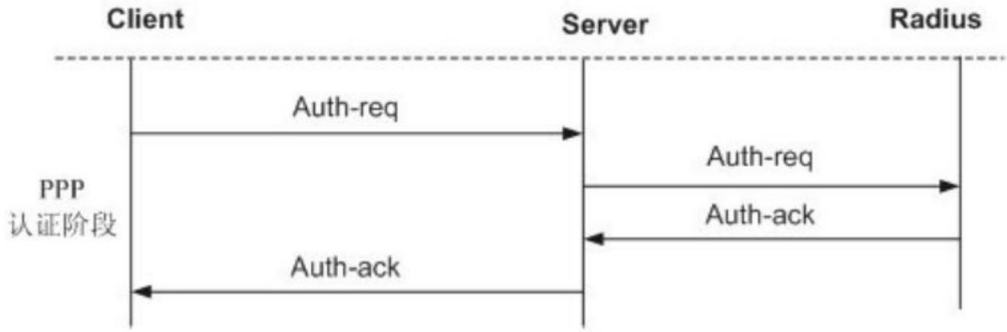
## 认证阶段

- PAP 认证

  PAP 为两次握手协议，它通过用户名及口令来对用户进行验证。PAP 验证过程如下：当两端链路可相互传输数据时，被验证方发送本端的用户名及口令到验证方，验证方根据本端的用户表（或 Radius 服务器）查看是否有此用户，口令是否正确。如正确则会给对端发送 Authenticate-ACK 报文，通告对端已被允许进入下一阶段协商；否则发送 NAK 报文，通告对端验证失败。此时，并不会直接将链路关闭。只有当验证不过次数达到一定值（缺省为 10）时，才会关闭链路。PAP 的特点是在网络上以明文的方式传递用户名及口令，如在传输过程中被截获，便有可能对网络安全造成极大的威胁。因此，它适用于对网络安全要求相对较低的环境。

  用户发送认证端发验证请求报文、并且接收到 ME 设备回应认的证成功报文后，表示 PAP 认证已经成功。否则 ME 设备会回应认证失败报文，通知用户认证不成功。

  图 3 PAP 认证流程




- CHAP 认证

  CHAP 为三次握手协议。只在网络上传输用户名，并不传输用户口令，因此它的安全性要比 PAP 高。CHAP 的验证过程为：首先由验证方向被验证方发送一些随机产生的报文，并同时将本端的主机名附带上一起发送给被验证方。被验证方接到对端对本端的验证请求(Challenge)时，便根据此报文中验证方的主机名和本端的用户表查找用户口令字，如找到用户表中与验证方主机名相同的用户，便利用报文 ID、此用户的密钥用 Md5 算法生成应答（Response），随后将应答和自己的主机名送回。验证方接到此应答后，用报文 ID、本方保留的口令字（密钥）和随机报文用 Md5 算法得出结果，与被验证方应答比较，根据比较结果返回相应的结果（ACK or NAK）

  - 接受认证端发送 Challenge