目 录

WLAN 安全

WLAN 安全概述

WLAN 具有安装便捷、使用灵活、经济节约、易于扩展等有线网络无法比拟的优点，但是由于无线局域网信道开放的特点，使攻击者能够很容易的进行窃听，恶意修改，因此安全性成为阻碍无线局域网发展的最重要因素。

802.11 协议提供的无线安全性能可以很好地抵御一般性网络攻击，但是仍有少数黑客能够入侵无线网络，从而无法充分保护包含敏感数据的网络。为了更好的防止未授权用户接入网络，需要实施一种性能高于 802.11 的高级安全机制。

H3C 的 WLAN 安全完全实现了 IEEE802.11 协议以及 WPA 规定的服务的安全标准，而且可以配合的端口安全特性使用，提供更安全的接入保护、更灵活的服务应用组合以适应各种网络需要。

说明

AC 和 FAT AP 支持本文所介绍的所有 WLAN 安全技术，为方便描述，这里以 AC 为例。

链路认证方式

1. 开放系统认证（Open system authentication）

开放系统认证是缺省使用的认证机制，也是最简单的认证算法，即不认证。如果认证类型设置为开放系统认证，则所有请求认证的客户端都会通过认证。开放系统认证包括两个步骤：第一步是请求认证，第二步是返回认证结果。

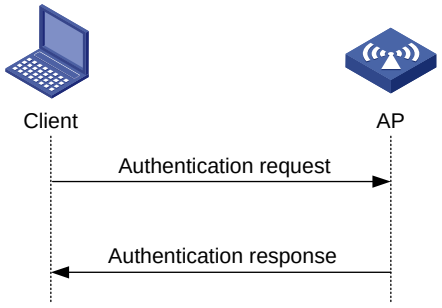

图1 开放系统认证过程

2. 共享密钥认证（Shared key authentication）

共享密钥认证是除开放系统认证以外的另外一种认证机制。共享密钥认证需要客户端和设备端配置相同的共享密钥。

共享密钥认证的认证过程为：客户端先向设备发送认证请求，无线设备端会随机产生一个 Challenge 包（即一个字符串）发送给客户端；客户端会将接收到字符串拷贝到新的消息中，用密钥加密后再发送给无线设备端；无线设备端接收到该消息后，用密钥将该消息解密，然后对解密后的字符串和最初给客户端的字符串进行比较。如果相同，则说明客户端拥有无线设备端相同的共享密钥，即通过了 Shared Key 认证；否则 Shared Key 认证失败。

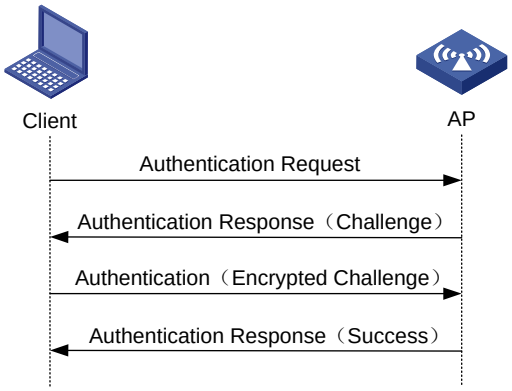

图2 共享密钥认证过程

WLAN 服务的数据安全

相对于有线网络，WLAN 存在着与生俱来的数据安全问题。在一个区域内的所有的 WLAN 设备共享一个传输媒介，任何一个设备可以接收到其他所有设备的数据，这个特性直接威胁到 WLAN 接入数据的安全。

802.11 协议也在致力于解决 WLAN 的安全问题，主要的方法为对数据报文进行加密，保证只有特定的设备可以对接收到的报文成功解密。其他的设备虽然可以接收到数据报文，但是由于没有对应的密钥，无法对数据报文解密，从而实现了 WLAN 数据的安全性保护。目前支持四种安全服务。

(1) 明文数据

该种服务本质上为无安全保护的 WLAN 服务，所有的数据报文都没有通过加密处理。

(2) WEP 加密

WEP（Wired Equivalent Privacy，有线等效加密）用来保护无线局域网中的授权用户所交换的数据的机密性，防止这些数据被随机窃听。WEP 使用 RC4 加密算法来保证数据的保密性，通过共享密钥来实现认证，理论上增加了网络侦听，会话截获等的攻击难度，虽然 WEP104 在一定程度上提高了 WEP 加密的安全性，但是受到

