

wlan 技术白皮书

安全

1.00

	Wlan 技术白皮书—安全
---	---------------

修订记录

日期	修订版本	修改章节	修改描述	作者
08/8/1	1.00		第一稿	沈翀



目 录

1. Wlan安全机制.....	4
2. 名词解释.....	5
3. 无线安全标准历史.....	5
3.1. 802.11.....	5
3.2. WPA.....	6
3.3. 802.11i.....	6
3.4. WAPI.....	6
3.5. EAP相关RFC.....	7
4. 无线加密机制.....	7
4.1. WEP.....	7
4.2. TKIP.....	8
4.3. CCMP.....	10
5. 无线认证机制.....	11
5.1. 开放的无线接入.....	11
5.2. 共享密钥.....	11
5.3. EAP.....	12
5.3.1. EAP协议.....	12
5.3.2. EAP多种认证方式.....	14
5.3.3. 802.1X.....	16
5.3.4. 无线局域网的 802.1X认证.....	17
6. 密钥管理机制.....	18
6.1. 密钥的产生和管理.....	18
6.2. 密钥交互和握手流程.....	20
6.2.1. 单播密钥更新的四次握手流程.....	20
6.2.2. 广播密钥更新流程.....	21
7. 参考文献.....	22
8. 附录：一个完整的 802.1X认证过程.....	23

1. Wlan 安全机制

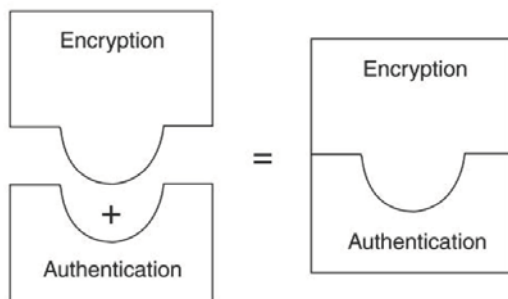
无线局域网相对于有线局域网而言,其所增加的安全问题原因主要是其采用了公共的电磁波作为载体来传输数据信号,而其他各方面的安全问题两者是相同的。

由于无线网络的开放性,为了保证其安全,至少需要提供以下 2 个机制:

- 1、判断谁可以使用 wlan 的方法—认证机制
- 2、保证无线网数据私有性的方法—加密机制

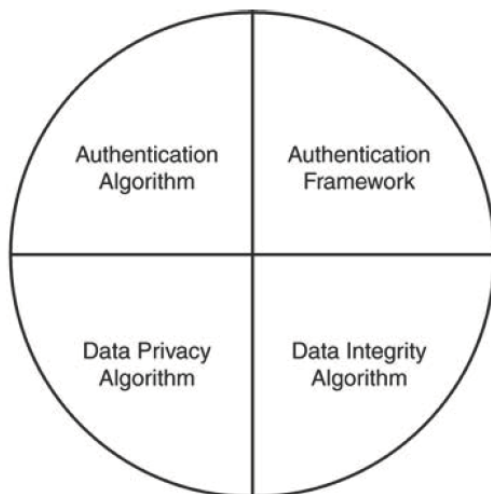
因此,早期的无线安全(802.11)包含认证和加密两部分。

Encryption + Authentication = Wireless Security



为了解决 802.11 的安全漏洞,802.11i 将无线安全分为 4 个方面:

The Four Facets of Wireless Security



实际上是把早期的认证机制细分为认证算法(Authentication Algorithm)和认证框架(Authentication Framework);加密机制则包含了数据加密算法(Data Privacy Algorithm)以及数据完整性校验算法(Data Integrity Algorithm)。

2. 名词解释

MIC: 消息完整性校验码 (message integrity code)。针对一组欲保护数据计算出的散列值，用以防止数据遭篡改。

IV: 初始化向量 (Initialization Vector)，加密标头中公开的密钥材料。

ICV: 完整性校验值 (Integrity Check Value)，数据帧的校验码，用于防止数据遭篡改。

Michael: 数据完整性的校验算法，由 TKIP 规范。

TLS: 传输层安全协议 (TLS) 是确保互联网上通信应用和其用户隐私的协议 (RFC 2246)。当服务器和客户机进行通信，TLS 确保没有第三方能窃听或盗取信息。TLS 是安全套接字层 (SSL) 的后继协议。

PRF: 伪随机功能 (Pseudo-Random Function) 是 TLS 标准定义的一种生成密钥的算法。

PMK: 成对主密钥 (pairwise master key)，申请者 (supplicant) 与认证者 (authenticator) 之间所有密钥数据的最终来源。它可以衍生自身份验证过程的 EAP method，或由预共享密钥 (PSK) 直接提供。

PSK: 预共享密钥 (pre-shared key)，一种 802.11i 身份验证方式，以预先设定好的静态密钥进行身份验证。

PTK: 成对临时密钥 (pairwise transient key)，从成对主密钥中产生的密钥，用于加密和完整性校验。

GMK: 组主密钥 (group master key)，认证者 (authenticator) 用来生成组临时密钥 (GTK) 的密钥。

GTK: 组临时密钥 (group transient key)，用来保护广播和组播数据的密钥。

3. 无线安全标准历史

3.1.802.11

2003 年版 802.11 规范采用 WEP 作为认证和加密的基础。



有线等效保密（WEP）协议是由 802.11 标准定义的，用于在无线局域网中保护链路层数据。WEP 使用 40 位钥匙，采用 RSA 开发的 RC4 对称加密算法，在链路层加密数据。

WEP 加密采用静态的保密密钥，各 WLAN 终端使用相同的密钥访问无线网络。WEP 也提供认证功能。当加密机制功能启用，客户端要尝试连接上 AP 时，AP 会发出一个 ChallengePacket 给客户端，客户端再利用共享密钥将此值加密后送回存取点以进行认证比对，如果正确无误，才能获准存取网络的资源。现在的 WEP 也一般支持 128 位的钥匙，提供更高等级的安全加密。

WEP 算法已被证明是可以破解的。

注：2007 年版本 802.11 规范合并了 802.11i 的内容。为示区别，本文提到的 802.11 都是指 2003 年版，而提到 802.11i 则包含了 2004 年通过的 802.11i 规范以及 2007 年版 802.11 中关于安全的内容。

3.2. WPA

在 IEEE802.11i 标准最终确定前，WPA（Wi-Fi Protected Access）技术是在 2003 年正式提出并推行的一项无线局域网安全技术，成为代替 WEP 的无线，为现有的大量的无线局域网硬件产品提供一个过渡性的高安全解决方案。WPA 是 IEEE802.11i 的一个子集，其核心就是 IEEE 802.1X 和 TKIP。

端口访问控制技术（IEEE802.1X）和可扩展认证协议（EAP）该技术也是用于无线局域网的一种增强性网络安全解决方案。当无线工作站与无线访问点 AP 关联后，是否可以使用 AP 的服务要取决于 802.1x 的认证结果。如果认证通过，则 AP 为无线工作站打开这个逻辑端口，否则不允许用户上网。

TKIP 是一种临时的密钥完整性协议。开发 TKIP 主要动机是为了升级旧式的基于 WEP 硬件的安全性。如前所述，WEP 算法是可破解的。TKIP 对现有的 WEP 进行了改进，在其加密引擎中增加了“密钥细分”、“消息完整性检查”、“具备序列功能的初始向量”以及“密钥生成和定期更新功能”等 4 种算法，极大地提高了加密的安全度。

3.3. 802.11i

2004 年正式通过的 IEEE 802.11i 标准提出 RSN 的概念。强健安全网络（RSN）在接入点和移动设备之间使用的是动态身份验证方法和加密运算法则。在 802.11i 标准中所建议的身份验证方案是以 802.1X 框架和可扩展身份验证协议（EAP）为依据的。加密运算法则使用的是“高级加密标准”AES 加密算法。

3.4. WAPI

除了国际上的 IEEE 802.11i 和 WPA 安全标准之外，我国也在 2003 年 5 月份提出了无线



局域网国家标准 GB15629.11，这是目前我国在这一领域惟一获得批准的协议。标准中包含了全新的 WAPI (WLAN Authentication and Privacy Infrastructure) 安全机制，这种安全机制由 WAI (WLAN Authentication Infrastructure) 和 WPI (WLAN Privacy Infrastructure) 两部分组成，WAI 和 WPI 分别实现对用户身份的鉴别和对传输的数据加密。

3.5.EAP 相关 RFC

[RFC 2284]PPP Extensible Authentication Protocol (EAP). L. Blunk, J.Vollbrecht. March 1998.

