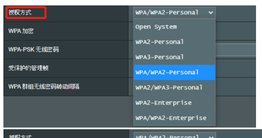

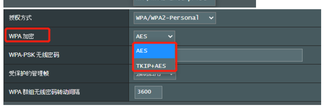

根据路由器设置分析不同的授权方式与加密方式(即认证方式与加密套件选择)

授权方式 open system时，即没有WIFI密码时
1.Probe Response是没有RSN字段的，过滤器 wlan.addr == fc:34:97:39:f1:e0 && wlan.tag.number == 48
2.没有四次握手，只有认证与关联，后面直接是DHCP流程
3.因为没有加密的原因，能直接解析出来DHCP 等应用层的协议，有加密的时候只能看到是Qos Data数据帧

WPA = IEEE 802.11i draft 3 = 802.1X Auth Service/PSK + WEP(选择性项目)/TKIP
WPA2 = IEEE 802.11i = 802.1X Auth Service/PSK + WEP(选择性项目)/TKIP/CCMP
CCMP也表示为AES / AES-CCMP

WPA3 的AKM认证支持SAE(Simultaneous authentication of equals)同步认证，加密套件还是AES-CCMP

```
Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (SHA256)
  Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: SAE (SHA256) (8)
RSN Capabilities: 0x00cc
```

```
72:47:f7:b1:bd:96   fc:34:97:39:f1:e0 802.11    240 Probe Request, SN=3008, FN=0, Flags=........C, SSID=123
fc:34:97:39:f1:e0   72:47:f7:b1:bd:96 802.11    422 Probe Response, SN=3349, FN=0, Flags=........C, BI=100, SSID=123
72:47:f7:b1:bd:96   fc:34:97:39:f1:e0 802.11    188 Authentication, SN=3009, FN=0, Flags=........C
fc:34:97:39:f1:e0   72:47:f7:b1:bd:96 802.11    188 Authentication, SN=3350, FN=0, Flags=........C
72:47:f7:b1:bd:96   fc:34:97:39:f1:e0 802.11    124 Authentication, SN=3010, FN=0, Flags=........C
fc:34:97:39:f1:e0   72:47:f7:b1:bd:96 802.11    124 Authentication, SN=3352, FN=0, Flags=........C
72:47:f7:b1:bd:96   fc:34:97:39:f1:e0 802.11    278 Association Request, SN=3011, FN=0, Flags=........C, SSID=123
fc:34:97:39:f1:e0   72:47:f7:b1:bd:96 802.11    318 Association Response, SN=3353, FN=0, Flags=........C
fc:34:97:39:f1:e0   72:47:f7:b1:bd:96 EAPOL     215 Key (Message 1 of 4)
72:47:f7:b1:bd:96   fc:34:97:39:f1:e0 EAPOL     224 Key (Message 2 of 4)
fc:34:97:39:f1:e0   72:47:f7:b1:bd:96 EAPOL     281 Key (Message 3 of 4)
72:47:f7:b1:bd:96   fc:34:97:39:f1:e0 EAPOL     193 Key (Message 4 of 4)
```

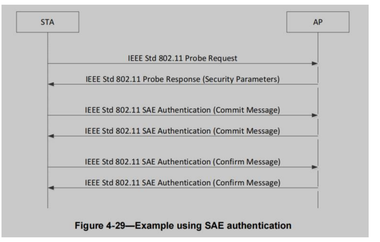

Figure 4-29—Example using SAE authentication

SAE is an RSNA authentication protocol SAE是一种认证协议
12.4.5 SAE protocol
12.4.5.1 Message exchanges 消息交换
The protocol consists of two message exchanges, a commitment exchange and a confirmation exchange.两个消息交换流程：承诺交换与确认交换
The commitment exchange is used to force each party to the exchange to commit to a single guess of the password. 承诺交换用于强制交换每一方对密码的单一猜测
The confirmation exchange is used to prove that the password guess was correct. 确认交换用于证明密码猜测是正确的
Authentication frames are used to perform these exchanges (see 9.3.3.12 and 12.4.7.3). 使用Auth 认证帧进行交换
The rules for performing these exchanges are specified by the finite state machine in 12.4.8. 交换规则参考12.4.8

