 你肯定不会设计一个没有防火墙的互联网接入的网络。因此，你怎么会架设一个没有加密的无线网络?理解无线加密对于部署一个安全的无线网络是非常重要的。 无线传输的安全类似于一个书面信息。有各种各样的方法来发送一个书面信息。每一种方法都提供一种增强水平的安全和保护这个信息的完整性。你可以发送一张明信片，这样，这个信息对于看到它的每一个人都是公开的。你可以把这个信息放在信封里，防止有人随意看到它。如果你确实要保证只有收件人能够看到这个信息，你就需要给这个信息加密并且保证收件人知道这个信息的解码方式。 无线数据传输也是如此。没有加密的无线数据是在空中传输的，任何在附近的无线设备都有可能截获这些数据。 使用有线等效协议(WEP)加密你的无线网络可提供最低限度的安全，因为这种加密是很容易破解的。如果你确实要保护你的无线数据，你需要使用WPA(Wi-Fi保护接入)等更安全的加密方式。为了帮助你了解这些选择，这里简要介绍一些现有的无线加密和安全技术： 有线等效协议(WEP) 有线等效协议是厂商作为一种伪标准匆忙推出的一种加密方式。厂商要在这个协议标准最后确定下来之前匆忙开始生产无线设备。因此，这个协议后来发现存在一些漏洞。甚至一个初入道的攻击者也能够利用这个协议中的安全漏洞。 Wi-Fi保护接入(WPA) 制定Wi-Fi保护接入协议是为了改善或者替换有漏洞的WEP加密方式。WPA提供了比WEP更强大的加密方式，解

决了WEP存在的许多弱点。 临时密钥完整性协议(TKIP) TKIP是一种基础性的技术，允许WPA向下兼容WEP协议和现有的无线硬件。TKIP与WEP一起工作，组成了一个更长的128位密钥，并根据每个数据包变换密钥，使这个密钥比单独使用WEP协议安全许多倍。 可扩展认证协议(EAP) 有EAP的支持，WPA加密可提供与控制访问无线网络有关的更多的功能。其方法不是仅根据可能被捕捉或者假冒的MAC地址过滤来控制无线网络的访问，而是根据公共密钥基础设施(PKI)来控制无线网络的访问。 虽然WPA协议给WEP协议带来了很大的改善，它比WEP协议安全许多倍，但是，任何加密都比一点都不加密好得多。如果WEP是你的无线设备上拥有的惟一的保护措施，这种保护措施仍然可以阻止随意地危害你的无线数据并且使大多数新入道的攻击者寻找没有保护的无线网络来利用。 特别推荐： 2009年9月全国计算机等级考试时间及科目预告 2009年上半年全国计算机等级考试参考答案请进入计算机考试论坛 2009年全国计算机等级考试报名信息汇总 2009年NCRE考试有新变化 2009年全国计算机等级考试大纲 2009年上半年全国计算机二级考试试题及答案 2009年上半年全国计算机等级考试试题答案汇总 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