WPA 四次握手分析

刘森林
嵌入式 1 班
SA15226261

WPA/RSN 使用四次握手（4-Way Handshake）的方式生成所需的密钥

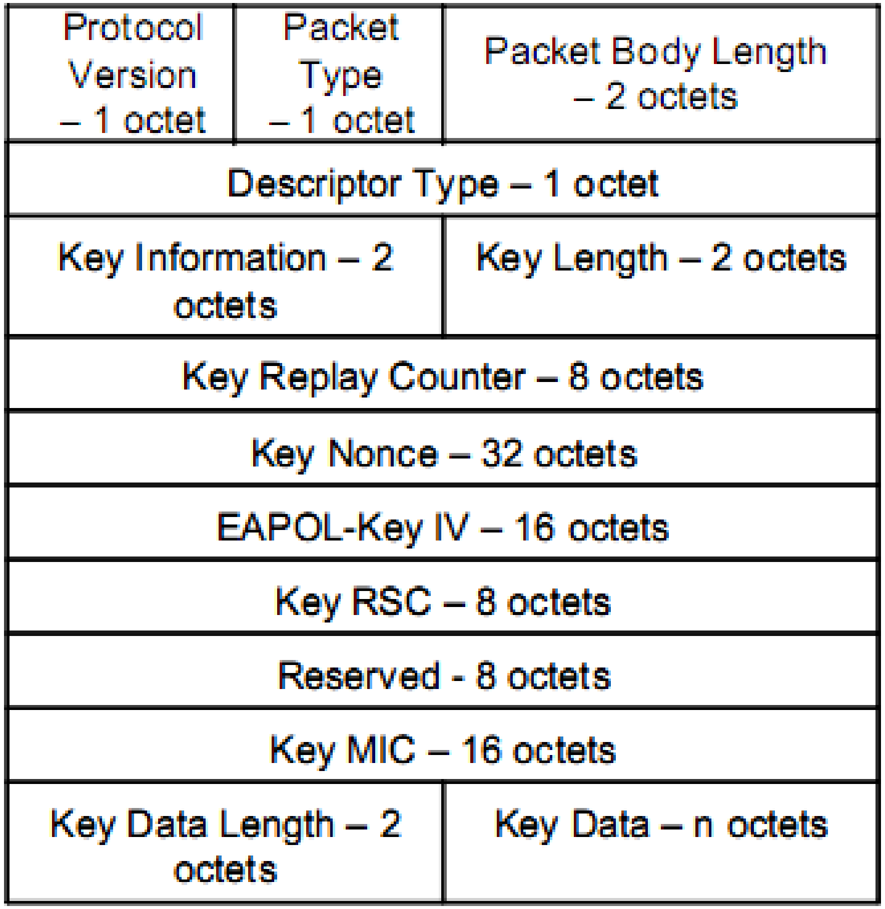
- 四次握手通过一系列的交互，从 PMK （Pairwise Master Key）生成 PTK （Pairwise Transient Key）。 PMK 来自 MSK （Master Session Key），是 MSK 的前 256 位， 32 字节。

PTK(Pairwise Transient Key) 的内容

- PTK包含3个部分，KCK （Key Confirmation Key），KEK （Key Encryption Key），TK （Temporal Key）。
-
- PTK的总长度根据加密方式不同而不同。
-
- 当加密方式是TKIP时，PTK长512位，按顺序分别为KCK占128位，KEK占128位，TK占256位。
-
- 当加密方式是CCMP时，PTK长384位，按顺序分别为KCK占128位，KEK占128位，TK占128位。
-
- KEK和KCK是给EAPOL-Key，也就是四次握手时，加密和完整性验证用的。TK用于后续的数据加密。

