数据表

ARUBAOS

为当今数字化工作场所提供增强型网络操作系统

概述

ArubaOS是Aruba Mobility Master、移动控制器以及控制器管理的园区接入点的网络操作系统。通过行业领先的软件创新，ArubaOS为各种规模的企业部署提供企业级性能和关键任务可靠性。

Aruba支持最新的Wi-Fi联盟标准，例如Wi-Fi 6（802.11ax）和802.11ad，以及WPA3和Enhanced Open安全协议。Aruba也支持以前所有的标准和协议，例如802.11a/b/g/n/ac，这使您的网络能够满足现在和未来的使用案例（见表1）。

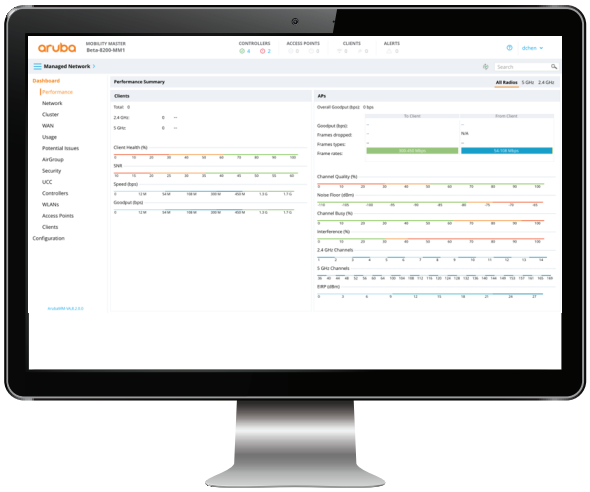
简单和安全的接入

ArubaOS也在动态网络隔离中发挥重要作用：基于用户角色、设备类型、应用程序和位置执行策略，简化有线和无线网络接入并确保安全。这个功能可以通过策略执行防火墙（PEF）许可证实现，并消除为网络上的每个新客户端人工配置SSI、VLAN或ACL的需求。

欲了解详细功能列表，请参阅ArubaOS版本说明。

Aruba Air Slice

ArubaOS为Air Slice提供完整编排。Air Slice 是Aruba Wi-Fi 6接入点特有的SLA等级应用保障技术。通过分配射频资源（例如时间、频率和空间流），并结合策略执行防火墙（PEF）收集的智能，接入点为特定用户和应用程序提供保用带宽。阅读 Air Slice 技术简报，了解更多信息。



关键特性

- 支持新Wi-Fi 6（802.11ax）、WPA3和Enhanced Open以及所有现有标准；
- 先进的人工智能驱动闭环无线/射频优化；
- 增强接入点效用和客户端漫游；
- 通过Air Slice提供SLA等级应用保障（ArubaOS 8.7+）；
- 通过零接触预配和分层配置，实现自动化部署；
- 动态网络隔离执行有线和无线接入策略，从而简化网络接入并确保网络接入安全；
- 无需附加硬件，可以感知3,000多个应用程序；
- 不中断系统的升级和无缝的故障转移。

企业安全框架	
认证类型	• IEEE 802.1X（EAP、LEAP、PEAP、EAP-TLS、EAP-TTLS、EAP-FAST、EAP-SIM、EAP-POTP、EAP-GTC、EAP-TLV、EAP-AKA、EAP-Experimental、EAP-MD5） • RFC 2548 Microsoft供应商特定的RADIUS属性 • RFC 2716 PPP EAP-TLS • RFC 2865 RADIUS认证 • RFC 3579 RADIUS EAP支持 • RFC 3580 IEEE 802.1X RADIUS指南 • RFC 3748可扩展认证协议 • MAC地址认证 • 基于Web的强制网络门户认证
认证服务器	• 内部数据库 • LDAP/SSL安全LDAP • RADIUS • TACACS+ • 经过测试的认证服务器互操作性： - Microsoft活动目录（AD） - Microsoft IAS和NPS RADIUS服务器 - Cisco ACS、ISE服务器 - Juniper Steel Belted RADIUS、Unified Access服务器 - RSA ACE/服务器 - Infoblox - Interlink RADIUS 服务器 - FreeRADIUS
加密协议	• CCMP/AES • WEP 64- and 128 位 • TKIP • SSL and TLS: - RC4 128 位 - RSA 1024 位 - RSA 2048 位 • L2TP/IPsec (RFC 3193) • XAUTH/IPsec • PPTP (RFC 2637)
可编程加密引擎	可以通过软件更新，支持未来的加密标准。
基于Web的强制网络门户（SSL）	支持身份验证方法的灵活性
集成访客接入管理	提供安全的访客接入选项。
站点到站点VPN	在移动控制器和IPsec设备之间建立IPsec隧道；为X.509 PKI、IKEv2、IKE PSK、IKE积极模式提供认证支持。

表 1

24x7关键任务网络连接

随着基于云的应用程序、服务、物联网和移动设备不断增长，终端用户期望无论何时何地连接都可以使用网络资源。同样，企业网络必须突破传统的安全边界，同时提供无缝的用户体验。通过最新版本ArubaOS，控制器集群能够提升网络性能，并最终帮助组织每年提高数百甚至数千小时的生产能力。

控制器集群是Mobility Master管理的独特功能，使一个集群中的多达12个移动控制器能够作为一个虚拟实例。通过使网络要求与各个硬件限制分离，这能够提升网络功能，显著扩展性能和可靠性。

为了减少网络中断，用户会话信息在集群中共享，从而维持活跃语音通话、视频流、数据传输、漫游客户端和网络管理。不中断系统升级和不中断业务升级用于消除维护窗口期和非预期停机计划。在独立、园区或分支机构模式中的移动控制器也能够以传统1:1或1:N基于VRRP的冗余配置方式进行部署（见表2和表3）。

通过基于浏览器的GUI（见图1和表4）或通过网络管理员熟悉的CLI，提供管理、配置和故障排除功能。Mobility Master能够在大型园区或分布式分支机构环境中集中配置和管理移动控制器和接入点，并能够提供基于任务的直观向导，从而简化配置。

高可用性部署模式	
主用/主用（1:1）	每个移动控制器通常提供 0%的额定容量。两个控制器互为备用。如果一个控制器发生故障，这个控制器的接入点切换到另一个控制器，确保所有接入点的高可用性。
主用/备用（1+1）	一个移动控制器终止所有接入点，而另一个控制器充当备用。如果主控制器发生故障，接入点切换到备用控制器。
N+1	单个备用控制器作为多个主用移动控制器的备份。

表 2

特性	优点
接入点与主用和备用移动控制器同时建立通信信道	一个移动控制器发生故障时，立即切换到冗余移动控制器。
在故障转移期间，接入点不会关闭和打开射频	SSID始终可用。
解决方案适用于三层网络	无需特殊拓扑结构。
客户端状态同步	进行凭证缓存，消除重新认证需求和RADIUS服务器超负载
N+1 超额订阅	简化配置，并减少所需移动控制器数量。

