思科 Aironet 无线安全常见问题解答

文档编号：68583

简介
一般常见问题
排错和设计常见问题
相关信息

简介

本文档所提供的信息是关于思科 Aironet 无线安全最常见问题(FAQ)。

一般常见问题

问：无线安全需要什么？

答：在有线网络中，数据仍然在连接终端设备电缆中传递。但是，无线网络传输和接收数据是通过在空气中广播的射频信号。由于无线局域网使用的广播性质，存在黑客或入侵者可以访问或损坏数据的威胁。为了缓解这一问题，所有的无线局域网需要增加：

1. 用户身份验证，防止未经授权访问网络资源。
2. 数据私密以保护数据完整性和数据传输私密性。

问：无线局域网定义的 802.11 标准有哪些不同的验证方法?

答：802.11 标准定义了两种验证无线局域网客户端的机制：

1. 开放式认证
2. 共享密钥认证

还有其他两个常用的机制：

1. 基于 SSID 认证
2. MAC 地址认证

问：什么是开放验证？

答：开放认证基本上是一个空认证认证算法，这意味着对于用户或机器不需要验证。开放验证允许任何设备向接入点(AP)发送认证要求。开放验证中客户端使用明文传输关联 AP。如果没有加密功能，任何知道无线局域网 SSID 的设备都可以进入该网络。如果在 AP 上启用了有线对等加密协议(WEP)，WEP 密钥则成为一种访问控制的手段。没有正确的 WEP 密钥的设备即使认证成功也不能通过 AP 传输数据，同时这样的设备也不能解密由 AP 发出的数据。

问：开放认证中客户端关联 AP 需要什么步骤？

1. 客户端发送一个探测请求 。
2. 周边的 AP 回复探测响应。
3. 客户端评估 AP 的响应并选择信号最好的 AP。
4. 客户端发送一个验证请求给选定的 AP。
5. 该 AP 确认该认证并注册客户端。
6. 客户端然后发送一个关联请求给 AP。
7. AP 确认该关联并注册客户端。

问：开放认证的优点和缺点是什么？

答：以下是开放认证的优点和缺点：

优点：开放认证是一个基本的验证机制，你可以使用不支持复杂的认证算法无线设备。802.11 规范中认证的是面向连接的。对于需要验证允许设备得以快速进入网络的设计，在这种情况下，您可以使用开放式身份验证。

缺点：开放认证没办法检验是否客户端是一个有效的客户端，而不是黑客客户端。如果你使用不带 WEP 加密的开放验证，任何知道无线局域网 SSID 的用户都可以访问网络。

问：什么是共享密钥认证?

答：共享密钥认证与开放验证类似而有一个主要的区别。当你使用带 WEP 加密密钥的开放认证时，WEP 密钥是用来加密和解密数据，但在认证的步骤中却不使用。在共享密钥认证中，WEP 加密被用于验证。和开放验证类似，共享密钥认证需要客户端和 AP 具有相同的 WEP 密钥。AP 使用共享密钥认证发出一个挑战文本包到客户端，客户端使用本地配置的 WEP 密钥来加密挑战文本并且回复随后而来的身份验证请求。如果 AP 可以解密认证要求，并恢复原始的挑战文本，AP 将回复一个准许访问的认证响应给该客户端。

问：共享密钥认证中客户端关联到 AP 需要什么步骤？

1. 客户端发送一个探测请求 。
2. 周边的 AP 回复探测响应。
3. 客户端评估 AP 的响应并选择信号最好的 AP。
4. 客户端发送一个验证请求给选定的 AP。
5. 该 AP 发送一个包含未加密挑战文本的认证响应。
6. 客户端利用 WEP 密钥加密挑战文本，并将加密后的文件回复给该 AP。
7. AP 比较未加密的挑战文本和加密的挑战文本。如果验证可以解密和恢复原始的挑战文本，则该认证是成功的。

共享密钥认证在客户端关联过程中使用 WEP 加密。

问：共享密钥认证的优点和缺点是什么？

答：在共享密钥认证中，客户端和 AP 的交换挑战文本(明文)并且加密的该挑战文本。因此，这种认证方式易受到中间人攻击。黑客可以收到未加密的挑战文本和已加密的挑战文本，并从这些信息中提取 WEP 密钥(共享密钥)。当黑客知道 WEP 密钥时，整个认证机制将受到威害并且黑客可以自由访问该 WLAN 网络。这是共享密钥认证的主要缺点。

