 提到无线网络，尤其是关于小区“ 蹭网族 ”的报道，大部分的用户都会怀疑无线网络的安全性，据了解，由于无线网络的便捷性，越来越多的家庭开始使用无线路由器上网，“ 蹭网族 ”随之迅速壮大。用户声称无线安全是他们优先考虑的因素，尤其作为企业中的无线网络，由于许多企业网络管理员在实施无线网络的过程中并没有安装所有的安全选项。他们往往会认为无线易于安装，却难以确保安全并且不易管理。 在无线网络上，每一个接入点都可以根据不同的用户要求设置不同的安全级别。它是一种严格基于身份认证的网络，并且更难被利用。无线网络希望用户能够通过提供密码、数字证书或者生物识别例如拇指指纹来证明身份。该系统将与AAA (即鉴别、授权、记帐)服务器进行比对，确认你就是公司内部的成员，才获准进入，否则，将无法共享企业中的无线网络资源。 很多人会说：“ 如果遭遇身份盗窃或者设备盗窃该如何处理?最近的新闻提到俄罗斯ElcomSoft公司采用Nvidia显卡将无线密码恢复的时间提高了100倍，对此有何看法?这些方式是否还不足以保证网络的安全? ”来源：考试大 加密技术只是保证无线网络安全的的一个重要因素。ElcomSoft提及破解WPA 或者WPA2时，它确实意味着通过“ 暴力 ”攻击着恢复WPA-PSK的密码。这并不是新技术。你需要对比一下8位数(PSK要求至少8位)密码，它有 208，827，064，576种变化。在这种情况下，就需要花至少345天来找出一个没有任何规律

可循的密码。如果设置9位数密码的话，你大概要寻找 25年。而WPA-PSK最多可以设置有64个字符的密码。一旦你验证了该用户，你如何为该用户验证其网络，以确保该网络的真实性?无线系统将向你的设备出示其证书，以确认你正在登录的网络是真实有效的。来源：www.examda.com 无线网络另一层保险是授权证书。无线网络的资源是被锁定的，所以当你在网络上漫游的时候，每当你从一个新接入点移动到一个新区域，它将检查确认你的访问权限。接入点还会记录每一次行动，并实时将信息发送到服务器上，以尽量减少违反安全的行为。比如访客获得了他们不应该访问的内容，并对安全规章的遵从情况进行审核跟踪。 除了设备本身的安全以外，有线网络关注所有物理层面的问题，把网络安全寄托于你办公室的前台十分危险。人们是可以越过安全防御的，但是如果使用无线网络，一旦你没有相应的证明网络就会立即阻止你登入。大多数解决方案很少或者不能管理访客连上访客网络去了解时间、地点以及访客网是如何使用的。并非所有的设备都支持802.11i安全，因此对企业网络资源的访问必须加以限制。 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