[RFC 3748]Extensible Authentication Protocol (EAP). B. Aboba, L. Blunk, J.Vollbrecht, J. Carlson, H. Levkowitz, Ed.. June 2004.

[RFC 4017]Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs. D. Stanley, J. Walker, B. Aboba. March 2005.

[RFC 2433]Microsoft PPP CHAP Extensions. G. Zorn, S. Cobb. October 1998.

[RFC 2759] Microsoft PPP CHAP Extensions, Version 2. G. Zorn. January 2000.

[RFC 2246]The TLS Protocol Version 1.0. T. Dierks, C. Allen. January 1999.

[RFC 4346]The Transport Layer Security (TLS) Protocol Version 1.1. T.Dierks, E. Rescorla. April 2006.

[RFC 5216]The EAP-TLS Authentication Protocol. D. Simon, B. Aboba, R.Hurst. March 2008.

[EAP Ms-Chapv2]draft-kamath-pppext-eap-mschapv2-01.txt

[PEAP]draft-josefsson-pppext-eap-tls-eap-10.txt

[RFC 3078] Microsoft Point-To-Point Encryption (MPPE) Protocol. G. Pall, G. Zorn. March 2001.

[RFC 3079] Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE). G. Zorn. March 2001.

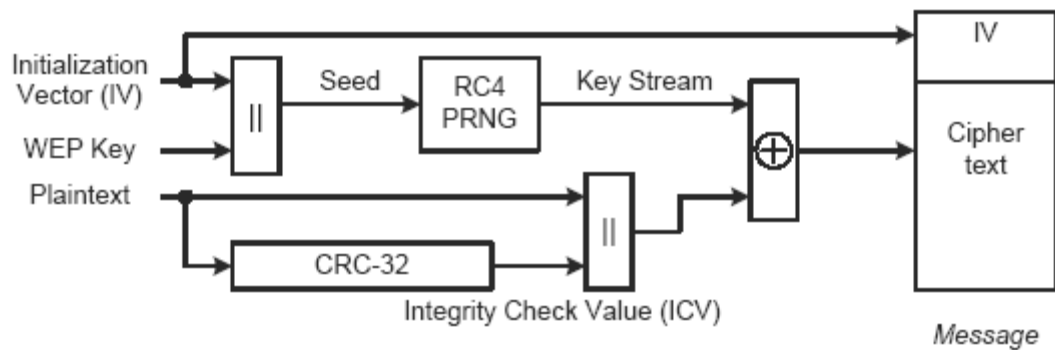
4. 无线加密机制

4.1.WEP

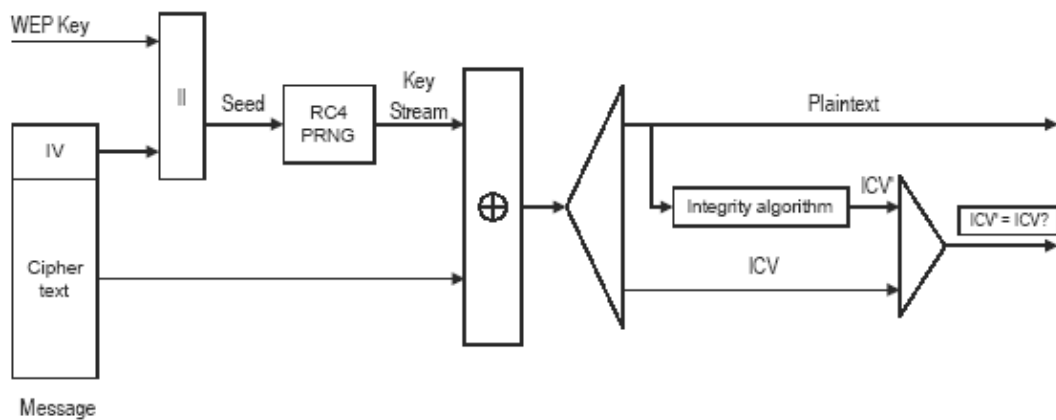
WEP 是 Wired Equivalent Privacy 的简称。WEP 提供了 40 (64 位) 和 128 位长度的密钥机制。

WEP 的加密方式是对称的(Symmetric)，所以双方需要有相同的一把 Key，然而对于密钥管理(即如何让双方达成协议，协商出同一 key)，IEEE 802.11 是假设已经成功了。

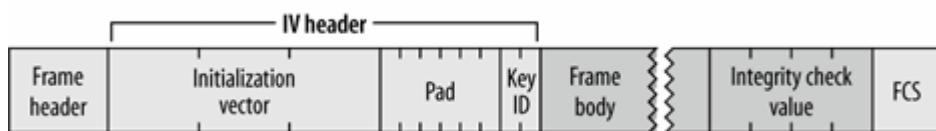
WEP 加密流程图：



WEP 解密流程图：



WEP 帧格式



4.2. TKIP

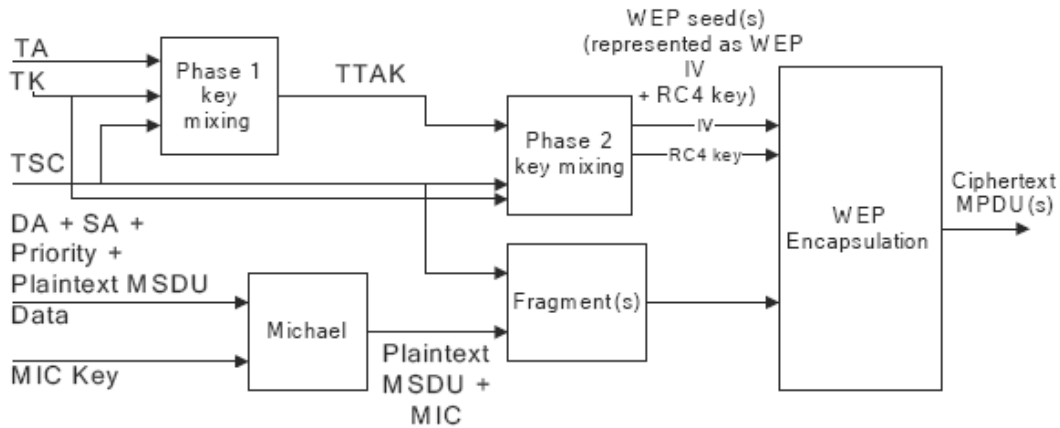
TKIP 是作为 IEEE 802.11i 的一部分，为加强无线安全性而创建的。它也是基于 RC4 封装算法。TKIP 通过动态密钥管理增强了加密功能，这种管理要求每个传输的数据包有一个与众不同的密钥。