问：什么是 MAC 地址认证？

答：虽然 802.11 标准没有指定 MAC 地址认证，但无线局域网普遍使用该认证技术。因此，大多数的无线设备厂商，包括思科，均支持 MAC 地址验证。

在 MAC 地址认证中，客户端的认证是基于 MAC 地址的，客户端的 MAC 地址的核实存储在 AP 本地或外部认证服务器上的 MAC 地址列表。相对于 802.11 规定的开放和共享密钥认证，MAC 认证是一个更强有力的安全机制。这种形式的认证，进一步降低的未经授权的设备接入网络的可能性。

问：为什么在 Cisco IOS 软件版本 12.3 (8) JA2 上 MAC 认证不能和 Wi - Fi 保护访问(WPA)同时运行？

答：MAC 认证的唯一安全级别是客户端的 MAC 地址与所允许的 MAC 地址列表比对。这被认为是非常薄弱的。在以前的 Cisco IOS 软件版本，你可以同时配置 MAC 认证和 WPA 来加密信息，但是，由于 WPA 自己包括 MAC 地址检测，思科公司决定在后续 Cisco IOS 软件版本不再允许这种类型的配置 。

问：我能将 SSID 作为一种无线设备认证方式吗？

答：服务集标识符(SSID)是一个唯一的，区分大小写，数字值化的能够被无线局域网作为一个网络的名称来使用的标记。SSID 是允许逻辑划分无线局域网的一种机制， SSID 没有提供任何数据隐私功能，而且 SSID 也不对 AP 提供真正验证客户端的功能。SSID 的值在如 Beacons/信标, Probe Requests/探测请求, Probe responses/探测响应以及其他类似的数据帧中是采用明文方式广播的，一个窃听者可以很容易的利用一个 802.11 无线局域网数据包分析器来测定 SSID，例如 Sniffer Pro。思科并不建议你使用的 SSID 作为一种保证你的 WLAN 网络的方法。

问：如果我禁用 SSID 的广播，我可以在 WLAN 网络中实现更高的安全性吗？

答：当你禁用 SSID 广播，在 Beacon 信息中将不会发 SSID。然而，其他类型的数据帧，如 Probe Requests 和 Probe Responses 仍以明文方式包含 SSID。所以，如果你禁用 SSID 广播并没有达到增强无线安全的目的。SSID 不是作为一个安全机制设计和使用的。此外，如果你禁用 SSID 广播，你可以在混合客户端的部署上遇到与 Wi - Fi 互操作性的问题。因此，思科并不建议您使用的 SSID 作为安全模式。

问：802.11 安全已经发现的漏洞是什么？

答：802.11 安全的主要弱点可归纳如下：

- 脆弱的验证方式：仅验证客户端设备，而不是用户。
- 脆弱数据加密：有线等效保密(WEP)作为加密数据的手册已经被证明是无效的。
- 无信息完整性检测：完整性校验值(ICV)作为确保数据完整性的手段已经被证明是无效的

问：在 WLAN 中，802.1x 认证的扮演什么角色？

答：为了解决 802.11 标准定义的原始认证方式所带来的缺陷和安全漏洞，在 802.11 MAC 层的安全性增强草案中包含了 802.1X 认证框架，在 IEEE 802.11 任务组 i(TGi)目前正在开发这些增强功能。802.1X 框架规定了在链路层进行可扩展的认证，而通常这只有在更高层次才使用。

问：802.1X 柜架定义了哪三个项目？

答：在 WLAN 网络中，802.1x 协议的框架需要以下三个逻辑实体来验证设备。

1. 请求端—该请求端驻留在在无线局域网客户端，也称为 EAP 客户端。

2. 认证端—认证端驻留在 AP。
3. 认证服务器—认证服务器驻留在 RADIUS 服务器。

问：当我使用 802.1x 认证框架时无线客户端是如何进行认证的？

答：当无线客户端(EAP 客户端)激活后，无线客户端会与 AP 关联(认证端)。客户端然后发送认证证书给 AP，AP 反过来将该信息转发给认证服务器。认证服务器将证书与用户数据库比对验证，以确定用户是否能够访问该网络。认证服务器通常是一个 RADIUS 或其他 AAA 服务器。

