

WindowsXP无线网络安全计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/619/2021\\_2022\\_WindowsXP\\_E6\\_c98\\_619348.htm](https://www.100test.com/kao_ti2020/619/2021_2022_WindowsXP_E6_c98_619348.htm) 虽然早期的无线网络由于特殊原因一直没有开展开来，导致在以前相当长的一时间内无法引起网络重视。而现在随着无线价格的偏移，跨入了寻常百姓家，越来越多的网民用上了无线网络。无线安全日渐引起了各界的关注。影响无线网络安全不稳定因素发生的客观原因依然是病毒与恶意用户，其：服务盗用、数据盗取，数据破坏、对无线网络的正常使用影响很大。下面将分步为读者解答！还是应了上面的那句话：“简易就是不安全的代名词”，XP的无线安全风险的最大因素，恰恰是来自于XP最简单易用的功能“无线零配置”(WIRELESS? ZERO? CONFIGURATION)，由于接入点可以自动发送接收信号，因此XP客户端一旦进入了无线网络信号的覆盖范围，就可以自动建立连接，如果进入了多个无线网络的信号覆盖范围，系统能自动与最近的接入点联系，并自动配置网卡进行连接，完成后，在“可用网络”中将出现建立的连接的SSID，由于不少厂商使用网卡的半个MAC地址来默认命名SSID，因此，使得SSID默认名可以推测，攻击者知道了默认名称后，至少连到接入点的网络是轻而易举了。主要的针对措施有三个：1、启用无线设备的不广播功能，不进行SSID的扩散。这个功能需要在硬件设备的选项里寻找，启用后将封闭网络，这个时候想连接网络的人必须提供准确的网络名，而不是XP系统自动提供的网络名。2、使用不规则网络名，禁止使用默认名。如果不广播了，攻击者还是可以通过猜测网络名连入网络，因此有必要修改

默认名。这里的不规则可以借鉴一下密码设置技巧，不设置具有敏感信息的网络名。

### 3、客户端MAC地址过滤

设定只有具有指定的MAC的客户端才可以连接接入点，可以将连入者进一步把关。上面的三个办法只是属于XP无线安全的初级设置，不要指望设置了这三个步骤后就可以高枕无忧了，从目前的安全设置来看，虽然可以防备部分无线攻击了，但是，由于并没有对传输中的数据采取任何加密措施，因此，只要攻击者使用一些特定的无线局域网工具，就可以抓取空中的各种数据包，通过对这些数据包的内容分析，可以获得各种信息，其中就包括SSID和MAC地址，因此前面的三个办法对于这种攻击就形同虚设了。我们下一步面临的是无线传输的加密问题----WEP。这是一个极具争议的话题，因此，为避免走入误区，我们将不对这个问题的强项和弱点一一详细解释，只一句话带过：“WEP为无线局域网提供了从数据安全性、完整性到数据来源真实性较为全面的安全性，但是WEP的密钥容易被攻击者得到”。虽然目前针对这一点厂商有计算机等级考试，加入收藏所加强，微软也发布了相关的升级包(KB826942

, [support.microsoft.com/default.aspx?scid=kb.zh-cn.826942](http://support.microsoft.com/default.aspx?scid=kb.zh-cn.826942)), 但是不能从根本上解决这个问题。WEP运行于接入点，如果我们是在2000上启用WEP，那么必须使用客户端软件提供的共享密钥，如果是使用的XP，就不需要了，系统会在第一次接入启用WEP的时候进行提示，输入密钥后可继续以下的配置：

- 1、打开“网络连接”，点击无线网卡的属性。
- 2、选中“首选网络”，选中或添加一个条目，然后点击属性。
- 3、打开“无线网络属性”后进行以下操作：1)修改“网络名” 2)

将“数据加密(WEP)”打勾 3)将“网络验证”打勾 4)选择匹配接入点的“密钥格式”(ASCII或十六进制)和“密钥长度”(40或104)。 5)需要输入正确的“网络密钥” 6)不选“自动选中密钥”。 4、保存关闭。OK, 针对XP下针对WEP的设置基本上就完成了, 但是为了无线网络的更加稳固, 我们再看看其他需要注意的安全措施: 1、网络中尽可能包含一个验证服务器。将网络配置成所有连接请求必须先通过验证服务器的验证, 将大大提高无线网络的安全性。 2、每月修改一次WEP密钥 因为WEP有记录缺陷, 所以最好每隔一段时间就修改一次WEP密钥。 3、避免有线与无线网络互联。无线网络应该是独立的, 为避免互相牵连, 避免增加安全风险, 应将有线与无线网络分开, 至少应该在二者之间建立防火墙。 4、建立VPN验证 在接入点和网络之间再加入一台VPN服务器, 这样一来攻击者可能可以接上接入点, 但只是死蟹一只, 进不了网络, 无法对网络搞任何破坏。 5、定期维护 维护的内容是检查网络和审查日志, 检查网络可以使用一些攻击无线网络的扫描工具, Netstumbler(.netstumbler.com/"&gt;.www.netstumbler.com) Kismet www.kismetwireless.net 审查日志的重点是审查帐户登陆事件。最后附上Ed Bott的无线网络的检查清单: 1、给接入点设置一个强壮的密码。 2、禁用接入点的远程管理功能。 3、无线网络设备的固件(FirmWare)保持升级到最新。 4、修改接入点的网络名的默认名。 5、使用MAC过滤控制 6、启用WEP并设置强壮密码。 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)