在Cisco Aironet无线安全常见问题

Contents

Introduction

本文档提供了有关 Cisco Aironet 无线安全的最常见问题 (FAQ) 的信息。

一般常见问题解答

Q. 什么是对无线安全的需要？

A. 在有线网络中，数据在连接终端设备的电缆依然是。但是无线网络通过RF信号广播传输并且接受数据到露天。由于广播性质WLAN使用，有能访问或破坏数据黑客或入侵者的一个更加巨大的威胁。为了缓和此问题，所有WLANs需要添加：

1. 防止对网络资源的未被授权的访问的用户认证。
2. 数据保密性保护完整性的和保密性传送的数据(亦称加密)。

Q. 什么是无线LAN 802.11标准定义了的不同的认证方法？

A. 802.11标准定义了无线局域网客户端的认证的两个机制：

1. 开放式验证
2. 共享密钥认证

有其他两个常用的机制：

1. 基于SSID的认证
2. MAC地址验证

Q. 什么是开放式验证？

A. 开放式验证基本上是一种空验证算法，因此意味着没有用户或机器的验证。开放式验证允许放置认证请求对接入点(AP)的所有设备。开放式验证使用明文发射允许客户端联合到AP。如果加密不是启用的，认识WLAN的SSID的所有设备能获得访问到网络。如果有线等效保密(WEP)在AP允许，WEP密钥成为访问控制方法。没有正确的WEP密钥的设备不能通过AP传输数据，即使认证是成功的。都不能AP发送的这样设备解密数据。

Q. 开放式验证介入为了客户端能连结什么步骤与AP ？

1. 客户端发送一个探测请求到APs。
2. APs发送探测回应。
3. 客户端评估AP回应并且选择最佳的AP。
4. 客户端发送认证请求到AP。
5. AP确认认证并且注册客户端。
6. 客户端然后发送一关联申请到AP。
7. AP确认关联并且注册客户端。

Q. 什么是Open开放式验证优点和缺点？

A. 这是Open开放式验证优点和缺点：

优点：开放式验证是基本认证机制，您能以无线设备使用不支持复杂认证算法。在802.11规格的认证面向连接的。由设计认证的需求允许设备获取快速存取到网络。在这种情况下，您能使用开放式验证。

缺点：开放式验证不提供方式检查客户端是否是一个有效客户端而不是黑客客户端。如果不以开放式验证使用WEP加密，认识WLAN的SSID的所有用户能访问网络。

Q. 什么是共享密钥认证？

A. 共享密钥认证工作类似于与一个主要区别的开放式验证。当您以WEP加密密钥时使用开放式验证，WEP密钥用于加密和解码数据，但是没有用于认证步骤。在共享密钥认证，WEP加密使用认证。类似开放式验证，共享密钥认证要求客户端和AP有同一把WEP密钥。AP使用的共享密钥认证发送一个质询文本信息包到客户端。客户端使用本地配置的WEP密钥加密质询文本和回复以随后的认证请求。如果AP能解码认证请求和检索原始质询文本，AP回应准许对客户端的访问的认证回应。

Q. 共享密钥认证介入为了客户端能连结什么步骤与AP ？

1. 客户端发送一个探测请求到APs。
2. APs发送探测回应。
3. 客户端评估AP回应并且选择最佳的AP。
4. 客户端发送认证请求到AP。
5. AP发送包含末加密的质询文本的一种认证回应。
6. 客户端加密与WEP密钥的质询文本并且发送文本到AP。
7. AP末加密的质询文本与被加密的质询文本比较。如果认证能解码和检索原始质询文本，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。

Q. 什么是共享密钥认证优点和缺点？

A. 在共享密钥认证，客户端和AP交换质询文本(明文)和被加密的挑战。所以，此种认证易受到中间人攻击。黑客能听末加密的挑战和被加密的挑战，并且从此信息提取WEP密钥(共享密钥)。当黑客认识WEP密钥时，全部的认证机制减弱，并且黑客能访问WLAN网络。这是与共享密钥认证的专业缺点。