必须认识到，加密是实现网络安全的必需手段，但加密只能提供数据私密功能。TKIP 在加密基础上更进一步，通过 64 位消息完整性检查（MIC）来提供数据修改保护，该数据完整性的算法被称为 Michael。它可以有效防止黑客截获消息、修改数据片断、修改完整性检查值（ICV）片断进行匹配、重新创建循环冗余检查（CRC）并将数据包转发到目的地。

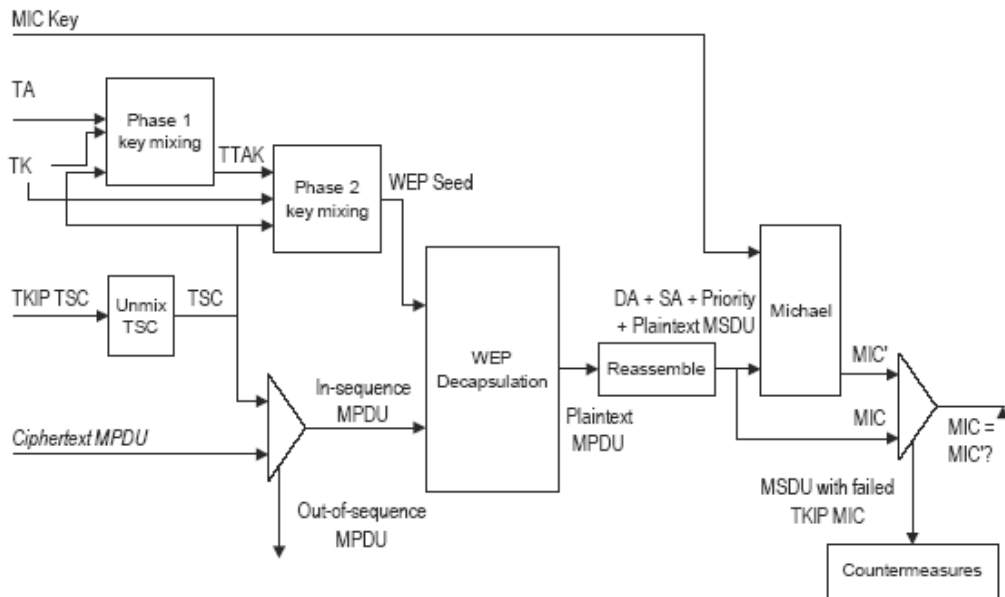
上述过程就是 TKIP 的重发保护措施。MIC 故障首次出现时，端点需要断开与 AP 的连接并重新接入。对于在 60 秒内检测到两次 MIC 故障的端点，IEEE 802.11i 要求其停止所有通信 60 秒。

通过扩展密钥的长度，增加利用密钥的数量，并创建完整性验证机制，TKIP增大了在 Wi-Fi网络上解码数据所蕴含的复杂性和难度，使入侵者更难以侵入网络。

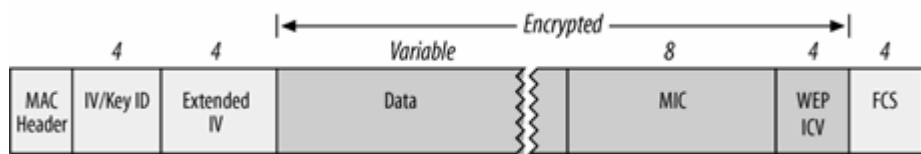
TKIP加密流程图：



TKIP解密流程图：



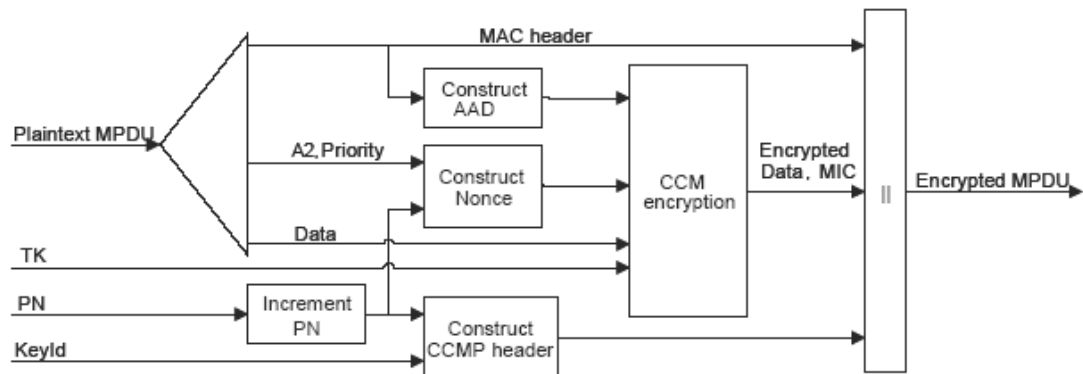
TKIP报文格式：



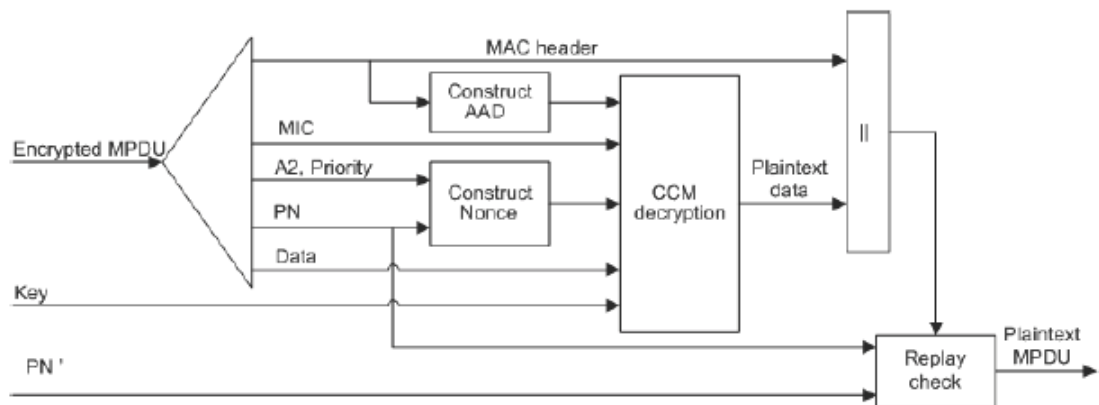
4.3. CCMP

CCMP 是面向大众的最高级无线安全协议。IEEE 802.11i 要求使用 CCMP 来提供全部四种安全服务：认证、机密性、完整性和重发保护。CCMP 使用 128 位 AES 加密算法实现机密性，CCMP 使用 CBC-MAC 来保证数据的完整性和认证。

