精细配置提高安全系数无线网络配置六要素思科认证 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__E7_B2_BE_E7_BB_86_E9_85_8D_E7_c101_644105.htm 建立安全的无线网络访问节点(access point )的出发点在于如阿防止信息向非授权外部访问的泄漏。这一原则往往是知宜行难。由于无线网络的安全设置要比一般的线缆网络复杂的多，因为线缆网络的访问节点都是固定的，而在无线网络的信号收发范围内，所有的节点都可以接入。 无线网络本身的特点所造成的问题是无法避免的，但采取正确的无线网络系统防护手段将保护用户的系统，并避免严重的安全问题。而如草率配置，该非安全无线网络将导致“ 服务不可用 ”或成为攻击其它网络的“ 跳板 ”。为了把安全漏洞所造成的风险降至最低，请确保网络技术人员按照以下建议进行配置和测试。 1、规划好天线安装位置 这是实现“ 非泄漏 ”无线访问节点的第一步，通过无线信号的覆盖范围来确定访问节点天线的摆放位置。请注意不要把天线放置在窗户旁边，因为玻璃无法挡住信号的外泄。在理想情况下，信号发射天线最好放置在工作区域的正中间，这样就可以把信号泄漏降至最低程度。当然上述情况不大可能完全做到，但只要尽量保证按上述原则来执行就不会有错。 2、使用WEP(无线加密协议) WEP(无线加密协议)是针对无线网络数据传输加密的标准。尽管它仍存在明显的脆弱性，但用来防范普通黑客还是相当有效的。许多无线访问节点产品的厂商都把WEP设置为disable，以方便安装。因此节点天线一旦开始收发信号，黑客就可以通过嗅探器对无线数据明文进行访问。 3、更改SSID设置并取消广播 服务设置

初始化校验器(SSID，service set identifier)用来鉴别无线访问节点所使用的初始化字符串，客户端要通过SSID来完成连接的初始化。该校验器由制造商进行设定，同一厂商产品使用同样的默认值，比如3Com公司的设备使用“101”字符串。如果被黑客了解到相应的初始化字符串，那么就可以轻易建立非授权链接。因此笔者建议，在配置贵单位无线网络时，请更改SSID初始化字符串，使其难于猜测，并在条件许可的情况下，限制校验器的SSID广播，以此来杜绝非法链接。该网络将依然可用，但不会给黑客以可乘之机。 4、取消DHCP 这一安全策略听起来颇有些奇怪，但对于无线网络的安全来说是非常有效的。采取了这一措施后，黑客将不得不猜错贵单位网络的IP地址、子网掩码以及其它所必须的TCP/IP参数。即使黑客可以访问贵单位的无线网络节点，但如果不知道IP地址等上述内容，仍是不得其门而入。 5、取消或更改SNMP设置 如果贵单位访问节点支持SNMP，那么或者取消它或者更改Public和Private公用字符串。如果不采取这一步骤，那么黑客将利用SNMP来获取贵单位网络的重要信息。 6、使用访问列表 为了更进一步的保护好贵单位无线网络，请设置一个访问列表。并非所有的无线访问节点都支持这一特性，但如果贵单位网管做到这一步，那将实现精确规定可连接入访问节点的机器。支持这一特性的访问节点设备有的使用TFTP协议来周期性的下载更新访问列表，这样网管人员就不需要在每台设备上进行访问列表的同步设定了。 