

白皮书



使用个人iPad工作

2011年3月

ARUBA[®]
networks

目录

带着自己的iPad去上班

1	介绍	2
2	IT部门面临的挑战	2
3	设备识别	3
4	设备注册	4
5	设备身份验证和授权	5
6	设备可视性	6
7	总结	7
8	结论	7
9	参考资料	8

1 介绍

最近几个月，CIO们发现自己的处境很艰难。从高层主管到新招聘的年轻员工都在兴致勃勃地谈论如何在工作之外的日常生活中提高办事效率。社交网络、高速Wi-Fi接入以及功能强大的新型智能手机允许他们通过各种方式进行沟通、协作，这一切在几年前是难以想象的。

技术已经有了长足发展，但尚未在企业中得到应用。CIO们一直在问，如果允许在办公室使用这些设备，必须实施什么样的安全策略方可保护网络服务和公司数据。这是一大挑战。但如果能很好地应对，企业将能大大提升工作效率。

引领此次个人移动设备革命的先驱就是Apple iPhone和Apple iPad。Apple iPad激发了员工的想象力，他们可以在家中和旅途中享受个性体验；随着新功能和新服务的涌现，iPad也可以用于办公。

将Apple iOS设备带到办公室的员工发现，通过Wi-Fi接入企业无线网(WLAN)是最理想的选择；这样可以方便地获得更高的连接速度和更好的可靠性 – 尤其是在手机信号不好的区域，更是如此。而且，如果需要访问企业资源和数据，也必须接入企业WLAN。但IT部门很自然地会担心这些不受管理的新型移动设备可能会存在安全隐患。

例如，多数IT部门都在WLAN网络中实施了基于企业RADIUS服务器的WPA2企业身份验证，这种方式非常安全。但用户发现，他们在PC机上输入的用户ID/密码组合同样能使他们的Apple iOS设备通过身份验证，接入企业WLAN。尽管对员工很有用，这对于IT人员却很棘手，因为员工拥有的设备可能有安全漏洞，而IT部门提供的、配置锁定的PC机则不存在这些问题。

急待解决的问题是，如何识别Smith先生使用的是IT部门提供的PC机而非自己的个人设备，以及如何对员工拥有的、而不受IT部门控制或配置的个人设备实施网络策略。除此之外，重要的是如何自动完成这一过程以防止帮助台工作人员应接不暇，同时提供在企业网络上管理和监控这些个人设备所需的工具。

Aruba新开发的移动设备接入控制(MDAC)解决方案就实现了这些目标。MDAC为IT人员接纳这些重要的新兴办公工具铺平了道路。MDAC解决方案包括三个主要组件：

- Aruba Device Fingerprinting – 运行于所有Aruba移动控制器的ArubaOS的一部分 – 可准确识别设备类型，允许精确控制和管理企业WLAN上的移动设备。
- Aruba Amigopod - 可自动完成设备的配置与注册,设置Apple iOS设备完成与设备相关的、而不是与用户相关的身份验证。
- Aruba AirWave - 支持设备特定的监控、故障排除和报告功能。

2 IT部门面临的挑战

接入企业网络的员工自有设备对IT部门提出了许多挑战。

首先要了解用户行为及用户期望。尽管这些移动设备都面向普通消费者提供了各种便捷功能，但许多用户并不擅长使用高技术产品，他们需要IT人员帮助自己连接到企业网络，连接建立后还可能

能及其他应用问题。由于帮助台工作人员不了解用户自有设备的产地和配置，他们很难提供支持。

另一方面，有些员工已经发现他们可以使用自己的认证信息连接到WLAN。在今天的大多数网络中，IT部门无法监测到成功连接网络的用户所使用的设备 – 不能辨别他们是通过个人的iPad完成身份验证的，还是通过IT部门提供的PC机完成身份验证的。因此，无法恰当地管理这些用户。正如我们所知，不受管理的移动设备可能导致企业数据和服务遭到入侵。