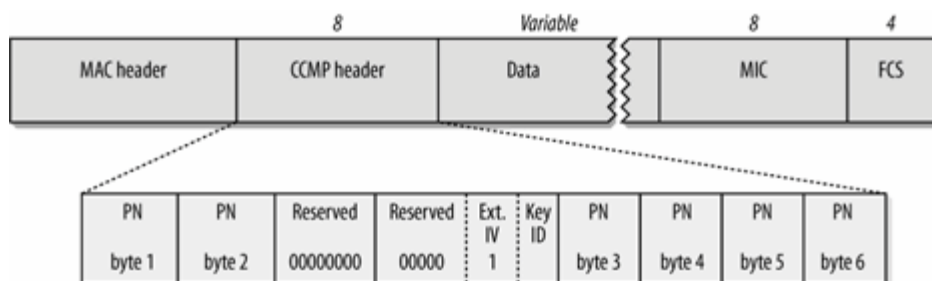
CCMP 加密



CCMP 解密



CCMP 报文格式：

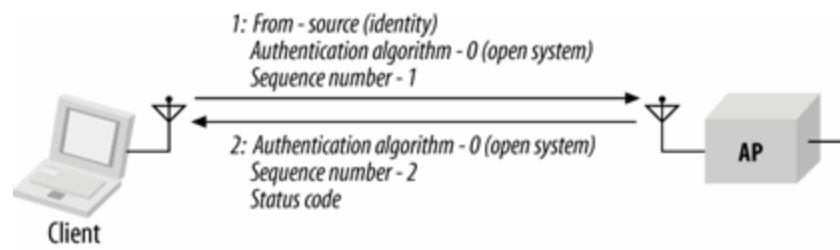


5. 无线认证机制

5.1. 开放系统身份验证

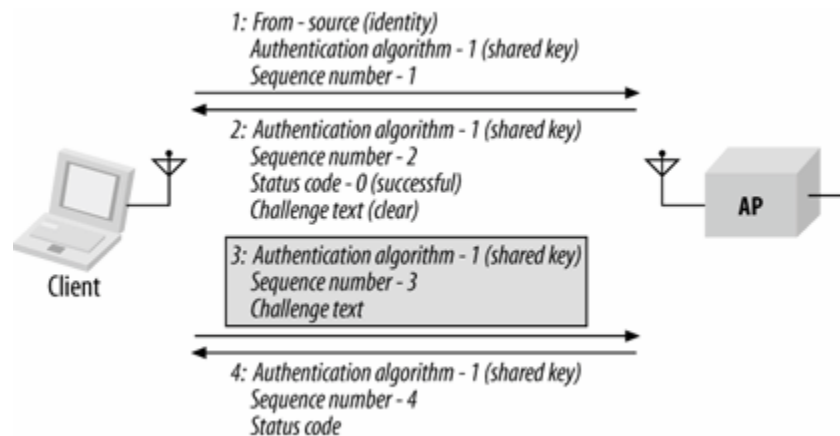
开放系统认证允许任何用户接入到无线网络中来。从这个意义上来说，实际上并没有提供对数据的保护。

开放系统型认证只包含两次通信。第一次通信是客户机发出认证请求，请求中包含客户端 ID（通常为 MAC 地址）。第二次通信是接入点发出认证响应，响应中包含表明认证成功还是失败的消息。



5.2. 共享密钥身份验证

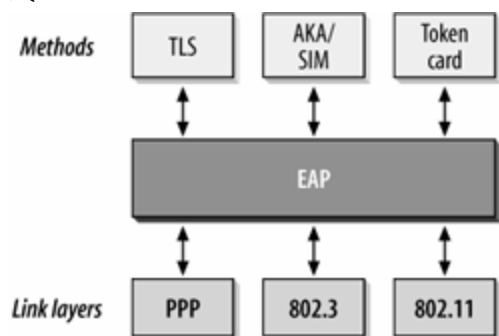
这个过程步骤包括：客户机发送认证请求，接入点以明文形式发出盘问文本，客户机对盘问文本进行加密并发送加密结果给接入点，接入点做出认证响应。



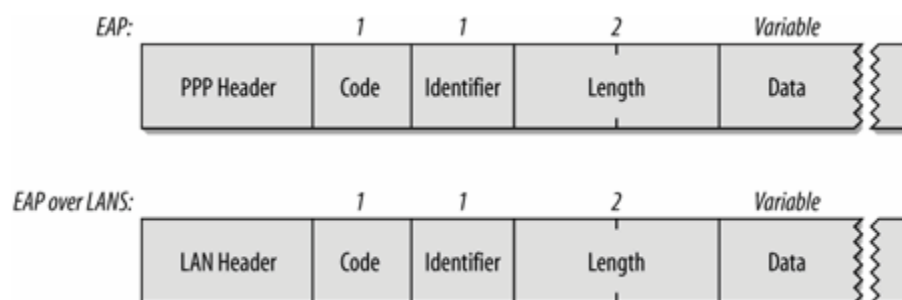
5.3. EAP

5.3.1. EAP 协议

EAP (Extensible Authentication Protocol) 定义了可扩展的身份验证协议。属于一种框架协议。EAP 本身并未规范如何识别用户,但允许协议设计人员打造自己的 EAP 认证方式(EAP method)。如下图, EAP 的设计目的是为了能够运行于任何链路层以及使用各种身份验证方式。



EAP 使用的报文格式如下图:



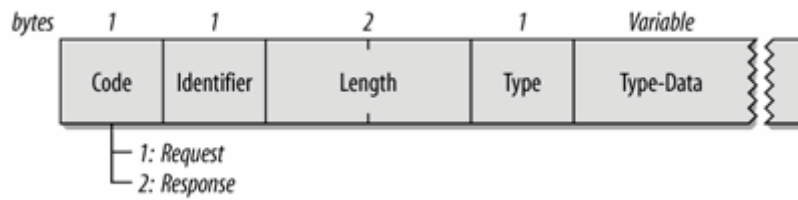
Code 域表示报文类型:

- 1—Request (请求)
- 2—Response (响应)
- 3—Success (成功)
- 4—Failure (失败)

Identifier 为标示符编号。用来匹配请求与响应。新的传送使用新的 Identifier, 重传则使用相同的 Identifier。

Length 为整个报文长度。包括 Code, Identifier, Length 和 Data。

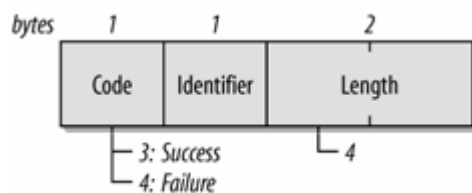
EAP 请求和响应报文格式如下:



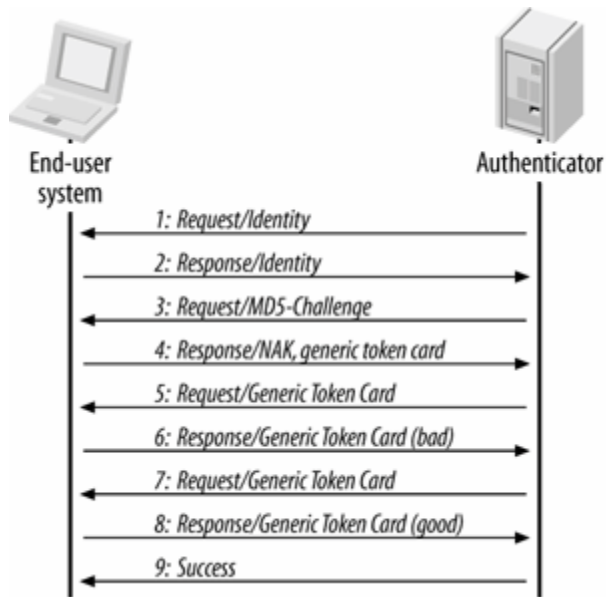
Type 代表请求或响应的类型。1 表示身份（Identify）。2 表示通知（Notification），是认证系统提示给用户消息，例如密码即将过期等。3 表示 NAK，用于建议使用新的认证方式。大于或等于 4 的 Type 代表认证方式（EAP method）。