Q. 什么是MAC地址验证？

A. 虽然802.11标准不指定MAC地址验证， WLAN网络通常使用此认证技术。因此，大多无线设备供应商，包括Cisco，支持MAC地址验证。

在MAC地址验证，客户端根据客户端MAC地址被验证MAC地址列表存储本地在AP或在一个外部认证服务器的他们的MAC地址验证。MAC验证比开放和共享密钥认证是更加严格的安全机制该802.11提供。更加进一步此的认证形式降低能访问网络未授权的设备的可能性。

Q. MAC验证为什么不与在Cisco IOS Software Release 12.3(8)JA2的Wi-Fi保护访问(WPA)一起使用？

A. 唯一的安全级别MAC验证的是检查客户端的MAC地址根据允许的MAC地址列表。这被认为非常弱。在初期的Cisco IOS软件版本中，您可能配置MAC验证和WPA加密信息。但是，因为WPA有检查的MAC地址， Cisco决定不允许被决定的这类配置在最新Cisco IOS软件版本和只改进安全功能。

Q. 能否使用SSID作为方法验证无线设备？

A. 服务集标识(SSID)是唯一，区分大小写，字母数字值该WLAN使用作为网络名。SSID是a -允许无线LAN的逻辑分离的机制。SSID不提供任何数据保密性功能，亦不SSID真验证客户端对AP。SSID值是广播作为在引导、探测请求，探测回应和帧的其他类型的明文。偷听者能容易地确定与使用的SSID 802.11无线局域网信息包分析程序，例如， Sniffer Pro。Cisco不建议您使用SSID作为方法巩固您的WLAN网络。

Q. 如果我禁用SSID广播，能实现在WLAN网络的高级安全？

A. 当您禁用SSID广播时， SSID在引导消息没有被发送。然而，其他帧例如，探测请求和探测回应仍然有SSID在明文。不因此，如果禁用SSID，您实现被增强的无线安全。SSID没有设计，亦不供使用使用，作为安全机制。另外，如果禁用SSID广播，您能遇到Wi-Fi互通性的问题混合客户端配置的。所以， Cisco不建议您使用SSID作为安全模式。

Q. 什么是在802.11安全找到的弱点？

A. 802.11安全的主要弱点可以被总结如下：

- 弱的只设备的认证：客户端设备没有验证，没有用户。
- 弱的数据加密：有线等效保密(WEP)是证明的无效的作为方法加密数据。
- 没有消息完整性：总校验值(ICV)是证明的无效的作为方法保证消息完整性。

Q. 什么是802.1x认证的角色在WLAN ？

A. 为了针对缺点和安全漏洞在802.11标准定义了的原始验证方法， 802.1X身份验证框架在草稿包括802.11 MAC控制层安全性增强的。IEEE 802.11任务组我(TGi)当前开发这些增进。802.1X框架提供链路层可扩充验证，通常仅看到在更高层。

Q. 什么是802.1x框架定义了的三个实体？

A. 802.1x框架要求这三逻辑实体验证在WLAN网络的设备。

1. **请求方**—亦称请求方在无线局域网客户端驻留，并且是EAP客户机。
2. **证明人**—证明人在AP驻留。
3. **认证服务器**—认证服务器在RADIUS服务器驻留。

Q. 当我使用802.1x身份验证框架，无线客户端认证如何出现？

A. 当无线客户端(EAP客户机)时变得激活，无线客户端验证与开放或共享验证。在客户端顺利地联合对AP后， 802.1x与开放式验证一起使用并且开始。客户端工作站联合，但是能在成功的802.1x认证之后通过数据流量。这是在802.1x认证的步骤：

1. 为802.1x (证明人)配置的AP请求从客户端的用户的身份。
2. 客户端回应其在一个被规定的时间的身份。
3. 如果用户的身份是存在其数据库，服务器检查用户的身份并且从客户端开始认证。
4. 服务器传送一个成功消息到AP。
5. 一旦客户端验证，服务器寄用于加密/到/从客户端被发送的解密数据流的加密密钥给AP。
6. 在第4步，如果用户的身份不是存在数据库，服务器下降认证并且发故障消息到AP。
7. AP寄此消息给客户端，并且客户端必须再验证与正确的证件。