12.4.5.2 PWE and secret generation PWE生成
The PWE shall be generated for that group (according to 12.4.4.2.2 or 12.4.4.3.2, depending on whether the group is ECC or FFC, respectively) using the identities of the two STAs and the configured password.
使用两个 STA 的身份ID和配置的密码为该组生成 PWE
PWE的具体生成参考 12.4.4.2.2 Generation of the password element with ECC groups
r is the (prime) order of the group,两个随机数rand , mask 的数值在（1，r）之间

12.4.5.3 Construction of an SAE Commit message
commit-scalar = (rand + mask) mod r
COMMIT-ELEMENT = inverse(scalar-op(mask, PWE)) 构造出Scalar 和 Commit Element

12.4.5.4 Processing of a peer's SAE Commit message
校验接收到的Scalar 和 Commit Element，如果一个校验不通过就会对方的认证

12.4.5.5 Construction of an SAE Confirm message
A peer generates an SAE Confirm message by passing the KCK, the current value of the send-confirm counter (see 9.4.1.38), the scalar and element from the sent SAE Commit message, and the scalar and element from the received SAE Commit message to the confirmation function CN.
confirm = CN(KCK, send-confirm, commit-scalar, COMMIT-ELEMENT, peer-commit-scalar,PEER-COMMIT-ELEMENT) 构造一个confirm 值

12.4.5.6 Processing of a peer's SAE Confirm message
收到SAE的confirm以后使用CN函数计算出 verifier
verifier = CN(KCK, peer-send-confirm, peer-commit-scalar, PEER-COMMIT-ELEMENT, commit-scalar, COMMIT-ELEMENT)
If the verifier equals peer-confirm, the STA shall accept the peer's authentication
If the verifier differs from the peer-confirm, the STA shall reject the peer's authentication and delete the PMK.
比较verifier 和 peer-confirm，如果相等就会接收认证，如果不相等就会拒绝认证

```
IEEE 802.11 Wireless Management
  Fixed parameters (104 bytes)
    Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
    SAE Message Type: Commit (1)
    Group Id: 256-bit random ECP group (19)
    Scalar: 6f97086e0abc9c731112dd80e0884d71302f1888d953ff7b…
    Finite field Element: 37af551f19e1bbde7342c29abf1fec3e7f94c48d23cd58dd…
```

```
IEEE 802.11 Wireless Management
  Fixed parameters (40 bytes)
    Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
    Authentication SEQ: 0x0002
    Status code: Successful (0x0000)
    SAE Message Type: Confirm (2)
    Send-Confirm: 0
    Confirm: cf5b88f38e0f7b74d030c23a809cc81d3b3585da8a9653eb…
```

Table 9-131—Cipher suite selectors
Table 9-132—Cipher suite usage
加密方法的分类与使用场景

Table 9-131—Cipher suite selectors

OUI	Suite type	Meaning
00-0F-AC	0	Use group cipher suite
00-0F-AC	1	WEP-40
00-0F-AC	2	TKIP
00-0F-AC	3	Reserved
00-0F-AC	4	CCMP-128
00-0F-AC	5	WEP-104
00-0F-AC	6	BIP-CMAC-128

Table 9-131—Cipher suite selectors *(continued)*

OUI	Suite type	Meaning
00-0F-AC	7	Group addressed traffic not allowed
00-0F-AC	8	GCMP-128
00-0F-AC	9	GCMP-256
00-0F-AC	10	CCMP-256
00-0F-AC	11	BIP-GMAC-128
00-0F-AC	12	BIP-GMAC-256
00-0F-AC	13	BIP-CMAC-256
00-0F-AC	14–255	Reserved
Other OUI or CID	Any	Vendor-specific