表 3

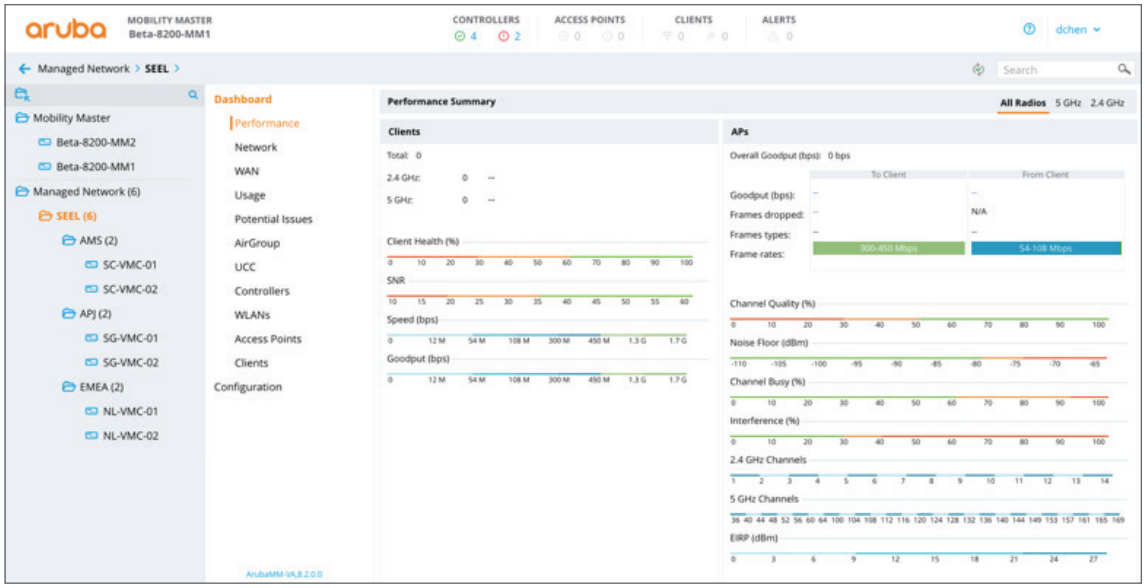


图1：ArubaOS 8用户界面

Wi-Fi网络管理和配置	
基于Web的配置	使具有标准Web浏览器的任何管理员能够管理系统。
命令行	控制台和SSH。
系统日志	支持多服务器、多级别和多设施。
SNMP v2c	是
SNMP v3	通过密码安全性，增强标准SNMP。
移动控制器的集中化配置	指定的主移动控制器可以配置和管理多个下游本地控制器。
VRRP	支持多个移动控制器之间的高可用性。
冗余数据中心支持	是 – 可以用备份控制器IP地址配置接入设备。
OSPF	是 – Stub模式支持学习缺省路由或将本地路由加入上游路由器。
快速生成树协议	是 – 提供快速L2收敛。

表 4

性能

自适应射频管理（ARM）

通过动态选择最佳802.11信道和发射功率，ARM最大程度地提高接入点的Wi-Fi稳定性和可预测性。这个功能帮助为所有客户端和应用程序确保最佳性能，特别是在具有大量移动用户和性能苛刻型应用程序导致网络争用和干扰的环境中（见表5）。

ClientMatch

作为自适应射频管理（ARM）的组成部分，射频优化专利技术ClientMatch能够缓解粘滞客户端问题，从而提升Wi-Fi客户端性能。ClientMatch能够使客户端设备连接最佳接入点；基于客户端设备支持的标准（例如下行链路或上行链路MU-MIMO），ClientMatch也能够将客户端设备分组，从而提升系统容量。这非常适合于具有复杂漫游要求的环境。

集中式隧道

接入点许可证使各个接入点能够将所有流量、策略、管理和控制决定转发到控制器，从而为具有复杂二层和三层要求的网络提高接入点效用（例如内存、处理和带宽）。ArubaOS 8和更高版本也使Aruba接入交换机能够模拟接入点角色（例如有线接入点），交换机配置和管理通过Aruba AirWave提供（见表6）。

自适应射频管理优点	
自适应射频管理（ARM）	自动管理所有射频参数，实现最高性能。
802.11ac VHT20、VHT40和VHT80支持	为所有802.11ac网络管理频谱。
802.11n HT20和HT40支持	为所有802.11n网络管理频谱。
客户端频段引导	使双频段客户端处于最佳射频频段。
在故障接入点周围自修复	自动调节功率水平，抵偿故障接入点。
空口时间公平性	管理客户端接入空口资源。经过配置可以提供公平接入，或为通过最新802.11标准连接的客户端提供优先接入。
射频频谱负载平衡	在可用信道中均匀分布客户端。
单个信道协调接入	确保最佳性能，即使同一信道上有邻近接入点。
射频规划	基于容量、覆盖和安全要求，进行接入点和射频监控器的自动预部署建模、规划和布置。
覆盖盲区和干扰检测	检测因覆盖缺口而无法联系的客户端。
基于计时器的接入点接入控制	在规定工作时间之外关闭接入点。
远程无线抓包	将802.11原始帧和流远程抓取到协议分析器。
第三方分析工具插接	Wireshark、OmniPeek、AirMagnet。
非法接入点检测和抑制	检测并自动关闭未经授权接入点。

表 5

统一接入框架	
用户连接方法	• 安全的企业级Wi-Fi • 有线以太网 • VPN远程访问
接入点连接方法	• 私有或公共IP云 - 以太网 - 无线WAN（EVDO、HSDPA） • Wi-Fi网状网（点对点和点对多点）
流量转发	• 集中式 – 所有用户流量流向移动控制器 • 策略路由 – 根据流量类型和策略而定，有选择地将用户流量转发到移动控制器，或为用户流量进行本地桥接
Wi-Fi加密	• 集中式 – 流量在设备和移动控制器之间加密 • 分布式 – 流量在设备和接入点之间加密 • 开放式 – 无加密
与现有网络集成	• 二层和三层集成 – 移动控制器能够在每个VLAN的基础上进行流量的切换或路由选择 • 快速生成树 – 实现快速L2收敛 • OSPF – 与现有路由拓扑结构进行简单集成

表6

情境感知控制

支持802.11e和Wi-Fi多媒体（WMM），通过WMM标签和内部硬件队列之间的映射，为延迟敏感型应用程序确保无线服务质量（QoS）。移动控制器使802.1p和IP DiffServ标签能够映射到硬件队列，用于提高有线端服务质量；

移动控制器也能够按照指示将某些802.1p和IP DiffServ标签应用于有需要的不同应用程序。ArubaOS也包含设备指纹识别技术，使网络管理员能够在设备类型和固件（例如iPhone、Android等等）的基础上分配策略。这使网络能够调控为哪些设备提供网络接入以及如何使用这些设备（见表7）。

情境感知控制网络	
T-SPEC/TCLAS	是
WMM	是
WMM 优先级映射	是
U-APSD（非排程自动节能传送）	是
用于高效组播传送的IGMP侦听	是
应用程序和设备指纹识别	是

表7

无缝二层和三层漫游

rubaOS包含代理移动IP/DHCP功能，在用户在楼层之间、在建筑物之间或在整个网络上移动时提供无缝连接，即使用户在使用视频和音频应用程序。漫游切换时间仅为2-3毫秒，无需重新验证和变更IP地址，也不会失去防火墙状态。当ArubaOS在Mobility Master上运行时，通过控制器集群实现漫游（见表8）。