其次，为员工自有的移动设备提供保护不同于为IT部门提供的标准PC机采用的安全措施。除非经过特殊配置，否则移动设备是无法监控的。访问这些设备并不要求密码；而当这些员工的移动设备检测到企业WLAN并成功登录后，就可以在移动设备上保存认证信息以完成后续的自动身份验证。

这会带来很多难题 – 即便IT人员可以跟踪到这些设备连接，也无法保证企业网络中Smith先生的iPad确实在Smith的手中：有可能在几小时前就丢失或被盗了。允许配置iPad获得企业防火墙内的访问权限增加了企业服务器被人渗透的风险：入侵者可能会把Smith先生忘记带走的设备带入办公区域，通过WLAN访问敏感企业数据。

第三，由于无法识别可疑的设备，网络管理成本可能会高得无法承受。如果IT策略允许员工自有设备接入企业WLAN，IT管理员必须有办法识别并监控这些设备并能在员工遇到连接问题时有效地排除故障。最后还有一个潜在的问题：员工使用LAN和WLAN上的资源可能会影响正常的企业流量。例如，使用视频电话（我们在随附的文章中讨论了合理使用FaceTime的问题）以及流媒体电视服务。个人设备用于办公目的之外的活动可能会在企业网络上产生大量流量，进而影响企业服务。此外，网络中的每个新的移动设备都需要有自己的IP地址而且可能会占用带宽资源，进一步减少可用的资源。

Aruba的MDAC解决方案就解决了上述问题，允许IT部门分阶段地建立安全的管理和防护措施，方便员工把自己的移动设备带到办公室。

3 设备识别

移动设备网络上的接入问题实质上是控制问题：监控并限制员工自有设备的行为。在实现控制之前，首先要完成一项最重要的任务 – 即把这些员工自有移动设备与IT提供的PC机区别开来。

大多数企业都会在WLAN上配置一个访客专用SSID和一个面向员工的企业SSID。前者通过强制网络门户完成身份验证 – 点击接受使用条款协议或者使用附属服务器发布的当日有效密码。它会将所有流量转向位于防火墙之外的Internet。我们可以请带着自己的设备上班的员工以访客身份连接网络，但这种方式很繁琐，每天都要重新通过身份验证，接入企业服务时还必需使用VPN或类似的安全身份验证手段。

最好能允许这些设备通过身份验证使用防火墙内的员工SSID，这样也会提高工作效率。如上所述，大多数基于用户的身份验证方法确实无法阻止员工使用自己的用户ID和密码配置个人设备，然后接入网络。在这种情况下，公司有关此类设备应使用访客SSID的规定很难得到贯彻。

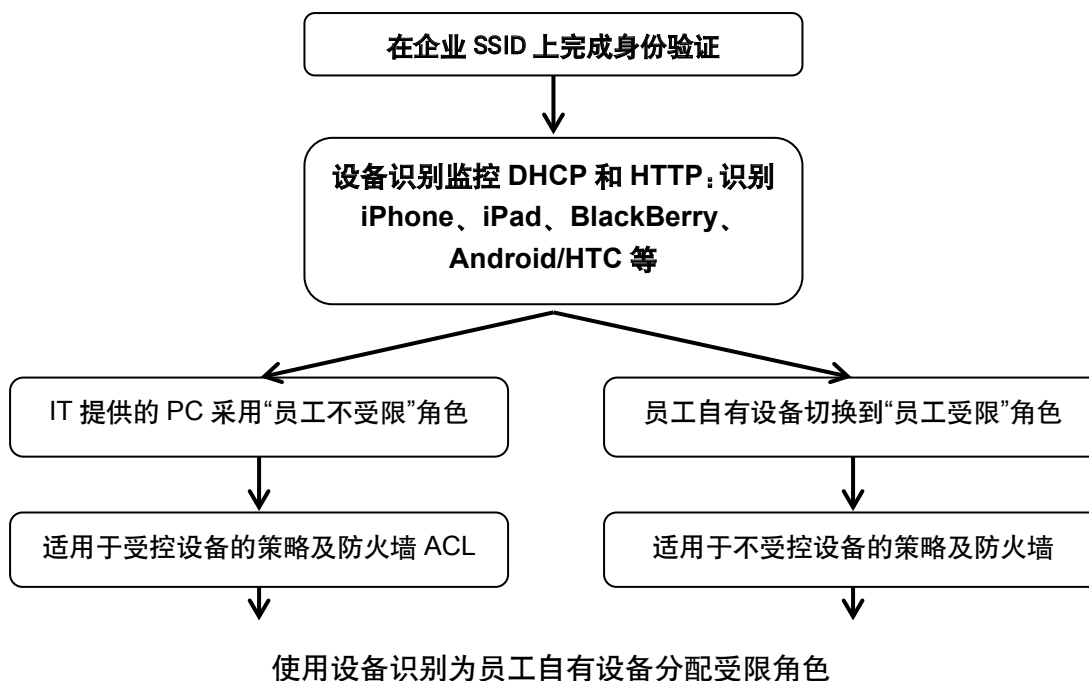
Aruba解决了这个问题，允许使用标准方法进行身份验证，但此后可立即识别出客户端是一台个人移动设备并对其应用不同的策略。ArubaOS中的设备识别技术可以在移动设备通过身份验证的同时识别出他

