在Cisco Aironet无线安全常见问题

目录

简介

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. 为什么需要无线安全？

A. 在有线网络中，数据通过连接终端设备的电缆传输。但无线网络通过在空间中广播的 RF 信号传送和接收数据。鉴于 WLAN 采用的广播特性，数据遭到黑客或入侵者访问或破坏的威胁更大。为了缓解这一问题，所有 WLAN 都额外要求：

1. 用户身份验证，以防止对网络资源进行未经授权的访问。
2. 数据保密性（也称为加密），以保护所传输数据的完整性和保密性。

Q. 无线 LAN 的 802.11 标准定义了哪些不同的身份验证方法？

A. 802.11 标准针对无线 LAN 客户端定义了两种身份验证机制：

1. 开放式身份验证
2. 共享密钥身份验证

除此之外，还有两种常用的机制：

1. 基于 SSID 的身份验证
2. MAC 地址身份验证

Q. 什么是开放式身份验证？

A. 开放式身份验证基本上是一种零身份验证算法，即意味着不对用户或计算机进行验证。开放式身份验证允许对接入点 (AP) 提出身份验证请求的所有设备。开放式身份验证使用明文传输以允许客户端与 AP 关联。如果不启用加密，则知道 WLAN 的 SSID 的所有设备就都能访问该网络内部。如果对 AP 启用了 Wired Equivalent Privacy (WEP)，WEP 密钥就会变成一种访问控制方式。即使身份验证成功，没有正确 WEP 密钥的设备也不能通过 AP 传送数据。此类设备也不能解密 AP 发送的数据。

Q. 为使客户端能与 AP 关联，开放式身份验证需要涉及哪些步骤？

1. 客户端向 AP 发送探测请求。
2. AP 发回探测响应。
3. 客户端对 AP 响应进行评估并选择最佳 AP。
4. 客户端向 AP 发送身份验证请求。
5. AP 确认身份验证并注册客户端。
6. 然后客户端向 AP 发送关联请求。
7. AP 确认关联并注册客户端。

Q. 开放式身份验证有什么优点和缺点？

A. 开放式身份验证的优点和缺点如下：

优点：开放式身份验证是一种基本身份验证机制，可以将其用于不支持复杂身份验证算法的无线设备。802.11 规范中的身份验证是面向连接的。根据设计，身份验证的要求允许设备快速访问网络。在这种情况下，您可以使用开放式身份验证。

缺点：开放式身份验证未提供任何方法来检查客户端是否为有效客户端以及客户端是否不是黑客客户端。如果开放式身份验证不使用 WEP 加密，则知道 WLAN 的 SSID 的所有用户就都能访问网络。

Q. 什么是共享密钥身份验证？

A. 共享密钥身份验证的工作方式与开放式身份验证类似，只有一个主要区别。当您使用带 WEP 加密密钥的开放式身份验证时，WEP 密钥用于加密和解密数据，但不用于身份验证步骤。在共享密钥身份验证中，WEP 加密用于身份验证。与开放式身份验证类似，共享密钥身份验证要求客户端和 AP 拥有相同的 WEP 密钥。使用共享密钥身份验证的 AP 向客户端发送质询文本数据包。客户端使用本地配置的 WEP 密钥对质询文本进行加密，然后发送一个身份验证请求作为应答。如果 AP 能解密身份验证请求并检索原始质询文本，AP 将发送准许访问客户端的身份验证响应。

Q. 为使客户端能与 AP 关联，共享密钥身份验证需要涉及哪些步骤？

1. 客户端向 AP 发送探测请求。
2. AP 发回探测响应。
3. 客户端对 AP 响应进行评估并选择最佳 AP。
4. 客户端向 AP 发送身份验证请求。
5. AP 发送包含未加密质询文本的身份验证响应。
6. 客户端使用 WEP 密钥对质询文本进行加密并将该文本发送到 AP。
7. AP 将未加密的质询文本与加密的质询文本进行比较。如果身份验证能解密并检索原始质询文本，则该身份验证成功。

