集中在一台服务器中作出有关鉴别和接入（通常是敏感）的决定，降低了 AP 的成本和复杂性。802.11i 运行分为 4 个阶段：

1）发现。在发现阶段，AP 通告它的存在以及它能够向无线客户结点提供的鉴别和加密形式。客户则请求它希望的特定鉴别和加密形式。尽管客户和 AP 已经交换了报文，但该客户还没有被鉴别，也还没有加密密钥，因此在该客户能够通过无线信道与任何远程主机通信之前，还需要进行几个其他步骤。

2）相互鉴别和主密钥（MK）生成。鉴别发生在无线客户和鉴别服务器之间。在这个阶段，接入点基本是起中继的作用，在客户和鉴别服务器之间转发报文。**可扩展鉴别协议**（Extensible Authentication Protocol，EAP）［RFC 3748］定义了客户和鉴别服务器之间交互时简单的请求/响应模式中使用的端到端报文格式。如图 8-32 中所示，EAP 报文使用 EAPoL（EAP over LAN，［IEEE 802.1x］）进行封装，并通过 802.11 无线链路发送。这些 EAP 报文在接入点拆封，然后再使用 RADIUS 协议重新封装，经 UDP/IP 传输到鉴别服务器。尽管 RADIUS 服务器和协议［RFC 2865］并不为 802.11i 所要求，但它们是 802.11i 的事实上的标准组件。最近标准化的 DIAMETER 协议［RFC 3588］很可能在不久的将来替代 RADIUS。

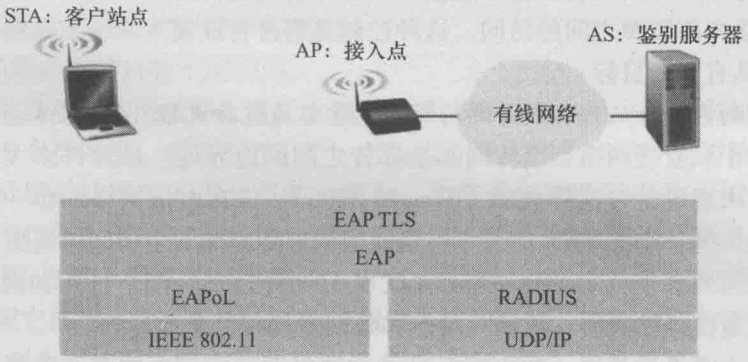

图 8-32　EAP 是一个端到端协议。EAP 报文使用 EAPoL（运行在客户和接入点之间的无线链路上）封装，并使用 RADIUS（运行在接入点和鉴别服务器之间的 UDP/IP 上）

使用 EAP，鉴别服务器能够选择若干方式中的一种来执行鉴别。802.11i 虽未强制一种特殊的鉴别方法，但经常使用 EAP-TLS 鉴别方案［RFC 5216］。EAP-TLS 使用类似于我们在 8.3 节中研究的公钥技术（包括不重数加密和报文摘要），以允许客户和鉴别服务器彼此相互鉴别，并导出为双方所知的一个主密钥。

3）成对主密钥（Pairwise Master Key，PMK）生成。MK 是一个仅为客户和鉴别服务器所知的共享密钥，它们都使用 MK 来生成一个次密钥，即成对主密钥（PMK）。鉴别服务器则向 AP 发送该 PMK。这正是我们所希望达到的目的！客户和 AP 现在具有一个共享的密钥（前面讲过在 WEP 中根本不涉及密钥分发的问题），并彼此相互鉴别。它们此时已经快要能发挥效用了。

4）临时密钥（Temporal Key，TK）生成。使用 PMK，无线客户和 AP 现在能够生成附加的、将用于通信的密钥。其中的关键是临时密钥，TK 将被用于执行经无线链路向任意远程主机发送数据的链路级的加密。

802.11i 提供了几种加密形式，其中包括基于 AES 的加密方案和 WEP 加密的强化版本。