产品资料

ArubaOS 8 控制器操作系统

这个更为智能化的操作系统专为当今移动化的办公场所打造。

概述

移动设备、物联网（IoT）和关键业务应用程序使移动工作人员能够提高生产力和效率，但这同时提高了他们对网络的需求。

ArubaOS 是所有 Aruba 移动控制器、虚拟移动控制器、Mobility Master 和控制器管理的无线接入点的操作系统。凭借广泛的集成技术和功能，ArubaOS 8 提供统一的有线和无线接入、无缝漫游、企业级安全、以及始终在线的网络，交付所需的性能、用户体验和可靠性，以支持高密度环境。

Mobility Master 是 Aruba 架构的一个新组件，使客户能够利用要求集中协调的高级功能，以及因移动和 IoT 设备需求增加而扩展的网络。它还可以替代主控制器的先前功能，并且可以部署为 VM 或 x86 硬件设备。Mobility Master 自动优化 RF，并在不太可能发生的控制器宕机故障中实现无中断故障转移。

Aruba 当前的移动控制器客户可以从 ArubaOS 版本 6 升级到版本 8，并立即受益于一些新特性和功能。对于更高级的功能（例如第三方集成），客户需要在部署中添加 Mobility Master。有关 ArubaOS 8 上详细功能的说明，请参阅此处提供的列表说明。

ArubaOS 8系统中的以下技术仅在MOBILITY MASTER中得到支持	
功能特性	优点
AirMatch	Aruba 利用 AirMatch 进一步增强了自适应射频管理（ARM）技术——新的自动化信道优化、发射功率调整和信道宽度系统，利用动态机器学习智能自动地优化整个 WLAN 网络。
控制器集群	通过在一个集群中支持多达 12 个控制器，控制器集群能够在发生故障或人群密度极高的情况下，跨越大型园区提供无缝体验。
MultiZone	Mobility Master 中的新 MultiZone 功能可让 IT 企业机构在同一物理位置使用相同的接入点时，拥有多个独立的安全网络。
北向API接口	Mobility Master 拥有一套完整的北向 API，能够帮助深入了解网络。北向 API 接口以易于集成的格式提供 RF 健康度量、应用程序利用率、设备类型和用户数据的信息。第三方应用程序可以从控制器中接收信息，并分析所有这些指标，以提高可视性和监控能力。
在线模块升级	Mobility Master 引入了动态更新 Mobility Master 中各个独立服务模块（AppRF、AirGroup、ARM、AirMatch、KIBAPI、UCM、WebCC 和 IP 分类）的能力，而无需重新启动整个系统。

以下技术是ARUBA操作系统的核心	
功能特性	优点
ClientMatch	Aruba 获得专利的 ClientMatch 技术消除了粘性客户端，并通过确保客户端连接最佳接入点，提高了 Wi-Fi 性能。它还将 MU-MIMO 客户端分组，用于同时传输到多个设备，从而提高整体 WLAN 容量。
AppRF	AppRF 技术是可选的 ArubaOS 策略执行防火墙（P E F）模块的一部分，为 WLAN 带来了应用感知功能。它使 IT 能够为每个用户确定应用程序的优先级，并扩展自带设备（BYOD）事务和设备密度。
AirGroup 技术	AirGroup 可以轻松地跨子网共享 Apple TV、打印机、Google Chromecast 和其他 DNS 广告设备。简单的配置选项确保所有设备可以看到彼此，而高级选项则减少了基于物理位置、当日时间、角色和自配置共享岛的共享范围。
自适应射频管理（ARM）技术	自适应射频管理（ARM）技术动态调整 RF 环境，以最大程度地提高 Wi-Fi 稳定性和可预测性，确保所有客户端和应用程序包括 Microsoft Skype for Business voice、视频、桌面共享和聊天信息流的最佳性能。
RFProtect模块	为了保护网络资源免受无线威胁并优化网络性能，ArubaOS 8 集成了行业领先的非法 AP 遏制和分类解决方案——ArubaOS RFProtect 模块。 RFProtect 模块将无线安全集成到网络基础设施中，而无需单独的 RF 传感器和安全设备系统，从而实现政府级无线入侵防护。 注意：这是一个可选的许可功能。
高级加密	ArubaOS 高级加密（ACR）模块为 Aruba 移动控制器提供军用级 Suite B 加密技术，为用户带来可移动性，并能够安全访问处理敏感、机密和分类信息的网络。
虚拟内部网访问（VIA）客户端	VIA 是一种自由混合的 IPsec / SSL VPN，可自动扫描并选择到公司网络的最佳安全连接。与传统 VPN 软件不同，VIA 提供零接触终端用户体验，并能在客户端设备上自动配置 WLAN 设置。VIA 完全感知 Wi-Fi。
Clarity	IT 企业机构可以查看非 RF 指标（RADIUS、DHCP 和 DNS 服务器），不仅能够为他们提供端到端的无线用户体验的可视性，还能够在用户受到影响之前预见连接问题。 Clarity 不仅能够查看通过网络的实际流量，还能够让 WLAN 管理员模拟流量，在用户体验服务中断和性能问题之前识别这些问题。这个主动的工作流程可以在数千个地点按需或按计划启动。 注意：这是一个可选的许可功能。

简化操作

与在包含全局和本地配置的平面配置模型上操作的 ArubaOS6 相反，ArubaOS 8 新的 UI 界面使用集中式多层体系结构，清晰地分离了管理、控制和转发功能。Mobility Master 和受管设备的所有配置都在一个集中的地点进行——这能够带来更好的可见性和监控能力，并能够简化配置流程，并最大程度避免重复作业。