Table 9-132—Cipher suite usage

Cipher suite selector	GTK	PTK	IGTK
Use group cipher suite	No	Yes	No
WEP-40	Yes	No	No
WEP-104	Yes	No	No
TKIP	Yes	Yes	No
CCMP-128	Yes	Yes	No
BIP-CMAC-128	No	No	Yes
GCMP-128	Yes	Yes	No
GCMP-256	Yes	Yes	No
CCMP-256	Yes	Yes	No
BIP-GMAC-128	No	No	Yes
BIP-GMAC-256	No	No	Yes
BIP-CMAC-256	No	No	Yes

Table 9-133—AKM suite selectors
AKM的分类 常用的 1(802.1X) 2(PSK) 8(SAE)

Table 9-133—AKM suite selectors

OUI	Suite type	Meaning		
		Authentication type	Key management type	Key derivation type
00-0F-AC	0	Reserved	Reserved	Reserved
00-0F-AC	1	Authentication negotiated over IEEE Std 802.1X or using PMKSA caching as defined in 12.6.10.3	RSNA key management as defined in 12.7 or using PMKSA caching as defined in 12.6.10.3	Defined in 12.7.1.2
00-0F-AC	2	PSK	RSNA key management as defined in 12.7, using PSK	Defined in 12.7.1.2
00-0F-AC	3	FT authentication negotiated over IEEE Std 802.1X	FT key management as defined in 12.7.1.7	Defined in 12.7.1.7.2 using SHA-256

Table 9-133—AKM suite selectors *(continued)*

OUI	Suite type	Meaning		
		Authentication type	Key management type	Key derivation type
00-0F-AC	4	FT authentication using PSK	FT key management as defined in 12.7.1.7	Defined in 12.7.1.7.2 using SHA-256
00-0F-AC	5	Authentication negotiated over IEEE Std 802.1X or using PMKSA caching as defined in 12.6.10.3	RSNA key management as defined in 12.7 or using PMKSA caching as defined in 12.6.10.3	Defined in 12.7.1.7.2 using SHA-256
00-0F-AC	6	PSK	RSNA Key Management as defined in 12.7 using PSK	Defined in 12.7.1.7.2 using SHA-256
00-0F-AC	7	TDLS	TPK handshake	Defined in 12.7.1.7.2 using SHA-256
00-0F-AC	8	SAE authentication with SHA-256 or using PMKSA caching as defined in 12.6.10.3	RSNA key management as defined in 12.7, PMKSA caching as defined in 12.6.10.3 or authenticated mesh peering exchange as defined in 14.5	Defined in 12.7.1.7.2 using SHA-256
00-0F-AC	9	FT authentication over SAE	FT key management defined in 12.7.1.7	Defined in 12.7.1.7.2 using SHA-256
00-0F-AC	10	APPeerKey Authentication with SHA-256 or using PMKSA caching as defined in 12.6.10.3	RSNA key management as defined in 12.7 or using PMKSA caching as defined in 12.6.10.3	Defined in 12.7.1.7.2 using SHA-256
00-0F-AC	11	Authentication negotiated over IEEE Std 802.1X or using PMKSA caching as defined in 12.6.10.3 using a Suite B compliant EAP method supporting SHA-256	RSNA key management as defined in 12.7 or using PMKSA caching as defined in 12.6.10.3	Defined in 12.7.1.7.2 using SHA-256
00-0F-AC	12	Authentication negotiated over IEEE Std 802.1X or using PMKSA caching as defined in 12.6.10.3 using a Suite B compliant EAP method supporting SHA-384	RSNA key management as defined in 12.7 or using PMKSA caching as defined in 12.6.10.3	Defined in 12.7.1.7.2 using SHA-384
00-0F-AC	13	FT authentication negotiated over IEEE Std 802.1X	FT key management as defined in 12.7.1.7	Defined in 12.7.1.7.2 using SHA-384
00-0F-AC	14–255	Reserved	Reserved	Reserved
Other OUI or CID	Any	Vendor-specific	Vendor-specific	Vendor-specific