四次握手的报文都是基于EAPOL-Key

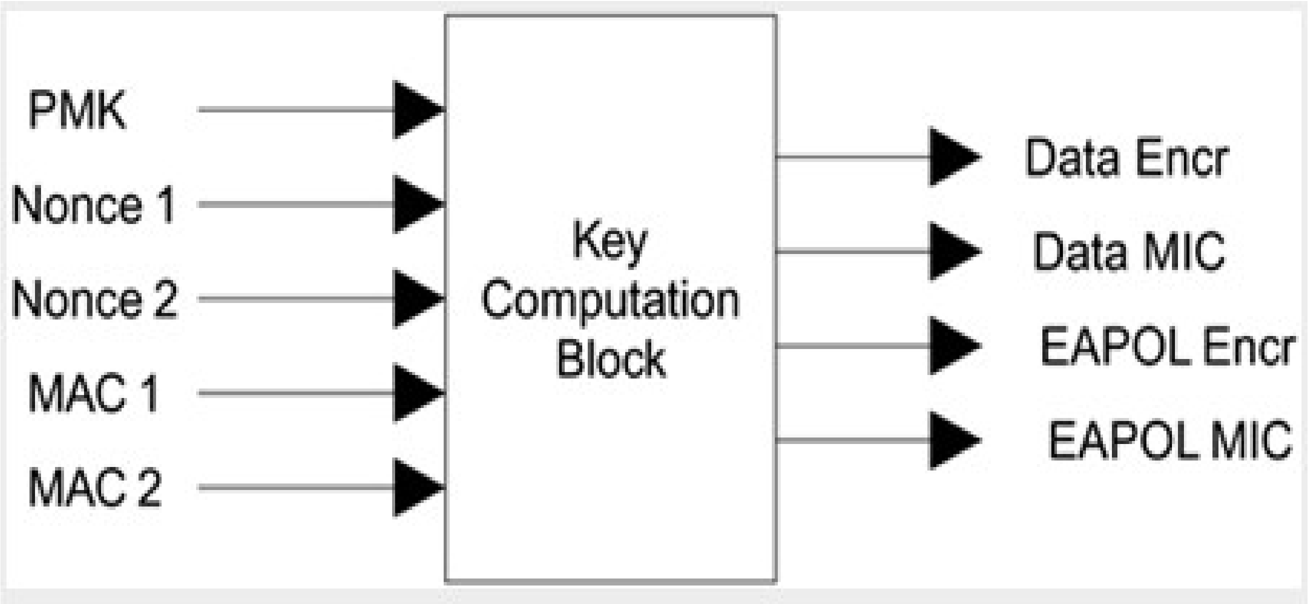
EAPOL-Key 的结构如下：



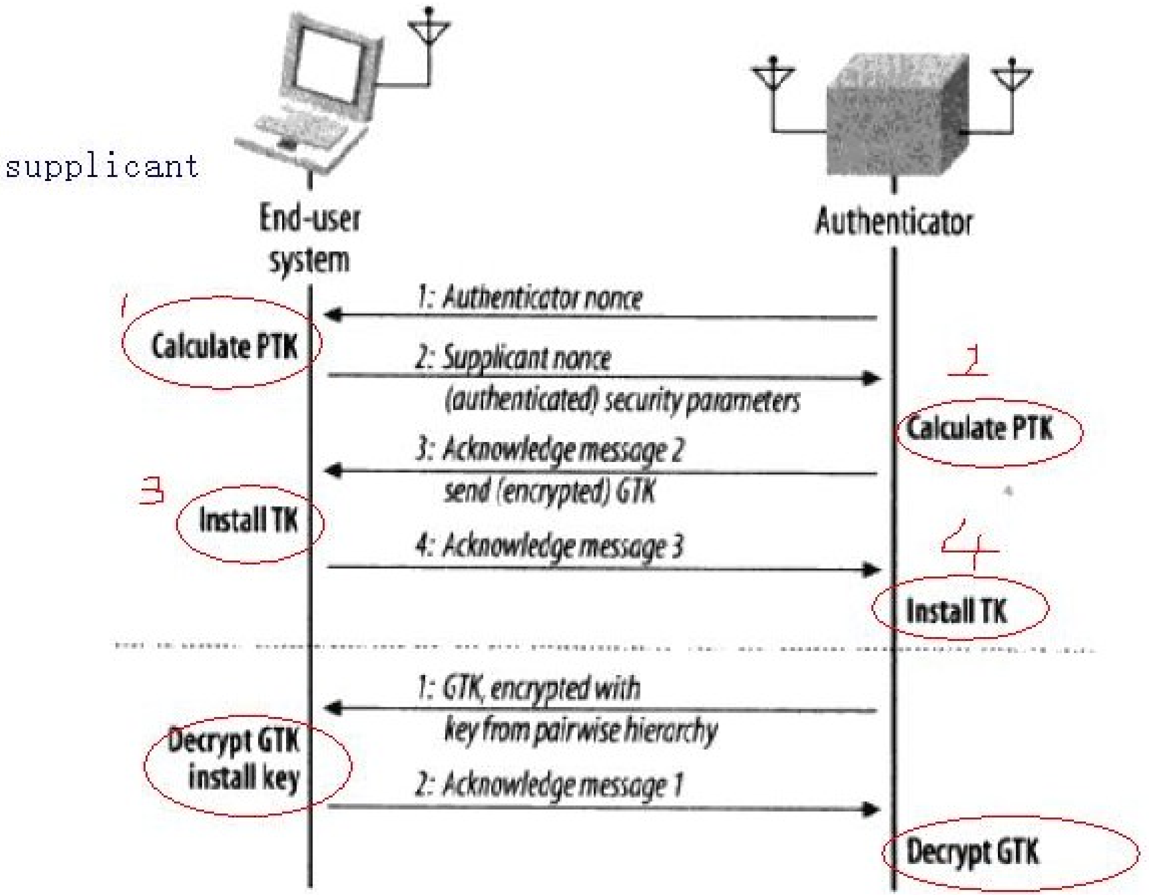
<table>
<tr><td>Protocol Version – 1 octet</td><td>Packet Type – 1 octet</td><td>Packet Body Length – 2 octets</td></tr>
<tr><td colspan="3">Descriptor Type – 1 octet</td></tr>
<tr><td colspan="2">Key Information – 2 octets</td><td>Key Length – 2 octets</td></tr>
<tr><td colspan="3">Key Replay Counter – 8 octets</td></tr>
<tr><td colspan="3">Key Nonce – 32 octets</td></tr>
<tr><td colspan="3">EAPOL-Key IV – 16 octets</td></tr>
<tr><td colspan="3">Key RSC – 8 octets</td></tr>
<tr><td colspan="3">Reserved - 8 octets</td></tr>
<tr><td colspan="3">Key MIC – 16 octets</td></tr>
<tr><td colspan="2">Key Data Length – 2 octets</td><td>Key Data – n octets</td></tr>
</table>