Note: 在802.1x认证中， AP到/从客户端转发认证消息。

Q. 什么是我能以802.1x身份验证框架使用的不同的EAP变形？

A. 802.1x定义了程序验证客户端。用于802.1x框架的EAP类型定义了用于802.1x交换和验证方法的证件类型。802.1x框架能使用这些EAP变形中的任一个：

- EAP-TLS —可扩展的认证协议传输层安全
- EAP-FAST — EAP灵活的认证通过安全隧道
- EAP-SIM — EAP订户身分组件
- Cisco LEAP —轻量级扩展身份认证协议
- EAP-PEAP — EAP保护可扩展的认证协议
- EAP-MD5 —消息摘要算法5
- EAP-OTP — EAP准时密码
- EAP-TTLS — EAP建立隧道传输层安全

Q. 如何从可用不同的变形选择802.1x EAP方法？

A. 您必须设想的重要因素是否EAP方法是与现有的网络兼容。另外， Cisco建议您选择支持相互验证的方法。

Q. 什么是本地EAP验证？

A. 本地EAP是WLC作为认证服务器的机制。用户凭证在WLC存储本地验证无线客户端，作为一个后端进程在远程办公室，当服务器断开时。用户凭证可以被检索从在WLC的本地数据库或从外部LDAP服务器。LEAP、EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2和PEAPv1/GTC是本地EAP支持的不同的EAP验证。

Q. 什么是Cisco LEAP ？

A. 轻量级扩展身份认证协议(LEAP)是Cisco所有权验证方法。Cisco LEAP是无线LAN (WLANs)的一种802.1X认证类型。Cisco LEAP通过登录密码支持在客户端和RADIUS服务器之间的严格的相互验证作为共有的秘密。Cisco LEAP提供动态单个用户，每会话加密密钥。LEAP是配置802.1x的最少复杂方法，并且要求仅RADIUS服务器。关于LEAP的信息，参考Cisco LEAP。

Q. EAP-FAST如何工作？

A. EAP-FAST使用对称密钥算法达到一个隧道验证过程。隧道建立依靠受保护的访问凭证(PAC)该EAP-FAST可以由EAP-FAST动态地设置和管理通过验证、授权和统计(AAA)服务器(例如思科安全访问控制服务器[ACS] v. 3.2.3)。使用一条相互验证的隧道， EAP-FAST提供保护免受词典攻击和人在这中间弱点。这是阶段EAP-FAST ：

EAP-FAST不仅缓和从被动词典攻击和中间人攻击的风险，而且enable (event)获取根据当前配置的基础设施的认证。

- 阶段1 ：建立相互验证的隧道—客户端和AAA服务器互相验证和设立安全隧道的使用PAC。
- 第2阶段：进行客户端验证在已建隧道—客户端发送用户名和密码验证和设立客户端授权策略。
- 随意地，第0阶段— EAP-FAST认证偶尔地使用对enable (event)的此阶段客户端动态地配置有PAC。此阶段安全地生成一单个用户的访问凭证在用户和网络之间。认证的阶段1使用此单个用户的凭证，叫作PAC。

参考Cisco EAP-FAST欲知更多信息。

Q. 有没有解释如何配置在Cisco WLAN网络的EAP在cisco.com的文件？

A. 关于如何配置在WLAN网络的EAP验证的信息参考EAP验证用RADIUS服务器。

关于如何配置PEAP认证的信息，请参见保护的EAP应用程序注释。

关于如何配置LEAP认证的信息，参考LEAP认证用一个本地RADIUS服务器。

Q. 什么是不同的加密机制最常用在无线网络？

A. 这是用于无线网络的最常用的加密机制：

- WEP
- TKIP
- AES

AES是硬件加密方法，而WEP和TKIP加密在固件被处理。使用固件升级WEP设备可以支持TKIP，因此他们是相互可操作的。AES是最安全和最快速的方法，而WEP最不安全。

Q. 什么是WEP加密？

A. WEP 代表有线等效加密 (Wired Equivalent Privacy)。WEP用于加密和解码传输在WLAN设备之间的数据信号。WEP是IEEE 802.11的一个可选功能，防止在运送中的包被发现和修改并且提供对使用网络的接入控制。WEP 使得 WLAN 链路与有线链路一样安全。当标准指定， WEP以40位或104-bit键使用RC4算法。RC4 在对数据进行加密和解密时均使用相同的密钥，因此是一种对称算法。当WEP是启用的时，每个无线电"位置"有一个键。关键字被用于在数据的发射前通过广播频道加扰数据。如果接收到了未使用相应密钥加扰的数据包，无线电站会丢弃该数据包，并且永不将这样的数据包传递给主机。