VLAN 池

ArubaOS实现在移动控制器中集中并通过隧道传送到接入点，而不是在每个网络边缘交换机上配置VLAN。主要优势包括降低网络配置复杂性和最大生成树直径。实现VLAN用户成员的负载平衡，在大群用户在网络上移动时维持最佳网络性能。

安全和可见性

动态网络隔离

对于每个无线客户端、有线端口或有线端口上的用户，流量可以转发到移动控制器或网关，然后用策略执行防火墙进行安全隔离。基于端口的隧道（PBT）可以用于转发来自有线端口的所有流量，而基于用户的隧道（UBT）可以转发特定角色的流量，完全消除网络管理员本地化配置ACL、VLAN和子网的需求。

策略执行防火墙（PEF）

作为动态网络隔离的关键组成部分，PEF是用于实现用户和应用程序可见性的ArubaOS许可证。基于WLAN、LAN和远程VPN连接上的用户角色、应用程序、设备和位置感知，PEF为远程接入点、Instant接入点和VIA VPN客户端服务提供全部策略执行。

策略可以在ArubaOS之中人工创建，或者由Aruba ClearPass策略管理器集中管理，并能够同时应用于多个网络。

应用程序可见性和控制

应用程序可见性是PEF的功能之一。这项功能为分类使用深度包检测（DPI），提供3,000多个应用程序的广泛可见性和控制。通过易于使用的控制面板，可以简便和直观地优化和限制每个应用程序的流量。通过应用程序定制*，也可以定义未识别应用程序和类别（见图2和表9）。

无缝漫游特性	
快速漫游	控制器之内：2-3毫秒； 控制器之间：10-15毫秒。
在子网和VLAN上漫游	在客户端在网络上漫游时，会话不会断开。
代理移动IP	自动在移动控制器之间建立本地代理/外部关系。
代理DHCP	防止客户端在漫游时变更IP地址。
VLAN 池	在多个VLAN上自动实现客户端的负载平衡。

表 8

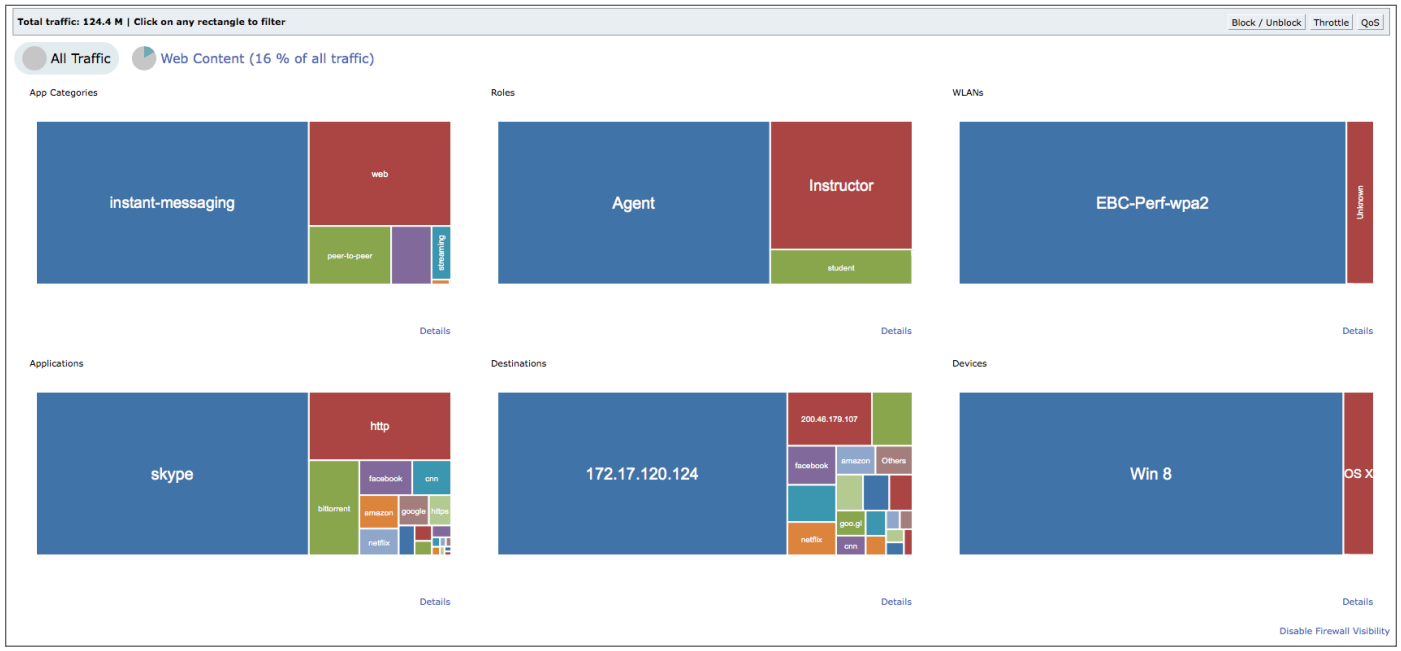


图2：应用程序流量分析控制面板

具有用户和应用程序可见性的策略执行防火墙	
特性	**优点**
全局或基于角色的策略	以一个命令控制所有用户流量的简便性，控制哪些用户可以运行哪些应用程序的灵活性。
3,000多个应用程序	高颗粒度的可见性和控制。
超过21个应用程序类别	简化对不同类型流量的控制。
实施服务质量（QoS）标签	使一个应用程序优先于另一个应用程序。
阻止不需要的应用程序	节省带宽并停止不需要的活动。
应用程序或应用程序类别的速率限制	允许非必要流量，同时防止其影响关键任务应用程序。

表9

远程接入点（RAP）性能

通过相同的ArubaOS接入点许可证，Aruba 远程接入点可以部署于分散地点，例如居家办公或临时工作地点。每个远程接入点与移动控制器建立一个混合IPSec/SSL-VPN连接，移动控制也作为VPN 连接器（VPNC），发挥双重作用（见图3和表10）。

虚拟内联网接入（VIA）VPN支持

VIA附加许可证使远程用户能够通过混合IPSec/SSL VPN客户端安全地连接到Aruba网络，无需企业DMZ中的专用VPNC。用户设备遵循与总部或分支机构相同的策略和服务定义。运用分割隧道或全隧道连接，ArubaOS支持Windows、Mac、iOS、Android和Linux（见表11）。

