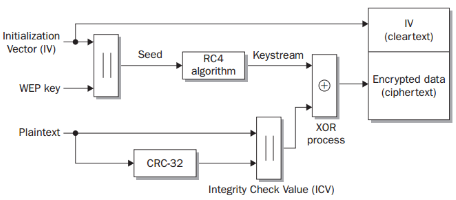
1.有线等效保密（Wired Equivalent Privacy – WEP）

WEP是一个Layer 2的加密方法，它使用的是ARC4流加密。它有一个数据完整性校验操作，也就是Integrity Check Value (ICV)，这个值是通过计算为加密的数据域（MSDU）而来的。

802.11标准定义了两个WEP版本，分别是WEP-40和WEP-104支持64bit和128bit加密，其实40和104都是从64与128减24得来的，这24位叫初始化向量Initialization Vector (IV)，注意和ICV进行区分。40和104则是指静态秘钥的bit长度，也就是说WEP-40支持输入10 hex characters or 5 ASCII characters，WEP-104支持输入26 hex characters or 13 ASCII characters

那么WEP加密过程是怎么实现的呢？下面根据流程图来分析一下



（1） IV是动态生成的24bit随机数，标准没有指定应该怎么生成，而且在数据帧中以明文的方式进行发送，它和key结合生成随机种子（seed），然后运用RC4算法生成秘钥流（keystream）。

（2）对需要加密的明文进行CRC-32运算，生成 ICV（32位），然后将这个 ICV 追加到 plaintext的后面

（3）将尾部有 ICV的plaintext 与密码流进行异或运算，得到加密数据

（4）将 IV 添加到加密数据的前面，进行传送。

2.Temporal Key Integrity Protocol (TKIP) 临时秘钥完整性协议

TKIP是用来解决WEP容易被破解而提出的临时性加密协议，它并不是802.11推荐的强制加密协议， 简单来说，TKIP主要是用来加强WEP加密，这个升级主要体现在算法上，这一点很重要，为什么这么说呢？因为使用TKIP加密，并不需要进行硬件的升级，也就是说只要你的硬件支持WEP加密，那么同时也能够支持更安全的TIKP加密，同过软件升级来达到安全系数提高的目的，这种做法更加的平滑，也更容易被市场接受。

但是CCMP不同，它必须要更新的硬件支持才能使用，所以TKIP成了从WEP过渡到CCMP的中间产物，按照标准来说，如果你的设备可以用TKIP加密，就不要用WEP加密，如果可以支持CCMP加密，就不要用TKIP。

基于WEP，TKIP主要做了以下改动：

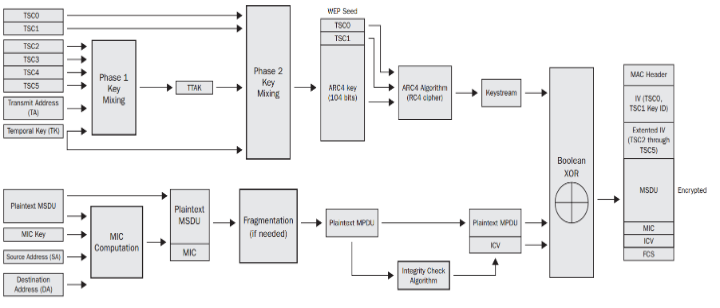
（1）发送端会使用加密算法计算一个MIC（message integrity code，消息完整码），这个MIC是通过计算 SA， DA，priority 和plaintext data而来，TKIP会将MIC追加到MSDU的后面，如果MSDU + MIC 的size过大，需要分片，那么只要将 MSDU + MIC 看成一个整体 MSDU‘ 进行分片就好了。也就是说，TKIP只要在MSDU进行分片前将MIC追加到MSDU后面，形成一个新的MSDU就好了，分片的事，它不管,那是MPDU的事情。接收端收到MPDU分片以后，会先将它们重组成一个MSDU，然后进行MIC的校验。

（2）TKIP虽然包含了MIC，但仍然不够，所以TKIP实现了countermeasures功能，它可以限制可能的伪装和学习被攻击的信息

（3）TKIP使用一个per-MPDU TKIP sequence counter (TSC) 来理顺MPDUs的发送，如果接收端收到的MPDUs不符合顺序（比如序号没有递增），那么将会被丢弃.TKIP会像WEP IV和附加 IV一样 对TSC进行编码。

