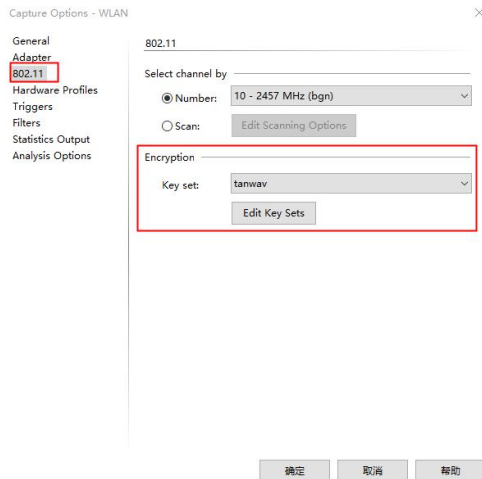


wifi 连接认证流程

如果路由器设置了密码，数据包数据会进行加密发送，所以在抓包前需要将路由器设置为开放或者在 Omnipcap 中设置路由器的密码，如果选择第二种，在 Omnipcap 工具栏中选择 Capture→Capture Options，在弹出的窗口中选择 802.11，如下图所示：



设置好密码后，需要 Omnipcap 成功抓取到对应的认证数据包后才能对数据包进行解密，否则抓取到的数据包中的数据还是会以密文显示。**wifi** 接入需要经过三个阶段：1）扫描阶段（SCAN）；2）认证阶段（Authentication）；3）关联（Association）。其中认证方式有 Open 和 Shared-key Authentication，Shared-key Authentication 一般采用 WEP 加密的方式，Open 一般采用 WPA/WPA2 加密方式。WEP 加密和 WPA 加密其一般流程如下：

a)WEP 加密方式一般流程：

```
STA----(probe req)---->AP
AP ----(probe rsp)---->STA
STA----( auth )---->AP
AP ----( auth )---->STA
STA----( auth )---->AP
AP ----( auth )---->STA
STA----(assoc req)---->AP
AP ----(assoc rsp)---->STA
```

b)WPA 加密方式一般流程：

```
STA----(probe req)---->AP
AP ----(probe rsp)---->STA
STA----( auth )---->AP
AP ----( auth )---->STA
STA----(assoc req)---->AP
AP ----(assoc rsp)---->STA
AP ----( eapol )---->STA
STA ----( eapol )---->AP
AP ----( eapol )---->STA
STA ----( eapol )---->AP
```