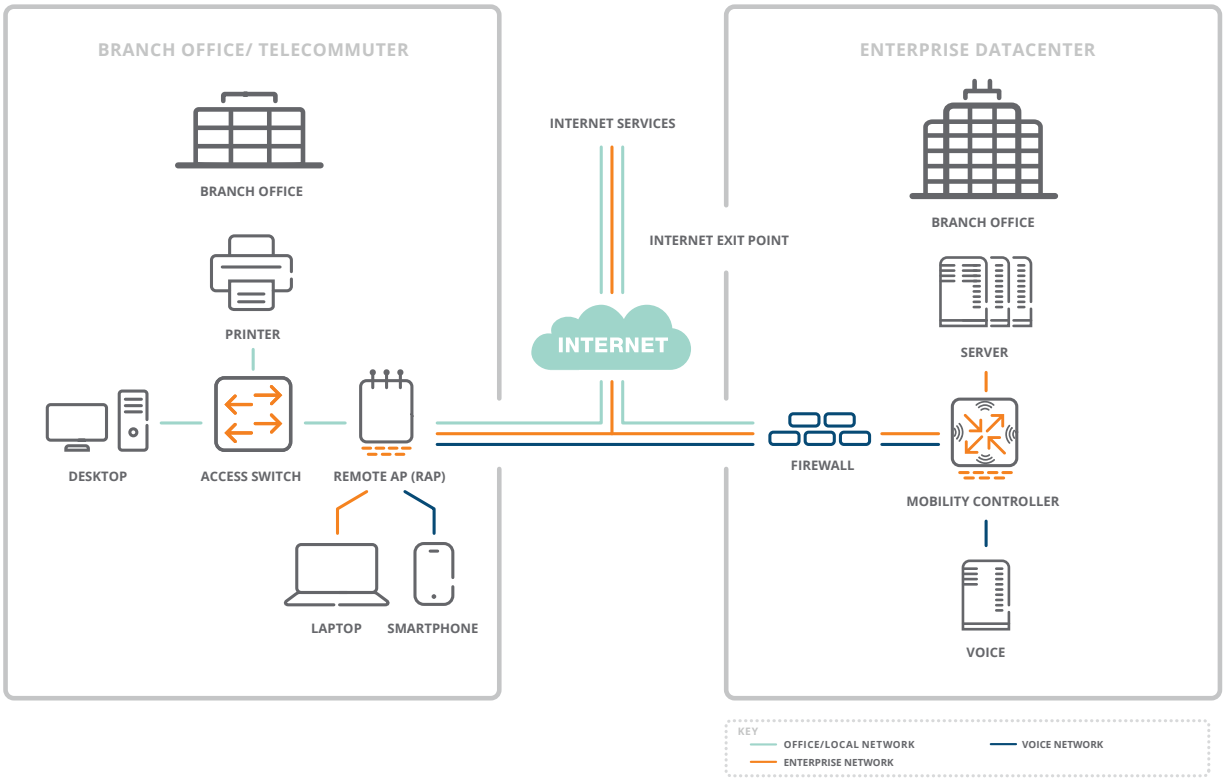


图3：与微型分支机构和小型办公场所建立安全移动连接的Aruba远程接入点

用于远程办公人员的远程接入点	
零接触预配	管理员无需任何预先配置就可以部署远程接入点；只需将远程接入点发运给终端用户。
有线和无线	用户通过有线以太网方式、Wi-Fi方式或通过上述两种方式连接到远程接入点。
灵活认证	每端口和每用户的802.1X、强制网络门户和MAC地址认证。
集中式管理	无需在接入点上执行本地配置，配置和管理由移动控制器完成。
3G/4G LTE WAN连接	远程接入点支持USB无线WAN适配器（EV-DO、HSDPA），用于主用或备用因特网连接。
FlexForward流量转发	• 集中式 – 所有用户流量流向移动控制器。 • 本地桥接 – 所有用户流量通过接入设备桥接到本地LAN网段。 • 策略路由 – 根据流量类型和策略而定（需要PEF许可证），有选择地将用户流量转发到移动控制器，或为用户流量进行本地桥接。
企业级安全	远程接入点使用X.509证书向移动控制器进行身份验证，然后建立安全的IPsec隧道。
上行链路带宽预留	为丢包敏感型应用协议（例如语音）定义预留带宽。
本地诊断	如果需要帮助，本地用户可以浏览预定义的URL，访问全部远程接入点诊断内容。
远程网状网入口	远程接入点也可以作为网状网入口，提供到下游接入点的无线链路。
支持的AP	所有Aruba AP
最低链路速率要求	每SSID 64 kbps。
加密协议（远程接入点到移动控制器）	AES-CBC-256（IPsec ESP内）。

表 10

用于远程接入的安全VPN连接	
经测试的客户端支持	• Windows、Mac OS、Android、iOS、Linux上的Aruba VIA客户端 • Cisco和Nortel VPN客户端 • OpenVPN、Apple/Windows原生客户端
VPN协议	• L2TP/IPsec (RFC 3193) • XAUTH/IPsec • PPTP (RFC 2637)
认证	• 用户名/密码 • X.509 PKI • RSA SecurID • 智能卡 • 多因素

表 11

高级加密法（ACR）

经过完全FIPS 140-2验证和通用标准认证的ACR附加许可证提供Suite B加密法，从而为处理受控非保密、机密和保密信息的远程用户提供安全接入。

增强Wi-Fi身份验证安全

增加WPA3支持，带来更加强大的加密和身份验证方法；Enhanced Open提供开放网络上的每用户加密。新MPSK功能为WPA2设备实现更加简单的密钥管理，如果一个设备类型的Wi-Fi密码需要变更，网络上的其他设备类型无需变更密钥（见表1）。阅读白皮书。

Web分类（WebCC）

通过可选订阅，ArubaOS提供基于云的Web内容分类，用于URL过滤的策略和声誉服务，以及IP声誉和地理位置过滤。根据Aruba基于密度的控制，这可以用于阻止连接和限制连接速率（见图4和表12）。

WIPS/WIDS和非法接入点防护

为了防御自组织网络、中间人攻击和拒绝服务攻击，并区分Wi-Fi来源和非Wi-Fi来源，ArubaOS RFProtect t模块提供集成的WIPS/WIDS/非法接入点抑制和分类，无需射频传感器和安全设备的单独系统。

Aruba的非法接入点分类算法能够准确区分连接到网络的非法接入点和在附近干扰的接入点。

第三方集成

基于REST的API允许与安全供应商（例如Palo Alto Networks和Check Point Software）进行集成，从而确保端到端安全。可以为特定类型流量预先定义策略；可以将策略转发到内部部署安全防火墙，用于附加检查。

