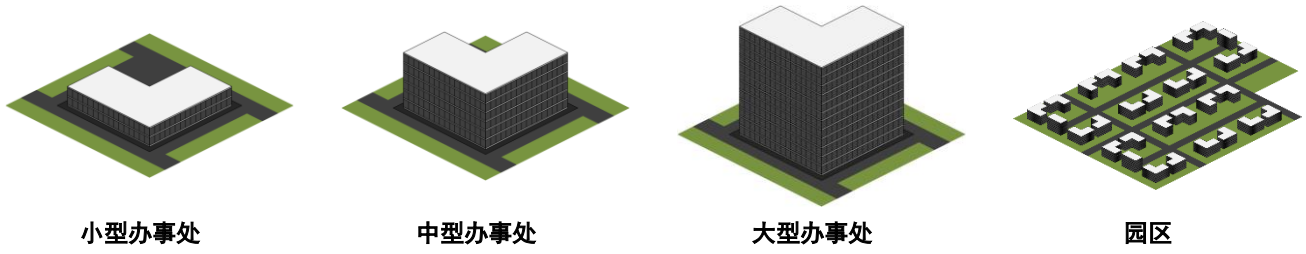


图 114 *设计范围*

本章不提供逐步配置示例或垂直的特定无线设计。详细配置示例由 Aruba 解决方案交换 (ASE) 提供，而垂直的特定设计在单独 VRD 文档中提供。

设计原则

本章中提供的每个参考架构的基础是底层模块化 LAN 设计模式，该模式将网络分成更小、更加可管理的模块化组件。典型 LAN 包括一组公共互连层，例如形成主网络的核心、分布和接入层，以及提供特定功能的附加模块，例如 Internet、WAN、无线和服务器聚合。

这种模块化方法可简化 LAN 的整体设计和管理，同时具有以下优势：

1. 模块可轻松加以复制，从而实现增长和可扩展性
2. 随着网络要求的发展，可添加和删除模块，同时可最大程度降低对其他层的影响
3. 模块可将操作变更的影响限制在较小的网络子集
4. 模块将网络划分为多个具体的故障域，从而提供容错功能

本章概述的模块化设计理念与业界最佳实践一致，并且可被应用于任何规模的网络。

模块化设计

为特定 LAN 部署选择的模块化设计取决于许多因素。业界最佳实践是使用 2 层或 3 层模块化 LAN 设计构建网络，这些设计因包含或不包含分布层而彼此不同。附加的分布层位于核心层与接入层之间，用于提供聚合和路由：

- **2 层模块化 LAN** - 将核心层和分布层折叠成一个层。核心/分布层中的交换机通过提供到接入层模块的聚合以及执行 IP 路由功能来执行双重角色
- **3 层模块化 LAN -** 在核心层与接入层之间使用专用分布层。分布层交换机提供到接入层的聚合，并且直接与核心层相连。分布层交换机通常部署在较大的网络中，一般用于连接不同的模块，例如无线、WAN、Internet 和服务器

NOTE

出于本章的目的，术语“聚合层”和“分布层”可互换。

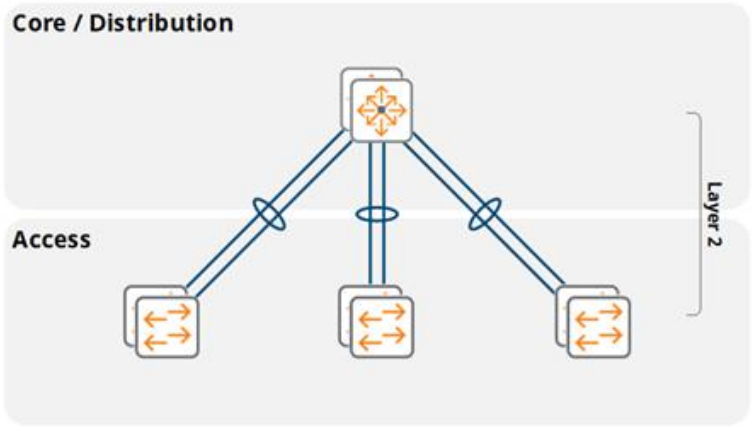


图 115 *2 层模块化 LAN*

2 层模块化 LAN 非常适用于具有很少配线柜和接入交换机的小型楼宇。接入层 VLAN 使用 802.1Q 中继在接入层交换机与核心/分布层交换机之间扩展。核心/分布层交换机包括用于每个 VLAN 的 IP 接口，并且作为接入层主机的默认网关运行。

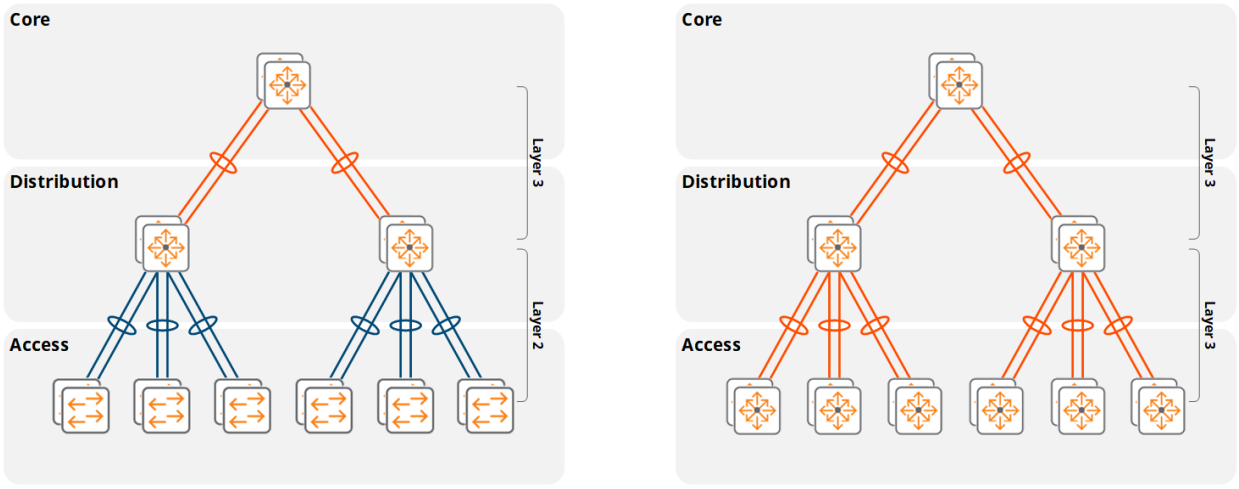


图 116 *第 2 层和被路由的接入层 3 层 LAN 设计*

在 3 层模块化设计中，IP 路由功能分布在核心层与聚合层之间。根据设计，可将它们扩展到接入层。所有 3 层 LAN 设计均将使用开放式最短路径优先 (OSPF) 等动态路由协议在聚合与核心交换机之间实施 IP 路由，从而实现可访问性和地址汇总：

- **第 2 层接入层** - 使用 802.1Q 中继将来自接入层的所有 VLAN 扩展到聚合层交换机。聚合层交换机为每个 VLAN 提供第 3 层接口（VLAN 接口或 SVI），以及为 IP 网络的其余部分提供可访问性
- **被路由的接入层** - 在聚合层交换机与接入层交换机之间（以及在聚合层与核心层之间）执行 IP 路由。在该部署模式中，每个接入层交换机或堆栈均为 IP 网络的其余部分提供可访问性

Aruba 移动优先架构支持这两种设计，从而使我们客户能够充分利用采用任一网络设计的 Aruba 解决方案的优势。

LAN 聚合层

在设计和计划移动优先网络时，是否部署聚合层的决定取决于几个关键因素：

1. 需要连接的接入层交换机数量。最终，连接接入层所需的 SFP/SFP+/QSFP 端口数量将超过核心层交换机的物理端口容量。在核心层与接入层之间添加一个额外层可提供聚合，从而减少核心层中所需的物理端口数量
2. 楼宇的结构化布线设计。较大楼宇中的中间配线架 (IDF) 一般通过光纤在楼宇内的关键位置连接到主配线架 (MDF)。每个 MDF 一般连接到服务器机房或数据中心。
   - 由于 MDF 与主服务器机房或数据中心之间的光纤容量有限，在 MDF 中通常需要聚合层交换机
   - 当部署多模光纤时，在组合的光纤长度（IDF + MDF + 服务器机房）超过光纤连接的距离规格时，通过聚合层交换机可连接 IDF

3. MDF 为聚合层交换机提供理想的位置，因为它们一般聚合来自接入层的光纤连接，并且提供与在主服务器机房或数据中心内部署的核心层的连接
4. 网络可管理性、稳定性和可扩展性问题决定了应将特定故障域引入到网络中。这一般通过在核心层与各个聚合层之间实施 IP 路由来实现。以这种方式设计网络可确保将核心层与源自其他层或模块的第 2 层故障或操作变化隔离开来
5. 减少核心层上的第 2 层和第 3 层处理负载。随着网络的增长，MAC 地址表大小和 IP 协议处理开销成比例增加。包含聚合层可将第 2 层学习和 IP 协议处理开销从核心层卸载到各个聚合层交换机。然后，聚合层成为客户端的第 2 层和第 3 层分界点，从而使核心层能够专用于 IP 路由功能

无线模块聚合层

一旦无线和动态分段的客户端主机地址数量超过特定阈值，一般将为无线模块引入专用聚合层。无线和动态分段的客户端流量通过隧道从 AP 或接入层交换机传输到移动控制器 (MC) 群集，这会导致这些 VLAN 的第一跳路由器产生 MAC 学习和 IP 处理开销。在 2 层模块化网络设计中，融合的核心层和聚合层设备会产生此开销。在 3 层模块化网络设计中，核心层会产生此开销。添加专用无线模块聚合层可减小来自核心层的 MAC 学习和 IP 处理开销，并将其转移到专用无线聚合层，从而实现稳定性、故障隔离和可扩展性。

作为最佳实践，Aruba 建议当来自无线和动态分段客户端的主机地址总数超过 4,096 时，实施专用无线聚合层。遵循此做法可确保网络免受未来增长的影响，可确保在添加新设备类或引入 IPv6（这会显著增加主机 IP 地址总数）时，核心层不会不堪重负，从而保护网络，防止其受到未来增长的影响。

对无线模块可扩展性的限制取决于为无线模块部署的聚合层交换机的扩展功能。以太网交换机专为特定应用而设计，因此其将为交换或路由操作而进行优化。根据交换机及其推荐用法，其将能够学习、处理和维护特定数量的数据链路地址和网络层绑定。与为聚合层或数据中心设计的交换机相比，为核心路由应用程序设计的交换机将支持数量更少的 MAC 地址、IPv4 ARP 条目和 IPv6 邻居。

根据交换机型号和 IP 环境，Aruba 最新一代以太网交换机可扩展到支持最多 64,000 个主机设备。作为最佳实践，无线模块的设计应使 IPv4 和 IPv6 主机地址的总数不超过无线聚合层交换机的容量。此外，无线模块的设计还应适应未来增长。Aruba 建议将 MC 群集和聚合层设计为容纳不超过其最大容量的 80%。这种方法允许未来计划内和计划外增长，无需重新设计网络。

超过单个无线模块扩展限制的大型部署将需要部署额外无线模块。每个额外无线模块均由专用无线聚合层和 MC 群集组成。所需的无线模块总数将因部署规模和 IP 环境而异。与支持本机 IPv6 或双堆栈客户端的部署相比，仅具有 IPv4 客户端的大型部署一般将需要更少的无线服务模块。这种差异主要是由于实现 IPv6 的方式导致的，其中每个主机均可获取消耗额外交换机资源的多个 IPv6 全局地址。

确定无线聚合层所需的容量取决于众多因素。两个主要考虑因素是：

1. 聚合层交换机可支持的 MAC 地址、IPv4 ARP 条目和 IPv6 邻居条目的总数
2. 聚合层交换机的架构

深入了解用户数、设备数和 IP 环境对于成功确定无线聚合层交换机是否能够满足无线模块的扩展需求至关重要。

大多数组织将知道无线基础设施需要支持多少用户，以及对于每个用户需要将多少个设备连接到无线网络有一般性了解（一般每个用户 2-3 个设备）。这些要求自然会因垂直和环境而异。例如，在高等教育环境中，学生连接三个或更多设备的情况很常见。假设每用户 3 个设备，拥有 4,000 个用户的组织应计划支持至少 12,000 个客户端设备（如果遵循允许 20% 增长空间的最佳实践，则为 14,400 个）。

知道了客户端设备的总数后，需要了解 IP 环境，以便确定无线聚合层交换机需要支持多少个 MAC 地址和网络层绑定（ARP 和/或邻居）：

IP 环境	MAC 条目	IPv4 ARP 条目	IPv6 邻居条目
本机 IPv4	1	1	0
本机 IPv6	1	0	2（最低）
双堆栈	1	1	2（最低）

表 22 - *聚合层地址要求*

计算 IPv4 扩展相对简单，因为每个客户端设备均将被分配一个 IPv4 地址。无线聚合层交换机为每个 IPv4 客户端分配一个 MAC 和一个 IPv4 ARP 表条目。因此，具有 14,400 个客户端设备的环境将需要一个能够支持 14,400 个 MAC 地址和 14,400 个 IPv4 ARP 条目的无线聚合层交换机。

对于本机 IPv4 部署，无线聚合层交换机的最大扩展容量通过评估可同时支持的 MAC 地址和 IPv4 ARP 条目总数来确定。这些信息一般在产品数据表或文档中提供。两者的最低值将确定对于每个无线模块最终可支持的最大 IPv4 主机数。例如，Aruba 8320 系列交换机最多可支持 49,000 个 MAC 地址（路由时）和 120,000 个 IPv4 ARP 条目。MAC 地址表大小是这两个值中较小的一个，这意味着 8320 系列交换机的有效限制为 49,000 个 IPv4 主机。因此，使用 8320 系列聚合层的无线模块将被限制为 49,000 个 IPv4 客户端设备。

计算 IPv6 地址要求稍微复杂些。该过程需要知道正在为每个客户端设备分配多少个全局 IPv6 地址。此数量将因已部署的 IPv6 寻址方法以及客户端操作系统而异。对于大多数 IPv6 环境，一般会为一个客户端设备分配一个链路本地地址（强制）和三个全局地址。

计算本机 IPv6 或双堆栈部署的扩展要求是一个更复杂的过程，因为需要考虑第 3 层交换机架构和每主机所分配的全局 IPv6 地址数等因素。MAC 地址表大小通常不是考虑因素，因为一般在达到 MAC 地址限制前先达到 IPv6 邻居条目的总数。根据交换机型号和供应商，在计算中还可能需要考虑链路本地地址。

Aruba 交换机根据系列和型号实施不同的架构：

- **3810/5400R 系列 -** 实施共享 ARP/邻居表。扩展计算必须考虑链路本地和全局地址。
- **8320 系列 -** 实施共享 ARP/邻居表，其中每个 IPv6 全局地址均使用两个表条目。扩展计算不需要包含链路本地地址。
- **8400 系列 -** 实施独立 ARP/邻居表。扩展计算不需要包含链路本地地址。

计算 IPv6 扩展需要了解每个客户端将分配多少个全局 IPv6 地址。如果全局地址数量未知，最好首先依靠每客户端三个全局地址。回到上一个示例，具有 14,400 个客户端设备的组织将使用约 43,400 个 IPv6 全局地址。可参考交换机数据表或文档，以便确定该交换机是否能够满足 IPv6 邻居的扩展要求。下表提供了对于本机 IPv4、本机 IPv6 和双堆栈部署，ArubaOS 和 ArubaOS-CX 交换机的最大扩展数。当使用 Aruba 交换机作为无线模块聚合层时，可参考这些扩展数量来提供无线模块中可支持的最大客户端设备数量（无线和动态分段）：

交换机系列	仅限 IPv4 的最大客户端数	最大本机 IPv6 客户端数 *	最大双堆栈客户端数 *
Aruba 3810 系列 (版本 16.04)	25,000	6,250	5,000

Aruba 5400R 系列 (版本 16.04)	25,000	6,250	5,000
Aruba 8320 系列 (版本 10.01)	49,000	20,000	17,000
Aruba 8400 系列 (版本 10.01)	82,000	21,300	21,300

**假设每个主机均被分配了 3 个 IPv6 全局地址*

表 23 *Aruba 交换机可扩展性*

请注意，已计算了上表中的本机 IPv6 和双堆栈扩展数，假设每主机分配了三个全局 IPv6 地址。如果部署需要支持额外全局地址，则该表将不适用。提醒一下，Aruba 最佳实践要求减去 20%，以适应未来的设备增长。

NOTE

"园区参考架构"部分中讨论了扩展超过 64,000 个主机地址的策略和架构。Aruba 移动优先架构可通过实施多个 MC 群集（每个均有自己的聚合层）进行扩展，以便支持每 MM 最多 100,000 个客户端。

无线模块冗余

Aruba 移动优先冗余设计的一个重要方面是包含 MC 的无线模块的连接。控制器群集端接 AP 管理和控制隧道，以及无线和动态分段的客户端隧道。要启用冗余，每个群集至少包含两个 MC，并且能够最多扩展到四个或十二个群集成员（取决于控制器型号）。作为最佳实践，每个群集必须包含相同型号的成员。

群集中的每个 MC 均使用动态端口通道连接到一对 Aruba 交换机，从而形成链路聚合连接 (LAG)。启用了链路聚合控制协议 (LACP)，以验证对等可用性并提供第 2 层环路预防。除无线和动态分段主机的数量外，根据为部署选择了 2 层还是 3 层分层网络设计，还将 MC 连接到了核心或无线聚合层交换机。

在多个层上提供了无线模块内的冗余：

- **ArubaOS 8 群集** - 每个 AP 和客户端均建立到群集内主要和辅助 MC 的隧道。这可确保在实时升级或 MC 中断时，AP 和客户端可获得网络路径
- **设备和链路冗余** - 每个 MC 均连接到两个 Aruba 交换机，如果这些交换机为核心交换机，则它们支持网络虚拟化功能 (NVF)，如果它们是无线聚合层交换机，则支持 LAG。这可确保在交换机中断或发生链路故障时，MC、AP 和客户端始终可获得网络路径
- **路径冗余** - 链路聚合控制协议 (LACP) 是 IEEE 802.3ad 标准的一部分，可确保所有路径完全冗余。LACP 是一种活动协议，其可使交换机对等体检测对等设备及其连接端口的运行状态
- **第一跳路由器冗余** - 网络必须确保在发生默认网关故障时继续转发数据包。第一跳路由器冗余由支持 NVF 的 Aruba 交换机本机提供，无需实施第一跳路由冗余协议，例如 VRRP

在为所有移动优先参考架构实施 NVF 的 Aruba 交换机对之间分配 LAG 中的 MC 端口。对于 MC 连接到的交换机，所选型号将取决于为该部署选择的 2 层或 3 层分层网络设计以及支持的无线客户端数量。支持无线模块的交换机可以是 Aruba 3810M 的堆栈，为虚拟交换框架 (VSF) 配置的一对 Aruba 5400R，也可以是为 MC-LAG 配置的一对 Aruba 8320s/8400s。

Aruba 3810M 交换机

下图展示了如何将 MC 群集连接到在核心层、核心/聚合层或无线聚合层中部署的 Aruba 3810M 交换机堆栈。Aruba 堆叠架构对控制和数据平面均进行虚拟化，从而使 3810M 交换机堆栈能够转发流量，以及作为单个虚拟交换机加以配置和管理。

在该示例中，每个 MC 中的两个或更多个 1 千兆或 10 千兆以太网端口被配置为 LAG，并且在堆栈中的 Aruba 3810M 交换机之间进行分配。这些交换机端口在 Aruba MC 上被配置为动态端口通道，在 Aruba 3810M 交换机上被配置为 LACP 中继。

群集管理和客户端 VLAN 的第一跳路由器冗余由 Aruba 3810M 交换机堆栈本机提供，这些交换机为每个 VLAN 提供默认网关。该堆栈中的一个 Aruba 3810M 交换机以主交换机角色运行，而第二个交换机作为备用交换机运行。可自动或手动分配交换机角色。主交换机在正常运行过程中提供 IP 转发，备用交换机在主交换机出现故障时提供备份。

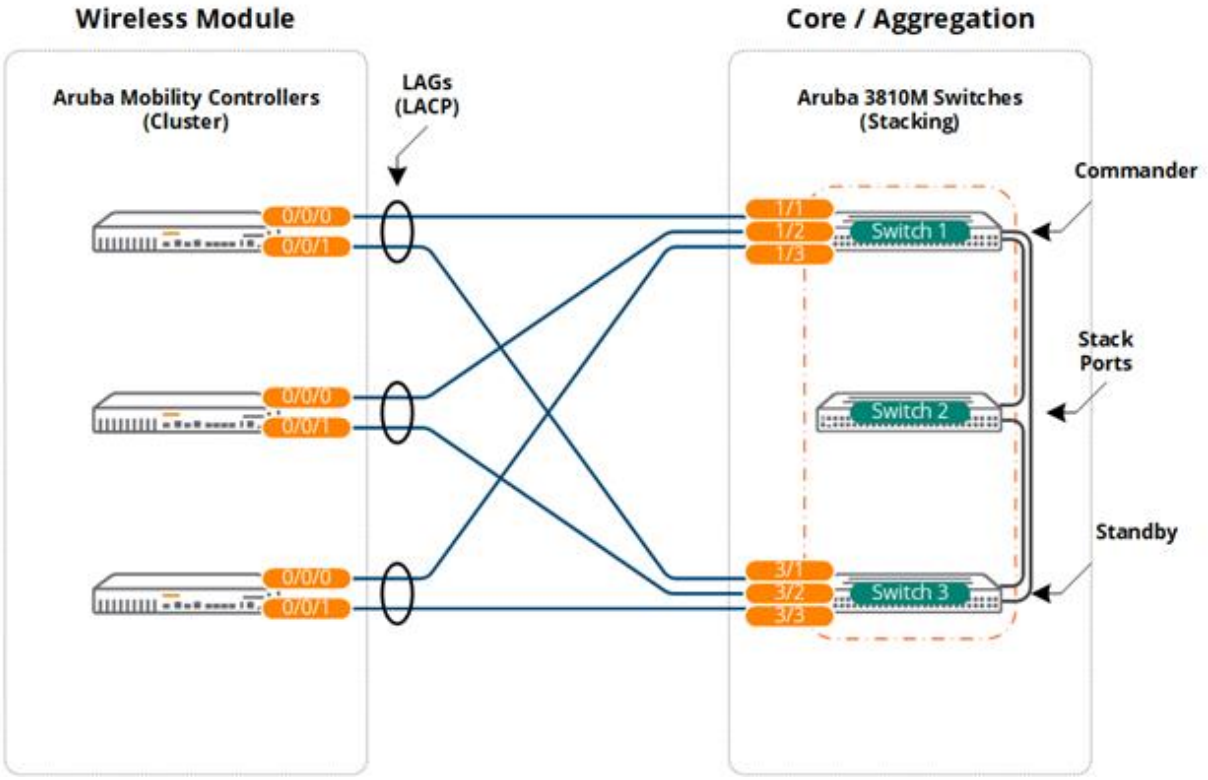


图 117 *使用堆叠的核心/聚合层*

Aruba 5400R 交换机

图 112 展示了如何将 MC 群集连接到针对 VSF 进行了配置并且已部署在核心或无线聚合层中的一对 Aruba 5400R 交换机。Aruba VSF 架构对控制和数据平面均进行虚拟化，从而使所有 5400R 交换机对均能够转发流量，以及作为单个虚拟交换机加以配置和管理。

在该示例中，每个 MC 中的两个或更多个 1 千兆、10 千兆或 40 千兆以太网端口被配置为 LAG，并且在 Aruba 5400R 交换机对之间进行分配。这些交换机端口在 Aruba MC 上被配置为动态端口通道，在 Aruba 5400R 交换机上被配置为 LACP 中继。

群集管理和客户端 VLAN 的第一跳路由器冗余由 Aruba 5400R 交换机的 VSF 对本机提供，这些交换机为每个 VLAN 提供默认网关。一个 Aruba 5400R 交换机以“主”交换机角色运行，而第二个交换机作为备用交换机运行。可自动或手动分配交换机角色。“主”交换机在正常运行过程中提供 IP 转发，同时“备用”交换机在“主”交换机出现故障时提供备份。

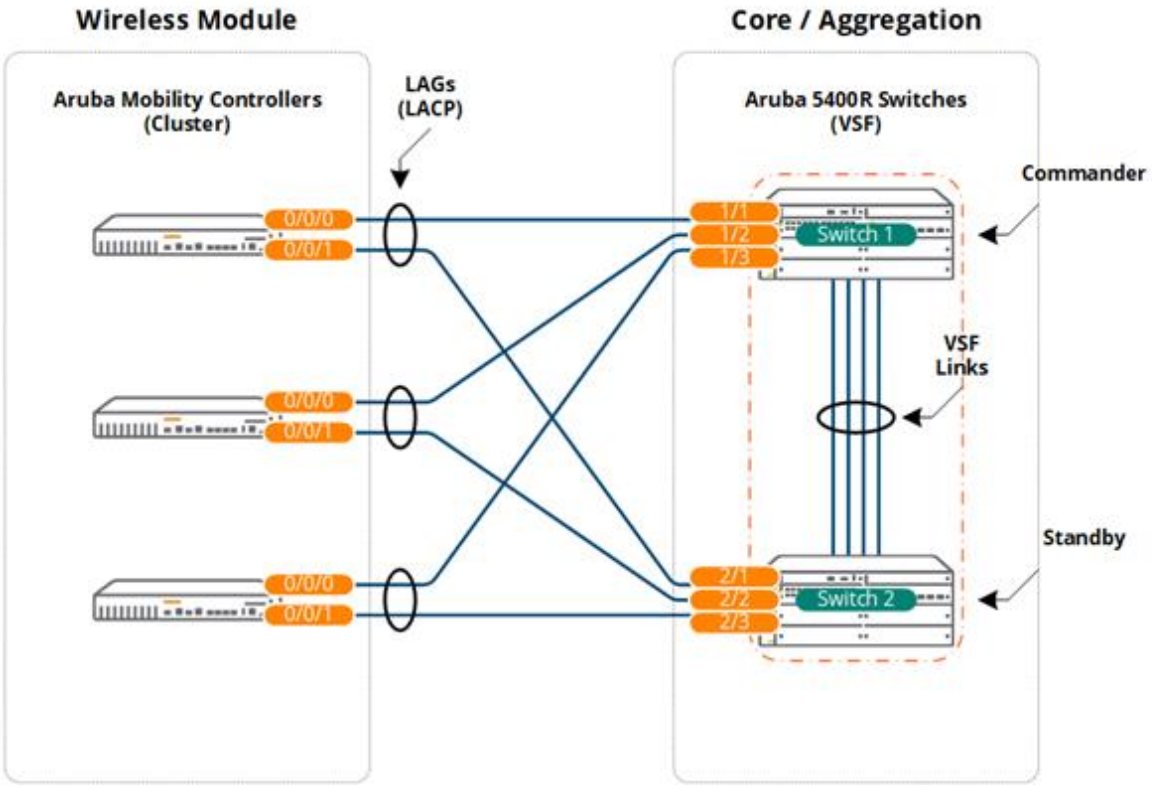


图 118 *使用虚拟交换框架的核心/聚合层*

Aruba 8320/8400 交换机

下图展示了如何将 MC 群集连接到已针对多信道 LAG 进行了配置并且部署在核心或无线聚合层中的一对 Aruba 8320 或 8400 交换机。Aruba MC-LAG 架构对数据平面进行虚拟化，从而使所有 8320/8400 交换机均能够作为单个虚拟交换机转发流量。与 Aruba 堆叠或 VSF 架构不同，每个 8230/8400 均独立加以配置和管理。

在该示例中，每个 MC 中的两个或更多个 1 千兆、10 千兆或 40 千兆以太网端口被配置为 LAG，并且在 Aruba 8320/8400 交换机对之间进行分配。这些交换机端口在 Aruba MC 上被配置为动态端口通道，在 Aruba 8320/8400 交换机上被配置为 MC-LAG。

群集管理和客户端 VLAN 的第一跳路由器冗余由 Aruba 8320/8400 交换机的 MC-LAG 对本机提供，这些交换机为每个 VLAN 提供默认网关。活动网关功能已启用，以便使每个 VLAN 都能够在这两个交换机上提供 IP 转发和故障切换。

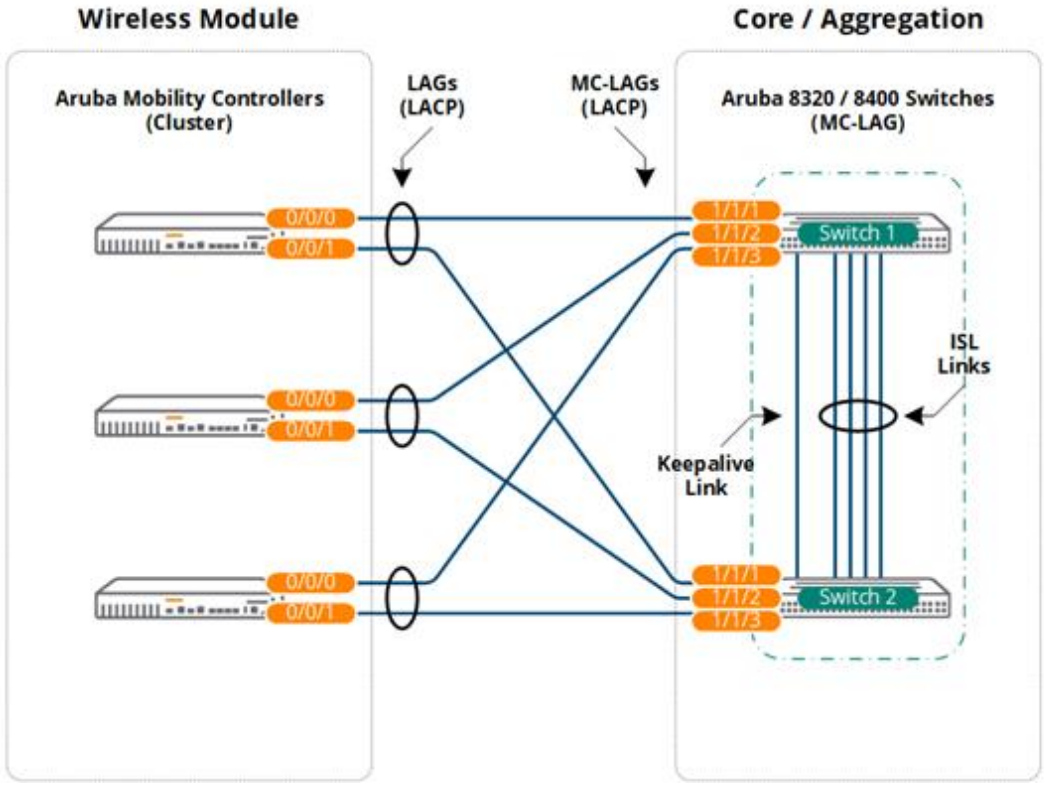


图 119 *使用多机箱 LAG 的核心/聚合层*

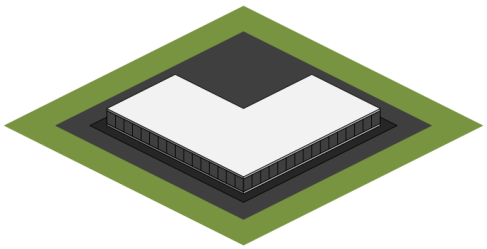
参考架构

本节所述的移动优先参考架构适用于小型、中型和大型楼宇，以及由多个不同大小楼宇组成的园区。为每个架构提供一个方案，以便为模块化网络和无线模块设计提供基础。每个架构还基于先前设计，从而在接入层和客户端数量增加时添加更多层。

小型办事处

方案

以下参考设计针对由单个楼层组成的小型办事处。该楼宇包括一个 MDF/服务器机房，以及使用多模光纤连接到 MDF 的一个 IDF。该楼宇最多支持 150 名员工，并且需要 15 个 802.11ac Wave 2 接入点来提供完全 2.4GHz 和 5GHz 覆盖范围。



楼宇特点：

- 1 层/总面积 20,000 平方英尺
- 150 名员工/300 个并发 IPv4 客户端
- 15 个 802.11ac Wave 2 接入点
- 1 个组合服务器机房/配线柜 (MDF)
- 1 个配线柜 (IDF)

图 120 *小型办事处特点*

该楼宇只有两个配线柜，因此在核心层与接入层之间不需要聚合层。该楼宇将实施 2 层模块化网络设计，其中接入层交换机和模块直接连接到折叠的核心/聚合层。此 2 层模块化网络设计还可适应具有更大面积和更多楼层（如果需要）的小型楼宇。

以下是模块化网络架构和设计的摘要：

LAN 核心/聚合：

- 具有混合端口的群集或交换机堆栈：
  - SFP/SFP+（接入层互连）
  - 10/100/1000BASE-T 端口（模块连接）
- IP 路由
- 到接入层设备的第 2 层链路聚合和模块连接

LAN 接入：

- 每配线柜两个或更多交换机的堆栈
  - SFP/SFP+（核心/聚合层互连）
  - 具有 PoE+ 的 10/100/1000BASE-T（边缘端口）
- 到核心/聚合层设备的第 2 层链路聚合
- 802.11ac Wave 2 AP

根据楼宇的面积以及无线密度和容量要求计算了此假设方案所需的 AP 数量。假设每个 AP 提供 1,200 平方英尺的覆盖范围，已确定使用 15 个 AP 合适。此方案中的每个 AP 均支持 20 个客户端。

应使用站点调查来确定实际 AP 数量以及它们针对生产环境的布局，该调查考虑每个单独覆盖区域的密度要求。

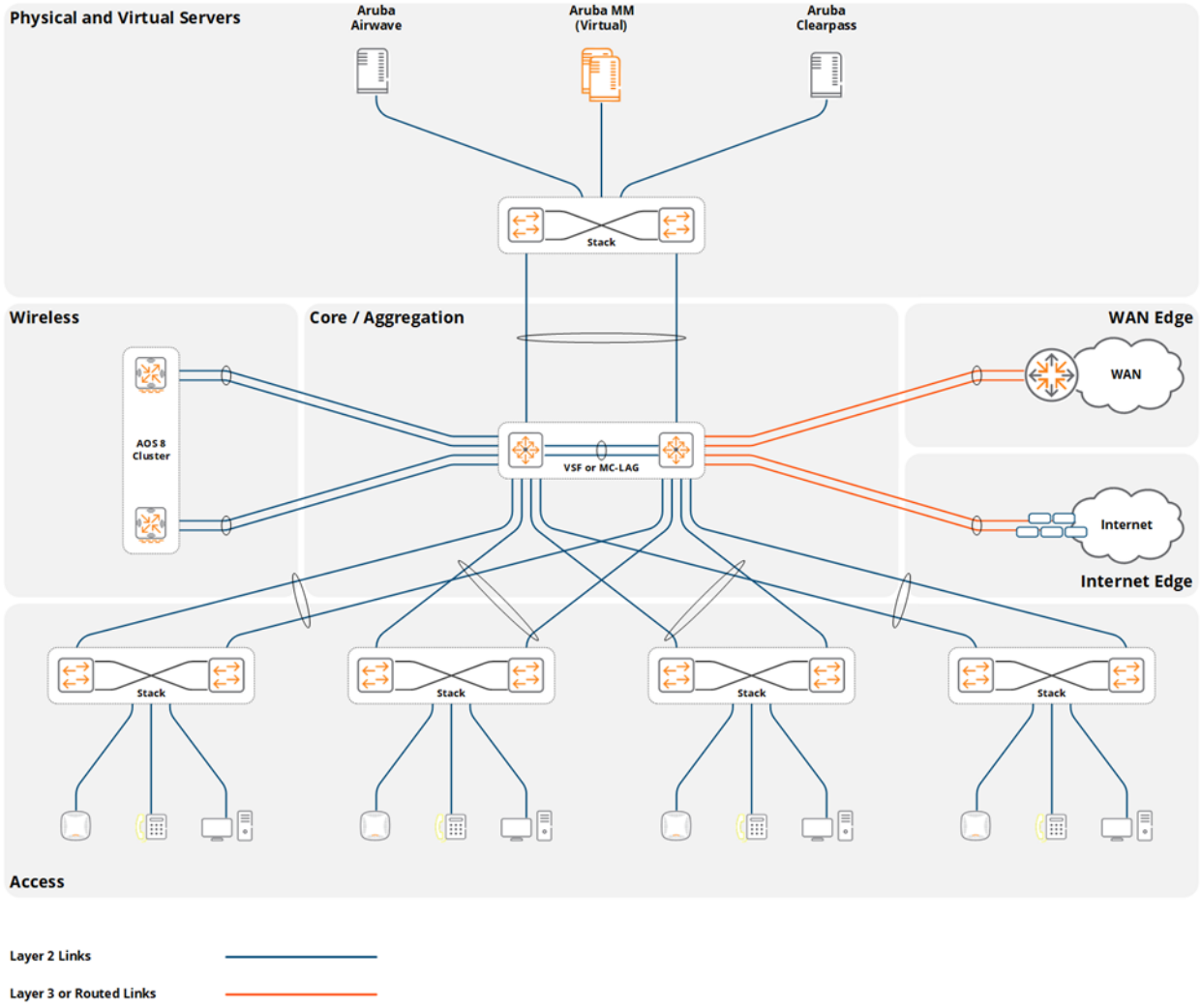


图 121 *小型办事处 2 层模块化网络设计*

考虑因素和最佳实践

无线 LAN 组件

Aruba 为小型部署提供无控制器和基于控制器的部署选择。无控制器架构是使用 Aruba Instant 接入点 (IAP) 提供的，而基于控制器的架构是使用 MC 和 Campus AP 提供的。这两个部署选择对此参考设计均有效，但本指南特别侧重于基于控制器的架构。

此方案中的小型楼宇包括部署在无线模块或服务器机房中的各种无线组件。需要使用 MM 和单个 MC 群集来适应 AP 和客户端数。群集成员的确切数量由已选择的硬件或虚拟 MC 模式来确定。出于冗余目的，MC 群集至少包含两个 MC。在单个 MC 出现故障时，每个群集成员都需要提供足够的容量和性能来运行无线网络。

以下表 24 提供了这些组件的摘要：

组件	描述	注释
Aruba MM (MM)	虚拟设备	需要 1 个，建议 2 个
Aruba MC	硬件或虚拟设备	最小 2 个（群集）
Aruba 接入点	802.11ac Wave 2 接入点	需要 15 个
Aruba ClearPass	虚拟设备	推荐