这里以 WPA 抓包为例，其 wifi 连接认证抓包如下所示。

Packet	Source	Destination	Flow ID	BSSID	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Application
1	18:8B:86:6D:B9:49	Ethernet Broadcast		Ethernet Broadcast	*	10	100%	6.0	83	0.000000	802.11 Probe Req	
2	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*P	10	100%	1.0	389	0.001740	802.11 Probe Rsp	
3	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*P	10	100%	1.0	389	0.007432	802.11 Probe Rsp	
4	18:8B:86:6D:B9:49	WinstarsTei:A9:AB:4E		WinstarsTei:A9:AB:4E	*	10	100%	6.0	52	0.109920	802.11 Probe Req	
5	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	6.0	34	0.109930	802.11 Ack	
6	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*P	10	100%	1.0	389	0.109920	802.11 Probe Rsp	
7	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*P	10	100%	1.0	389	0.109930	802.11 Probe Rsp	
8	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*P	10	100%	1.0	389	0.201325	802.11 Probe Rsp	
9	18:8B:86:6D:B9:49	WinstarsTei:A9:AB:4E		WinstarsTei:A9:AB:4E	*	10	100%	1.0	34	0.253336	802.11 Auth	
10	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	34	0.253332	802.11 Ack	
11	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	34	0.253323	802.11 Action	
12	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	34	0.254420	802.11 Action	
13	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	34	0.255763	802.11 Auth	
14	18:8B:86:6D:B9:49	WinstarsTei:A9:AB:4E		WinstarsTei:A9:AB:4E	*	10	100%	1.0	118	0.257447	802.11 Assoc Req	
15	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	213	0.257717	802.11 Assoc Rsp	
16	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	213	0.261644	802.11 Assoc Rsp	
17	18:8B:86:6D:B9:49	WinstarsTei:A9:AB:4E		WinstarsTei:A9:AB:4E	**	10	100%	1.0	118	0.263390	802.11 Assoc Req	
18	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	14	0.263400	802.11 Ack	
19	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	137	0.360323	EAPOL-Key	
20	18:8B:86:6D:B9:49	WinstarsTei:A9:AB:4E		WinstarsTei:A9:AB:4E	*	10	100%	1.0	159	0.360462	EAPOL-Key	
21	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	14	0.364470	802.11 Ack	
22	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	153	0.367313	EAPOL-Key	
23	18:8B:86:6D:B9:49	WinstarsTei:A9:AB:4E		WinstarsTei:A9:AB:4E	*	10	100%	1.0	137	0.370699	EAPOL-Key	
24	18:8B:86:6D:B9:49	WinstarsTei:A9:AB:4E		WinstarsTei:A9:AB:4E	*	10	100%	1.0	137	0.372256	EAPOL-Key	
25	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	14	0.372260	802.11 Ack	
26	18:8B:86:6D:B9:49	Ethernet Broadcast		Ethernet Broadcast	U	10	100%	1.0	82	0.374410	802.11 Encrypted ...	
27	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	U	10	100%	1.0	14	0.374410	802.11 Ack	
28	18:8B:86:6D:B9:49	Ethernet Broadcast		WinstarsTei:A9:AB:4E	U	10	100%	1.0	390	0.379031	802.11 Encrypted ...	
29	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	U	10	100%	1.0	14	0.379030	802.11 Ack	
30	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	U	10	100%	1.0	382	0.380621	802.11 Encrypted ...	
31	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	U	10	100%	1.0	382	0.380432	802.11 Encrypted ...	
32	18:8B:86:6D:B9:49	WinstarsTei:A9:AB:4E		WinstarsTei:A9:AB:4E	*	10	100%	1.0	37	0.390463	802.11 Action	
33	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	14	0.390604	802.11 Ack	
34	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	37	0.390607	802.11 Action	
35	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	37	0.390950	802.11 Action	
36	18:8B:86:6D:B9:49	Ethernet Broadcast		WinstarsTei:A9:AB:4E	U	10	100%	1.0	390	0.395970	802.11 Encrypted ...	
37	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	U	10	100%	1.0	14	0.395963	802.11 Ack	
38	WinstarsTei:A9:AB:4E	18:8B:86:6D:B9:49		WinstarsTei:A9:AB:4E	*	10	100%	1.0	32	0.397736	802.11 BA	
39	18:8B:86:6D:B9:49	WinstarsTei:A9:AB:4E		WinstarsTei:A9:AB:4E	*	10	100%	1.0	37	0.396870	802.11 Action	

1.扫描阶段（SCAN）

STA 发送 Probe Req，AP 回复 Probe Rsp 帧。抓包如下：

（1）sta 发出探测请求包 Probe Req

Packet Info Packet Number=4 Flags=0x00000000 Status=0x00000000 Packet Length=52 Timestamp=14:35:55.559706200 08/12/2021

802.11 MAC Header

- Version: 0 [0 Mask 0x03]
- Type: 800 Management [0 Mask 0x0C]
- Subtype: 80100 Probe Request [0 Mask 0xF0]
- Frame Control Flags: 800000000 [1]
- Duration: 304 Microseconds [2-3]
- Destination: 80:3F:5D:A9:A0:4E WinstarsTei:A9:A0:4E [4-9]
- Source: 18:8B:86:6D:B9:49 [10-15]
- BSSID: 80:3F:5D:A9:A0:4E WinstarsTei:A9:A0:4E [16-21]
- Seq Number: 13 [22-23 Mask 0xFFFF0]
- Frag Number: 0 [22 Mask 0x0F]