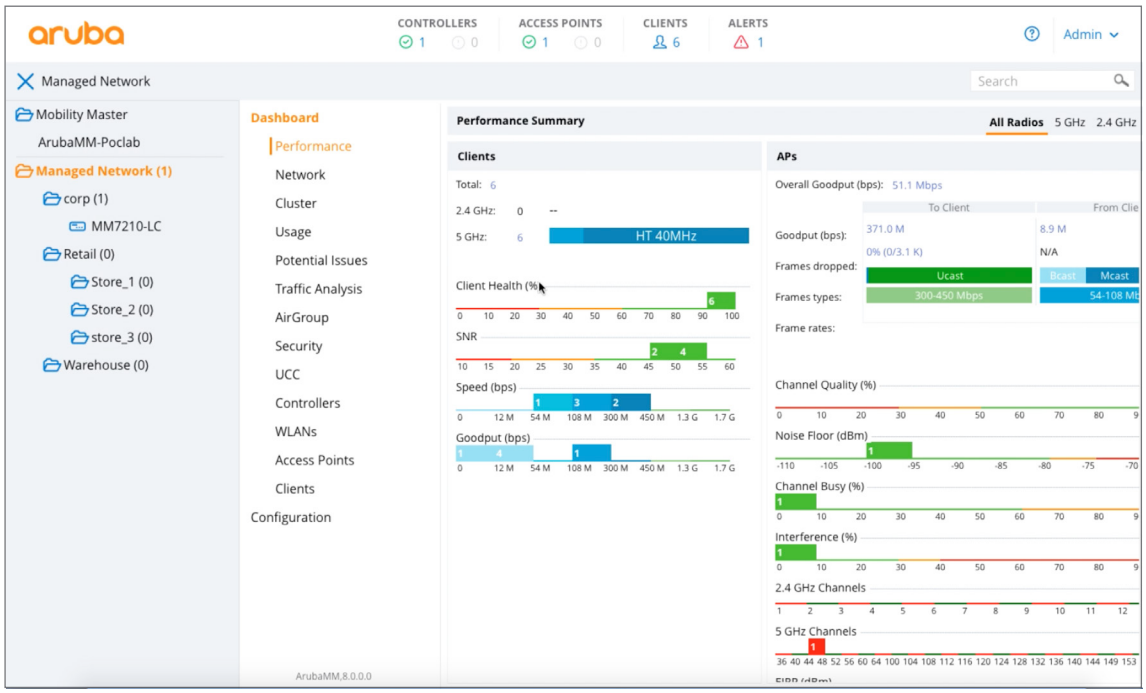
ArubaOS 8 中的新 UI 界面具有现代化的外观，采用快速化的工作流程，使用起来更为简单。ArubaOS 8 中的以下功能简化了网络操作：

带池的集中许可：IT 团队可通过来自 Mobility Master 或主控制器的集中式许可，在一个集中式位置管理所有许可证。在新的 AOS 8 当中，我们扩展了此功能，包含了带池的集中式许可。对于在企业内部为不同团体提供单独资助的一些客户，他们可以选择为每个团体分配许可，以便他们进行自我管理和使用。

零接触配置服务（ZTP）：ZTP 自动部署 AP 和受管设备。即插即用可实现快速简便的部署和简单化操作，降低成本并减少配置错误。ZTP 在 7xxx 移动控制器中引入，现在在 ArubaOS 8 中，我们正在将这个功能包含在 72xx 移动控制器当中。移动控制器从主控制器或 Mobility Master 接收其本地配置、全局配置和许可证限制的信息，并实现自动配置。

启用统一访问

Aruba 允许任何用户，无论地理位置在哪里，采用有线还是无线，都能够始终如一的安全访问企业网络。统一的安全和访问策略可应用于总部、分支机构、家庭办公室或者在出差的用户。用户和设备通过简单轻便的接入设备或软件连接公司网络，这些接入设备或软件能安全且自动地连接到移动控制器。



图I：ArubaOS 8新UI

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 - 无线广域网（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，将用户流量选择性地转发到移动控制器或本地桥接
Wi-Fi加密	• 集中式 - 流量在设备和移动控制器之间进行加密。 • 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	• Layer 2和Layer 3层集成 - 移动控制器可以基于每个VLAN切换或路由流量。 • 快速生成树 - 快速实现Layer 2收敛。 • OSPF - 与现有路由拓扑结构简单集成。

移动控制器由ArubaOS 8驱动，管理Aruba接入设备和接入软件。它们还管理软件映像、配置和用户连接状态，并执行策略。整个基础设施，无论是无线还是有线，都通过一个单一的虚拟管理平台 Aruba AirWave 控制。Aruba AirWave 可让 IT 管理跨越几代多供应商网络的应用程序和设备的用户体验。AirWave 提供影响无线和移动服务级协议（SLA）所有因素的可视性信息，可让您主动计划容量，实现客户端性能的可视化，并在您寻求服务台帮助之前解决应用程序问题。

无缝移动架构

企业用户在从一个位置移到另外一个位置的时候，日益需要网络接入服务。对于 Wi-Fi 网络而言，ArubaOS 可在用户在整个网络中移动时提供无缝连接。由于漫游切换时间仅为 2-3 毫秒，对延迟敏感的语音和视频等应用程序都能够流畅运行。

ArubaOS 集成了代理移动 IP 和代理 DHCP 功能，无需使用特殊的客户端软件，用户就能在各个子网、端口、接入点和控制器之间漫游。甚至当用户在整个网络中作业移动，并且远远偏离最初连接的接入点的时候，也能够确保无缝的性能。

VLAN 池是另一个强大的简化了网络设计的接入优势。它们并没有将 VLAN 拉到网络边缘，而是集中在在移动控制器中，并通过隧道连接到接入点。这具有几个主要优点，包括减少网络配置复杂性和缩减生成树直径。VLAN 的用户成员的负载是均衡的，当大群用户围绕网络移动时，能够维持最佳网络性能。

Aruba 的统一接入方式还可跨越私有 WAN 或使用公共网络将企业扩展到远程地点。用户无论身处何地，都能获得相同的接入体验。对于远离企业网络基础设施的用户，移动控制器作为标准 VPN 集中器运行，与其他企业用户一样，通过同样的接入和安全框架连接远程用户。