问：在 802.1x 认证框架中，我可以使用的 EAP 变种是什么？

答：802.1x 认证框架能够使用以下任意 EAP 变种。

1. EAP-TLS – 基于传输层安全的可扩展认证协议
2. EAP-FAST - 基于隧道的灵活认证协议
3. EAP-SIM – 基于客户识别模块的可扩展认证协议
4. Cisco LEAP – 思科轻量级可扩展认证协议
5. EAP-PEAP – 受保护的扩展认证协议
6. EAP-MD5 – 基于 MD5 的扩展认证协议
7. EAP-OTP – 基于一次性密码扩展认证协议
8. EAP-TTLS – 基于隧道传输层安的扩展认证协议

问：我该如何从不同的 EAP 变种选择一个有效的 802.1x EAP 模式？

答：最重要的因素，你必须考虑是否 EAP 模式是否与现有网络兼容。此外，思科建议你选择一种支持相互验证的模式。

问：思科轻量级可扩展认证协议(Cisco LEAP)是什么？

答：轻量级可扩展认证协议(LEAP)是思科专有的认证模式。思科轻量级可扩展认证协议是无线局域网(WLAN)内 802.1X 的一种认证类型。思科轻量级可扩展认证协议支持在客户端和 RADIUS 服务器之间通过登录密码作为共享密钥的强相互验证方式。思科轻量级可扩展认证协议提供每

个用户，每个会话的动态密钥。思科轻量级可扩展认证协议是部署 802.1x 协议最简单的一种模式，仅只需要一个 RADIUS 服务器。更多思科轻量级可扩展认证协议相关信息请参见 Cisco LEAP

问：基于隧道的灵活认证协议(EAP–FAST)是如何工作的?

答：基于隧道的灵活认证协议(EAP–FAST)采用对称密钥算法实现隧道认证过程。这条隧道建立依赖于受保护访问凭证(PAC)，PAC 是 EAP–FAST 通过认证，授权和记账(AAA)服务器(如思科安全访问控制服务器 [ACS]v3.2.3)来动态配置和管理的。利用相互验证的隧道，EAP–FAST 能够为字典攻击和中间人攻击这样的弱点提供保护。以下是 EAP–FAST 的几个阶段：

EAP–FAST 不仅降低了被动字典攻击和中间人攻击的风险，同时也在目前已部署基础设施之上实现了安全认证。

- 第 1 阶段：建立相互验证的隧道—客户端和 AAA 服务器使用 PAC 相互验证，并建立一个安全的隧道。
- 第 2 阶段：在建立隧道中执行客户身份验证—客户端发送用户名和密码来验证和建立用户端授权策略。
- 或者，第 0 阶段—EAP – FAST 很少使用此阶段验证来让客户端能够用 PAC 动态配置。在这一阶段在用户和网络之间生成了一个每用户的安全接入证书。验证的第 1 阶段将使用这个每用户证书，称之为 PAC。

更多信息请参考 Cisco EAP-FAST

问：在 cisco.com 有哪些文档是解释如何在思科 WLAN 网络配置 EAP 的？

答：如何在 WLAN 网络配置 EAP 认证请参考 EAP Authentication with RADIUS Server

如何配置 PEAP 认证请参见 Protected EAP Application Note

如何配置 LEAP 认证请参见 LEAP Authentication with a Local RADIUS server

问：什么是 WEP 加密？

答：WEP 全称为有线等效保密(Wired Equivalent Privacy)。WEP 协议是用来加密和解密无线局域网设备之间传输的数据信号的。WEP 协议是一个防止在传输时信息暴露和修改数据包及为使用中的网络提供访问控制的 IEEE 802.11 可选功能，WEP 协议使无线局域网连接变得和有线连结一样安全。作为标准规定，WEP 使用 40 位或 104 位密钥的 RC4 算法。RC4 是一种对称的 RC4 算法，因为其使用相同的密钥加密和解密数据。当 WEP 启用，每个无线电“站”都拥有一个密钥。该密钥用来将通过空气传输的数据加密。如果一个站收到一个不用正确的密钥加密的数据包，则该站会丢弃数据包而不会把数据包发送给主机。

如何设定的 WEP 请参见 Configuring Wired Equivalent Privacy (WEP)。

问：什么是广播密钥轮换？广播密钥轮换的频率是什么？

答：广播密钥轮换允许 AP 生成最佳的随机组密钥。广播密钥轮换定期更新所有能够管理密钥客户端密钥。当你启用广播 WEP 密钥轮换时，AP 提供了一个动态的广播 WEP 密钥，并在设定的时间间隔内更换密钥。如果你不能把思科客户端升级到最新固件，而你的无线局域网支持非思科的无线客户端或无线设备，那么广播密钥轮换是 TKIP 的最佳替代。如何配置广播关键轮换功能请参见 Enabling and Disabling Broadcast Key Rotation。

问：什么是 TKIP?