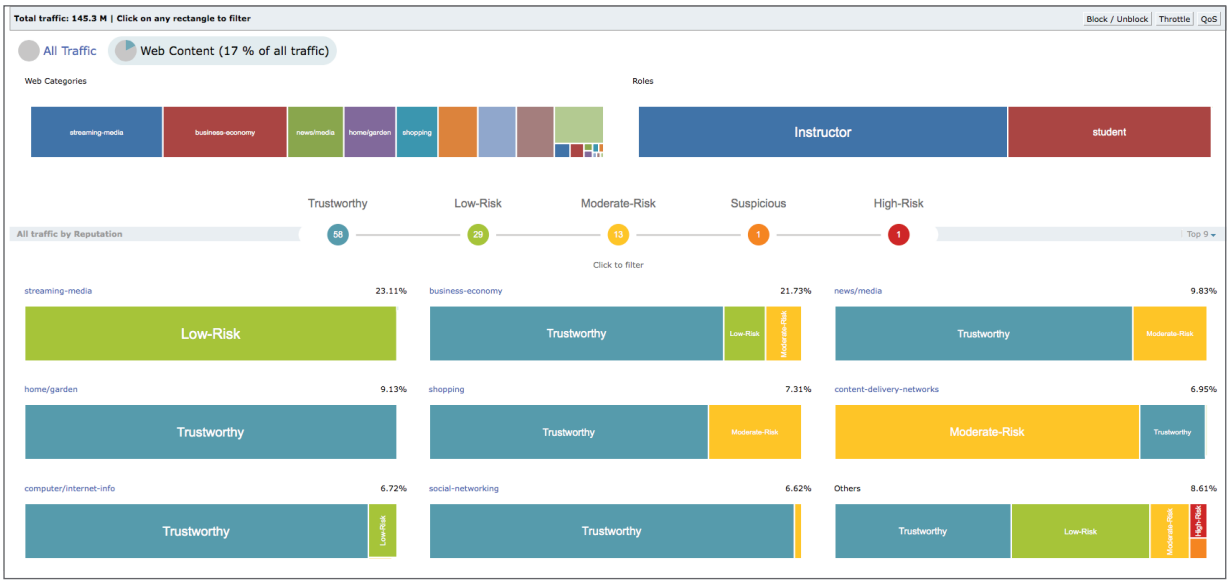


图4：WebCC控制面板

WebCC特性	
将Web流量分为83个类别	确定如何使用网络带宽。
按类别阻止网站	执行网络可接受的使用策略。
按类别提供服务质量和带宽控制	降低娱乐应用程序的网络使用率。
按声誉阻止网站	减少恶意软件进入网络的机会。

表 12

Microsoft特性

Aruba与Microsoft集成，提供独特的应用程序智能，用于检测Office 365、Teams和Skype for Business流量，然后使它们优先于不太重要的应用程序。对于Skype for Business/Lync流量，IT团队也能够优先处理特定媒体，例如视频、音频和消息。

统一通信和协作（UCC）

集成控制面板

通过集成UCC控制面板，ArubaOS为Microsoft Skype for Business/Lync、Alcatel Lucent New Office Environment（NOE）、Microsoft Teams*、Apple Facetime、Cisco Jabber、Cisco Spark、Cisco Skinny Call Control Protocol（SCCP）、Spectralink Voice Priority（SVP）、SIP、H.323和Vocera提供通话质量衡量指标（时延、抖动、丢包）。这为网络管理员提供增强应用程序可见性以及关键Wi-Fi故障排除能力。Aruba的应用程序指纹识别技术也使ArubaOS能够遵循加密信号协议，并延迟ARM扫描和ClientMatch漫游，从而优化活跃呼叫会话期间的用户体验（见图5）。

Wi-Fi Calling支持

运营商将Wi-Fi Calling用于减轻Wi-Fi网络上的蜂窝语音流量，在蜂窝覆盖差的建筑和区域内改善连接。ArubaOS将Wi-Fi Calling当作UCC语音应用程序，并实施服务质量，通过集成UCC控制面板阻止和节制通话。Aruba也提供基于每用户、每设备和每运营商的可见性。

WAN性能

路由和衡量指标

ArubaOS使用众多功能（例如基于策略的路由、动态路径导向和压缩），以涵盖WLAN和WAN的智能提升WAN健康度。集成控制面板也帮助在公用和私有上行链路实现关键WAN衡量指标（例如时延、抖动和丢包）的可视化（见图6）。

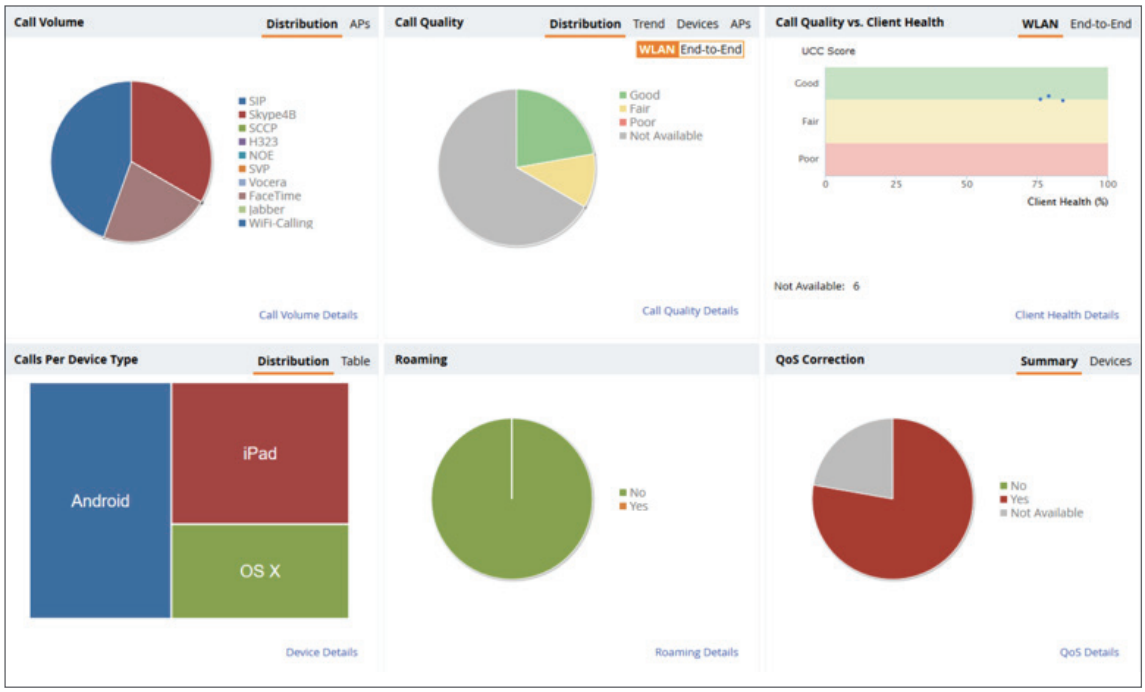


图5：UCC控制面板

图6：WAN控制面板

运行

集成强制网络门户

对于无头客户端设备或没有WPA、VPN或其他安全软件的设备，ArubaOS支持基于Web浏览器的强制网络门户，从而提供安全的基于Web的认证。强制网络门户认证用SLL加密，并能够支持具有登录名和密码的注册用户或仅仅提供电子邮件地址的访客用户。关于先进访客接入需求，请参阅Aruba ClearPass Guest。

MDNS和DLNA支持（AirGroup）

通过AirGroup，Aruba改进Apple、Google和第三方服务，例如AirPlay, AirPrint和Google Cast。这个独特功能优化IP组播视频流量，排列服务优先顺序，并增加策略控制。

简单配置选项确保这些客户端设备能够互相可见，而高级选项基于物理位置、当日时间和用户/角色详情，限制接入某些设备。

Mesh网状组网功能

在没有布设或者不具有足够的光纤或电缆的情况下，基于ArubaOS无线接入点可以灵活地支持无线上行链路。无线Mesh网状组网经常用于点到点无线回传、安全视频监控等应用场景，以及需要现场临时架设接入网络，提供标准的、与基于有线回传完全相同的无线和有线接入服务的场景。每个Aruba接入点通过智能链路管理算法，可以自动调整和优化Mesh网络的无线中继链路和数据转发路径。所有的Aruba室内或者室外接入点都具有多种工作模式，网络管理员可以轻松地利用这些Aruba接入点快速搭建无线Mesh网络，或者利用更新一代的802.11ad技术以满足更高性能和更远距离的联网需求。
（见图7和表13）。