802.11 Management - Probe Request

- SSID: 10-OSSID Len=6 SSID=tanwav [24-31]
- Rates: 1D=1 Rates: Len=8 Rate=1.0Mbps(BSS Basic Rate) Rate=2.0Mbps(BSS Basic Rate) Rate=5.5Mbps(BSS Basic Rate) Rate=11.0Mbps(BSS Basic Rate) [32-39]
- Extended Supported Rates: 50 Extended Supported Rates Len=4 Rate=6.0Mbps(Not BSS Basic Rate) Rate=12.0Mbps(Not BSS Basic Rate) [40-43]

FCS - Frame Check Sequence

- FCS: 0x413BA600 [48-51]

（2）ap 发出探测响应包 Probe Rsp

Packet Info Packet Number=6 Flags=0x00000000 Status=0x00000000 Packet Length=389 Timestamp=14:35:55.563700200 08/12/2021

802.11 MAC Header

- Version: 0 [0 Mask 0x03]
- Type: 800 Management [0 Mask 0x0C]
- Subtype: 80101 Probe Response [0 Mask 0xF0]
- Frame Control Flags: 800000000 [1]
- Duration: 0 Microseconds [2-3]
- Destination: 18:8B:86:6D:B9:49 [4-9]
- Source: 80:3F:5D:A9:A0:4E WinstarsTei:A9:A0:4E [10-15]
- BSSID: 80:3F:5D:A9:A0:4E WinstarsTei:A9:A0:4E [16-21]
- Seq Number: 1369 [22-23 Mask 0xFFFF0]
- Frag Number: 0 [22 Mask 0x0F]

Probe Rsp: Probe Timestamp=883536223239 Beacon Interval=200 Capability Info=80000010000010001 SSID[10=6 SSID=tanwav [24-384]

FCS - Frame Check Sequence

- FCS: 0x227DC2F0 [385-388]

2.认证阶段（Authentication）

（1）STA 发出链路认证请求包 Authentication Req

Packet Info Packet Number=9 Flags=0x00000000 Status=0x00000000 Packet Length=34 Timestamp=14:35:55.623093200 08/12/2021

802.11 MAC Header

- Version: 0 [0 Mask 0x03]
- Type: 800 Management [0 Mask 0x0C]
- Subtype: 81011 Authentication [0 Mask 0xF0]
- Frame Control Flags: 800000000 [1]
- Duration: 304 Microseconds [2-3]
- Destination: 80:3F:5D:A9:A0:4E WinstarsTei:A9:A0:4E [4-9]
- Source: 18:8B:86:6D:B9:49 [10-15]
- BSSID: 80:3F:5D:A9:A0:4E WinstarsTei:A9:A0:4E [16-21]
- Seq Number: 14 [22-23 Mask 0xFFFF0]
- Frag Number: 0 [22 Mask 0x0F]

802.11 Management - Authentication Auth Algorithm=0 Auth Seq Num=1 Status Code=0 [24-29]

FCS - Frame Check Sequence

- FCS: 0xB87FCC73 [30-33]

(2) AP 发出链路认证响应包 Authentication Rsp

Packet Info Packet Number=13 Flags=0x00000000 Status=0x00000000 Packet Length=34 Timestamp=14:35:55.625540200 08/12/2018

802.11 MAC Header

- Version: 0 [0 Mask 0x03]
- Type: %00 Management [0 Mask 0x0C]
- Subtype: %1011 Authentication [0 Mask 0xF0]
- Frame Control Flags: %00000000 [1]
 - 0... Non-strict order
 - .0... Non-Protected Frame
 - ..0... No More Data
 - ...0... Power Management - active mode
 -0... This is not a Re-Transmission
 -0... Last or Unfragmented Frame
 -0... Not an Exit from the Distribution System
 -0... Not to the Distribution System
- Duration: 314 Microseconds [2-3]
- Destination: 18:B8:86:6D:B9:49 [4-9]
- Source: 80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [10-15]
- BSSID: 80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [16-21]
- Seq Number: 1375 [22-23 Mask 0xFFFF0]
- Frag Number: 0 [22 Mask 0x0F]