PTK 的生成

- PMK
- ANonce （ Nonce 1 ） ， SNonce （ Nonce 2 ）
- Authenticate MAC （ MAC 1 ）
- Supplicant MAC （ MAC 2 ）



更新成对密钥的 4 次握手



1/4 ： Authenticator -> Supplicant

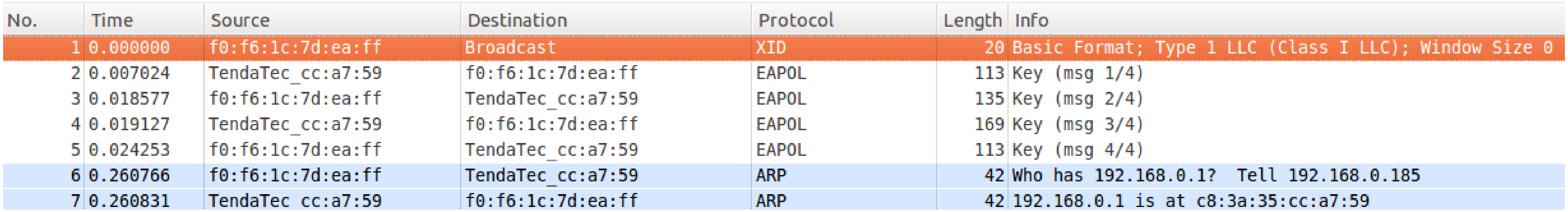
Authenticator 把 ANonce 送给 Supplicant 。 Supplicant 收到 1/4 后，就有了生成 PTK 的所有元素。因为 1/4 里同时也包含了 Authenticator 的 MAC 地址。

第一次握手 AP-->STA ， PMK 已经预设好了，这个 AP 时候发送一个随机产生的 nOnce 数。

hostapd 输出 log

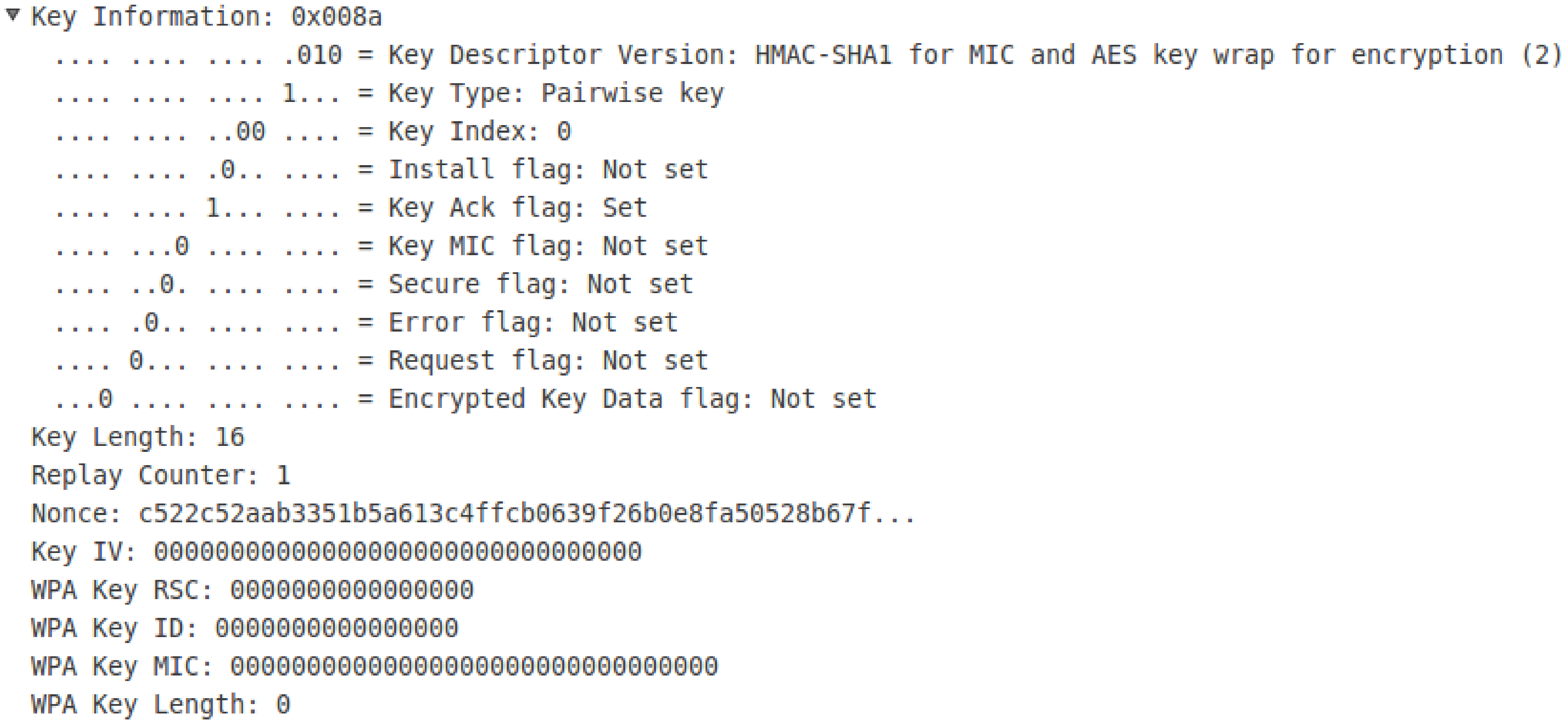
- 1450356424.588011: WPA: f0:f6:1c:7d:ea:ff WPA_PTK_GROUP entering state IDLE
- 1450356424.588027: WPA: f0:f6:1c:7d:ea:ff WPA_PTK entering state AUTHENTICATION
- 1450356424.588047: WPA: f0:f6:1c:7d:ea:ff WPA_PTK entering state AUTHENTICATION2
- 1450356424.588063: WPA: Re-initialize GMK/Counter on first station
- 1450356424.588571: GMK - hexdump(len=32): [REMOVED]
- 1450356424.589093: Key Counter - hexdump(len=32): [REMOVED]
- 1450356424.589589: GTK - hexdump(len=16): [REMOVED]
- 1450356424.589627: wpa_driver_nl80211_set_key: ifindex=4 alg=3 addr=0x458c6a key_idx=1 set_tx=1 seq_len=0 key_len=16
- 1450356424.589653:   broadcast key
- 1450356424.592742: WPA: Assign ANonce - hexdump(len=32): 35 82 88 c0 ad eb 5c 2d ce 81 9c 8d 1f f4 87 06 22 9d 91 05 b2 6c 36 6c f6 16 da bb dd c0 22 28
- 1450356424.592760: WPA: f0:f6:1c:7d:ea:ff WPA_PTK entering state INITPSK
- 1450356424.592765: WPA: f0:f6:1c:7d:ea:ff WPA_PTK entering state PTKSTART
- 1450356424.592772: wlan4: STA f0:f6:1c:7d:ea:ff WPA: **sending 1/4 msg of 4-Way Handshake**
- 1450356424.592775: WPA: Send EAPOL(version=2 secure=0 mic=0 ack=1 install=0 pairwise=8 kde_len=0 keyidx=0 encr=0)