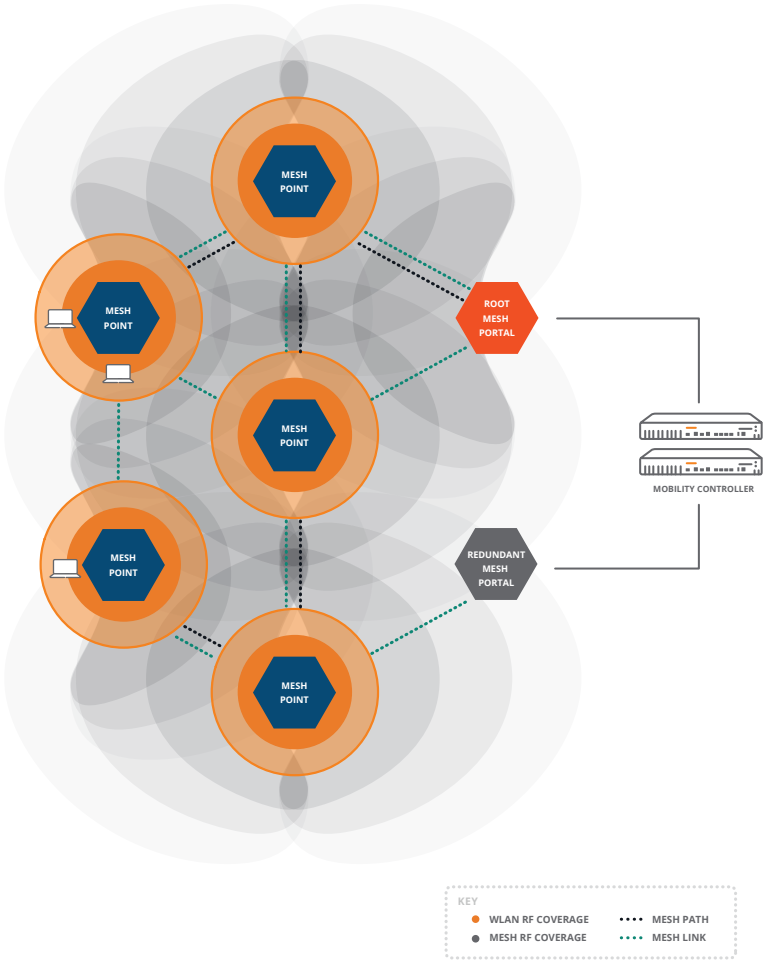


图7：安全企业网状网

安全企业网状网	
广泛应用支持	Wi-Fi接入、并发无线入侵防护、无线回传、LAN桥接、点对多点连接。
统一网络接入	将网状网络与园区和分支机构办公场所WLAN整合；用户在园区和分支机构Wi-Fi与网状网络之间无缝漫游。
协作控制	智能射频链路管理决定最优性能路径，并使网络能够自行组织。
自修复	富有弹性的自修复网状网克服路径损坏或接入点故障。
集中式加密	从客户端到核心进行端对端数据加密，即使网状网接入点被盗，也能保护网络。
网状网集群	通过将大型网状网分割成多个高可用性集群来支持扩展性。
集中式管理	所有网状网节点均由移动控制器集中配置和控制，不需要本地管理。
广泛的图形化支持工具	整个网络可视化，包括覆盖热图、自动链路分配计算、平面布置图、网络拓扑结构图。
基于标准的设计	基于IEEE 802.11s设计原则，确保企业网状网安全。

表 13

IPv6 支持

ArubaOS支持IPv6环境以及IPv4网络中的IPv6双栈互操作性。这非常适合几乎已经耗尽可用IPv4地址并需要从IPv4过渡到IPv6（可增加很大地址空间）的组织（见表14）。

多供应商网络管理

Aruba AirWave为Aruba控制器管理的接入点以及多供应商无线、有线和WAN环境提供统一网络管理。AirWave可以用于监控、分析和排除故障方面的规划和部署。AirWave也提供长期趋势和报告、帮助台集成工具以及可定制警报。

网络分析和保障

ArubaOS与Aruba NetInsight集成，提供自动化网络优化和性能提升。人工智能驱动的机器学习算法收集来自ArubaOS的数据，将网络与类似同级网络进行对标，并建议射频、认证和DHCP Request性能方面所需的配置变化。

高级策略管理

ArubaOS与Aruba ClearPass集成，用于多供应商有线、无线和分布式远程网络上的策略管理、AAA功能、高级访客接入和设备注册。ClearPass为面临越来越多物联网、自带设备（BYOD）和隔离挑战的企业解决安全要求（见表1）。

物联网和定位准备就绪的无线支持*

ArubaOS包含与Aruba Meridian、ALE以及第三方Wi-Fi、BLE、Zigbee和基于USB的供应商解决方案的集成。每个接入点充当物联网和定位准备就绪的网关，无需附加ArubaOS软件。

IPV6支持	
IPV6 IPsec	是
IPv6管理	GRE, SSH, Telnet, SCP, Web UI, FTP,TFTP, Syslog, SNMP
IPv6 DHCP 服务器	是
IPv6强制网络门户	是
在移动控制器上支持IPv6 VLAN接口地址	是
支持IPv6上的接入点-移动控制器通信	是
USGv6认证防火墙	是

表 14

增强Mobility Master性能

人工智能驱动的射频管理（AirMatch）

射频管理创新技术AirMatch为整个网络实现射频信道、信道带宽和发射功率分配的自动化。AirMatch运用机器学习算法，基于不断变化的环境条件和系统容量，主动学习和适应网络（见表15）。

分层配置和更高可见性

在Mobility Master上运行的ArubaOS 8使用集中化多层架构。通过专用管理控制台，这个架构合并所有部署模式（例如全主、单主/多本地和多主/本地）。通过零接触预配（ZTP），可以从Mobility Master执行网络配置，并将网络配置分布到所有移动控制器。Mobility Master也允许能够基于地点需求将许可证分配到各个控制器的许可池。

无中断故障转移和自动化负载平衡

使用控制器集群，实现用户会话和接入点流量的负载平衡，从而优化网络高峰时期的网络利用率，并最大程度地提高计划外停机期间的可用性（图1）。这意味着，万一发生控制器失去连接，用户在语音通话、视频流或数据传输方面不会察觉到任何影响。

不中断系统升级和多版本支持

通过Mobility Master，ArubaOS可以在升级的同时支持活跃用户会话，从而消除计划内维护窗口期或停机时间需求。可以有选择地升级每个控制器集群或各个服务模块（AppRF、AirGroup、ARM等等），不会影响网络的其余部分。

多租户Wi-Fi支持（MultiZone）

不同的控制器可以用于同一接入点基础设施，从而终止不同Aruba控制器上的不同SSID，同时为所有网络、策略、管理和可见性保持完全隔离和安全。这非常适合多租户的需求（多个组织处于一个办公空间），也非常适合一个需要多个单独安全网络的组织。欲了解更多信息，请参阅MultiZone技术简报。

北向API（NBAPI）

Mobility Master包含一整套NBAPI，从而实现网络的深入可见性。NBAPI以易于集成的格式，提供射频健康衡量指标、应用程序利用率、设备类型和用户数据。第三方应用程序可以接收这些信息，用于提升可见性和监控水平。

