# Wifi 认证及加密详解

## 1. 无线安全概述

无线安全是 WLAN 系统的一个重要组成部分。由于无线网络使用的是开放性媒介采用公共电磁波作为载体来传输数据信号，通信双方没有线缆连接。如果传输链路未采取适当的加密保护，数据传输的风险就会大大增加。因此在 WLAN 中无线安全显得尤为重要。

为了增强无线网络安全性，至少需要提供认证和加密两个安全机制：

- 认证机制：认证机制用来对用户的身份进行验证，以限定特定的用户（授权的用户）可以使用网络资源。
- 加密机制：加密机制用来对无线链路的数据进行加密，以保证无线网络数据只被所期望的用户接收和理解。

## 2. 基本概念

802.11i：新一代 WLAN 安全标准。IEEE 为弥补 802.11 脆弱的安全加密功能而制定的修正案，802.11i 提出了 RSN(强健安全网络)的概念，增强了 WLAN 中的数据加密和认证性能，并且针对 WEP 加密机制的各种缺陷做了多方面的改进。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 AES 加密算法。

RC4：在密码学领域，RC4 是应用最广泛的流加密算法，属于对称算法的一种。

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

EAPOL-KEY 包( EAP over LAN key ):AP 同 STA 之间通过 EAPoL-key 报文进行密钥协商。

PMK（Pairwise Master Key，成对主密钥）：申请者（Supplicant）与认证者（Authenticator）之间所有密钥数据的最终来源。它可以由申请者和认证服务器动态协商而成，或由预共享密钥（PSK）直接提供。

PTK( Pairwise Transient Key ,成对临时密钥):PTK 是从成对主密钥( PMK )中生成的密钥，用于加密和完整性验证。

GMK( Group Master Key ,组主密钥):认证者用来生成组临时密钥( GTK )的密钥，通常是认证者生成的一组随机数。

GTK（Group Transient Key，组临时密钥）：由组主密钥（GMK）通过哈希运算生成，是用来保护广播和组播数据的密钥。

MIC（message integrity code，消息完整性校验码）。针对一组需要保护的数据计算出的散列值，用来防止数据遭篡改。

## 3. 链路认证方式

链路认证即 802.11 身份验证，是一种低级的身份验证机制。在 STA 同 AP 进行 802.11 关联时发生，该行为早于接入认证。任何一个 STA 试图连接网络之前，都必须进行 802.11 的身份验证进行身份确认。可以把 802.11 身份验证看作是 STA 连接到网络时的握手过程的起点，是网络连接过程中的第一步。

IEEE 802.11 标准定义了两种链路层的认证：

开放系统身份认证

共享密钥身份认证

### 3.1(open)开放系统身份认证

开放系统身份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，即不认证。也就是说，如果认证类型设置为开放系统认证，则所有请求认证的 STA 都会通过认证。

开放系统认证包括两个步骤：

第一步，STA 请求认证。STA 发出认证请求，请求中包含 STA 的 ID（通常为 MAC 地址）。

第二步，AP 返回认证结果。AP 发出认证响应，响应报文中包含表明认证是成功还是失败的消息。如果认证结果为“成功”，那么 STA 和 AP 就通过双向认证。

**3.2(shared)共享密钥身份认证**

接入认证是一种增强WLAN网络安全性的解决方案。当STA同AP关联后，是否可以使用无线接入点的服务要取决于接入认证的结果。如果认证通过，则无线接入点共享密钥认证是除开放系统认证以外的另外一种认证机制。共享密钥认证需要 STA 和 AP 配置相同的共享密钥。共享密钥认证的过程如下：

第一步，STA 先向 AP 发送认证请求；

第二步，AP 会随机产生一个 Challenge 包（即一个字符串）发送给 STA；

第三步，STA 会将接收到字符串拷贝到新的消息中，用密钥加密后再发送给 AP；

第四步，AP 接收到该消息后，用密钥将该消息解密，然后对解密后的字符串和最初给 STA 的字符串进行比较。如果相同，则说明 STA 拥有无线设备端相同的共享密钥，即通过了共享密钥认证；否则共享密钥认证失败。

接入认证方式

为 STA 打开这个逻辑端口，否则不允许用户连接网络。

本节介绍以下两种接入认证方式：

PSK 接入认证

802.1X 接入认证

**3.3PSK 接入认证**

PSK （Pre-shared key，预共享密钥）是一种 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。该认证方式需要在无线用户端和无线接入设备端配置相同的预共享密钥。如果密钥相同， PSK 接入认证成功；如果密钥不同，PSK 接入认证失败。

**3.4802.1X 接入认证**

IEEE 802.1X 协议是一种基于端口的网络接入控制协议。这种认证方式在 WLAN 接入设备的端口这一级对所接入的用户设备进行认证和控制。连接在接口上的用户设备如果能通过认证，就可以访问 WLAN 中的资源；如果不能通过认证，则无法访问 WLAN 中的资源。