[24-29] 802.11 Management - Authentication Auth Algorithm=0Open System Auth Seq Num=2 Status Code=0Successful

FCS - Frame Check Sequence

FCS: 0xB4C68567 [30-33]

3.关联 (Association)

(1) STA 发出关联请求包 Association Req

Packet Info Packet Number=14 Flags=0x00000000 Status=0x00000000 Packet Length=118 Timestamp=14:35:55.627224200 08/12/2018

802.11 MAC Header

- Version: 0 [0 Mask 0x03]
- Type: %00 Management [0 Mask 0x0C]
- Subtype: %0000 Association Request [0 Mask 0xF0]
- Frame Control Flags: %00000000 [1]
 - 0... Non-strict order
 - .0... Non-Protected Frame
 - ..0... No More Data
 - ...0... Power Management - active mode
 -0... This is not a Re-Transmission
 -0... Last or Unfragmented Frame
 -0... Not an Exit from the Distribution System
 -0... Not to the Distribution System
- Duration: 304 Microseconds [2-3]
- Destination: 80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [4-9]
- Source: 18:B8:86:6D:B9:49 [10-15]
- BSSID: 80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [16-21]
- Seq Number: 15 [22-23 Mask 0xFFFF0]
- Frag Number: 0 [22 Mask 0x0F]

