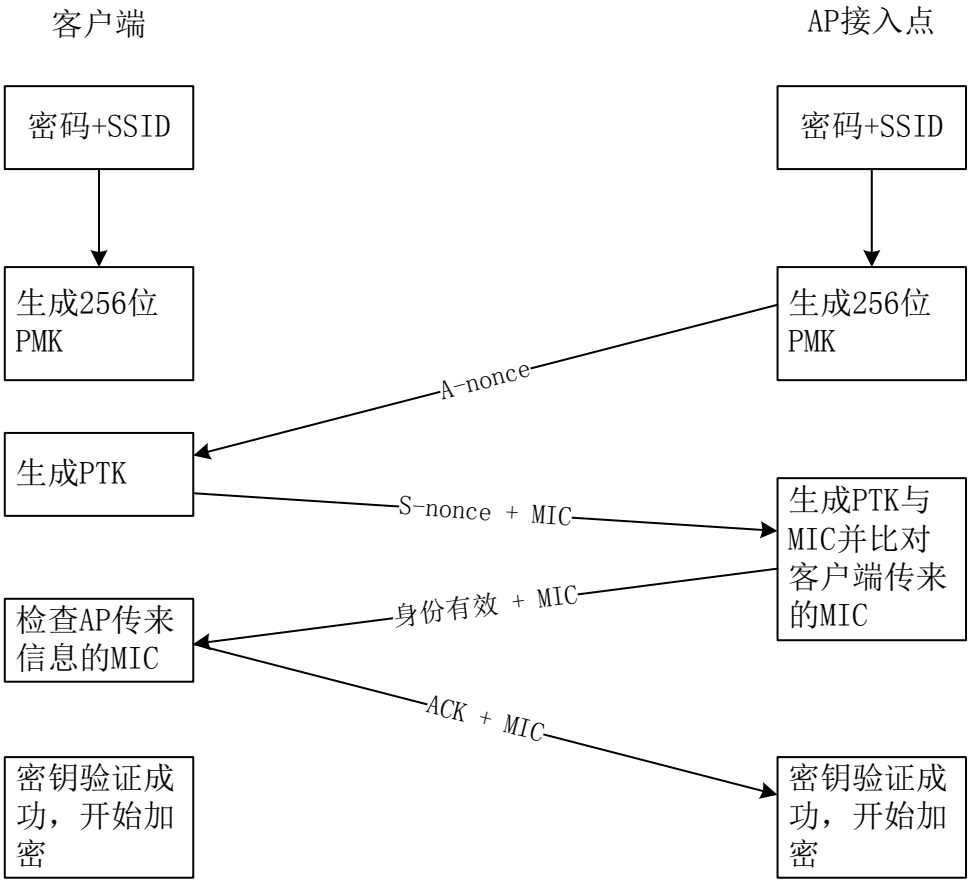
# WPA/WPA2-PSK 认证机制初探

我们知道，使用 wpa/wpa2-psk 认证的 AP（或者无线路由器）的密码可以是 8~63 位长度之间任意的 ASCII 码字符。但是 wpa/wpa2-psk 认证的具体过程是怎样的呢？下面我们就一起来认识一下。

首先我们来看一下流程图，此过程被称为 WPA/WPA2-PSK 的“四次握手”。




图一 一次成功的“四次握手”过程

| | Time | Source | Destination | Protocol | Length | Info | RSSI | TX | Channel |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | e8:91:20:b3:e2:4d | 12:0e:0e:20:d5:9f | 802.11 | 136 | Probe Request, SN=3658, FN=0, Flags=........C, SSID=SUNDRAY | -62 dBm | 1.0 | 2412 MHz |
| 2 | 0.003671 | 12:0e:0e:20:d5:9f | e8:91:20:b3:e2:4d | 802.11 | 322 | Probe Response, SN=3149, FN=0, Flags=........C, BI=100, SSID=SUNDRAY | -34 dBm | 1.0 | 2412 MHz |
| 3 | 0.029803 | e8:91:20:b3:e2:4d | 12:0e:0e:20:d5:9f | 802.11 | 70 | Authentication, SN=3659, FN=0, Flags=........C | -45 dBm | 1.0 | 2412 MHz |
| 4 | 0.031101 | 12:0e:0e:20:d5:9f | e8:91:20:b3:e2:4d | 802.11 | 70 | Authentication, SN=256, FN=0, Flags=........C | -32 dBm | 1.0 | 2412 MHz |
| 5 | 0.032977 | e8:91:20:b3:e2:4d | 12:0e:0e:20:d5:9f | 802.11 | 163 | Association Request, SN=3660, FN=0, Flags=........C, SSID=SUNDRAY | -42 dBm | 1.0 | 2412 MHz |
| 6 | 0.038213 | 12:0e:0e:20:d5:9f | e8:91:20:b3:e2:4d | 802.11 | 186 | Association Response, SN=257, FN=0, Flags=........C | -30 dBm | 1.0 | 2412 MHz |
| 7 | 0.163040 | 12:0e:0e:20:d5:9f | e8:91:20:b3:e2:4d | EAPOL | 173 | Key (Message 1 of 4) | -36 dBm | 1.0 | 2412 MHz |
| 8 | 0.166688 | e8:91:20:b3:e2:4d | 12:0e:0e:20:d5:9f | EAPOL | 195 | Key (Message 2 of 4) | -41 dBm | 1.0 | 2412 MHz |
| 9 | 0.411759 | 12:0e:0e:20:d5:9f | e8:91:20:b3:e2:4d | EAPOL | 253 | Key (Message 3 of 4) | -34 dBm | 1.0 | 2412 MHz |
| 10 | 0.420825 | e8:91:20:b3:e2:4d | 12:0e:0e:20:d5:9f | EAPOL | 173 | Key (Message 4 of 4) | -41 dBm | 1.0 | 2412 MHz |
| 11 | 0.498865 | e8:91:20:b3:e2:4d | 33:33:ff:b3:e2:4d | 802.11 | 154 | QoS Data, SN=0, FN=0, Flags=.p.....TC | -41 dBm | 1.0 | 2412 MHz |
| 12 | 0.506555 | e8:91:20:b3:e2:4d | 33:33:00:00:00:16 | 802.11 | 166 | QoS Data, SN=1, FN=0, Flags=.p.....TC | -39 dBm | 1.0 | 2412 MHz |
| 13 | 0.522893 | e8:91:20:b3:e2:4d | ff:ff:ff:ff:ff:ff | 802.11 | 412 | QoS Data, SN=2, FN=0, Flags=.p.....TC | -44 dBm | 1.0 | 2412 MHz |
| 14 | 1.504258 | e8:91:20:b3:e2:4d | 33:33:00:00:00:02 | 802.11 | 146 | QoS Data, SN=3, FN=0, Flags=.p.....TC | -39 dBm | 1.0 | 2412 MHz |
| 15 | 2.527705 | 12:0e:0e:20:d5:9f | e8:91:20:b3:e2:4d | 802.11 | 73 | Action, SN=258, FN=0, Flags=........C | -32 dBm | 1.0 | 2412 MHz |
| 16 | 2.537384 | e8:91:20:b3:e2:4d | 12:0e:0e:20:d5:9f | 802.11 | 73 | Action, SN=3661, FN=0, Flags=........C | -39 dBm | 1.0 | 2412 MHz |