Type code	Authentication protocol	Description
4	MD5 Challenge	CHAP-like authentication in EAP
6	GTC	Originally intended for use with token cards such as RSA SecurID
13	EAP-TLS	Mutual authentication with digital certificates
21	TTLS	Tunneled TLS; protects weaker authentication methods with TLS encryption
25	PEAP	Protected EAP; protects weaker EAP methods with TLS encryption
18	EAP-SIM	Authentication by mobile phone Subscriber Identity Module (SIM)
29	MS-CHAP-V2	Microsoft encrypted password authentication; compatible with Windows domains

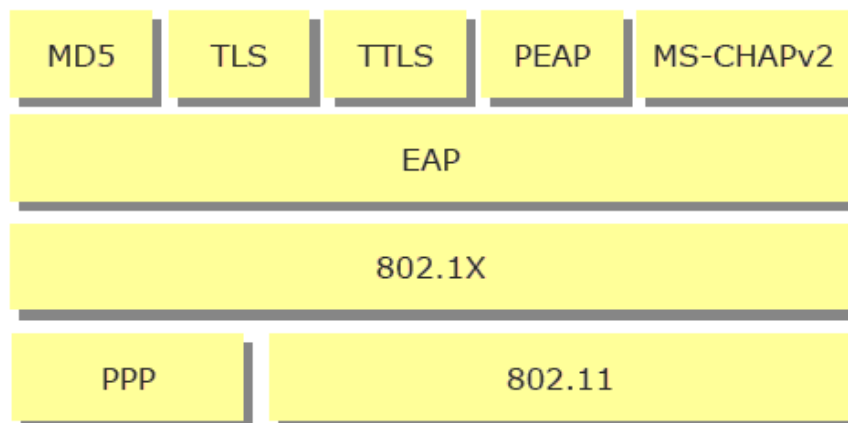
EAP 认证成功和失败报文格式如下：



EAP 认证过程非常简单，是由一系列请求/响应以及最终的成功或失败构成。下图为认证过程的范例：



5.3.2. EAP 多种认证方式



EAP-MD5

MD5 是一种基本的认证方法，当需要很强的安全需求的时候，他并不十分适当。系统产生一个随机数，这个用于挑战的随机数发送给客户端，客户端取出共享的密钥，采用 HASH 算法计算出挑战的响应并回送给服务器。MD5 容易受到基于字典的攻击，因此对于用户来讲，选择非字典的密码非常重要。此外 MD5 是一种单向认证方法。

EAP-TLS: Transport Layer Security。

在 Client 和 Server 之间建立一个 TLS 会话，证明（certification）和确认（Validation）是基于数字证书的双向认证。对服务器和终端双方都要求拥有数字证书。

PEAP

PEAP 的全称为 protected eap(受保护的 EAP)，它是由微软创导的，得到了思科的强烈拥护。它的主要思想是：802.1X 认证的过程被分成两个阶段，第一阶段先做 eap-tls 认证，借助 TLS 的握手，先建立一个安全（防中间人攻击，防报文回放，防报文篡改）的通道（就是加密手段），在 TLS 通道之内进行第二次的 eap 认证（在协议中规定，必须是 EAP），这样 eap 认证的整个过程都是加密的，就达到了保护 eap 认证的目的。

PEAP 认证和 TLS 认证最大的不同就是，PEAP 上客户端不需要在 TLS 握手的阶段把 TLS 证书上传上去（因为 PEAP 将在第二阶段做 eap 认证来完成服务器对客户端的校验）。

PEAP 认证过程中需要从服务器把自己的 x.509 证书（服务器证书，或者是一个证书链）下发到客户端上来。客户端需要对服务器证书进行校验，通常情况下需要在客户端安装一个信任的根证书来校验服务器证书的合法性，从而证明服务器的身份。

EAP-TTLS（Tunneled Transport Layer Security 隧道传输层安全协议）：

TTLS 是 TLS 的扩展，TTLS 这种方式应用时，首先在客户端和 TTLS 服务器间建一个 TLS 加密隧道，这个加密隧道只是用于保护客户端的认证数据。而在第二阶段，TTLS 与 PEAP 类似。TTLS 与 PEAP 区别是，peap 必须做的是 EAP 认证，而不能是其他的认证方式，比如 pap 和 chap，而 ttls 允许在第二阶段进行 pap 或者 chap 认证。

LEAP（轻量级扩展身份认证协议）

Cisco LEAP 是一种用于认证 802.11 客户端的 RADIUS EAP 认证协议。LEAP 的特点就是双向认证、每用户的动态安全会话密钥的分发、每用户的会话的 WEP 密钥。双向认证的安全性依赖于用户共享密钥—用户的登录密码—认证服务器和认证客户端都知道这个密码。用户密码用于 RADIUS 服务器和客户端之间的挑战报文的计算。起初 Cisco 的 LEAP 协议只支持 Cisco 自己 AP 和网卡设备，Cisco 公司启动了思科兼容扩展 CCX 的活动，将对 LEAP 有兴趣的芯片进行了处理，使得 Cisco 接入点可认证那些采用 LEAP 认证技术的非 Cisco 的客户端。

MS-CHAP V2

Ms-Chapv2 协议是微软发明的一种认证方式，它最初是被使用在 PPP 线路上的一种用来替代 CHAP 的一种认证方式。它提供了双向认证的功能（即服务器可以认证客户端，客户端可以认证服务器）。

具体的认证原理如下：

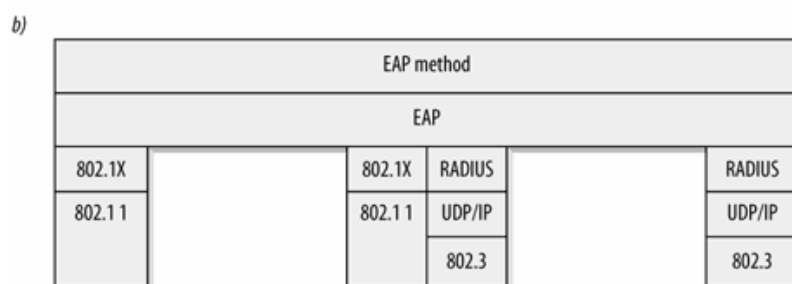
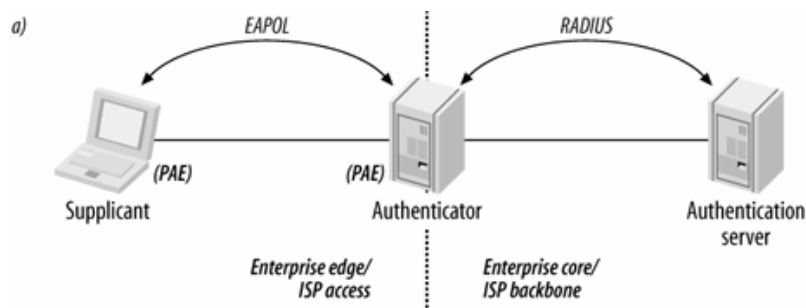
1. 服务器给客户端发送一个挑战字(challenge)
2. 客户端把自己的密码和服务器的 challenge 进行运算 client hash 值，同时产生一个自己的挑战字，发送给服务器。
3. 服务器比较客户端发送过来的 client hash 值（对客户端进行认证，验证了客户端的密码是正确的），然后把客户端的密码和客户端发送过来的 challenge 计算 server hash 值，把 server hash 发送给客户端，同时通知客户端认证成功。
4. 客户端比较服务器发送过来的 server hash，完成对服务器的认证（验证了服务器知道客户端的密码）。