表 24 *小型楼宇无线 LAN 组件*

尽管此设计所需的 802.11ac Wave 2 AP 数量相对较少，但 Aruba 建议实施 MM，以便利用在无线为主要接入介质时提供关键任务无线服务所需的特定功能。在该设计中添加 MM 可提供集中式配置和监控，支持群集、AirMatch 和实时升级等功能，以及提供集中式应用程序支持（UCC 和 AppRF）。

尽管可以在没有 MM 的情况下部署基于控制器的解决方案，但这不是推荐的最佳实践。如果部署 MM 不可行，则可选择将 MC 作为一对独立设备加以部署，并对其进行配置，以实现主冗余。但以这种方式实施的部署模式将不支持群集，因此将缺少特定功能，例如快速故障切换、实时升级、AirMatch 和集中式应用程序支持。

冗余

在所有层间都提供了小型楼宇参考架构的冗余。建立基础网络的 2 层模块化网络设计中内置的冗余决定提供给模块的冗余级别。通常，断电造成的损失在实施并提供网络冗余方面是一个关键推动因素。大多数小型网络使用双电源，并且通常使用交换机堆栈作为它们主要冗余机制。

对于此方案，MM 和 MC 群集成员部署在服务器机房内，并直接连接到核心/聚合层交换机。要提供完全冗余，需要两个虚拟 MM 和一个硬件或虚拟 MC 群集：

- Aruba MM (MM)：
  - 两个虚拟 MM
  - L2 主冗余（主用/备用）

- 硬件 MC (MC)：
  - 一个硬件 MC 群集
  - 至少两个群集成员
- 虚拟 MC (MC)：
  - 一个虚拟 MC 群集
  - 至少两个群集成员
  - 单独虚拟服务器主机
- 接入点
  - AP 主控制器指向群集的 VRRP VIP
  - 使用群集冗余功能实现的快速故障切换

图 117 和 118 提供了虚拟和硬件群集成员如何连接到核心/聚合层的详细示例。硬件 MC 通过 LAG 组中配置的两个或更多个 1 千兆以太网端口直接连接到核心/聚合层交换机。LAG 端口成员在核心/聚合层堆栈成员之间进行分配。

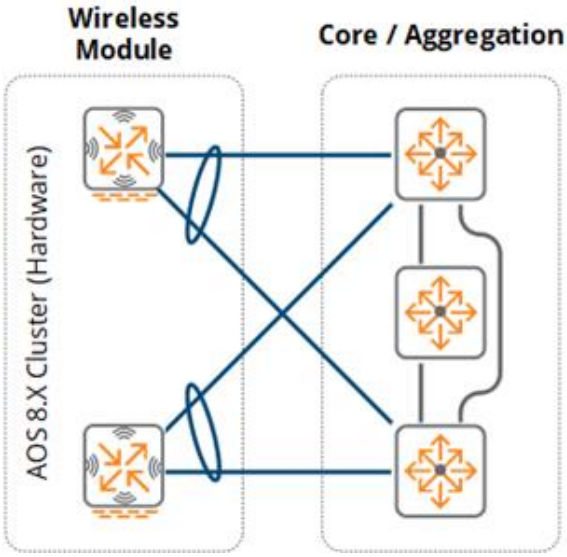


图 122 *硬件 MC 群集 – 核心/聚合层*

VMC 以逻辑方式连接到虚拟服务器主机中的虚拟交换机。虚拟主机服务器通过两个或更多个实施 802.3ad 链路聚合或专有负载分担/故障切换机制的 1 千兆或 10 千兆以太网端口直接连接到核心/聚合层交换机。每个端口均在核心/聚合层交换机堆叠成员之间进行分配。

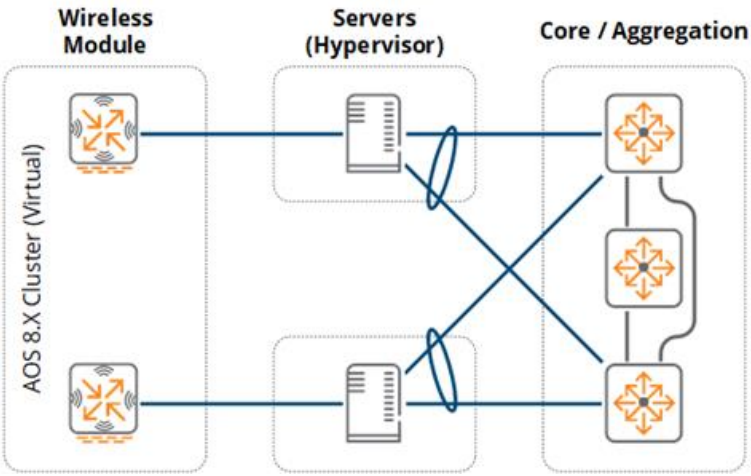


图 123 *虚拟 MC 群集 - 核心/聚合层*

MM 采用与 VMC 群集类似的方式加以部署。每个虚拟服务器主机均支持一个在主用/备用模式下运行的 VMM。尽管可为小型楼宇实施单个 MM，但实施备用不需要额外许可。此类模式的唯一网络开销将是虚拟服务器主机上的额外 CPU、内存和存储利用率。

NOTE

虚拟服务器的冗余依赖虚拟机监控程序。为防止网络受到链路、路径和节点故障的影响，虚拟机监控程序可实施 802.3ad 链路聚合或专有负载分担/故障切换机制。

虚拟 MC

可选择为小型楼宇环境部署虚拟 MC。如果部署了 VMC，则必须相应地扩展虚拟服务器基础设施，以便为群集中的每个 VMC 均提供必要的 CPU 和内存资源：

1. 每个 VMC 都应在不同的虚拟服务器主机中加以部署。此设计需要两个虚拟服务器主机
2. 必须相应地扩展虚拟服务器主机与核心/聚合层之间的上行链路，以便支持无线和动态分段的客户端吞吐量要求。安装在虚拟服务器主机上的以太网 PHY 会限制群集的吞吐量

虚拟服务器主机与其对等交换机之间的冗余可使用标准 802.3ad 链路聚合或虚拟机监控程序特定的专有负载分担和故障切换机制。每个虚拟机监控程序均支持特定的负载分担和故障切换机制，例如主动/备用、循环负载分担或链路聚合。为支持特定实施要求，应选择适当的冗余机制。

可扩展性

对于此方案，没有需要考虑的特定 LAN 可扩展性注意事项。核心/聚合层和接入层可轻松适应 AP 和客户端数，无需修改或从基本设计派生。必要时可在未来添加无线聚合层，以便容纳添加到网络的额外 AP 和客户端。

无线模块可扩展性也不是问题，因为可随时间扩展 MM 以及添加额外群集成员，以便随网络规模的增加而容纳更多 AP、客户端和交换容量。

作为最佳实践，Aruba 建议根据平台建议实施 MM-VA-50 MM 以及用于此类小型楼宇设计的两个硬件或虚拟 MC 组成的群集。为此设计选择的 MM 可进行扩展，以支持 50 个 AP、500 个客户端和 5 个 MC。

虚拟 LAN

对于此设计，核心/聚合层提供第 2 层传输（通过 802.1q 中继进行的 VLAN 扩展），并且使用第 3 层接口端接来自接入层和无线模块的所有 VLAN。Aruba 建议在整个网络中使用已标记的 VLAN。

根据安全性和策略模式，无线模块由一个或多个客户端 VLAN 组成。对于单个 VLAN 设计，所有无线和动态分段的客户端均被分配一个公共 VLAN，角色和策略确定每个客户端的相应网络接入级别。单个 VLAN 从核心/聚合层交换机扩展到每个物理或虚拟 MC 群集成员。可根据需要添加和扩展其他 VLAN。例如，出于策略合规性目的，移动优先设计可能需要将单独 VLAN 分配给无线和动态分段的客户端。

核心/聚合层与每个 MC 群集成员之间至少需要两个 VLAN。一个 VLAN 专用于管理和 MM 通信，而第二个 VLAN 用于客户端流量。为实现无缝移动性，所有 VLAN 在群集成员之间都是通用的。核心/聚合层交换机配置有第三层接口和寻址，以便作为每个 VLAN 的默认网关运行。Aruba 堆叠架构本机提供了第一跳路由器冗余。

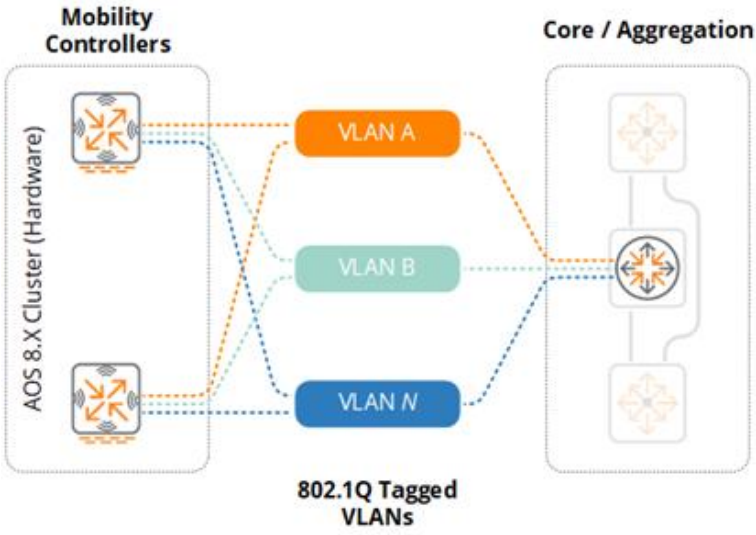


图 124 *硬件 MC 群集 - VLAN*

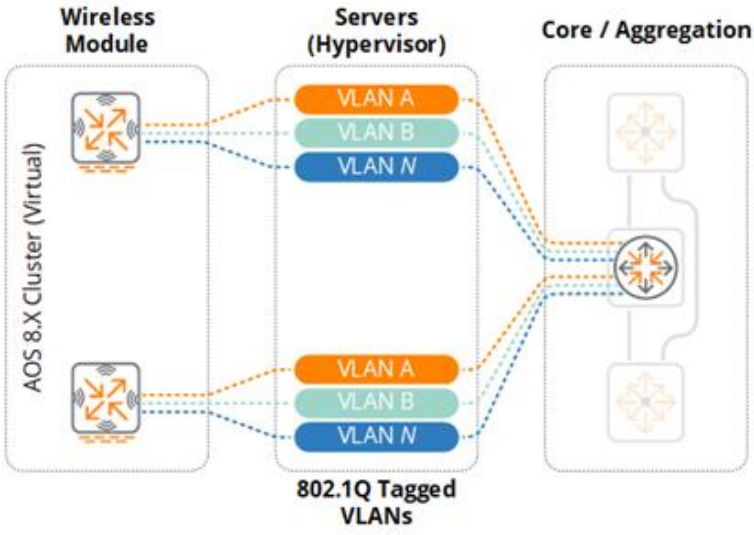


图 125 *虚拟 MC 群集 - VLAN*

作为最佳实践，Aruba 建议在无线模块中实施唯一 VLAN ID。这可实现未来在不中断网络内其他层的情况下引入聚合层。这还有助于创建较小的第 2 层域，这对于减少第 2 层不稳定性至关重要。源自网络中其他层或模块的操作更改、循环或错误配置可能会对无线模块产生不利影响，除非已使用相应大小的第 2 层域对网络进行了正确分段。

平台建议

以下图 121 为支持 15 个 AP 和 300 个并发客户端的小型楼宇方案提供了平台建议。基于功能、性能和扩展功能，做出了“良好、更好、最佳建议”。这些建议特定于方案，您可以自己酌情替代这些建议。

		良好	更好	最好
交换	核心/聚合层	2930	3810	3810
	接入层	2930	2930	2930
无线	MM	MM-VA-50		
	虚拟 MC 群集	MC-VA-50		
	MC 群集	7024	7030	
	802.11ac Wave 2 接入点	300 系列	310 系列	330/340 系列

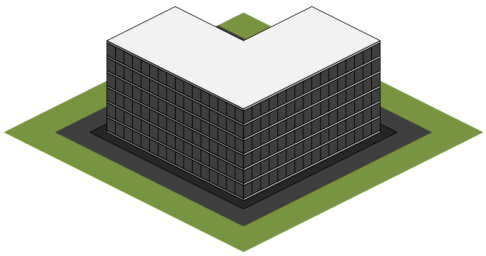
Features, Performance & Scaling

图 126 *小型楼宇平台建议*

中型办事处

方案

以下参考设计针对六层楼的中型办公楼。该楼宇包括一个数据中心，此数据中心通过单模光纤连接到每层楼的 MDF。每一层均包括三个 IDF，它们通过多模光纤连接到 MDF。该楼宇最多支持 1,500 名员工，并且需要 120 个 802.11ac Wave 2 AP 来提供完全 2.4GHz 和 5GHz 覆盖范围。



楼宇特点：

- 6 层/总面积 150,000 平方英尺
- 1,500 名员工/3,000 个并发 IPv4 客户端
- 120 个 802.11ac Wave 2 接入点
- 1 个计算机室
- 每层 1 个 MDF（共 6 个）
- 每层 2 个 IDF（共 12 个）

图 127 *中型办事处特点*

由于此设计使用 MDF 和 IDF 实施结构化布线设计，因此需要使用聚合层来连接接入层。该楼宇还将实施 3 层模块化网络设计，其中接入层交换机连接到每个 MDF 中的聚合层交换机，然后这些聚合层交换机又直接连接到核心层。此模块化网络设计还包括用于计算机室的额外聚合层，这有助于实现可扩展性、聚合和故障域隔离。

以下列表概括了模块化网络架构和设计：

- **LAN 核心：**具有光纤端口的交换机群集：
  - SFP/SFP+（模块连接）
- 到聚合层设备和模块的 IP 路由

LAN 聚合：

- 用于每个 MDF 的具有光纤端口的两交换机堆栈：
  - SFP/SFP+/QSFP+（核心层和接入层互连）
- 到核心层设备的 IP 路由
- 到接入层设备的第 2 层链路聚合

LAN 接入：

- 用于每个 MDF 和 IDF 的由两个或更多个交换机组成的堆栈：
  - SFP/SFP+（聚合层互连）
  - 具有 PoE+ 的 10/100/1000BASE-T（边缘端口）
- 到聚合层设备的第 2 层链路聚合
- 802.11ac Wave 2 AP

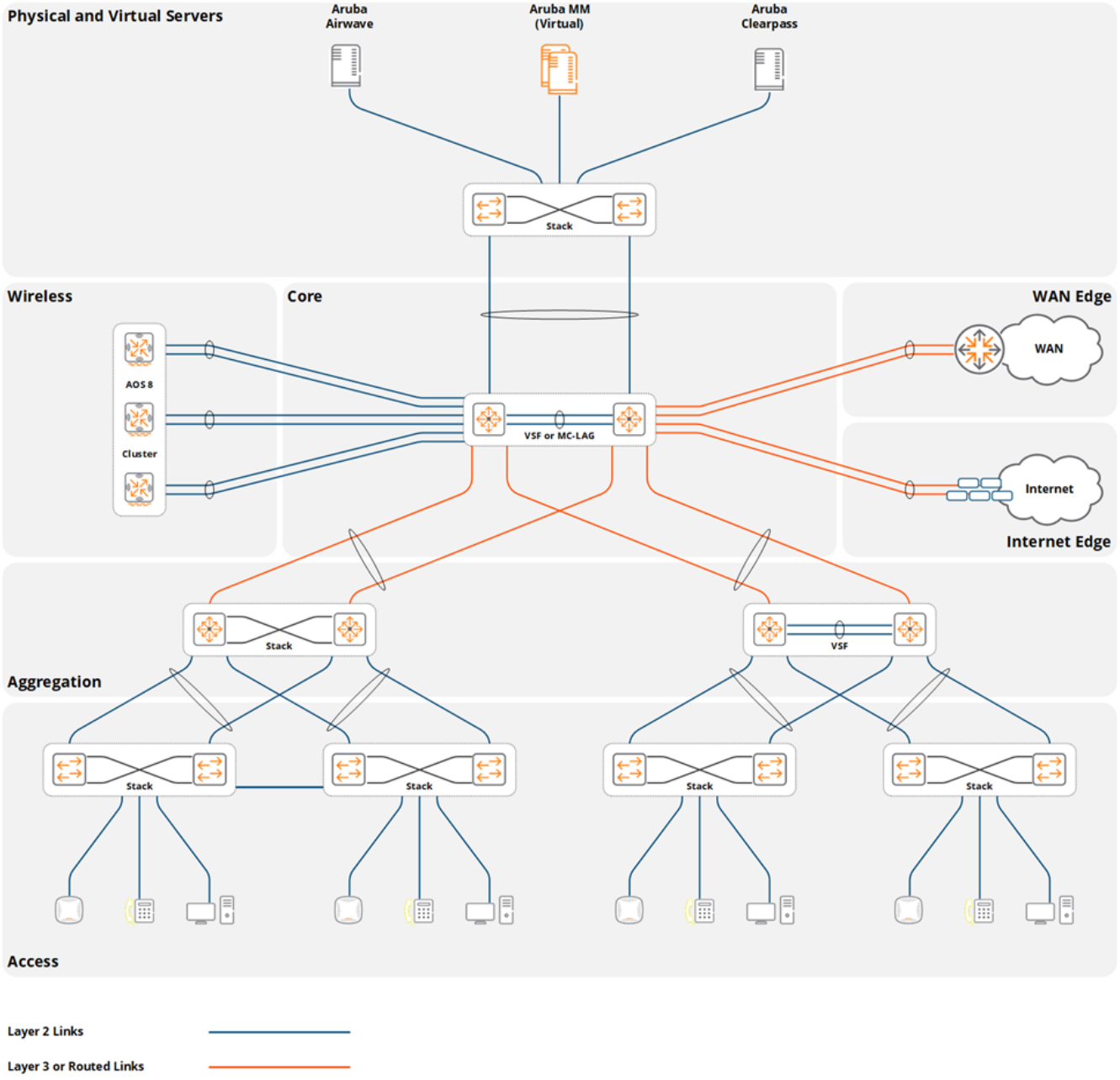


图 128 *中型办事处 3 层模块化网络设计*

根据楼宇的面积、无线密度和容量要求计算了此假设方案所需的 AP 数量。根据每个 AP 将提供 1,200 平方英尺的覆盖范围并且支持 25 个客户端这一假设，已确定将需要 120 个 AP。

应使用站点调查来确定实际 AP 数量以及它们针对生产环境的布局，该调查考虑每个单独覆盖区域的密度要求。

考虑因素和最佳实践

无线 LAN 组件

此方案中的中型楼宇包括部署在无线模块或服务器机房中的各种无线组件。为适应 AP 和客户端数，需要 MM 和单个 MC 群集。群集成员的数量由所选的 MC（硬件或虚拟）模式决定。出于冗余目的，MC 群集至少包含两个 MC。在单个 MC 出现故障时，每个成员均提供足够的容量和性能，以便使无线网络能够继续运行。

表 25 提供了这些组件的摘要：

组件	描述	注释
Aruba MM (MM)	虚拟设备	需要 1 个 MM，建议 2 个
Aruba MC	硬件或虚拟设备	至少需要 2 个 MC（群集）
Aruba 接入点	802.11ac Wave 2 接入点	需要 120 个 AP
Aruba ClearPass	虚拟设备	推荐

表 25 *中型楼宇 - 无线 LAN 组件*

冗余

在所有层间都提供了中型楼宇参考架构的冗余。建立基础网络的 3 层模块化网络设计中内置的冗余决定提供给模块的冗余级别。Aruba 建议使用 NVF 功能（堆叠或 MC LAG）来提供网络和链路冗余，以及使用冗余电源来最大程度地提高网络可用性和弹性。

对于此方案，MM 和群集成员部署在计算机室，并直接连接到核心或计算机室聚合层交换机。需要两个 VMM 和一个硬件或虚拟 MC 群集才能完全实现冗余：

- Aruba MM (MM)：
  - 两个虚拟 MM
  - L2 主冗余（主用/备用）
- 硬件 MC (MC)：
  - 一个硬件 MC 群集
  - 至少两个群集成员
- 虚拟 MC (VMC)：
  - 一个虚拟 MC 群集
  - 至少两个群集成员
  - 单独虚拟服务器主机
- 接入点
  - AP 主控制器指向群集的 VRRP VIP 地址
  - 使用内置群集冗余进行的快速故障切换

图 124 和 125 提供了虚拟和硬件群集成员如何连接到它们各自层的详细示例。硬件 MC 通过 LAG 组中配置的两个或更多个 1 千兆或 10 千兆以太网端口直接连接到核心层交换机。正在冗余核心/聚合层交换机之间分配的 LAG 端口成员。

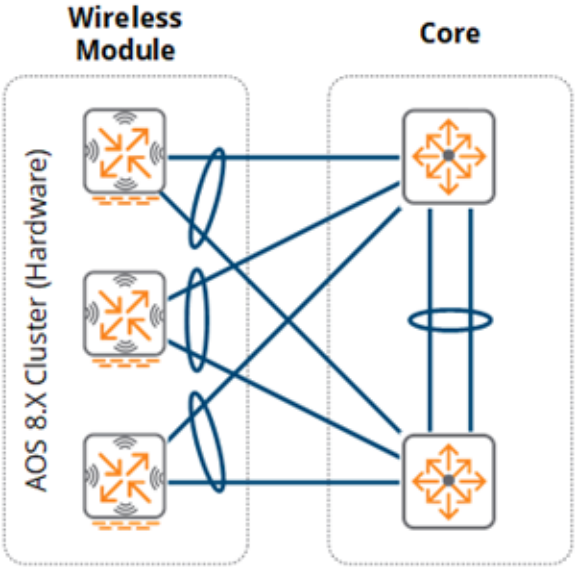


图 129 *硬件 MC 群集 – 核心层*

VMC 以逻辑方式连接到虚拟服务器主机中的虚拟交换机。虚拟主机服务器通过两个或更多个实施 802.3ad 链路聚合或专有负载分担和故障切换机制的 1 千兆或 10 千兆以太网端口直接连接到计算机室聚合层交换机。每个端口均在冗余计算机室聚合层交换机之间进行分配。

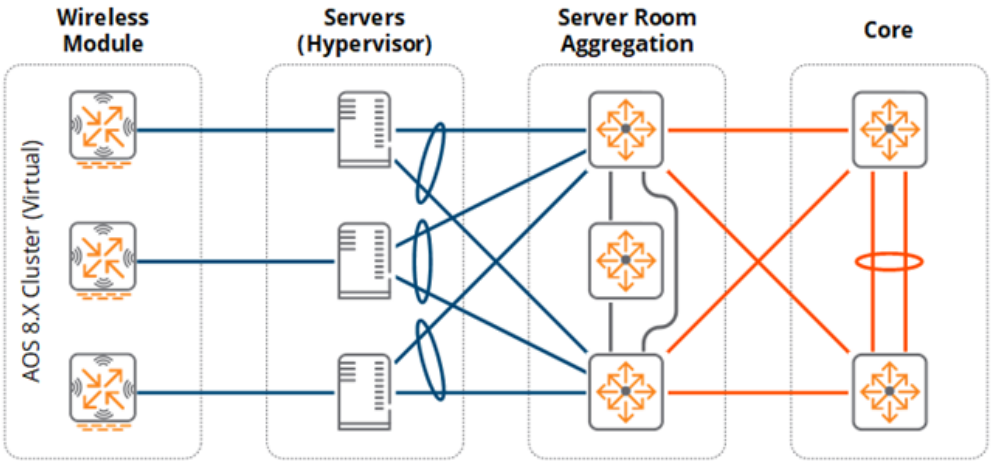


图 130 *虚拟 MC 群集 - 计算机室聚合层*

MM 采用与 VMC 群集类似的方式加以部署。每个虚拟服务器主机均支持一个在主用/备用模式下运行的虚拟 MM。

NOTE

虚拟服务器的冗余取决于虚拟机监控程序。为防止链路、路径和节点故障，虚拟机监控程序可实施 802.3ad 链路聚合或专有负载分担和故障切换机制。

虚拟 MC

对于中型楼宇部署，VMC 也可以作为硬件 MC 的替代方案加以部署。如果部署了 VMC，则必须相应地扩展虚拟服务器基础设施，以便提供必要的 CPU 和内存资源来支持群集中的每个虚拟 MC：

1. 群集中的每个 VMC 都应在不同的虚拟服务器主机中加以部署。对于此设计，需要两个虚拟服务器主机。
2. 必须相应地扩展虚拟服务器主机与计算机室聚合层之间的上行链路，以便支持无线和动态分段的客户端吞吐量要求。安装在虚拟服务器主机上的以太网 PHY 会限制群集的吞吐量。

虚拟服务器主机与其对等交换机之间的冗余可使用标准 802.3ad 链路聚合或虚拟机监控程序特定的专有负载分担和故障切换机制。每个虚拟机监控程序均支持特定的负载分担和故障切换机制，例如主动/备用、循环负载分担或链路聚合。为支持每个站点的特定实施要求，应选择适当的冗余机制。

可扩展性

对于此方案，没有需要考虑的特定 LAN 可扩展性注意事项。核心/聚合层和接入层可轻松适应 AP 和客户端数，无需修改或从该设计派生。未来在将更多 AP 和客户端添加到网络时，可添加无线聚合层。

无线模块扩展也不是问题，因为可随时间扩展 MM 以及添加额外群集成员，以便随网络的扩展而容纳更多 AP、客户端和交换容量。

对于这种中型楼宇设计，Aruba 建议根据平台建议实施 MM-VA-500 MM 以及由两个或更多个硬件或虚拟 MC 组成的群集。为此设计选择的 MM 可进行扩展，以支持 500 个 AP、5,000 个客户端和 50 个 MC。

虚拟 LAN

在中型办事处设计中，核心或计算机室聚合层端接来自 MC 的所有 VLAN。使用 802.1Q 中继将这些 VLAN 从 MC 扩展到核心或计算机室聚合层。Aruba 建议尽可能使用已标记的 VLAN 来提供额外环路预防。根据安全性和策略模式，无线模块由一个或多个用户 VLAN 组成。对于单个 VLAN 设计，所有无线和动态分段的客户端均被分配到公共 VLAN ID。角色和策略确定在网络上为每个用户提供的访问级别。单个 VLAN 从核心或计算机室聚合层交换机扩展到了每个物理或虚拟 MC 群集成员。可根据需要添加和扩展其他 VLAN。例如，出于策略合规性原因，移动优先设计可能需要将单独 VLAN 分配给无线和动态分段的客户端。

核心或计算机室聚合层与每个 MC 群集成员之间至少需要两个 VLAN。一个 VLAN 专用于管理和 MM 通信，而第二个 VLAN 被映射到客户端。为实现无缝移动性，所有 VLAN 在群集成员之间都是通用的。核心或计算机室聚合层交换机定义了基于 VLAN 的 IP 接口，并且作为每个 VLAN 的默认网关运行。Aruba 堆叠架构本机提供了第一跳路由器冗余。

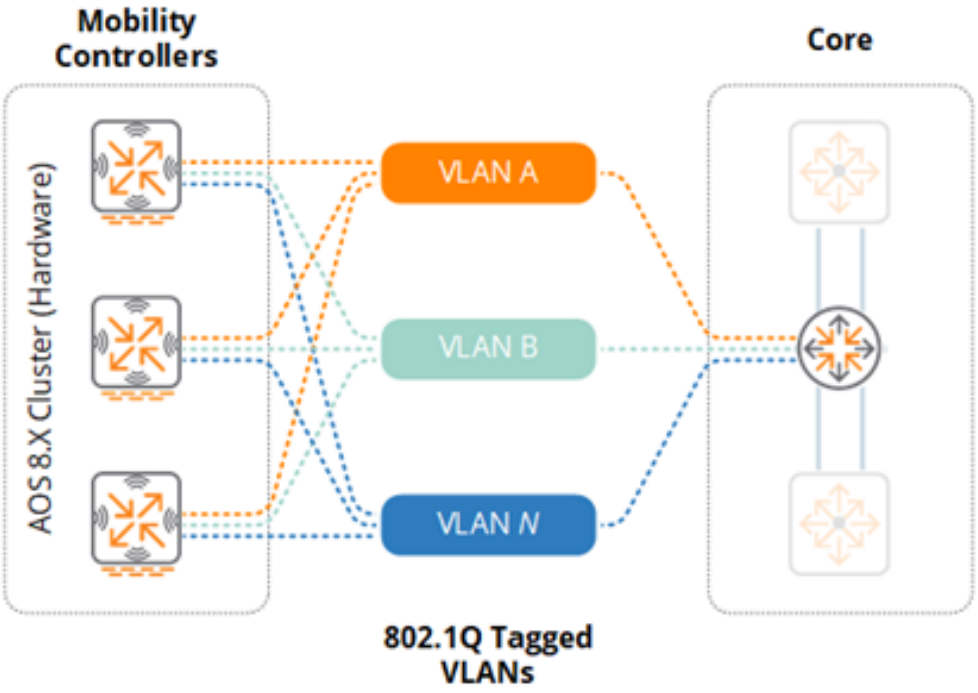


图 131 *硬件 MC 群集 - VLAN*

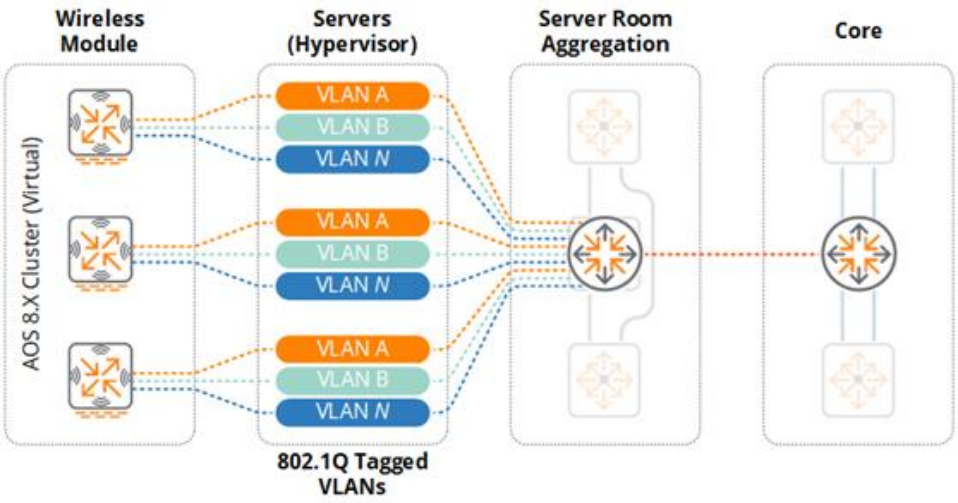


图 132 *虚拟 MC 群集 - VLAN*

作为最佳实践，Aruba 建议在无线模块中实施唯一 VLAN ID。这可实现未来在不中断网络内其他层的情况下引入聚合层。这还可实现创建更小的第 2 层域。以这种方式对网络进行分段可减少第 2 层不稳定性，以及保护无线模块，防止其受到来自其他层或网络模块的操作变更、循环或错误配置的影响。

平台建议

下图为支持 120 个 AP 和 3,000 个并发客户端的中型楼宇方案提供了平台建议。基于功能、性能和可扩展性，做出了良好、更好、最佳建议。这些建议基于所描述的方案，并且可根据网络管理员的判断而改变。

		Good	Better	Best
Switching	Core Layer	3810	5400R	8230
	Aggregation Layer	3810	5400R	8320
	Access Layer	2930	3810	5400R
	Wireless Module	3810	5400R	8320
Wireless	Mobility Masters	MM-VA-500		
	Virtual Mobility Controller Cluster	MC-VA-250		
	Mobility Controller Cluster	7205	7210	
	802.11ac Wave 2 Access Points	300 Series	310 Series	330/340 Series

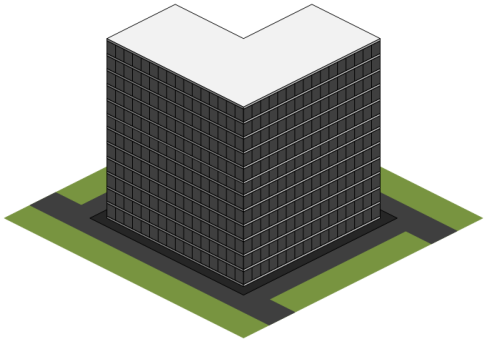
Features, Performance & Scaling

图 133 *中型楼宇平台建议*

大型办事处

方案

以下参考设计针对由 12 个楼层组成的大型办事处。该楼宇包括一个数据中心，此数据中心通过单模光纤连接到每层楼的 MDF。每一层还包括三个 IDF，它们通过多模光纤连接到 MDF。该楼宇最多支持 3,000 名员工，并且需要 300 个 802.11ac Wave 2 AP 来提供完全 2.4GHz 和 5GHz 覆盖范围。



楼宇特点：

- 12 层/总面积 360,000 平方英尺
- 3,000 名员工/6,000 个并发 IPv4 客户端
- 300 个 802.11ac Wave 2 接入点
- 1 个计算机室
- 每层 1 个 MDF（共 12 个）
- 每层 2 个 IDF（共 24 个）

图 134 *大型办事处特点*

大型楼宇设计使用 MDF 和 IDF 实施结构化布线设计，这需要使用聚合层来连接接入层。该楼宇实施 3 层模块化网络设计，其中接入层交换机通过每个 MDF 中的聚合层交换机进行连接，然后这些聚合层交换机又直接连接到核心层。此模块化网络设计还包括用于计算机室和无线模块的额外聚合层，从而实现可扩展性、聚合和故障域隔离。

以下列表概括了模块化网络架构和设计：

LAN 核心：

- 具有 10G 和 40G 混合光纤端口的一对冗余交换机：
  - SFP/SFP+/QSFP+（聚合层互连）
- 到聚合层设备和模块的 IP 路由
- 可选 NVF 功能 (MC LAG)

LAN 聚合：

- 每 MDF 的具有光纤端口的两交换机堆栈：
  - SFP/SFP+/QSFP+（核心层和接入层互连）
- NVF 功能 (MCLAG/VSX)
- 到核心层设备的 IP 路由

LAN 接入：

- 每 MDF 和 IDF 的由两个或更多个交换机组成的堆栈：
  - SFP/SFP+（聚合层互连）
  - 具有 PoE+ 的 10/100/1000BASE-T（边缘端口）
- 到接入层设备的第 2 层链路聚合
- 802.11ac Wave 2 AP

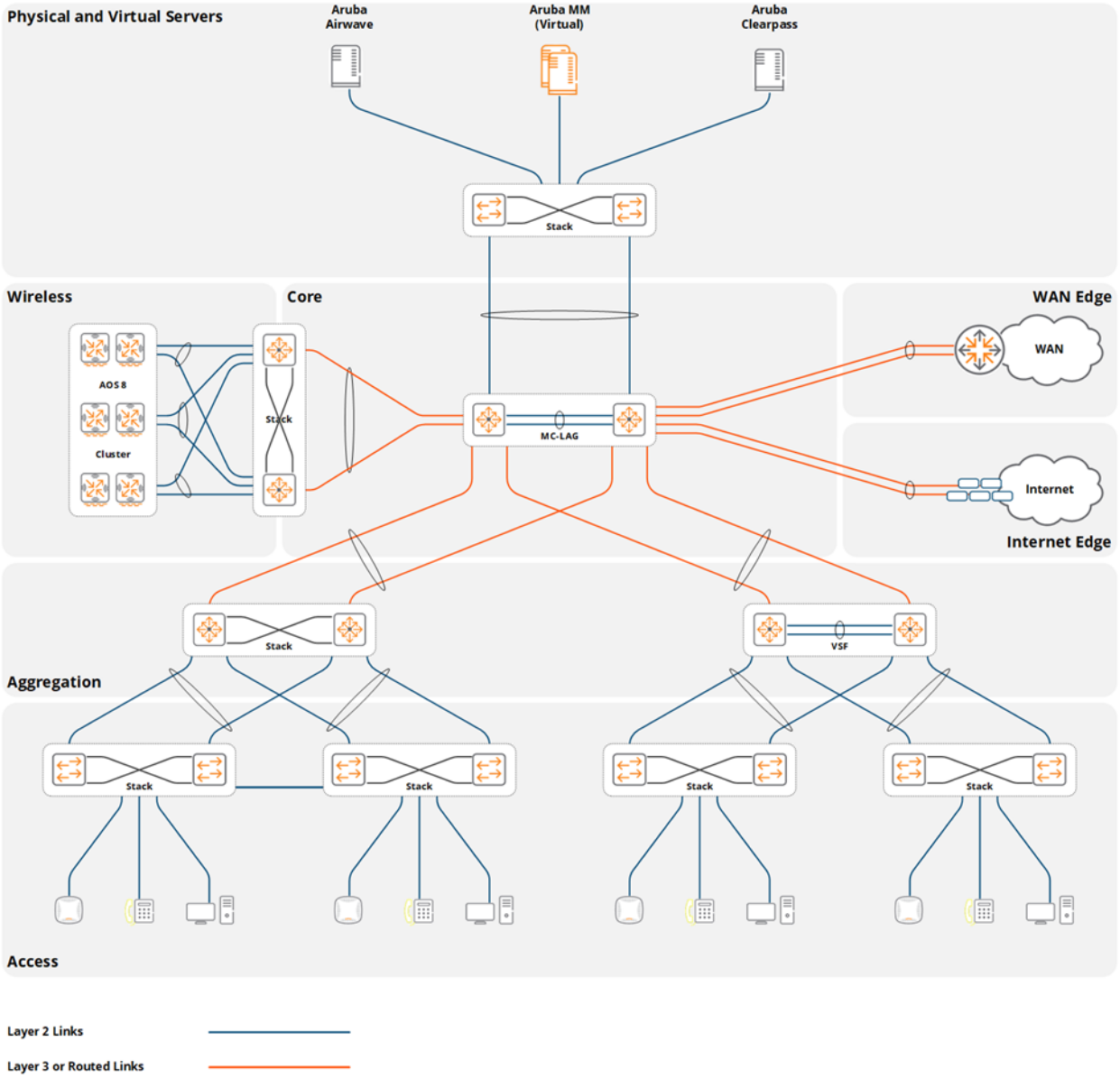


图 135 *大型办事处 – 3 层模块化网络设计*

根据楼宇的面积、无线密度和容量要求计算了此假设方案所需的 AP 数量。根据每个 AP 提供 1200 平方英尺的覆盖范围并且支持 20 个客户端这一假设，已确定将需要 300 个 AP。

应使用站点调查来确定实际 AP 数量以及它们针对生产部署的布局，该调查考虑每个覆盖区域的密度要求。

考虑因素和最佳实践

无线 LAN 组件

此方案中的大型楼宇包括部署在无线模块或服务器机房中的各种无线组件。为适应此方案的 AP 和客户端数，需要 MM 和单个 MC 群集。群集成员的数量由所选的硬件或虚拟 MC 模式决定。出于冗余目的，MC 群集至少包含两个 MC。在单个 MC 出现故障时，每个成员均提供足够的容量和性能，以便使无线网络能够继续运行。