wireshake 抓包内容



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	f0:f6:1c:7d:ea:ff	Broadcast	XID	20	Basic Format; Type 1 LLC (Class I LLC); Window Size 0
2	0.007024	TendaTec_cc:a7:59	f0:f6:1c:7d:ea:ff	EAPOL	113	Key (msg 1/4)
3	0.018577	f0:f6:1c:7d:ea:ff	TendaTec_cc:a7:59	EAPOL	135	Key (msg 2/4)
4	0.019127	TendaTec_cc:a7:59	f0:f6:1c:7d:ea:ff	EAPOL	169	Key (msg 3/4)
5	0.024253	f0:f6:1c:7d:ea:ff	TendaTec_cc:a7:59	EAPOL	113	Key (msg 4/4)
6	0.260766	f0:f6:1c:7d:ea:ff	TendaTec_cc:a7:59	ARP	42	Who has 192.168.0.1? Tell 192.168.0.185
7	0.260831	TendaTec_cc:a7:59	f0:f6:1c:7d:ea:ff	ARP	42	192.168.0.1 is at c8:3a:35:cc:a7:59

wireshake 抓包内容



```
▼ Key Information: 0x008a
    .... .... .... .010 = Key Descriptor Version: HMAC-SHA1 for MIC and AES key wrap for encryption (2)
    .... .... .... 1... = Key Type: Pairwise key
    .... .... ..00 .... = Key Index: 0
    .... .... .0.. .... = Install flag: Not set
    .... .... 1... .... = Key Ack flag: Set
    .... ...0 .... .... = Key MIC flag: Not set
    .... ..0. .... .... = Secure flag: Not set
    .... .0.. .... .... = Error flag: Not set
    .... 0... .... .... = Request flag: Not set
    ...0 .... .... .... = Encrypted Key Data flag: Not set
  Key Length: 16
  Replay Counter: 1
  Nonce: c522c52aab3351b5a613c4ffcb0639f26b0e8fa50528b67f...
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 00000000000000000000000000000000
  WPA Key Length: 0
```

hostapd 源码

- wpa_auth.c
- wpa_auth_set_eapol()
- wpa_auth_send_eapol()