当使用 Mobility Master 时，可通过控制器集群在大型园区进行无缝漫游。当用户在大型园区移动的时候，他们的关键任务应用程序（如 Skype 商用电话）并不会遭遇任何延迟。集群中的所有控制器共同管理用户。用户可以在 10,000 个接入点之间漫游，而无需获取新的 IP 地址，进行重新验证或丢失防火墙状态信息。

整个网络中的无线安全

为了确保企业网络的安全，ArubaOS 为用户和设备执行身份验证、访问控制和加密。在 Aruba 架构中，身份验证是标准的功能，有线和无线网络都可使用。对于有线网络而言，802.IX 是标准的认证方式。对于无线网络而言，802.1X 是 WPA2 和 802.11i 协议的一个组件，而 WPA2 和 802.11i 协议被广泛认为是确保 Wi-Fi 安全的最佳协议。

ArubaOS 支持 AAA FastConnect，AAA FastConnect 可让 802.1X 身份验证交换的加密部分在移动控制器上终止，允许它在不同的身份识别存储库（包括 RADIUS 和 LDAP）之间联合。AAA FastConnect 支持 PEAP-MSCHAPv2、PEAP-GTC 和 EAP-TLS，不要求外部认证服务器兼容 802.1X。

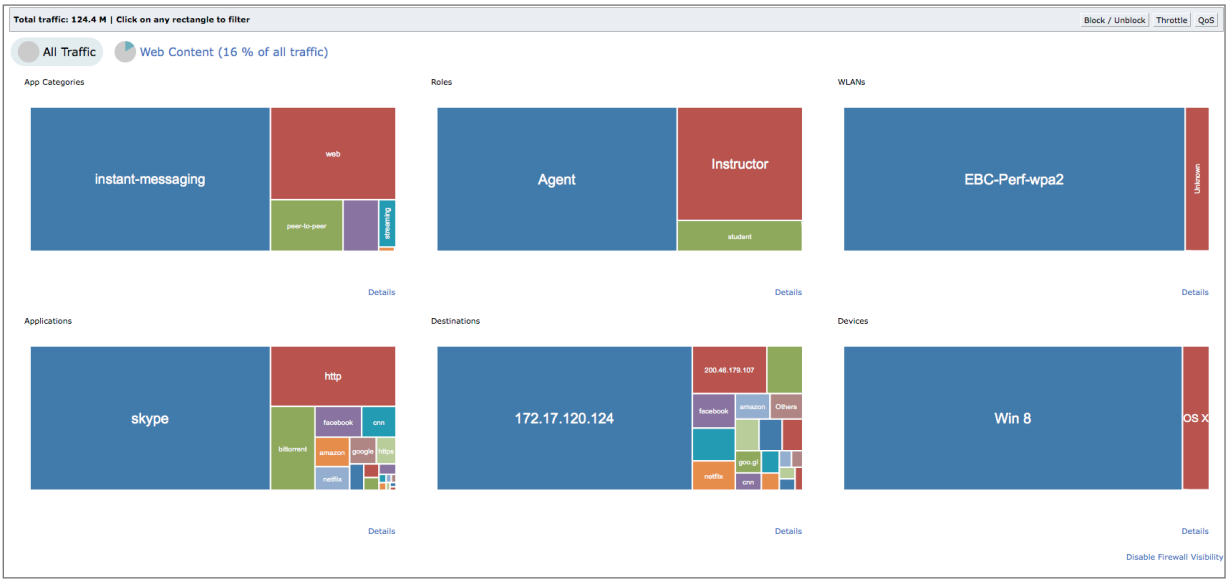
对于没有 WPA、VPN 或其他安全软件的客户端，Aruba 支持基于 Web 的强制网络门户，该网络门户提供安全的基于浏览器的身份验证。强制网络门户网站认证使用 SSL 进行加密，并且可以支持具有登录名和密码的注册用户或仅提供电子邮箱地址的访客用户。

为了防止未授权的无线设备，Aruba 的非法接入点分类算法可让系统准确地区分连接到网络且具有威胁性的接入点和邻近具有干扰性的接入点。这些接入点一旦被确认为非法的，就会通过无线和有线网络自动禁用。基本的 ArubaOS 系统能够提供非法 AP 分类和遏制功能，并不需要额外的移动控制器许可。

由于网络已经成为一个必不可少却危险的场所，我们希望能够快速确定用户正在访问的网站类型，并评估这些网站对网络及其用户造成的相对威胁。为了以最准确和最新的方式做到这一点，ArubaOS 8 针对 URL 过滤、IP 信誉和地理位置提供了可选的订阅 Web 内容策略，通过适当的策略可进行阻止和限速。目前，AOS 8 仅支持 URL 过滤和 URL 信誉。

在综合无线入侵防护（WIP）方面，移动控制器的 RFProtect 模块可抵御 ad hoc 网络、中间人攻击、拒绝服务（DoS）攻击和许多其他威胁，同时实现无线入侵特征检测功能。

ArubaOS 8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 微软供应商特有的 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可拓展认证协议 • 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 secure LDAP • RADIUS • TACACS+ • 已通过互操作性测试的认证服务器： - Microsoft Active Directory (AD) - 微软IAS和NPS RADIUS服务器 - 思科ACS、ISE服务器 - Juniper Steel Belted RADIUS、统一访问服务器 - RSA ACE/服务器 - Infoblox - Interlink RADIUS服务器 - FreeRADIUS
加密协议	• CCM P/AES • WEP 64和128位 • TKIP • SSL and TLS: - RC4 128位 - RSA 1024位 - RSA 2048位 • L2TP/IPsec (RFC 31 93) • XAUTH/IPsec • PPTP (RFC 2637)
可编程加密引擎	可以通过软件升级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
综合访客接入管理	提供安全的访客接入方案
站点到站点式VPN	在移动控制器和IPsec设备之间建立IPsec隧道。支持X.509 PKI、IKEv2、IKE PSK、IKE aggressive mode的认证。


