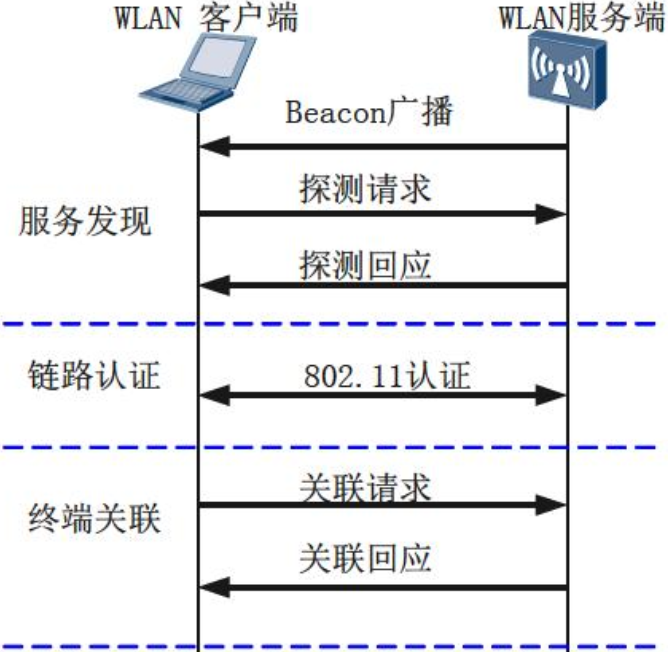
**WLAN的安全共分为三个方面：**

* STA身份验证：对客户端的认证，只有通过认证后，才能进入后续的关联阶段。
* 数据加密：对数据报文进行加密，保证只有特定的设备才可以对接收到的报文成功解密，无线网络中的其他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WLAN数据的安全性保护。
* 用户身份验证与加密：对用户身份进行区分，并在用户访问网络前限制其访问权限。使用户在进行链路认证使只允许有限的网络访问权限，只有确定用户身份后才会允许完整的网络访问。

**概述**

可以简单地将WLAN组网分成客户端和WLAN服务端两部分，WLAN客户端为有无线网卡的主机设备，而WLAN服务端则为AP设备。

下图简单描述了客户端接入到WLAN服务的协议过程。



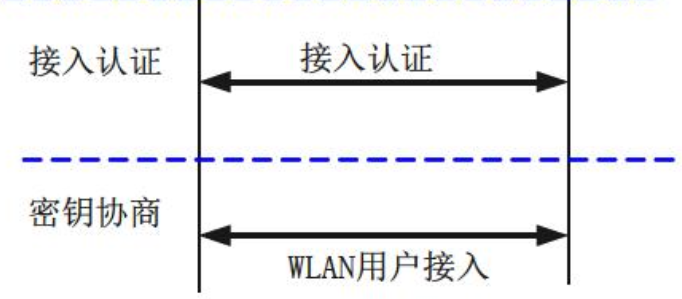


图1-1 WLAN用户接入

1. WLAN服务发现

使用任何网络之前，首先必须找出网络何在。使用有线网络，要找出网络所在并不难，只要循着网线或者找到墙上的插座即可。在无线领域中，STA加入任何无线网络之前，必须先经过一番辨识工作。这种于所在区域辨识现有网络的程序称为WLAN服务发现过程。

---WLAN服务端主动发送Beacon通告提供WLAN服务，客户端可以根据该报文确定周围存在的WLAN服务。

---WLAN客户端可以指定SSID（WLAN服务的标识）或者使用广播SSID（即没有指定SSID）主动地探测是否存在指定的网络，WLAN服务端存在指定的WLAN服务，会发送确认信息给客户端。

服务发现成功后进入链路认证过程。

1. 链路认证

只要工作站打算连接网络，就必须进行802.11“身份认证”。

当前802.11的链路认证支持两种认证方式：开放认证（open System Authentication）和Shared-key认证（SharedKey Authentication）。两种认证方式都是在802.11中定义，802.11链路认证通过Authentication报文实现。

1. 终端关联

一旦完成身份认证，STA就可以跟基站进行；连接（或者跟新的基站进行重新连接），以便获得网络的完全访问权。

在WLAN服务发现过程中，WLAN客户端已经获得了当前服务的配置和参数（WLAN服务端会在Beacon和Probe Response报文中携带，例如接入认证算法以及加密密钥）。WLAN客户端发起的Association或者Re-association请求时，会携带WLAN客户端自身的各种参数，以及根据服务配置选择的各种参数（主要包括支持的速率，支持的信道，支持的QoS的能力，以及选择的接入认证和加密算法）。