表 26 提供了这些组件的摘要：

组件	描述	注释
Aruba MM (MM)	硬件或虚拟设备	需要 2 个
Aruba MC	硬件或虚拟设备	最小 2 个（群集）
Aruba 接入点	802.11ac Wave 2 接入点	需要 300 个
Aruba Airwave	硬件或虚拟设备	推荐
Aruba ClearPass	硬件或虚拟设备	推荐

表 26 *大型楼宇 - 无线 LAN 组件*

冗余

在所有层间都提供了大型楼宇架构的冗余。建立基础网络的 3 层模块化网络设计中内置的冗余决定提供给模块的冗余级别。Aruba 建议使用 NVF 功能（堆叠或 MC LAG）来提供网络冗余，以及使用冗余链路和电源来最大程度地提高网络可用性和弹性。Aruba 8400 在任何 Aruba 交换机中均可提供最大冗余功能，建议将其用于核心层、聚合层和无线聚合层。

对于此方案，MM 和移动群集成员部署在计算机室，并直接连接到无线聚合层或计算机室聚合层交换机。需要两个硬件或虚拟 MM 和一个硬件或虚拟 MC 群集才能完全实现冗余：

- Aruba MM (MM)：
  - 两个硬件或虚拟 MM
  - L2 主冗余（主用/备用）
- 硬件 MC (MC)：
  - 一个硬件 MC 群集
  - 至少两个群集成员
- 虚拟 MC (MC)：
  - 一个虚拟 MC 群集
  - 至少两个群集成员
  - 单独虚拟服务器主机

- 接入点
  - AP 主控制器指向群集的 VRRP VIP
  - 使用内置群集冗余进行的快速故障切换

以下图 131 和 132 提供了虚拟和硬件群集成员如何连接到它们各自层的详细示例。基于硬件的 MC 通过 LAG 中配置的两个或更多个 10 千兆以太网端口直接连接到核心层交换机。在冗余无线聚合层交换机之间分配的 LAG 端口成员。

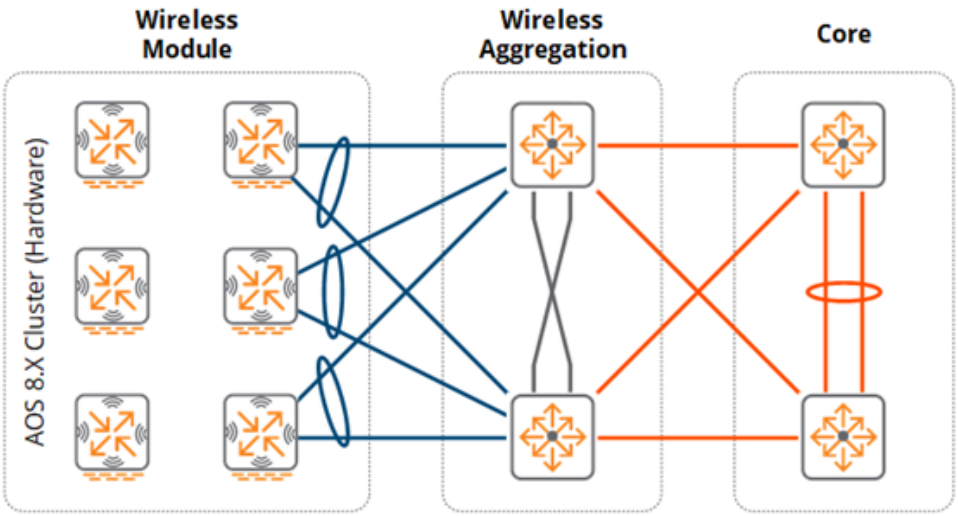


图 136 *硬件 MC 群集 - 无线聚合层*

VMC 以逻辑方式连接到虚拟服务器主机中的虚拟交换机。虚拟主机服务器通过两个或更多个实施 802.3ad 链路聚合或专有负载分担和故障切换机制的 10 千兆以太网端口直接连接到计算机室聚合层交换机。每个端口均在冗余计算机室聚合层交换机之间进行分配。

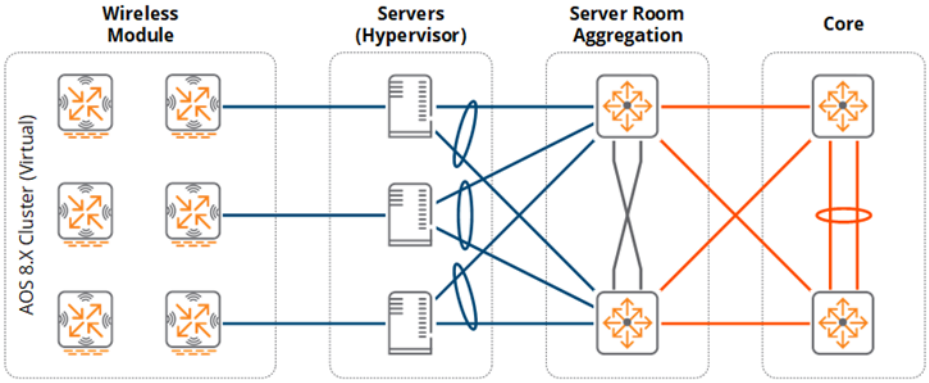


图 137 *虚拟 MC 群集 - 计算机室聚合层*

MM 采用与 VMC 群集类似的方式加以部署。每个虚拟服务器主机均支持一个在主用/备用模式下运行的虚拟 MM。

NOTE

虚拟服务器的冗余依赖虚拟机监控程序。为防止链路、路径和节点故障，虚拟机监控程序可实施 802.3ad 链路聚合或专有负载分担和故障切换机制。

虚拟 MC

对于大型楼宇部署，可选择部署 VMC。如果部署了 VMC，则必须相应地扩展虚拟服务器基础设施，以便为群集中的每个 VMC 均提供必要的 CPU 和内存资源：

1. 每个 VMC 都应在不同的虚拟服务器主机中加以部署。大型办事处设计需要两个虚拟服务器主机。
2. 必须相应地扩展虚拟服务器主机与计算机室聚合层之间的上行链路，以便支持无线和动态分段的客户端吞吐量要求。安装在虚拟服务器主机上的以太网 PHY 会限制群集的吞吐量。

虚拟服务器主机与其对等交换机之间的冗余可使用标准 802.3ad 链路聚合或虚拟机监控程序特定的专有负载分担和故障切换机制。每个虚拟机监控程序均支持特定的负载分担和故障切换机制，例如主动/备用、循环负载分担和链路聚合。为支持部署的特定实施要求，应选择适当的冗余机制。

可扩展性

大型办事处设计包括一个无线聚合层，其可容纳网络上的 6,000 个无线 IPv4 主机。作为一般最佳实践，Aruba 建议在 IPv4 和 IPv6 主机总数超过 4,094 个后，考虑使用无线聚合层。如果部署硬件 MC 并并将其直接连接到核心层，则需要使用无线聚合层。如果部署 VMC，则计算机室聚合层交换机提供聚合功能。

未来增长不是一个问题，因为可随时间轻松扩展 MM 以及添加额外群集成员，以便容纳更多 AP、客户端和交换容量。对于这种大型楼宇设计，Aruba 建议实施 MM-HW-5K 或 MM-VA-5K MM 以及由两个或更多个硬件或虚拟 MC 组成的群集。为此设计选择的 MM 可进行扩展，以支持 5,000 个 AP、50,000 个客户端和 500 个 MC。

虚拟 LAN

在大型办事处设计中，无线模块聚合层端接来自 MC 的所有第 2 层 VLAN。使用 802.1Q 中继将这些 VLAN 从 MC 扩展到其各自的聚合层交换机。Aruba 建议尽可能使用已标记的 VLAN 来提供额外环路预防。

根据已实施的安全性和策略模式，无线模块由一个或多个用户 VLAN 组成。对于单个 VLAN 设计，所有无线和动态分段的客户端均被分配到一个公共 VLAN ID，其角色和策略确定在网络上为每个用户提供的访问级别。单个 VLAN 从各自的聚合层交换机扩展到每个物理或虚拟 MC 群集成员。可根据需要添加和扩展其他 VLAN。例如，出于策略合规性原因，移动优先设计可能需要将单独 VLAN 分配给无线和动态分段的客户端。

每个聚合层交换机与各自 MC 群集成员之间至少需要两个 VLAN。一个 VLAN 专用于管理和 MM 通信，而第二个 VLAN 被映射到客户端。为了为客户端启用无缝漫游功能，所有 VLAN 在群集成员之间都是通用的。聚合层交换机已定义了基于 VLAN 的 IP 接口，并且作为每个 VLAN 的默认网关运行。Aruba 群集和堆叠架构本机提供了第一跳路由器冗余。

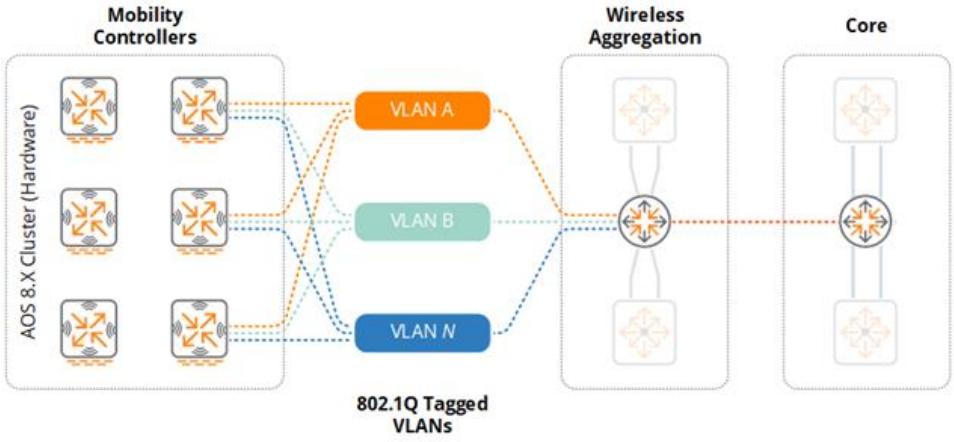


图 138 *硬件 MC 群集 - VLAN*

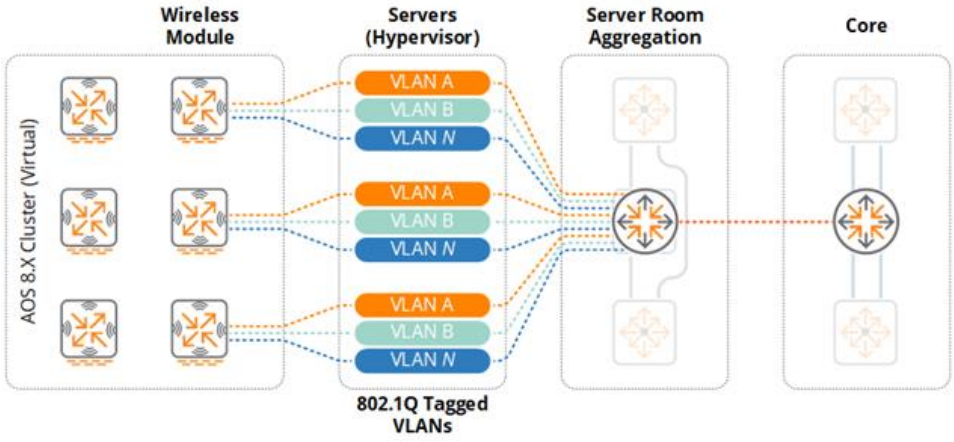


图 139 *虚拟 MC 群集 - VLAN*

作为最佳实践，Aruba 建议在无线模块中实施唯一 VLAN ID。这可实现未来在不中断网络内其他层的情况下引入聚合层。这还可实现创建更小的第 2 层域。以这种方式对网络进行分段可减少第 2 层不稳定性，以及保护无线模块，防止其受到来自其他层或网络模块的操作变更、循环或错误配置的影响。

平台建议

图 135 为基于支持 300 个 AP 和 6,000 个并发客户端这一假设的中型楼宇方案提供了平台建议。基于功能、性能和可扩展性，做出了良好、更好、最佳建议。这些建议基于所描述的方案，并且可根据网络管理员的判断而改变。

		Good	Better	Best
Switching	Core Layer	8320	8320	8400
	Aggregation Layer	8320	8320	8400
	Access Layer	2930	3810	5400R
	Wireless Module	8320	8320	8400
Wireless	Mobility Masters	MM-VA-5K or MM-HW-5K		
	Virtual Mobility Controller Cluster	MC-VA-250		
	Mobility Controller Cluster	7210	7220	
	802.11ac Wave 2 Access Points	300 Series	310 Series	330/340 Series

Features, Performance & Scaling

图 140 *大型楼宇平台建议*

园区

以下参考设计用于由多个不同规模楼宇和两个数据中心组成的园区部署。园区内的每个楼宇均实施连接到园区主干网各自 2 层或 3 层模块化网络。此方案中的园区需要支持 64,000 个并发双堆栈客户端，并且需要 6,000 个 802.11ac Wave 2 AP。

园区部署需要考虑的关键决策是将 MC 群集（无线模块）放置在哪里。由于极具挑战性的可扩展性要求，这种规模的园区通常需要多个 MC 群集，这些群集可集中在数据中心，也可以策略性地分布在楼宇之间。在这两种情况下，这些群集均由跨数据中心部署的硬件或虚拟 MM 加以管理。

集中式和分布式 MC 部署模式对园区部署均有效，每种模式均支持不同的移动性需求。由于只能在由公共群集管理的 AP 之间提供无缝移动性，因此这些移动性需求通常是影响所选群集部署模式的决定因素。

流量是在确定群集布局时需要考虑的另一个因素。如果用户应用程序主要托管在数据中心，则集中式群集为合适的选择，因为无线和动态分段的客户端会话在群集中进行端接。使群集位置更靠近应用程序可优化流量。如果主要应用程序分布在园区中的楼宇之间，则分布式 MC 模式可能是更有效的设计。

集中式群集

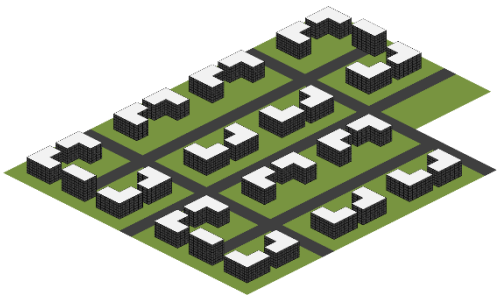
- 当需要覆盖室内和室外范围时，可实现更大的移动域。
- 在主应用程序托管在云或数据中心时非常高效。

分布式群集

- 可实现较小的移动域，例如在楼宇内或同位置的楼宇之间。
- 主应用程序为分布式或基于工作组时非常高效。

方案 1 - 集中式群集

集中式群集参考设计适用于具有两个数据中心且它们实施集中式群集的公司总部等园区。园区 LAN 实施高速第 3 层主干网，该主干网将每个楼宇与两个数据中心进行互连。该园区需要在 6,000 个 802.11ac Wave 2 AP 间支持 64,000 个并发双堆栈无线客户端。该示例中的每个主机均从有状态 DHCPv6 服务器被分配了一个全局 IPv6 地址。为在大楼宇组之间实现漫游，具有重叠覆盖范围的室内和室外 AP 将被分配到相同 MC 群集。



园区特点：

- 6,000 个 802.11ac Wave 2 接入点
- 64,000 个并发双堆栈客户端
- 2 个具有第 2 层扩展的数据中心

图 141 *方案 1 园区特点*

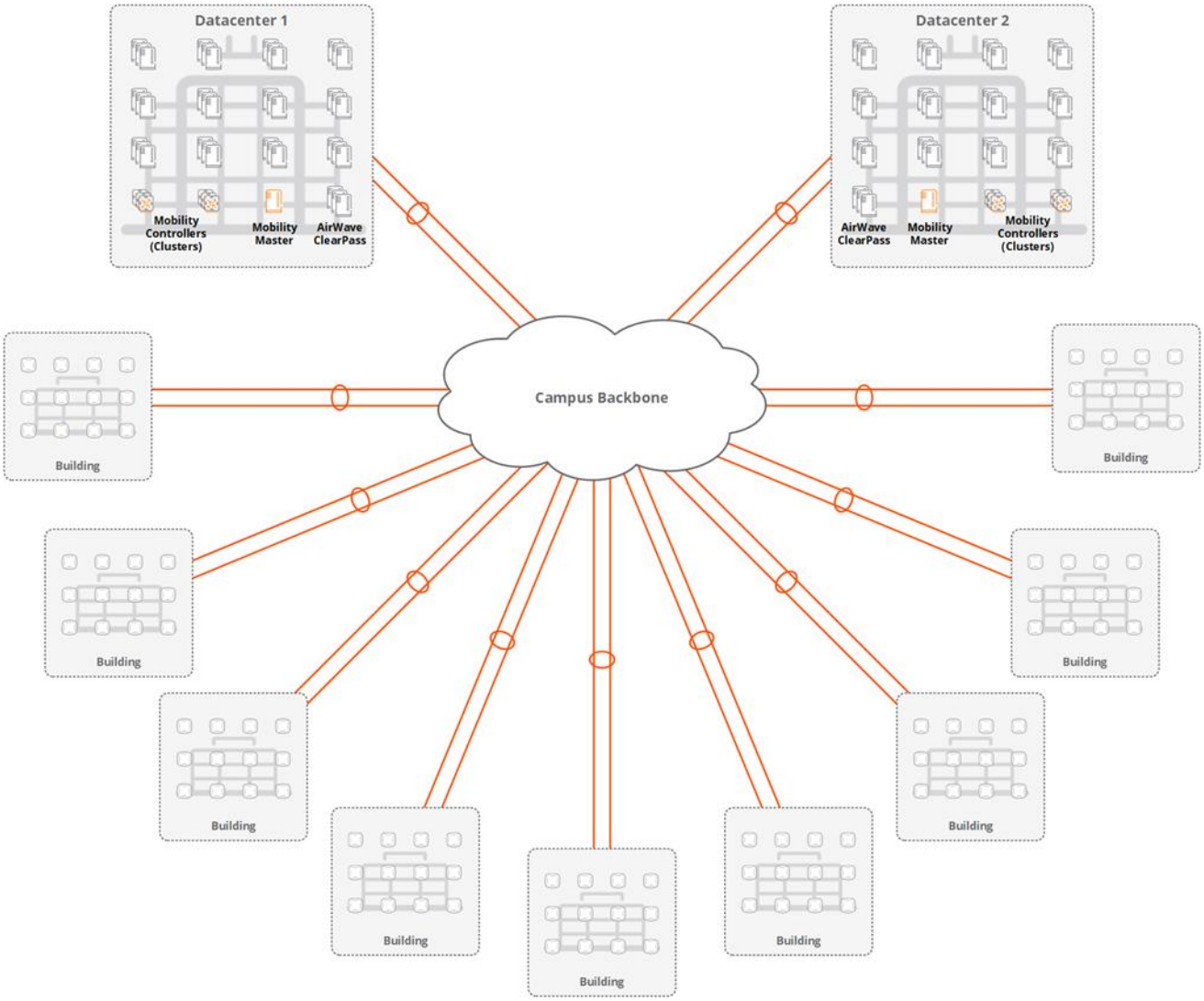


图 142 *园区模块化网络设计 - 集中式 MC 群集*

无线 LAN 组件

此方案中的园区包括分布在两个数据中心间的 MM 和 MC 群集。实现完全冗余所需的 MM 和 MC 群集数量将受数据中心设计的影响。这些数据中心可支持第 2 层 VLAN 扩展，或者可在第 3 层加以分离：

- **第 2 层扩展** - VLAN 及其关联的广播域在数据中心之间是通用的。
- **第 3 层分离** - VLAN 及其关联的广播域对每个数据中心都是唯一的。

当在这些数据中心之间扩展 VLAN 时，可在这些数据中心之间拆分 MM 和 MC 群集成员。每个数据中心均托管 1 个 MM 和半数 MC。需要两个 MM 和两个 MC 群集才能适应此方案的 AP 和客户端数。为实现聚合层可扩展性以及故障域隔离，每个移动 MC 群集均被连接到单独 Aruba 8400 系列聚合层交换机。每个聚合层最多可容纳 32,000 个 IPv4 和 64,000 个 IPv6 主机地址。

组件	描述	注释
Aruba MM (MM)	硬件或虚拟设备	需要 2 个
Aruba MC	硬件或虚拟设备	2 个群集
Aruba 接入点	802.11ac Wave 2 接入点	需要 6,000 个
Aruba Airwave	硬件或虚拟设备	推荐
Aruba ClearPass	硬件或虚拟设备	推荐

表 27 *无线 LAN 组件 - 第 2 层扩展*

当在第 3 层分离数据中心时，需要采用不同方法。为支持 AP 和客户端数并保持完全冗余，实施了主用/备用模式。在此类设计中，每个数据中心均托管相同数量的 MM 和 MC：

1. **MM** - 每数据中心托管两个 MM，从而实施第 2 层和第 3 层主冗余。在每个数据中心内的 MM 之间提供了第 2 层主冗余，而第 3 层主冗余在数据中心之间提供冗余。
2. **MC 群集** - 每数据中心托管两个 MC 群集。这些 AP 配置有主 LMS 和备用 LMS，以便确定它们的主要和辅助群集分配。主群集中提供了快速故障切换，而需要完全启动才能在主要群集与辅助群集之间进行故障切换。

每个 MC 群集均被连接到单独 Aruba 8400 系列聚合层交换机，以便实现聚合层扩展和故障域隔离。每个聚合层交换机最多可容纳 32,000 个 IPv4 和 64,000 个 IPv6 主机地址。在第 3 层分开每个数据中心，这需要四个无线模块和无线聚合层才能适应单个数据中心故障。

组件	描述	注释
Aruba MM (MM)	硬件或虚拟设备	需要 4 个（L3 冗余）
Aruba MC	硬件或虚拟设备	4 个群集（每数据中心 2 个）
Aruba 接入点	802.11ac Wave 2 接入点	需要 6,000 个
Aruba Airwave	硬件或虚拟设备	推荐
Aruba ClearPass	硬件或虚拟设备	推荐

表 28 *无线 LAN 组件 - 第 3 层分离*

漫游域

在 ArubaOS 8 架构中，在公共群集管理的 AP 之间提供了无缝移动性。每个无线和动态分段的客户端均被分配了一个主要 UAC 和 S-UAC 群集成员，以便在群集成员出现故障或实时升级时提供快速故障切换。为确保足够的可扩展性，需要使用两个 MC 群集。

务必考虑到无缝漫游只能在同一群集管理的 AP 之间进行。需要考虑以下因素：

1. 同一楼宇中的 AP 必须由同一群集加以管理。这可确保无线客户端会话不会因客户端在楼宇内漫游而中断。
2. 覆盖范围重叠的同位置楼宇中的室内和室外 AP 必须由同一群集加以管理。这可确保客户端会话不会因客户端在楼宇内或楼宇间漫游而中断。

地理位置分离且没有覆盖范围不重叠的楼宇中的 AP 可根据要求分布在群集之间，同时注意确保 AP 和客户端容量尽可能分配均匀：

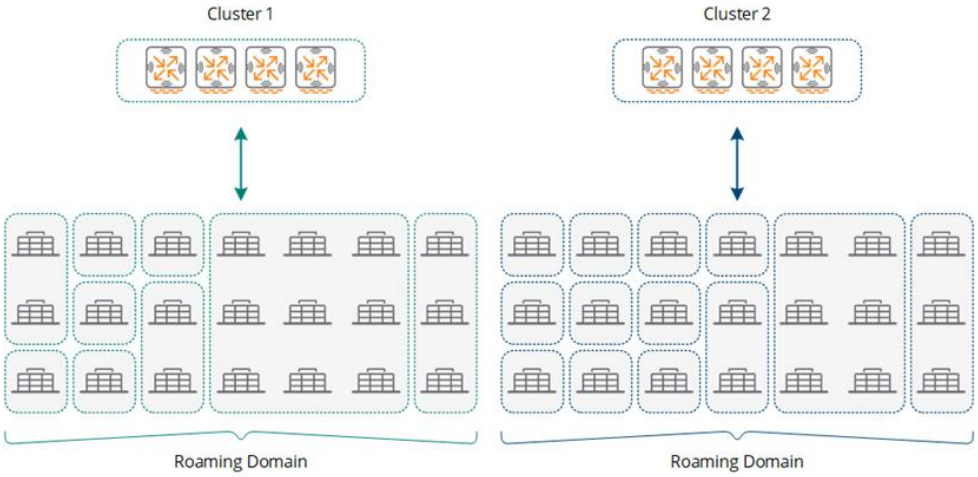


图 143 *漫游域*

NOTE

如果园区部署同时支持无线和动态分段的客户端，则部署单独群集可能有利。

冗余

在集中式群集方案中，数据中心位于连接到园区主干网的单独楼宇中。这些数据中心使用高速链路进行互连，从而确保可获得足够的带宽容量来支持每个数据中心托管的应用程序和服务。

对于双数据中心设计，MM 和 MC 群集分布在两个数据中心之间。可使用多种策略部署无线组件以实现冗余，这取决于数据中心设计：

- **第 2 层扩展 -** 如果在数据中心之间扩展 VLAN，可在这些数据中心之间拆分 MM 和 MC 群集成员。每个数据中心将托管 1 个 MM 和半数群集成员。
- **第 3 层分离** - 在每个数据中心内复制这些 MM 和 MC 群集成员。

第 2 层扩展

第 2 层数据中心冗余模式相对简单，因为其运行方式与单数据中心部署模式相同。每个数据中心均托管 1 个 MM 和每个群集的半数 MC。MM 被配置为可实现 L2 冗余，而每个群集均提供了 AP 和客户端负载分担以及快速故障切换功能：

- Aruba MM (MM)：
  - 两个硬件或虚拟 MM（每数据中心一个）
  - L2 主冗余（主用/备用）
- 硬件 MC (MC)：
  - 两个硬件 MC 群集
  - 群集成员在数据中心之间平均分配
- 接入点
  - AP 主控制器指向群集的 VRRP VIP 地址
  - 使用群集内置冗余实现的快速故障切换
  - 基于每个楼宇的漫游要求的 AP 群集分配

默认情况下，AP 和客户端将在位于每个数据中心的群集成员之间进行负载分担和分配。通过集中式群集园区设计，可将楼宇内的 AP 和客户端分配到不同数据中心内的群集成员。

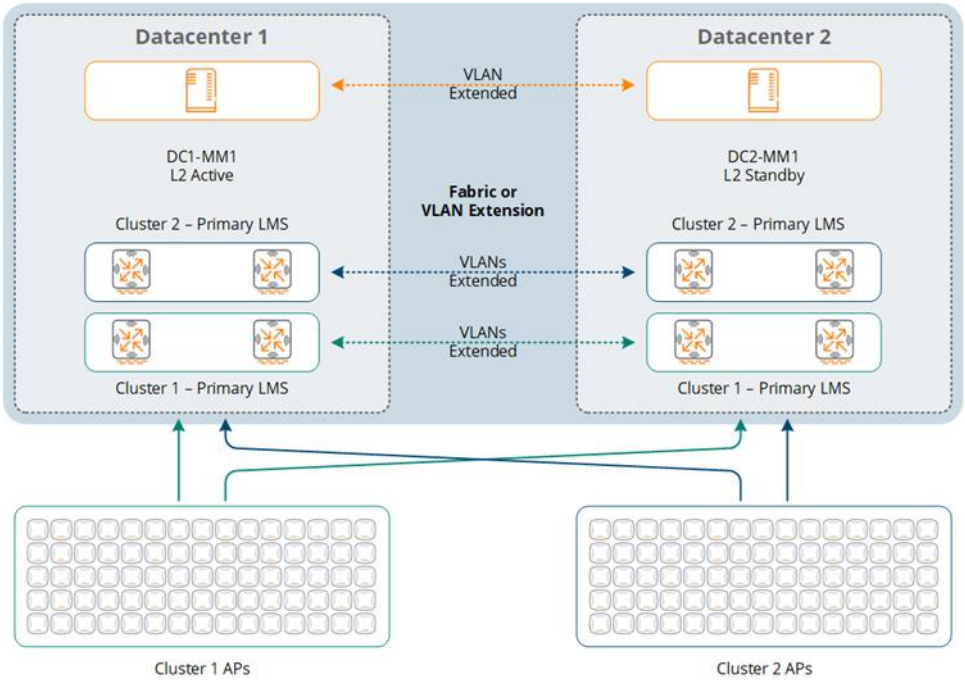


图 144 *冗余 - 第 2 层扩展*

第 3 层分离

在复制数据中心内的 MM 和群集方面，第 3 层分离式数据中心冗余模式与第 2 层扩展不同。每个数据中心均托管两个 MM 和两个 MC 群集。MM 被配置为可在数据中心内实现 L2 冗余，以及在数据中心

之间实现 L3 冗余。使用主 LMS 和备用 LMS 为每个楼宇内的 AP 均分配了主群集和备用群集。在每个群集中均提供了 AP 和客户端快速故障切换功能，而必需进行完全启动才能在群集之间实现故障切换：

- Aruba MM (MM)：
  - 四个硬件或虚拟 MM（每数据中心两个）
  - L2 主冗余（主用/备用）
  - L3 主冗余（主要/辅助）
- 硬件 MC (MC)：
  - 四个硬件 MC 群集（主要/辅助）
  - 群集成员在数据中心之间进行复制
  - 主群集在数据中心之间交替
- 接入点
  - 使用主要和辅助群集 VRRP VIP 地址的主要和备用 LMS
  - 使用群集内置冗余实现的快速故障切换
  - 在主群集与辅助群集之间进行的启动故障切换
  - 基于每个楼宇的漫游要求的 AP 群集分配

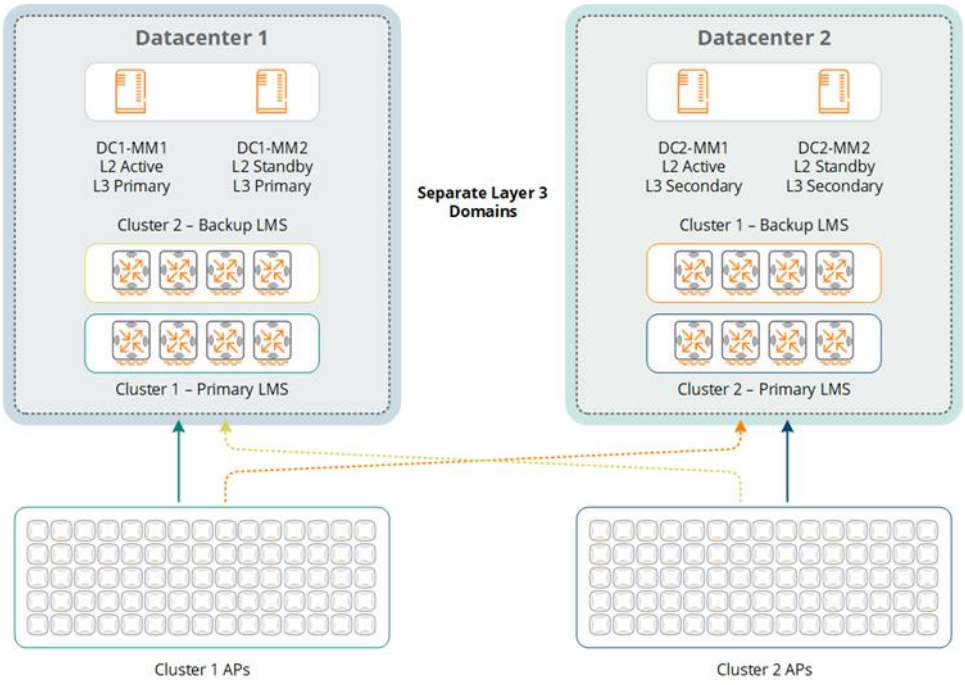


图 145 *冗余 - 第 3 层分离*

可扩展性

此园区方案主要关注可扩展性，在数据中心部署模式中包含辅助数据中心可能会带来挑战。为适应网络增长和冗余要求，必须考虑数据中心聚合层和 MC 群集设计。

数据中心聚合层

两个数据中心部署模式都需要使用连接到各自数据中心聚合层的 MC 群集。需要使用两个 MC 群集来容纳 64,000 个并发双堆栈主机，每个主机最多支持 32,000 个。该示例中的每个 IPv6 主机均被分配了一个全局 IPv6 地址。

由于必须支持大量客户端，因此将每个群集连接到单独 Aruba 8400 系列无线聚合层交换机。此建议适用于第 2 层扩展和第 3 层分离式数据中心设计：

- **第 2 层扩展** - 需要在数据中心之间拆分的两个数据中心聚合层。每个无线聚合层均支持一个 MC 群集。
- **第 3 层分离** - 每个数据中心需要两个数据中心聚合层。每个无线聚合层均被连接到 MC 的主要或辅助群集。

此数据中心聚合层设计可确保在正常运行期间单个聚合层从不会超过 64,000 个 IPv4 或 IPv6 主机地址，以及在数据中心出现故障时提供足够的容量来继续正常运行：

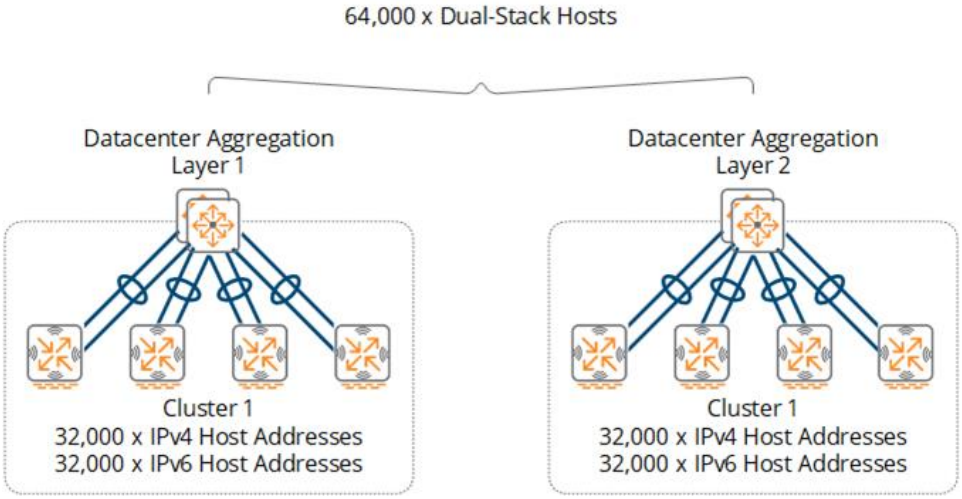


图 146 *数据中心无线聚合第 3 层分离式设计*

MC 群集

通过选择适当的控制器型号并确定每群集的正确成员数量提供了每个群集的可扩展性。所选 MC 型号的吞吐量能力也是一个因素，因为每个型号具有不同的交换容量和物理接口。对于此园区方案，建议使用 7200 系列控制器，每个群集由四个 MC 组成。

尽管可为园区部署选择 VMC，但出于吞吐量和性能原因，Aruba 建议部署硬件 MC。此硬件专用这一事实确保可提供特定性能级别。

MM

对于集中式群集园区设计，Aruba 建议实施 MM-HW-10K 或 MM-VA-10K MM。数据交换吞吐量不像在使用 MC 群集时那样是个大问题，因此硬件或虚拟 MM 均可加以部署。

为此设计选择的 MM 应进行扩展，以支持 10,000 个 AP、100,000 个客户端和 1,000 个 MC。实施这一容量级别将确保为 AP、客户端和 MC 提供足够的支持，同时提供更多未来增长提供空间。通过添加更多聚合层和 MC 群集，可随着园区的增长添加更多客户端和 AP。

通过在数据中心内部署更多 MC 群集，可实现为集中式部署模式扩展超过 64,000 个双堆栈客户端。在 ArubaOS 8 部署中，MM 可进行扩展，以支持最多 100,000 个客户端、10,000 个 AP、1,000 个 MC。通过部署更多 MM 和 MC 群集可实现更高的可扩展性。

虚拟 LAN

在集中式群集设计中，数据中心聚合层端接 MC 群集成员中的所有 VLAN。数据中心架构决定了 VLAN 设计。在这两种设计中均使用 802.1Q 中继将这些 VLAN 从 MC 扩展到其各自的数据中心聚合层交换机。这些设计之间的主要区别在于所需的 VLAN 数量。

第 2 层扩展

在数据中心之间扩展 VLAN 时，每个群集均实施自己的唯一 VLAN ID 和广播域。根据已实施的 VLAN 模式，每个群集均由一个或多个用户 VLAN 组成。对于单个 VLAN 设计，所有无线和动态分段的客户端均被分配到一个公共 VLAN ID，其角色和策略确定在网络上为每个用户提供的访问级别。每个群集均实施唯一 VLAN ID。

这些用户 VLAN 从聚合层交换机扩展到每个 MC 群集成员。数据中心聚合层与每个 MC 群集成员之间至少需要两个 VLAN。一个 VLAN 专用于管理、群集和 MM 通信，而其他 VLAN 被映射到客户端。为实现无缝移动性，VLAN 在数据中心间拆分的群集成员之间是通用的。数据中心聚合层交换机已定义了基于 VLAN 的 IP 接口，并且作为每个 VLAN 的默认网关运行。VRRP 或 Aruba 群集架构本机提供了第一跳路由器冗余。

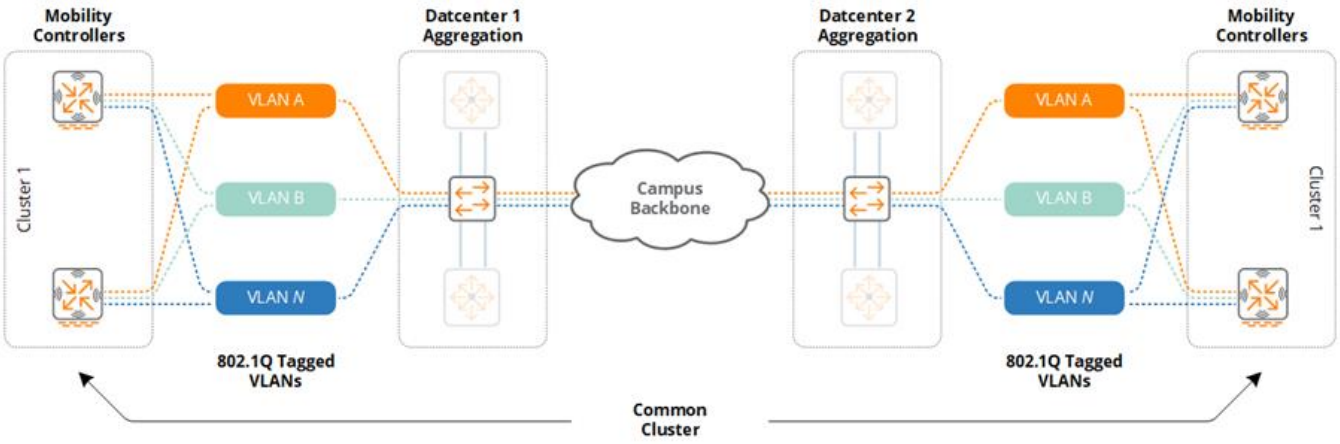


图 147 *无线和动态分段的客户端 VLAN - 第 2 层扩展*

第 3 层分离

当在第 3 层分离数据中心时，VLAN 对于每个数据中心都是唯一的。每个数据中心内的主要和辅助群集，每个群集均需要自己的唯一 VLAN ID 和广播域。根据已实施的 VLAN 模式，每个群集均由一个或多个用户 VLAN 组成。对于单个 VLAN 设计，所有无线和动态分段的客户端均被分配到一个公共 VLAN ID，其角色和策略确定在网络上为每个用户提供的访问级别。每个群集均实施唯一 VLAN ID。

