

四步安全设置保护WiFi网络思科认证 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/644/2021_2022__E5_9B_9B_E6_AD_A5_E5_AE_89_E5_c101_644145.htm WEP使用的加密密钥包括收发双方预先确定的40位（或者104位）通用密钥，和发送方为每个分组信息所确定的24位、被称为IV密钥的加密密钥。由于加强了生成加密密钥的算法，因此即便收集到分组信息并对其进行解析，也几乎无法计算出通用密钥。

- 1)在您浏览器中为路由器的IP地址分类 怎么通过管理系统，你必须查看你的路由器的IP地址(一般为192.168.0.1)和路由器的默认口令，而现在路由器操作界面都不同，不可能每个都在这里讲解，所以你需要根据我所说的做调整。
- 2)设置管理员密码 不要忘记这第一步，这通常不在安全保护之下，所以请不要忘记查看设备和系统设置，一旦看到共有用户，你要将密码设置成你的密码.
- 3)打开加密设置 查看无线安全技术或者相似的标签部分。你想对标签进行加密，如果你所有的网络设备都支持的话，就使用无限安全技术(WPA-PSK)，否则你在关键型就使用WEP(如果你使用的WEP,你就可以使用passphrase生成的主键). 记录你使用的passphrase，你就可以用密码进入客户机了.
- 4)改变SSID "hack me"是SSID默认的名字，路由器的名称是"linksys"、"belkin"，我不能想象有人愿意尝试修改网络，你从客户机浏览无线网络时,记住你很需要这个SSID，在菜单目录下你能找到叫Channel或者SSID，这样就能保障你的基本安全，在这个过程中你可能要多次重起你的路由器，(所以最好使用电缆进行配置)。同时在你每次微调之后请不要忘记点击：“提供改变”和保存“改变”。来源：www.100test.com

注释：WEP是一种在接入点和客户端之间以“RC4”方式对分组信息进行加密的技术，密码很容易被破解。WEP使用的加密密钥包括收发双方预先确定的40位(或者104位)通用密钥，和发送方为每个分组信息所确定的24位、被称为IV密钥的加密密钥。但是，为了将IV密钥告诉给通信对象，IV密钥不经加密就直接嵌入到分组信息中被发送出去。如果通过无线窃听，收集到包含特定IV密钥的分组信息并对其进行解析，那么就连秘密的通用密钥都可能被计算出来。WPA是继承了WEP基本原理而又解决了WEP缺点的一种新技术。由于加强了生成加密密钥的算法，因此即便收集到分组信息并对其进行解析，也几乎无法计算出通用密钥。SSID(Service Set Identifier)也可以写为ESSID，用来区分不同的网络，最多可以有32个字符，无线网卡设置了不同的SSID就可以进入不同网络，SSID通常由AP广播出来，通过XP自带的扫描功能可以相看当前区域内的SSID。出于安全考虑可以不广播SSID，此时用户就要手工设置SSID才能进入相应的网络。简单说，SSID就是一个局域网的名称，只有设置为名称相同SSID的值的电脑才能互相通信。编辑特别推荐: 成本速度成关键解析 四种宽带接入技术 常用TCP端口作用及其操作建议 统一通信将成为IP语音未来发展趋势 提高企业网络可靠性的捷径 防御攻击策略之保持领先黑客一步 网络安全八个潜规则 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