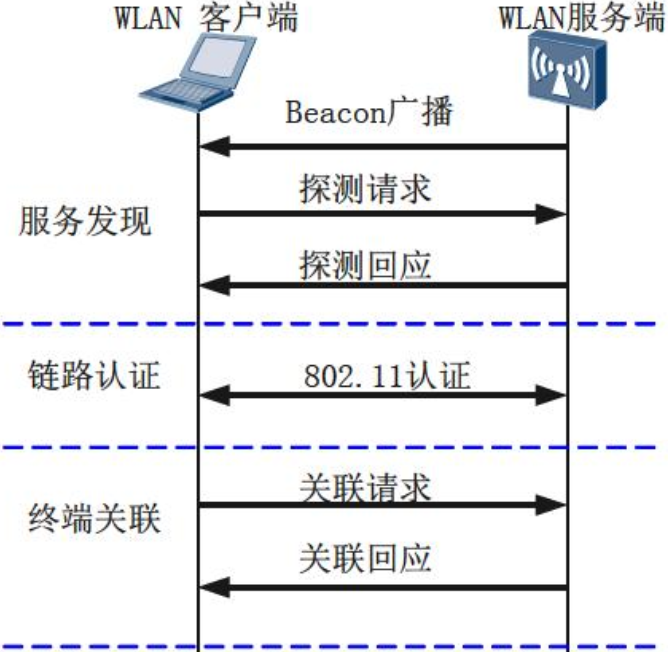
**WLAN的安全共分为三个方面：**

* 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。



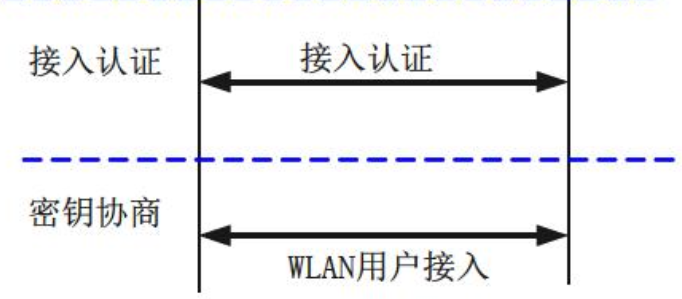


图1-1 WLAN用户接入

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