答：TKIP 全称为临时密钥完整性协议(Temporal Key Integrity Protocol)。TKIP 的引入是为了解决 WEP 加密的缺点。TKIP 也称为 WEP 密钥散列，最初称为 WEP2。TKIP 是一个修复 WEP 密钥重用问题的临时解决方案，和 WEP 协议一样，TKIP 也使用 RC4 算法进行加密。与 WEP 的主要区

别是，TKIP 为每个数据包生成不同密钥。因为每个数据包的散列值在改变，所以每个数据包的临时的密钥也在同时改变。

问：使用 TKIP 加密的设备能够与使用 WEP 加密的设备互通？

答：TKIP 的优势是，现有的基于 WEP 加密的 AP 和无线设备能够通过简单的固件补丁升级到 TKIP，此外，只支持 WEP 的设备也能够和与支持 TKIP 功能的设备通过 WEP 协议互通。

问：什么是信息完整性检查(MIC) ？

问：MIC 是另一个解决 WEP 加密漏洞的增强功能。MIC 在加密的数据包中可防止位翻转攻击。当位翻转攻击时，入侵者截获了加密信息，修改该信息后传输该修改的讯息。接收器不知道这个信息是已被破坏和不合法的。为了解决这个问题，MIC 特性在无线数据帧中添加了一个 MIC 字段。MIC 字段提供了一个数据帧完整性检查功能，不再像 ICV 那样存在数字缺点漏洞，MIC 在无线数据帧中还增加了序号字段，AP 会丢弃收到的超过序号范围的数据帧。

问：什么是 WPA？WPA2 与 WPA 有什么区别 ？

答：WPA 是一种基于 Wi - Fi 联盟的标准安全解决方案，以解决本地无线局域网漏洞。WPA 为 WLAN 系统提供了增强的数据保护和访问控制。WPA 在原来的 IEEE 802.11 标准的执行基础上解决了所有已知的有线等效保密(WEP)的漏洞，给 WLAN 网络带来了直接的安全解决方案，包括企业和小型办公室，家庭办公室(SOHO)这样的 WLAN 网络环境。

WPA2 是新一代的 Wi - Fi 安全协议。WPA2 是 Wi - Fi 联盟共同实施批准的 IEEE 802.11i 标准。WPA2 执行国家标准和技术局(NIST)建议基于高级加密标准(AES)加密算法的计数器模式及密码区块链信息认证码协议(CCMP)。AES 计数器模式是一种分组密码，该模式每次用一个 128 位密钥加密 128 位的数据块。WPA2 比 WPA 提供了更高级别的安全性。

WPA2 在每次关联都要创建新的会话密钥。WPA2 为网络中的每个客户端所使用的加密密钥都是独一无二的并且仅限于该客户端。最终，在空气中发送的每个数据包都使用唯一的密钥。

WPA1 和 WPA2 都可以使用 TKIP 或 CCMP 加密。(的确有些接入点和客户端限制了密码组合，但实际上有四种可能的密码组合)。WPA1 和 WPA2 之间的区别在于加入到 beacons，关联数据帧(association frame)和 4 次握手帧(4-way handshake)中的信息元素。在这些信息元素中的数据基本上是相同的，但使用的标识却是不同的。主要密钥交换区别是 WPA2 包括初始组密钥在 4 次握手中，并且第一次密钥握手被忽略，而 WPA 需求做这次额外的握手来提供初始组密钥。同样的，重新生成组密钥也以同样方式发生。握手发生在为用户传输数据选择和使用密码组成(TKIP 或 AES)之前，在 WPA1 或 WPA2 握手期间，确定使用何种密码组成。一旦选中，该密码组成将用于加密所有用户流量。因此 WPA1 加 AES 并不是 WPA2，WPA1 允许(但往往是有限的客户端)TKIP 或 AES 来作为加密密码。

问：什么是 AES?

