

WindowsXP系统中如何部署802.1X计算机等级考试 PDF转换  
可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/580/2021\\_2022\\_WindowsXP\\_E7\\_c98\\_580472.htm](https://www.100test.com/kao_ti2020/580/2021_2022_WindowsXP_E7_c98_580472.htm) 802.11 WLAN 协议并不是非常安全，而且您也做不了什么。但幸运的是，IEEE（以及Microsoft、Cisco和其他行业领先的公司）发现了802.11的缺陷；其结果是，IEEE 802.1x标准为无线局域网（WLAN）和普通局域网提供了一套坚固得多的身份验证和安全性机制。您可以使用Windows 2000或Windows Server 2003域控制器和Windows XP客户端的组合，来部署802.1x。802.1x是如何工作的 802.1x实施基于端口的访问控制。在WLAN中，端口就是访问点（AP）和工作站之间的连接。在802.1x中拥有两种类型的端口：非控制的和控制的。您现在正在使用的可能就是非控制端口：它允许设备连接到端口，与其他任何网络设备进行通讯。相反，控制端口限制了连接设备所能够通讯的网络地址。您可能已经能够了解到接下来是什么情况了：802.1x允许所有的客户端连接到控制端口，但是这些端口仅将流量发送给身份验证服务器。在客户端通过身份验证以后，才被允许开始使用非控制端口。802.1x的奥秘在于非控制和控制端口是并存于同一个物理网络端口上的逻辑设备。针对身份验证，802.1x进一步为网络设备定义了两种角色：申请者（supplicant）和认证者（authenticator）。申请者是一个请求访问网络资源的设备（例如配备了802.11b网卡的膝上型计算机）。认证者是对申请者进行身份验证的设备，由它来决定是否授予申请者访问权限。无线AP可以作为认证者；但是使用行业标准的远程身份验证拨入用户服务(RADIUS)协议更灵活一些。这个协议包

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

题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)