这些用户 VLAN 从聚合层交换机扩展到每个 MC 群集成员。数据中心聚合层与每个 MC 群集成员之间至少需要两个 VLAN。一个 VLAN 专用于管理、群集和 MM 通信，而其他 VLAN 被映射到客户端。为

实现无缝移动，每个数据中心内的 VLAN 在群集成员之间都是通用的。数据中心聚合层交换机已定义了基于 VLAN 的 IP 接口，并且作为每个 VLAN 的默认网关运行。VRRP 或 Aruba 群集架构本机提供了第一跳路由器冗余。

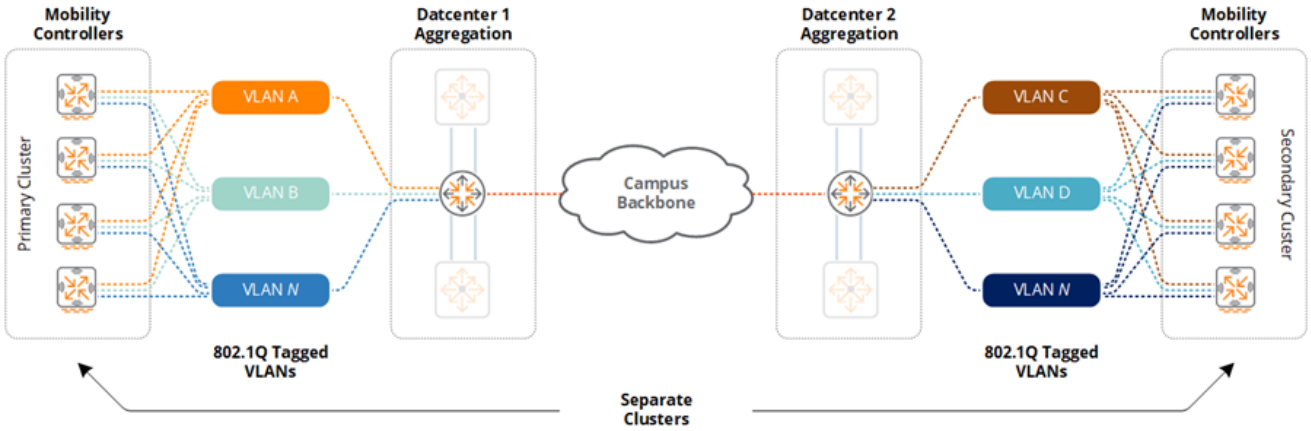


图 148 *无线和动态分段的客户端 VLAN - 第 3 层分离*

两个数据中心设计之间的一个关键区别是在数据中心故障期间的客户端 VLAN 分配和广播域成员资格。尽管这两种模式均提供完全冗余，但只有第 2 层 VLAN 扩展模式可在数据中心中断时提供快速故障切换：

1. **第 2 层扩展** - 受影响的客户端在数据中心故障切换后保持其 VLAN ID 和 IP 地址。AP、Aruba 交换机和客户端被分配到其余数据中心的现有群集中的新群集成员。
2. **第 3 层分离** - 在数据中心故障切换后，受影响的客户端被分配了新的 VLAN ID 和 IP 地址。AP、Aruba 交换机和客户端将被分配到其余数据中心内的辅助群集成员。

平台建议

图 144 为支持 6,000 个 AP 和 64,000 个并发客户端的集中式群集园区部署方案提供了平台建议。在适当时，基于功能、性能和可扩展性要求，做出了良好、更好、最佳建议。这些建议基于所描述的方案，并且可根据网络管理员的判断而改变。

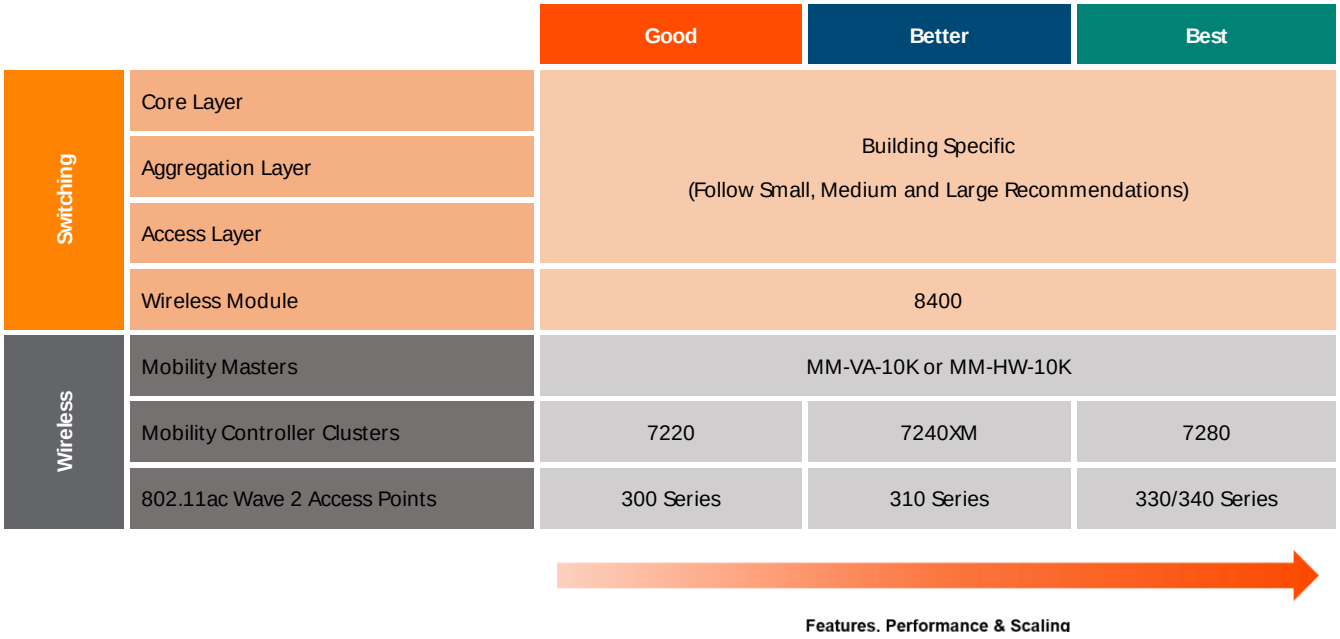
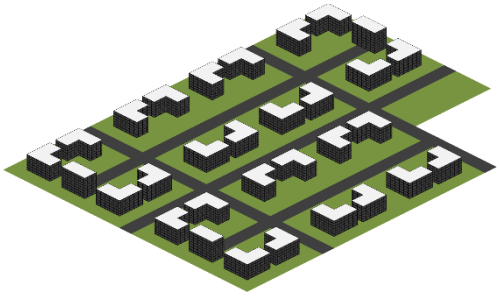


图 149 *集中式群集园区楼宇平台建议*

由于园区中每个楼宇的大小各不相同，每个楼宇均将需要自己的 2 层或 3 层分层网络设计。因此没有提供针对核心层、聚合层和接入层的交换建议，因为这些选择对于每个楼宇都是唯一的。应按照先前部分中强调的小型、中型和大型建议进行单独楼宇选择。

方案 2 - 分布式群集

以下参考设计针对大型园区，例如在 900 英亩的场地上分布着 285 个楼宇的大学。每个楼宇均实施连接到公共园区主干网的各自 2 层或 3 层模块化网络设计。该大学拥有 20,000 名教职员工和学生，并且具有 IPv4 和 IPv6 客户端。该大学已部署了 3,500 个 802.11ac Wave 2 AP，以便提供足够的覆盖范围。



园区特点：

- 3,500 个 802.11ac Wave 2 接入点
- 40,000 个并发客户端（本机 IPv4 和/或双堆栈）
- 1 个数据中心

图 150 *方案 2 园区特点*

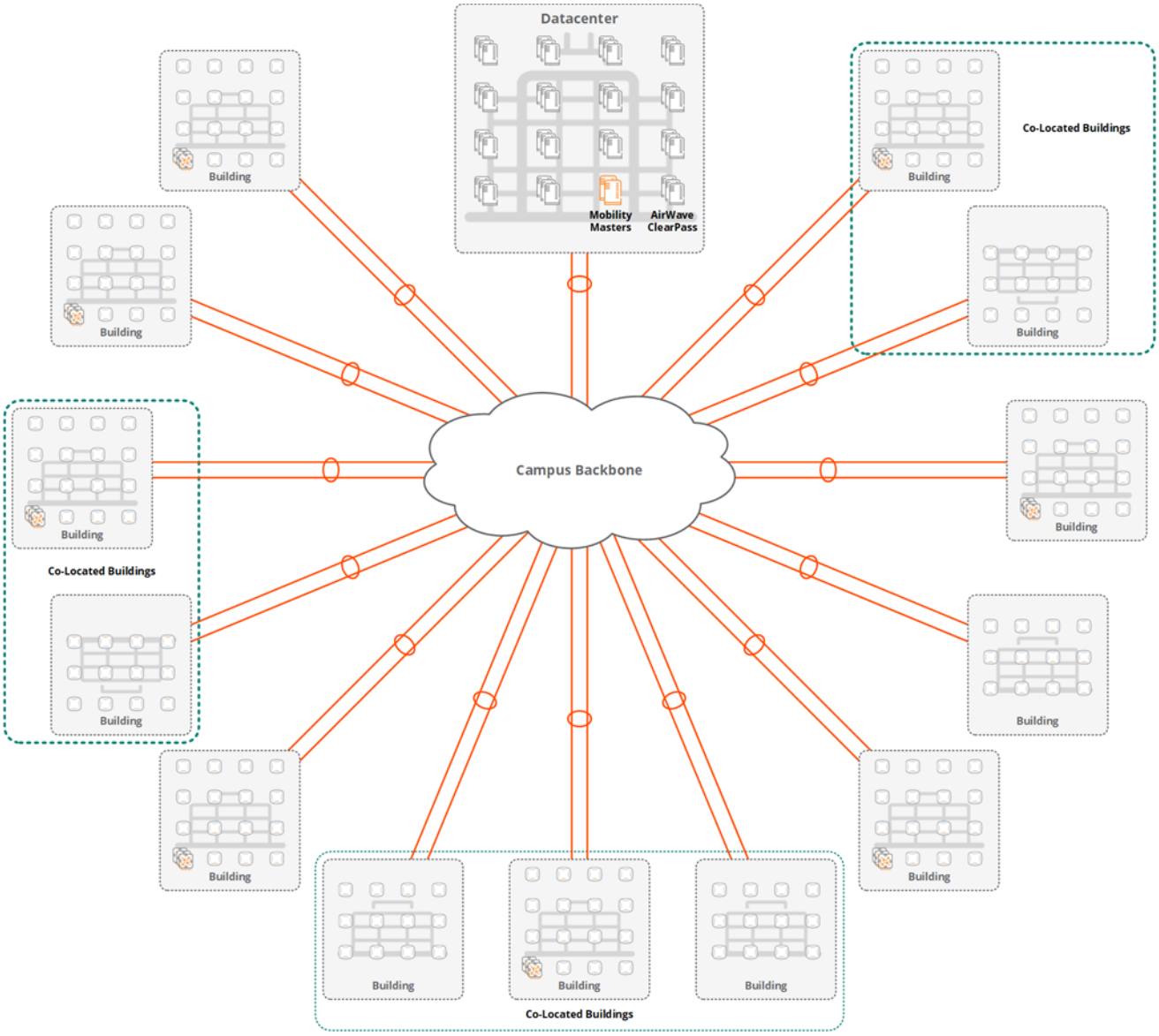


图 151 *分布式群集园区架构*

无线 LAN 组件

此方案中的园区包括部署在数据中心内的 MM 以及分布在楼宇之间的 MC 群集。此方案中的园区包括单个数据中心，但生产部署中可能存在多个数据中心。如果存在多个数据中心，则先前章节中详细说明的园区参考架构会提供有关 MM 部署选项的详细信息，第 2 层和第 3 层数据中心部署模式可选择这些选项。

与先前园区示例不同，本节中描述的 MC 群集分布在单个楼宇之间，而不是部署在数据中心内。这意味着无线和动态分段的流量在楼宇内进行端接，而不是在数据中心内。漫游只能在 MC 群集中进行，因此位于同位置楼宇中的 AP 需要重叠覆盖范围，并且由策略性地部署在其中一个楼宇中的 MC 群集提供服务。被隔离楼宇中的 AP 和客户端需要由各自的 MC 群集提供服务。

针对园区中每个楼宇的模块化网络设计和 MC 群集布局建议遵循为小型、中型和大型办事处参考设计提供的相同建议。MC 群集根据楼宇大小连接到各自层。与先前建议一样，当无线和动态分段的客户端数超过 4,096 时，建议使用无线聚合层。

随着楼宇规模的增加，AP 和主机数量将会不同。MC 群集可针对每个楼宇或同位置楼宇进行定制，以符合特定 AP、客户端和吞吐量要求。为实现轻松部署、故障排除和维修，建议对小型、中型和大型楼宇的常用 MC 模式进行标准化。设计可包括根据需要支持的楼宇大小范围，指定两个或三个不同的控制器型号。

组件	描述	注释
Aruba MM (MM)	硬件或虚拟设备	需要 2 个
Aruba MC	硬件或虚拟设备	变化
Aruba 接入点	802.11ac Wave 2 接入点	需要 3,500 个（分布式）
Aruba Airwave	硬件或虚拟设备	推荐
Aruba ClearPass	硬件或虚拟设备	推荐

表 29 *无线 LAN 组件*

漫游域

在 ArubaOS 8 架构中，在公共群集管理的 AP 之间提供了无缝移动性。每个无线和动态分段的客户端均被分配了一个主要 UAC 和辅助 S-UAC 群集成员，以便在群集成员出现故障或实时升级时提供快速故障切换。

此园区设计包括独立楼宇和同位置楼宇。在每个楼宇内提供了漫游，以及在提供重叠覆盖范围的同位置楼宇之间策略性地提供了漫游。同位置楼宇提供室内和室外覆盖范围，并且当教职员工和学生在楼宇之间移动时可实现漫游：

- **独立楼宇** - 由部署在每个楼宇内的 MC 群集提供服务。必要时，小型楼宇中的 AP 由邻近楼宇中的 MC 群集提供服务。
- **同位置楼宇** - 由在同位置楼宇的其中一个楼宇中策略性部署的 MC 群集提供服务。每个群集均服务于两个或更多个楼宇间的 AP。

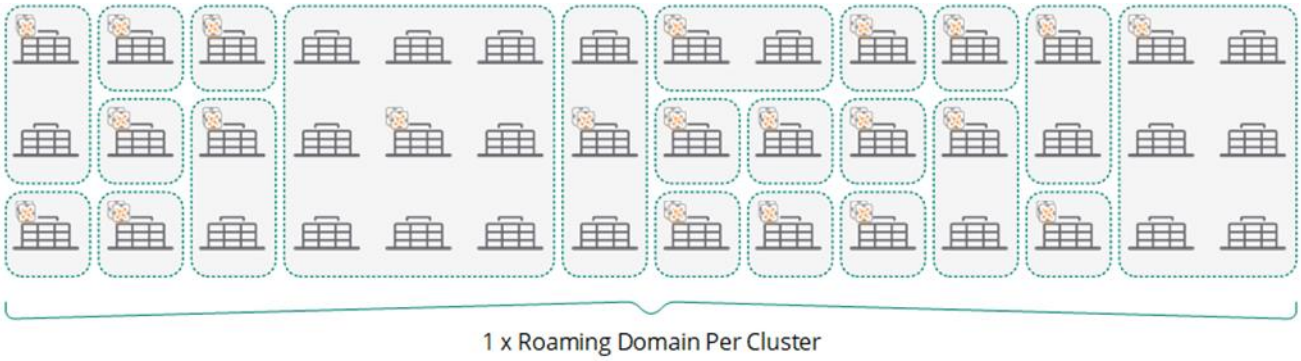


图 152 *漫游域*

冗余

对于此方案，MM 部署在数据中心内，并且直接连接到单独数据中心聚合层交换机。每个楼宇内的冗余由模块化网络设计和 MC 群集提供。按照为小型、中型和大型办事处参考设计提供的相同建议部署这些 MC：

- Aruba MM (MM)：
  - 两个硬件或虚拟 MM
  - L2 主冗余（主用/备用）
- 硬件 MC (MC)：
  - 两个硬件 MC 群集
  - 至少两个群集成员
- 虚拟 MC (MC)：
  - 多个虚拟 MC 群集
  - 至少两个群集成员
- 接入点
  - AP 主控制器指向群集的 VRRP VIP 地址
  - 使用群集内置冗余实现的快速故障切换

如果需要，可通过实施备用 LMS 选项来实现群集之间的额外冗余。在发生群集或无线聚合层故障时，这将使楼宇中的 AP 能够故障切换到指定的替代群集。如果发生此类事件，AP 将执行完全启动，以便故障切换到替代群集，这将影响用户。此外还必须相应地扩展替代群集和聚合层，以便适应 AP 和客户端数。

可扩展性

分布式群集园区方案的主要可扩展性问题是 MM 扩展。对于此园区设计，除分布在楼宇之间的 MC 总数外，还需要适应 AP 和客户端总数。此方案中的 285 个楼宇将由 180 个群集提供服务，其中每个群集至少有两个成员。某些较大楼宇中的群集可根据需要包含三个或四个群集成员。

对于此园区设计，Aruba 建议实施 MM-HW-5K 或 MM-VA-5K MM。可部署硬件或虚拟 MM，因为分布式 MC 的数量为关键问题。为此设计选择的 MM 需要进行扩展，以支持 5,000 个 AP、50,000 个客户端和 500 个 MC。这将提供足够的容量来支持 AP、客户端和 MC 数，同时提供更多未来增长空间。如果特定园区设计需要更多 MC，则可选择 MM-HW-10K 或 MM-VA-10K MM。这些 MM 每个最多支持 1,000 个 MC。

虚拟 LAN

对于分布式群集设计，楼宇核心或无线聚合层端接来自每个楼宇无线模块的所有 VLAN。使用 802.1Q 中继将这些无线和动态分段的客户端 VLAN 从 MC 扩展到其各自的楼宇交换机。

根据实施的架构模式，无线模块由一个或多个用户 VLAN 组成。对于单个 VLAN 设计，所有无线和动态分段的客户端均被分配到一个公共 VLAN ID，其角色和策略确定在网络上为每个用户提供的访问级别。单个 VLAN 从各自的聚合层交换机扩展到每个物理或虚拟 MC 群集成员。可根据需要添加和扩展其他 VLAN。例如，出于策略合规性目的，特定的优先设计可能需要将单独 VLAN 分配给无线和动态分段的客户端。

每个楼宇中的核心或无线聚合层交换机与每个 MC 群集成员之间至少需要两个 VLAN。一个 VLAN 专用于管理和 MM 通信，而其他 VLAN 被映射到客户端。为在每个楼宇内实现无缝移动，这些 VLAN 在群集成员之间是通用的。

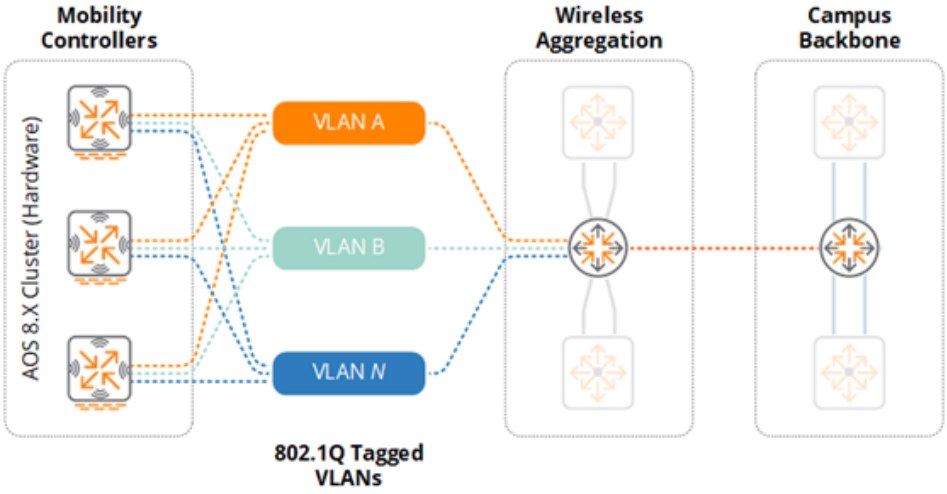


图 153 *硬件 MC 群集 - VLAN*

每个楼宇均可根据需要实施公共 VLAN ID 或唯一 VLAN ID。每个楼宇均与园区内的其他楼宇进行了第 3 层分离。这意味着可重用这些 VLAN ID，从而可简化 WLAN 和动态分段的客户端部署。但每个 VLAN 均需要自己的 IPv4 和 IPv6 子网分配。

平台建议

分布式园区方案需要根据针对每个楼宇的特定要求选择交换和无线组件。应根据先前部分中强调的小型、中型和大型建议为每个楼宇选择组件。园区中的每个楼宇均将通过相应的选择来实施 2 层或 3 层分层网络设计，以便符合每个楼宇的有线和无线连接、性能和冗余要求。

如前所述，Aruba 建议对小型、中型和大型楼宇的常用 MC 型号进行标准化，因为这样做将简化部署、故障排除和维修。特定园区设计可标准化所有楼宇的常用 MC 型号或为每个楼宇大小标准化的一个型号。应调整每个楼宇的群集成员数量，以便满足每个楼宇的冗余和性能需求。

为支持这种分布式园区方案，Aruba 建议使用 MM-VA-5K 或 MM-HW-5K，其可进行扩展，以容纳 5,000 个 AP、50,000 个客户端和 500 个 MC。建议的 MM 模式可满足支持 3,500 个 AP 和 40,000 个并发客户端的初始要求，同时可实现未来网络可扩展性。如果需要，MM-VA-10K 或 MM-HW-10K 等较大 MM 可用于支持更大的分布式园区。MM-VA-10K 或 MM-HW-10K 均能够支持 10,000 个 AP、100,000 个客户端和 1,000 个 MC。

迁移到 ArubaOS 8

将 Aruba 部署从 ArubaOS 6 迁移到 ArubaOS 8 涉及的步骤和预防措施比执行简单的控制器映像升级更多一些。本章涉及了迁移方法、有关何时选择特定方法而不选择其他方法的最佳实践建议等主题，并且概述了如何将典型 ArubaOS 6 网络拓扑结构迁移到 ArubaOS 8。根据 ArubaOS 6 拓扑结构，可手动执行迁移，也可以使用迁移工具执行迁移。

NOTE

没有从 8.x 独立或 MC Master 到 ArubaOS 8 MM 的自动迁移

迁移策略

迁移工具

迁移工具是基于 VM 的服务器，其可用于将 ArubaOS 6 部署迁移到 ArubaOS 8。迁移工具 GUI 用于为需要迁移的所有控制器提供 IP 地址、凭据和所需角色。然后该工具与 MM、控制器和 VMware/KVM（如果协调）进行通信，获取所需的控制器备份，将映像升级到 ArubaOS 8，以及配置控制器，以便与 MM 进行通信。

优点

- 在迁移过程中保留 ArubaOS 6 中的现有 WLAN 配置元素，这可这节省可能重建它们所需的时间和工作量
- 多个 ArubaOS 6 部署拓扑结构（例如多个主-本地控制器）可折叠在单个 MM 下
- 自动执行配置备份、映像下载/升级和许可迁移
- 支持单阶段和多阶段迁移方法。例如，现有主控制器可用作 MM 配置源，而其他控制器在 MM 下进行迁移，主控制器本身可在稍后阶段进行迁移
- 支持与 VMware 和 KVM 的协同

用于迁移的支持拓扑结构

- 将“主-本地”设置迁移到 MM 或主控制器模式
- 将“所有-主”设置迁移到 MM
- 迁移到独立控制器

NOTE

迁移工具保留先前配置的所有方面，包括旧的和未使用的配置元素。有关迁移工具的其他详细信息，请参阅 ArubaOS 迁移指南。

手动迁移

手动迁移涉及从所有控制器获取备份，通过将每个控制器单独升级到 ArubaOS8 来重新构建它们，以及执行初始设置，以便将它们转换到 MM 托管的控制器或独立控制器。转换到 MM 托管的控制器需要安装、配置 MM，并使其准备好接受控制器连接。此外还可通过并行建立 MM、构建配置，然后一次移动一个控制器来执行手动迁移。

优点

- 尽管迁移工具可利用标准网络配置为 ArubaOS 6 部署提供安全、轻松的迁移路径，但 ArubaOS 8 引入的拓扑结构和功能优势可能在迁移后需要新的配置元素。在此类情况下，更有效的方式可能是与您的现有 ArubaOS 6 部署并行启动 MM，然后手动重新配置 WLAN 的元素，以适应这些新功能
- 通过手动迁移可执行和测试较小的渐进式更改，同时使现有网络在迁移过程中能够继续运行
- 现有拓扑结构可能包含过时或已弃用的功能，而通过手动迁移可相应地计划和配置替代方案
- 如果现有配置非常复杂（例如，大量静态 GRE/IPsec 隧道、大型网状网部署、复杂的静态信道计划、AP 特定设置等），则手动迁移可能更有效

支持的拓扑结构

由于手动迁移涉及单独使每个控制器做好迁移准备，因此可使用许多迁移拓扑结构。有关推荐的拓扑结构，请参阅本章稍后的“迁移不同 ArubaOS 6 拓扑结构”部分。可手动迁移的拓扑结构示例包括：

- 主-本地到 MM 或 MC Master (MCM)
- 所有-主到 MM
- 主-分支 (BOC) 到 MM
- 主/备用-主到独立/备用-独立
- 独立到 MM、MC Master 或独立
- 迁移到独立控制器

迁移工具与手动迁移

确定使用迁移工具而不使用手动迁移（反之亦然）没有严格的规则。选择实际上取决于环境和现有部署的复杂性。高度复杂的现有部署可能需要手动重建。迁移工具能够也可能无法处理不常见或非常复杂的配置元素（随时间的推移，最终可通过更新的迁移工具版本解决这一问题），因此将始终需要根据工具的功能权衡现有复杂性。以下几点提供了一系列粗略指导原则，这些指导原则可帮助确定哪个选项最适合给定的部署：

- 如果正在执行迁移的目的主要是为了支持新拓扑结构（或者需要迁移到更新拓扑结构的功能），那么执行手动迁移可能会更好
- 该迁移工具适用于在单个 MM 下折叠多个单独拓扑结构
- 该迁移工具还适用于具有基本 Wi-Fi 和来宾功能的部署。但可能必须在迁移后重新构建使用自定义强制网络门户网页和映像的部署

迁移最佳实践建议

- 在迁移前始终备份您现有拓扑结构中的所有内容
- 在迁移生产部署前，始终在实验室环境中测试所需的迁移方法。通过该迁移工具可在无需迁移现有主控制器的情况下迁移本地控制器，这有助于进行实验室测试
- 在进行实验室测试时，当通过“我的网络门户”(MNP) 测试许可迁移时时应小心。三种许可迁移存在限制
- 如果使用 Activate，则确保在迁移前根据需要更新 ZTP 设置

迁移警告

- 6000/M3、3000 或 600 控制器平台不支持迁移到 ArubaOS 8。迁移的先决条件是拥有 7000 和/或 7200 系列控制器
- 对主控制器的 7000/7200 控制器要求仍适用于仅需要迁移本地控制器而非主控制器的情况。如果该部署具有的主控制器不是来自 7000/7200 系列，则在使用迁移工具前，将需要使用 7000/7200 系列控制器临时替换主控制器，否则这些设备将需要手动迁移
- 所有正在迁移的控制器都需要在同一*我的网络门户*帐户中具有各自许可，否则许可迁移将不工作。这适用于手动迁移和迁移工具。
- 正在迁移的所有控制器都必须配置控制器 IP 和默认网关
- 可能必须在迁移后重新构建使用自定义强制网络门户网页和映像的部署
- 只有 7030 及更高型号的控制器可在 MC Master 模式下作为 MC Master 运行
- 7024 及更低型号的控制器只能被转换为 MM 托管、独立或 MC Master 托管控制器
- 在需要将现有主-本地部署迁移到 MC Master 托管部署的情况下，MC Master 无法端接 AP。如果 AP 先前在主控制器上进行端接，则需要将它们安置于在 MC Master 下移动的本地控制器上，或者新的控制器上
- ArubaOS 8 当前没有迁移路径来获取独立或 MC Master 托管控制器并将其置于 MM 下
- 如果在 ArubaOS 6 与 ArubaOS 8 之间反复升级或降级控制器，则由于在该控制器上创建的临时文件将导致迁移前检查失败，因此后续迁移可能会失败。如果需要反复升级或降级，则最佳解决方案是在升级之前捕获闪存备份，然后在第二次或后续升级之前恢复此备份

一般迁移要求

控制器

下表提供了 ArubaOS 8 迁移所需的最小控制器型号的建议：

传统 ArubaOS 6 控制器	AP	客户端	用于 ArubaOS 8 迁移的最小 7000/7200 平台	AP	客户端
6000/M3	512	8K	7210-7240	512-2K	16K-32K
3600	128	8K	7205	256	8K
3400	64	4K	7030	64	4K
3200	32	2K	7010	32	2K
651	16	512	7005/7008	16	1K
650	16	512	7005/7008	16	1K
620	8	256	7005/7008	16	1K

表 30 *ArubaOS 8 推荐的控制器*

虚拟专用网集中器

MC 可被配置为 VPNC，以便使其作为数据中心内针对不同地理位置的控制器的 IPsec 端接点。

- 从拓扑结构的角度讲，VPNC 是以分支控制器为轮辐的中心
- 从配置的角度讲，VPNC 充当由 MM 管理的另一个 MC。VPNC 被放置在包含 VPNC 特定配置的 MM 上的它们各自分层节点下
- 出于冗余目的，VPNC 可由备用 VPNC 加以备份
- 尽管 MC 可直接在 MM 上端接其 IPsec 连接（假设此 MM 是根据 SKU 规定的硬件规范进行构建的），但强烈建议在需要将来自任何分支站点的用户流量路由到数据中心时端接 VPNC 上的控制器

不支持的接入点

从 ArubaOS 8.2.0.1 开始，在 ArubaOS 8 下不支持以下 AP。与往常一样，请参阅最新的 ArubaOS 发行说明，以确认支持的硬件：

- AP-60
- AP-65
- AP-68
- AP-70
- AP-85
- AP-120/121
- AP-124/125
- AP-92/93（最高支持 ArubaOS 8.2）

ArubaOS 6 拓扑结构迁移

本节介绍生产环境中正在使用的常见 ArubaOS 6 拓扑结构，并且提供相应的 ArubaOS 8 拓扑结构迁移建议。

每个拓扑结构建议均包含以下详细信息：

- 描述
- 优点和缺点
- 迁移要求
- 迁移程序（手动）

主控制器和备用主控制器

在此 ArubaOS 6 设计中，主控制器端接网络中的所有 AP。备用主控制器使用虚拟路由器冗余协议 (VRRP) 支持此主用主控制器，以实现冗余。在主控制器上配置高可用性（AP 快速故障切换）意味着除建立到备用主控制器的备用隧道外，AP 还端接它们在主用主控制器上的主用隧道。

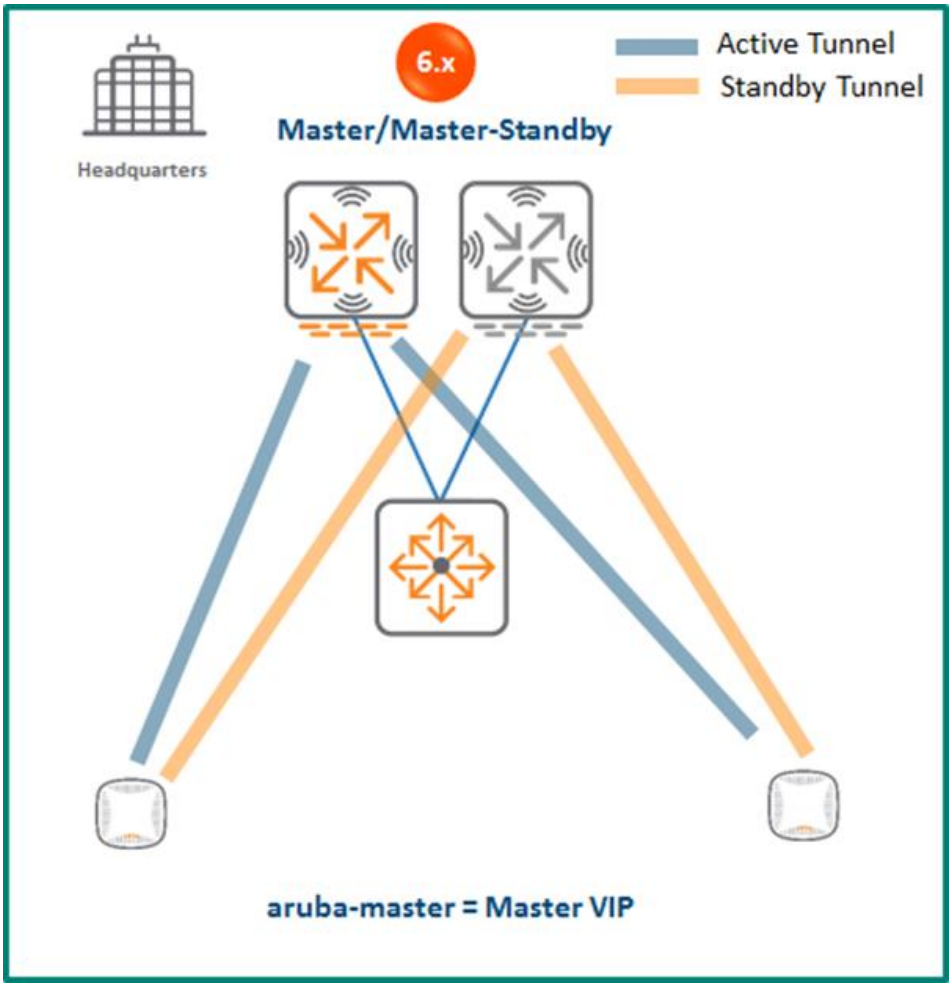


图 154 *ArubaOS 6 主/备用架构*

由于正在使用 VRRP 进行主控制器故障检测，并且主-备用主控制器设计不支持 AP 快速故障切换的控制器间心跳功能，因此故障检测将不是亚秒级。即，在触发故障切换到备用主控制器前，AP 将等待八次错过的心跳才能到主控制器。但对于所有 AP，此故障切换过程都将是即时且同时进行的，这与传统 VRRP 故障切换不同，后者要求 AP 在故障切换时重新启动。

MM 端接 MC

拓扑结构

要实施此 ArubaOS 8 设计，必须首先部署和配置 MM。ArubaOS 6 主控制器和备用主控制器成为由 MM 管理的 MC。这些控制器可形成群集，以用于冗余以及 AP 和客户端负载分担目的。被选为群集领导者的控制器将确定如何在群集中对 AP 和客户端进行负载分担。

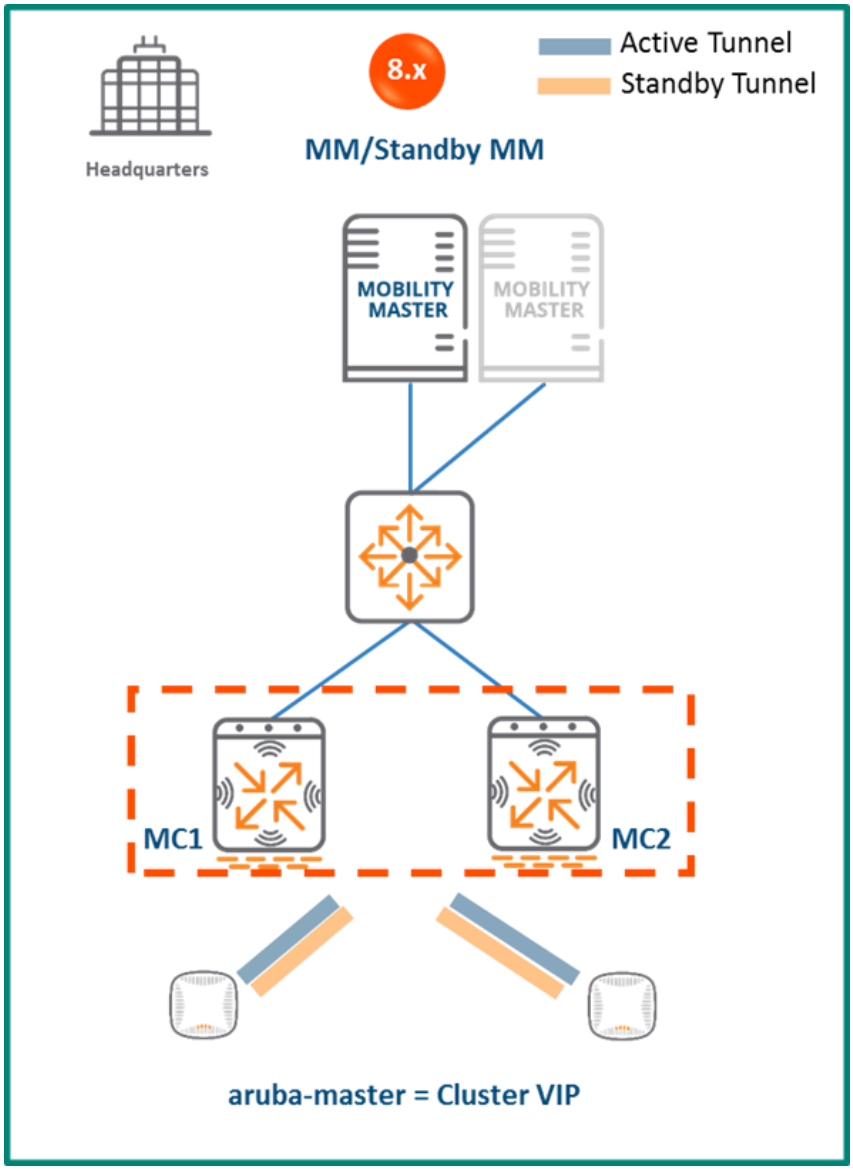


图 155 *MM 端接 MC*

配置层次结构

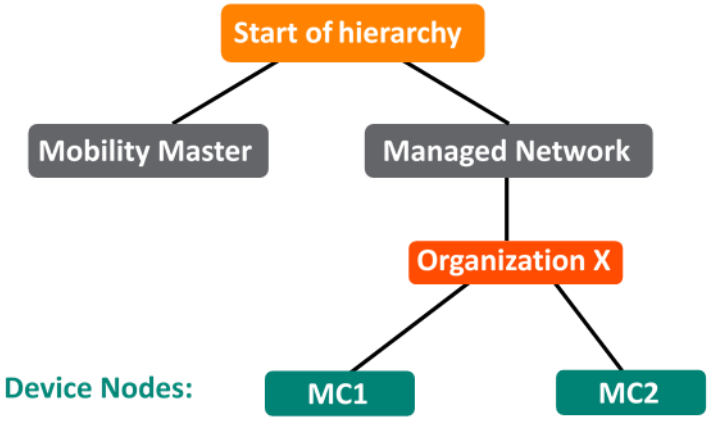


图 156 *MM 端接 MC 配置层次结构*

设计优势

- **最大化优势** - MM 端接 MC 设计是充分利用 ArubaOS 8 功能的理想选择
- **可扩展性** - 通过 MM 可轻松添加和管理新控制器
- **易于迁移** - 如果现有部署具有多个拓扑结构，则在 MM 下可将它们全部迁移到层次结构中它们自己的节点中
- **管理** - 集中式控制器配置和管理
- **分层配置模型** - 在节点（USA、West Coast、California、Santa Clara 等逻辑文件夹）上执行配置，以及根据位置和环境将每个控制器分配到特定节点
- **群集** - 在群集中具有控制器可在控制器之间实现无缝客户端故障切换，同时不影响用户体验。群集功能还可促进客户端漫游以及 AP 和客户端负载分担。必须进行群集才能支持实时升级。
- **实时升级** - 实时升级控制器群集，并且最终用户不会遇到任何连接或性能损失。无需为网络升级安排维护周期
- **AirMatch** - RF 智能集中在 MM 上，这可显著改进 WLAN 的 RF 管理和干扰抑制功能
- **REST API 支持**
- **多版本支持** - 可灵活地升级单个控制器，以便测试新功能或故障修复。群集中的控制器需要运行相同的 ArubaOS 软件版本，并且可一同进行升级
- **在线软件模块升级** - 可在运行时更新 UCC、AirGroup、AppRF 等可加载服务模块 (LSM)，无需安排任何维护周期