答：AES 全称为先进加密标准(Advanced Encryption Standard)。AES 提供更强大的加密技术。AES 使用 Rijndael 算法，这是一种使用 128 位，192 位，256 位进行分组加密的技术，其安全性远高于 RC4。对于支持 AES 的无线局域网设备，硬件必须支持 AES 而不是 WEP 协议。

问：微软 Internet 验证服务(IAS)服务器支持什么是验证方法？

答：IAS 支持以下这些验证协议：

- 密码验证协议(PAP)
- Shiva 密码验证协议(SPAP)
- 挑战握手认证协议(CHAP)
- 微软挑战握手验证协议(MS - CHAP)
- 微软挑战握手认证协议第 2 版 (MS – CHAP v2)

- 基于消息摘要5协议的可扩展认证协议 CHAP(EAP-MD5 CHAP)
- 基于传输层安全的可扩展认证协议(EAP - TLS)
- 受保护的 EAP -MS - CHAP 第 2 版(PEAP-MS-CHAP v2)(也称为 PEAPv0/EAP-MSCHAPv2)

当 Windows 2000 Server 的 Service Pack 4 补丁已安装时，PEAP-TLS IAS 在 Windows 2000 Server 支持的 PEAP-MS-CHAP v2 and PEAP-TLS。欲了解更多信息，请参阅 Authentication Methods for use with IAS 。

排错和设计常见问题

问：在室外无线局域网是否有部署无线安全的最佳做法？

答：参见 Best Practices For Outdoor Wireless Security。这份文档提供了在室外无线局域网部署无线安全的最佳做法。

问：我能用 Windows 2000 或 2003 服务器的活动目录作为 RADIUS 服务器来验证无线客户端吗？

答： Windows 2000 或 2003 服务器的活动目录可以作为一个 RADIUS 服务器。如需关于如何设定这个 RADIUS 服务器，你需要联系微软公司，因为思科公司不提供 windows 服务器配置的帮助。

问：我的情况是关于从一个开放的无线网络(350 和 1200 系列 AP)迁移到 PEAP 验证网络的。我想让 OPEN SSID(一个 SSID 设定为开放式认证)和 PEAP SSID(一个 SSID 的配置为 PEAP 身份验证)同时工作在同一 AP。这使我们有时间将客户端迁移到 PEAP SSID。是否有办法在同一 AP 同时工作 OPEN SSID 和 PEAP SSID？

答：思科 AP 支持的 VLAN 功能(仅二层)。这实际上是实现你所要求的唯一方法。你需要创建两个 VLAN，(默认 VLAN 和其他 VLAN)。然后你就可以让一个 VLAN 用 WEP 加密，而另一个则不使用 WEP 加密。这样，你就可以设定一个 VLAN 用来开放认证而另一个 VLAN 用 PEAP 身份验

证。如果你想了解如何设定的 VLAN 请参阅 Using VLANs with Cisco Aironet Wireless Equipment。

请注意，你需要在交换机配置 dot1Q，若实现 VLAN 间的路由，你需要三层交换机或路由器。

问：我想设置我的思科 AP 1200 Vxworks，让无线用户能够通过思科 3005VPN 集中器认证。我需要在 AP 和客户端上配置什么吗？

答：这种情况下没有必要在 AP 或客户端上进行配置，所有配置均在 VPN 集中器上完成。

问：我正在部署一个思科 1232 AP。我想知道部署该 AP 最安全的方法。我手头没有 AAA 服务器，我仅有的资源就只有这个 AP 和一个 Windows 2003 域。我熟悉如何使用静态 128 位 WEP 密钥，非广播 SSID 和 MAC 地址限制。用户端大多工作在 Windows XP 工作站和一些 PDA 上。对于这种配置什么是最安全的方法呢？

答：如果你没有像思科 ACS 这样的 RADIUS 服务器，你也可以设定你的 AP 作为 LEAP 认证, EAP-FAST 认证或 MAC 认证的本地 RADIUS 服务器。

注：很重要的一点，你必须确认你是否要让客户端使用 LEAP 或 EAP-FAST 认证。如果是这样，你的客户端必须有一个实用工具来支持 LEAP 或 EAP-FAST 认证。Windows XP 只支持 PEAP 身份或 EAP-TLS 认证。

问：PEAP 认证失败，提示“EAP-TLS or PEAP authentication failed during SSL handshake”。为什么？

答：这种错误发生是由于 Cisco bug ID CSCee06008 (仅限注册用户)。使用 ADU 1.2.0.4 造成 PEAP 认证失败。此问题的解决方法是使用最新版本的 ADU。

问：我是否能在同一 SSID 同时启用 WPA 认证和本地 MAC 认证？

答：思科 AP 不支持在同一服务集标识符(SSID)内启用本地 MAC 认证和 Wi - Fi 保护访问预共享密钥(WPA-PSK)认证。当你启用本地 MAC 认证和 WPA-PSK 时，WPA-PSK 并不工作。发生这个问题是因为本地 MAC 认证从配置中移除了 WPA-PSK ASCII 密码行。