Total traffic: 124.4 M | Click on any rectangle to filter
Block / Unblock
Throttle
QoS
All Traffic
Web Content (16 % of all traffic)
App Categories
instant-messaging
web
peer-to-peer
streaming
Details
Roles
Agent
Instructor
student
Details
WLANs
EBC-Perf-wpa2
Unknown
Details
Applications
skype
http
facebook
cnn
bittorrent
amazon
google
https
netflix
Details
Destinations
172.17.120.124
200.46.179.107
facebook
amazon
Others
goo.gl
netflix
cnn
Details
Devices
Win 8
OS X
Details
Disable Firewall Visibility

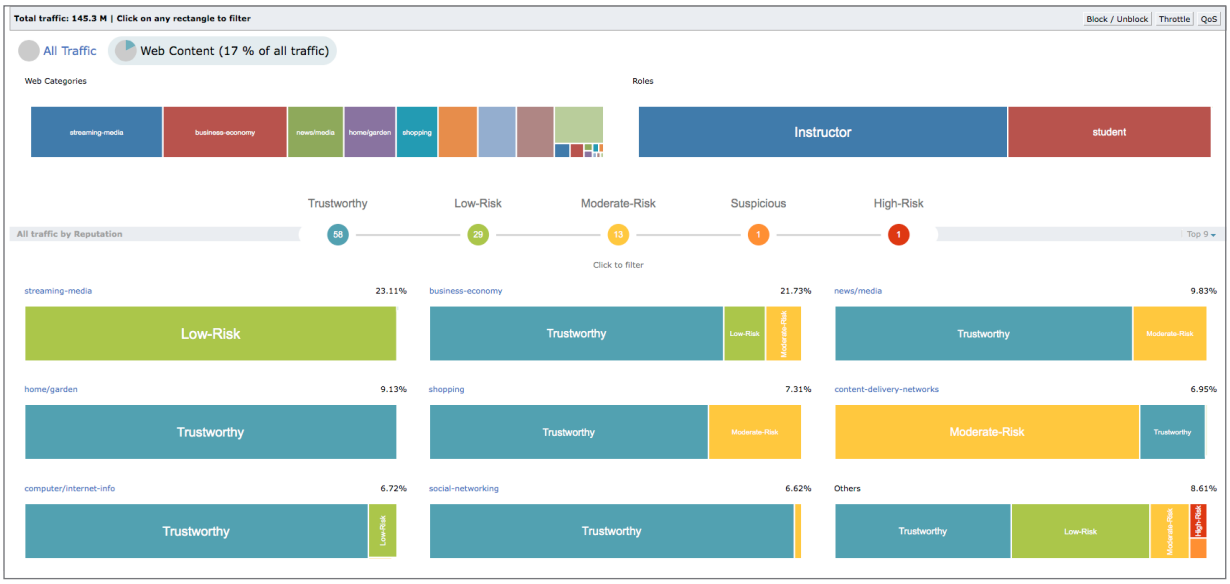

Total traffic: 145.3 M | Click on any rectangle to filter
Block / Unblock
Throttle
QoS
All Traffic
Web Content (17 % of all traffic)
Web Categories
streaming-media
business-economy
news/media
home/garden
shopping
Roles
Instructor
student
Trustworthy
Low-Risk
Moderate-Risk
Suspicious
High-Risk
All traffic by Reputation
58
29
13
1
1
Top 9
Click to filter
streaming-media 23.11%
Low-Risk
business-economy 21.73%
Trustworthy
Low-Risk
Moderate-Risk
news/media 9.83%
Trustworthy
Moderate-Risk
home/garden 9.13%
Trustworthy
shopping 7.31%
Trustworthy
Moderate-Risk
content-delivery-networks 6.95%
Moderate-Risk
Trustworthy
computer/internet-info 6.72%
Trustworthy
Low-Risk
social-networking 6.62%
Trustworthy
Others 8.61%
Trustworthy
Low-Risk
Moderate-Risk
High-Risk

图2：WebCC仪表板

应用感知可见性和基于角色的安全

ArubaOS PEF 许可证增强了以用户为中心的安全性，应用程序的可见性和控制能力。它将下一代移动防火墙的功能带到大多数用户流量首先接触的网络无线边缘。它使用深度包检测（DPI）来分类和优化流量，并通过一个简单的仪表板提供完整的可视性流量数据。

PEF 通过基于每个用户在无线边缘实施的集成的防火墙控制，添加基于身份的完整的安全功能，简化和增强了访问的安全性。这允许 ArubaOS 围绕每个用户或设备创建网络安全周边，严格控制用户或设备可能访问企业网络资源的方式。

AppRF 是 PEF 许可证的一部分，为 WLAN 带来应用感知功能和控制能力。通过提供在 Wi-Fi 网络上运行的流量类型的可视性，AppRF 可让管理员了解哪些类型的用户流量正在消耗重要的无线资源。AppRF 还提供前所未有的流量控制能力，这种灵活和强大的控制能力可让管理员在 2500 多个应用程序中选择让哪些用户的流量，以何种优先级通过无线传播。

在当前的 ArubaOS 8 系统当中，我们通过为客户添加定义定制化应用和应用程序类别的功能——AppRF 定制化来扩展 AppRF 功能。这将使客户能够针对定制化类别和与该类别相关的所有应用程序应用策略，并优先处理定制化应用程序的流量，在无需等待 Aruba 在未来发布的软件版本中进行定制的情况下，就能够获得更好的用户体验。

提升用户体验以推动统一通信和协作（UCC）

如今的员工偏好移动 UCC 所带来的自由和协作。Aruba UCC- 解决方案通过为以下应用程序自动分类和监控网络质量来提供更好的用户体验，这些应用程序包括：Apple FaceTime、阿尔卡特朗讯新办公环境（KIOE）、Microsoft Lync / Skype for Business、Cisco Jabber、Cisco Skinny 呼叫控制协议（SCCP）、Spectralink 语音优先（SVP）、SIP、H.323、Vocera 和蜂窝 Wi-Fi 呼叫。

Aruba 商用 Skype 解决方案将 SDN 与 Microsoft Skype for Business 和 AppRF 技术集成，提升服务质量（QoS）和可见性，从而实现可预测的统一的通信体验。ArubaOS 8 功能进一步加强了 UCC 解决方案，并引入了以下 UCC 特性：