1. 接入认证

用户接入认证实现了对接入用户的身份认证，为网络服务提供了安全保护。接入认证主要有802.1X认证、PSK认证、Portal认证、MAC认证等方式。其中802.1X接入认证、MAC接入认证、Portal认证可以支持对有线用户和WLAN无线接入用户进行身份认证，而PSK认证则是专门为WLAN无线用户提供认证的一种方法。

WLAN服务应用中，对于WPA（Wi-Fi Protected Access）用户或者WPA2用户需要进行EAPOL-Key密钥协商。根据WLAN协议服务定义，对于WPA服务，需要和802.1X接入认证以及PSK接入认证配合使用：在802.11链路协商的过程中，可以确定用户使用的接入认证算法；并且在链路协商成功后触发对用户的接入认证；随后需要为该接入用户协商密钥；之后WLAN客户端才可以访问WLAN网络。

1. 密钥协商

密钥协商为数据安全提供有力保障，为了保证WLAN数据的安全，IEEE 802.11i和IEEE 802.1X 定义了EAPOL-Key密钥协商机制（也称4-Way Handshake），WLAN就是用该机制实现WLAN服务端和WLAN客户端的密钥协商，协商出来的密钥将作为802.11数据传输过程中的加密/解密密钥。

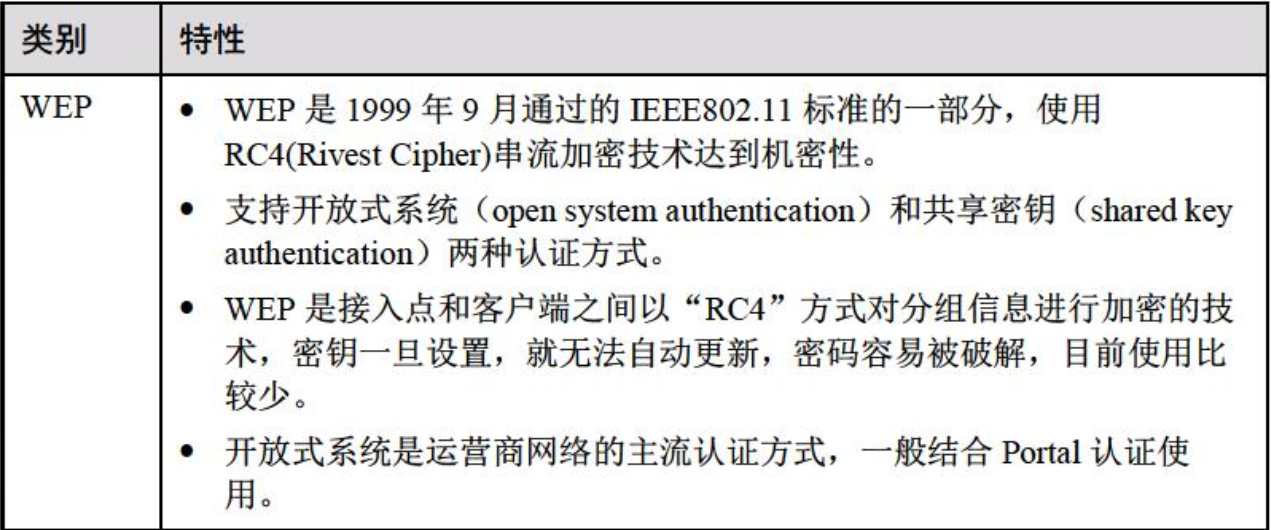
对于支持WPA和RSN（robust security network）服务的WLAN，需要进行EAPOL-Key 密钥协商。协商过程在逻辑上可以看做接入认证的一部分，所以只有在EAPOL-Key密钥协商成功以后，接入认证才会打开端口，允许用户的报文通过。