在客户端关联过程中，共享密钥身份验证会使用 WEP 加密。

Q. 共享密钥身份验证有哪些优点和缺点？

A. 在共享密钥身份验证中，客户端和 AP 会交换质询文本（明文）和加密质询。因此，这种类型的身份验证易受到中间人攻击。黑客能监听未加密质询和加密质询，并且从此信息中提取 WEP 密钥（共享密钥）。黑客知道 WEP 密钥后，整个身份验证机制就被攻陷，因此黑客能访问 WLAN 网络。这是共享密钥身份验证的主要缺点。

Q. 什么是 MAC 地址身份验证？

A. 虽然 802.11 标准未指定 MAC 地址身份验证，但 WLAN 网络通常使用这种身份验证技术。因此，大多数无线设备供应商（包括 Cisco）都支持 MAC 地址身份验证。

在 MAC 地址身份验证中，根据客户端的 MAC 地址对客户端进行身份验证。将对照 AP 上本地存储的或外部身份验证服务器上存储的 MAC 地址列表验证客户端的 MAC 地址。与 802.11 提供的开放式身份验证和共享密钥身份验证相比，MAC 身份验证机制的安全性更高。这种身份验证形式进一步降低了未授权的设备能够访问网络的可能性。

Q. MAC 身份验证为什么不能与 Cisco IOS 软件版本 12.3(8)JA2 中的 Wi-Fi Protected Access (WPA) 一起使用？

A. MAC 身份验证的唯一安全级别是对照允许的 MAC 地址列表检查客户端的 MAC 地址。这被认为安全性非常低。在较低的 Cisco IOS 软件版本中，您可以配置 MAC 身份验证和 WPA 以加密信息。但因为 WPA 自身具有需要检查的 MAC 地址，Cisco 决定不允许在较高的 Cisco IOS 软件版本中进行此类配置，并决定只改善安全功能。

Q. 能否将 SSID 用作对无线设备进行身份验证的一种方法？

A. 服务集标识符 (SSID) 是一个区分大小写的字母数字唯一值，WLAN 将该值用作网络名称。SSID 是一种允许逻辑分离无线 LAN 的机制。SSID 既不提供任何数据保密性功能，也不真正向 AP 验证客户端。SSID 值以明文形式在信标、探测请求、探测响应和其他类型的帧中进行广播。窃听者通过使用 802.11 无线 LAN 数据包分析程序（例如，Sniffer Pro）很容易确定 SSID。Cisco 建议您不要将 SSID 用作保护 WLAN 网络的方法。

Q. 如果禁用 SSID 广播，能否增强 WLAN 网络的安全性？

A. 当您禁用 SSID 广播后，将不会在信标消息中发送 SSID。不过，其他帧（例如，探测请求和探测响应）仍然具有明文形式的 SSID。因此，禁用 SSID 不能增强无线安全性。从设计或预期用途的角度讲，SSID 不是一种安全机制。另外，如果禁用 SSID 广播，对于混合客户端部署，您可能会遇到 Wi-Fi 互操作性问题。因此，Cisco 建议您不要将 SSID 用作安全模式。

Q. 802.11 安全标准中发现了哪些漏洞？

A. 802.11 安全标准存在的主要漏洞可以汇总为如下内容：

- 仅对设备进行身份验证不是很安全：对客户端设备而不是用户进行身份验证。
- 数据加密不是很安全：Wired Equivalent Privacy (WEP) 已被证明是一种无效的数据加密方法。
- 消息的完整性没有保证：完整性校验值 (ICV) 在确保消息完整性方面已被证明是一种无效的方法。

Q. 802.1x 身份验证在 WLAN 中扮演什么角色？

A. 为了应对 802.11 标准定义的原始身份验证方法存在的缺点和安全漏洞，802.11 MAC 层安全性增强草案中包括了 802.1X 身份验证框架。IEEE 802.11 任务组 i (TGi) 当前正在开发这些增强功能。802.1X 框架所提供的链路层具有通常仅在更高层中才能看到的可扩展身份验证。