[24-113] Assoc Req: Capability Info=%0000010000010001 Listen Interval=3 SSID[ID=0 Len=6 SSID=tanwav] Rates=[ID=1 Len=8 Rate=1.0 Rate=2.0 Rate=5.5 Rate=11 Rate=22 Rate=48 Rate=96 Rate=192 Rate=384 Rate=768 Rate=1536 Rate=3072 Rate=6144 Rate=12288 Rate=24576 Rate=49152 Rate=98304 Rate=196608 Rate=393216 Rate=786432 Rate=1572864 Rate=3145728 Rate=6291456 Rate=12582912 Rate=25165824 Rate=50331648 Rate=100663296 Rate=201326592 Rate=402653184 Rate=805306368 Rate=1610612736 Rate=3221225472 Rate=6442450944 Rate=12884901888 Rate=25769803776 Rate=51539607552 Rate=103079215104 Rate=206158430208 Rate=412316860416 Rate=824633720832 Rate=1649267441664 Rate=3298534883328 Rate=6597069766656 Rate=13194139533312 Rate=26388279066624 Rate=52776558133248 Rate=105553116266496 Rate=211106232532992 Rate=422212465065984 Rate=844424930131968 Rate=1688849860263936 Rate=3377699720527872 Rate=6755399441055744 Rate=13510798882111488 Rate=27021597764222976 Rate=54043195528445952 Rate=108086391056891904 Rate=216172782113783808 Rate=432345564227567616 Rate=864691128455135232 Rate=1729382256910270464 Rate=3458764513820540928 Rate=6917529027641081856 Rate=13835058055282163712 Rate=27670116110564327424 Rate=55340232221128654848 Rate=110680464442257309696 Rate=221360928884514619392 Rate=442721857769029238784 Rate=885443715538058477568 Rate=1770887431076116955136 Rate=3541774862152233910272 Rate=7083549724304467820544 Rate=14167099448608935641088 Rate=28334198897217871282176 Rate=56668397794435742564352 Rate=113336795588871485128704 Rate=226673591177742970257408 Rate=453347182355485940514816 Rate=906694364710971881029632 Rate=1813388729421943762059264 Rate=3626777458843887524118528 Rate=7253554917687775048237056 Rate=14507109835375550096474112 Rate=29014219670751100192948224 Rate=58028439341502200385896448 Rate=116056878683004400771792896 Rate=232113757366008801543585792 Rate=464227514732017603087171584 Rate=928455029464035206174343168 Rate=1856910058928070412348686336 Rate=3713820117856140824697372672 Rate=7427640235712281649394745344 Rate=14855280471424563298789490688 Rate=29710560942849126597578981376 Rate=59421121885698253195157962752 Rate=118842243771396506390315925504 Rate=237684487542793012780631851008 Rate=475368975085586025561263702016 Rate=950737950171172051122527404032 Rate=1901475900342344102245054808064 Rate=3802951800684688204490109616128 Rate=7605903601369376408980219232256 Rate=15211807202738752817960438464512 Rate=30423614405477505635920876929024 Rate=60847228810955011271841753858048 Rate=121694457621910022543683507716096 Rate=243388915243820045087367015432192 Rate=486777830487640090174734030864384 Rate=973555660975280180349468061728768 Rate=1947111321950560360698936123457536 Rate=3894222643901120721397872246915072 Rate=7788445287802241442795744493830144 Rate=15576890575604482885591488987660288 Rate=31153781151208965771182977975320576 Rate=62307562302417931542365955950641152 Rate=124615124604835863084731911901282304 Rate=249230249209671726169463823802564608 Rate=498460498419343452338927647605129216 Rate=996920996838686904677855295210258432 Rate=1993841993677373809355710590420516864 Rate=3987683987354747618711421180841033728 Rate=7975367974709495237422842361682067456 Rate=15950735949418990474845684723364134912 Rate=31901471898837980949691369446728269824 Rate=63802943797675961899382738893456539648 Rate=127605887595351923798765477786913079296 Rate=255211775190703847597530955573826158592 Rate=510423550381407695195061911147652317184 Rate=1020847100762815390390123822295304634368 Rate=2041694201525630780780247644590609268736 Rate=4083388403051261561560495289181218537472 Rate=8166776806102523123120990578362437074944 Rate=16333553612205046246241981156724874149888 Rate=32667107224410092492483962313449748299776 Rate=65334214448820184984967924626899496599552 Rate=130668428897640369969935849253798993199104 Rate=261336857795280739939871698507597986398208 Rate=522673715590561479879743397015195972796416 Rate=1045347431181122959759486794030391945592832 Rate=2090694862362245919518973588060783891185664 Rate=4181389724724491839037947176121567782371328 Rate=8362779449448983678075894352243135564742656 Rate=16725558898897967356151788704486271129485312 Rate=33451117797795934712303577408972542258970624 Rate=66902235595591869424607154817945084517941248 Rate=133804471191183738849214309635890169035882496 Rate=267608942382367477698428619271780338071764992 Rate=535217884764734955396857238543560676143529984 