RC4 加密算法、过短的初始向量和静态配置密钥的限制，WEP 加密还是存在比较大的安全隐患。

WEP 加密方式可以分别和 Open system、Shared key 链路认证方式使用。

- 采用 Open system authentication 方式：此时 WEP 密钥只做加密，即使密钥配的不一致，用户也是可以上线，但上线后传输的数据会因为密钥不一致被接收端丢弃。
- 采用 Shared key authentication 方式：此时如果双方密钥不一致，客户端就不能通过 Shared key 认证，无法上线。也就是说，当 WEP 和 Shared key 认证方式配合使用时，WEP 也可以作为一种认证方法。

(3) TKIP 加密

TKIP 是一种加密方法，用于增强 pre-RSN 硬件上的 WEP 协议的加密的安全性，其加密的安全性远远高于 WEP。WEP 主要的缺点在于，尽管 IV（Initial Vector，初始向量）改变但在所有的帧中使用相同的密钥，而且缺少密钥管理系统，不可靠。

TKIP 和 WEP 加密机制都是使用 RC4 算法，但是相比 WEP 加密机制，TKIP 加密机制可以为 WLAN 服务提供更加安全的保护。

首先，TKIP 通过增长了算法的 IV 长度提高了 WEP 加密的安全性。相比 WEP 算法，TKIP 将 WEP 密钥的长度由 40 位加长到 128 位，初始化向量 IV 的长度由 24 位加长到 48 位；

其次，TKIP 支持密钥的动态协商，解决了 WEP 加密需要静态配置密钥的限制。TKIP 使用一种密钥构架和管理方法，通过由认证服务器动态生成分发的密钥来取代单个静态密钥，虽然 TKIP 采用的还是和 WEP 一样的 RC4 加密算法，但其动态密钥的特性很难被攻破；

另外，TKIP 还支持了 MIC 认证（Message Integrity Check，信息完整性校验）和 Countermeasure 功能。当 MIC 发生错误的时候，数据很可能已经被篡改，系统很可能正在受到攻击。此时，可以采取一系列的对策，来阻止黑客的攻击。

(4) CCMP 加密

CCMP(Counter mode with CBC-MAC Protocol，[计数器模式]搭配[区块密码锁链－信息真实性检查码]协议)加密机制是基于 AES（Advanced Encryption Standard，高级加密标准）加密机制的 CCM（Counter-Mode/CBC-MAC，区块密码锁链－信息真实性检查码）方法。CCM 结合 CTR（Counter mode，计数器模式）进行机密性校验，同时结合 CBC-MAC（区块密码锁链－信息真实性检查码）进行认证和完整性校验。CCM 可以保护了 MPDU 数据段和 IEEE 802.11 首部中被选字段的完整性。CCMP 中所有的 AES 处理进程都使用 128 位的密钥和 128 位的块大小。CCM 中每个会话都需要一个新的临时密钥。对于每个通过给定的临时密钥加密的帧来说，CCM 同样需要确定唯一的随机值（nonce）。CCMP 使用 48 位的 PN（packet number）来实现这个目的。对于同一个临时密钥，重复使用 PN 会使所有的安全保证无效。

用户接入认证

(1) PSK 认证

PSK 认证需要实现在无线客户端和设备端配置相同的预共享密钥，如果密钥相同，PSK 接入认证成功；如果密钥不同，PSK 接入认证失败。

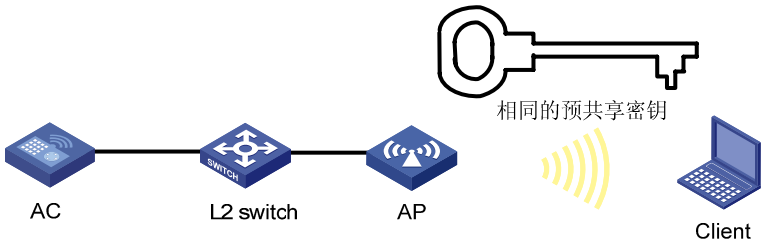

图3 PSK 认证

(2) MAC 接入认证

MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法。通过手工维护一组允许访问的 MAC 地址列表，实现对客户端物理地址过滤，但这种方法的效率会随着终端数目的增加而降低，因此 MAC 地址认证适用安全需求不太高的场合，如家庭、小型办公室等环境。

