 无线局域网的第一个安全协议802.11 Wired Equivalent Privacy(WEP)，一直受到人们的质疑。虽然WEP可以阻止窥探者进入无线网络，但是人们还是有理由怀疑它的安全性，因为WEP破解起来非常容易，就像一把锁在门上的塑料锁。 在过去一年里，许多厂商的轻型可扩展认证协议(LEAP) 安全方案在无线网络中得到了应用。但是这些方案提供的互操作性十分有限，在多数情况下，客户端无线网卡和接入点必须来自同一家厂商，而这在公共场所和许多没有采用标准桌面系统的环境中是行不通的。在去年年底，Wi-Fi联盟宣布推出Wi-Fi保护接入(Wi-Fi Protected Access，WPA)，这是一种可以解决802.11大多数安全问题的标准安全机制。这种无线安全标准可以推动无线局域网在公共场所和学术环境的部署。 WPA基础 WPA建立在仍处在开发中的802.11i标准的目前版本之上。考虑到IEEE要到今年年底才有望获得批准，长期等待会阻碍市场发展，Wi-Fi联盟推出了WPA。WPA有望应用在今年春季上市的产品中。 WPA的一个优势是，它使公共场所和学术环境安全地部署无线网络成为可能。而在此之前，这些场所一直不能使用WEP。WEP的缺陷在于其加密密钥为静态密钥而非动态密钥。这意味着，为了更新密钥，IT人员必须亲自访问每台机器，而这在学术环境和公共场所是不可能的。另一种办法是让密钥保持不变，而这会使用户容易受到攻击。由于互操作问题，学术环境和公共场所一直不能使用专有的安全机制

。 WPA采用有效的密钥分发机制，可以跨越不同厂商的无线网卡实现应用。为了确保WPA得到认真对待，Wi-Fi联盟已经要求在今年年底之前所有的新Wi-Fi证书都必须采用这种安全机制。WPA很有可能成为无线设备缺省的出厂配置，这将方便大多数小型办公室和家庭办公室(SOHO)用户。在此之前的产品不需要符合这种要求，但是厂商肯定会提供合适的升级途径。 WPA工作原理 WPA包括暂时密钥完整性协议(Temporal Key Integrity Protocol，TKIP)和802.1x机制。TKIP与802.1x一起为移动客户机提供了动态密钥加密和相互认证功能。WPA通过定期为每台客户机生成惟一的加密密钥来阻止黑客入侵。 TKIP为WEP引入了新的算法，这些新算法包括扩展的48位初始向量与相关的序列规则、数据包密钥构建、密钥生成与分发功能和信息完整性码(也被称为“ Michael ”码)。在应用中，WPA可以与利用802.1x和EAP(一种验证机制)的认证服务器(如远程认证拨入用户服务)连接。这台认证服务器用于保存用户证书。这种功能可以实现有效的认证控制以及与已有信息系统的集成。 由于WPA具有运行“ 预先共享的密钥模式 ”的能力，SOHO环境中的WPA部署并不需要认证服务器。与WEP类似，一部客户机的预先共享的密钥 (常常被称为“ 通行字 ”)必须与接入点中保存的预先共享的密钥相匹配，接入点使用通行字进行认证，如果通行字相符合，客户机被允许访问接入点。 除了无法解决拒绝服务(DoS)攻击外，WPA弥补了WEP其他的安全问题。黑客通过每秒发送至少两个使用错误密钥的数据包，就可以造成受 WPA保护的网络瘫痪。当这种情况发生时，接入点就会假设黑客试图进入网络，这台接入点会将所有的连接关闭一分钟，以避免给网

络资源造成危害，连接的非法数据串会无限期阻止网络运行，这意味着用户应该为关键应用准备好备份进程。 部署时需要考虑的问题 用户可以通过对所获得Wi-Fi认证的接入点进行简单的软件升级来安装WPA。WPA在采用不同无线网卡的客户设备之间实现了有效的安全性(假设这些无线网卡也部署了WPA)。部署WPA的接入点将支持混合客户设备环境，即一些客户设备部署了WPA，另一些则没有部署。 WPA将保持与802.11i标准的向前兼容性。最终的802.11i标准将包含比RC4更强的高级加密标准(AES)。不过，由于AES需要性能更高的处理器，因此它可能要求更换遗留的接入点。可以说，802.11i将定位于新设备。 读到这里，很多用户就会要问，WPA究竟是临时应对措施还是长期解决方案?毫无疑问，WPA能够提供很好的安全性，可以为用户保证了即插即用的安全性，而即插即用的安全性一直是阻碍无线局域网普及的真正障碍。客户应当通过升级已有的设备来部署WPA，应当坚持要求新设备中提供WPA。由于 802.11i对硬件提出的新要求，因此WPA是一种使用户迁移到下一代硬件时的安全解决方案。WEP势必要退出实际应用，WPA则作为通向 802.11i道路的不可缺失的一环出现。 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