



- (1)远端系统 Host 发起呼叫连接请求;
- (2)Host 和 LAC 端 (RouterA) 进行 PPP LCP 协商;
- (3)LAC 对 Host 提供的用户信息进行 PAP 或 CHAP 认证;
- (4)LAC 将认证信息 (用户名、密码) 发送给 RADIUS 服务器进行认证;
- (5)RADIUS 服务器认证该用户, 如果认证通过, LAC 准备发起 Tunnel 连接请求;
- (6)LAC 端向指定 LNS 发起 Tunnel 连接请求;
- (7) 在需要对隧道进行认证的情况下, LAC 端向指定 LNS 发送 CHAP challenge 信息, LNS 返回该 challenge 响应消息 CHAP response, 并发送 LNS 侧的 CHAP challenge, LAC 返回该 challenge 的响应消息 CHAP response;
- (8) 隧道验证通过;
- (9)LAC 能将用户 CHAP response、response identifier 和 PPP 协商参数传送给 LNS;
- (10) LNS 将接入请求信息发送给 RADIUS 服务器进行认证;
- (11) RADIUS 服务器认证该请求信息, 如果认证通过则返回响应信息;
- (12) 若用户在 LNS 侧配置强制本端 CHAP 认证, 则 LNS 对用户进行认证, 发送 CHAP challenge, 用户侧响应 CHAP response;
- (13) LNS 再次将接入请求信息发送给 RADIUS 服务器进行认证;
- (14) RADIUS 服务器认证该请求信息, 如果认证通过则返回响应信息;
- (15) 验证通过, LNS 会给远端用户分配一个企业网内部 IP 地址, 用户即可以访问企业内部资源。