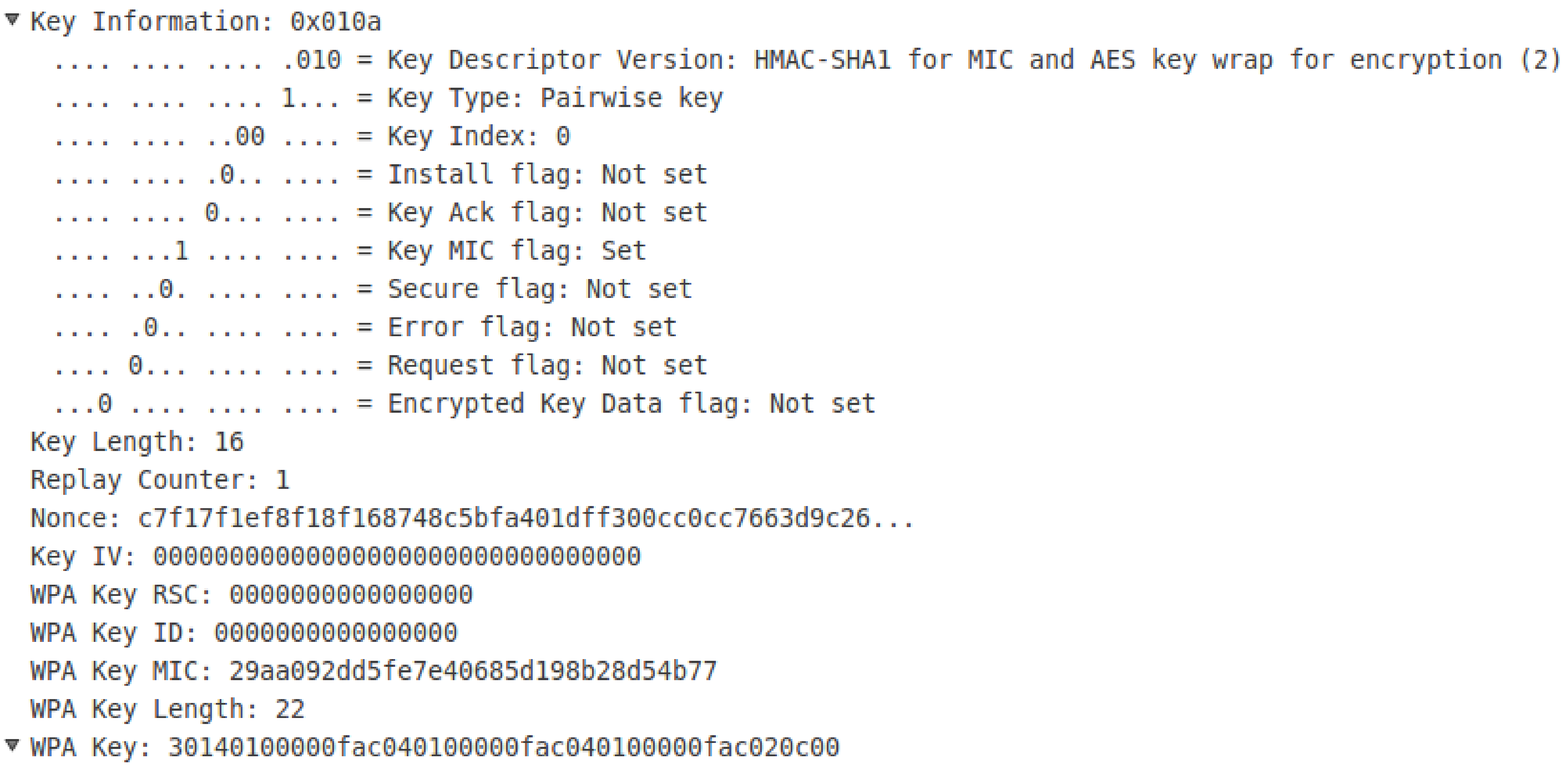
2/4 ： Supplicant -> Authenticator

- Supplicant 计算出 PTK ，把 SNonce 和自己的 MAC 地址送给 Authenticator 。同时，从 2/4 报文开始，后面的每个报文都会有 MIC 。
- 第 2 步的整个消息是用 EAPOL 密钥确认密钥 (KCK) 来进行完整性校验值校验的 , 如果 authenticator 根据已经算出的 PTK 中的 KCK 对整个消息进行完整性校验未成功 , 握手就失败了 , 这时消息还不能通过 KEK 加密 , 是因为还没有计算出 PTK 。

hostapd 输出 log

```
• 1450356424.592840: nl80211: New station f0:f6:1c:7d:ea:ff
• 1450356424.596285: wlan4: Event EAPOL_TX_STATUS (48) received
• 1450356424.596321: IEEE 802.1X: f0:f6:1c:7d:ea:ff TX status - version=2 type=3 length=95 - ack=1
• 1450356424.596335: WPA: EAPOL-Key TX status for STA f0:f6:1c:7d:ea:ff ack=1
• 1450356424.596345: WPA: Increase initial EAPOL-Key 1/4 timeout by 1000 ms because of acknowledged frame
• 1450356424.597633: wlan4: Event EAPOL_RX (27) received
• 1450356424.597665: IEEE 802.1X: 121 bytes from f0:f6:1c:7d:ea:ff
• 1450356424.597677:    IEEE 802.1X: version=2 type=3 length=117
• 1450356424.597686: WPA: Received EAPOL-Key from f0:f6:1c:7d:ea:ff key_info=0x10a type=2 key_data_length=22
• 1450356424.597697: WPA: Received Key Nonce - hexdump(len=32): e1 0a f7 ab 7a bb 54 43 a2 1c 21 c4 f1 d9 71 37 13 70 9b 83 47 c0
  7c 01 e0 08 ff 7e f7 eb 40 a7
• 1450356424.597718: WPA: Received Replay Counter - hexdump(len=8): 00 00 00 00 00 00 00 01
• 1450356424.597744: wlan4: STA f0:f6:1c:7d:ea:ff WPA: received EAPOL-Key frame (2/4 Pairwise)
• 1450356424.597757: WPA: f0:f6:1c:7d:ea:ff WPA_PTK entering state PTKCALCNEGOTIATING
• 1450356424.597796: WPA: PTK derivation - A1=c8:3a:35:cc:a7:59 A2=f0:f6:1c:7d:ea:ff
• 1450356424.597807: WPA: Nonce1 - hexdump(len=32): 35 82 88 c0 ad eb 5c 2d ce 81 9c 8d 1f f4 87 06 22 9d 91 05 b2 6c 36 6c f6 16
  da bb dd c0 22 28
• 1450356424.597857: WPA: Nonce2 - hexdump(len=32): e1 0a f7 ab 7a bb 54 43 a2 1c 21 c4 f1 d9 71 37 13 70 9b 83 47 c0 7c 01 e0 08
  ff 7e f7 eb 40 a7
```