们的特征并相应执行DHCP和HTTP操作。这样，便可对设备进行识别和分类。因此，Aruba网络能够分辨使用个人iPAD的Smith和使用IT提供的PC机的Smith。

借助这种识别功能，IT管理员可以看到网络中所有用户的自有设备以及他们的类型和所有者。

设备识别技术可以识别iPhone、iPad和iPod设备以及Windows、BlackBerry、Android和其他用于笔记本电脑、智能手机和平板电脑的操作系统。

设备被识别之后，Aruba基于身份的移动架构允许制定各种灵活策略，以限制它的活动范围及行为方式。分配的角色将调用一系列访问控制列表(ACL)及其他策略执行机制。通过定制这些机制，网络设计人员可以限制对不同企业资源的访问权限 – 按照IP地址或子网、协议、时间段及其他参数。



例如，IT策略可能允许Smith在使用企业PC机时接入电子邮件、内部Web资源、人力资源和财务服务器。但在使用iPad时，可能会限制他访问人力资源或财务数据。与此同时，还能允许、甚至鼓励Smith使用自己的iPhone拨打视频电话：这种角色可调用Aruba的应用识别，为Apple FaceTime流量提供高优先级的服务质量(QoS)，而不会让它与低优先级的Web和电子邮件流量抢夺资源。

4 设备注册

尽管可以发布针对WLAN连接和身份验证的指导原则及相关说明，允许员工自行配置自己的设备，但是多数IT部门还是希望采用控制手段更强的方式。Aruba的架构提供了许多备选方案。为了简单起见，本文只介绍应用最为广泛的方案。

首先，员工以访客身份连接到WLAN。现有企业强制门户网站提供一个选项，指向特殊的“员工自有设备注册”网页。该网页由Aruba的Amigopod设备管理，要求提供常规的登录凭据，以根据IT的现有身份验证基础架构确定雇员身份。

现在，Amigopod设备将通过用户选择或HTTP检测的方式确定设备类型，为该用户的设备准备一个专门的可以自动安装的配置文件，并通过IP连接、电子邮件或SMS将其发送到用户设备中。

设备收到配置文件后，将会显示一个按钮，用户可以单击执行。现在，设备将设置以下配置选项：

- 安装设备特定的X.509证书（由Amigopod颁发），建立设备的唯一身份。
- 配置企业WLAN的SSID以及所需的Wi-Fi选项。
- 可以安装设备配置文件，例如：要求定期输入设备的屏幕解锁密码。用户不能绕开这些设置。

该注册流程可达到几个重要目的。首先，用户使用简便 – 单击即可完成安装，无需手动输入Wi-Fi网络参数，降低出错的风险、提高用户满意度、减少帮助台呼叫。其次，可在其中结合双向身份验证。特别重要的是，网络可以通过输入的用户现有认证信息来确认用户身份，而且用户也可确认该网络确实是企业网络，而非冒名顶替的恶意网络。