Rate=1070435769529469910793714477087121352287059968 Rate=2140871539058939821587428954174242704574119936 Rate=4281743078117879643174857908348485409148239872 Rate=8563486156235759286349715816696970818296479744 Rate=17126972312471518572699431633393941636592959488 Rate=34253944624943037145398863266787883273185918976 Rate=68507889249886074290797726533575766546371837952 Rate=137015778499772148581595453067151533092743675904 Rate=274031556999544297163190906134303066185487351808 Rate=548063113999088594326381812268606132370974703616 Rate=1096126227998177188652763624537212264741949407232 Rate=2192252455996354377305527249074424529483898814464 Rate=4384504911992708754611054498148849058967797628928 Rate=8769009823985417509222108996297698117935595257856 Rate=17538019647970835018444217992595396235871190515712 Rate=35076039295941670036888435985190792471742381031424 Rate=70152078591883340073776871970381584943484762062848 Rate=140304157183766680147553743940763169886969524125696 Rate=280608314367533360295107487881526339773939048251392 Rate=561216628735066720590214975763052679547878096502784 Rate=1122433257470133441180429951526105359095756193005568 Rate=2244866514940266882360859903052210718191512386011136 Rate=4489733029880533764721719806104421436383024772022272 Rate=8979466059761067529443439612208842872766049544044544 Rate=17958932119522135058886879224417685745532099088089088 Rate=35917864239044270117773758448835371491064198176178176 Rate=71835728478088540235547516897670742982128396352356352 Rate=143671456956177080471095033795341485964256792704712704 Rate=287342913912354160942190067590682971928513585409425408 Rate=574685827824708321884380135181365943857027170818850816 Rate=1149371655649416643768760270362731887714054341637701632 Rate=2298743311298833287537520540725463775428108683275403264 Rate=4597486622597666575075041081450927550856217366550806528 Rate=9194973245195333150150082162901855101712434733101613056 Rate=18389946490390666300300164325803710203424869466203226112 Rate=36779892980781332600600328651607420406849738932406452224 Rate=73559785961562665201200657303214840813699477864812904448 Rate=147119571923125330402401314606429681627398955729625808896 Rate=294239143846250660804802629212859363254797911459251617792 Rate=588478287692501321609605258425718726509595822918503235584 Rate=1176956575385002643219210516851437453019191645837006471168 Rate=2353913150770005286438421033702874906038383291674012942336 Rate=4707826301540010572876842067405749812076766583348025884672 Rate=9415652603080021145753684134811499624153533166696051769344 Rate=18831305206160042291507368269622999248307066333392103538688 Rate=37662610412320084583014736539245998496614132666784206717376 Rate=75325220824640169166029473078491996993228265333568413434752 Rate=150650441649280338332058946156983993986456530667136826869504 Rate=301300883298560676664117892313967987972913061334273653739008 Rate=602601766597121353328235784627935975945826122668547307478016 Rate=1205203533194242706656471569255871951891652245337094614956032 Rate=2410407066388485413312943138511743903783304490674189229912064 Rate=4820814132776970826625886277023487807566608981348378459824128 Rate=9641628265553941653251772554046975615133217962696756919648256 Rate=19283256531107883306503545108093951230266435925393513839296512 Rate=38566513062215766613007090216187902460532871850787027678593024 Rate=77133026124431533226014180432375804921065743701574055357186048 Rate=154266052248863066452028360864751609842131487403148110714372096 Rate=308532104497726132904056721729503219684262974806296221428744192 Rate=617064208995452265808113443459006439368525949612592442857488384 Rate=1234128417990904531616226886918012878737051899225184885714976768 Rate=2468256835981809063232453773836025757474103798450369771429953536 Rate=4936513671963618126464907547672051514948207596900739542859907072 Rate=9873027343927236252929815095344103029896415193801479085719814144 Rate=19746054687854472505859630190688206059792830387602958171439628288 Rate=39492109375708945011719260381376412119585660775205916342879256576 Rate=78984218751417890023438520762752824239171321550411832685758513152 Rate=157968437502835780046877041525505648478342643100823665371517026304 Rate=315936875005671560093754083051011296956685286201647330743034052608 Rate=631873750011343120187508166102022593913370572403294661486068105216 Rate=1263747500022686240375016332204045187826741144806589322972136210432 Rate=2527495000045372480750032664408090375653482289613178645944272420864 