Q. 802.1x 框架定义了哪三个实体？

A. 802.1x 框架要求以下三个逻辑实体验证 WLAN 网络上的设备。

1. **请求方** - 请求方驻留在无线 LAN 客户端上，也称为 EAP 客户端。
2. **身份验证程序** - 身份验证程序驻留在 AP 上。
3. **身份验证服务器** - 身份验证服务器驻留在 RADIUS 服务器上。

Q. 使用 802.1x 身份验证框架时，无线客户端身份验证是如何进行的？

A. 当无线客户端（EAP 客户端）激活后，它将通过开放式或共享身份验证方式进行身份验证。802.1x 使用开放式身份验证进行工作，并在客户端成功与 AP 关联后启动。客户端工作站可以关联，但只能在成功通过 802.1x 身份验证后才能传递数据流。802.1x 身份验证中的步骤如下：

1. 针对 802.1x 配置的 AP（身份验证程序）从客户端请求用户的身份。
2. 客户端在规定的时间内响应自己的身份。
3. 服务器检查用户的身份，如果用户的身份存在于其数据库中，服务器便开始验证客户端。
4. 服务器向 AP 发送成功消息。
5. 客户端通过身份验证后，服务器就会将加密密钥转发给 AP 以用于加密/解密发送至及来自客户端的数据流。
6. 在步骤 4 中，如果用户的身份不存在于数据库中，服务器会停止身份验证并向 AP 发送失败消息。
7. AP 会将此消息转发给客户端，客户端必须使用正确的凭据再次进行身份验证。

注意： 在整个 802.1x 身份验证过程中，AP 只是向客户端转发身份验证消息以及从客户端转发身份验证消息。

Q. 哪些不同的 EAP 变体可以用于 802.1x 身份验证框架？

A. 802.1x 定义了验证客户端的过程。802.1x 框架中使用的 EAP 类型定义了 802.1x 交换中使用的凭据类型和身份验证方法。802.1x 框架可以使用以下任何一个 EAP 变体：

- EAP-TLS —可扩展的认证协议传输层安全
- EAP-FAST - EAP 通过安全隧道的灵活身份验证
- EAP-SIM — EAP 用户身份模块
- Cisco LEAP - 轻量级可扩展的认证协议 (LEAP)
- EAP-PEAP — EAP 受保护的可扩展的认证协议 (PEAP)
- EAP-MD5 — EAP – 消息摘要算法 5
- EAP-OTP - EAP 一次性口令
- EAP-TTLS - EAP 隧道化传输层安全

Q. 如何从不同的可用变体选择 802.1x EAP 方法？

A. 您必须考虑 EAP 方法是否与现有网络兼容这一最重要的因素。另外，Cisco 建议您选择一种支持

相互身份验证的方法。

Q. 什么是本地 EAP 身份验证？

A. 本地 EAP 是一种 WLC 充当身份验证服务器的机制。用户凭据存储在 WLC 本地以用于对无线客户端进行身份验证，这是服务器停机后在远程办公室执行的一个后端进程。用户凭据可以从 WLC 的本地数据库或从外部 LDAP 服务器进行检索。LEAP、EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2 和 PEAPv1/GTC 是本地 EAP 支持的不同 EAP 身份验证。

Q. 什么是 Cisco LEAP？

A. 轻量级可扩展的认证协议 (LEAP) 是 Cisco 专有的一种身份验证方法。Cisco LEAP 是一种针对无线 LAN (WLAN) 的 802.1X 身份验证类型。Cisco LEAP 支持在客户端和 RADIUS 服务器之间通过作为共享密钥的登录口令进行强相互身份验证。Cisco LEAP 针对每个用户、每个会话提供动态加密密钥。LEAP 是部署 802.1x 的最简单方法，只需要一台 RADIUS 服务器即可。有关 LEAP 的信息，请参阅 Cisco LEAP。