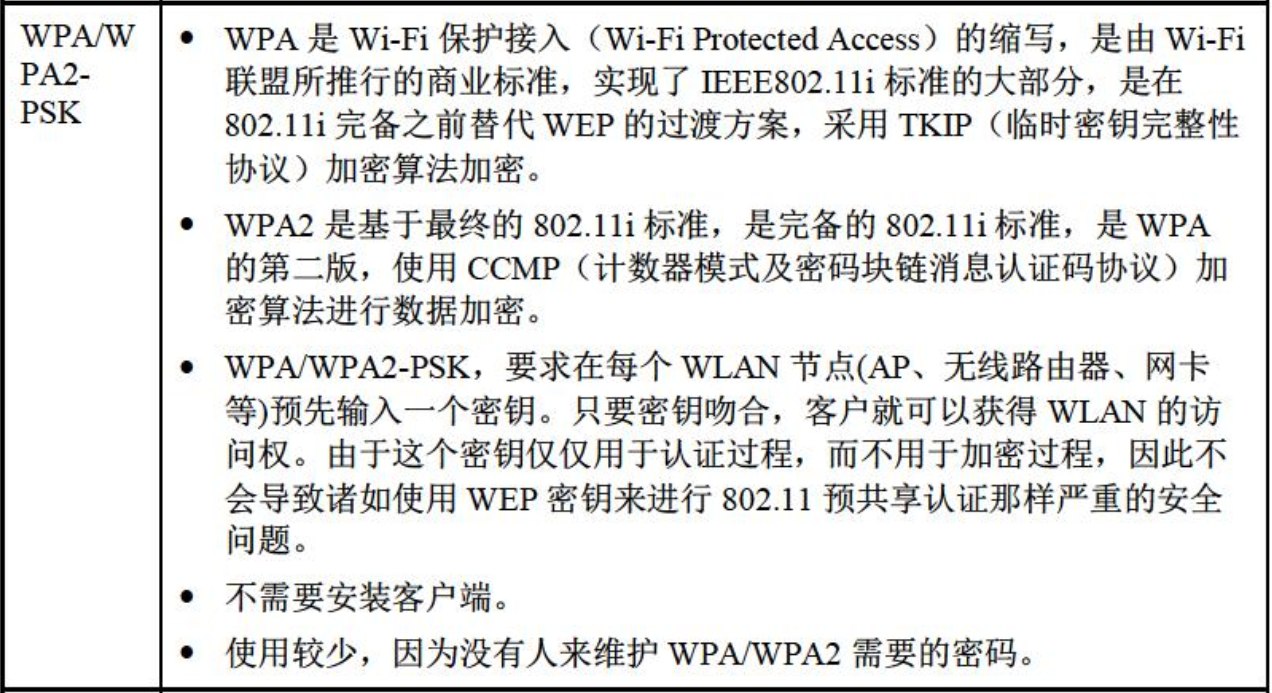
WLAN密钥协商主要包括四次握手密钥协商和组密钥协商过程，这两种密钥协商都通过EAPOL-Key报文协商实现。WLAN客户端和WLAN服务端使用四次握手机制协商该客户端的单播数据报文使用的密钥，而WLAN服务端可以通过组密钥协商过程将广播和组播使用的密钥通知所有的WLAN客户端。

