IEEE802.11i的网络构架和安全改进 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/492/2021_2022_IEEE80211_c67_492430.htm 安全性对于无线局域网来说可谓老生常谈，自它诞生之日起，与其灵活便捷的优势共存的就是安全漏洞这个挥之不去的阴影。据统计，不愿采用无线局域网的理由中，安全问题高居第一位，达40%以上，已经成为阻碍WLAN进入信息化应用领域的最大障碍。现有的安全机制由于不能提供足够安全的基础建设模块，让解决WLAN安全成本的负担转移到整个WLAN价值链上的产品制造厂商、系统集成商和用户，这种不合理的成本转嫁使市场上产生了多种安全安装解决方案，而最终用户为了能够实施设备厂商提供的多种安全安装方案而不断付出更多的安全成本。 为了使WLAN技术从这种被动局面中解脱出来， IEEE 802.11i工作组致力于制订被称为IEEE 802.11i的新一代安全标准， 802.11i的网络构架 802.11i标准规定了两种网络构架：过渡安全网络(TSN)和强健的安全网络(RSN)。 TSN：规定在其网络中可以兼容现有的使用WEP方式工作的设备，使现有的无线局域网系统可以向802.11i网络平稳过渡。市场对于提高WLAN安全的需求是十分紧迫的，IEEE 802.11i不能解决上述RSN对于现有设备升级困难的问题，标准的制定进展也不能完全满足这一需要。因此，TSN的发展和制定就显得十分重要。 在这种情况下，Wi-Fi联盟制定了WPA（Wi-Fi Protected Access）标准，作为向IEEE 802.11i过渡的中间标准。这一标准采用了IEEE 802.11i的草案，保证了与未来出现的协议的前向兼容。 RSN：为了使WLAN技术从这种被动局面中解脱出来， IEEE

802.11的i工作组致力于制订被称为IEEE 802.11i的新一代安全标准，这种安全标准为了增强WLAN的数据加密和认证性能，定义了RSN(Robust Security Network，健壮安全网络)的概念，并且针对WEP加密机制的各种缺陷做了多方面的改进。IEEE 802.11i的安全改进： 相比以往的无线安全协议，IEEE 802.11i具有以下一些技术优势： WLAN底层引入AES算法，克服WEP的缺陷 有线对等保密(WEP)协议的缺陷延缓了无线局域网(WLAN)在许多企业内的应用和普及。无线局域网网络会暴露某个网络，因此，从安全的角度来讲，不能像核心企业网络而必须像接入网络那样来对待。如果企业用户通过一个局域网交换中心互相连接，人们就可认为他们已经成为信任用户。 WEP在接入点和客户端之间以“ RC4 ”方式对分组信息进行加密的技术，密码很容易被破解。WEP使用的加密密钥包括收发双方预先确定的40位（或者104位）通用密钥，和发送方为每个分组信息所确定的24位、被称为IV密钥的加密密钥。但是，为了将IV密钥告诉给通信对象，IV密钥不经加密就直接嵌入到分组信息中被发送出去。如果通过无线窃听，收集到包含特定IV密钥的分组信息并对其进行解析，那么就连秘密的通用密钥都可能被计算出来。 为了帮助堵住无线局域网中的安全漏洞，IEEE 802.11工作组建立了802.11i任务小组，为802.11标准开发安全升级。802.11i规定了一个基于“ 高级加密标准 ”AES加密算法的CCMP(Counter-Mode/CBC-MAC Protocol)数据加密模式CCMP，以实施更强大的加密和信息完整性检查。 AES是1997年1月由NIST提出的，其目的是开发一种新的能保证政府信息安全的编码算法。AES是一种对称的块加密技术，提

供比WEP/TKIP中RC4算法更高的加密性能。对称密码系统要求收发双方都知道密钥，而这种系统的最大困难在于如何安全地将密钥分配给收发的双方，特别是在网络环境中。AES加密算法使用128bit分组加码数据。 它的输出更具有随机性，对128比特、轮数为7的密文进行攻击时需要几乎整个的密码本，对192、256比特加密的密文进行攻击不仅需要密码本，还需要知道相关的但并不知道密钥的密文，这比WEP具有更高的安全性，攻击者要获取大量的密文，耗用很大的资源，花费更长的时间破译。它解密的密码表和加密的密码表是分开的，支持子密钥加密，这种做法优于最初的用一个特殊的密钥解密，很容易防护幂攻击和同步攻击，加密和解密的速度快，在安全性上优于WEP。 AES算法支持任意分组的大小，密钥的大小为128、192、256，可以任意组合。它初始时间快，其固有的并行性可以有效地利用处理器资源，有很好的软件性能。在加密和解密分别进行的时候，很适合有限距离的环境，并且对ROM和RAM要求很低；当加密和解密同时进行的时候，对ROM要求有所上升，但仍适合距离有限的环境。AES还适用于交叉存取和非交叉存取两种情况。在这两种情况下，它的性能几乎没有变化，这使得DSP设备可以有效地优化其密码。此外，AES还具有应用范围广、等待时间短、相对容易隐藏、吞吐量高的优点。经过比较分析，可知此算法在性能等各方面都优于WEP，利用此算法加密，无线局域网的安全性会获得大幅度提高，从而能够有效地防御外界攻击。 采用WPA规范使现有设备向IEEE802.11i平稳过渡 企业对无线局域网技术的主要担心是Wi-FI技术缺少一个可靠的安全标准。而WiFi联盟为了满足现在市场的需求，制定

了WPA(Wi-Fi Protected Access)标准作为一种可替代 WEP的无线安全技术，在 IEEE 802.11i 标准最终确定前，将为IEEE 802.11 无线局域网 (WLAN)提供更强大的安全性能。 WPA是IEEE 802.11i的一个子集，其核心就是IEEE 802.1x和TKIP。IEEE 802.11i与WPA的关系如图2所示。 WPA考虑到了不同的用户和不同的应用安全需要，例如：企业用户需要很高的安全保护（企业级），否则可能会泄漏非常重要的商业机密；而家庭用户往往只是使用网络来浏览 Internet、收发Email、打印和共享文件，这些用户对安全的要求相对较低。为了满足不同要求用户的需要，WPA中规定了两种应用模式： 企业模式。通过使用认证服务器和复杂的安全认证机制来保护无线网络通信安全。 家庭模式（包括小型办公室）。在AP（或者无线路由器）以及连接无线网络的无线终端上输入共享密钥来保护无线链路的通信安全。 WPA是继承了WEP基本原理而又解决了WEP缺点的一种新技术。由于WPA利用暂时密钥完整协议(TKIP)作为改进WEP所使用密钥的安全性的协议和算法，加强了生成加密密钥的算法，因此即便收集到分组信息并对其进行解析，也几乎无法计算出通用密钥。另外，TKIP与WEP一样将此密钥用于RC4加密处理。WPA和以AES加密方式工作的11i不同，可以以软件方式和附加硬件设备实现的，避免了更换硬件带来的成本问题。WPA还采用IEEE 802.11x来实现防止数据中途被篡改的功能和认证功能。 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