MAC 地址认证分为以下两种方式：

- 本地 MAC 地址认证：当选用本地认证方式进行 MAC 地址认证时，需要在设备上预先配置允许访问的 MAC 地址列表，如果客户端的 MAC 地址不在允许访问的 MAC 地址列表，将被拒绝其接入请求。

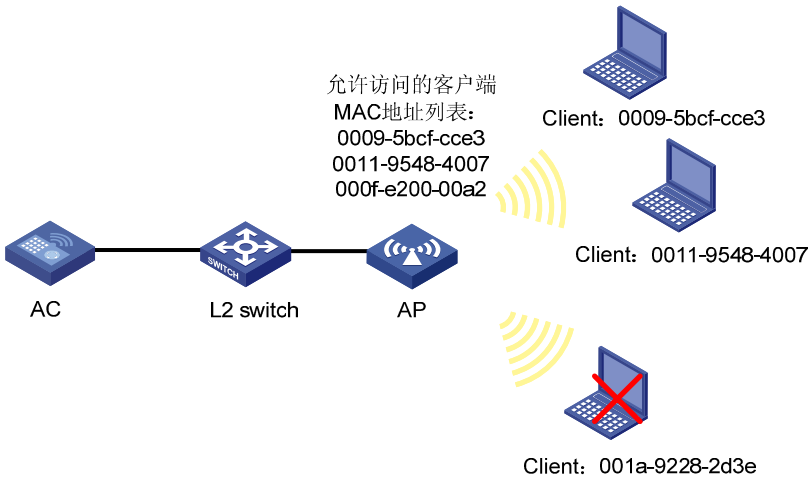

图4 本地 MAC 地址认证

- 通过 RADIUS 服务器进行 MAC 地址认证：当 MAC 接入认证发现当前接入的客户端为未知客户端，会主动向 RADIUS 服务器发起认证请求，在 RADIUS

服务器完成对该用户的认证后，认证通过的用户可以访问无线网络以及相应的授权信息。

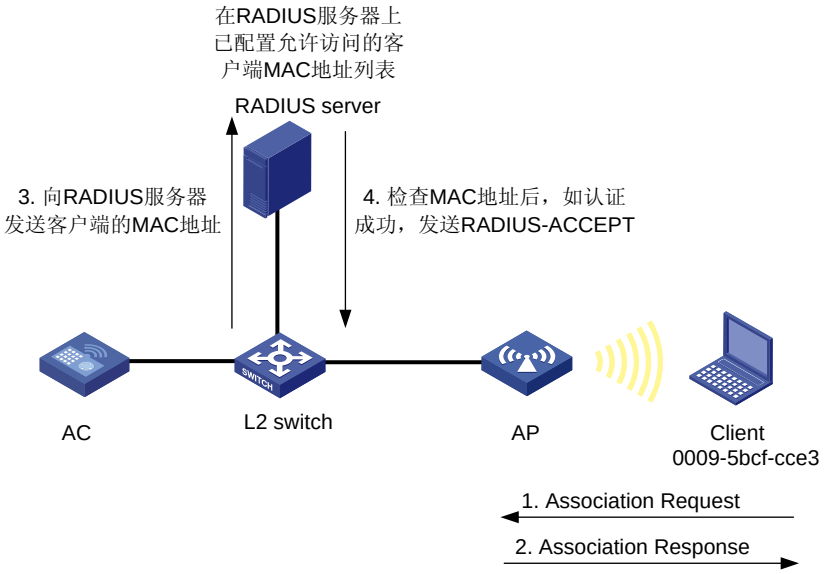

图5 通过 RADIUS 服务器进行 MAC 地址认证

(3) 802.1x 认证

802.1x 协议是一种基于端口的网络接入控制协议，该技术也是用于 WLAN 的一种增加网络安全的解决方案。当客户端与 AP 关联后，是否可以使用 AP 提供的无线服务要取决于 802.1x 的认证结果。如果客户端能通过认证，就可以访问 WLAN 中的资源；如果不能通过认证，则无法访问 WLAN 中的资源。