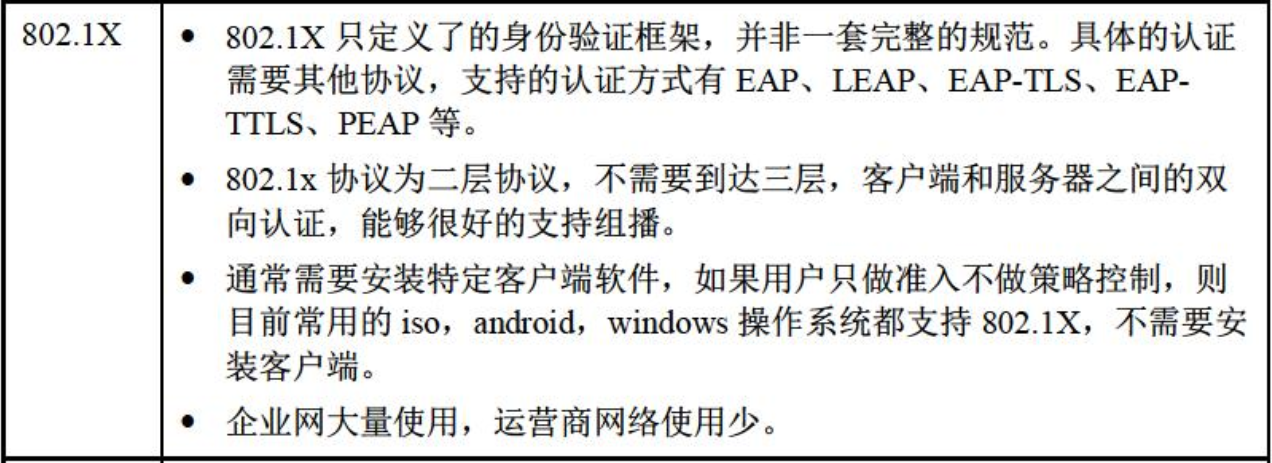
1. 数据加密

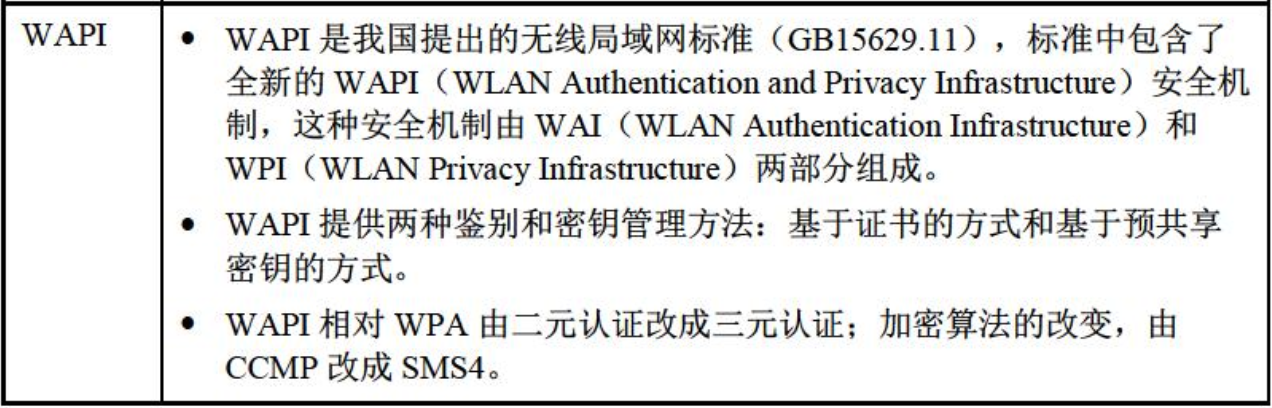
使用者身份确定无误并赋予访问权限后，网络必须保护用户所传送的数据不被窥视。保护无线链路数据的私密性，是所有无线网络需要面对的挑战。数据的私密性通常是靠加密协议来达成，只允许拥有密钥并经过授权的用户访问数据，确保数据在传输过程中未遭篡改。