wireshake 抓包内容



```
▼ Key Information: 0x010a
    .... .... .... .010 = Key Descriptor Version: HMAC-SHA1 for MIC and AES key wrap for encryption (2)
    .... .... .... 1... = Key Type: Pairwise key
    .... .... ..00 .... = Key Index: 0
    .... .... .0.. .... = Install flag: Not set
    .... .... 0... .... = Key Ack flag: Not set
    .... ...1 .... .... = Key MIC flag: Set
    .... ..0. .... .... = Secure flag: Not set
    .... .0.. .... .... = Error flag: Not set
    .... 0... .... .... = Request flag: Not set
    ...0 .... .... .... = Encrypted Key Data flag: Not set
  Key Length: 16
  Replay Counter: 1
  Nonce: c7f17f1ef8f18f168748c5bfa401dff300cc0cc7663d9c26...
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 29aa092dd5fe7e40685d198b28d54b77
  WPA Key Length: 22
▼ WPA Key: 30140100000fac040100000fac040100000fac020c00
```

hostapd 源码

- wpa_auth.c
- wpa_receive()

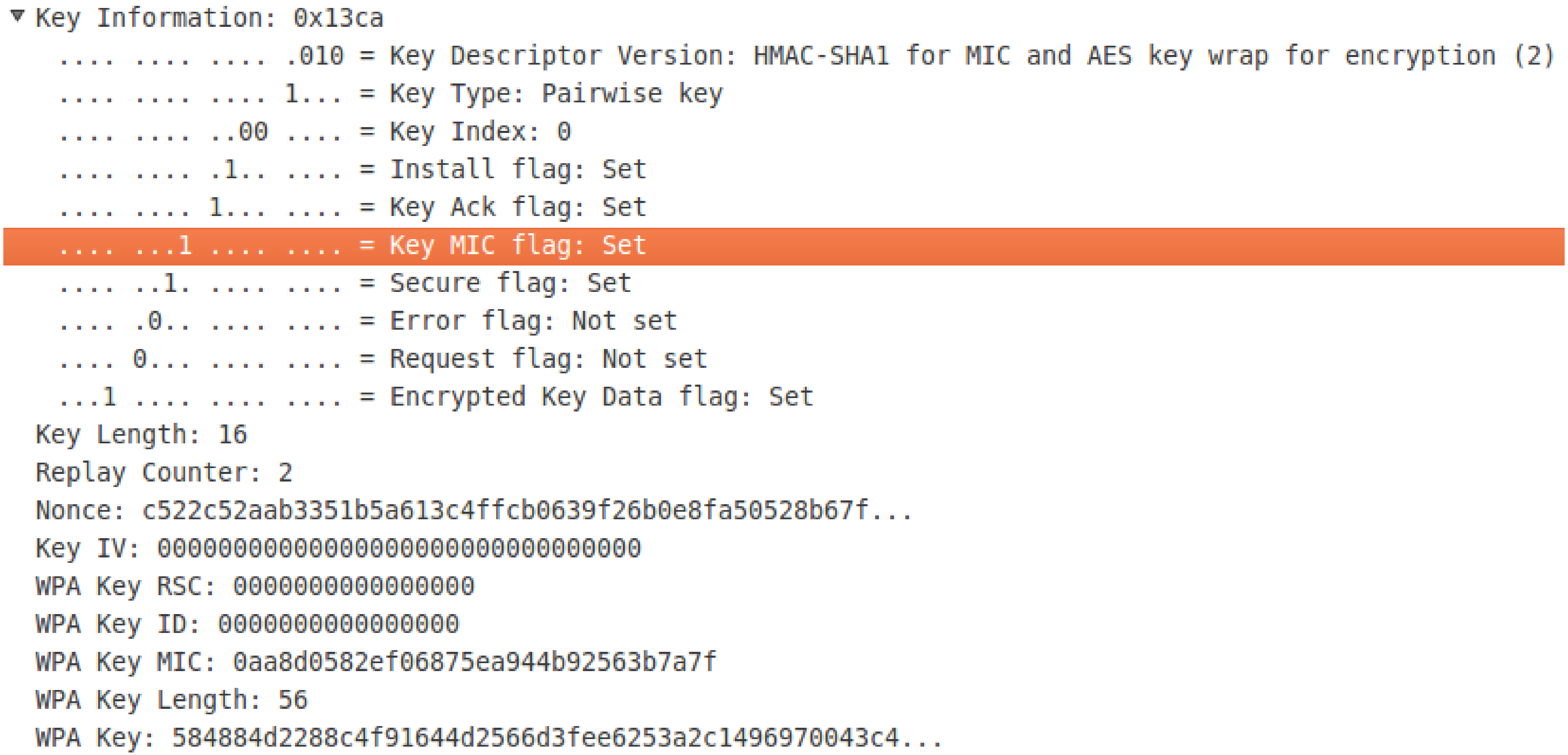
3/4 ： Authenticator -> Supplicant

- Authenticator 向 Supplicant 证明自己有有效的，同样有 MIC 加入其中
- 第三次握手， AP 接收到这个随机数后，使用相同的方法生成 PTK ，并取出其中的 MIC 密钥对第二次握手包进行较验，如果相同，那么 AP 知道这个时候 STA 拥一个跟它一样的 PMK 。这个时候 AP 有了 PTK 后就可以对它第一次握手生成的 EAP 包进行检验生成一个 MIC 序列号，并发送给 STA 。

hostapd 输出 log

- 1450356424.597876: WPA: PMK - hexdump(len=32): [REMOVED]
- 1450356424.597884: WPA: PTK - hexdump(len=48): [REMOVED]
- 1450356424.597901: WPA: f0:f6:1c:7d:ea:ff WPA_PTK entering state PTKCALCNEGOTIATING2
- 1450356424.597911: WPA: f0:f6:1c:7d:ea:ff WPA_PTK entering state PTKINITNEGOTIATING
- 1450356424.598056: wlan4: STA f0:f6:1c:7d:ea:ff WPA: **sending 3/4 msg of 4-Way Handshake**