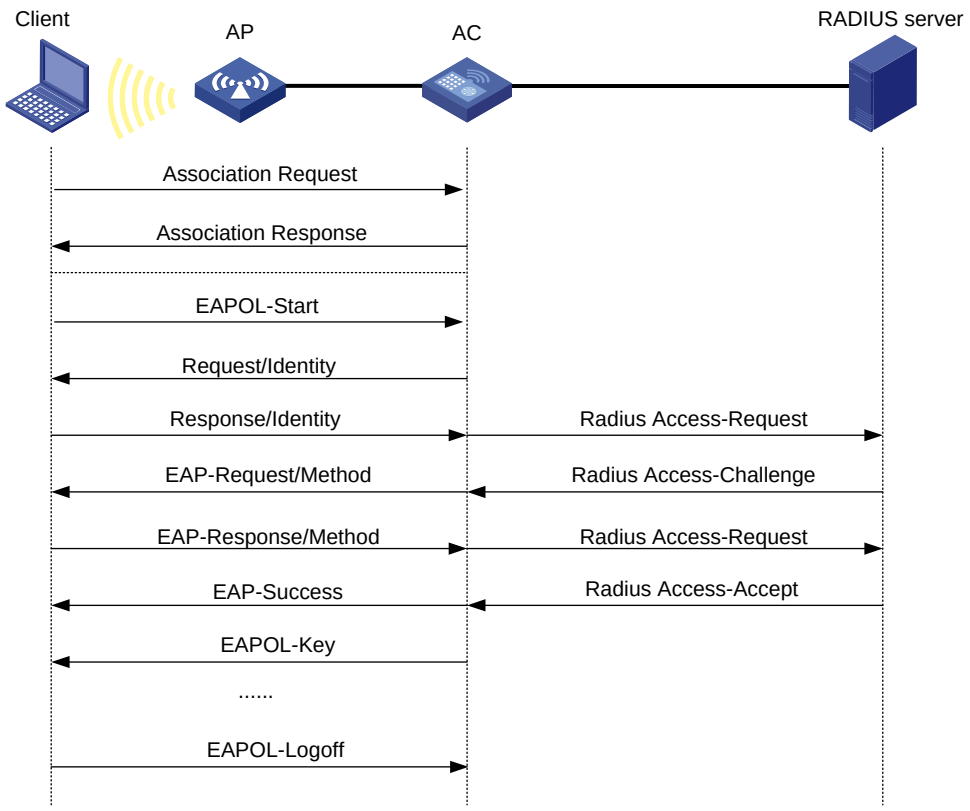

图6 802.1x 认证

WLAN 安全策略

对于小型企业和家庭用户而言，无线接入用户数量比较少，一般没有专业的 IT 管理人员，通常情况下不会配备专用的认证服务器，对于这种对网络安全性的要求相对较低的无线环境下，可采用“WPA-PSK+接入点隐藏”的安全策略来保证安全。

在仓库物流、医院、学校等环境中，考虑到网络覆盖范围以及客户端数量，AP和无线客户端的数量必将大大增加，安全隐患也相应增加，此时简单的WPA-PSK已经不能满足此类用户的需求，可以采用 表 1中的中级安全方案。使用支持IEEE 802.1x认证技术的AP作为无线网络的安全核心，并通过Radius服务器进行用户身份验证，有效地阻止未经授权的用户接入。

在各类公共场合以及网络运营商、大中型企业、金融机构等环境中，有些用户需要在热点公共地区（如机场、咖啡店等）通过无线接入Internet，因此用户认证问题就显得至关重要。如果不能准确可靠地进行用户认证，就有可能造成服务盗用，这种服务盗用会对无线接入服务提供商造成不可接受的损失，表 1中的专业级解决方案可以较好地满足用户需求，通过用户隔离技术、IEEE802.1i、Radius用户认证以及计费方式确保用户的安全。

表1 典型场合下的 WLAN 安全策略

安全级别	典型场合	安全策略
初级安全	小型企业，家庭用户等	WPA-PSK＋接入点隐藏
中级安全	仓库物流、医院、学校、餐饮娱乐	IEEE802.1x认证＋TKIP加密
专业级安全	各类公共场合及网络运营商、大中型企业、金融机构	用户隔离技术＋IEEE802.11i＋Radius认证和计费（对运营商）