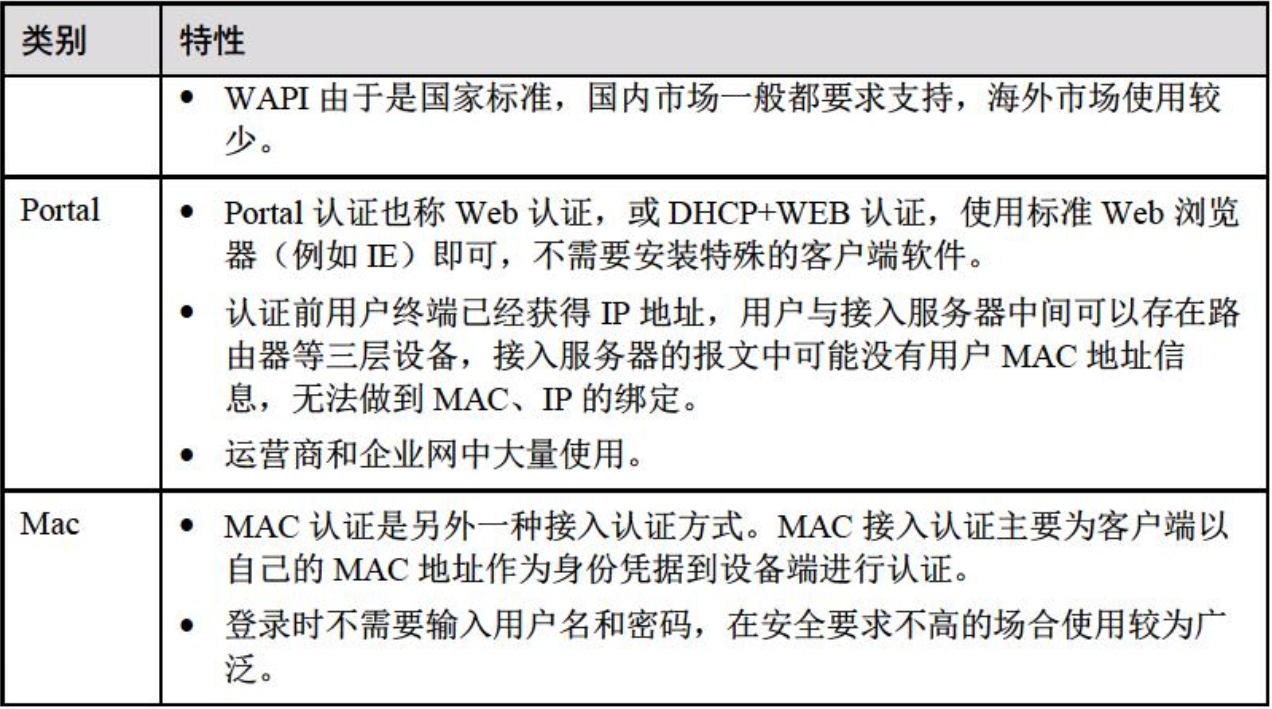
表1-1 华为WLAM认证加密特性











**1.2.2 STA 身份验证**

802.11标准要求STA在打算连接到网络时，必须进行802.11“链路认证”。由于这种认证并没有传递或者验证任何加密密钥，也没有进行相互认证过程，所以可以将这个链路认证视为STA连接到WLAN网络时握手过程的起点。

STA身份认证主要有两种方式：开放式和共享密钥式。有些产品也可以提供MAC地址过滤功能，可以在身份认证阶段过滤掉未授权的STA的MAC地址。

**开放系统认证（Open system authentication）**

开放系统认证是802.11要求必备的一种方法。在这种方式下，接入点并未验证STA的真是身份，STA以MAC地址作为身份证明，这种验证方式可以让所有符合802.11标准的终端都可以接入到WLAN网络中来。开放系统身份验证比较适合有众多用户的运营商部署的大规模的WLAN网络。

开放系统认证只有两个步骤，只确认AP和网卡采用了相同的鉴权方式，不对WEP加密密钥进行验证。认证过程如下图：

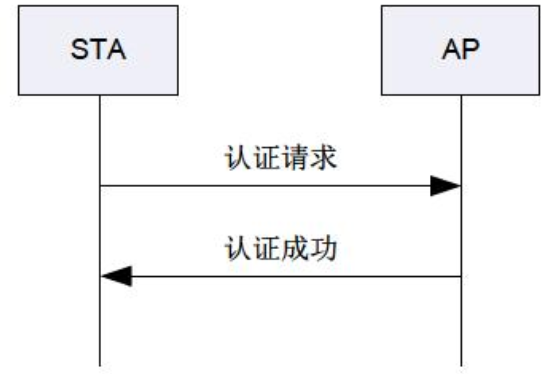


图1-2 开放系统认证过程

开放系统认证的过程为：

1. STA发送一个认证请求给选定的AP。
2. 该AP发送一个认证成功响应报文给客户端确认该认证并在AP上注册客户端。

开放系统验证的优缺点：

* 优点：开放认证是一个基本的验证机制，可以使用不支持复杂的认证算法的无线设备。802.11协议中认证是面向连接的，对于需要允许设备快速进入网络的场景，可以使用开放式身份认证。
* 缺点：开放认证没办法检验客户端是否是一个有效的客户端，而不是黑客客户端。如果使用不带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。

**共享密钥认证（Shared-key authentication）**

共享密钥认证是除开放系统认证外的另一种链路认证机制。

共享密钥认证必须使用WEP加密方式，要求STA和AP使用相同的共享密钥（key），通常被称为静态WEP密钥。认证过程包含4不，后三步包含了一个完整的WEP加密/解密过程（框架与CHAP）类似，对WEP加密的密钥进行了验证，确保网卡在发起关联时与AP配置了相同的加密密钥。共享密钥的认证过程如下图所示：