AirMatch优点	
均匀信道分配	在可用信道上均匀分布射频，抑制干扰，最大程度地提升系统容量。
动态信道带宽调整	在20 MHz、40 MHz和80 MHz之间动态调整，从而匹配环境密度。
自动发射功率调整	检查整个WLAN覆盖，并自动调整接入点发射功率，确保最佳覆盖和用户体验。

表 15

认证

- Wi-Fi联盟认证（802.11a/b/g/n/d/h/ac/ad、WPA™个人、WPA™企业、WPA2™个人、WPA2™企业、WPA3™企业、WPA3™个人、Enhanced Open™、WMM™、WMM Power Save）
- FIPS 140-2验证（在FIPS模式下运行时）
- 通用标准EAL-2
- RSA认证
- Polycom/Spectralink VIEW认证
- USGv6防火墙

支持的标准

通用交换和路由

- RFC 1812 IPv4路由器技术要求
- RFC 1519 CIDR
- RFC 1256 IPv4 ICMP路由器发现（IRDP）
- RFC 1122 主机要求
- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 894 以太网承载IP
- RFC 1027 代理 ARP
- RFC 2236 IGMPv2
- RFC 2328 OSPFv2
- RFC 2338 VRRP
- RFC 2460 因特网协议版本6（IPv6）
- RFC 2516 以太网点对点协议（PPPoE）
- RFC 3220 IP对IPv4的IP移动支持（部分支持）
- RFC 4541 IGMP和MLD侦听
- IEEE 802.1D-2004 – MAC 桥接
- IEEE 802.1Q – 1998 虚拟桥接局域网
- IEEE 802.1w – 快速生成树协议

服务质量（QoS）和策略

- IEEE 802.1D – 2004 (802.1p) 包优先
- IEEE 802.11e – 服务质量增强
- RFC 2474 差异化服务

无线

- IEEE 802.11a/b/g/n/ac 5 GHz、2.4 GHz
- IEEE 802.11d附加监管域
- IEEE 802.11e服务质量（QoS）
- IEEE 802.11h欧洲5 GHz频谱和传输功率扩展
- IEEE 802.11i MAC安全增强
- IEEE 802.11k射频资源管理
- IEEE 802.11ac超高吞吐量增强
- IEEE 802.11n高吞吐量增强
- IEEE 802.11v无线网络管理（部分支持）

管理和流量分析

- RFC 2030 简单网络时间协议（SNTP）v4
- RFC 854 Telnet客户端和服务器
- RFC 783 TFTP协议（修订版本2）
- RFC 951 Bootstrap协议（BOOTP）
- RFC-1542 Bootstrap协议的说明和扩展
- RFC 2131 动态主机配置协议
- RFC 1591 DNS（客户端操作）
- RFC 1155 管理信息结构（SMIv1）
- RFC 1157 SNMPv1
- RFC 1212 简明MIB规范
- RFC 1213 基于TCP/IP的因特网网络管理的管理信息库 - MIB-II
- RFC 1215 SNMP使用SNMP定义Trap的惯例
- RFC 1286 桥接 MIB
- RFC 3414 用于简单网络管理v.3的基于用户的安全模型（USM）
- RFC 1573 接口演进
- RFC 2011 使用 SMIv2的因特网协议的SNM Pv2管理信息库
- RFC 2012 SNMPv2 管理信息
- RFC 2013 SNMPv2 管理信息
- RFC 2578 管理信息结构版本 2（SMIv2）
- RFC 2579 SMIv2的文本约定
- RFC 2863 接口组MIB
- RFC 3418 SNMP的管理信息库（MIB）
- RFC 959 文件传输协议（FTP）
- RFC 2660 安全超文本传输协议（HTTPS）
- RFC 1901 1908 SNMP v2c SMIv2 和修订版MIB-II
- RFC 2570, 2575 SNMPv3 基于用户的安全、加密和认证
- RFC 2576 SNMP版本1、版本2和版本3之间的共存
- RFC 2233 接口 MIB
- RFC 2251 轻量级目录访问协议（v3）
- RFC 1492 访问控制协议，TACACS+
- RFC 2865 远程访问拨号用户服务（RADIUS）
- RFC 2866 RADIUS会计

- RFC 2869 RADIUS扩展
- RFC 3576 远程RADIUS的动态授权扩展
- RFC 3579 RADUIS可扩展认证协议支持（EAP）
- RFC 3580 IEEE 802.1X 远程认证拨号用户服务（RADIUS）
- RFC 2548 Microsoft RADUIS 属性
- RFC 1350 TFTP协议（修订版本2）
- RFC 3164 BSD 系统日志协议（syslog）
- RFC 2819 远程网络监视（RMON）MIB

安全和加密

- IEEE 802.1X 基于端口的网络接入控制
- RFC 1661 点对点协议（PPP）
- RFC 2104 用于消息认证的键入-散列法（HMAC）
- RFC 2246 TLS协议（SSL）
- RFC 2401 因特网协议的安全架构
- RFC 2403 在ESP和AH中使用HMAC-MD5-96
- RFC 2404 在ESP和AH中使用HMAC-SHA-1-96
- RFC 2405 带显式IV的 ESP DES-CBC密码算法
- RFC 2406 IP封装安全有效载荷（ESP）
- RFC 2407 用于解释ISAKMP的IP安全域
- RFC 2408 因特网安全联盟和密钥管理协议（ISAKM P）
- RFC 2409 因特网密钥交换（IKE）v1
- RFC 2451 ESP CBC模式密码算法
- RFC 2661 第二层隧道协议（L2TP）
- RFC 2716 PPP EAP TLS认证协议
- RFC 3079 生成密钥用于Microsoft点对点加密（MPPE）
- RFC 3162 IPv6网络中的RADIUS
- RFC 3193 使用IPsec保护L2TP
- RFC 3602 AES-CBC密码算法及其与IPsec的使用
- RFC 3706 死点检测（DPD）
- RFC 3736 IPv6的DHCP服务
- RFC 3748、5247可扩展认证协议（EAP）
- RFC 3947 IKE中的NAT穿越协商
- RFC 3948 IPsec数据包的UDP封装
- RFC 4017 无线局域网的EAP方法要求
- RFC 4106 GCM 用于 IPSEC
- RFC 4137 EAP Peer和认证器的状态机
- RFC 4306 因特网密钥交换（IKE）v2
- RFC 4793 EAP-POTP
- RFC 5246 TLS1.2
- RFC 5247 密钥管理框架
- RFC 5281 EAP-TTLS v0
- RFC 5430 TLS的Suite-B概况
- RFC 6106 用于DNS配置的IPv6路由器广告选项
- IETF 草案 RadSec – TLS 的TLS加密