关于如何配置WEP的信息，参考配置有线等效保密(WEP)。

Q. 什么是广播密钥交替？什么是频率广播密钥交替？

A. 广播密钥交替允许AP生成最好随机的组密钥。播放密钥交替周期地更新所有客户端有能力在密钥管理上。当您enable (event)广播WEP密钥循环， AP提供一把动态广播WEP密钥并且更换键在间隔时您设置。广播密钥交替是一个非常好的选择对TKIP，如果您的无线局域网支持您不能升级到Cisco客户端设备的最新的固件的非Cisco的无线客户端设备或设备。关于如何配置广播密钥交替功能的信息，参考启用和禁用广播密钥交替。

Q. 什么是TKIP ？

A. TKIP代表临时关键完整性协议。介绍TKIP寻址在WEP加密的缺点。亦称TKIP是WEP密钥hash算法和最初称为WEP2。TKIP是解决WEPs键重新使用问题的一个临时解决方案。TKIP使用RC4算法进行加密，是相同的象WEP。从WEP的一个主要区别是TKIP更换临时键每个信息包。临时关键变动每个信息包，因为每个信息包的Hash值更改。

Q. 能请使用TKIP与设备兼容使用WEP加密的设备？

A. 与TKIP的一个优点是与现有的基于WEP的APs的WLANs和无线电能升级到TKIP通过简单的固件补丁程序。并且，仅WEP设备与使用WEP的已启用TKIP设备仍然兼容。

Q. 什么是Message Integrity Check (MIC) ？

A. MIC是针对WEP加密的弱点的另外增进。MIC防止对加密的信息包的位翻转攻击。在位翻转攻击期间，入侵者拦截一个加密的消息，修改消息然后重新传输修改过的消息。接受器不知道消息是损坏而不是一合法一个。为了解决此问题， MIC功能添加一个MIC字段到无线帧。MIC字段提供不是易受攻击对数学缺点和ICV一样的帧完整性检查。MIC也添加一序列号字段到无线帧。AP丢包帧接收的故障中。

Q. 什么是WPA ？如何是WPA 2与WPA不同？

A. WPA 是一个来自 Wi-Fi 联盟的基于标准的安全解决方案，用于解决本地 WLAN 中的漏洞。WPA 为 WLAN 系统提供增强的数据保护和访问控制。WPA针对原始IEEE 802.11安全实施的所有已知有线等效保密(WEP)弱点并且给在企业和小型办公室、家庭办公室环境的WLAN网络带来一个立即安全问题解决方案。

WPA2是Wi-Fi安全的下一代。WPA2是被批准的IEEE 802.11i标准的Wi-Fi联盟可互操作的实施。WPA2实现美国标准技术研究所(NIST) -与使用的推荐的高级加密标准(AES)加密算法计数器模式与密码块连锁消息认证编码协议(CCMP)。AES 计数器模式是一次使用一个 128 位加密密钥加密 128 位数据块的块加密程序。WPA2比WPA提供高水平安全。WPA2创建在每个关联的新对话键。WPA2使用网络的每个客户端的加密密钥是唯一和特定的对该客户端。最终，通过空气发送的每个

数据包都会使用一个唯一的密钥进行加密。

WPA1和WPA2能使用TKIP或CCMP加密。(是真的一些接入点和一些客户端限制组合，但是那里是四个可能的组合)。在WPA1和WPA2之间的区别在获得放到引导、关联帧和4方式握手帧的信息要素。在这些信息要素的数据基本上是相同的，但是使用的标识是不同的。在关键握手上的主要区别是WPA2在4方式握手包括最初的组密钥，并且第一组密钥握手未参加，而WPA需要执行此额外的握手提供首字母组键。组密钥的密钥相似地发生。握手在选择和使用密码套件前发生(TKIP或AES)用户数据报发射的。在WPA1或WPA2握手期间，确定使用的密码套件。一旦选择，密码套件使用所有用户数据流。因而WPA1加上AES不是WPA2。WPA1允许(但是经常是被限制的客户端) TKIP或AES密码。