	EAP-MD5	EAP-TLS	EAP-PEAP	EAP-TTLS	EAP-MSCHAPV2
密码学原理	对称	非对称	非对称	非对称	对称
支持双向认证	否	是	可选	可选	是
产生会话密钥	否	是 (TLS Master Key)	是 (TLS Master Key)	是 (TLS Master Key)	是(根据 MPPE 算法)
抗字典攻击	否	是	是	是	是
数据签名	否	是	是	是	否
服务器证书	否	是	是	是	否
客户端证书	否	是	可选	可选	否
用户名&密码	是	否	可选	可选	是

5.3.3. 802.1X

IEEE 802.1X 称为基于端口的访问控制协议 (Port based network access control protocol)。它定义了一种认证的框架。802.1X 为认证的会话过程定义了 3 个组件：申请者 (supplicant)，认证者 (authenticator) 和认证服务器 (AS)。

802.1X 定义的认证过程如下图：

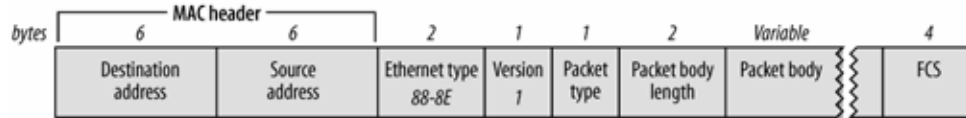


802.1X 指定 EAP 作为认证方法，同时定义了 EAPOL 帧对 EAP 帧进行封装。下图为 EAPOL 帧格式：

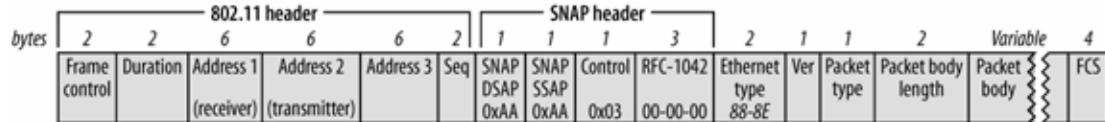


Wlan 技术白皮书—安全

a) EAPOL on Ethernet



b) EAPOL on 802.11



Ethernet type 表示以太网类型。对 EAPOL 帧，这个值为 0X888E。

Version 表示 802.1X 版本号。

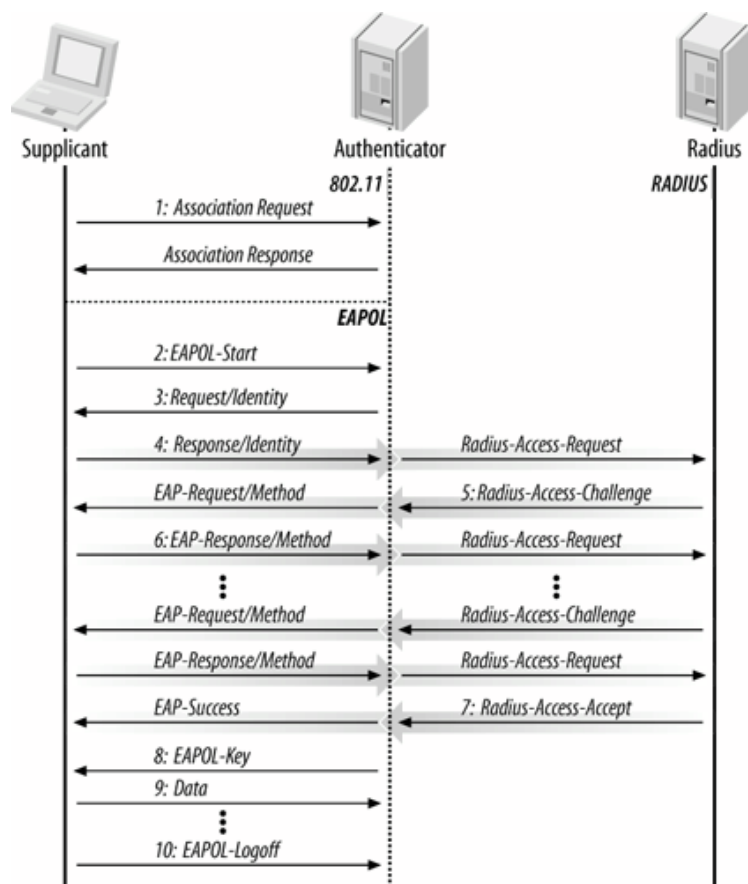
Packet Type 表示 EAPOL 帧的类型，如下表：

Packet type	Name	Description
0000 0000	EAP-Packet	Contains an encapsulated EAP frame. Most frames are EAP-Packet frames.
0000 0001	EAPOL-Start	Instead of waiting for a challenge from the authenticator, the supplicant can issue an EAPOL-Start frame. In response, the authenticator sends an EAP-Request/Identity frame.
0000 0010	EAPOL-Logoff	When a system is done using the network, it can issue an EAPOL-Logoff frame to return the port to an unauthorized state.
0000 0011	EAPOL-Key	EAPOL can be used to exchange cryptographic keying information.
0000 0100	EAPOL-Encapsulated-ASF-Alert	The Alerting Standards Forum (ASF) has defined a way of allowing alerts, such as SNMP traps, to be sent to an unauthorized port using this frame type.

5.3.4. 无线局域网的 802.1X 认证

802.1X 认证过程与 EAP 认证过程基本相同，主要差别是申请者可以发出 EAPOL-Start 帧触发 EAP 交换，也可以在网络使用完毕后发出 EAPOL-Logoff 消息解除连接端口的授权。

下图为无线局域网的 802.1X 认证的范例：



6. 密钥管理机制

6.1. 密钥的产生和管理

安全的核心就是对加密密钥的管理。802.11i 用于数据加密、校验的密钥都是由 Master key 衍生。Master Key 的获取方式没有在 802.11i 中明确规定，可参照运营商标准或自己标准实现。

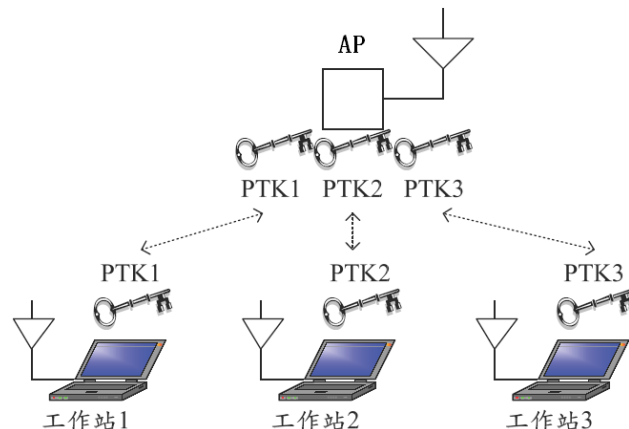
1、Master Key 的来源

EAP-TLS、EAP-PEAP 等认证方式的 Master Key 是在认证过程动态协商生成(由认证方式协议中规定)，由 AS(认证服务器)和 STA 上实现，对 AP 来说是透明的。如果是 EAP-MD5 认证，由于没有 STA 和 AS 协商 Master Key 过程，Master Key 直接用用户密码。但由于 AP 不知道 Master Key，需要从 AS 上发给 AP。如果是 AP 发起认证，AP 上会有 Radius Client，则 Master Key 会记录在 Radius Access-Accept 报文中的 MS-MPPE-Send-Key 属性。