设计警告

- MM 不端接 AP。只能在 MC 上端接 AP

迁移要求

- 迁移需要购买虚拟 MM 容量许可或购买硬件 MM（也可以选择购买备用硬件 MM）
- 如果可获得备用 MM，则将聚合并同步每个 MM 上的许可
- 需要手动或通过“我的网络门户”迁移其他许可，例如 AP 和 PEF

迁移选项

- 可手动或通过迁移工具进行迁移
- 以下详细说明了手动迁移。要使用迁移工具执行迁移，请参阅 ArubaOS 8 迁移指南

迁移策略

现有 ArubaOS 6 部署

- 主用和备用主控制器
- AP 在主用主控制器上进行端接，备用主控制器作为备份

新 ArubaOS 8 部署

- MM 管理控制器 MC1 和 MC2
- AP 在 MC1 和 MC2 上进行端接

迁移程序

手动迁移需要通过以下步骤完全重新构建现有 ArubaOS 6 拓扑结构：

1. 部署 MM 并执行初始设置
2. 在 MM 上配置许可
3. 在 MM 上创建配置层次结构以及将主用和备用主控制器 MAC 地址列入白名单
4. 如果还正在安装备用 MM，则重复第 1 步
5. 如果已安装了备用 MM，则配置 MM 冗余。从现在开始，MM VIP 将用于配置管理
6. 在控制器之间配置群集，以及实现 AP 负载分担
7. 在群集成员 IP 之间创建 VIP，也可以选择为 RADIUS COA 创建 VIP
8. 创建 AP 组和 SSIDGUI：**托管网络 > （选择节点） > AP 组。**GUI：**托管网络 > （选择节点） > 任务 > 创建新 WLAN**
9. 通过填充 CPSec 白名单表（包括将 AP 映射到相应 AP 组）将 MM 列入 MM 白名单。GUI：**托管网络 > （选择节点） > 配置 > 接入点 > 白名单**
10. 备份 ArubaOS 6 主控制器上的现有配置。GUI：**维护 > 备份 Flash**
11. 将主用主控制器上的映像升级到 ArubaOS 8，然后重新启动。GUI：**维护 > 映像管理**
12. 通过 CLI 设置对话框配置将由 MM 管理的主控制器。主控制器现在将成为 MC1

13. 重复第 11-12 步，将备用主控制器转换到 ArubaOS 8 并作为 MC2
14. 更改 **aruba-master**，使其指向群集 VIP
15. 先前在主控制器上端接的 AP 将查找群集 VIP，升级其映像，在 MC1 或 MC2 上进行端接（取决于群集领导者如何对 AP 进行负载分担），以及广播配置的 SSID
16. 将无线客户端连接到 SSID 以测试连接
17. 可选择通过运行语音/视频应用程序并断开用户的主用控制器来测试无缝客户端故障切换

独立 MC 和备用独立

拓扑结构

此 ArubaOS 8 设计包含由另一个独立 MC 备份的独立 MC。与在主控制器和备用主控制器 ArubaOS 6 设计中一样，VRRP 在主用-备用配置下在两个独立控制器之间使用。同样，在这些控制器之间配置高可用性（AP 快速故障切换），以便除设置到备用独立控制器的备用隧道外，AP 还在主用独立控制器上端接其隧道。

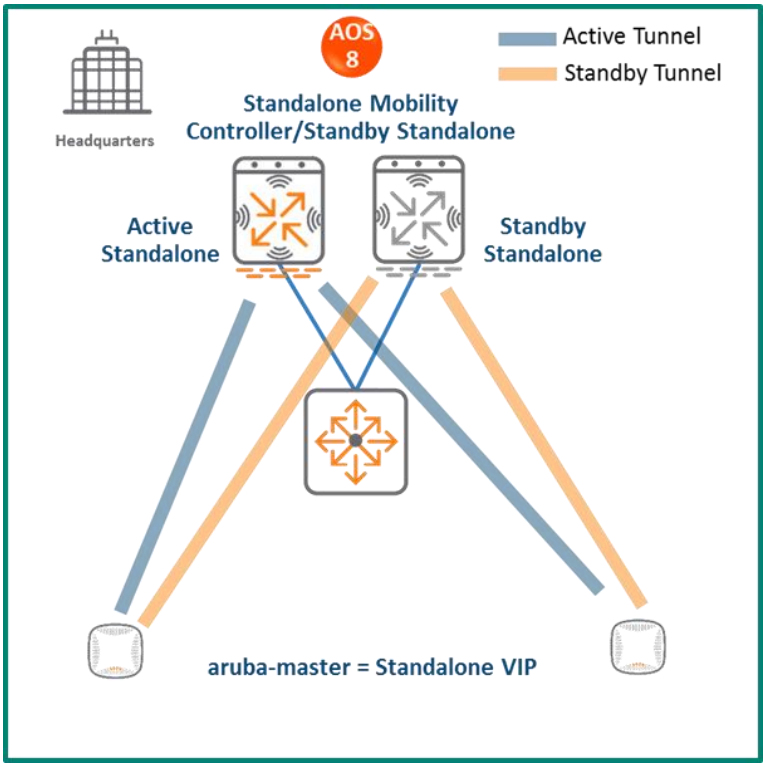


图 157 *独立 MC 和备用独立拓扑结构*

与 ArubaOS 6 主控制器和备用主控制器设计一样，AP 快速故障切换检测不是亚秒级（即 AP 将等待八次错过的心跳才能到主控制器），但由于 AP 已经具有到备用独立控制器的备用隧道，因此故障切换本身会快速进行。如果出现故障，独立控制器将成为新的主用控制器。

设计优势

- 迁移不需要其他硬件
- 多线程 CLI
- 自动完成配置文件名称

设计警告

- AP 只能在主用独立控制器上进行端接
- 已配置了 VRRP 和 AP 快速故障切换，但在此设计中不支持 AP 快速故障切换的控制器间心跳。AP 快速故障切换检测将不是亚秒级，因为该故障切换取决于 VRRP 延迟。检测时，对于所有 AP，实际故障切换本身都将因它们的现有备用隧道而快速同时进行

迁移要求

需要手动或通过“我的网络门户”迁移 AP 和 PEF 等许可

迁移选项

无迁移工具支持。迁移只能手动执行。

迁移策略

现有 ArubaOS 6 部署

- 主用和备用主控制器
- AP 在主用主控制器上进行端接，备用主控制器作为备份

新 ArubaOS 8 部署

- 主用独立和备用独立控制器
- 具有主用和备用隧道的 AP 分别在主用和备用控制器上进行端接

迁移程序

手动迁移需要完全重新构建现有 ArubaOS 6 拓扑结构。

1. 备份 ArubaOS 6 主控制器上的现有配置
2. 将主用主控制器上的映像升级到 ArubaOS 8，然后重新启动控制器。
3. 通过 CLI 设置对话框将主用主控制器设置为 ArubaOS 8 独立控制器。该主控制器现在将成为 ArubaOS 8 独立控制器
4. 重复第 2-3 步，将备用主控制器转换为 ArubaOS 8 独立控制器
5. 在主用独立控制器上配置许可。在作为第 6 步的一部分配置了数据库同步后，备用独立控制器将从主用独立控制器继承许可
6. 在两个独立控制器之间配置主冗余。由于 VRRP 配置，将在 MC1 与 MC2 之间创建 VIP。从现在开始，配置管理将通过 VIP 进行
7. 在 MM 节点（CLI 中的 /mm）下创建 AP 组和 SSID。这会将通用配置推送到两个独立控制器
8. 为两个独立控制器配置 AP 快速故障切换
9. 在 **MM > 配置 > 接入点 > 白名单**下，将 AP 列入白名单
10. 更改 **aruba-master**，使其指向独立 VIP
11. 然后这些 AP 将查找 VIP（即主用独立控制器），升级其映像，在 VIP 上端接它们的隧道，以及广播配置的 SSID
12. 将无线客户端连接到 SSID 并测试连接
13. （可选）通过断开主用独立控制器的连接来测试客户端故障切换

主控制器和单本地控制器

在该 ArubaOS 6 设计中，主控制器正在管理本地控制器。对于主控制器和本地控制器，建议使用相同控制器型号。这种设计可有两种变体：

- **冗余模式**（也称为主用-备用模式）- AP 在本地控制器上进行端接，主控制器为本地控制器提供冗余。在这些控制器之间配置高可用性（AP 快速故障切换），以便在这些 AP 失去与本地控制器的连接时，它们能够立即故障切换到主控制器。
- **容量模式**（也称为主用-主用模式）- 这是一种替代的单-主、单本地控制器设计，其中主控制器除管理本地控制器外，还与本地控制器分担 AP 负载。在控制器之间配置高可用性（AP 快速故障切换），以便在一个控制器出现故障时，其 AP 能够无缝故障切换到其他控制器。

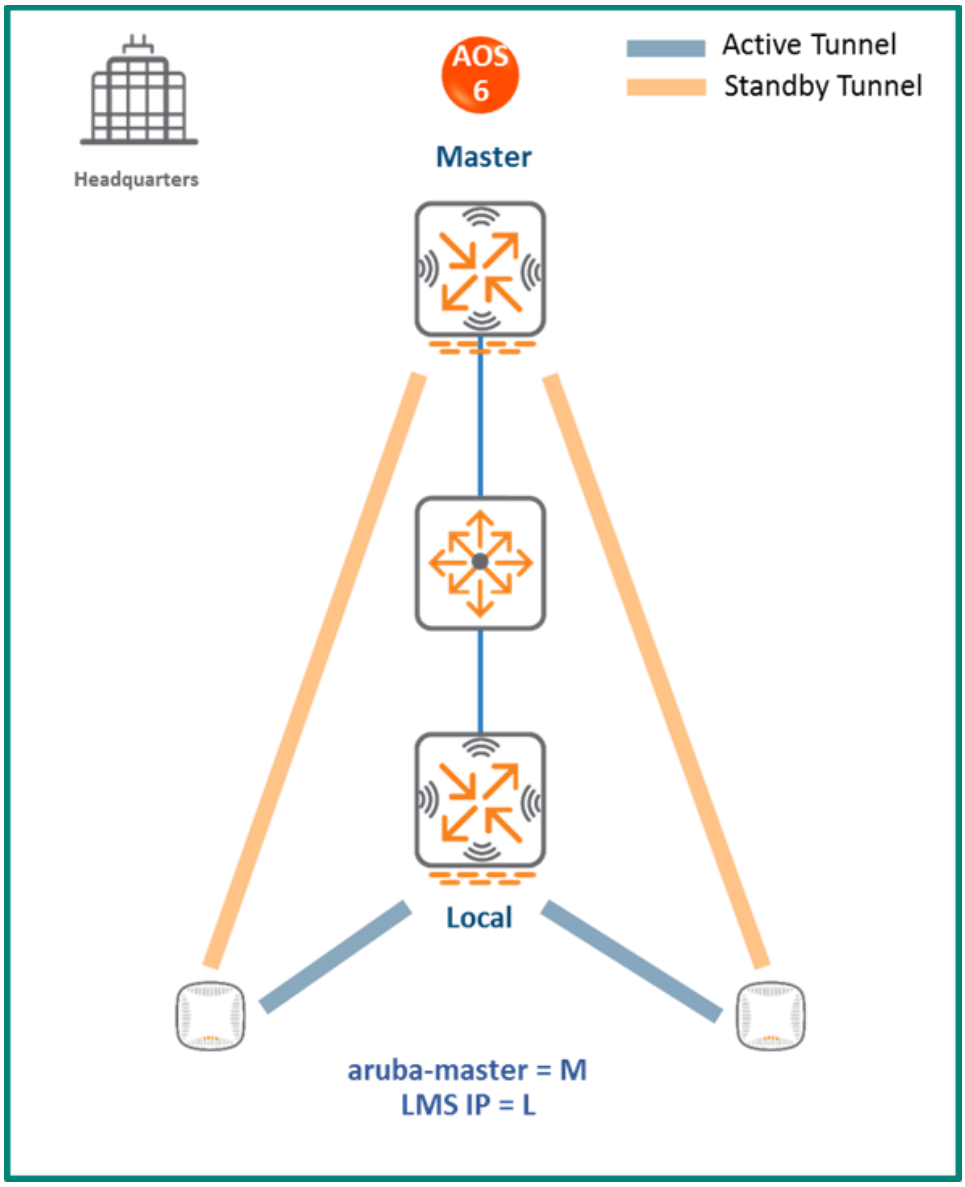


图 158 *主控制器和单本地控制器*

在这两种设计中：

- 每个控制器都需要有足够的容量来容纳可能从第二个控制器故障切换的 AP 数量。在冗余模式中，每个控制器一般以最多 80% 的控制器容量端接 AP。在容量模式中，每个控制器一般以最多 40% 的控制器容量端接 AP
- AP 快速故障切换检测不是亚秒级（即 AP 将等待八次错过的心跳才能到主控制器），但由于所有 AP 已经构建了到备用独立控制器的备用隧道，因此故障切换本身会快速进行。备用独立控制器在故障切换时成为新的主用控制器

MM 端接 MC

拓扑结构

在该 ArubaOS 8 设计中，最初部署和配置了 MM。ArubaOS 6 主控制器和本地控制器成为由 MM 管理的 MC。这些控制器可形成群集，以用于冗余和 AP/客户端负载分担目的。被选为群集领导者的控制器将确定如何在群集中对 AP 和客户端进行负载分担。

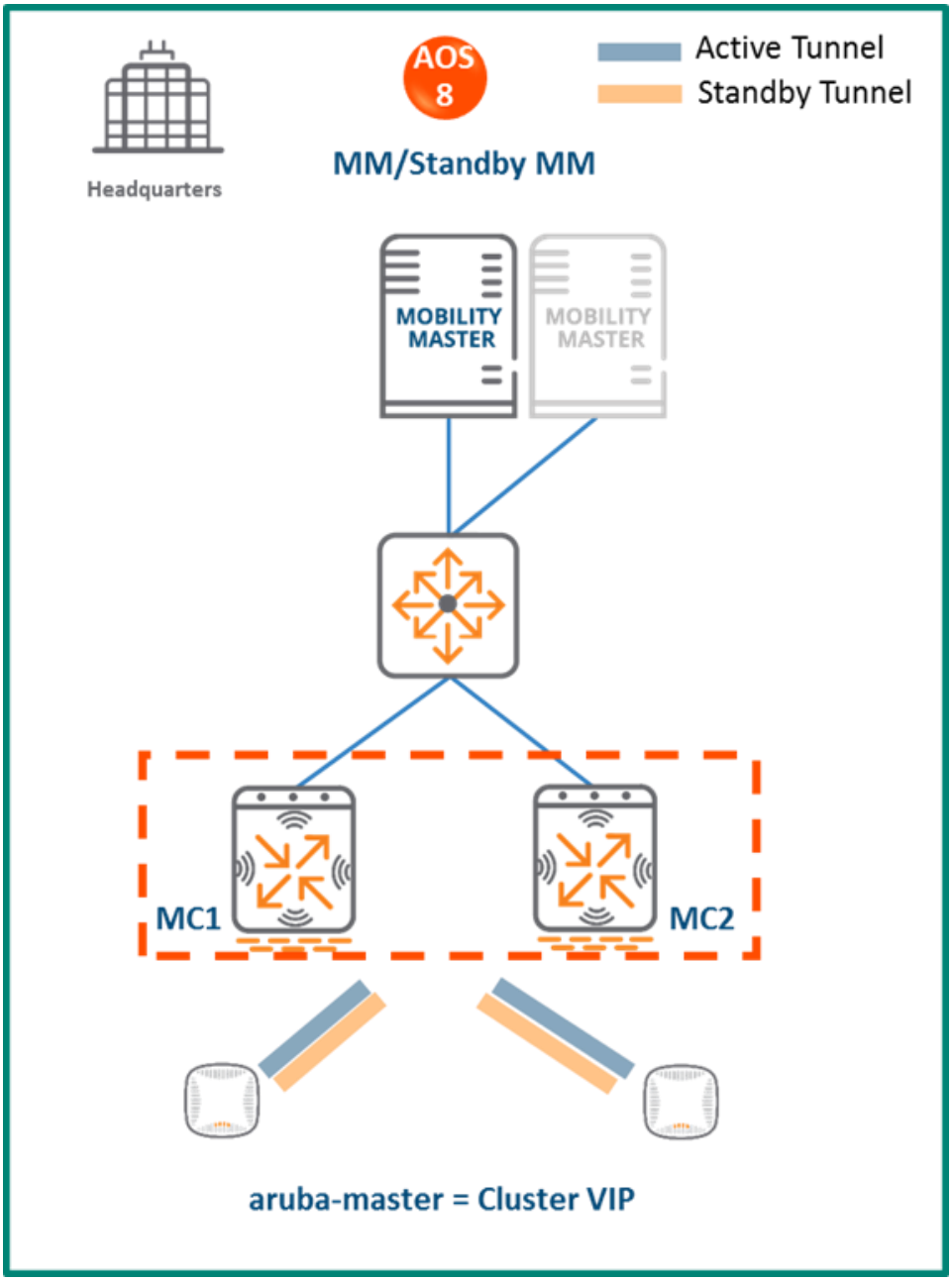


图 159 *MM 端接 MC 拓扑结构*

配置层次结构

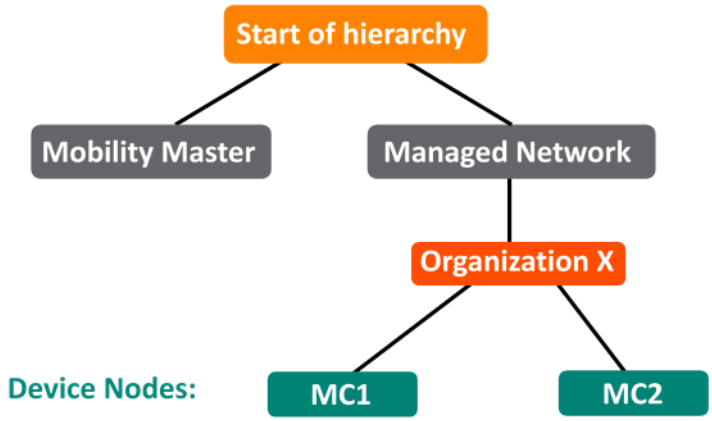


图 160 *MM 端接 MC 配置层次结构*

设计优势

- **最大化优势** - MM 端接 MC 设计是充分利用 ArubaOS 8 功能的理想选择
- **可扩展性** - 通过 MM 可轻松添加和管理新控制器
- **易于迁移** - 如果现有部署具有多个拓扑结构，则在 MM 下可将它们全部迁移到层次结构中它们自己的节点中
- **管理** - 集中式控制器配置和管理
- **分层配置模型** - 在节点（USA、West Coast、California、Santa Clara 等逻辑文件夹）上执行配置，以及根据位置和环境将每个控制器分配到特定节点
- **群集** - 在群集中具有控制器可在控制器之间实现无缝客户端故障切换，同时不影响用户体验。群集功能还可促进客户端漫游以及 AP 和客户端负载分担。必须进行群集才能支持实时升级
- **实时升级** - 实时升级控制器群集，并且最终用户不会遇到任何连接或性能损失。无需为网络升级安排维护周期
- **AirMatch** - RF 智能集中在 MM 上，这可显著改进 WLAN 的 RF 管理和干扰抑制功能
- **REST API 支持**
- **多版本支持** - 可灵活地升级单个控制器，以便测试新功能或故障修复。群集中的控制器需要运行相同的 ArubaOS 软件版本，并且可一同进行升级
- **在线软件模块升级** - 可在运行时更新 UCC、AirGroup、AppRF 等可加载服务模块 (LSM)，无需安排任何维护周期

设计警告

- MM 不端接任何 AP。只能在 MC 上端接 AP。

迁移要求

- 需要购买虚拟 MM 容量许可或购买硬件 MM（也可以选择购买备用硬件 MM）
- 如果您有备用 MM，则将在这两个 MM 间聚合并同步每个 MM 上的许可
- 需要手动或通过“我的网络门户”迁移其他许可，例如 AP 和 PEF

迁移选项

- 可手动或通过迁移工具进行迁移
- 以下详细说明了手动迁移。要使用迁移工具执行迁移，请参阅 ArubaOS 8 迁移指南

迁移策略

现有 ArubaOS 6 部署

- 主和本地
- AP 在本地控制器上进行端接，主控制器作为备份

新 ArubaOS 8 部署

- MM 由备用 MM 进行备份
- MM 管理控制器 MC1 和 MC2
- AP 在 MC1 和 MC2 上进行端接

迁移程序

手动迁移需要通过执行以下步骤完全重新构建现有 ArubaOS 6 拓扑结构：

1. 部署 MM 并执行初始设置
2. 在 MM 上配置许可
3. 在 MM 上创建配置层次结构以及将主和本地主控制器 MAC 地址列入白名单
4. 如果还正在安装 MM，则重复第 1 步
5. 如果已部署了 MM，则配置 MM 冗余。将使用 MM VIP 进行配置管理
6. 在 MC 之间配置群集，以及实现 AP 负载分担
7. 在群集成员 IP 之间创建 VIP，也可以选择为 RADIUS COA 创建 VIP
8. 创建 AP 组和 SSIDGUI：**托管网络 > （选择节点） > AP 组。**GUI：**托管网络 > （选择节点） > 任务 > 创建新 WLAN**
9. 将 MM 上的 AP 列入白名单，并将它们映射到相应的 AP 组。GUI：**托管网络 >（选择节点）> 配置 > 接入点 > 白名单**
10. 备份 ArubaOS 6 主控制器和本地控制器上的现有配置。GUI：**维护 > 备份 Flash**
11. 将本地控制器上的映像升级到 ArubaOS 8，然后重新启动。GUI：**维护 > 映像管理**

12. 通过 CLI 设置对话框配置将由 MM 管理的本地控制器。本地控制器现在将成为 MC1
13. 现在重复第 11-12 步，将主控制器转换为 MC2
14. 更改 **aruba-master**，使其指向群集 VIP
15. 先前在本地控制器上端接的 AP 将查找群集 VIP，升级其映像，在 MC1 或 MC2 上进行端接（取决于群集领导者如何对 AP 进行负载分担），以及广播配置的 SSID
16. 将无线客户端连接到 SSID 并测试连接
17. 可选择通过运行语音/视频应用程序并断开用户的主用控制器来测试无缝客户端故障切换

具有主冗余的独立 MC

拓扑结构

此 ArubaOS 8 设计包含由另一个独立 MC 备份的独立 MC。在主用-备用配置下，在两个独立控制器之间启用 VRRP。此外还在这些控制器之间配置高可用性（AP 快速故障切换），以便使 AP 除在主用独立控制器上端接其隧道外，还设置到备用独立控制器的备用隧道。

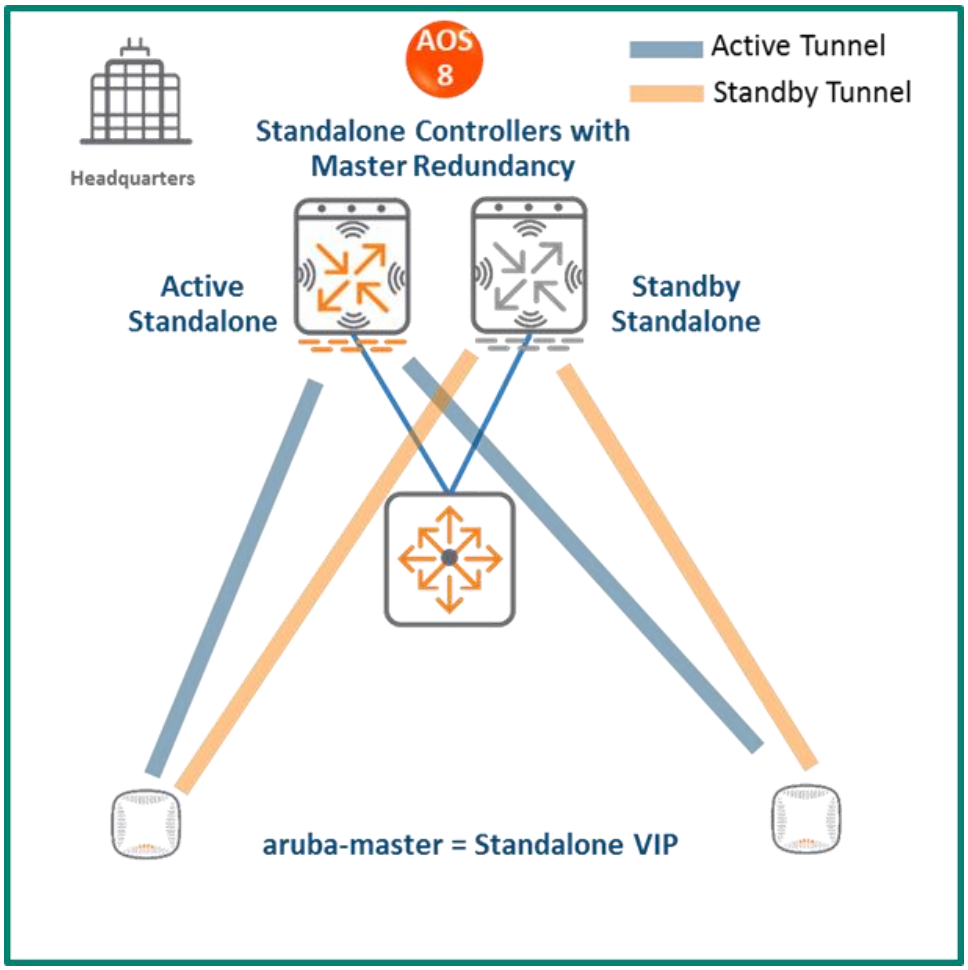


图 161 *具有主冗余的独立 MC*

AP 快速故障切换检测不是亚秒级（即 AP 将等待八次错过的心跳才能到主控制器），但由于这些 AP 已经具有到备用独立控制器的备用隧道，因此故障切换本身会快速进行。如果出现故障，独立控制器将成为新的主用控制器。

设计优势

- 迁移不需要其他硬件
- 多线程 CLI
- 自动完成配置文件名称

设计警告

- AP 只能在主用独立控制器上进行端接
- 无 AP 快速故障切换。这两个独立控制器之间的主冗余配置使用 VRRP 检测故障切换，这意味着 AP 故障切换将不是亚秒级，因为该故障切换机制取决于 VRRP 延迟

迁移要求

需要手动或通过“我的网络门户”迁移 AP 和 PEF 等许可

迁移选项

无迁移工具支持。迁移只能手动执行。

迁移策略

现有 ArubaOS 6 部署

- 主和本地
- AP 在本地控制器上进行端接，主控制器作为备份

新 ArubaOS 8 部署

- 主用独立和备用独立控制器
- 具有主用和备用隧道的 AP 分别在主用和备用控制器上进行端接

迁移程序

手动迁移需要完全重新构建现有 ArubaOS 6 拓扑结构。

1. 备份 ArubaOS 6 主控制器和本地控制器上的现有配置
2. 将本地控制器上的映像升级到 ArubaOS 8，然后重新启动控制器
3. 通过 CLI 设置对话框将本地控制器设置为 ArubaOS 8 独立控制器。本地控制器将成为独立控制器
4. 将主控制器上的映像升级到 ArubaOS 8，然后重新启动控制器
5. 通过 CLI 设置对话框将主控制器设置为 ArubaOS 8 独立控制器。主控制器将成为另一个独立控制器
6. 在主用独立控制器上配置许可。在作为第 7 步的一部分配置了数据库同步后，备用独立控制器将从主用独立控制器继承许可
7. 在两个独立控制器之间配置主冗余。由于 VRRP 配置，将创建 VIP。从现在开始，配置管理将通过 VIP 进行
8. 导航到 **/mm**，然后创建 AP 组和 SSID
9. 为两个独立控制器配置 AP 快速故障切换
10. 在 **MM > 配置 > 接入点 > 白名单**下，将您的 AP 列入白名单
11. 更改 **aruba-master**，使其指向独立 VIP
12. 然后这些 AP 将查找 VIP（即主用独立控制器），升级其映像，在 VIP 上端接它们的隧道，以及广播配置的 SSID
13. 将无线客户端连接到 SSID 并测试连接
14. （可选）通过断开主用独立控制器的连接来测试客户端故障切换

主控制器和多本地控制器（单园区）

在该 ArubaOS 6 设计中，主（由备用主控制器备份）控制器正在管理一组本地控制器。AP 在一个本地控制器上进行端接，其他本地控制器作为备份。AP 快速故障切换被配置为在与主控制器的连接中断时为 AP 提供亚秒级故障切换。

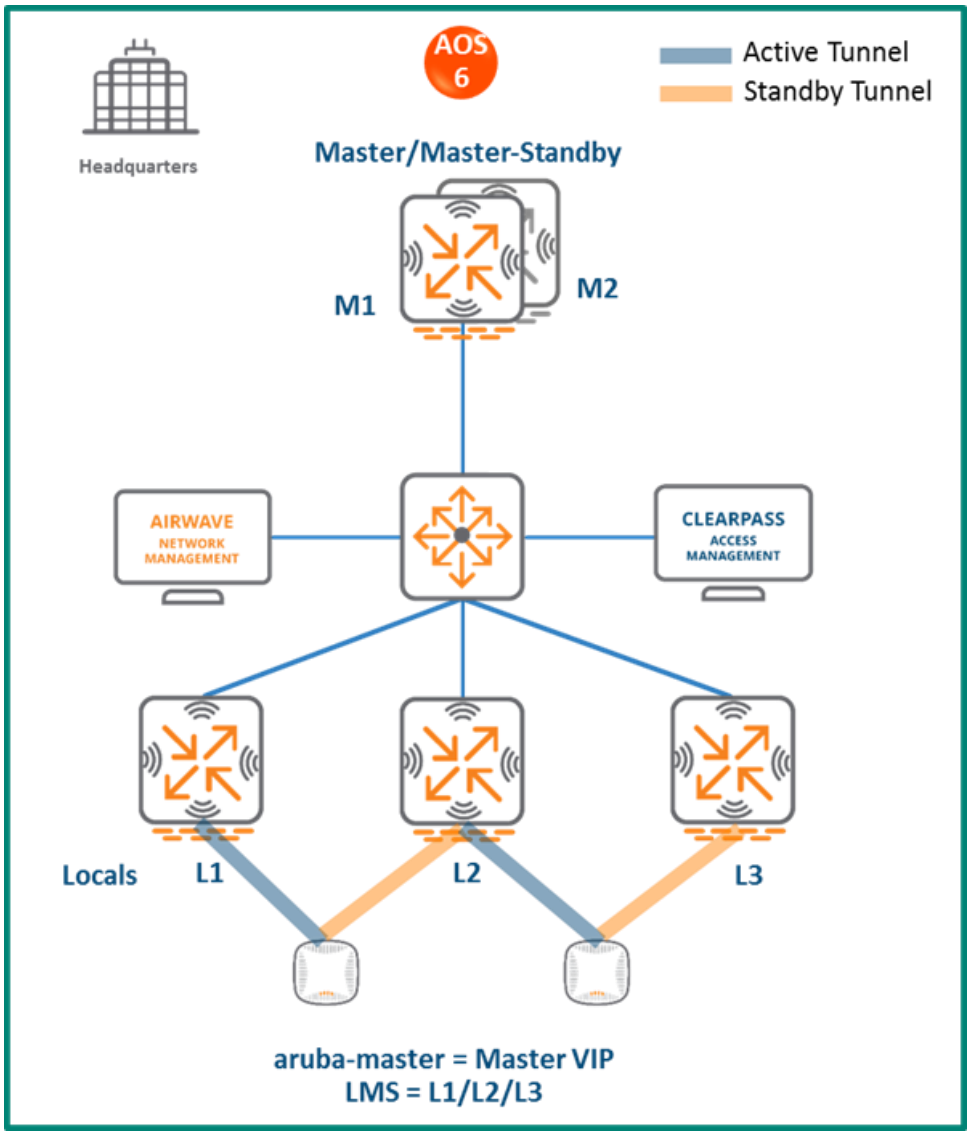


图 162 *主控制器和单本地控制器*

MM 端接 MC

拓扑结构

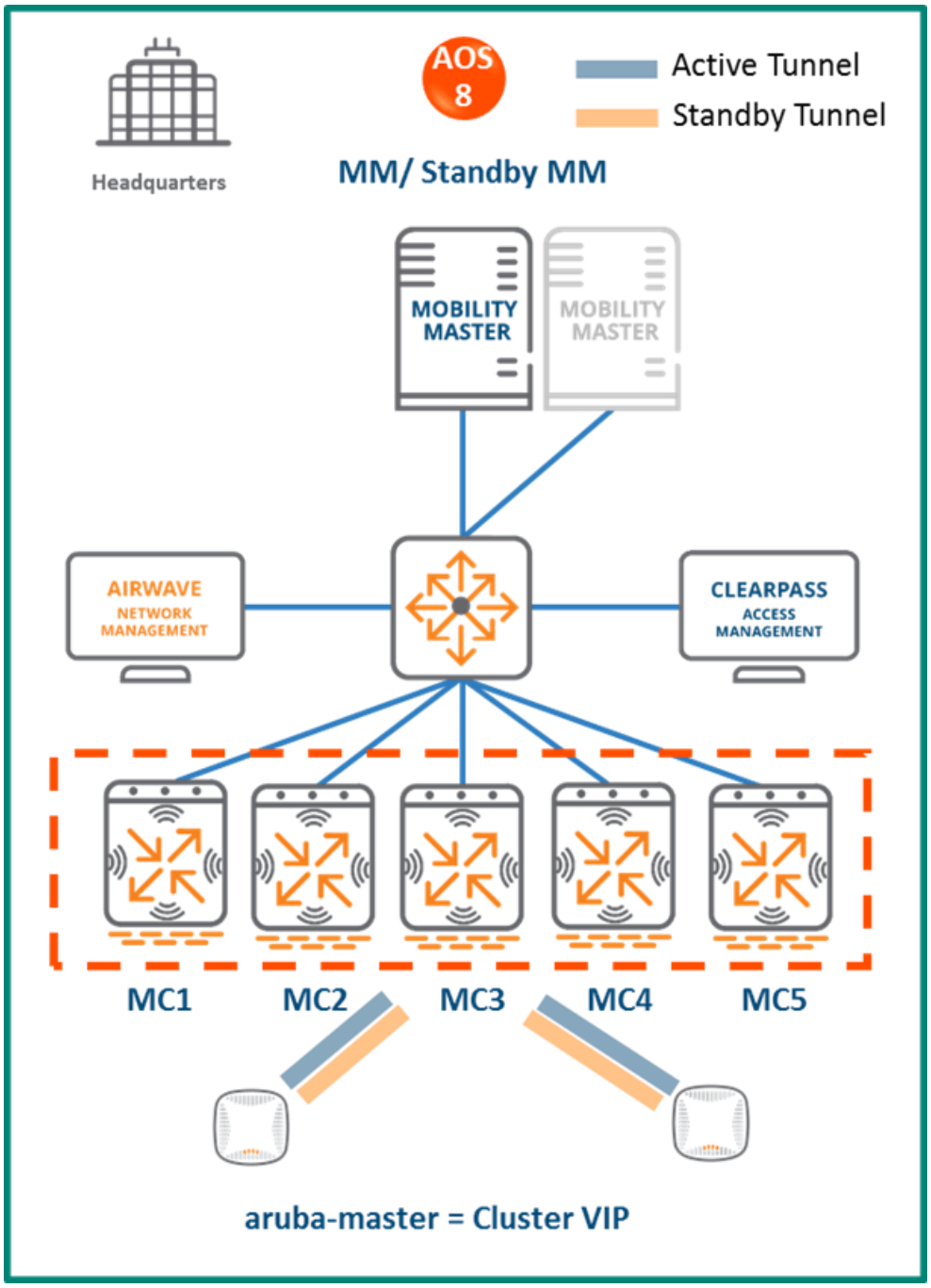


图 163 *MM 端接 MC 拓扑结构*

在该 ArubaOS 8 设计中：

- MM（虚拟或硬件）与备用 MM 一同加以部署和配置
- 每个 ArubaOS 6 本地控制器（L1、L2 和 L3）均成为 ArubaOS 8 MC（MC1、MC2、MC3）
- ArubaOS 6 主控制器 (M1) 和备用主控制器 (M2) 成为两个额外 ArubaOS 8 MC（MC4 和 MC5）