Q. 什么是AES ？

A. AES代表高级加密标准。AES提供强加密。AES使用Rijndael算法，比RC4是与128-， 192-和256-bit键技术支持的一个分组密码并且严格。为了使支持的WLAN设备AES，硬件必须支持AES而不是WEP。

Q. Microsoft互联网认证服务(IAS)服务器支持什么认证方法？

A. IAS支持这些身份验证协议：

- 密码认证协议
- Shiva密码验证协议(SPAP)
- 质询握手验证协议(CHAP)
- 微软询问握手认证协议
- 微软询问握手认证协议版本2 (MS-CHAP v2)
- 可扩展认证协议消息摘要5个CHAP (EAP-MD5 CHAP)
- EAP 传输层安全 (EAP-TLS)
- 保护的EAP-MS-CHAP v2 (PEAP-MS-CHAP v2) (亦称PEAPv0/EAP-MSCHAPv2)

当安装，在Windows 2000服务器的PEAP-TLS IAS支持PEAP-MS-CHAP v2和PEAP-TLS Windows 2000服务器服务包4。欲知更多信息，请参见认证方法为了用在IAS上 。

Q. VPN如何实现在无线envrionment ？

A. VPN是第3层安全机制;无线加密机制是被实施的在第2.层VPN在802.1x、EAP、WEP、TKIP和AES是被实施的。当第2层机制到位时， VPN添加在头顶上到实施。在安全不是被实施的地方类似公共热点和旅馆， VPN是实现的一个有用的解决方案。

排除故障和设计FAQ

Q. 有没有任何最佳实践配置在户外无线LAN的无线安全？

A. 参考户外无线安全的最佳实践。本文在安全最佳实践提供信息配置户外无线LAN。

Q. 能否以激活目录使用Windows 2000或2003服务器RADIUS服务器验证无线客户端？

A. Windows 2000或2003服务器有一个激活目录的能工作作为RADIUS服务器。关于如何，因为

Cisco不支持Windows服务器配置，配置此RADIUS服务器的信息，您需要与Microsoft联系。

Q. 我的站点将从开放无线网络(350和1200系列APs)移植到PEAP网络。我希望同时有开放SSID (为Open开放式验证配置的SSID)和在同样AP的PEAP SSID (为PEAP认证配置的SSID)工作。这提供我们时刻移植客户端到PEAP SSID。有没有方式同時主机一开放SSID和一PEAP SSID在同样AP ？

A. Cisco APs技术支持VLAN (第2层仅)。这实际上是达到什么的唯一方法您要执行。您需要创建两VLAN， (本地和您的其他VLAN)。然后您不能有一个的一把WEP密钥和别的WEP密钥。这样，您能配置一Open开放式验证的VLAN和PEAP认证的另一个VLAN。如果要知道如何配置VLAN，请参见使用VLAN以Cisco Aironet无线设备。

请注意:您需要配置您的交换机dot1q的和VLAN间路由、您的L3交换机或者您的路由器的。

Q. 我要设置我的Cisco AP1200 VxWorks让无线用户验证到Cisco 3005 VPN集中器。什么配置需要是存在完成此的AP和客户端？

A. 没有特定配置必要在AP或客户端为此方案。您必须执行在VPN集中器的所有配置。

Q. 我配置Cisco 1232 AG AP。我希望称作我能配置与此AP的多数安全的方法。我没有一个AAA服务器，并且仅我的资源是AP和Windows 2003域。我熟悉如何使用静态128-bit WEPs键、非广播SSID和MAC地址限制。用户主要工作与Windows XP工作站和某PDA。什么是此设置的最安全的实施？

A. 如果没有一个RADIUS服务器类似Cisco ACS，您能配置您的AP作为LEAP、EAP-FAST或者MAC验证的一个本地RADIUS服务器。

Note: 您必须考虑的一个非常重要点是您是否要以LEAP或EAP-FAST使用您的客户端。如果那样，您的客户端必须有支持的工具LEAP或EAP-FAST。Windows XP工具只支持PEAP或EAP-TLS。