2、单播密钥衍生算法

AP 上获得的 Master key 只是种子密钥，要由它来衍生出数据加密密钥、MIC Key、EAPOL-Key 报文 MIC Key、EAPOL-Key 报文加密密钥等。密钥衍生算法在 STA 和 AP 上实现，同样的 Master Key 可衍生同样的子密钥。802.11i 定义了四次握手流程。

$$PTK = PRF(PMK, \text{"Pairwise key expansion", Min(AA, SA) \parallel Max(AA, SA) \parallel Min(SNonce, ANonce) \parallel Max(SNonce, ANonce)})$$



以 TKIP 为例：

PRF 输出为 0-127bit 是 MIC Key，它用于检查 802.1X 组密钥分发过程中的 EAPOL-Key 报文的 MIC 检查。128-255bit 是 EK，用于对广播密钥交换的过程中对 EAPOL-Key Descriptor 的 Key 进行加密。256-383bit 是 TK1，用于单播数据的 TKIP 加密；384-447bit 是发送时计算单播 MIC 的 MICKey；447-511bit 是接收时校验 MIC 的 MIC Key。

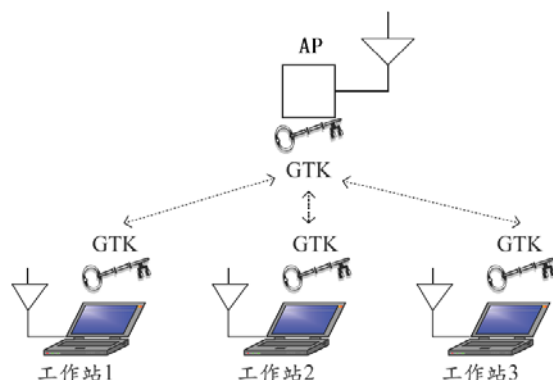
注：增强的伪随机功能（PRF）是 TLS 标准定义的一种生成密钥的算法。

3、多播的密钥衍生算法

在 AP 和多个 STA 之间传递的多播报文，由于是点对多点，需要在 AP 与多个 STA 之间生成相同加密密钥，所以多播密钥的衍生与单播是不相同的。单播密钥实际是通过特定算法在 STA 与 AP 上同时生成的，而多播密钥是在 AP 上生成后经过加密发送给 STA 的。

在四次握手之后才可以进行广播密钥的派生。GMK 应该只存在于 AP 中，它被初始化为一个随机数或 AP 收到的第一个 PMK，它应该周期更新。并且如果有 STA 分离，且当时使用的 GMK 正好是该 STA 的 PMK，则 GMK 需要更新为其它正在使用的 PMK。

$$GTK = PRF(GMK, \text{"Group key expansion", AA \parallel GNonce})$$



对于 TKIP 来说, GMK 通过 PRF 生成的 TGK 有 256bit, 0-127 为 TEK 用于加密广播包; 127-191 为 TX MIC Key 用于对发送的广播报文计算 MIC; 192-255 为 RX MIC Key 用于对收到的广播报文校验 MIC Key。

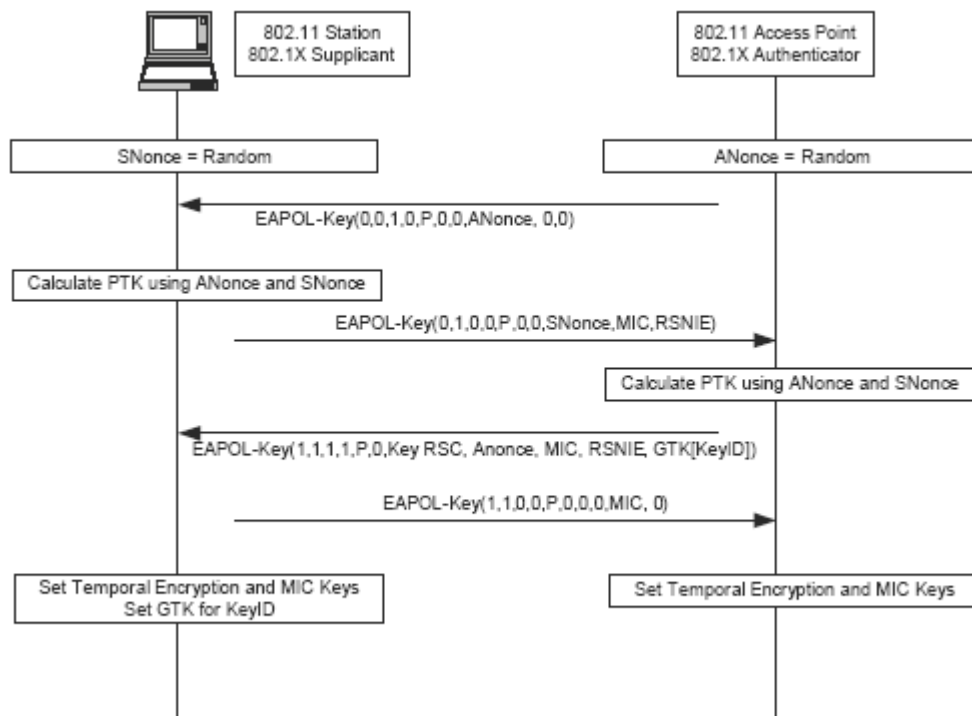
6.2. 密钥交互和握手流程

6.2.1. 单播密钥更新的四次握手流程

802.11i 中定义了单播密钥更新的四次握手过程。新的数据加密密钥没有在空中传递, 而是通过确定的衍生算法在 STA 和 AP 上同时产生, 条件触发时, 执行握手流程。

单播密钥更新策略: 收到 STA 的密钥更新请求时; 收到 AS 发来的 MasterKey 时; 收到的报文 MIC 检查错误时; 计时器发起周期性更新。四种情况发起更新流程:

- 1、AP 通过产生 ANonce 发送给 STA, 该 EAPOL-Key 不进行 MIC 校验;
- 2、STA 通过产生 SNonce 计算生成 PTK, STA 将 SNonce 发给 AP, 对消息进行 MIC 校验;
- 3、AP 对消息进行 MIC 校验, 若正确则使用步骤 2 中的算法得到 PTK;
- 4、AP 再次将 ANonce 发送给 STA, 指示 STA 临时密钥是否可用, 对该消息进行 MIC 校验;
- 5、如果临时密钥可用, STA 回应消息确认, 该消息要 MIC 校验, 同时用新密钥加密。

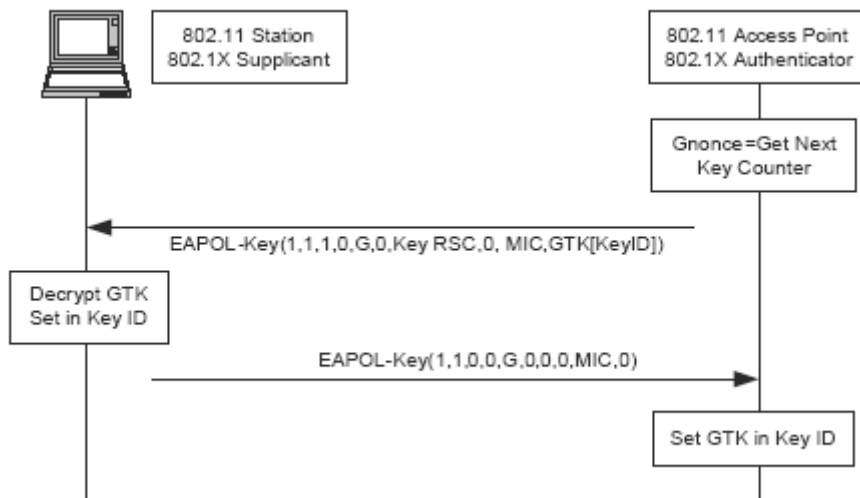


6.2.2. 广播密钥更新流程

在 AP 与 STA 之间的广播包(特指 AP 的广播包,STA 发的广播包还是用单播密钥加密),用广播密钥进行加密。鉴于广播密钥是 AP 对应多个 STA,不能象单播密钥那样通过四次握手来完成更新,而是由 AP 把密钥经过加密后发给 STA,所以又定义了两次握手的流程。