- 这些 MC 可成为群集的一部分，并且分担 AP 和客户端负载
- 如果这些本地控制器位于不同地理位置，则在迁移后，在 L1、L2 和 L3 上端接的 AP 现在将分别在 MC1、MC2 和 MC3 上进行端接
- 如果所有本地控制器均为一个大型园区的一部分，则群集领导者将在 MC1-MC5 之间分配 AP 和客户端负载

配置层次结构

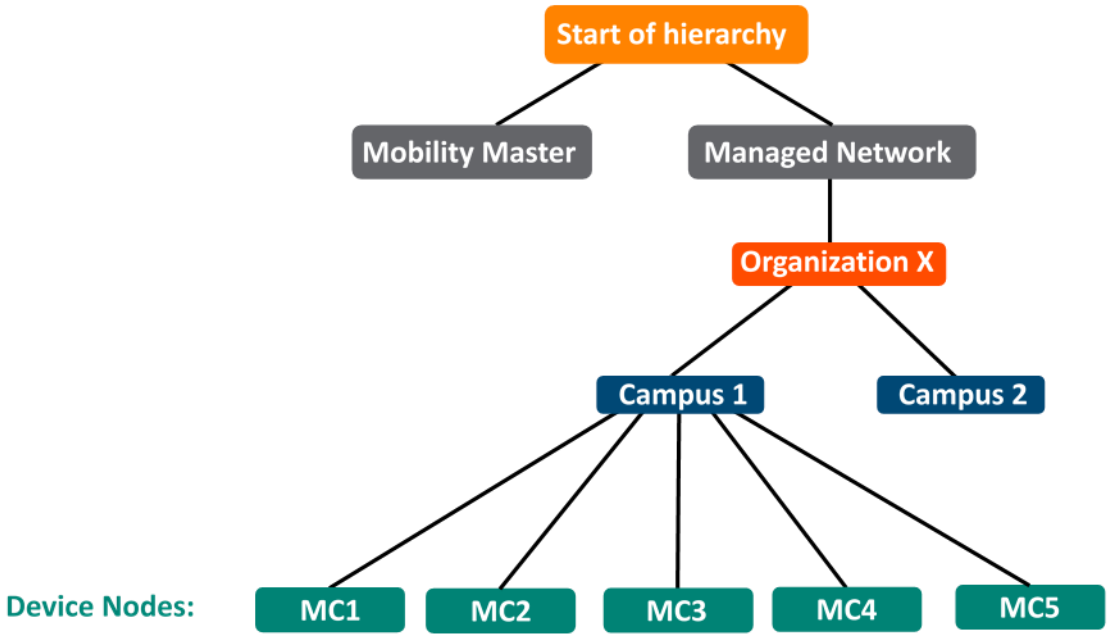


图 164 *MM 端接 MC 配置层次结构*

设计优势和注意事项

- **最大化优势** - MM 端接 MC 设计是充分利用 ArubaOS 8 功能的理想选择
- **可扩展性** - 通过 MM 可轻松添加和管理新控制器
- **易于迁移** - 如果现有部署具有多个拓扑结构，则在 MM 下可将它们全部迁移到层次结构中它们自己的节点中
- **管理** - 集中式控制器配置和管理
- **分层配置模型** - 在节点（USA、West Coast、California、Santa Clara 等逻辑文件夹）上执行配置，以及根据位置和环境将每个控制器分配到特定节点
- **群集** - 在群集中具有控制器可在控制器之间实现无缝客户端故障切换，同时不影响用户体验。群集功能还可促进客户端漫游以及 AP 和客户端负载分担。必须进行群集才能支持实时升级。
- **实时升级** - 实时升级控制器群集，并且最终用户不会遇到任何连接或性能损失。无需为网络升级安排维护周期
- **AirMatch** - RF 智能集中在 MM 上，这可显著改进 WLAN 的 RF 管理和干扰抑制功能
- **REST API 支持**

- **多版本支持** - 可灵活地升级单个控制器，以便测试新功能或故障修复。群集中的控制器需要运行相同的 ArubaOS 软件版本，并且可一同进行升级
- **在线软件模块升级** - 可在运行时更新 UCC、AirGroup 和 AppRF 等可加载服务模块 (LSM)，无需安排任何维护周期。

迁移要求

- 需要购买虚拟 MM 容量许可或购买硬件 MM（也可以选择购买备用硬件 MM）
- 如果您有备用 MM，则将在这两个 MM 间聚合并同步每个 MM 上的许可
- 需要手动或通过“我的网络门户”迁移其他许可，例如 AP 和 PEF

迁移选项

- 可手动或通过迁移工具进行迁移
- 以下详细说明了手动迁移。要使用迁移工具执行迁移，请参阅 ArubaOS 8 迁移指南

迁移策略

现有 ArubaOS 6 部署

- 本地控制器 L1、L2 和 L3 以及主控制器 M1 和 M2
- 3 个 AP 组被配置为使 AP 组在 L1、L2 和 L3 中的每一个上进行端接。

新 ArubaOS 8 部署

- MM 由备用 MM 进行备份
- MM 管理 MC1、MC2、MC3、MC4 和 MC5
- AP 端接于：
  - MC1、MC2、MC3（在多站点园区且每个站点均有一个控制器的情况下）
  - 针对大型园区的群集 VIP

迁移程序

手动迁移需要通过执行下列步骤完全重新构建现有 ArubaOS 6 拓扑结构：这些步骤涉及在群集 VIP 上端接 AP。在多站点园区的情况下，这些 AP 可在三个本地管理交换机 (LMS) IP（MC1、MC2 或 MC3）中的一个上进行端接。

1. 部署 MM 并执行初始设置
2. 在 MM 上配置许可
3. 创建配置层次结构以及将 MM 上的 M1、M2 和 L1-L3 的 MAC 地址列入白名单
4. 如果安装备用 MM，则重复第 1 步
5. 如果正在安装备用 MM，则配置 MM 冗余。从现在开始，使用 MM VIP 进行配置管理
6. 在 MC 之间配置群集，以及实现 AP 负载分担
7. 在群集成员 IP 之间创建 VIP，也可以选择为 RADIUS COA 创建 VIP
8. 创建 AP 组和 SSIDGUI：**托管网络 > （选择节点） > AP 组。**GUI：**托管网络 > （选择节点） > 任务 > 创建新 WLAN**
9. 将 MM 上的 AP 列入白名单，并将它们映射到相应的 AP 组。GUI：**托管网络 > （选择您的节点） > 配置 > 接入点 > 白名单。**
10. 备份 ArubaOS 6 主控制器和本地控制器上的现有配置。GUI：**维护 > 备份 Flash**
11. 将本地控制器 L1 上的映像升级到 ArubaOS 8，然后重新启动。GUI：**维护 > 映像管理**
12. 通过 CLI 设置对话框配置将由 MM 管理的本地控制器 L1。L1 将成为 ArubaOS 8 MC1
13. 对 L2 和 L3，重复第 11-12 步，将它们转换为 ArubaOS 8 MC2 和 MC3
14. 重复第 11-12 步，将 M1 和 M2 转换为 MC4 和 MC5。可将这些控制器添加到群集中，以便在群集成员之间分担 AP 和客户端负载
15. 更改 **aruba-master**，使其指向群集 VIP
16. 在本地控制器上端接的 AP 将查找群集 VIP，升级其映像，在 MC1-MC5 中的一个上进行端接（取决于群集领导者如何对 AP 进行负载分担），以及广播配置的 SSID
17. 将无线客户端连接到 SSID 并测试连接
18. 可选择通过运行语音/视频应用程序并断开用户的主用控制器来测试无缝客户端故障切换

MC Master 端接 MC

拓扑结构

此 ArubaOS 8 设计包含一个作为 MC Master 部署的硬件控制器（可选择由另一个 MC Master 进行备份），其管理一组 MC。

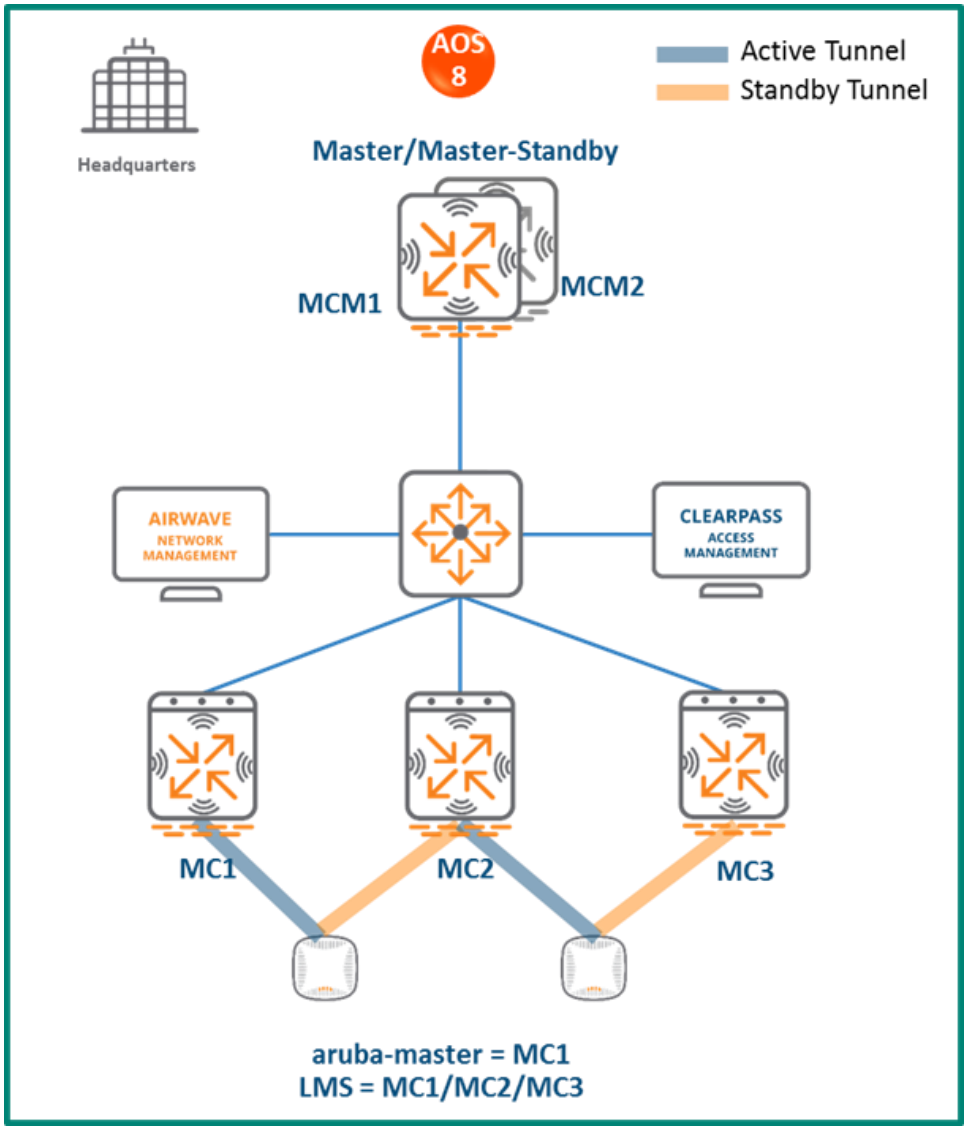


图 165 *MC Master 端接 MC 拓扑结构*

此设计有助于将部署过渡到无法部署 MM 的 ArubaOS 8。最终应将此 MC Master 拓扑结构迁移到 MM 拓扑结构，以便充分利用 ArubaOS 8 提供的功能。

在该设计中：

- ArubaOS 6 主控制器 (M1) 和备用主控制器 (M2) 成为 ArubaOS 8 MC Master（MCM1 和 MCM2）。
- ArubaOS 6 本地控制器（L1、L2 和 L3）成为 ArubaOS 8 MC（MC1、MC2 和 MC3）。
- 在 L1、L2 和 L3 上端接的 AP 现在将分别在 MC1、MC2 和 MC3 上进行端接。

配置层次结构

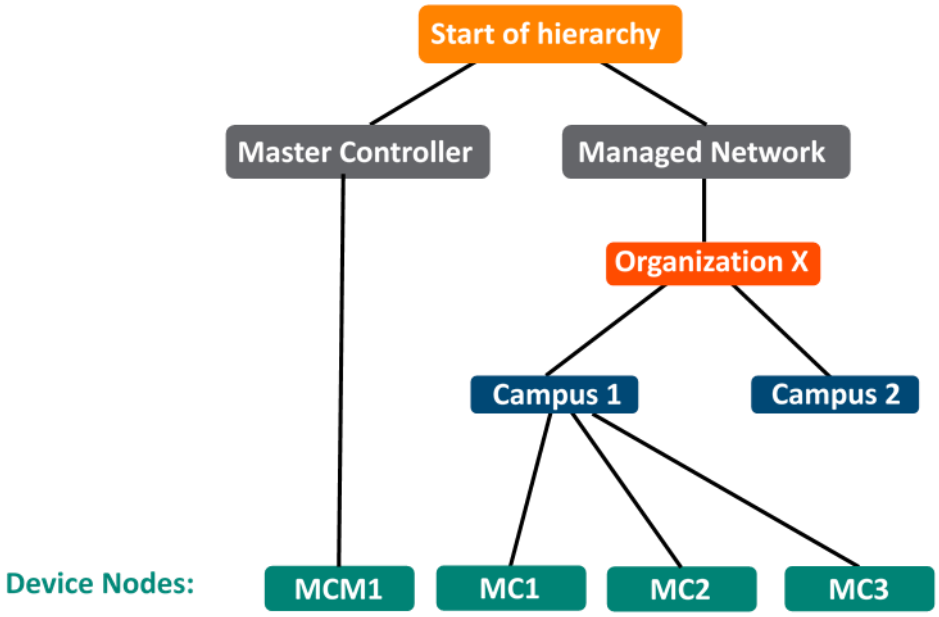


图 166 *MC Master 端接移动性配置层次结构*

设计优势

- 保持类似的拓扑结构，在该拓扑结构中，MC Master 管理 MC，并且只要 MC Master 是 Aruba 7030 或更大的控制器，便不需要额外硬件
- 分层配置模式提供 WLAN 的完全集中式配置和管理
- 其他控制器可稍后添加，并由 MC Master 加以管理

设计警告

- 需要购买 Aruba 7030 或更大的控制器来作为 MC Master 以及备用 MCM（如果尚未存在）
- 不支持在 MC Master 上端接 AP。这对 AP 端接选择具有以下影响：
  - 在 ArubaOS 6 中的主控制器上端接的任何 AP 在迁移前都将需要在本地控制器间重新分配。本地控制器应具有足够的容量来容纳额外 AP
  - AP 可在 MC 之间进行故障切换，但无法故障切换到 MC Master
- 在 MC Master 部署中不支持群集功能。MC 之间的 AP 快速故障切换是唯一的控制器冗余选择
- 不支持 AirMatch
- 该拓扑结构中的所有控制器都必须运行相同的 ArubaOS 版本
- 没有集中式监控

迁移要求

- 验证 ArubaOS 6 主控制器是否满足 MC Master 硬件要求（Aruba 7030 或任何 Aruba 7200 系列控制器）
- 确保 ArubaOS 6 主控制器未端接任何 AP，因为 ArubaOS 8 MC Master 不支持 AP 端接
- 确保已手动或通过“我的网络门户”迁移了 AP、PEF 和其他所有许可

迁移选项

- 可手动或通过迁移工具进行迁移
- 以下详细说明了手动迁移。要使用迁移工具执行迁移，请参阅 ArubaOS 8 迁移指南

迁移策略

现有 ArubaOS 6 部署

- 本地控制器 L1、L2、L3 和主控制器 M1 和 M2
- 3 个 AP 组被配置为在 L1、L2 和 L3 上进行端接。

新 ArubaOS 8 部署

- MCM1 由 MCM2 备份
- MCM1 管理 MC1、MC2 和 MC3

迁移程序

手动迁移需要通过执行下列步骤完全重新构建现有 ArubaOS 6 拓扑结构：

1. 备份 ArubaOS 6 主控制器和本地控制器上的现有配置。GUI：**维护 > 备份 Flash**
2. 将主控制器 M1 上的映像升级到 ArubaOS 8，然后重新启动控制器
3. 通过 CLI 设置对话框将 M1 配置为 MC Master。M1 现在将成为 MCM1
4. 重复第 2 步和第 3 步，将 M2 转换为 MCM2
5. 在 MCM1 与 MCM2 之间配置主冗余。MC Master VIP 将用于配置管理
6. 在 MC Master 上配置许可
7. 在 MC Master 上创建配置层次结构，以及将控制器 L1-L3 的 MAC 地址列入白名单
8. 在 **/md**（或子节点）下创建三个 AP 组，每个 AP 组分别具有 MC1、MC2 和 MC3 的 LMS IP。GUI：**托管网络 > （选择节点） > AP 组**
9. 为每个 AP 组均创建一个 SSID。GUI：**托管网络 > （选择节点） > 任务 > 创建新 WLAN**
10. 将 MC Master 上的 AP 列入白名单。这包括将它们映射到各自的 AP 组。GUI：**托管网络 > （选择节点） > 配置 > 接入点 > 白名单**
11. 将本地控制器 L1 上的映像升级到 ArubaOS 8，然后重新启动。GUI：**维护 > 映像管理**

12. 通过 CLI 设置对话框配置将由 MC Master 管理的本地控制器 L1。L1 将成为 MC1
13. 现在对 L2 和 L3，重复第 11-12 步，将它们转换为 ArubaOS 8 MC2 和 MC3
14. 将 **aruba-master** 更改为 MC1 的 IP
15. 在 MC1 可显示在 MC Master 上后，L1 上端接的 AP 将查找 MC1，升级其映像，下载用于 MC1 的 LMS-IP，在 MC1 上端接它们的隧道，以及广播配置的 SSID
16. 同样，L2 和 L3 上的 AP 将分别显示在 MC2 和 MC3 上
17. 将无线客户端连接到 SSID 并测试连接
18. 可选择通过 MC Master 配置 AP 快速故障切换，以便在 MC 之间实现亚秒级 AP 故障切换

主控制器和多本地控制器（多园区）

在该 ArubaOS 6 设计中，由备用主控制器备份的主控制器正在管理一组本地控制器。AP 在一个本地控制器上进行端接，其他本地控制器作为备份。AP 快速故障切换被配置为在与主控制器的连接中断时为 AP 提供亚秒级故障切换。

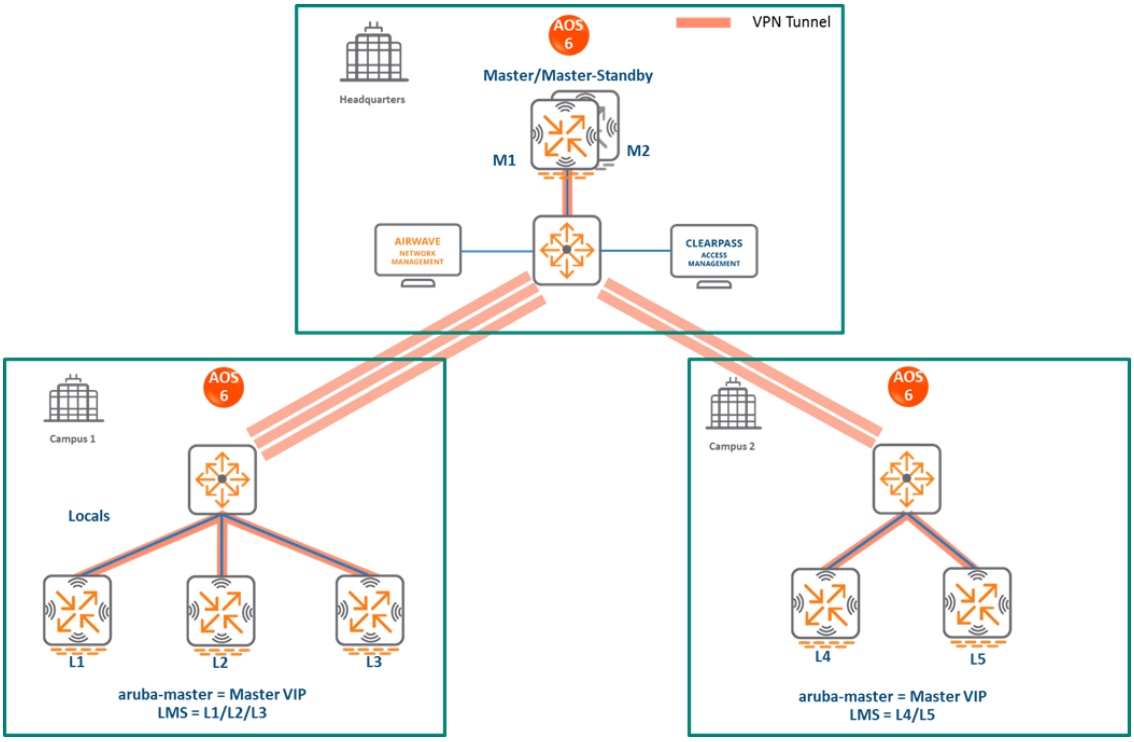


图 167 *主控制器和多本地控制器（多园区）*

MM 端接 MC

拓扑结构

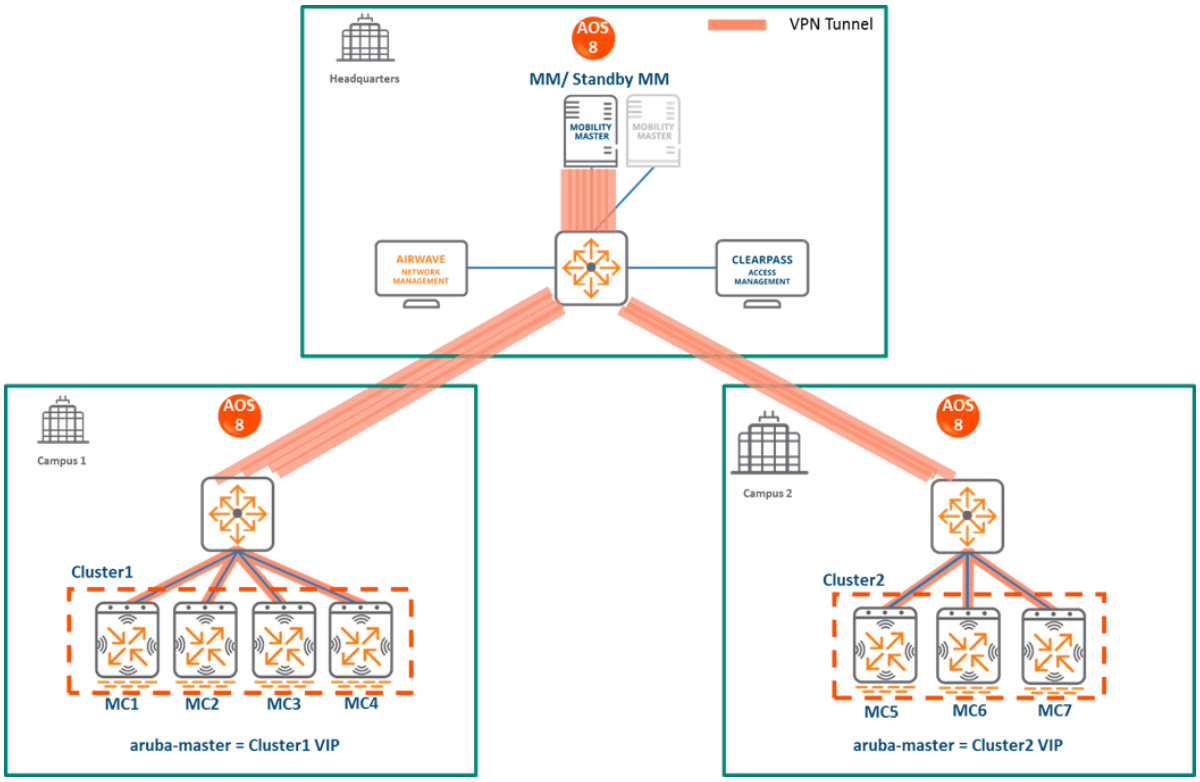


图 168 *MM 端接 MC 拓扑结构*

在该 ArubaOS 8 设计中：

- MM（虚拟或硬件）与备用 MM 一同加以部署和配置
- 在 Campus 1 中，每个 ArubaOS 6 本地控制器（L1、L2 和 L3）均成为 ArubaOS 8 MC（MC1、MC2、MC3）
- 在 Campus 2 中，每个 ArubaOS 6 本地控制器（L4 和 L5）均成为 ArubaOS 8 MC（MC5 和 MC6）
- 每个园区中的 MC 均被配置为群集，并且将分担 AP 和客户端负载
- 所有 MC 均在 MM 上端接它们的 IPsec 隧道
- 如果这些本地控制器位于不同地理位置，则执行迁移，这样在 L1、L2 和 L3 上端接的 AP 现在将分别在 MC1、MC2 和 MC3 上进行端接
- 如果每个园区中的所有本地控制器均在同一位置，则在迁移后，群集领导者将在群集成员之间分配 AP 和客户端负载
- ArubaOS 6 主控制器 (M1) 和备用主控制器 (M2) 成为两个额外 ArubaOS 8 MC（MC4 和 MC7），在每个园区中可改变它们的用途，使它们成为群集成员
- 在通过 MPLS 和/或 Internet 链路将远程站点与 MM 分离的情况下，如果需要路由用户流量以访问 HQ 资源，则建议在 HQ 部署硬件 VPNC，以便在每个站点端接来自控制器的 IPsec 连接。

配置层次结构

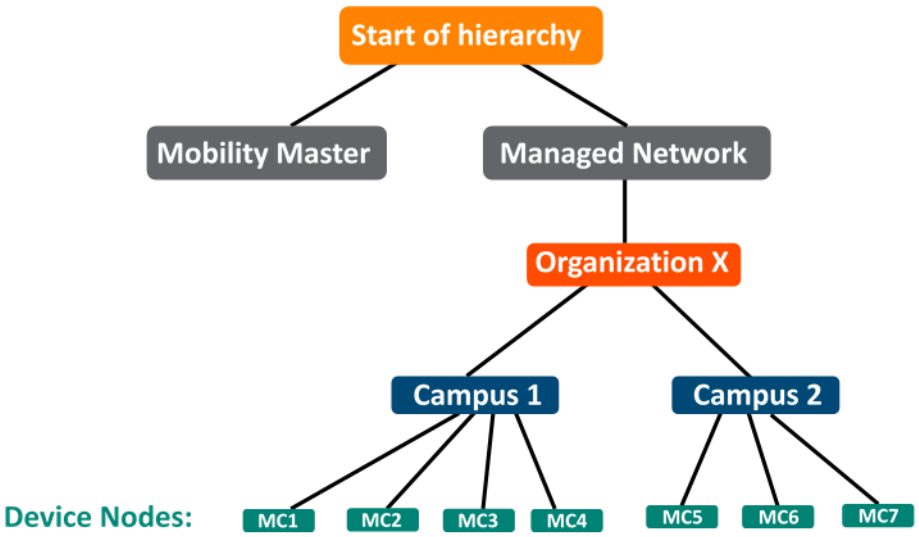


图 169 *MM 端接 MC 配置层次结构*

设计优势

- **最大化优势** - MM 端接 MC 设计是充分利用 ArubaOS 8 功能的理想选择
- **可扩展性** - 通过 MM 可轻松添加和管理新控制器
- **易于迁移** - 如果现有部署具有多个拓扑结构，则在 MM 下可将它们全部迁移到层次结构中它们自己的节点中
- **管理** - 集中式控制器配置和管理
- **分层配置模型** - 在节点（USA、West Coast、California、Santa Clara 等逻辑文件夹）上执行配置，以及根据位置和环境将每个控制器分配到特定节点
- **群集** - 在群集中具有控制器可在控制器之间实现无缝客户端故障切换，同时不影响用户体验。群集功能还可促进客户端漫游以及 AP 和客户端负载分担。必须进行群集才能支持实时升级。
- **实时升级** - 实时升级控制器群集，并且最终用户不会遇到任何连接或性能损失。无需为网络升级安排维护周期
- **AirMatch** - RF 智能集中在 MM 上，这可显著改进 WLAN 的 RF 管理和干扰抑制功能
- **REST API 支持**
- **多版本支持** - 可灵活地升级单个控制器，以便测试新功能或故障修复。群集中的控制器需要运行相同的 ArubaOS 软件版本，并且可一同进行升级
- **在线软件模块升级** - 可在运行时更新 UCC、AirGroup、AppRF 等可加载服务模块 (LSM)，无需安排任何维护周期

设计警告

- MM 不端接 AP。只能在 MC 上端接 AP
- 如果现有 ArubaOS 6 部署有超过 1000 个控制器和/或 10,000 个 AP，则迁移到 ArubaOS 8 MM 部署需要部署多个 MM

迁移要求

- 需要购买虚拟 MM 容量许可或购买硬件 MM
- 还可以部署备用硬件 MM，在这种情况下，每个 MM 上的许可都将在两个 MM 间进行聚合和同步
- 需要手动或通过“我的网络门户”迁移其他许可，例如 AP 和 PEF

迁移选项

- 可手动或通过迁移工具进行迁移
- 以下详细说明了手动迁移。要使用迁移工具执行迁移，请参阅 ArubaOS 8 迁移指南

迁移策略

现有 ArubaOS 6 部署

- **HQ**：主控制器 M1 和 M2
- **Campus1**：L1、L2 和 L3。三个 AP 组被配置为在每个本地控制器上进行端接
- **Campus2**：L4 和 L5。两个 AP 组被配置为在每个本地控制器上进行端接

新 ArubaOS 8 部署

- MM 由备用 MM 进行备份
- 除 Campus2 中的 MC5、MC6 和 MC7 外，MM 还将管理 Campus1 中的 MC1、MC2、MC3、MC4
- AP 在每个园区中的一个群集成员上进行端接

迁移程序

手动迁移需要通过执行下列步骤完全重新构建现有 ArubaOS 6 拓扑结构：这些步骤涉及在群集 VIP 上端接 AP。在多站点园区的情况下，这些 AP 可在三个 LMS IP（MC1、MC2 或 MC3）中的任何一个上进行端接

MM 特定

1. 部署 MM 并执行初始设置
2. 在 MM 上配置许可
3. 创建配置层次结构以及将 MM 上的 M1、M2 和 L1-L5 的 MAC 地址列入白名单。将以下配置层次结构下的每个设备列入白名单：
   - 在**托管网络 > Campus1** 下列入白名单的 L1、L2、L3 和 M1
   - 在**托管网络 > Campus2** 下列入白名单的 L4、L5 和 M2
4. 如果正在安装备用 MM，则重复第 1 步
5. 如果正在安装备用 MM，则配置 MM 冗余。MM VIP 将用于配置管理

Campus1

1. 在 MC1-MC4 之间配置群集。此外还可实现 AP 负载分担。GUI: **托管网络 > Campus1 > 服务 > 群集**
2. 在群集成员 MC1-MC4 之间创建 VIP（现在称为“Cluster1 VIP”）。GUI: **托管网络 > Campus1 > 服务 > 冗余 > 虚拟路由器表。**可选择为 RADIUS COA 创建 VIP
3. 创建 AP 组和 SSID。GUI: **托管网络 > Campus1 > AP 组。**GUI: **托管网络 > Campus1 > 任务 > 创建新 WLAN**
4. 将 MM 上的 Campus1 AP 列入白名单。这包括将它们映射到相应的 AP 组。GUI: **托管网络 > Campus1 > 配置 > 接入点 > 白名单**
5. 备份 ArubaOS 6 控制器 L1-L3 和 M1 上的现有配置。GUI: **维护 > 备份 Flash**
6. 将本地控制器 L1 上的映像升级到 ArubaOS 8，然后重新启动。GUI: **维护 > 映像管理**
7. 通过 CLI 设置对话框配置将由 MM 管理的本地控制器 L1。L1 现在将成为 MC1
8. 重复第 6-7 步，将 L2、L3 和 M1 分别转换为 MC2、MC3 和 MC4
9. 在 Campus1 网络中，将 **aruba-master** 指向 Cluster1 VIP
10. 在 L1-L3 上端接的 AP 将查找群集 VIP，升级其映像，在 MC1-MC4 范围中的一个控制器上进行端接（取决于群集领导者如何对 AP 进行负载分担），以及广播 Campus1 的已配置 SSID
11. 将无线客户端连接到 SSID 并测试连接
12. 可选择通过运行语音/视频应用程序并断开用户的主用控制器来测试无缝客户端故障切换

Campus2

1. 在 MC5、MC6 和 MC7 之间配置群集，以及实现 AP 负载分担。GUI：**托管网络 > Campus2 > 服务 > 群集**
2. 在群集成员 MC5、MC6 和 MC7 之间创建 VIP（现在称为“Cluster2 VIP”）。GUI：**托管网络 > Campus2 > 服务 > 冗余 > 虚拟路由器表。**可选择为 RADIUS COA 创建 VIP
3. 创建 AP 组和 SSIDGUI：**托管网络 > Campus2 > AP 组。**GUI：**托管网络 > Campus2 > 任务 > 创建新 WLAN**
4. 将 MM 上的 Campus2 AP 列入白名单。这包括将它们映射到相应的 AP 组。GUI：**托管网络 > Campus1 > 配置 > 接入点 > 白名单**
5. 备份 ArubaOS 6 控制器 L4、L5 和 M2 上的现有配置。GUI：**维护 > 备份 Flash**
6. 将本地控制器 L4 上的映像升级到 ArubaOS 8，然后重新启动。GUI：**维护 > 映像管理**
7. 通过 CLI 设置对话框配置将由 MM 管理的本地控制器 L4。L4 现在将成为 MC5
8. 重复第 6-7 步，将 L5 转换为 MC6，以及将 M2 转换为 MC7
9. 在 Campus2 网络中，将 **aruba-master** 指向 Cluster2 VIP
10. 在 L4 和 L5 上端接的 AP 将查找群集 VIP，升级其映像，在 MC5-MC7 范围中的一个控制器上进行端接（取决于群集领导者如何对 AP 进行负载分担），以及广播 Campus2 的已配置 SSID
11. 将无线客户端连接到 SSID 并测试连接
12. 可选择通过运行语音/视频应用程序并断开用户的主用控制器来测试无缝客户端故障切换

MC Master 端接 MC

拓扑结构

此 ArubaOS 8 设计包含一个作为 MC Master 部署的硬件控制器（可选择由另一个 MC Master 进行备份），其管理不同园区中的一组 MC。

此设计有助于将部署过渡到无法部署 MM 的 ArubaOS 8。最终应将此 MC Master 拓扑结构迁移到 MM 拓扑结构，以便充分利用 ArubaOS 8 提供的功能。

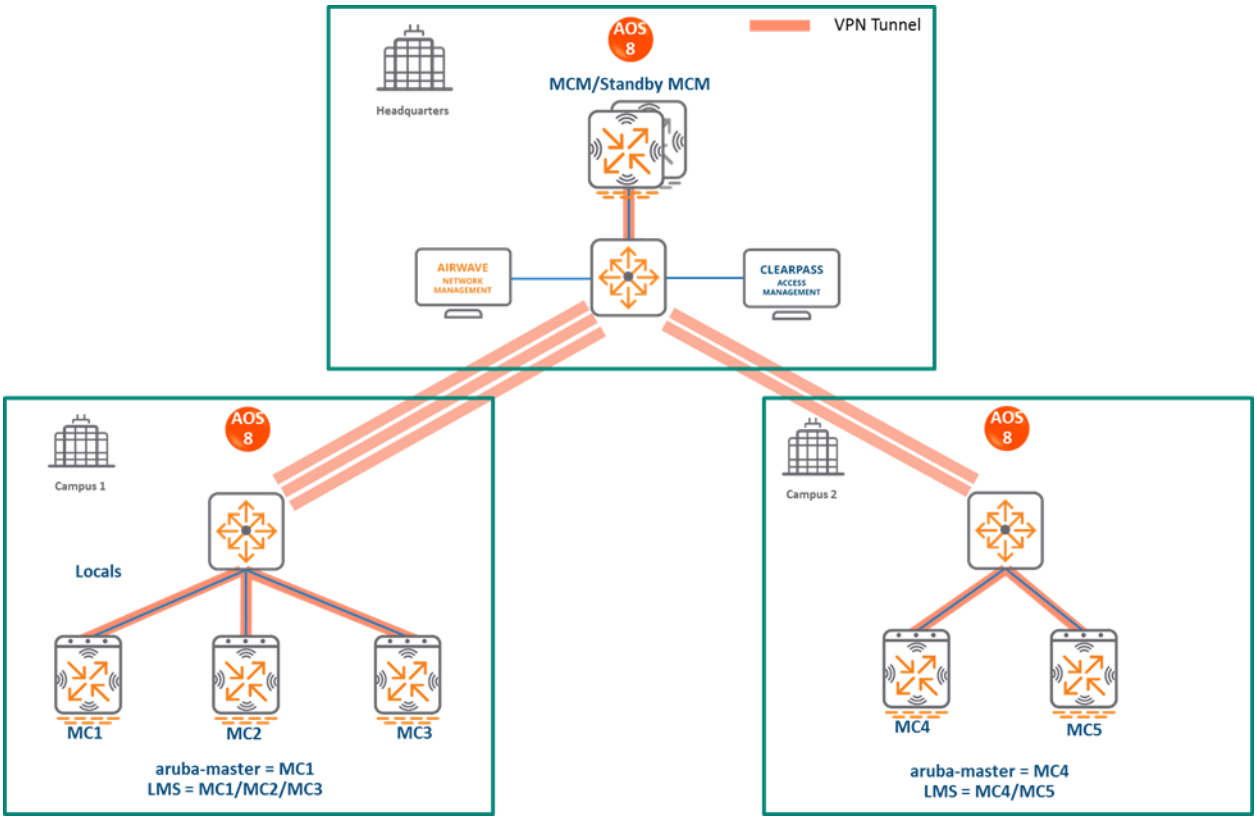


图 170 *MC Master 端接 MC 拓扑结构*

在该设计中：

- ArubaOS 6 主控制器 (M1) 和备用主控制器 (M2) 成为 ArubaOS 8 MC Master（MCM1 和 MCM2）
- 在 Campus1 中，ArubaOS 6 本地控制器（L1、L2 和 L3）成为 ArubaOS 8 MC（MC1、MC2 和 MC3）
- 在 Campus2 中，ArubaOS 6 本地控制器（L4 和 L5）成为 ArubaOS 8 MC（MC4 和 MC5）
- 所有 MC 均在 MC Master MCM1 上端接它们的 IPsec 隧道
- 在 L1、L2 和 L3 上端接的 AP 现在将分别在 MC1、MC2 和 MC3 上进行端接
- 在 L4 和 L5 上端接的 AP 现在将分别在 MC4 和 MC5 上进行端接