但最重要的是，IT人员无需花费大量时间置备用户自有设备以通过基于证书的身份验证。用户可以在企业网络中安全地自行完成注册。在为IT管理员提供的各种选项中，Amigopod可以配置为只向预先经过审批的用户或设备或者只在特定时间段内颁布凭据，这对临时办公人员或合同制员工很有用。

自助安装完成之后，设备便就有了唯一的、可验证的证书，以证明自己的身份。此后每次通过WLAN身份验证时，该证书都能用来标识设备身份。可将其作为一种主要手段，允许设备使用EAP-TLS身份验证协议，在维护整体安全性的同时避免重复输入用户名和密码。该证书支持跟踪和审计日志，以记录设备在网络中的活动；如果移动设备丢失或被盗，可调用这些记录，禁止该设备接入企业网络。

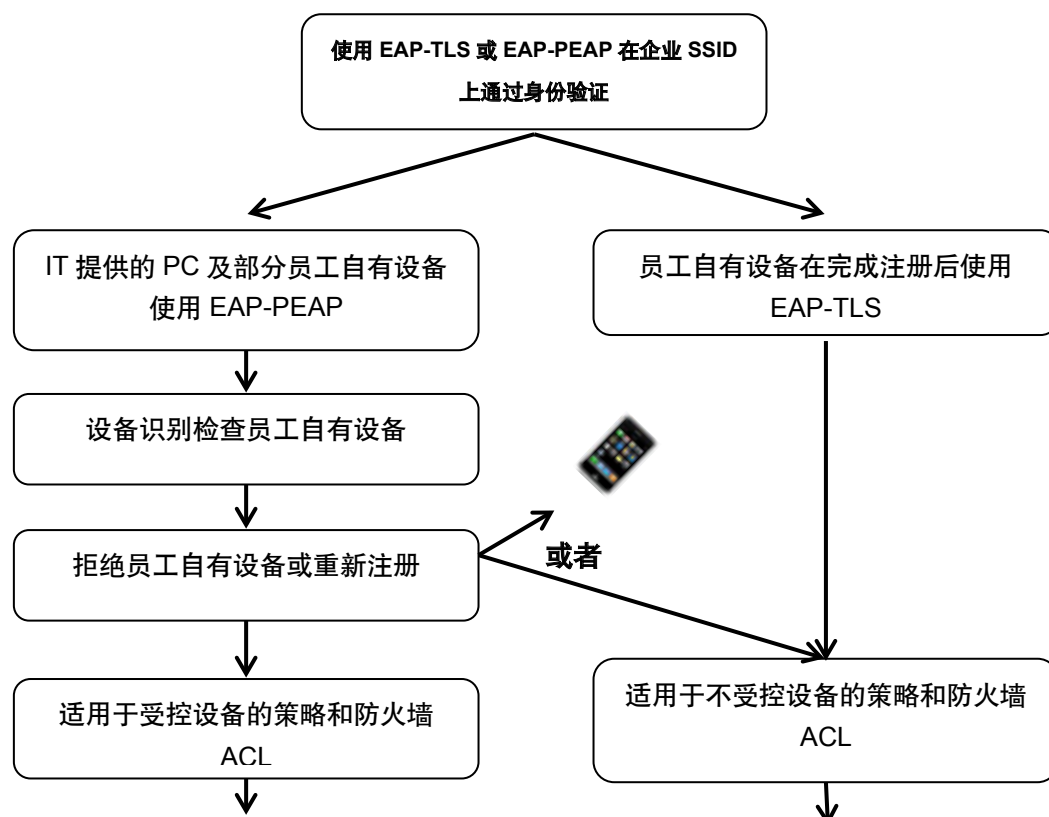
5 设备身份验证和授权

上一节介绍了如何使用Aruba设备识别完成身份验证，以区分员工自有设备和IT提供的PC机。此项技术允许为员工的移动设备分配特定角色，限制其只能使用IT部门允许的功能和服务、遵循最低权限的安全原则。