Auth帧中认证算法字段的取值
Pre-RSNA authentication中有 Open System authentication, Shared Key authentication
RSNA authentication中有 Open System authentication, SAE, Fast BSS Transition
Fast BSS Transition , FT 参考 Figure 13-5—Over-the-DS FT protocol in an RSN

Authentication algorithm number = 0: Open System
Authentication algorithm number = 1: Shared Key
Authentication algorithm number = 2: Fast BSS Transition
Authentication algorithm number = 3: Simultaneous Authentication of Equals (SAE)
Authentication algorithm number = 65 535: vendor specific use
NOTE—The use of this value implies that a Vendor Specific element is included with more information.
All other values of authentication algorithm number are reserved.

Figure 9-65—Authentication Algorithm Number field

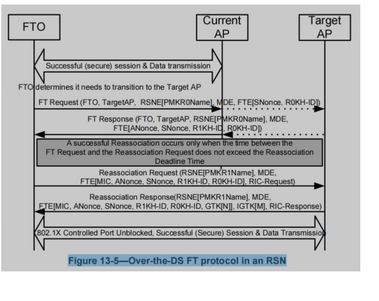

Figure 13-5—Over-the-DS FT protocol in an RSN

总结：
1.Auth frame的Authentication algorithm 字段的取值
Pre-RSNA authentication中有 Open System authentication, Shared Key authentication
RSNA authentication中有 Open System authentication, SAE, Fast BSS Transition
Open System authentication : 开放认证算法仅仅就是一个形式，目前应用较多。
SAE：这就是WPA3认证
Fast BSS Transition : 为了应用FT协议 引入的认证算法。FT主要是为了STA在同一个ESS中的不同AP实现快速切换，省略四次握手流程
主要分为FT initial 与 FT Protocol两个阶段
Figure 13-2—FT initial mobility domain association in an RSN
Figure 13-4—Over-the-air FT protocol in an RSN
Shared Key authentication : 在WEP加密的路由中还可以看见
一共有四个Auth帧，WEP加密的路由没有四次握手流程，probe response帧也没有RSN字段，具体可以参考WEP的sniff包

2.RSNE字段的Cipher suite selectors
常见的TKIP CCMP-128

3.RSNE字段的AKM suite selectors
AKM的分类 常用的 1(802.1X) 2(PSK) 8(SAE)

```
6877 80.093191051  32:3a:48:05:2d:a7  D-LinkIn_2f:1a:94  802.11  170 Probe Request, SN=3579, FN=0, Flags=........C, SSID=WEP
6879 80.094623502  D-LinkIn_2f:1a:94  32:3a:48:05:2d:a7  802.11  157 Probe Response, SN=54, FN=0, Flags=........C, BI=100, SSID=WEP
6881 80.100957096  32:3a:48:05:2d:a7  D-LinkIn_2f:1a:94  802.11   90 Authentication, SN=3580, FN=0, Flags=........C
6883 80.110708270  D-LinkIn_2f:1a:94  32:3a:48:05:2d:a7  802.11  220 Authentication, SN=55, FN=0, Flags=........C
6887 80.117529461  32:3a:48:05:2d:a7  D-LinkIn_2f:1a:94  802.11  228 Authentication, SN=3581, FN=0, Flags=.p.....C
6889 80.118282077  D-LinkIn_2f:1a:94  32:3a:48:05:2d:a7  802.11   90 Authentication, SN=56, FN=0, Flags=........C
6892 80.123691612  32:3a:48:05:2d:a7  D-LinkIn_2f:1a:94  802.11  153 Association Request, SN=3582, FN=0, Flags=........C, SSID=WEP
6897 80.131058713  D-LinkIn_2f:1a:94  32:3a:48:05:2d:a7  802.11  140 Association Response, SN=57, FN=0, Flags=........C
```