配置层次结构

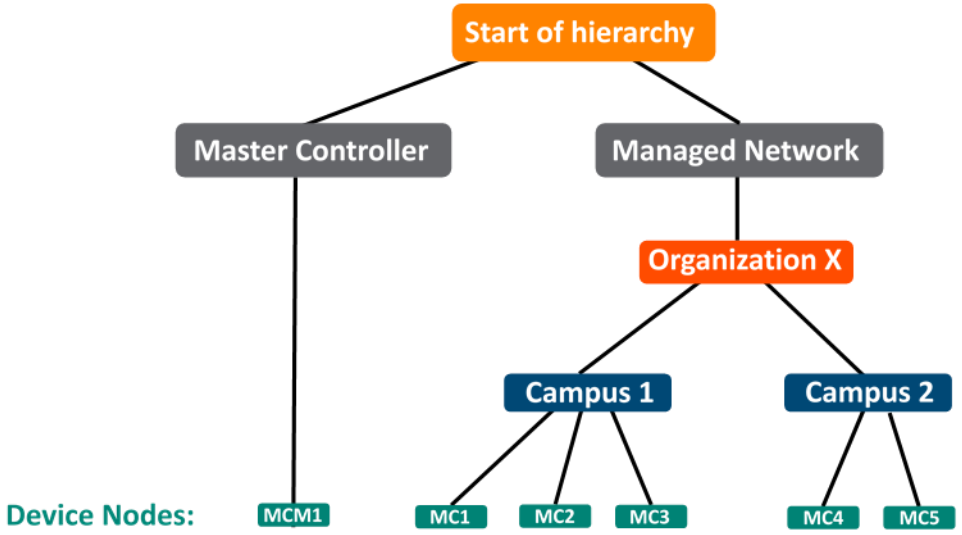


图 171 *MC Master 端接 MC 配置层次结构*

设计优势

- 保持类似的拓扑结构，在该拓扑结构中，MC Master 管理 MC，并且只要 MC Master 是 Aruba 7030 或更大的控制器，便不需要额外硬件
- 分层配置模式提供 WLAN 的完全集中式配置和管理
- 其他控制器可稍后添加，并由 MC Master 加以管理

设计警告

- 需要购买 Aruba 7030 或更大的控制器来作为 MC Master 以及备用 MCM（如果尚未存在）
- 不支持在 MC Master 上端接 AP。这对 AP 端接选择具有以下影响：
  - 在 ArubaOS 6 中的主控制器上端接的任何 AP 在迁移前都将需要在本地控制器间重新分配。本地控制器应具有足够的容量来容纳额外 AP
  - AP 可在 MC 之间进行故障切换，但无法故障切换到 MC Master
- 在 MC Master 部署中不支持群集功能。MC 之间的 AP 快速故障切换是唯一的控制器冗余选择
- 不支持 AirMatch
- 该拓扑结构中的所有控制器都必须运行相同的 ArubaOS 版本
- 没有集中式监控

迁移要求

- 验证 ArubaOS 6 主控制器是否满足 MC Master 硬件要求（Aruba 7030 或任何 Aruba 7200 系列控制器）
- 确保 ArubaOS 6 主控制器未端接任何 AP，因为 ArubaOS 8 MC Master 不支持 AP 端接
- 确保已手动或通过“我的网络门户”迁移了 AP、PEF 和其他所有许可

迁移选项

- 可手动或通过迁移工具进行迁移
- 以下详细说明了手动迁移。要使用迁移工具执行迁移，请参阅 ArubaOS 8 迁移指南

迁移策略

现有 ArubaOS 6 部署

- **HQ**：M1 和 M2
- **Campus1**：L1、L2 和 L3
- **Campus2**：L4 和 L5
- 在 Campus1 中，三个 AP 组被配置为在 L1、L2 和 L3 上进行端接
- 在 Campus2 中，两个 AP 组被配置为在 L4 和 L5 上进行端接

新 ArubaOS 8 部署

- MCM1 由 MCM2 备份
- MCM1 管理 Campus1 中的 MC1、MC2 和 MC3 以及 Campus2 中的 MC4 和 MC5

迁移程序

手动迁移需要通过执行下列步骤完全重新构建现有 ArubaOS 6 拓扑结构：

MC Master 特定

1. 备份 ArubaOS 6 主控制器和本地控制器上的现有配置。GUI: **维护 > 备份 Flash**
2. 将主 M1 升级到 ArubaOS 8，然后重新启动控制器。GUI: **维护 > 映像管理**
3. 通过 CLI 设置对话框将 M1 配置为 MC Master。M1 将成为 MCM1
4. 重复第 2 步和第 3 步，将 M2 转换为 MCM2
5. 在 MCM1 与 MCM2 之间配置主冗余。MC Master VIP 将用于配置管理
6. 在 MC Master 上配置许可

7. 在 MC Master 上创建配置层次结构，以及将控制器 L1-L5 的 MAC 地址列入白名单。将以下配置层次结构下的每个设备列入白名单：
   - 在**托管网络 > Campus1** 下列入白名单的 L1-L3
   - 在**托管网络 > Campus2** 下列入白名单的 L4 和 L5

Campus1

1. 创建三个 AP 组，每个 AP 组分别具有 MC1、MC2 和 MC3 的 LMS IP。GUI: **托管网络 > Campus1 > AP 组**
2. 创建公共 SSID 或为每个 AP 组创建一个 SSIDGUI: **托管网络 > Campus1 > 任务 > 创建新 WLAN**
3. 将 MC Master 上的 AP 列入白名单。这包括将它们映射到相应的 AP 组。GUI: **托管网络 > Campus1 > 配置 > 接入点 > 白名单**
4. 将本地控制器 L1 上的映像升级到 ArubaOS 8，然后重新启动。GUI: **维护 > 映像管理**
5. 通过 CLI 设置对话框配置将由 MC Master 管理的本地控制器 L1。L1 将成为 MC1
6. 对 L2 和 L3，重复第 4-5 步，将它们转换为 ArubaOS 8 MC2 和 MC3
7. 将 **aruba-master** 更改为指向 MC1 的 IP
8. 在 MC1 可显示在 MC Master 上后，L1 上端接的 AP 将查找 MC1，升级其映像，下载用于 MC1 的 LMS-IP，在 MC1 上端接它们的隧道，以及广播配置的 SSID
9. 同样，L2 和 L3 上的 AP 将分别显示在 MC2 和 MC3 上
10. 将无线客户端连接到 SSID 并测试连接
11. 可选择通过 MC Master 配置 AP 快速故障切换，以便在 MC 之间实现 AP 故障切换

Campus2

1. 创建两个 AP 组，每个 AP 组分别具有 MC1 和 MC2 的 LMS IP。GUI: **托管网络 > Campus2 > AP 组**
2. 创建公共 SSID 或为每个 AP 组创建一个 SSIDGUI: **托管网络 > Campus2 > 任务 > 创建新 WLAN**
3. 将 MC Master 上的 AP 列入白名单。这包括将它们映射到相应的 AP 组。GUI: **托管网络 > Campus2 > 配置 > 接入点 > 白名单**
4. 将本地控制器 L4 上的映像升级到 ArubaOS 8，然后重新启动。GUI: **维护 > 映像管理**
5. 通过 CLI 设置对话框配置将由 MC Master 管理的本地控制器 L4。L4 将成为 MC4
6. 重复第 4-5 步，将 L5 转换为 MC5
7. 将 **aruba-master** 更改为指向 MC4 的 IP
8. L4 上端接的 AP 将查找 MC4，升级其映像，下载其 LMS IP（即 MC4），在 MC1 上端接它们的隧道，以及广播配置的 SSID
9. 同样，L5 上的 AP 将显示在 MC5 上

10. 将无线客户端连接到 SSID 并测试连接
11. 可选择通过 MC Master 配置 AP 快速故障切换，以便在 MC 之间实现 AP 故障切换

多主-本地控制器

此 ArubaOS 6 设计由多个站点组成，每个站点的主控制器（一般由备用主控制器备份）管理一组本地控制器。

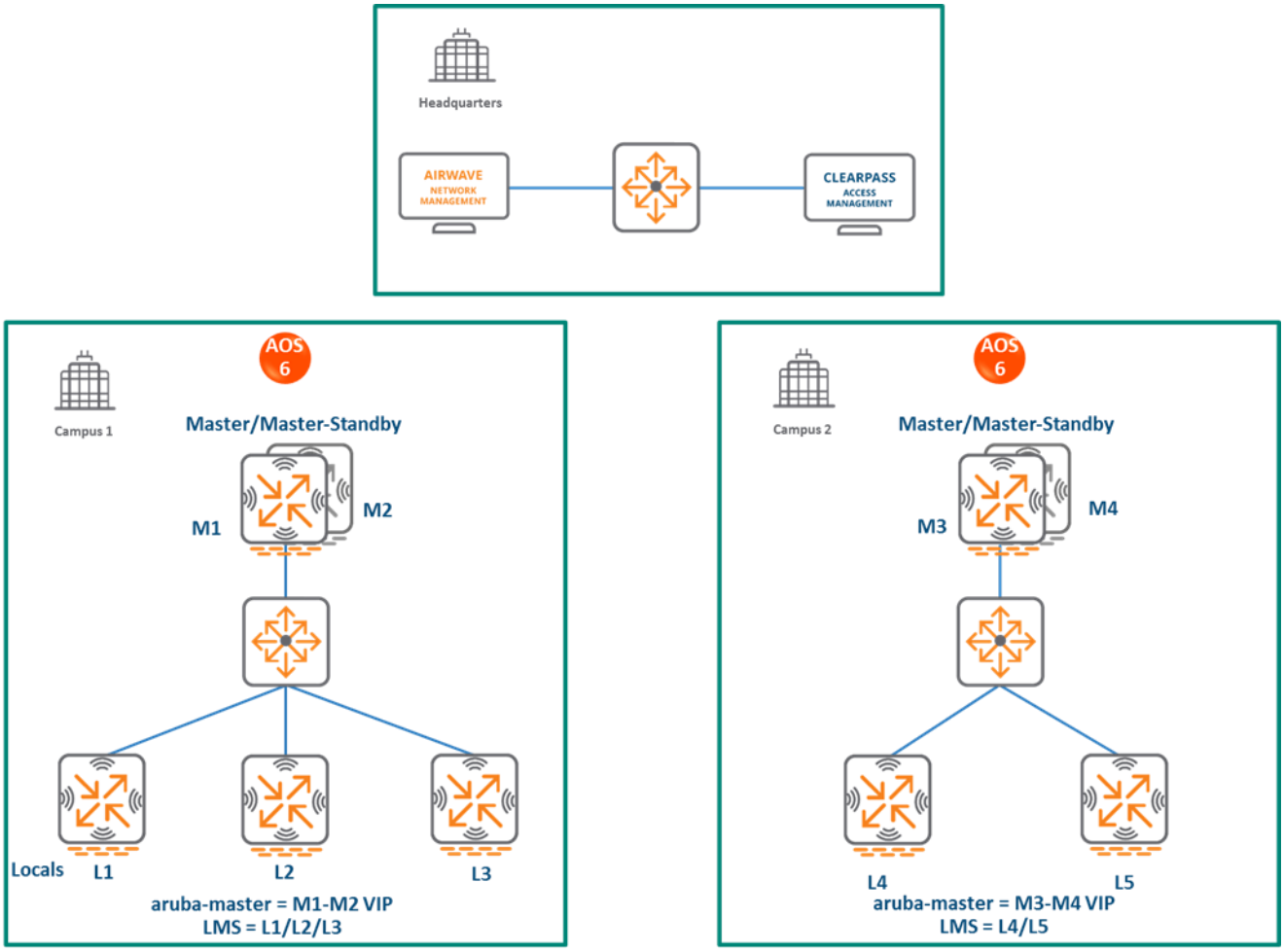


图 172 *多主-本地控制器*

在该设计中：

- 每个站点都有自己的配置，该配置在主控制器上加以定义，并被推送到各自本地控制器。多个站点没有中心配置点
- 每个站点的 AP 均在一个本地控制器上进行端接，其他本地控制器作为备份。例如，Campus 1 中的一些 AP 可在 L1 上进行端接，L2 和 L3 为 L1 提供备份
- AP 快速故障切换被配置为在与主控制器的连接中断时为 AP 提供亚秒级故障切换

MM 端接 MC

拓扑结构

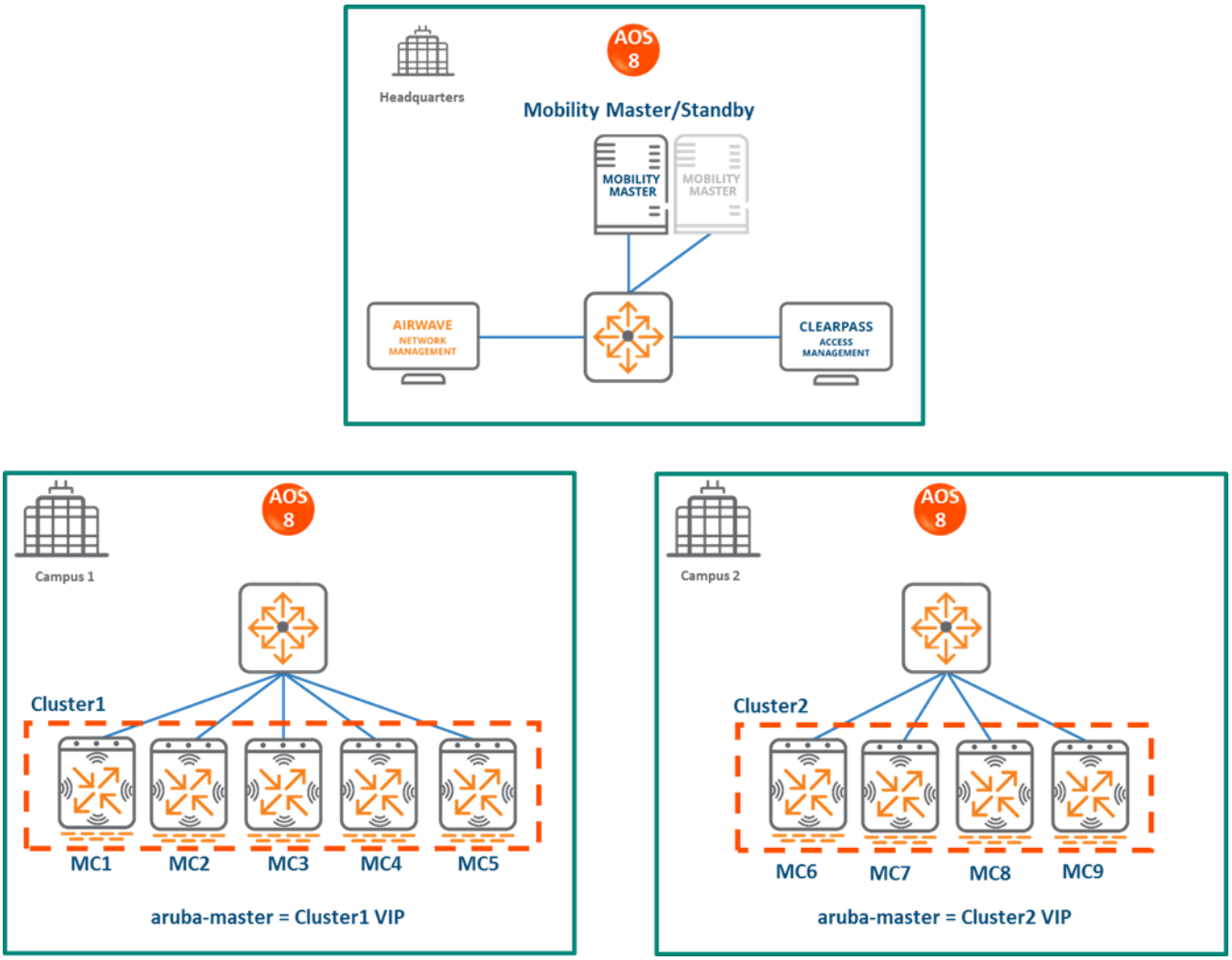


图 173 *MM 端接 MC 拓扑结构*

HQ/DC

- MM（硬件或虚拟）在 HQ/DC 以及备用 MM 中加以部署和配置
- 两个园区均由 MM 集中管理

Campus1

- ArubaOS 6 本地控制器 L1、L2 和 L3 分别成为 ArubaOS 8 MC1、MC2 和 MC3
- 在 MC1、MC2 和 MC3 之间形成一个群集，以实现控制器冗余、负载分担，以及 AP 和客户端的故障切换
- ArubaOS 6 主控制器 M1 和 M2 成为 ArubaOS 8 MC4 和 MC5
- 在 L1、L2 和 L3 上端接的 AP 现在将分别在 MC1、MC2 和 MC3 上进行端接

- MC4 和 MC5 可包含在群集中，以实现更多冗余以及客户端和 AP 负载分担

Campus2

- 同样，ArubaOS 6 本地控制器 L4 和 L5 分别成为 ArubaOS 8 MC6 和 MC7
- 在 MC6 与 MC7 之间形成一个群集，用于实现控制器冗余、负载分担，以及 AP 和客户端的故障切换
- ArubaOS 6 主控制器 M3 和 M4 成为 ArubaOS 8 MC8 和 MC9
- 在 L4 和 L5 上端接的 AP 现在将分别在 MC6 和 MC7 上进行端接
- MC8 和 MC9 可包含在群集中，以实现更多冗余以及客户端和 AP 负载分担

配置层次结构

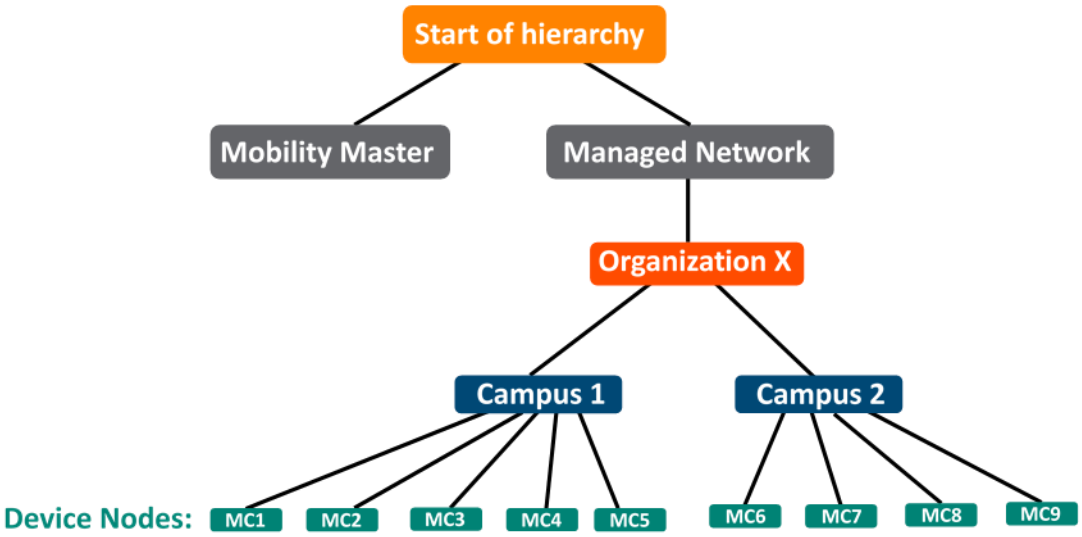


图 174 *MM 端接 MC 配置层次结构*

设计优势

- **最大化优势** - MM 端接 MC 设计是充分利用 ArubaOS 8 功能的理想选择
- **可扩展性** - 通过 MM 可轻松添加和管理新控制器
- **易于迁移** - 如果现有部署具有多个拓扑结构，则在 MM 下可将它们全部迁移到层次结构中它们自己的节点中
- **管理** - 集中式控制器配置和管理
- **分层配置模型** - 在节点（USA、West Coast、California、Santa Clara 等逻辑文件夹）上执行配置，以及根据位置和环境将每个控制器分配到特定节点
- **群集** - 在群集中具有控制器可在控制器之间实现无缝客户端故障切换，同时不影响用户体验。群集功能还可促进客户端漫游以及 AP 和客户端负载分担。必须进行群集才能支持实时升级
- **实时升级** - 实时升级控制器群集，并且最终用户不会遇到任何连接或性能损失。无需为网络升级安排维护周期

- **AirMatch** - RF 智能集中在 MM 上，这可显著改进 WLAN 的 RF 管理和干扰抑制功能
- **REST API 支持**
- **多版本支持** - 可灵活地升级单个控制器，以便测试新功能或故障修复。群集中的控制器需要运行相同的 ArubaOS 软件版本，并且可一同进行升级
- **在线软件模块升级** - 可在运行时更新 UCC、AirGroup、AppRF 等可加载服务模块 (LSM)，无需安排任何维护周期

设计警告

- MM 不端接 AP。只能在 MC 上端接 AP
- 如果现有 ArubaOS 6 部署有超过 1000 个控制器和/或 10,000 个 AP，则迁移到 ArubaOS 8 MM 部署需要部署多个 MM

迁移要求

- 需要购买虚拟 MM 容量许可或购买硬件 MM
- 还可以部署备用硬件 MM，在这种情况下，每个 MM 上的许可都将在两个 MM 间进行聚合和同步
- 需要手动或通过“我的网络门户”迁移其他许可，例如 AP 和 PEF

迁移选项

- 可手动或通过迁移工具进行迁移
- 迁移工具能够将每个主-本地控制器站点单独迁移到 ArubaOS 8。其不支持同时迁移多个主-本地控制器
- 以下详细说明了手动迁移。要使用迁移工具执行迁移，请参阅 ArubaOS 8 迁移指南

迁移策略

现有 ArubaOS 6 部署

- **Campus1：**
  - 本地控制器 L1、L2、L3
  - 主控制器 M1 和 M2
  - 3 个 AP 组被配置为使 AP 在 L1、L2 和 L3 之间进行端接

- **Campus2**
  - 本地控制器 L4 和 L5
  - 主控制器 M3 和 M4
  - 2 个 AP 组被配置为使 AP 在 L4 和 L5 之间进行端接

新 ArubaOS 8 部署

- MM 由备用 MM 进行备份
- MM 管理 Campus1 中的 MC1-MC5 和 Campus2 中的 M6-M9

迁移程序

手动迁移需要通过执行下列步骤完全重新构建现有 ArubaOS 6 拓扑结构：

MM 特定

1. 部署 MM 并执行初始设置
2. 在 MM 上配置许可
3. 创建配置层次结构以及将 MM 上的 M1-M4 和 L1-L5 的 MAC 地址列入白名单。将以下配置层次结构下的每个设备列入白名单：
   - 在**托管网络 > Campus1** 下列入白名单的 M1、M2、L1-L3
   - 在**托管网络 > Campus2** 下列入白名单的 M3、M4、L4 和 L5
4. 如果正在安装备用 MM，则重复第 1 步
5. 如果已安装了备用 MM，则配置 MM 冗余。MM VIP 将用于配置管理

Campus1

6. 在 MC1-MC5 IP 之间配置群集。此外还可实现 AP 负载分担。GUI: **托管网络 > Campus1 > 服务 > 群集**
7. 在群集成员 MC1-MC5 之间创建 VIP。GUI: **托管网络 > Campus1 > 服务 > 冗余 > 虚拟路由器表。**可选择为 RADIUS COA 创建 VIP
8. 创建 AP 组和 SSIDGUI: **托管网络 > Campus1 > AP 组。**GUI: **托管网络 > Campus1 > 任务 > 创建新 WLAN**
9. 将 MM 上的 Campus1 AP 列入白名单。这包括将它们映射到相应的 AP 组。GUI: **托管网络 > Campus1 > 配置 > 接入点 > 白名单**
10. 备份 ArubaOS 6 主控制器 M1、M2 和本地控制器 L1-L3 上的现有配置。GUI: **维护 > 备份 Flash**
11. 将本地控制器 L1 上的映像升级到 ArubaOS 8，然后重新启动。GUI: **维护 > 映像管理**
12. 通过 CLI 设置对话框配置将由 MM 管理的本地控制器 L1。L1 现在将成为 MC1

13. 重复第 6-7 步，将 L2、L3、M1 和 M2 分别转换为 MC2、MC3、MC4 和 MC5
14. 在 Campus1 网络中，将 **aruba-master** 指向 MC1-MC5 的群集 VIP
15. 在 L1-L3 上端接的 AP 将查找群集 VIP，升级其映像，在 MC1-MC5 中的一个上进行端接（取决于群集领导者如何对 AP 进行负载分担），以及广播 Campus1 的已配置 SSID
16. 将无线客户端连接到 SSID 并测试连接
17. 可选择通过运行语音/视频应用程序并断开用户的主用控制器来测试无缝客户端故障切换

Campus2

1. 在 MC6-MC9 IP 之间配置群集，以及实现 AP 负载分担。GUI: **托管网络 > Campus2 > 服务 > 群集**
2. 在群集成员 MC6-MC9 之间创建 VIP。GUI: **托管网络 > Campus2 > 服务 > 冗余 > 虚拟路由器表。**可选择为 RADIUS COA 创建 VIP
3. 创建 AP 组和 SSIDGUI: **托管网络 > Campus2 > AP 组。**GUI: **托管网络 > Campus2 > 任务 > 创建新 WLAN**
4. 将 MM 上的 Campus2 AP 列入白名单。这包括将它们映射到相应的 AP 组。GUI: **托管网络 > Campus2 > 配置 > 接入点 > 白名单**
5. 备份 ArubaOS 6 主控制器 M3 和 M4 以及本地控制器 L4 和 L5 上的现有配置。GUI: **维护 > 备份 Flash**
6. 将本地控制器 L4 上的映像升级到 ArubaOS 8，然后重新启动该设备。GUI: **维护 > 映像管理**
7. 通过 CLI 设置对话框配置将由 MM 管理的本地控制器 L4。L4 现在将成为 MC6
8. 重复第 6-7 步，将 L5、M3 和 M4 分别转换为 MC7、MC8 和 MC9
9. 在 Campus2 网络中，将 **aruba-master** 指向 MC6-MC9 的群集 VIP
10. 在 L4 和 L5 上端接的 AP 将查找群集 VIP，升级其映像，在 MC6-MC9 中的一个上进行端接（取决于群集领导者如何对 AP 进行负载分担），以及广播 Campus2 的已配置 SSID
11. 将无线客户端连接到 SSID 并测试连接
12. 可选择通过运行语音/视频应用程序并断开用户的主用控制器来测试无缝客户端故障切换

MC Master 端接 MC

拓扑结构

在此 ArubaOS 8 设计中，每个站点均包含一个作为 MC Master 部署的硬件控制器（可选择由另一个 MC Master 进行备份），其管理一组 MC。

此设计有助于将部署过渡到无法部署 MM 的 ArubaOS 8。最终应将此 MC Master 拓扑结构迁移到 MM 拓扑结构，以便充分利用 ArubaOS 8 提供的功能。

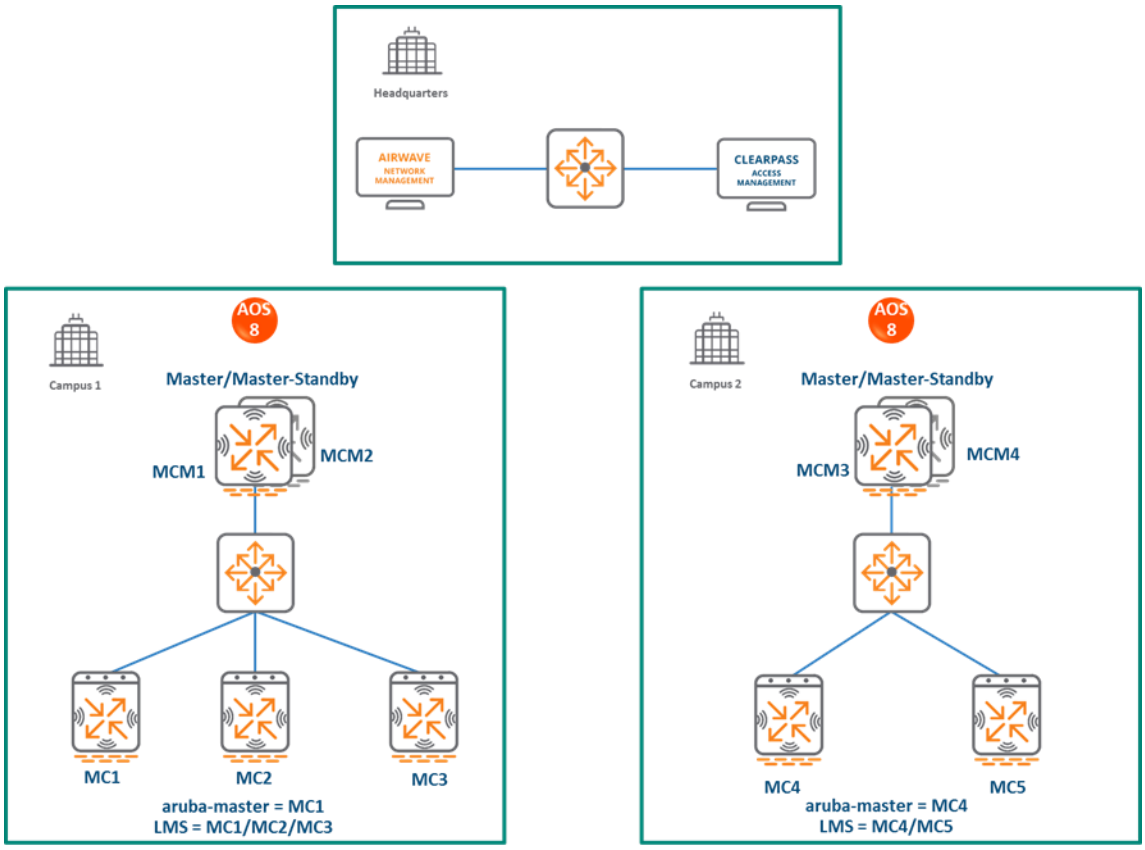


图 175 *MC Master 端接 MC 拓扑结构*

在此设计中，每个园区仍由其自己的 MC Master 加以管理。

Campus1

- ArubaOS 6 本地控制器 L1、L2 和 L3 分别成为 ArubaOS 8 MC1、MC2 和 MC3
- ArubaOS 6 主控制器 M1 和 M2 成为 ArubaOS 8 MCM1 和 MCM2
- 在 L1、L2 和 L3 上端接的 AP 现在将分别在 MC1、MC2 和 MC3 上进行端接

Campus2

- ArubaOS 6 本地控制器 L4 和 L5 分别成为 ArubaOS 8 MC4 和 MC5
- ArubaOS 6 主控制器 M3 和 M4 成为 ArubaOS 8 MCM3 和 MCM4
- 在 L4 和 L5 上端接的 AP 现在将分别在 MC4 和 MC5 上进行端接

配置层次结构

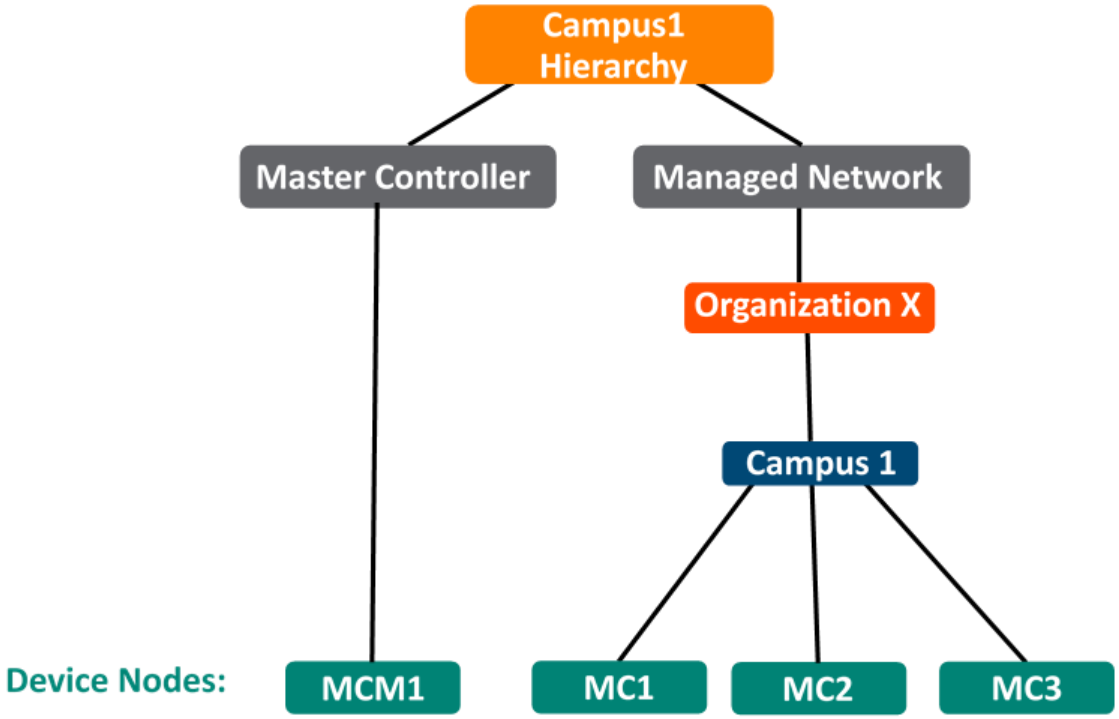


图 176 *MC Master 端接移动性配置层次结构 Campus 1*

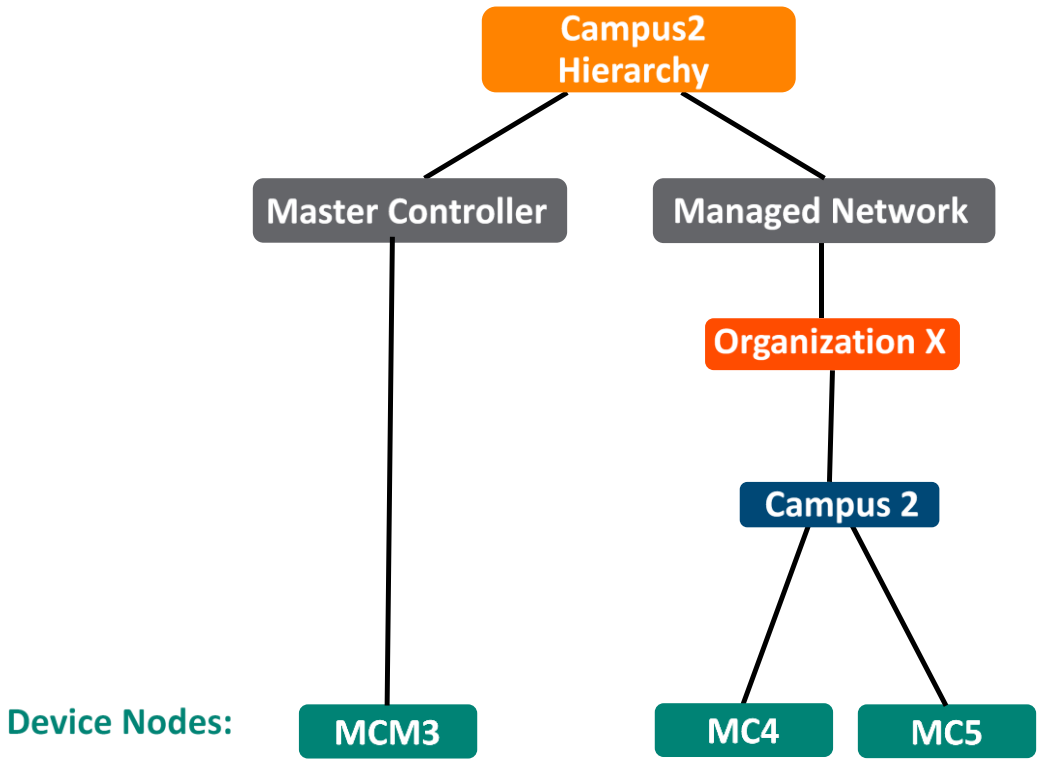


图 177 *MC Master 端接移动性配置层次结构 Campus 2*

设计优势

- 保持类似的拓扑结构，在该拓扑结构中，MC Master 管理 MC，并且只要 MC Master 是 Aruba 7030 或更大的控制器，便不需要额外硬件
- 分层配置模式提供 WLAN 的完全集中式配置和管理
- 其他控制器可稍后添加，并由 MC Master 加以管理

设计警告

- 需要购买 Aruba 7030 或更大的控制器来作为 MC Master 以及备用 MCM（如果尚未存在）
- 不支持在 MC Master 上端接 AP。这对 AP 端接选择具有以下影响：
  - 在 ArubaOS 6 中的主控制器上端接的任何 AP 在迁移前都将需要在本地控制器间重新分配。本地控制器应具有足够的容量来容纳额外 AP
  - AP 可在 MC 之间进行故障切换，但无法故障切换到 MC Master
- 在 MC Master 部署中不支持群集功能。MC 之间的 AP 快速故障切换是唯一的控制器冗余选择
- 不支持 AirMatch
- 该拓扑结构中的所有控制器都必须运行相同的 ArubaOS 版本
- 没有集中式监控

迁移要求

- 验证 ArubaOS 6 主控制器是否满足 MC Master 硬件要求（Aruba 7030 或任何 Aruba 7200 系列控制器）
- 确保 ArubaOS 6 主控制器未端接任何 AP，因为 ArubaOS 8 MC Master 不支持 AP 端接
- 确保已手动或通过“我的网络门户”迁移了 AP、PEF 和其他所有许可

迁移选项

- 可手动或通过迁移工具进行迁移
- 以下详细说明了手动迁移。要使用迁移工具执行迁移，请参阅 ArubaOS 8 迁移指南

迁移策略

现有 ArubaOS 6 部署

- 本地控制器 L1、L2、L3
- 主控制器 M1 和 M2
- 3 个 AP 组被配置为使 AP 组在 L1、L2 和 L3 之间进行端接

新 ArubaOS 8 部署

- **Campus1：**
  - MCM1 由 MC2 备份
  - MCM1 管理 MC1、MC2 和 MC3
- **Campus2：**
  - MCM3 由 MCM4 进行备份
  - MCM3 管理 MC4 和 MC5