问：目前在我们的数据 VLAN 中，我们有三个采用了 128 位 WEP 加密方法的思科 1231 无线 AP。我们没有广播 SSID。我们也没有一个单独的 RADIUS 服务器在我们的网络环境中。有人能够通过扫描工具找到 WEP 密钥，并用该工具在这几周的时间里监测我们的无线流量。我们怎么样才能解决这种情况，从而使网络变得安全？

答：静态的 WEP 在这种情况下很容易受到攻击，如果一个黑客获取足够的数据包，并能够获得两个或两个以上的同初始化向量(IV)包，则前面所说的问题就会发生。

下面有几种方法能够防止发生此问题：

- 使用动态的 WEP 密钥。
- 使用 WPA 认证协议。
- 如果你只有思科适配器，开启 Per Packet Key 和 MIC 功能。

问：如果我有两个不同的 WLAN，都配置了 Wi - Fi 保护访问与预共享密钥(WPA-PSK)认证，能够在每个不同的 WLAN 间预共享密钥吗？如果它们是不同的，它会影响到其他已经配置了不同预共享密钥的 WLAN 吗？

答：WPA-PSK 的设置是每个 WLAN 独立的，如果你改变的其中一个 WLAN 的 WPA-PSK，它是不会影响到其他已经配置完成的 WLAN 的。

问：我的环境中我使用的英特尔 PRO /无线网卡，采用了基于隧道的灵活认证协议进行身份验证，同时将思科安全访问控制服务器(ACS)3.3 与 Windows 活动目录(AD)的账户连接起来。问题是当用户的密码即将到期时，Windows 不提示用户更改密码，最终导致该帐户过期。是否有让 Windows 提示用户更改密码的解决方案？

答：启用 Cisco Secure ACS 密码有效期特性，能够让你当用户满足下列一个或多个条件时强制用户更改其密码：

- 经过指定天数(按日期的期限规则)
- 经过指定登录次数(按用户的期限规则)
- 新用户第一次登录(密码更改规则)

如需了解关于如何配置 Cisco Secure ACS 该特性的细节，请参阅 Enabling Password Aging for the CiscoSecure User Database。

问：当用户采用 LEAP 认证方式登录到无线网络中，他们能够运行映射网络驱动器中的登录脚本。然而，使用 Wi - Fi 保护访问(WPA)或采用 PEAP 认证的 WPA2，登录脚本则不运行。客户端和 AP 以及 RADIUS(ACS)都是思科的产品。为什么登录脚本无法运行在 RADIUS(ACS)上？

答：机器认证会强制性运行登录脚本，这使无线用户在登录前能够访问网络中的加载脚本。

如需了解如何配置基于 PEAP-MS-CHAPv2 的机器认证，请参阅 Configuring Cisco Secure ACS for Windows v3.2 With PEAP-MS-CHAPv2 Machine Authentication。

问：思科 Aironet 桌面工具(ADU) 3.0 版本中，当用户配置基于传输层安全的可扩展认证协议的机器验证(EAP - TLS)，ADU 不允许用户创建配置文件。为什么？

答：这是因为 Cisco bug ID CSCsg32032 (仅限注册用户) 。这可能会发生如果客户端 PC 机已安装机器验证却没有用户证书的情况下。

解决方法是复制机器证书到用户端，建立一个的 EAP-TLS 配置文件，然后为了进行机器验证，从用户端删除该证书而仅余下配置。

问：在无线局域网中，是否有其他方式来基于客户端 MAC 地址分配 VLAN？

答：没有。这是不可能的。从 RADIUS 服务器分配 VLAN 只能工作在 802.1x 协议下，而不是 MAC 验证。如果 MAC 地址在 RADIUS 服务器(在 LEAP/PEAP 中定义为用户帐号/密码)已经验证过,则你可以使用 RADIUS 推动带 MAC 验证功能的 VSAs。

相关信息

- **Wireless Network Security**
- **Wireless LAN Security White Paper**
- **Wireless LAN Security Overview**
- **EAP-TLS Deployment Guide for Wireless LAN Networks**
- **Cisco LEAP**
- **Configuring Wired Equivalent Privacy (WEP)**
- **Wireless Product Support**
- **Technical Support & Documentation - Cisco Systems**

更新时间: 2008-2-20 文档编号: 68583