但是，如果有Amigopod颁布的证书，整个过程可以变得更加简单。具有证书的设备能够使用EAP-TLS在WLAN上通过身份验证，而IT提供的PC机则使用EAP-PEAP-MSCHAPv2。因此，使用EAP-TLS的设备即为员工自有设备，可为其分配一个专门针对此类设备的适当角色。在这种情况下，企业员工WLAN SSID会配置为同时接受PEAP和EAP-TLS身份验证，而设备也将在身份验证过程中协商协议，自动区分两类不同的设备。

如果员工选择配置iPad使用PEAP，则有可能使用个人凭据通过身份验证，进而获得错误的角色 – 就如iPhone是IT提供的PC机一样。Aruba设备识别恰恰为这种情况提供了一个有用的备份方案。此项技术可识别试图使用PEAP通过身份验证的员工自有设备，可以自动调整它们的角色或者拒绝通过身份验证，强制要求员工按照公司策略注册自己的设备。

一旦iPad被WLAN识别并适当分类，IT管理便可以看到它们。可以显示网络中所有的员工自有设备，列出它们的访问控制，最重要的是能跟踪他们的使用记录。



使用 Amigopod 接入和设备识别功能为员工自由设备分配受限用户

Aruba AirWave管理系统中的审计跟踪记录能够显示每个客户端的移动及使用情况，而移动控制器中的历史记录则可以按协议或目的地地址显示接入服务器的时间。AirWave具有许多选项，可以按设备类别和身份验证类型显示带宽使用情况，允许IT部门监控iPAD是否在与传统WLAN流量争抢资源、了解趋势、采取相应措施，满足不断增长的带宽需求。

6 设备可视性

Aruba架构允许将设备列入黑名单，在设备丢失或被盗后立即阻止其在WLAN上通过身份验证。如果是在建筑内失窃的，AirWave能够标识上次发现设备时的位置和时间，准确定位它最后离开的那道门。AirWave还提供了被盗设备告警功能 – 如果标为被盗的设备在网络中重新出现，它可以发现电子邮件或发出警报。

WLAN作为一种网络平台提供了设备身份识别、访问控制、身份验证故障排除工具、设备审计跟踪以及黑名单功能，有时也能通过多种方式结合使用其他移动设备管理服务。Apple公司提供了许多工具，以帮助管理员工自有的iPhone。例如，远程擦除功能可在iPhone丢失或被盗后通过远程控制删除所有用户数据。

尽管可能很有用，但这些功能很具有侵入性而且设备是归用户所有的，所以只有在告知用户他们的个人设备将被更改并受IT部门控制的情况下才能加以实施：如果要实施这种更具侵入性的移动设备管理模式，可能需要充分考虑这些问题，适当修改员工入职和离职程序。

7 总结

下表列出了上文提出的问题以及如何在企业网络中解决这些问题。

功能	要求	建议的功能
注册与初始配置	安全的注册与一键式配置功能。	Amigopod注册可采用强制门户网站、证书安装以及发送到设备的等形式完成。
管理员可视性	允许IT部门查看并监控WLAN上的所有员工自有设备。	Aruba设备识别可按；类别、名称和用户列出设备。AirWave可显示审计跟踪记录。
故障排除工具	为帮助台提供必要的工具，帮助员工解决iPhone使用问题。	Airwavew采用设备识别技术允许IT人员监控并处理所有WLAN身份验证和连接的问题。
区分员工自有设备、IT部门提供的设备并制定相应网络策略	限制或增强为员工设备提供服务的水平。	Aruba以用户/设备为中心的角色与设备识别技术相结合，允许针对员工的iPad、而非PC机执行特定策略。
防止非法接入企业网络	iPhone是种很“活跃”的设备，可自动完成WLAN身份验证；如果使用不当，可能会引发网络渗透风险。	对员工自有设备实施比IT部门控制的设备更加严格的访问控制。Aruba的设备黑名单功能可在设备丢失后拒绝其接入WLAN。
在丢失或被盗的情况下防止设备和网络数据泄漏	即便拿到丢失或被盗的设备，读取其中的数据。	审计跟踪可显示企业网络上的历史活动记录。可利用Apple的远程擦除功能保护设备。AirWave被盗设备告警功能可在丢失的iPhone再次出现时通过电子邮件发出警报。
确保使用WLAN的个人应用不会影响高优先级的企业流量	管理视频等高带宽流量，防止其干扰其它高优先级企业服务，也可以为FaceTime分配高优先级，将其用作办公工具。	Aruba以用户/设备为中心的角色允许灵活地管理视频流量，包括重新分配QoS优先级、控制带宽使用等。AirWave可按设备或身份验证类型显示带宽使用情况。