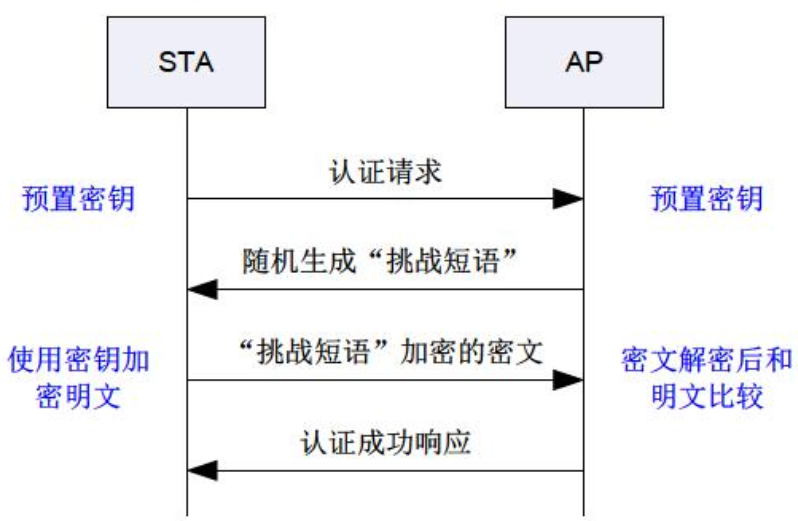


图1-3 共享密钥认证过程

共享密钥的认证过程为：

1. STA先向AP发送认证请求。
2. AP会产生一个“挑战短语”发送给STA。
3. STA会将收到的“挑战短语”拷贝到新的消息中，用密钥加密后再发送给AP。
4. AP接收到消息后，用密钥将该消息解密，然后对解密后的字符串和最初给STA的字符串进行比较。

-如果相同，则说明STA拥有与AP相同的共享密钥，即通过了共享密钥认证。

-如果不同，则共享密钥认证失败。

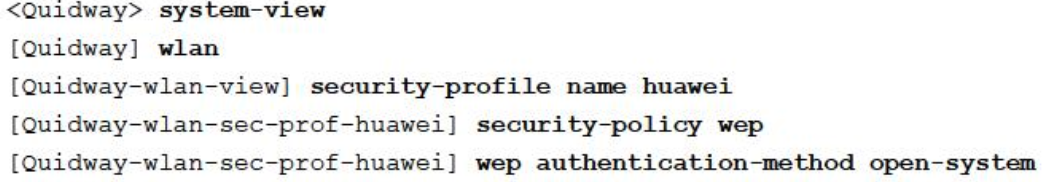
共享密钥认证的优缺点：

* 优点：由于采用了WEP加密方式对密钥进行保护，空口密钥数据不再明文传输，提供比开放认证更安全的认证机制。
* 缺点：

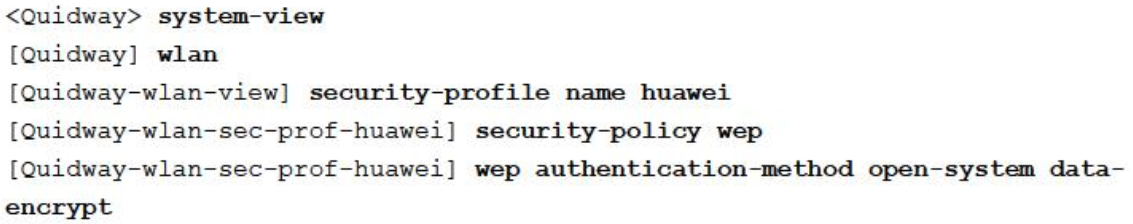
1. 可扩展性不佳，因为必须在每台设备上配置一个很长的密钥字符串。
2. 不是很安全，静态密码的使用时间非常长，直到手工配置了新密码为止。密钥的使用时间越长，恶意用户便有更长的时间来收集从它派生出来的数据，并最终通过逆向工程破解密码。静态WEP密钥是比较容易被破解的。

早期WLAM常用的加密方式是WEP。不需要认证的系统称为开放式系统，需要认证的系统称为共享密钥系统。但不管是哪种系统，都可以选择是否加密。WEP认证加密支持一下组合方式：