Q. EAP-FAST 如何工作？

A. EAP-FAST 使用对称密钥算法来实现隧道化身份验证过程。隧道的建立依靠受保护的访问凭据 (PAC)，其中可以由 EAP-FAST 通过身份验证、授权和记帐 (AAA) 服务器（例如 Cisco 安全访问控制服务器 [ACS] v. 3.2.3）来动态配置和管理 EAP-FAST。通过一个相互已验证的隧道，EAP-FAST 防御词典攻击和中间人漏洞。EAP-FAST 的各个阶段如下：

EAP-FAST 不仅能降低被动词典攻击和中间人攻击的风险，而且支持基于当前部署的基础架构的安全身份验证。

- 第 1 阶段：建立相互已验证的隧道 - 客户端和 AAA 服务器使用 PAC 互相进行身份验证并建立安全隧道。
- 第 2 阶段：在建立的隧道中执行客户端验证 - 客户端发送用户名和口令来进行身份验证并建立客户端授权策略。
- （可选）阶段 0 - EAP-FAST 身份验证偶尔会使用此阶段来允许为客户端动态配置 PAC。此阶段会在用户和网络之间安全地生成一个每用户访问凭据。身份验证的阶段 1 使用此每用户凭据，称为 PAC。

有关详细信息，请参阅 Cisco EAP-FAST。

Q. cisco.com 上有没有提供介绍如何在 Cisco WLAN 网络中配置 EAP 的文档？

A. 有关如何在 WLAN 网络中配置 EAP 身份验证的信息，请参阅使用 RADIUS 服务器执行 EAP 身份验证。

有关如何配置 PEAP 身份验证的信息，请参阅受保护的 EAP 应用说明。

有关如何配置 LEAP 身份验证的信息，请参阅使用本地 RADIUS 服务器执行 LEAP 身份验证。

Q. 无线网络中最常使用哪些不同的加密机制？

A. 无线网络中最常使用以下加密机制：

- WEP
- TKIP
- AES

AES 是一种硬件加密方法，而 WEP 和 TKIP 加密是在固件中处理的。通过升级固件，WEP 设备可以支持 TKIP，因此它们是可相互操作的。AES 是最安全和最快速的方法，而 WEP 是最不安全的方法。

Q. 什么是 WEP 加密？

A. WEP 代表有线等效加密 (Wired Equivalent Privacy)。WEP 用于加密和解密在 WLAN 设备之间传输的数据信号。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。根据标准中的规定，WEP 使用带有 40 位或 104 位密钥的 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被启用时，每个“station”有一个关键字。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。

有关如何配置 WEP 的信息，请参阅配置 Wired Equivalent Privacy (WEP)。

Q. 什么是广播密钥交替？广播密钥交替的频率是多少？

A. 广播密钥交替允许 AP 生成尽可能最佳的随机组密钥。广播密钥交替会定期更新所有具有密钥管理功能的客户端。当您启用广播 WEP 密钥交替后，AP 会提供一个动态广播 WEP 密钥并且以您设置的时间间隔更改该密钥。如果无线 LAN 支持 Cisco 设备之外的无线客户端设备，或者支持不能升级至 Cisco 客户端设备的最新固件的设备，则广播密钥交替是 TKIP 之外的最佳选择。有关如何配置广播密钥交替功能的信息，请参阅启用和禁用广播密钥交替。

Q. 什么是 TKIP？

A. TKIP 代表 Temporal Key Integrity Protocol (TKIP)。引入 TKIP 是为了应对 WEP 加密存在的缺点。TKIP 也称为 WEP 密钥散列算法，最初称为 WEP2。TKIP 是解决 WEP 密钥重用问题的一种临时解决方案。与 WEP 一样，TKIP 使用 RC4 算法执行加密。与 WEP 的一个主要区别是 TKIP 为每个数据包都更改临时密钥。每个数据包的临时密钥都发生更改，是因为每个数据包的哈希值都发生更改。