- Cisco Jabber 使用未加密版本的 Cisco Jabber 客户端，提供语音、视频呼叫和桌面共享会话的服务质量和可视性信息。
- 多应用层网关（ALG）支持对同一客户端设备上同时运行的多个应用程序进行识别和确定优先级。最多支持在客户端设备上同时运行 10 个应用程序。

随着 Wi-Fi 呼叫变得越来越普遍，您需要准备和重新评估您的内部 Wi-Fi 网络设计、切换、服务质量和 RF 覆盖目标。ArubaOS 8 改善了室内 Wi-Fi 的覆盖面，并应用了服务质量，阻断或节流呼叫，并提供了客户端健康的可视性信息，为客户提供电信级语音体验。除了提高服务重量之外，Aruba 还为每个用户、每个设备和每个 carrier 提供 Wi-Fi 呼叫的可视性信息。

应用感知的可见性和基于角色的安全性	
特性	优点
全局或基于角色的策略	使用单个命令简便地控制所有用户流量， 灵活控制哪些用户可以运行什么应用程序。
2500多个应用程序	高颗粒度的可见性和控制。
19个应用类别	简化对不同类型流量的控制。
实施服务质量（QoS）标记	将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，同时防止其影响任务 关键应用程序的运行。

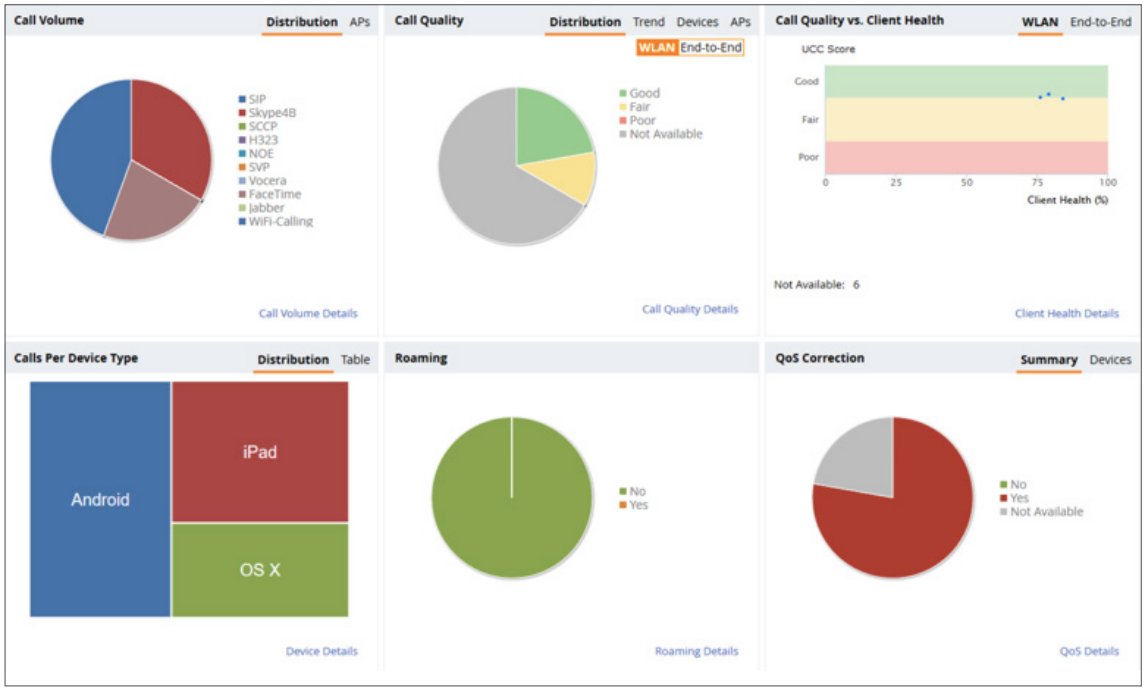


图3：AOS 8上的UCC仪表板

企业级自适应无线局域网

当今的商业世界要求移动设备和应用程序能够在任何时间在任何地方都能够访问。要提供这种可靠的访问服务需要 WLAN 根据动态移动环境，主动管理射频频谱（RF）。

自适应射频管理（ARM）技术是一种经过验证的专利技术，通过基于基础设施的自动控制来管理整个 RF 频谱。ARM 动态调整 RF 环境，以最大限度地提高 Wi-Fi 稳定性和可预测性，确保所有客户端和应用程序的最佳性能，包括对个人 Microsoft Skype for Business 语音、视频、桌面共享和聊天流程的可见性和控制。有了 ARM，无需 IT 干预，用户就能够获得始终如一的良好用户体验。

ArubaOS 8 通过 AirMatch——新的射频优化系统，进一步提升了自适应射频管理（ARM）技术。

Mobility Master 中的 AirMatch 在设计的时候将现代 RF 环境考虑在内。AirMatch 适用于高噪声，清洁或自由空间小的高密度环境。它收集过去 24 小时的 RF 统计信息，并主动优化第二天的网络。通过自动化信道，信道宽度和发射功率优化，AirMatch 可确保每个信道的均衡使用，帮助减轻干扰，并最大程度提升系统容量。

AirMatch 优势	
均衡的信道分配	能够让射频在可用信道中均匀分布，减轻干扰和最大化系统容量。
动态信道宽度调整	在20MHz、40MHz和80MHz之间动态调整，以匹配您环境的密度。
自动发射功率调整	检查整个WLAN的覆盖面，并自动调整AP的发射功率，以确保最佳的覆盖和用户体验。

提升可靠性和用户体验

移动设备、物联网和关键应用程序的海量流量正在涌向网络。用户希望他们的移动体验不会因控制器故障或在大型园区内移动而中断。ArubaOS 8 提供了一组强大的高可用性功能，旨在最大程度地减少发生控制器故障时的宕机时间。

