一个安全的无线网络如何选择无线加密 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/252/2021_2022__E4_B8_80_E4_B8_AA_E5_AE_89_E5_c104_252313.htm 你不会设计一个有互联网访问而没有防火墙的网络。那么，你为什么会有一个没有加密的无线网络呢?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封书信。有各种各样的发送书信的方法，而且每一种方法都能提高安全等级和保护这个信息的完整性。你可以发送一张明信片，但是，所有的人都可以看到明信片上的信息。你可以把信放到信封里面封好，这可以保护信件被人偶然看到。如果你确实要保证这封信只能被收件人看到，你就需要为这封信加密或者进行编码，并且确认收件人知道你的编码方式。 无线数据传输也是如此。没有加密的无线数据在空中传输，附近的任何无线设备都有可能拦截到这些数据。 使用WEP(有线等效协议)协议为你的无线网络加密能够提供最低限度的安全，因为这种加密方式很容易破解。如果你确实想让你的无线数据得到保护，你应该使用更安全的加密方法，如WPA。为了帮助你理解这些选择，下面简单介绍一下现有的一些无线加密方法和安全技术: WEP(有线等效协议)。WEP是一种加密方法，是在协议标准最后确定之前由一些急于生产无线设备的厂商匆忙拼凑起来的假冒的加密标准。因此，这个标准后来发现存在很多漏洞，甚至一个没有经验的攻击者也能利用这些安全漏洞。 WPA(Wi-Fi保护访问)。WPA是用来改善或者替换有漏洞的WEP协议的。WPA提供了比WEP更强大的加密功能，解决了WEP存在的许多弱点。 1.TKIP(临时密钥完整性协

议)。TKIP是一种基本的技术，允许WPA向下兼容WEP和现有的无线硬件。TKIP与WEP配合使用可组成更长的密钥，128位密钥以及对每个数据包每点击一次鼠标就改变一次的密钥，使这种加密方法比WEP更安全。 2.EAP(可扩展认证协议)。在EAP协议的支持下，WPA加密提供了更多的根据PKI(公共密钥基础设施)控制无线网络访问的功能，而不是仅根据MAC地址来进行过滤。过滤的方法很容易被人欺骗。 虽然WPA改善了WEP的安全性并且比WEP协议更安全，但是，任何加密都比一点也不加密强。如果WEP是你目前的无线设备拥有的惟一的一种保护措施，这种加密措施仍然能够阻止随意地攻破你的无线数据，使大多数没有经验的攻击者去寻找可以利用的没有保护措施的无线网络。 