AP 产生一个 GTK,将其加密后通过 EAPOL-Key 报文发给 STA 且带有 MIC。MIC Key 和加密 GTK 的密钥都是通过特定的衍生算法在 AP 与 STA 上同时产生的。

- 1、STA 收到该 Msg 后检查 MIC,解密出 GTK。并把该密钥记录,STA 回 Ack 消息,带有 MIC。
- 2、AP 检查 Ack 消息的 MIC,如果合法,把该密钥记录入加密引擎。密钥变换成功。



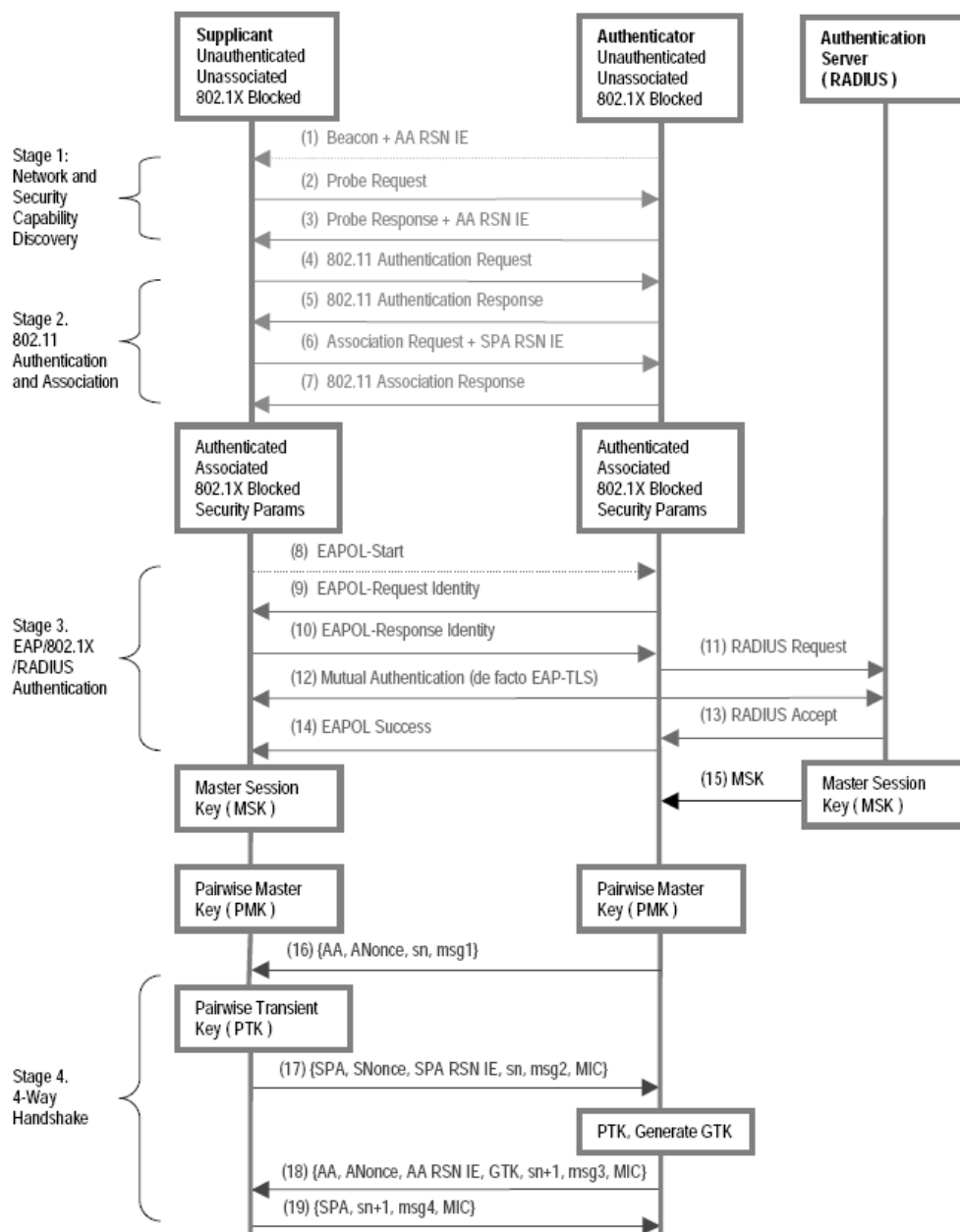
广播密钥更新策略:当收到广播报文 MIC 检查错误时;当某个用户退出或加入时;收到新的 GMK 时;收到密钥更新请求时;计时器发起周期性更新。发起更新流程。

7. 参考文献

《802.11 Wireless Networks The Definitive Guide》

《802.11 Wireless LAN Fundamentals (CISCO) .pdf》

8. 附录：一个完整的 802.1X 认证过程



在这个图中，整个无线的认证过程被分成了 4 个阶段：

第一阶段：

网络发现阶段，AP 发出广播无线信号，STA 发送探测请求，AP 回应探测，同时告知安全参数。



第二阶段:

802.11 associate 阶段:

STA 发送 802.11 的认证请求(Open System), AP 给出回应, STA 发送 Associate 请求, AP 给出 associate 的回应。

第三阶段:

STA 发起 802.1x 认证, AP(也有可能是 AC, 取决于组网方式)和 Radius 服务器对 802.1x 认证进行交互。值得注意的是在 802.11i 中, 在这个阶段必须能产生出一个 PMK(pairwise master key), 同时给 STA 和 AP, 这个 PMK(pairwise master key)是用来在下一个阶段使用的。

第四个阶段:

由 AP 发起 eapol-key 的交互过程, 通过这四次的交互过程, 产生了一个共享的密钥(PTK)。然后 802.1x 把 OID_802_11_ADD_KEY 这个 OID 设置入硬件中, 让硬件为数据加密产生基础。

对于第一阶段的客户端的实现原理如下:

通过 OID_802_11_BSSID_LIST_SCAN 这个 OID 向硬件请求扫描到的射频信息 SSID, 以及信号强度和所采用的安全信息, 认证方式和加密方式。

对于第二阶段的客户端实现原理如下:

通过 OID_802_11_INFRASTRUCTURE_MODE 设置无线网卡的工作模式, 通过 OID_802_11_PRIVACY_FILTER 设置无线网卡的加密密钥来源, 通过 OID_802_11_AUTHENTICATION_MODE 来设置网卡的认证方式, 通过 OID_802_11_ENCRYPTION_STATUS 来设置无线网卡的加密算法, 最后通过设置 OID_802_11_SSID 来设置网卡所选择的 SSID, 这样就可以让网卡实现 associate 了。

对于第三阶段的客户端实现原理如下:

做一种 802.1x 认证, 比如说 peap 认证, 保存协商出来的共享密钥 PMK。

对于第四阶段的客户端实现原理如下:

按照 ieee 802.11i 的 8.5.3.6 的节示范的例子来说明进行 eapol-key 的 4 次交互过程, 最后得到 PTK 以后, 通过 OID_802_11_ADD_KEY 来设置网卡的密钥 PTK。认证到这一步就成功了。