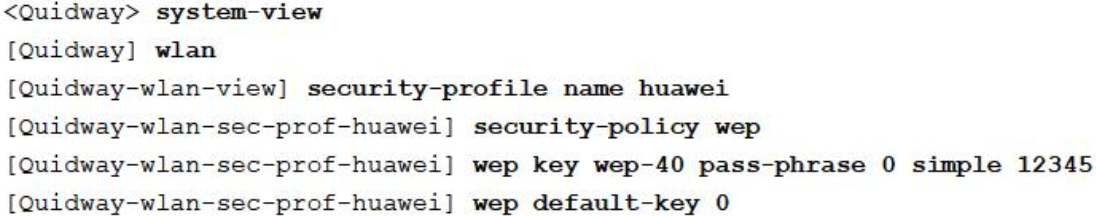
* 开放+明文，具体配置如下：



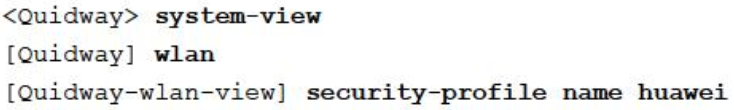
* 开放+密文，具体配置如下：

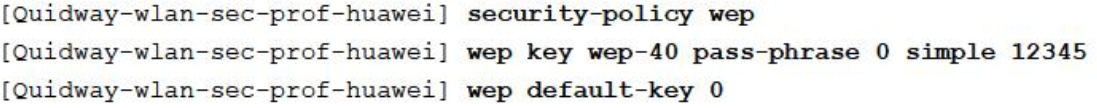


* 共享密钥+明文，具体配置如下：



* 共享密钥+密文，具体配置如下：





配置和管理静态密码非常复杂，因此一些产品支持动态WEP，即在开放系统下，采用802.1X认证来协商密钥。但由于WEP本身安全性差，且动态WEP和WPA流程类似，反而不如直接使用WPA，因此动态WEP现在已经基本不再使用。动态WEP的组合方式为：开放+802.1X+密文。

**MAC地址过滤**

网络上各个AP均有一份访问WLAN网络的MAC地址列表（白名单），也可以有一份禁止访问WLAN网络的MAC地址列表（黑名单）。根据事先配置的策略，可以只允许白名单的MAC接入，或者只禁止黑名单中的MAC地址接入。

MAC地址过滤与其说是一种认证方式，更应该是一种访问控制方式。由于MAC地址很容易被伪造或者复制，这种身份验证方法不建议单独使用，除非一些旧设备无法提供更好的机制。

STA的黑名单配置如下：



STA的白名单配置如下：

**1.2.3用户身份验证与加密**

相对于简单地STA身份验证机制，用户身份验证可谓是一大进步，体现在：

* 在进行链路认证时只允许有限的网络访问，只有确定用户身份后才允许完整的网络访问。
* 可以对用户进行区分并在用户访问网络之前限制访问权限。
* 对于网络协议而言，链路层认证可以配合任何网络层协议使用。

用户身份验证主要包括以下几大方面：

* WPA/WPA2-PSK认证
* 802.1X认证
* WAPI认证
* Portal认证
* MAC认证

**WPA-PSK认证**

WPA-PSK是一种通过Pre-shared key进行认证，并以Pre-shared key 作为PMK协商临时密钥的认证加密方式。

WPA-PSK要求在STA侧预先配置Key，通过与AP或AC侧的4次握手协商协议来验证STA侧Key的合法性。

WPA-PSK加密在STA与AP间的认证和关联过程中采用与Open的WEP方式一致，STA与AP关联成功后，进入四步握手协商密钥过程。

四次握手过程主要是为了产生PTK（Pairwise Transient Key）和GTK（Group Temporal Key），PTK用来加密单播无线报文，GTK用来加密组播和广播无线报文。

在802.11i里面定义了两种密钥层次模型，一种是成对密钥层次结构，主要用来描述一对设备之间的所有密钥；一种是租密钥层次结构，主要用来描述全部设备所共享的各种密钥。

在成对层次密钥结构下，TKIP加密方式根据主密钥衍生出四个临时密钥，每个临时密钥128比特，这四个key分别是EAPOL-Key-Encryption-key、EAPOL-Key-Integrity-key、Data-Encryption-Key、Data-Integrity-Key，前面两个EAPOLMIC密钥和EAPOL加密密钥用于在初始化握手信息过程中保护WLAN客户端可WLAN服务端的通信，后面两个用在WLAN客户端和WLAN服务端的加密数据和加密数据不被更改。对于CCMP加密的方式下，衍生出的临时密钥只有三个，因为数据的完整性和加密密钥是同一个。