一个具有 802.1x 认证功能的无线网络系统必须具备以下三个要素才能够完成基于端口的访问控制的用户认证和授权：

认证客户端

一般安装在用户的工作站上，当用户有上网需求时，激活客户端程序，输入必要的用户名和口令，客户端程序将会送出连接请求。

认证者

在无线网络中就是无线接入点 AP 或者具有无线接入点 AP 功能的通信设备。其主要作用是完成用户认证信息的上传、下达工作，并根据认证的结果打开或关闭端口。

认证服务器

通过检验客户端发送来的身份标识（用户名和口令）来判别用户是否有权使用网络系统提供的服务，并根据认证结果向认证系统发出打开或保持端口关闭的状态。

## 4. 无线加密方式

相对于有线网络，无线网络存在着更大的数据安全隐患。在一个区域内的所有的 WLAN 设备共享一个传输媒介，任何一个设备可以接收到其他所有设备的数据，这个特性直接威胁到 WLAN 接入数据的安全。IEEE 802.11 提供三种加密算法：有线等效加密（WEP）、暂时密钥集成协议（TKIP）和高级加密标准 AES-CCMP。

WEP 加密

TKIP 加密

AES-CCMP 加密

### 4.1WEP 加密

WEP（Wired Equivalent Privacy，有线等效加密）是原始 IEEE 802.11 标准中指定的数据加密方法，是 WLAN 安全认证和加密的基础，用来保护无线局域网中授权用户所交换的数据的私密性，防止这些数据被窃取。

WEP 使用 RC4 算法来保证数据的保密性，通过共享密钥来实现认证。WEP 没有规定密钥的管理方案，一般手动进行密钥的配置与维护。通常把这种不具密钥分配机制的 WEP 称为手动 WEP 或者静态 WEP。

WEP 加密密钥的长度一般有 64 位和 128 位两种。其中有 24Bit 的 IV（Initialization Vector，初始化向量）是由系统产生的，因此需要在 AP 和 STA 上配置的共享密钥就只有 40 位或 104 位。在实际中，已经广泛使用 104 位密钥的 WEP 来代替 40 位密钥的 WEP，104 位密钥的 WEP 称为 WEP-104。虽然 WEP104 在一定程度上提高了 WEP 加密的安全性，但是受到 RC4 加密算法以及静态配置密钥的限制，WEP 加密还是存在比较大的安全隐患，无法保证数据的机密性、完整性和对接入用户实现身份认证。

### 4.2 TKIP 加密

TKIP（Temporal Key Integrity Protocol，暂时密钥集成协议）是 IEEE 802.11 组织为修补 WEP 加密机制而创建的一种临时的过渡方案。它也和 WEP 加密机制一样使用的是 RC4 算法，但是相比 WEP 加密机制，TKIP 加密机制可以为 WLAN 服务提供更加安全的保护。主要体现在以下几点：

静态 WEP 的密钥为手工配置，且一个服务区内的所有用户都共享同一把密钥。而 TKIP 的密钥为动态协商生成，每个传输的数据包都有一个与众不同的密钥。

TKIP 将密钥的长度由 WEP 的 40 位加长到 128 位，初始化向量 IV 的长度由 24 位加长到 48 位，提高了 WEP 加密的安全性。

TKIP 支持 MIC 认证（Message Integrity Check，信息完整性校验）和防止重放攻击功能。

### 4.3 AES-CCMP 加密

AES-CCMP（Counter mode with CBC-MAC Protocol，计数器模式搭配 CBC-MAC 协议）是目前为止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 （Advanced Encryption Standard，高级加密标准）加密算法实现机密性，使用 CBC-MAC（区块密码锁链 - 信息真实性检查码协议）来保证数据的完整性和认证。

作为一种全新的高级加密标准，AES 加密算法采用对称的块加密技术，提供比 WEP/TKIP 中 RC4 算法更高的加密性能，它将在 IEEE 802.11i 最终确认后，成为取代 WEP 的新一代的加密技术，为无线网络带来更强大的安全防护。

## 5.WPA 安全技术

WPA（Wi-Fi Protected Access），是一种保护无线电脑网络(Wi-Fi)安全的系统，它是应研究者在前一代的系统有线等效加密（WEP）中找到的几个严重的弱点而产生的。

WPA 安全技术允许采用更多样的认证和加密方法来实现 WLAN 的访问控制、密钥管理与数据加密。例如，接入认证方式可采用预共享密钥（PSK 认证）或 802.1X 认证，加密方法可采用 TKIP 或 AES。WPA 同这些加密、认证方法一起保证了数据链路层的安全，同时保证了只有授权用户才可以访问无线网络 WLAN。

### 5.1 WPA

Wi-Fi 联盟在标准推出之前，在 802.11i 草案的基础上，制定了一种称为 WPA(Wi-Fi Protected Access)的安全机制，它使用 TKIP(临时密钥完整性协议)，它使用的加密算法还是 WEP 中使用的加密算法 RC4，所以不需要修改原来无线设备的硬件。

其目的在于代替传统的 WEP 安全技术，为无线局域网硬件产品提供一个过渡性的高安全解决方案，同时保持与未来安全协议的向前兼容。可以把 WPA 看作是 IEEE802.11i 的一个子集，其核心是 IEEE 802.1X 和 TKIP。

## 5.2 WPA2

WPA2 是经由 Wi-Fi 联盟验证过的 IEEE 802.11i 标准的认证形式。它使用 CCM(Counter-Mode/CBC-MAC)认证方式和 AES（Advanced Encryption Standard）加密算法，更进一步加强了无线局域网的安全和对用户信息的保护。