- 1450356424.598070: WPA: Send EAPOL(version=2 secure=1 mic=1 ack=1 install=1 pairwise=8 kde_len=46 keyidx=1 encr=1)
- 1450356424.598083: Plaintext EAPOL-Key Key Data - hexdump(len=56): [REMOVED]
- 1450356424.598220: WPA: Use EAPOL-Key timeout of 100 ms (retry counter 1)
- 1450356424.600781: wlan4: Event EAPOL_TX_STATUS (48) received
- 1450356424.600814: IEEE 802.1X: f0:f6:1c:7d:ea:ff TX status - version=2 type=3 length=151 - ack=1
- 1450356424.600828: WPA: EAPOL-Key TX status for STA f0:f6:1c:7d:ea:ff ack=1
- 1450356424.602948: wlan4: Event EAPOL_RX (27) received
- 1450356424.602960: IEEE 802.1X: 99 bytes from f0:f6:1c:7d:ea:ff
- 1450356424.602965:   IEEE 802.1X: version=2 type=3 length=95

wireshake 抓包内容



```
▼ Key Information: 0x13ca
    .... .... .... .010 = Key Descriptor Version: HMAC-SHA1 for MIC and AES key wrap for encryption (2)
    .... .... .... 1... = Key Type: Pairwise key
    .... .... ..00 .... = Key Index: 0
    .... .... .1.. .... = Install flag: Set
    .... .... 1... .... = Key Ack flag: Set
    .... ...1 .... .... = Key MIC flag: Set
    .... ..1. .... .... = Secure flag: Set
    .... .0.. .... .... = Error flag: Not set
    .... 0... .... .... = Request flag: Not set
    ...1 .... .... .... = Encrypted Key Data flag: Set
  Key Length: 16
  Replay Counter: 2
  Nonce: c522c52aab3351b5a613c4ffcb0639f26b0e8fa50528b67f...
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 0aa8d0582ef06875ea944b92563b7a7f
  WPA Key Length: 56
  WPA Key: 584884d2288c4f91644d2566d3fee6253a2c1496970043c4...
```