在组密钥层次结构下，TKIP的加密方式根据GMK（128比特）衍生出两个密钥，用来WLAN客户端和WLAN服务端之间的多播数据加密和完整性加密。而CCMP的方式数据加密和数据MIC密钥组合成一个密钥用来多播数据加密和完整性加密。

* 四次单播密钥协商过程

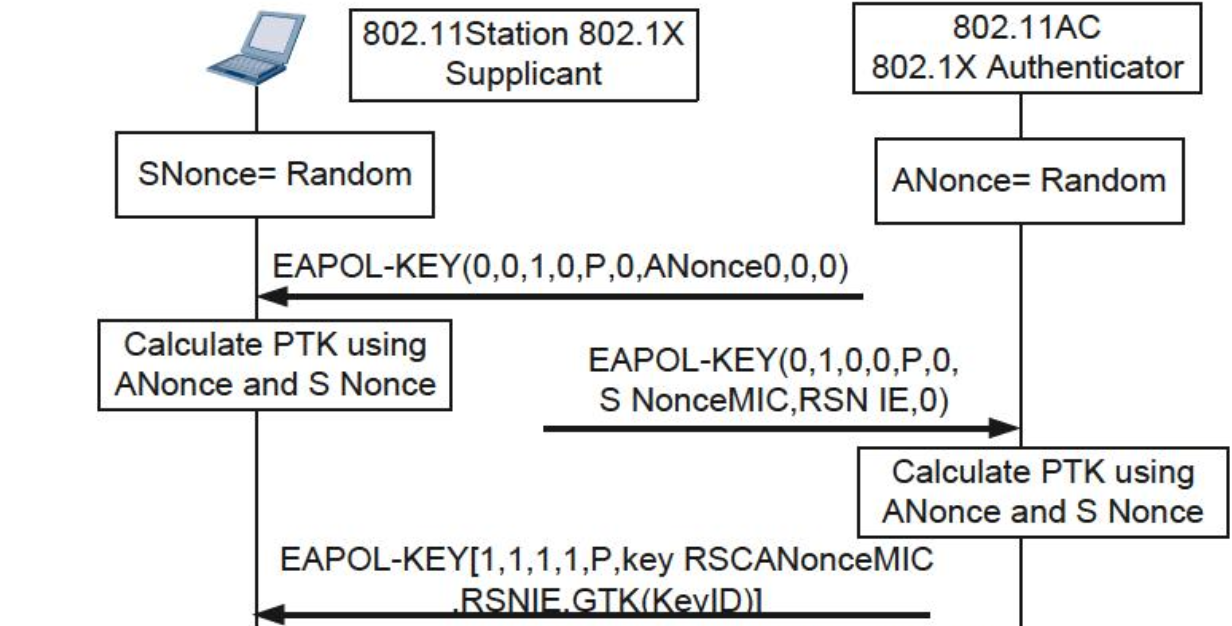




图1-4 EAPOL-key单播密钥协商

如题1-4所示，EAPOL-Key单播密钥协商流程说明如下：

1. WLAN服务端发送EAPOL-Key帧给WLAN客户端，帧中包含随机数Anonce（nonce是为了防止重放攻击的随机值，包含Anonce和Snonce两种，区别在于Anonce是AC随机产生并发送给STA，Snonce是STA收到Anonce后随机产生的）。
2. WLAN客户端根据PMK、ANonce、SNonce、自己的MAC地址、WLAN服务端的MAC地址计算出PTK，WLAN客户端发送EAPOL-Key帧给WLAN服务端，帧中包含Snonce、RSN信息元素、EAPOL-Key帧的消息完整码（MIC）。
3. WLAN服务端根据PMK、ANonce、SNonce、自己的MAC地址、WLAN服务端的MAC地址计算出PTK，并校验MIC，核实WLAN客户端的PMK是否和自己的一致。
4. WLAN服务端发送EAPOL-Key帧给WLAN客户端，并通知WLAN客户端安装密钥，帧中包含Anonce、RSN信息元素、帧MIC、加密过的GTK。
5. WLAN客户端发送EAPOL-Key帧给WLAN服务端，并通知WLAN服务端已经安装并准备开始使用加密密钥。WLAN服务端收到后本端安装加密密钥。