在 Mobility Master 当中，控制器集群允许在部署 WLAN 园区的过程中集群 12 个控制器，并提供无中断的故障转移。在罕见的控制器故障事件中，用户不会意识到任何问题。语音通话、视频和数据传输都会继续进行，而不会受到明显的影响。用户会话信息在集群中的控制器之间共享，确保任何用户都不会经历单点故障。

适用于分公司和远程办公人员的远程网络

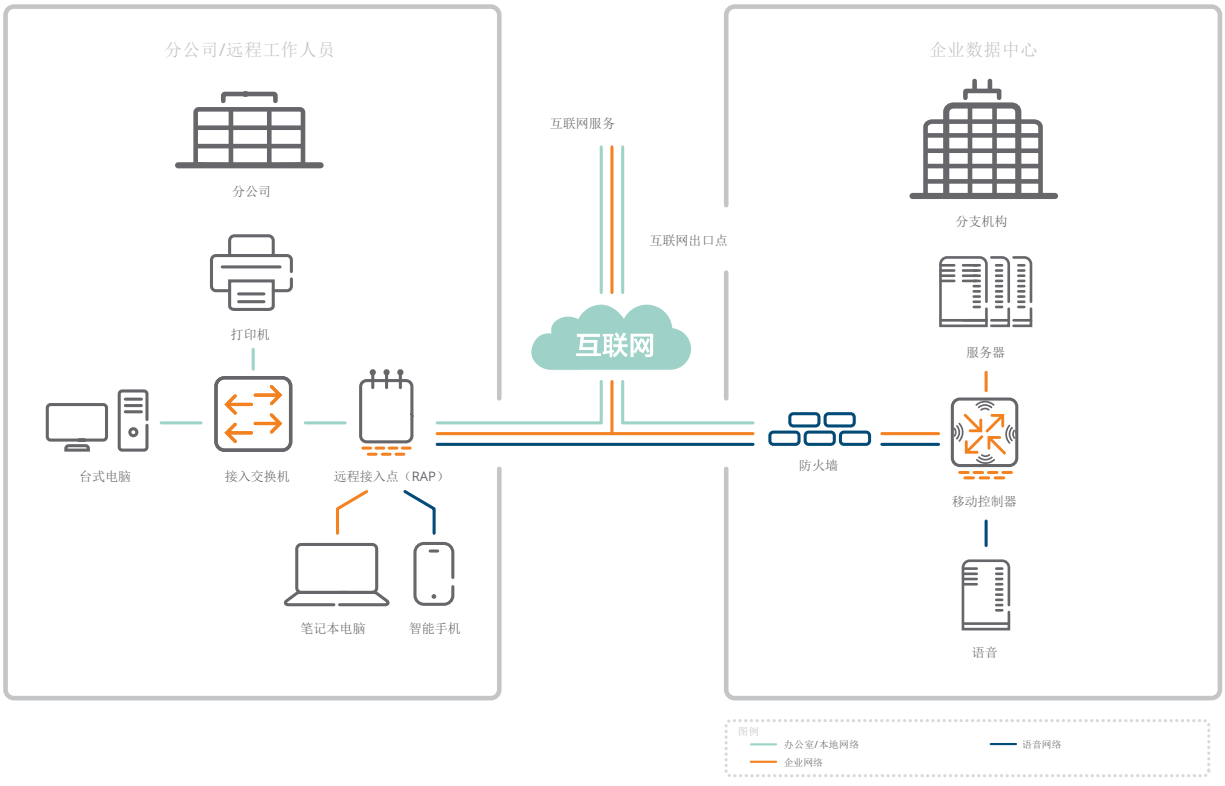
Aruba 远程和分公司网络解决方案为将公司网络扩展到分公司、小型驻外机构、门店、SOHO 和远程办公人员提供了一种简单、安全和经济的方式。ArubaOS 在移动控制器上集成了分公司专有的功能，包括园区或数据中心中的移动控制器上的 VPN 终止，以及部署为分公司网关的移动控制器上的 WAN 服务。

园区中的移动控制器处理所有复杂的配置、管理、软件更新、身份验证、入侵检测和远程站点终结的任务；而分公司中的移动控制器则处理网关任务，如基于策略的路由，压缩和本地网络功能。在较小的分支机构或作为远程使用案例的情况下，企业网络可以通过经济实惠的远程接入点（RAP）进行扩展，或通过 Aruba 虚拟内联网接入（VIA）VPN 服务投入使用。

高可用部署模式	
双活(1:1)	每个移动控制器通常提供50%的额定容量。两个移动控制器AP互为备用。 如果其中一个控制器出现故障，其AP将切换到另外一个控制器，确保所有AP的高可用性。
主用/备用(1+1)	一个移动控制器终止所有AP，而另一个控制器充当备用。 如果主控制器关闭，AP将迁移到备用控制器上。
N+1	多个主用的移动控制器采用单个备用控制器作为备份

特性	优点
AP与主用和备用移动控制器同时建立通信信道。	首次失败时，立即切换到冗余移动控制器
在切换期间，AP不会关闭和打开射频。	SSID始终可用
该解决方案适用于Layer 3网络	无需特殊的拓扑结构。
客户端状态同步	凭据被缓存，消除了重新认证的需求，避免了RADIUS服务器的超负载
N+1 超额订阅	简化配置，并减少所需的移动控制器数量。

用于远程办公人员的远程接入点	
零接触配置服务	管理员不需要任何预配置就可以部署 RAP。只需要将它交付给终端用户。
有线和无线	用户通过有线以太网、Wi-Fi或同时采用两种方式连接到RAP。
灵活的认证	可进行每个端口和每个用户的802.1 X、强制网络门户、MAC地址认证。
集中式管理	在AP上不执行本地配置 ——所有配置和管理都由移动控制器完成。
3G / 4G LTE WAN连接	RAP支持使用USB无线广域网适配器（EV-DO、HSDPA）， 用于主用或备份的互联网连接。
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 -所有用户流量由接入设备桥接到本地LAN网段。 • 策略路由 - 根据流量类型/策略，选择将用户流量转发到移动控制器或进行本地桥接（需要PEF授权）。
企业级安全	RAP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	为音频等丢包敏感应用协议定义预留带宽
本地诊断	万一遇到故障需要协助时，本地用户可以浏览预定义的URL， 访问RAP诊断的全部内容。
远程网状网入口	RAP还可以充当网状网入口，提供到下游AP的无线连接。
支持的AP	所有Aruba AP
所需的最低连接速度	每个SSID 64 kbps
加密协议（RAP到移动控制器）	AES-CBC-256（IPsec ESP内）