Q. PEAP认证失效与错误“在SSL握手期间失效的EAP-TLS或PEAP认证”。为什么？

A. 此错误能出现由于Cisco Bug ID CSCee06008 (仅限注册用户)。PEAP失效与ADU 1.2.0.4。此问题的解决方法是使用ADU的新版本。

Q. 能否有在同样SSID的WPA和本地MAC认证？

A. Cisco AP不支持本地MAC认证和Wi-Fi受保护的访问预共用键(WPA-PSK)在同样服务集标识(SSID)。当您enable (event)与WPA-PSK的本地MAC认证， WPA-PSK不工作。因为本地MAC认证从配置，删除WPA-PSK ASCII密码线路此问题发生。

Q. 我们当前有三Cisco 1231无线AP设置密码我们的数据VLAN 128-bit WEP加密。我们不播放SSID。我们在我们的环境里没有一个分开的RADIUS服务器。某人能通过扫描工具确定WEP密钥，并且使用工具两三周监控我们的无线数据流。防止此和如何能使网络安全？

A. 静态WEP是易受攻击对此问题，并且可以派生，如果黑客获取足够的信息包并且能得到与同一初始化矢量(iv)的两个或多个信息包。

有几个方式防止此问题出现时间：

1. 请使用动态WEP密钥。
2. 请使用WPA。
3. 如果有仅Cisco适配器、enable (event)每个小包键和MIC。

Q. 如果我有两不同WLANs，两个为Wi-Fi保护访问(WPA)配置了-预共享密钥(PSK)，预共享密钥可以是不同的每WLAN ？如果他们是不同的，它是否影响另一WLAN配置有不同的预共享密钥？

A. WPA-PSK的设置应该是每WLAN。如果更改一WPA-PSK，配置的不应该影响另一WLAN。

Q. 在我的环境里我使用主要Intel赞成/无线、可扩充验证灵活协议认证通过获取建立隧道(EAP-FAST)和思科安全访问控制服务器(ACS)与Windows激活目录(AD)连接的3.3帐户。问题是，当用户密码将到期时， Windows不提示用户更改密码。最终，帐户到期。有没有使Windows提示用户的解决方案更改密码？

A. Cisco Secure ACS密码过期功能enable (event)迫使用户的您更改他们的密码在一个或很多下这些情况：

- 在指定的编号几天以后(使用周期由DATE规则)
- 在指定的编号登录以后(使用寿命规则)
- 第一次新的用户登录(密码更改规则)

关于关于怎样的详细资料配置此功能的Cisco Secure ACS，请参见启用CiscoSecure用户数据库的密码过期。

Q. 当用户登录无线地使用LEAP他们获得他们的登录脚本映射网络驱动器。然而，使用Wi-Fi保护访问(WPA)或WPA2与PEAP认证，登录脚本不运行。客户端和接入点是Cisco象RADIUS (ACS)。登录脚本为什么不运行在RADIUS (ACS) ？

A. 机器认证对于登录脚本是必需工作。此enable (event)获取网络访问的无线用户在用户前装载脚本注册。

关于如何用PEAP-MS-CHAPv2配置机器认证的信息，请参见配置Windows的v3.2 Cisco Secure ACS用PEAP-MS-CHAPv2机器认证。

Q. 使用Cisco Aironet Desktop软件(ADU)版本3.0，当用户配置可扩充验证传输层安全的(EAP-TLS)时机器认证， ADU不允许用户创建配置文件。为什么？

A. 这是由于Cisco Bug ID CSCsg32032 (仅限注册用户)。这能发生，如果客户端PC机有安装的机器认证和没有用户证书。

解决方法是复制机器认证到用户存储，创建EAP-TLS配置文件从仅机器认证配置的用户存储然后删除认证。

Q. 有没有任何方式分配在根据客户机的MAC地址的无线局域网的VLAN ？

A. No.这不是可能的。从RADIUS服务器的VLAN分配只与802.1x一起使用，不是MAC验证。您能使

用RADIUS推进与MAC验证的VSAs，如果MAC地址验证在RADIUS服务器(被定义成userid/密码在LEAP/PEAP)。

Related Information

- 无线网络安全
- 无线LAN安全白皮书
- 无线LAN安全概述
- 无线 LAN 网络的 EAP-TLS 部署指南
- Cisco LEAP
- 配置有线等效保密(WEP)
- 无线产品支持
- Technical Support & Documentation - Cisco Systems