Q. 使用 TKIP 的设备可以与使用 WEP 加密的设备互操作吗？

A. TKIP 的一个优点是带有现有基于 WEP 的 AP 和无线电的 WLAN 能够通过简单固件补丁升级到 TKIP。并且，仅 WEP 设备仍然可以与使用 WEP 的已启用 TKIP 的设备互操作。

Q. 什么是消息完整性检查 (MIC)？

A. MIC 是应对 WEP 加密中所存在漏洞的另一种增强。MIC 可阻止对加密数据包的位翻转攻击。在位翻转攻击期间，入侵者会拦截加密的消息，修改消息，然后重新传输修改过的消息。接收方不知道消息已损坏并且并非合法消息。为了解决这个问题，MIC 功能在无线帧中添加了一个 MIC 字段。该 MIC 字段提供帧完整性检查，该检查不易受与 ICV 一样的数学缺点的攻击。MIC 还在无线帧中添加了一个序列号字段。AP 将丢弃接收到的顺序错误的帧。

Q. 什么是 WPA？WPA2 与 WPA 有何不同？

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 可以应对原始 IEEE 802.11 安全实施中存在的所有已知有线等效加密 (WEP) 漏洞，并为企业和小型办公室、家庭办公室 (SOHO) 环境中的 WLAN 网络提供一种即时安全解决方案。

WPA2 是新一代 Wi-Fi 安全证书。WPA2是被批准的IEEE 802.11i标准的wi-fi联盟可互操作的实施。WPA2 通过将计数器模式与口令块链消息身份验证码协议 (CCMP) 结合使用，实现了美国国家标准与技术研究所 (NIST) 推荐的高级加密标准 (AES) 加密算法。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 提供的安全级别比 WPA 高。WPA2创建在每个关联的新会话密钥。WPA2 用于网络上每个客户端的加密密钥都是唯一的，并且特定于相应客户端。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 都能使用 TKIP 或 CCMP 加密。（某些接入点和某些客户端确实会限制组合，但共有四种可能的组合）。WPA1 和 WPA2 之间的区别在于放入信标、关联帧和四次握手帧的信息元素。这些信息元素中的数据基本上是相同的，但使用的标识符不同。密钥握手中的主要区别是 WPA2 在四次握手中包括初始组密钥，并且跳过第一组密钥握手，而 WPA 需要执行此额外的握手以提供初始组密钥。组密钥的重发密钥过程与此相似。握手在为用户数据报传输选择和使用加密套件（TKIP 或 AES）之前发生。在 WPA1 或 WPA2 握手期间确定要使用的加密套件。一旦选择后，加密套件就会用于所有用户数据流。因此，WPA1 加上 AES 不等于 WPA2。WPA1 允许（但经常受客户端限制）TKIP 或 AES 加密程序。

Q. 什么是 AES？

A. AES 代表高级加密标准。AES 提供更强的加密。AES 使用 Rijndael 算法，它是一个支持 128、192 和 256 位密钥块加密程序并且远远强于 RC4。为了使 WLAN 设备支持 AES，硬件必须支持 AES 而不是 WEP。

Q. Microsoft Internet 身份验证服务 (IAS) 服务器支持哪些身份验证方法？

A. IAS 支持以下身份验证协议：

- 密码 认证 协议 (PAP)
- Shiva 口令身份验证协议 (SPAP)
- 质询 握手 验证 协议（CHAP）
- Microsoft 质询握手身份验证协议 (MS-CHAP)
- Microsoft 质询握手身份验证协议版本 2 (MS-CHAP v2)
- 可扩展的认证协议 - 消息摘要 5 CHAP (EAP-MD5 CHAP)
- EAP 传输层安全 (EAP-TLS)
- 受保护的 EAP-MS-CHAP v2 (PEAP-MS-CHAP v2)（也称为 PEAPv0/EAP-MSCHAPv2）

当安装了 Windows 2000 Server Service Pack 4 时，Windows 2000 Server 中的 PEAP-TLS IAS 支持 PEAP-MS-CHAP v2 和 PEAP-TLS。有关详细信息，请参阅用于 IAS 的身份验证方法 。