Aruba RAP为分公司和家庭办公室提供安全的移动连接服务。

为出差的专业人士提供简便、安全的连接服务

对于远离办公室但需要访问企业资源的用户来说，他们通常依赖于 VPN 客户端软件，该客户端软件可以连接到位于企业 DMZ 中的 VPN 集中器。

通过 Aruba，远程 VPN 用户可以像其他任何用户一样处理。他们使用的接入策略和服务定义与总部或分公司的 RAP 部署相同。移动控制器作为 VPN 集中器，消除了对并行接入基础设施的需求。

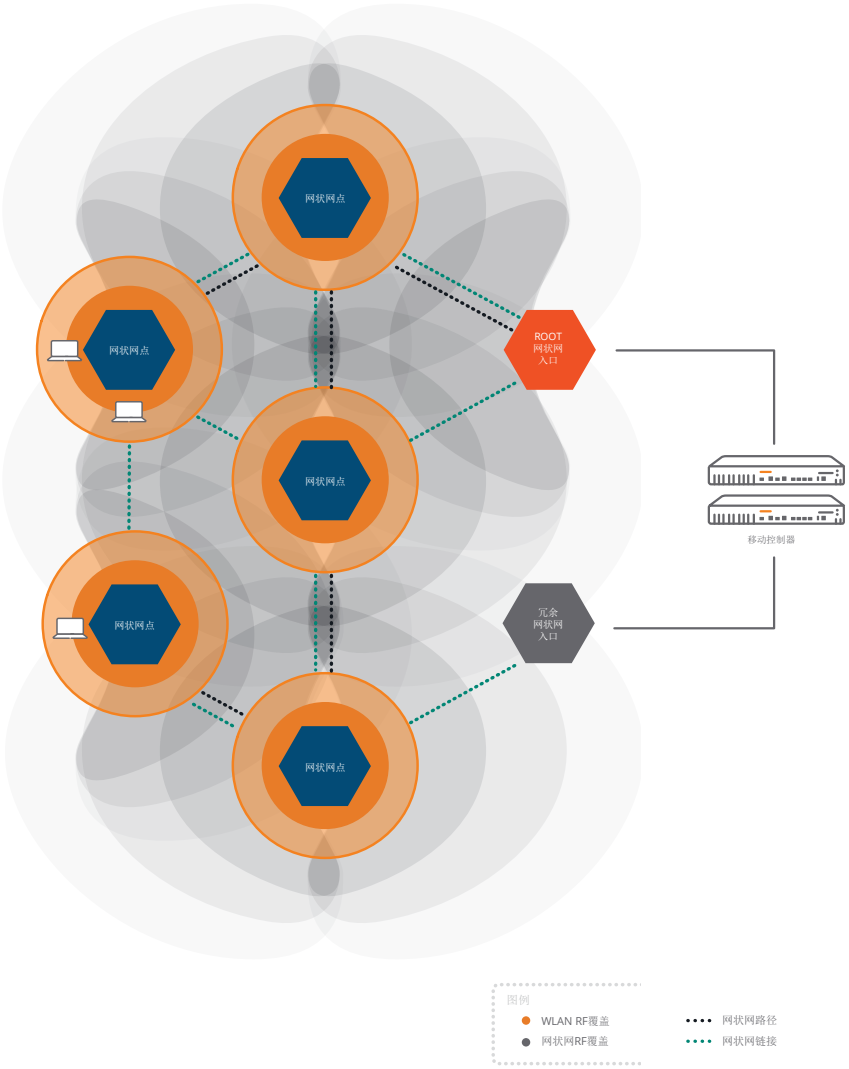
ArubaOS 与几款流行的 VPN 客户端，以及内置到主要客户端操作系统中的 VPN 客户端兼容。它还提供可选的 VIA 客户端，这些客户端可安装在 Android、iOS、Mac OS X 和 Windows 设备上。

通过将接入网络合并到一起，策略和接入配置实现了统一，提升了用户经验，减少了服务台电话，降低了 IT 成本。

针对远程接入的安全连接	
已测试客户端支持	• Windows系统上的Aruba VIA客户端 • Cisco和Nortel VPN客户端 • OpenVPN、Apple / Windows本地客户端
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

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。



ARUBA安全企业MESH解决方案

Aruba安全企业网解决方案	
广泛的应用支持	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	整合网状网网络与园区WLAN和分公司网络。 用户可在园区和分公司Wi-Fi和网状网网络间无缝漫游。
协作控制	智能RF链接管理决定最优性能路径， 并使网络能够自动组网。
自修复	富有弹性的自修复网状网能够自动克服路径拥堵或AP故障
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。
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、自动链接预算计算、 平面布置图、网络拓扑结构图
基于标准的设计	确保安全企业网状网遵循IEEE 802.11s设计原则

管理、配置和故障排除

移动控制器的配置、管理和故障排除都采用基于浏览器的 GUI 命令行界面，对任何网络管理员来说，都会觉得熟悉。

ArubaOS 还与 AirWave® 集成，AirWave® 简化了 WLAN 生命周期各阶段的管理— 从规划、布署到监控、分析和故障排除。AirWave 提供长期趋势和分析、服务台集成工具，以及各种可定制的报告。

所有接入点和移动控制器，甚至是分布在分支机构或区域办事处的接入点，都可以通过单个控制台进行集中配置和管理。为了简化常见任务的配置，直观的基于任务的向导会指导网络管理员完成该过程的每个步骤。