服务和保修信息

- 硬件：1年零件/人工，可以通过支持合同延长。
- 软件：90天，可以通过支持合同延长。

欲了解Aruba WLAN产品的更多信息，请参阅以下Web页面：

Aruba接入点

Aruba 网关和控制器

Aruba VPN 服务

订购信息*

零件编号	说明
JW471AAE	Aruba LIC-ENT企业（LIC-AP LIC-PEF LIC-RFP和LIC-AW）许可证绑定E-LTU
JW472AAE	Aruba LIC-AP控制器每接入点容量许可证E-LTU
JW473AAE	Aruba LIC-PEF控制器策略执行防火墙每接入点许可证E-LTU
JW474AAE	Aruba LIC-RFP控制器RFProtect每接入点许可证E-LTU
JZ148AAE	Aruba LIC-VIA每VIA客户端许可证E-LTU 这个许可证从Aruba VIA VPN客户端为VPN终端实现基于每会话的防火墙服务
Q9B90AAE	Aruba LIC-ACR控制器高级加密法1会话许可证LTU
JY028AAE	Aruba控制器Web内容分类1年订阅E-STU
JY029AAE	Aruba控制器Web内容分类3年订阅E-STU
JY030AAE	Aruba控制器Web内容分类5年订阅E-STU
JY031AAE	Aruba控制器Web内容分类7年订阅E-STU
JY032AAE	Aruba控制器Web内容分类10年订阅E-STU
JW495AAE	Aruba PEF VIA许可证用于7005控制器E-LTU
JY342AAE	Aruba PEF VIA许可证用于7008控制器E-LTU
JW496AAE	Aruba PEF VIA许可证用于7010控制器E-LTU
JW497AAE	Aruba PEF VIA许可证用于7024控制器E-LTU
JW498AAE	Aruba PEF VIA许可证用于7030控制器E-LTU
JW499AAE	Aruba PEF VIA许可证用于7205控制器E-LTU
JW500AAE	Aruba PEF VIA许可证用于7210控制器E-LTU
JW501AAE	Aruba PEF VIA许可证用于7220控制器E-LTU
JW502AAE	Aruba PEF VIA许可证用于7240控制器E-LTU

*注：LIC-VIA许可证是每VIA用户许可证，不与任何特定控制器绑定。LIC-VIA许可证可以从一个控制器转移到另一个控制器。与PEFV不同，在AOS 8.x部署中，LIC-VIA支持集中式许可，并可以由Mobility Master或主控制器管理。欲了解更多信息，请参阅7000系列和7200系列订购指南。

移动控制器部署

在园区或分支机构接入层部署中，可以使用Aruba移动控制器许可证部署Aruba 7200系列。在这个模式中，控制器不能同时用于SD-WAN。

在移动控制器模式中，7200系列也可以加入Aruba动态网络隔离框架，但网络中的每个Aruba接入点和交换机至少需要一个接入点许可证和一个策略执行防火墙（PEF）许可证。

移动控制器许可证

零件编号	说明
JW472AAE	Aruba LIC-AP控制器每接入点容量许可证E-LTU
JW473AAE	Aruba LIC-PEF控制器策略执行防火墙每接入点许可证E-LTU
JW474AAE	Aruba LIC-RFP控制器RFProtect每接入点许可证E-LTU
JW471AAE	Aruba LIC-ENT企业（LIC-AP LIC-PEF LIC-RFP和LIC-AW）许可证绑定E-LTU
Q9B90AAE	Aruba LIC-ACR控制器高级加密法1会话许可证E-LTU
JY028AAE	Aruba控制器Web内容分类1年订阅E-STU
JY029AAE	Aruba控制器Web内容分类3年订阅E-STU
JY030AAE	Aruba控制器Web内容分类5年订阅E-STU
JY031AAE	Aruba控制器Web内容分类7年订阅E-STU
JY032AAE	Aruba控制器Web内容分类10年订阅E-STU
Q9B90AAE	Aruba高级加密法1会话许可证E-LTU
JW499AAE	Aruba PEF VIA许可证用于7205控制器E-LTU
JW500AAE	Aruba PEF VIA许可证用于7210控制器E-LTU
JW501AAE	Aruba PEF VIA许可证用于7220控制器E-LTU
JW502AAE	Aruba PEF VIA许可证用于7240控制器E-LTU
JZ148AAE	Aruba LIC-VIA每VIA客户端许可证E-LTU

对于控制器所附的每个接入点，最低配置是每个接入点1个LIC-AP。

- LIC-ENT（JW471AAE）相当于LIC-AP、LIC-REF、LIC-RFP和LIC-AW各一个。
- LIC-AW是AirWave管理系统的设备许可证。
- 对于动态网络隔离，每接入点许可证数量必须等于通过隧道传送流量的接入点和交换机之和。对于虚拟交换机堆叠，每堆叠将消耗一个接入点许可证。
- PEFV许可证为VPN终端（例如Aruba VIA、Aruba RAP和IAP-VPN）实现基于每控制器的防火墙服务。

注：PEFV许可证也可以用于VIA VPN终端。但是，PEFV与一个特定控制器绑定，许可证容量随控制器用户容量变化。另一方面，LIC-VIA许可证是每VIA用户许可证，不与任何特定控制器绑定。LIC-VIA许可证可以从一个控制器转移到另一个控制器。与PEFV不同，在AOS 8.x部署中，LIC- VIA支持集中式许可，并可以由Mobility Master或主控制器管理。

在园区或分支机构接入层部署中，也可以使用Aruba移动控制器软件许可证部署Aruba 9000系列，9000系列将像7000系列或7200系列移动控制器一样发挥作用。在这个模式中，网关不能同时用于SD-WAN。

在移动控制器模式中，9000系列也可以加入Aruba的动态网络隔离框架，但网络中的每个Aruba接入点和交换机至少需要一个接入点许可证和一个策略执行防火墙（PEF）许可证。

移动控制器许可证

零件编号	说明
JW472AAE	Aruba LIC-AP控制器每接入点容量许可证E-LTU
JW473AAE	Aruba LIC-PEF控制器策略执行防火墙每接入点许可证E-LTU
JW474AAE	Aruba LIC-RFP控制器RFProtect每接入点许可证E-LTU
JW471AAE	Aruba LIC-ENT企业（LIC-AP LIC-PEF LIC-RFP和LIC-AW）许可证绑定E-LTU
Q9B90AAE	Aruba LIC-ACR控制器高级加密法1会话许可证E-LTU
JY028AAE	Aruba控制器Web内容分类1年订阅E-STU
JY029AAE	Aruba控制器Web内容分类3年订阅E-STU
JY030AAE	Aruba控制器Web内容分类5年订阅E-STU
JY031AAE	Aruba控制器Web内容分类7年订阅E-STU
JY032AAE	Aruba控制器Web内容分类10年订阅E-STU
JZ148AAE	Aruba LIC-VIA每VIA客户端许可证E-LTU

- 一个9000系列网关不能同时用于SD-WAN和移动控制器功能。
- 对于网关所附的每个接入点，最低配置是每个接入点1个LIC-AP。
- LIC-AW是AirWave网络管理系统的设备许可证。
- 对于动态网络隔离，每接入点许可证数量必须等于通过隧道传送流量的接入点和交换机之和。对于虚拟交换机堆叠，每堆叠将消耗一个接入点许可证。
- LIC-VIA许可证是每用户会话许可证，可以从一个网关/控制器转移到另一个网关/控制器。
- 在ArubaOS 8部署中，LIC-VIA支持集中式许可，并可以由Mobility Master或主控制器管理。

DS_ArubaOS_SK_072020 a00073441enw