Q. 如何在无线环境中实施 VPN？

A. VPN 是一种第 3 层安全机制；无线加密机制是在第 2 层实施的。VPN 在 802.1x、EAP、WEP、TKIP 和 AES 上实施。设置第 2 层机制后，VPN 会增加实施开销。在没有实施安全的地方（如公共热点和旅馆），VPN 将是一种有效的实施解决方案。

故障排除和设计常见问题解答

Q. 有没有任何在室外无线 LAN 中部署无线安全的最佳做法？

A. 请参阅室外无线安全的最佳做法。本文提供了有关部署室外无线 LAN 的最佳安全做法的信息。

Q. 能否将带 Active Directory 的 Windows 2000 或 2003 Server 用作 RADIUS 服务器来验证无线客户端？

A. 可以将带 Active Directory 的 Windows 2000 或 2003 Server 用作 RADIUS 服务器。因为 Cisco 不支持 Windows 服务器配置，所以有关如何配置此类 RADIUS 服务器的信息，您需要与 Microsoft 联系。

Q. 我的站点将从开放式无线网络（350 和 1200 系列 AP）迁移到 PEAP 网络。我希望开放式 SSID（为开放式身份验证配置的 SSID）和 PEAP SSID（为 PEAP 身份验证配置的 SSID）同时在同一 AP 上工作。这样我们就有时间将客户端迁移到 PEAP SSID 了。有没有办法可在同一 AP 上同時承载开放式 SSID 和 PEAP SSID？

A. Cisco AP 支持 VLAN（仅第 2 层）。实际上这是实现您的目的的唯一方法。您需要创建二个 VLAN（本地 VLAN 和另一个 VLAN）。然后您可以为一个 VLAN 设置 WEP 密钥，而不为另一个 VLAN 设置 WEP 密钥。这样，您就可以将一个 VLAN 配置为开放式身份验证，并将另一个 VLAN 配置为 PEAP 身份验证。如果要了解如何配置 VLAN，请参阅将 VLAN 用于 Cisco Aironet 无线设备。

请注意，您需要配置您用于 dot1q 和 VLAN 间路由的交换机、您的 L3 交换机或您的路由器。

Q. 我需要设置我的 Cisco AP1200 VxWorks 以让无线用户通过 Cisco 3005 VPN 集中器的身份验证。为此需要在 AP 和客户端上进行什么配置？

A. 对于这种情景，不需要在 AP 或客户端上进行特定配置。您必须在 VPN 集中器上进行所有配置。

Q. 我正在部署 Cisco 1232 AG AP。我想知道部署此 AP 的最安全方法。我没有 AAA 服务器，并且仅有的资源是 AP 和 Windows 2003 域。我知道如何使用静态 128 位 WEP 密钥、非广播 SSID 和 MAC 地址限制。用户主要使用 Windows XP 工作站和一些 PDA。针对此设置的最安全实施方法是什么？

A. 如果没有 RADIUS 服务器（如 Cisco ACS），您可以将 AP 配置为执行 LEAP、EAP-FAST 或者 MAC 身份验证的本地 RADIUS 服务器。

注意： 您必须考虑的非常重要的一点是您是否要将客户端用于 LEAP 或 EAP-FAST。如果用于的话，您的客户端就必须有支持 LEAP 或 EAP-FAST 的实用程序。Windows XP 实用程序仅支持 PEAP 或 EAP-TLS。

Q. PEAP 身份验证失败，错误为“EAP-TLS or PEAP authentication failed during SSL handshake”。为什么？

A. 此错误归因于 Cisco Bug ID CSCee06008（仅限注册用户）。PEAP 在使用 ADU 1.2.0.4 时失败。此问题的解决方法是使用最新版本的 ADU。

Q. 同一 SSID 上能否同时有 WPA 和本地 MAC 身份验证？

A. Cisco AP 不支持同一服务集标识符 (SSID) 中同时有本地 MAC 身份验证和 Wi-Fi Protected Access 预共享密钥 (WPA-PSK)。当您启用带 WPA-PSK 的本地 MAC 身份验证时，WPA-PSK 将停止工作。出现此问题是因为本地 MAC 身份验证从配置中删除了 WPA-PSK ASCII 口令行。