迁移程序

手动迁移需要通过执行下列步骤完全重新构建现有 ArubaOS 6 拓扑结构：

Campus1

1. 备份 ArubaOS 6 主控制器和本地控制器上的现有配置。GUI：**维护 > 备份 Flash**
2. 将主 M1 升级到 ArubaOS 8，然后重新启动控制器
3. 通过 CLI 设置对话框将 M1 配置为 MC Master。M1 现在将成为 MCM1
4. 重复第 2 步和第 3 步，将 M2 转换为 MCM2
5. 在 MCM1 与 MCM2 之间配置主冗余。MC Master VIP 将用于配置管理
6. 在 MC Master 上配置许可
7. 在 MC Master 上创建配置层次结构，以及将控制器 L1-L3 的 MAC 地址列入白名单
   - L1-L3 将在**托管网络 > Campus1** 下列入白名单
8. 创建三个 AP 组，每个 AP 组分别具有 MC1、MC2 和 MC3 的 LMS IP。GUI：**托管网络 > Campus1 > AP 组**
9. 创建公共 SSID 或为每个 AP 组创建一个 SSIDGUI：**托管网络 > Campus1 > 任务 > 创建新 WLAN**
10. 将 MC Master 上的 AP 列入白名单。这包括将它们映射到相应的 AP 组。GUI：**托管网络 > Campus1 > 配置 > 接入点 > 白名单**
11. 将本地控制器 L1 上的映像升级到 ArubaOS 8，然后重新启动。GUI：**维护 > 映像管理**
12. 通过 CLI 设置对话框配置将由 MC Master 管理的本地控制器 L1。L1 现在变为 MC1
13. 对 L2 和 L3，重复第 11-12 步，将它们转换为 ArubaOS 8 MC2 和 MC3
14. 将 **aruba-master** 更改为 MC1 的 IP
15. 在 MC1 可显示在 MC Master 上后，L1 上端接的 AP 将查找 MC1，升级其映像，下载用于 MC1 的 LMS-IP，在 MC1 上端接它们的隧道，以及广播配置的 SSID
16. 同样，L2 和 L3 上的 AP 将分别显示在 MC2 和 MC3 上
17. 将无线客户端连接到 SSID 并测试连接
18. 可选择通过 MC Master 配置 AP 快速故障切换，以便在 MC 之间实现亚秒级 AP 故障切换

Campus2

1. 备份 ArubaOS 6 主控制器和本地控制器上的现有配置。GUI: **维护 > 备份 Flash**
2. 将主 M3 升级到 ArubaOS 8，然后重新启动控制器
3. 通过 CLI 设置对话框将 M3 配置为 MC Master。M3 现在将成为 MCM3
4. 重复第 2 步和第 3 步，将 M4 转换为 MCM4
5. 在 MCM3 与 MCM4 之间配置主冗余。从现在开始，使用 MC Master VIP 进行配置管理
6. 在 MC Master 上配置许可
7. 在 MC Master 上创建配置层次结构，以及将控制器 L4 和 L5 的 MAC 地址列入白名单。
   - L4、L5 将在**托管网络 > Campus2** 下列入白名单
8. 创建两个 AP 组，每个 AP 组分别具有 MC4 和 MC5 的 LMS IP。GUI: **托管网络 > Campus2 > AP 组**
9. 创建公共 SSID 或为每个 AP 组创建一个 SSIDGUI: **托管网络 > Campus2 > 任务 > 创建新 WLAN**
10. 将 MC Master 上的 AP 列入白名单。这包括将它们映射到相应的 AP 组。GUI: **托管网络 > Campus2 > 配置 > 接入点 > 白名单**
11. 将本地控制器 L4 上的映像升级到 ArubaOS 8，然后重新启动。GUI: **维护 > 映像管理**
12. 通过 CLI 设置对话框配置将由 MC Master 管理的本地控制器 L4。L4 现在成为 MC4
13. 重复第 11-12 步，将 L5 转换为 MC5
14. 将 **aruba-master** 更改为 MC4 的 IP
15. L4 上端接的 AP 将查找 MC4，升级其映像，下载其 LMS IP（即 MC4），在 MC1 上端接它们的隧道，以及广播配置的 SSID
16. 同样，L5 上的 AP 将显示在 MC5 上
17. 将无线客户端连接到 SSID 并测试连接
18. 可选择通过 MC Master 配置 AP 快速故障切换，以便在 MC 之间实现亚秒级 AP 故障切换

所有主控制器

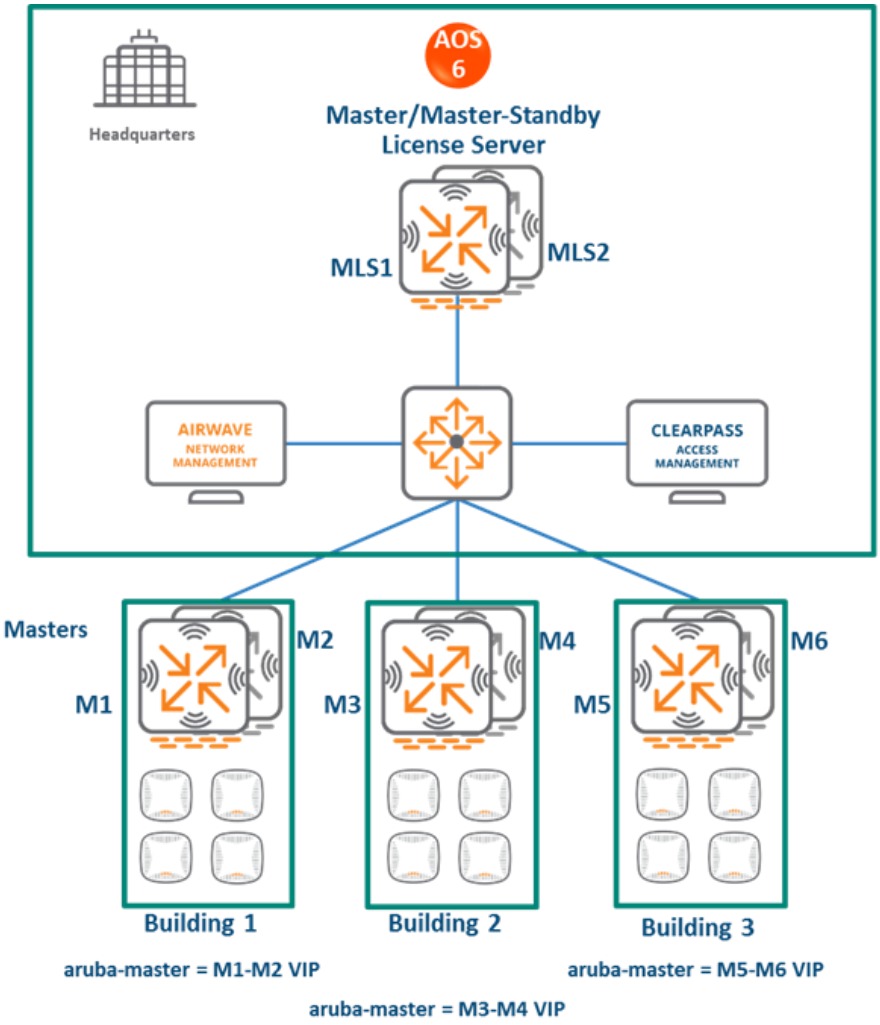


图 173 *所有主控制器拓扑结构*

- 在此 ArubaOS 6 设计中，每个站点均由各自的主控制器加以管理，由备用主控制器进行备份
- 有一个单独的主/备用对，其作为所有站点的许可服务器。
- 所有站点主控制器均由 AirWave 集中加以管理
- “所有-主”设计一般部署在需要运行不同 ArubaOS 版本的站点上（例如，测试新的 ArubaOS 功能）

MM 端接 MC

拓扑结构

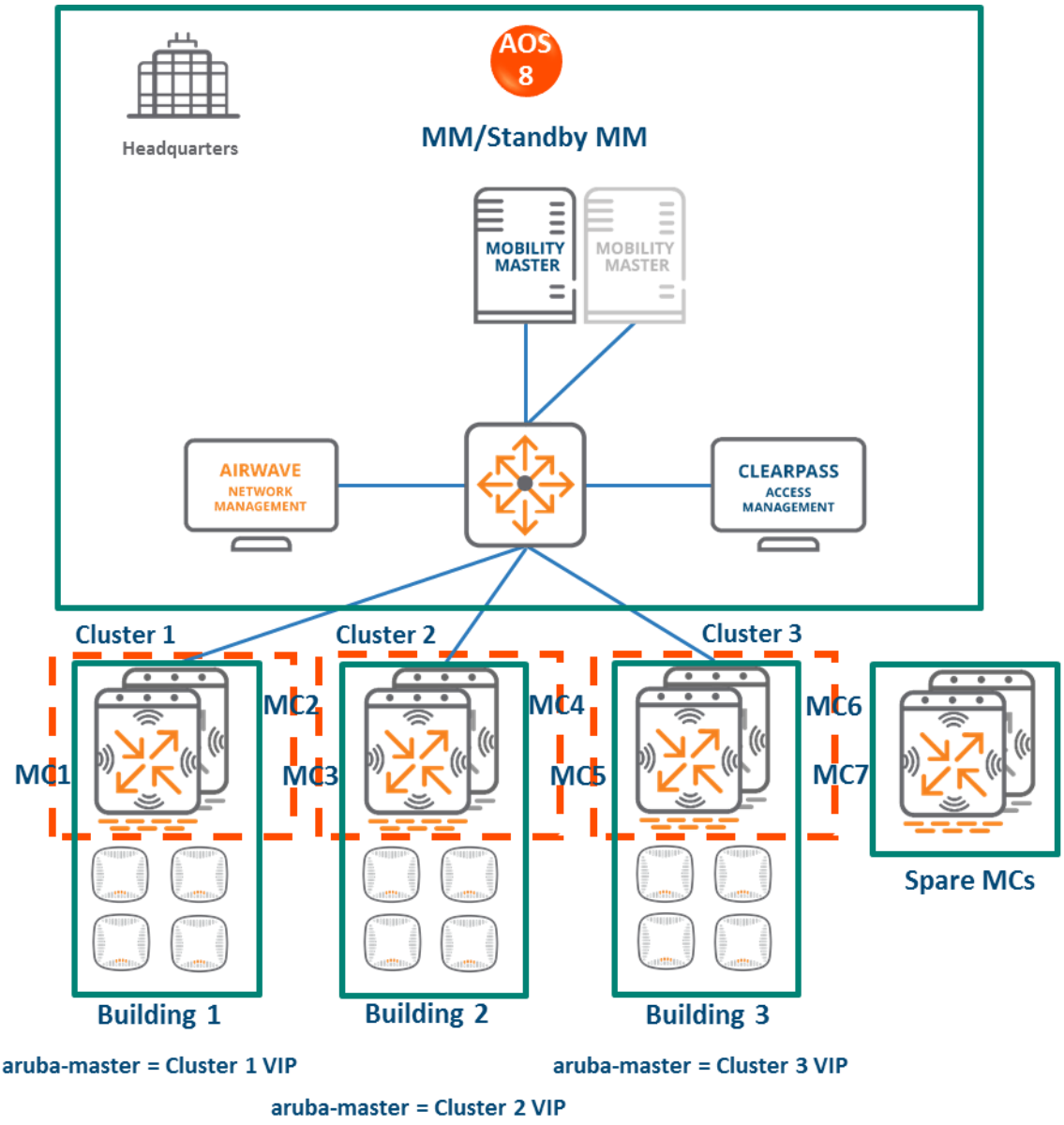


图 174 *MM 端接 MC 拓扑结构*

- **HQ/DC:**
  - MM（硬件或虚拟）与备用 MM 一同加以部署和配置。
  - 所有站点控制器均由 MM 集中加以管理
- **Building 1:**
  - ArubaOS 6 主控制器和备用主控制器成为 ArubaOS 8 MC1 和 MC2
  - 可在 MC1 与 MC2 之间形成群集，以实现控制器冗余以及客户端和 AP 负载分担

- **Building 2:** ArubaOS 6 主控制器成为 ArubaOS 8 MC3 和 MC4。两个 MC 都可成为群集成员
- **Building 3:** ArubaOS 6 主控制器成为 ArubaOS 8 MC5 和 MC6。两个 MC 都可成为群集成员
- **许可服务器：**
  - 先前作为许可服务器的 ArubaOS 6 主控制器和备用主控制器成为由 MM 管理的 MC
  - 这些 MC 可改变用途。例如，它们可作为临时控制器，以便将每个站点中的 AP 重定向到各自 LMS 控制器，或者可将它们添加到任何站点的群集中，以提供额外控制器冗余以及客户端和 AP 负载分担

配置层次结构

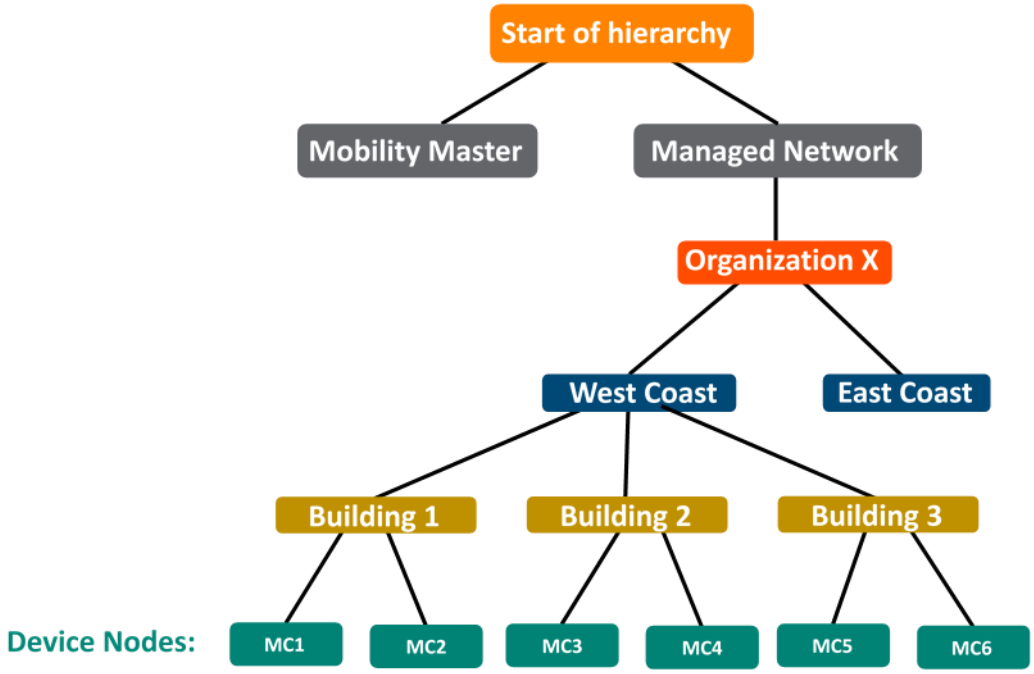


图 175 *MM 端接 MC 配置层次结构*

设计优势

- **最大化优势** - MM 端接 MC 设计是充分利用 ArubaOS 8 功能的理想选择
- **可扩展性** - 通过 MM 可轻松添加和管理新控制器
- **易于迁移** - 如果现有部署具有多个拓扑结构，则在 MM 下可将它们全部迁移到层次结构中它们自己的节点中
- **管理** - 集中式控制器配置和管理
- **分层配置模型** - 在节点（USA、West Coast、California、Santa Clara 等逻辑文件夹）上执行配置，以及根据位置和环境将每个控制器分配到特定节点
- **群集** - 在群集中具有控制器可在控制器之间实现无缝客户端故障切换，同时不影响用户体验。群集功能还可促进客户端漫游以及 AP 和客户端负载分担。必须进行群集才能支持实时升级。

- **实时升级** - 实时升级控制器群集，并且最终用户不会遇到任何连接或性能损失。无需为网络升级安排维护周期
- **AirMatch** - RF 智能集中在 MM 上，这可显著改进 WLAN 的 RF 管理和干扰抑制功能
- **REST API 支持**
- **多版本支持** - 可灵活地升级单个控制器，以便测试新功能或故障修复。群集中的控制器需要运行相同的 ArubaOS 软件版本，并且可一同进行升级
- **在线软件模块升级** - 可在运行时更新 UCC、AirGroup、AppRF 等可加载服务模块 (LSM)，无需安排任何维护周期

设计警告

- MM 不端接 AP。只能在 MC 上端接 AP
- 如果现有 ArubaOS 6 部署有超过 1000 个控制器和/或 10,000 个 AP，则迁移到 ArubaOS 8 MM 部署需要部署多个 MM

迁移要求

- 需要购买虚拟 MM 容量许可或购买硬件 MM
- 还可以部署备用硬件 MM，在这种情况下，每个 MM 上的许可都将在两个 MM 间进行聚合和同步
- 需要手动或通过“我的网络门户”迁移其他许可，例如 AP 和 PEF

迁移选项

- 可手动或通过迁移工具进行迁移
- 以下详细说明了手动迁移。要使用迁移工具执行迁移，请参阅 ArubaOS 8 迁移指南

迁移策略

现有 ArubaOS 6 部署

- **Building 1:** 主控制器 MM M1-M2
- **Building 2:** 主控制器 M3-M4
- **Building 3:** 主控制器 M5-M6
- **许可服务器：**MM maMasters MLS1 和 MLS2

新 ArubaOS 8 部署

- MM 管理 MC1、MC2、MC3、MC4、MC5、MC6、MC7 和 MC8。

迁移程序

手动迁移需要通过执行下列步骤完全重新构建现有 ArubaOS 6 拓扑结构：

MM 特定

1. 部署 MM 并执行初始设置
2. 在 MM 上配置许可
3. 创建配置层次结构以及将 MM 上的 M1-M6 的 MAC 地址列入白名单。将以下配置层次结构下的每个设备列入白名单：
   - 在**托管网络 > Building1** 下列入白名单的 M1、M2
   - 在**托管网络 > Building2** 下列入白名单的 M3、M4
   - 在**托管网络 > Building3** 下列入白名单的 M5、M6
4. 如果您正在安装备用 MM，则重复第 1 步
5. 如果已安装了备用 MM，则配置 MM 冗余。MM VIP 将用于配置管理

Building 1

1. 在 MC1 与 MC2 IP 之间配置群集，以及实现 AP 负载分担。GUI: **托管网络 > Building1 > 服务 > 群集**
2. 在群集成员 MC1 与 MC2 之间创建 VIP。GUI: **托管网络 > Building1 > 服务 > 冗余 > 虚拟路由器表。**可选择为 RADIUS COA 创建 VIP
3. 创建 AP 组和 SSIDGUI: **托管网络 > Building1 > AP 组。**GUI: **托管网络 > Building1 > 任务 > 创建新 WLAN**
4. 将 MM 上的 Building1 AP 列入白名单。这包括将它们映射到相应的 AP 组。GUI: **托管网络 > Building1 > 配置 > 接入点 > 白名单**
5. 备份 ArubaOS 6 主控制器上的现有配置。GUI: **维护 > 备份 Flash**
6. 将本地控制器 M1 上的映像升级到 ArubaOS 8，然后重新启动。GUI: **维护 > 映像管理**
7. 通过 CLI 设置对话框配置将由 MM 管理的本地控制器 M1。M1 现在将成为 MC1
8. 重复第 6-7 步，将 M2 转换为 MC2
9. 在 Building1 中，将 **aruba-master** 指向 MC1 和 MC2 的群集 VIP
10. 在 M1 上端接的 AP 将查找群集 VIP，升级其映像，在 MC1 或 MC2 上进行端接（取决于群集领导者如何对 AP 进行负载分担），以及广播 Building1 的已配置 SSID
11. 将无线客户端连接到 SSID 并测试连接
12. 可选择通过运行语音/视频应用程序并断开用户的主用控制器来测试无缝客户端故障切换

Building 2

1. 在 MC3 与 MC4 IP 之间配置群集，以及实现 AP 负载分担。GUI: **托管网络 > Building2 > 服务 > 群集**

2. 在群集成员 MC3 与 MC4 之间创建 VIP。GUI：**托管网络 > Building2 > 服务 > 冗余 > 虚拟路由器表。**可选择为 RADIUS COA 创建 VIP
3. 创建 AP 组和 SSIDGUI：**托管网络 > Building2 > AP 组。**GUI：**托管网络 > Building2 > 任务 > 创建新 WLAN**
4. 将 MM 上的 Building2 AP 列入白名单。这包括将它们映射到相应的 AP 组。GUI：**托管网络 > Building2 > 配置 > 接入点 > 白名单**
5. 备份 ArubaOS 6 主控制器上的现有配置。GUI：**维护 > 备份 Flash**
6. 将本地控制器 M3 上的映像升级到 ArubaOS 8，然后重新启动。GUI：**维护 > 映像管理**
7. 通过 CLI 设置对话框配置将由 MM 管理的本地控制器 M3。M3 现在将成为 MC3
8. 重复第 6-7 步，将 M4 转换为 MC4
9. 在 Building2 中，将 **aruba-master** 指向 MC3 和 MC4 的群集 VIP
10. 在 M3 上端接的 AP 将查找群集 VIP，升级其映像，在 M3 或 MC4 上进行端接（取决于群集领导者如何对 AP 进行负载分担），以及广播 Building 2 的已配置 SSID
11. 将无线客户端连接到 SSID 并测试连接
12. 可选择通过运行语音/视频应用程序并断开用户的主用控制器来测试无缝客户端故障切换

对 Building3 执行类似步骤。

备用 MC7 和 MC8

- 可将它们迁移到任何站点，以便将它们的用途变为群集成员，从而实现更多冗余以及 AP 和客户端负载分担

主控制器和分支控制器

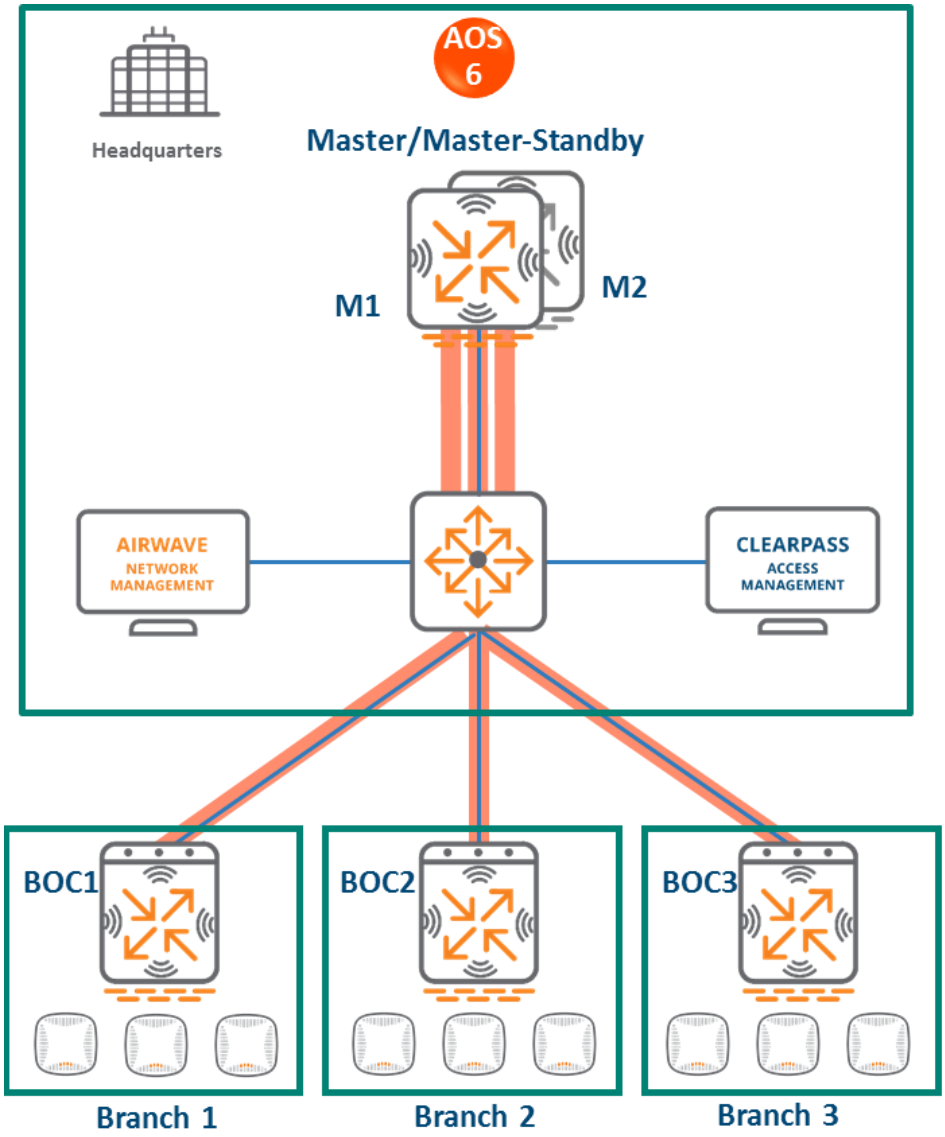


图 176 *主控制器和分支控制器拓扑结构*

在该 ArubaOS 6 设计中：

- 主控制器管理分布在不同地理位置的分支控制器
- 主控制器由第二个主控制器进行备份，以实现冗余
- 每个分支控制器均包含一个或多个 7000 系列控制器，即分支控制器/分支机构控制器 (BOC)
- 每个分支控制器均使用 ZTP 来发现和构建与主控制器的 IPsec 连接
- 分支控制器的配置在主控制器上进行管理

MM 端接 MC

拓扑结构

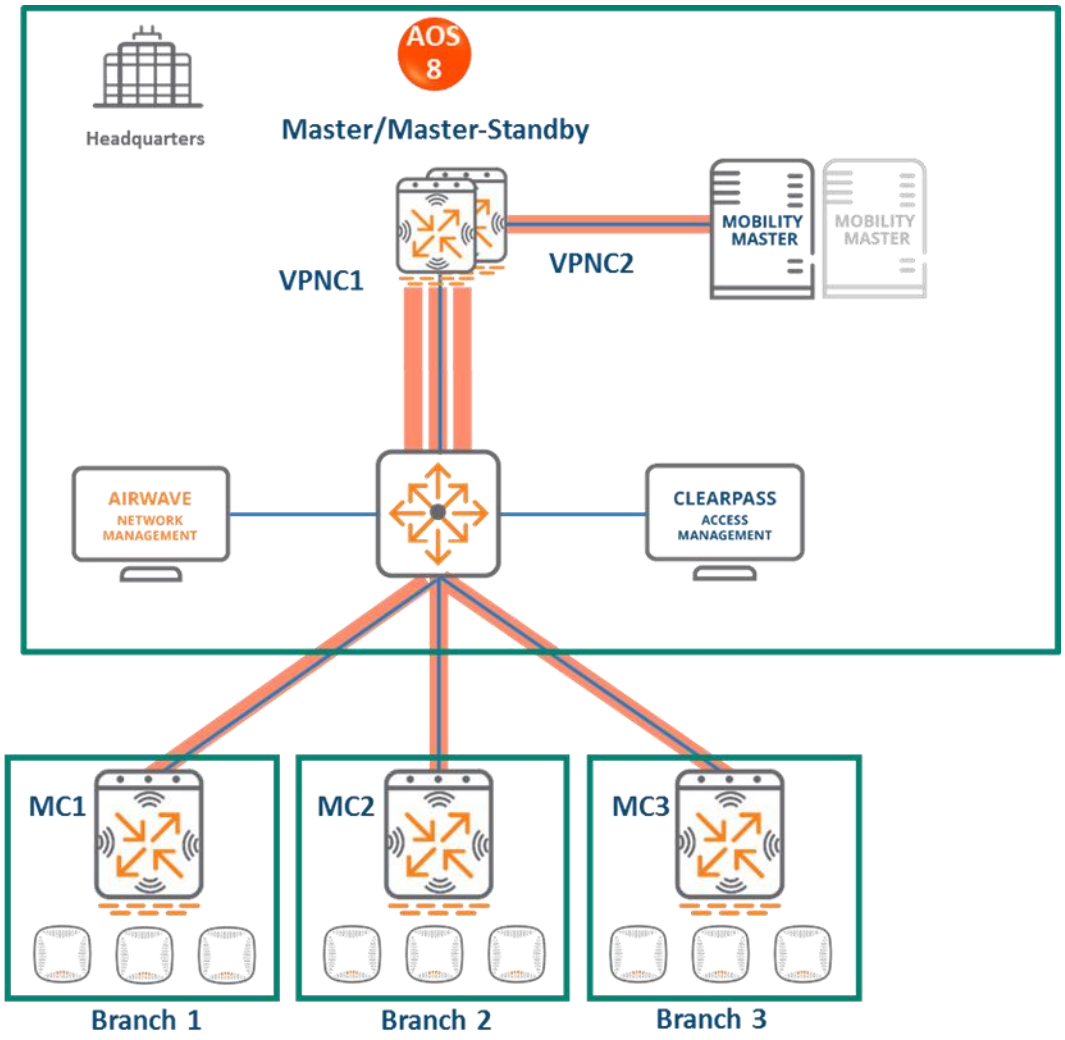


图 177 *MM 端接 MC 拓扑结构*

在该设计中：

- MM（硬件或虚拟）与备用 MM 一同加以部署和配置
- 每个 ArubaOS 6 BOC（BOC1、BOC2、BOC3）均成为 ArubaOS 8 MC（MC1、MC2、MC3）
- ArubaOS 6 主控制器 (M1) 和备用主控制器 (M2) 成为两个 ArubaOS 8 VPNC（MC4 与 MC5）
- 分支 MC 能够在 MM 上进行端接。但是，如果部署由分布式分支控制器组成，并且来自分支控制器的用户流量需要到达 HQ 中的公司资源，则强烈建议使用 VPNC。需要 HQ 访问权限的用户流量将是相对较高的带宽，加密/解密会占用大量 CPU。使用 VPNC 有助于将 MM 与增加的负载隔离开来
- 在 L1、L2 和 L3 上端接的 AP 现在将分别在 MC1、MC2 和 MC3 上进行端接

配置层次结构

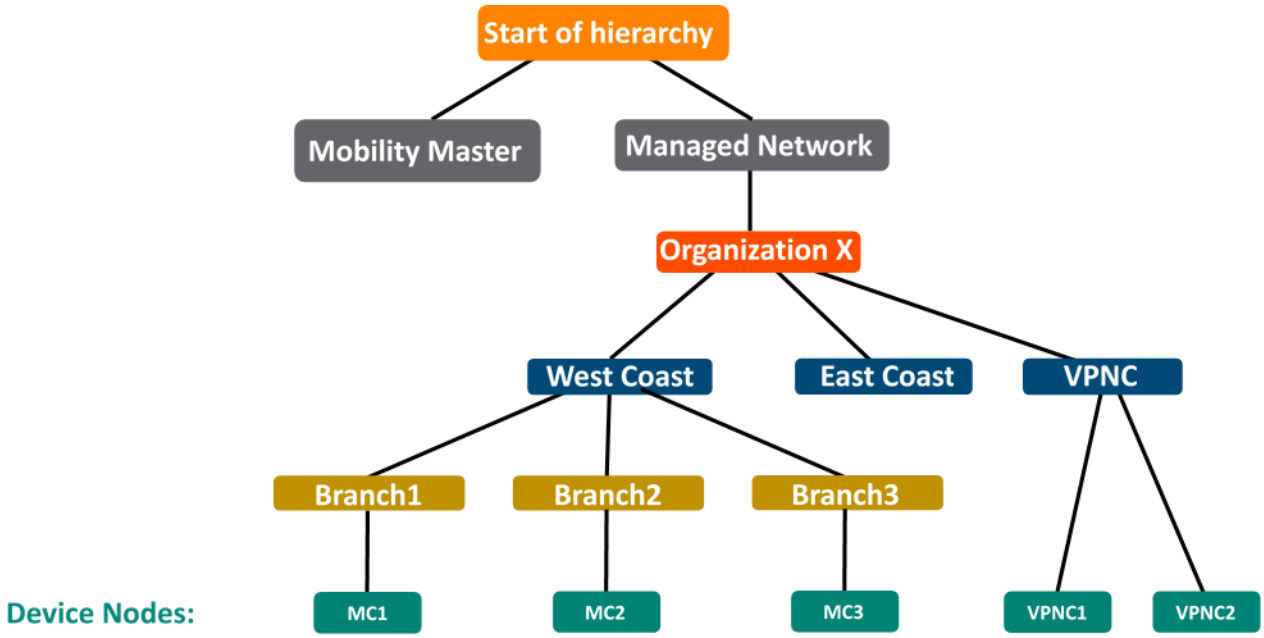


图 178 *MM 端接 MC 配置层次结构*

设计优势

- **最大化优势** - MM 端接 MC 设计是充分利用 ArubaOS 8 功能的理想选择
- **可扩展性** - 通过 MM 可轻松添加和管理新控制器
- **易于迁移** - 如果现有部署具有多个拓扑结构，则在 MM 下可将它们全部迁移到层次结构中它们自己的节点中
- **管理** - 集中式控制器配置和管理
- **分层配置模型** - 在节点（USA、West Coast、California、Santa Clara 等逻辑文件夹）上执行配置，以及根据位置和环境将每个控制器分配到特定节点
- **群集** - 在群集中具有控制器可在控制器之间实现无缝客户端故障切换，同时不影响用户体验。群集功能还可促进客户端漫游以及 AP 和客户端负载分担。必须进行群集才能支持实时升级
- **实时升级** - 实时升级控制器群集，并且最终用户不会遇到任何连接或性能损失。无需为网络升级安排维护周期
- **AirMatch** - RF 智能集中在 MM 上，这可显著改进 WLAN 的 RF 管理和干扰抑制功能
- **REST API 支持**
- **多版本支持** - 可灵活地升级单个控制器，以便测试新功能或故障修复。群集中的控制器需要运行相同的 ArubaOS 软件版本，并且可一同进行升级
- **在线软件模块升级** - 可在运行时更新 UCC、AirGroup 和 AppRF 等可加载服务模块 (LSM)，无需安排任何维护周期。

设计警告

- MM 不端接 AP。只能在 MC 上端接 AP
- 如果现有 ArubaOS 6 部署有超过 1000 个控制器和/或 10,000 个 AP，则迁移到 ArubaOS 8 MM 部署需要部署多个 MM

迁移要求

- 需要购买虚拟 MM 容量许可或购买硬件 MM
- 还可以部署备用硬件 MM，在这种情况下，每个 MM 上的许可都将在两个 MM 间进行聚合和同步
- 需要手动或通过“我的网络门户”迁移其他许可，例如 AP 和 PEF

迁移选项

- 可手动或通过迁移工具进行迁移
- 迁移工具能够将每个主-本地控制器站点单独迁移到 ArubaOS 8。其不支持同时迁移多个主-本地控制器
- 以下详细说明了手动迁移。要使用迁移工具执行迁移，请参阅 ArubaOS 8 迁移指南

迁移策略

现有 ArubaOS 6 部署

- **Branch1**：BOC1
- **Branch2**：BOC2
- **Branch3**：BOC3
- **HQ**：M1、M2

新 ArubaOS 8 部署

- MM 管理 MC1、MC2、MC3 以及 VPNC1、VPNC2。

迁移程序

手动迁移需要完全重新构建现有 ArubaOS 6 拓扑结构。使用以下步骤执行分支网络的手动迁移。ArubaOS8 分支网络 ASE 配置还可用于了解 ArubaOS 8 中的 MM/VPNC/分支控制器配置。

MM

1. 部署 MM 并执行初始设置
2. 在 MM 上配置许可
3. 如果正在安装备用 MM，则重复第 1 步
4. 如果已安装了备用 MM，则配置 MM 冗余。MM VIP 将用于配置管理
5. 配置 Activate、配置层次结构、VPN 对等以及将 MM 上的 M1、M2、BOC1、BOC2 和 BOC3 的 MAC 地址列入白名单将以下配置层次结构下的每个设备列入白名单：
   - 在**托管网络 > VPNC** 下列入白名单的 M1、M2
   - 在**托管网络 > Branch2** 下列入白名单的 BOC2
   - 在**托管网络 > Branch3** 下列入白名单的 BOC3
6. 配置接口、VLAN 和 VPNC VIP
7. 分支 MC 基本配置 - 为分支 MC 配置接口、VLAN、AP 和用户的 DHCP 池、控制器 IP 的 IP VLAN 池
8. 分支 MC 的上行链路配置 - 在分支 MC 中添加上行链路、负载分担和基于策略的路由
9. 播发分支 MC 到 VPNC 的路由
10. VPNC 的路由配置 - VPNC 中的静态路由和 OSPF 配置
11. 为 Branch1 创建 AP 组和 SSID。GUI: **托管网络 > Branch1 > AP 组**。GUI: **托管网络 > Branch1 > 任务 > 创建新 WLAN**
12. 将 MM 上的 Branch1 AP 列入白名单。这包括将它们映射到相应的 AP 组。GUI: **托管网络 > Branch1 > 配置 > 接入点 > 白名单**
13. 为 Branch2 创建 AP 组和 SSID。GUI: **托管网络 > Branch2 > AP 组**。GUI: **托管网络 > Branch2 > 任务 > 创建新 WLAN**
14. 将 MM 上的 Branch2 AP 列入白名单。这包括将它们映射到相应的 AP 组。GUI: **托管网络 > Branch2 > 配置 > 接入点 > 白名单**

Activate

1. 在 Activate 中设置配置规则，以便将分支控制器列入白名单，并将它们重定向到 MM
2. 如果正在使用 VPNC，则可选择设置配置规则，以便将它们也列入白名单并将它们重定向到 MM

VPNC

1. 备份 ArubaOS 6 主控制器上的现有配置。GUI: **维护 > 备份 Flash**
2. 将本地控制器 M1 上的映像升级到 ArubaOS 8，然后重新启动。GUI: **维护 > 映像管理**

3. 通过 CLI 设置对话框将 M1 配置成为由 MM 管理的 VPNC。M1 现在将成为 VPNC1
4. 重复第 2-3 步，将 M2 转换为 VPNC2

Branch 1

1. 备份 ArubaOS 6 BOC1 上的现有配置。GUI: **维护 > 备份 Flash**
2. 将 BOC1 上的映像升级到 ArubaOS 8，然后重新启动。GUI: **维护 > 映像管理**
3. 如果已在 Activate 上创建了配置规则，则控制器将执行 ZTP，与 MM 建立通信，以及下载其配置
4. 可选择手动配置控制器。通过 CLI 设置对话框将 BOC1 配置成为由 MM 管理的 MC。BOC1 现在将成为 MC1

Branch 2

1. 备份 ArubaOS 6 BOC2 上的现有配置。GUI: **维护 > 备份 Flash**
2. 将 BOC2 上的映像升级到 ArubaOS 8，然后重新启动。GUI: **维护 > 映像管理**
3. 如果已在 Activate 上创建了配置规则，则控制器将执行 ZTP，与 MM 建立通信，以及下载其配置
4. 可选择手动配置控制器。通过 CLI 设置对话框将 BOC2 配置成为由 MM 管理的 MC。BOC2 现在将成为 MC2

对 Branch 3 执行类似步骤。