含在 Windows 2000 中；通过 RADIUS，AP 接收身份验证请求，并将请求转发给 RADIUS 服务器，由这台服务器来根据 Active Directory 对用户进行身份验证。 802.1x 在身份验证时并不使用有线等效隐私（Wired Equivalent Privacy，WEP）；作为替代，它使用行业标准的可扩展身份验证协议（Extensible Authentication Protocol，EAP）或更新的版本。在任何一种情况下，EAP/PEAP 都拥有其独特的优势：它们允许选择身份验证方法。在默认情况下，802.1x 使用EAP-TLS (EAP-传输层安全性)，此时所有EAP保护的流量都由TLS协议（非常类似于SSL）进行加密。整个身份验证的过程是这样的： 1.无线工作站尝试通过非控制端口连接到AP。（由于此时该工作站还没有通过身份验证，因此它无法使用控制端口）。该AP向工作站发送一个纯文本质询。 2.作为响应，工作站提供自己的身份证明。 3.AP 将来自工作站的身份信息通过有线 LAN 转发给使用 RADIUS 的认证者。 4.RADIUS服务器查询指定帐户，确定需要何种凭证（例如，您可能将您的RADIUS服务器配置为仅接受数字证书）。该信息转换成凭证请求，返回到工作站。 5.工作站通过AP上的非控制端口发送它的凭证。 6.RADIUS 服务器对凭证进行验证；如果通过验证，则将身份验证密钥发送给AP。这个密钥是加密的，因此只有AP能够对其进行解密。 7.AP 对密钥进行解密，并用它来为工作站创建一个新的密钥。这个新的密钥将被发送给工作站，它被用来加密工作站的主全局身份验证密钥。 定期的，AP 会生成新的主全局身份验证密钥，并将其发送给客户端。这很好地解决了802.11中长寿命固定密钥的问题，攻击者能够很容易地通过暴力破解来攻击固定密钥。 100Test 下载频道开通，各类考试