图二 客户端与 AP 完整的交互过程空口抓包

wpawpa2psk.pcap

附件 1 客户端与 AP 通信过程空口抓包

首先解释图中的一些名词：

- **PMK** ——“成对主密钥”（Pairwise Master Key，PMK），由密码与 SSID 计算生成，长度 256 位，密码与 SSID 设置好的情况下，PMK 是不会变化；
- **PTK**——“成对临时密钥”（Pairwise Transient Key，PTK），由五个参数共同决定：“成对主密钥”PMK、AP 接入点生成的随机数 A-nonce、客户端生成的随机数 S-nonce、AP 接入点的 MAC 地址、客户端的 MAC 地址，PTK 是客户端连接 AP 接入点的时候动态创建的，并且之后的每次连接都会动态的更换；
- **MIC**——“信息完整性检查码”（Message Integrity Code,MIC），由 PMK 与 PTK 混合生成的一个加密散列函数，主要是用来防止篡改和验证客户端的主密钥；

**一次完整的四次握手过程：**

1、 AP 向客户端传送自己生成的随机数 A-nonce，MIC 为全 0，如图二中数据包 7；

```
▷ Key Information: 0x008a
  Key Length: 16
  Replay Counter: 1
  WPA Key Nonce: 275b42da1e26749e689c9df99139625e5f0d7b425fa02fd0...
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 00000000000000000000000000000000
  WPA Key Data Length: 0
```

2、 客户端收到 A-nonce 后加上自己生成的 S-nonce 就可以生成 PTK，然后生成 MIC，之后客户端把 S-nonce 与 MIC 一并传给 AP，如图二数据包 8；

```
  Key Length: 0
  Replay Counter: 1
  WPA Key Nonce: 36c66e6a38b5ee1e5168d4b0a0e69985d8ce60c2be7181eb...
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 326542d7382970a99859d7368522d246
  WPA Key Data Length: 22
▷ WPA Key Data: 30140100000fac040100000fac040100000fac020000
```

3、 AP 收到客户端的 S-nonce 后生成自己的 PTK，然后生成 MIC，比对客户端传来的 MIC，由于 MIC 是由 PMK 与 PTK 生成的，所以如果 MIC 不正确，那就意味着 PTK 或 PMK 是不正确的，如果不正确，则结束本次验证，如果正确，则传给客户端身份验证通过的报文，并附上 MIC，如图二数据包 9；

```
Key Length: 16
Replay Counter: 2
WPA Key Nonce: 275b42da1e26749e689c9df99139625e5f0d7b425fa02fd0...
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 26204c8554ce8a6c200a2b4e7e210a7e
WPA Key Data Length: 80
WPA Key Data: e98c278648fd45eb767651a113c08295d0bf608cba71b4b6...
```

4、 确认 3 中的消息，并附上 MIC，如图二数据包 10。

```
Key Information: 0x030a
Key Length: 0
Replay Counter: 2
WPA Key Nonce: 0000000000000000000000000000000000000000000000000...
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: c2e77deed7e181b4b172f4e257374e97
WPA Key Data Length: 0
```

至此，四次握手完成，之后就开始加密传输了。

**附：**

**WPA、WPA2、802.11i 和 802.11-2007**

WPA 的全称为 Wi-Fi Protected Access（Wi-Fi 保护访问），是由 Wi-Fi 联盟推出来解决 WEP 不安全的问题的临时解决办法（顺便说一句，我国为解决 WEP 不安全推出来的是 WAPI 标准，之后大国间的博弈导致全球推行失败，只能在中国大陆强制推行）。IEEE 802.11i 标准被批准过后，WPA 就成了 802.11i 的一个子集，被合并到 802.11i 标准中去了。802.11-2007 是 802.11i 的改进版本，拥有一些增强的安全性功能。