hostapd 源码

- wpa_auth.c
-

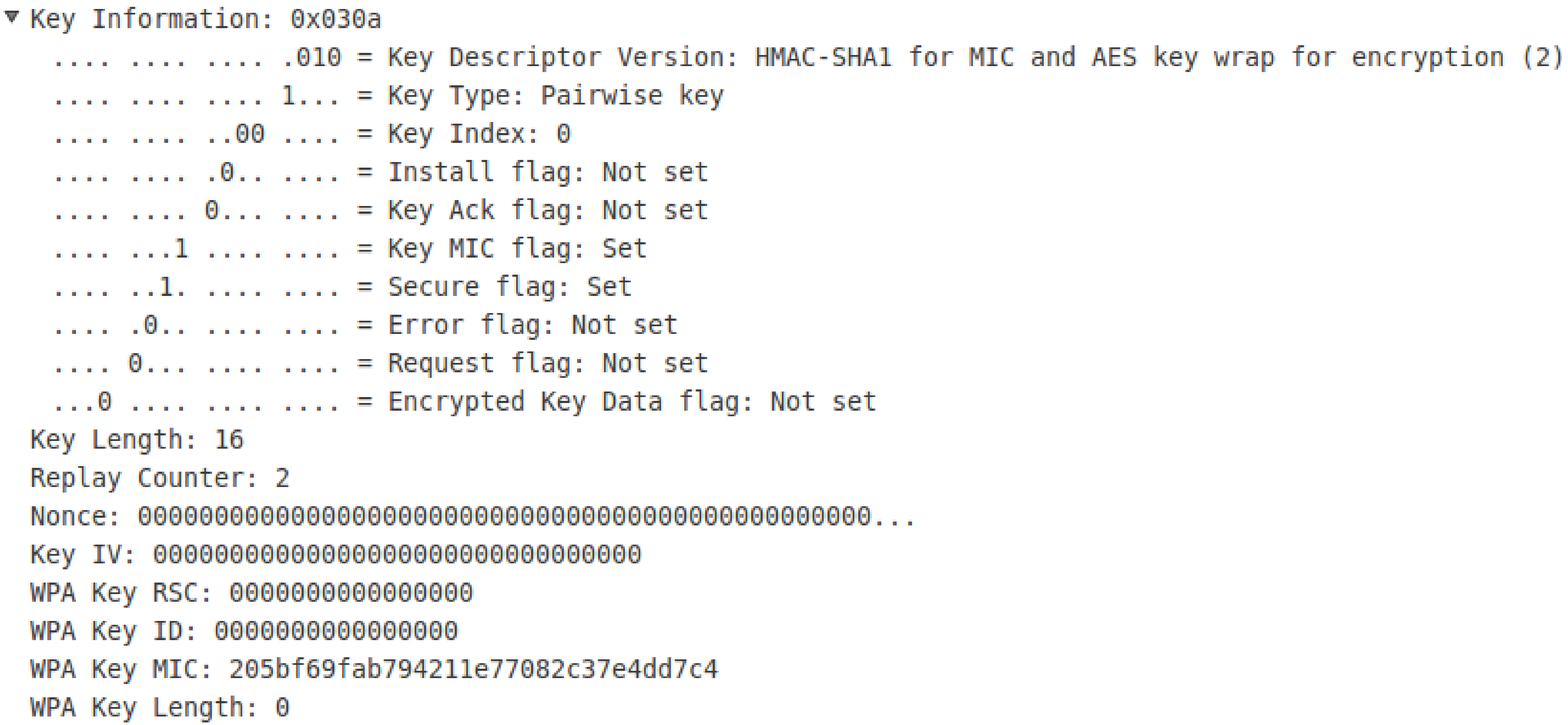
4/4 ： Supplicant -> Authenticator

- 仅是对 3/4 的一个 ACK 。说明 PTK 已经装好，后面的数据可以加密了。
- 第四次握手， STA 接收到这个包后，同样执行跟 AP 的检验操作以确认 AP 拥有跟自己一样的 PMK 。然后发送确实安装 PMK 。

hostapd 输出 log

- 1450356424.602968: WPA: Received EAPOL-Key from f0:f6:1c:7d:ea:ff key_info=0x30a type=2 key_data_length=0
- 1450356424.602972: WPA: Received Key Nonce - hexdump(len=32): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
- 1450356424.602981: WPA: Received Replay Counter - hexdump(len=8): 00 00 00 00 00 00 00 02
- 1450356424.602989: wlan4: STA f0:f6:1c:7d:ea:ff WPA: **received EAPOL-Key frame (4/4 Pairwise)**
- 1450356424.603001: WPA: f0:f6:1c:7d:ea:ff WPA_PTK entering state PTKINITDONE
- 1450356424.603019: wpa_driver_nl80211_set_key: ifindex=4 alg=3 addr=0x26030a0 key_idx=0 set_tx=1 seq_len=0 key_len=16
- 1450356424.603028:   addr=f0:f6:1c:7d:ea:ff
- 1450356424.603723: wlan4: AP-STA-CONNECTED f0:f6:1c:7d:ea:ff
- 1450356424.603781: wlan4: STA f0:f6:1c:7d:ea:ff IEEE 802.1X: authorizing port
- 1450356424.603791: wlan4: STA f0:f6:1c:7d:ea:ff RADIUS: starting accounting session 5672AEAA-00000000
- 1450356424.603827: wlan4: STA f0:f6:1c:7d:ea:ff WPA: pairwise key handshake completed (RSN)

wireshake 抓包内容



```
▼ Key Information: 0x030a
    .... .... .... .010 = Key Descriptor Version: HMAC-SHA1 for MIC and AES key wrap for encryption (2)
    .... .... .... 1... = Key Type: Pairwise key
    .... .... ..00 .... = Key Index: 0
    .... .... .0.. .... = Install flag: Not set
    .... .... 0... .... = Key Ack flag: Not set
    .... ...1 .... .... = Key MIC flag: Set
    .... ..1. .... .... = Secure flag: Set
    .... .0.. .... .... = Error flag: Not set
    .... 0... .... .... = Request flag: Not set
    ...0 .... .... .... = Encrypted Key Data flag: Not set
  Key Length: 16
  Replay Counter: 2
  Nonce: 000000000000000000000000000000000000000000000000...
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 205bf69fab794211e77082c37e4dd7c4
  WPA Key Length: 0
```

hostapd 源码

- wpa_auth.c