Q. 我们当前有三个 Cisco 1231 无线 AP 设置是使用加密程序对数据 VLAN 进行 128 位 WEP 加密的。我们不广播 SSID。我们的环境中没有单独的 RADIUS 服务器。有人能通过扫描工具确定 WEP 密钥，并且有两三周时间使用该工具监控我们的无线数据流。如何阻止这种情况以及如何能使网络安全？

A. 静态 WEP 易受这种攻击，如果黑客获取足够的数据包并且能得到有同一初始化矢量 (IV) 的两个或更多个数据包，就会产生这种情况。

有多种方式可防止出现此问题：

1. 使用动态 WEP 密钥。
2. 使用 WPA。
3. 如果只有 Cisco 适配器，请启用每包密钥和 MIC。

Q. 如果我有两个不同 WLAN，两个均配置为 Wi-Fi Protected Access (WPA) - 预先共享密钥 (PSK)，每个 WLAN 的预先共享密钥是否可以不同？如果它们不同，是否会影响使用不同预先共享密钥配置的另一 WLAN？

A. WPA-PSK 的设置应该是针对每个 WLAN 的。如果更改一个 WPA-PSK，不应该影响配置的另一个 WLAN。

Q. 在我的环境中，我主要使用 Intel Pro/Wireless、可扩展的认证协议 - 通过安全隧道的灵活身份验证 (EAP-FAST) 和链接至 Windows Active Directory (AD) 帐户的 Cisco 安全访问控制服务器 (ACS) 3.3。问题是当用户口令即将过期时，Windows 不提示用户更改口令。最终，帐户过期。有没有使 Windows 能提示用户更改口令的解决方案？

A. 您可以通过 Cisco Secure ACS 口令过期功能在以下一种或多种情况下强制用户更改口令：

- 在指定天数以后（日期寿命规则）
- 在指定的登录次数以后（使用次数寿命规则）
- 新用户第一次登录时（口令更改规则）

有关如何针对此功能配置 Cisco Secure ACS 的详细信息，请参阅针对 CiscoSecure 用户数据库启用口令过期。

Q. 当用户使用 LEAP 无线登录时，会获得映射网络驱动器的登录脚本。然而，使用带 PEAP 身份验证的 Wi-Fi Protected Access (WPA) 或 WPA2 时，登录脚本不能运行。与 RADIUS (ACS) 一样，客户端和接入点都是 Cisco。为什么登录脚本在 RADIUS (ACS) 上不能运行？

A. 要想使登录脚本工作，计算机身份验证是必需的。这使无线用户能够在用户登录之前访问网络以加载脚本。

有关如何配置带 PEAP-MS-CHAPv2 的计算机身份验证的信息，请参阅配置带 PEAP-MS-CHAPv2 计算机身份验证的 Cisco Secure ACS for Windows v3.2。

Q. 使用 Cisco Aironet Desktop Utility (ADU) 版本 3.0 后，当用户配置可扩展的认证协议 - 传输层安全 (EAP-TLS) 的计算机身份验证时，ADU 不允许用户创建配置文件。为什么？

A. 这归因于 Cisco Bug ID CSCsg32032（仅限注册用户）。如果客户端 PC 安装了计算机证书且没有用户证书，则会发生这种情况。

解决方法是将计算机证书复制到用户存储，创建 EAP-TLS 配置文件，然后从用户存储删除证书，以便使用仅计算机身份验证的配置。

Q. 有没有办法根据客户端的 MAC 地址在无线 LAN 上分配 VLAN？

A. 不能。无法做到这一点。来自 RADIUS 服务器的 VLAN 分配只能用于 802.1x，而不是 MAC 身份验证。如果在 RADIUS 服务器上验证 MAC 地址（在 LEAP/PEAP 中定义为用户 ID/口令），您可以使用 RADIUS 推送带 MAC 身份验证的 VSA。

相关信息

- 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
- 配置有线等效私密性 (WEP)
- 无线产品支持
- 技术支持和文档 - Cisco Systems