8 结论

许多用户都要求CIO们在WLAN上支持个人移动设备。就在一年前，某些分析人士还建议IT部门为移动办公人员统一配备标准的、采用企业配置的智能手机。现在，IT部门再也无法抵制带着个人移动设备来上班的潮流了。

在很多方面，CIO对这种趋势的担心是有道理的。员工自有设备引发了新的安全风险，可能会增加网络管理和帮助台的工作负担 – 虽然很难量化，但工作量肯定会大大增加。而且，现有的网络厂商也无法提供完成这些工作所需的功能和工具。

本文探讨了要求在办公室使用个人移动设备的员工为IT部门带来的问题。与大部分IT服务一样，我们需要一种分层的方法来管理、控制这些设备。Aruba已经开发出了设备识别和Amigopod注册技术，可结合我们以用户/设备为中心的移动架构，为企业提供必要的功能，以安全、可靠地支持Apple iOS系统。

Aruba相信，Amigopod注册、Aruba设备识别以及我们提供的其他功能适用于大多数企业，无需过多的侵入性操作即可管理Apple iOS设备并保护企业网络。但有些企业可能需要一项补充性的移动设备管理(MDM)功能，而Aruba的产品和技术可很好地融合这些厂商的设备。

随着面向普通消费者的技术逐步渗入企业网络，iPhone和iPad等员工自有设备带来的工作效率的提升必将使这些设备广受欢迎。例如，利用视频协作进行企业内部通讯就是一个新的趋势。

如能建立稳固的基础架构、全面管理和控制iPhone等员工自有移动设备，企业必将能够很好地利用消费市场 and 社交网络来提高生产力和提升服务质量。

9 参考资料

适用于Windows的Apple iPhone配置工具：<http://support.apple.com/kb/DL926>

Apple ‘iPhone in Business’ 安全性概述：http://images.apple.com/iphone/business/docs/iPhone_Security.pdf

关于Aruba Networks

Aruba作为全球分布式企业网络的领导者，屡获殊荣的校园、分支机构/远程工作人员产品组合与移动解决方案使用户无论使用何种设备，身处何地或何种网络，都能简化运营并安全访问所有公司应用和服务，显著提高了效率并降低了资本和运营成本。

Aruba公司在纳斯达克上市，股票同时作为罗素2000指数（Russell 2000® Index）成份股。公司总部设在加州森尼维尔，业务遍及美洲、欧洲、中东、亚太地区。如需了解详情，请访问Aruba公司网站<http://www.arubanetworks.com.cn>



北京

Tel: 010-65805588

Fax: 010-65805566

北京市朝阳区朝外大街丰联广场A座2101 (100020)

上海

Tel: 021-61323845

Fax: 021-63351336

上海黄浦区延安东路222号外滩中心18楼 (200002)

广州

Tel: 020-28858517

Fax: 020-28858222

广州市天河区林合西路161号中泰国际广场23楼 (510620)

研发及服务中心

Tel: 010- 58851177

Fax: 010- 58858479

北京市海淀区上地东路1号院鹏寰国际大厦10层 (100020)

E-mail: Chinamktg@arubanetworks.com

Website: www.arubanetworks.com.cn