（4）TKIP使用一个密码混合功能，结合TK，TA和TSC生成一个WEP seed。

下面我们来看一下TKIP加密的流程图：

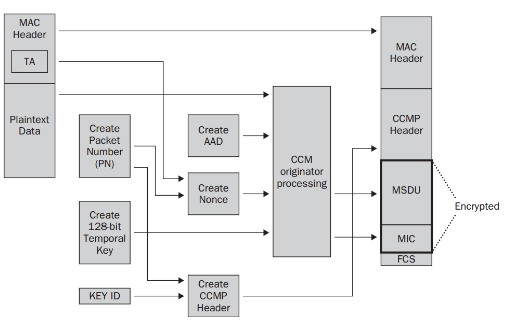


从流程图来看，其实TKIP相对于WEP主要是多了左半部分，右半部分的内容其实大同小异；从MPDU的内容来看，主要多了 extender IV和 MIC两个部分。

3. Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol(CCMP)

CCMP加密在802.11i修正案中定义，用于取代TKIP和WEP加密。CCMP使用AES块加密算法取代WEP和TKIP的RC4流算法，它也是WAP2指定的加密方式，值得注意的是，在CCMP加密使用的AES算法中都是使用的128bit的密钥和128bit的加密块。

下面我们来看看主要加密过程：



（1）每一个新的MPDU需要发送时，都会重新创建一个48bit的PN，如果是重传的MPDU，则使用原来发送MPDU的PN

（2）使用MPDU的头部构建AAD，如下图所示，它是MAC Header的构成，其中深灰色部分会被用来构建AAD，而且会被CCM保密；其中一些浅灰色的也会用于构建AAD，根据帧的类型不同，其中一些字段可能没有使用，那么就会用0覆盖。

我们可以看出，TKIP加密是基于MSDU的加密，而CCMP加密是基于MPDU的加密，这样就避免了针对MSDU的攻击，解决了在MSDU加密中不能解决的问题。

**4.总结**

安全性：CCMP>TKIP>WEP

TKIP是包裹在已有WEP密码外围的一层“外壳”。TKIP由WEP使用的同样的加密引擎和RC4算法组成。不过，TKIP中密码使用的密钥长度为 128位。这解决了WEP的第一个问题：过短的密钥长度。

　　TKIP的一个重要特性，是它变化每个数据包所使用的密钥。这就是它名称中“动态”的出处。密 钥通过将多种因素混合在一起生成，包括基本密钥（即TKIP中所谓的成对瞬时密钥）、发射站的MAC地址以及数据包的序列号。混合操作在设计上将对无线站和 接入点的要求减少到最低程度，但仍具有足够的密码强度，使它不能被轻易破译。

　　利用TKIP传送的每一个数据包都具有独有的48位序列号，这个序列号在每次传送新数据包时递增，并被用作初始化向量和密钥的一部分。将序列号加到密 钥中，确保了每个数据包使用不同的密钥。这解决了WEP的另一个问题，即所谓的“碰撞攻击”。这种攻击发生在两个不同数据包使用同样的密钥时。在使用不同 的密钥时，不会出现碰撞。

　　以数据包序列号作为初始化向量，还解决了另一个WEP问题，即所谓的“重放攻击（replay attacks）”。由于48位序列号需要数千年时间才会出现重复，因此没有人可以重放来自无线连接的老数据包：由于序列号不正确，这些数据包将作为失序 包被检测出来。

被混合到TKIP密钥中的最重要因素是基本密钥。如果没有一种生成独特的基本密钥的方法，TKIP尽管可以解决许多WEP存在的问题，但却不能解决最 糟糕的问题：所有人都在无线局域网上不断重复使用一个众所周知的密钥。为了解 决这个问题，TKIP生成混合到每个包密钥中的基本密钥。无线站每次与接入点建立联系时，就生成一个新基本密钥。这个基本密钥通过将特定的会话内容与用接 入点和无线站生成的一些随机数以及接入点和无线站的MAC地址进行散列处理来产生。由于采用802.1x认证，这个会话内容是特定的，而且由认证服务器安全地传送给无线站。

在应用方面，尽管DES在安全上是脆弱的，但由于快速 DES芯片的大量生产，使得DES仍能暂时继续使用，为提高安全强度，通常使用独立密钥的三级DES。但是DES迟早要被AES代替。流密码体制较之分组 密码在理论上成熟且安全，但未被列入下一代加密标准。

AES提供了比 TKIP更加高级的加密技术， 现在无线路由器都提供了这2种算法，不过比较倾向于AES。 TKIP安全性不如AES，而且在使用TKIP算法时路由器的吞吐量会下降3成至5成，大大地影响了路由器的 性能。