借助冗余数据中心的支持，可将控制器部署为 1:1 和 1:n VRRP 冗余架构。当以网络 Layer 3 拓扑结构部署时，OSPF 路由协议能实现自动路由学习和路由分配，以便于快速收敛。

无线网络管理和配置	
基于Web的配置	允许任何具有标准Web浏览器的管理员管理系统。
命令行	控制台和SSH
Syslog	支持多个服务器，多个级别和多个设施
SNMP v2c	是
SNMP v3	使用加密安全性增强标准SNMP。
移动控制器的集中配置	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 -接入设备可被配置成备份控制器的IP 地址。
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 - 提供快速的Layer 2收敛。

ArubaOS 支持 IPV6

随着可用 IPv4 地址的耗尽，企业机构正计划或已经开始在其网络中部署 IPv6。

虽然 IPv4 和 IPv6 都定义了数据如何在网络中传输，但 IPv6 比 IPv4 添加了更大的地址空间，可以支持数十亿独立 IP 地址。

随着各企业机构从 IPv4 过渡到 IPv6, 网络设备必须在 IPv4 网络中支持 IPv6 的双堆栈交互操作性，或完全部署纯粹的 IPv6 环境。

ArubaOS 加速了移动控制器和 AP 在当今 IPv6 和双堆栈环境中的部署。几乎所有功能（IPsec 除外）都可以在本地 IPv6 模式下部署。管理、监控和防火墙的每个方面都能够完全感知 IPv6。

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AP-移动控制器通信	是
USGv6认证防火墙	是

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的映射，确保延迟敏感型应用的无线服务质量。

移动控制器将 802.1p 和 IP DiffServ 标签映射到硬件队列，以提高有线侧的服务质量，并能在需要时根据指示将特定的 802.1p 和 IP DiffServ 标签应用于不同的应用当中。

添加 Aruba PEF 模块后，在 Aruba 移动控制器中将识别以下 IP 语音协议——Lync、会话发起协议（SIP）、Spectralink 语音优先级（SVP）、Alcatel Klew 办公环境（KIOE）、Vocera 和内部呼叫控制协议（SCCP）。Aruba 的应用指纹识别技术能够让移动控制器识别加密信号协议。

一旦识别了这些数据流，Aruba WLAN 就能在无线信道中优先传输它们，并触发一些基于语音的功能。

这些语音相关功能包含在通话期间推迟 ARM 扫描，以及对处于活动通话之中的客户端实施优先漫游的各个命令。对于布署大规模的 Wi-Fi 企业语音通讯来说，这些功能至关重要。

此外，ArubaOS 目前包含设备指纹识别技术，使网络管理员除了在基于应用和用户之外，还能基于设备类型分配网络策略。设备指纹识别技术对于允许哪些设备接入网络以及如何使用这些设备提供了更多的控制。

ArubaOS 可以准确识别和分类各种移动设备，如 Apple iPad、iPhone 或 iPod 以及运行 Android 或 BlackBerry 操作系统的设备。这些信息可以与 AirWave 共享，以增强网络对所有用户的可见性，无论用户的位置在哪，也无论用户使用何种移动设备。

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

认证

- Wi-Fi Alliance 认证（802.11a / b / g / n / d / h / ac、WPATM 个人、WPATM 企业、WPA2TM 个人、WPA2TM 个人、WMMTM、WMM 省 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 路由规格
- 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 IP over Ethernet
- RFC 1027 代理 ARP
- RFC 2236 IGM Pv2
- RFC 2328 0SPFv2

- RFC 2338 VRRP
- RFC 2460 Internet 协议版本 6（IPv6）
- RFC 2516 以太网点对点协议（PPPoE）
- RFC 3220 对 IPv4 的 IP 移动支持（部分支持）
- RFC 4541 IGMP 和 MLD 侦听
- IEEE 802.1 D-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

服务质量和策略

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

无线

- IEEE 802.11a / b / g / n / ac 5GHz、2.4GHz
- IEEE 802.11 d 附加监管域
- IEEE 802.lle 服务质量
- IEEE 802.11 h 欧洲 5 GHz 频谱和 TX 功率扩展
- IEEE 802.lli MAC 安全增强
- IEEE 802.11k 无线资源管理
- IEEE 802.11 ac 超高吞吐量增强
- IEEE 802.11n 高吞吐量增强
- EEE 802.11v 无线网络管理（部分支持）

管理和流量分析

- RFC 2030 SNTP，简单网络时间协议 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（SMlvl）
- RFC 1157 SNMPv1
- RFC 1212 简明 MIB 规范
- RFC 1213 基于 TCP/IP 的 Internet 网络管理的管理信息库 - MIB-II
- RFC 1215 使用 SNMP 定义 Trap 的惯例
- RFC 1286 Bridge 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 接口的演进
- RFC 2011 SNM Pv2 使用 SMlv2 的 Internet 协议的管理信息库
- RFC 2012 SNM Pv2 管理信息
- RFC 2013 SNM Pv2 管理信息
- RFC 2578 管理信息的结构版本 2（SMlv2）
- RFC 2579 SMlv2 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 SMlv2 和修订的 MIB-II
- FC 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 远程用户拨号认证（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 远程用户拨号认证（RADIUS）
- RFC 2548 Microsoft RADUIS 属性
- RFC 1350 TFTP 协议（修订版 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 Keyed-Hashing（HMAC）
- RFC 2246 TLS 协议（SSL）
- RFC 2401 Internet 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 加密算法
- RFC 2406 IP 封装安全有效载荷（ESP）
- RFC 2407 ISAKMP 解释 IP 安全域
- RFC 2408 Internet 安全联盟和密钥管理协议（ISAKM P）
- RFC 2409 互联网密钥交换（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（M PPE）
- RFC 3162 Radius over IPv6
- 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、5257 可扩展认证协议（EAP）
- RFC 3947 IKE 中 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 互联网密钥交换（IKE）v2
- RFC 4793 EAP-POTP
- RFC 5246 TLS1.2
- RFC 5247 EAP 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 - RADIUS 的 TLS 加密

a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | 电话 : 1.408.227.4500 | 传真 : 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com