Rate=5054990000090744961500065328816180751306964579226357291888544841728 Rate=10109980000181499923000130657632361502613929158452714583777089683456 Rate=20219960000362999846000261315264723005227858316905429167554179366912 Rate=40439920000725999692000522630529446010455716633810858335108358733824 Rate=80879840001451999384001045261058892020911433267621716670216717467648 Rate=161759680003039998768002090522117784041822866535243433340433434935296 Rate=323519360006079997536004181044235568083645733070486866680866869870592 Rate=647038720012159995072008362088471136167291466140973733361733739741184 Rate=1294077440024319990144016724176942272334582932281947466723467479482368 Rate=2588154880048639980288033448353884544669165864563894933446934958964736 Rate=5176309760097279960576066896707769089338331729127789866893869917929472 Rate=10352619520194559921152133793415538178676663458255579733787739835858944 Rate=20705239040389119842304267586831076357353326916511159467575479671717888 Rate=41410478080778239684608535173662152714706653833022318935150959343435776 Rate=82820956161556479369217070347324305429413307666044637870301918686871552 Rate=165641912323112958738434140694648610858826615332089275740603837373743104 Rate=331283824646225917476868281389297221717653230664178551481207674747486208 Rate=662567649292451834953736562778594443435306461328357102962415349494972416 Rate=1325135298584903669907473125557188886870612922656714205924830698989944832 Rate=2650270597169807339814946251114377773741225845313428411849661397979889664 Rate=5300541194339614679629892502228755547482451690626856823699322795959779328 Rate=10601082388679229359259785004457511094964903381253713647398645591919558656 Rate=21202164777358458718519570008915022189929806762507427294797291183839117312 Rate=42404329554716917437039140017830044379859613525014854589594582367678234624 Rate=84808659109433834874078280035660088759719227050029709179189164735356469248 Rate=169617318218867669748156560071320177519438454100059418358378329470712938496 Rate=339234636437735339496313120142640355038876908200118836716756658941425876992 Rate=678469272875470678992626240285280710077753816400237673433513317882851753984 Rate=1356938545750941357985252480570561420155507632800475346867026635765703507968 Rate=2713877091501882715970504961141122840311015265600950693734053271531407015936 Rate=5427754183003765431941009922282245680622030531201901387468106543062814031872 Rate=10855508366007530863882019844564491361244061062403802774936213086125628063744 Rate=21711016732015061727764039689128982722488122124807605549872426172251256127488 Rate=43422033464030123455528079378257965444976244249615211099744852344502512254976 Rate=86844066928060246911056158756515930889952488499230422199489704689005024509952 Rate=173688133856120493822112317513031861779904976998460844398979409378010049019904 Rate=347376267712240987644224635026063723559809953996921688797958818756020098039808 Rate=694752535424481975288449270052127447119619907993843377595917637512040196079616 Rate=1389505070848963950576898540104254894239239815987686755191835275024080392159232 Rate=2779010141697927901153797080208509788478479631975373510383670550048160784318464 Rate=5558020283395855802307594160417019576956959263950747020767341100096321568636928 Rate=11116040566791711604615188320834039153913918527901494041534682200192643137273856 Rate=22232081133583423209230376641668078307827837055802988083069364400385286274547712 Rate=444641622671668464

```

Packet Info Packet Number=19 Flags=0x00000000 Status=0x00000000 Packet Length=137 Timestamp=14:35:55.730100200 08/12/20
802.11 MAC Header
  Version: 0 [0 Mask 0x03]
  Type: %10 Data [0 Mask 0x0C]
  Subtype: %1000 QoS Data [0 Mask 0xF0]
  Frame Control Flags: %00000010 [1]
    0... Non-strict order
    0... Non-Protected Frame
    0... No More Data
    0... Power Management - active mode
    0... This is not a Re-Transmission
    0... Last or Unfragmented Frame
    0... Exit from the Distribution System
    0... Not to the Distribution System
  Duration: 314 Microseconds [2-3]
  Destination: 18:8B:86:1D:B9:49 [4-9]
  Source: 80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [10-15]
  Seq Number: 0 [22-23 Mask 0xFFF0]
  Frag Number: 0 [24 Mask 0x0F]
  QoS Control Field: %0000000000000000 [24-25]
    AP PS Buffer State: 0
    A-MSDU: Not Present
    Ack: Normal Acknowledge
    EOSP: Not End of Triggered Service Period
    0000 UP: 0 - Best Effort
802.2 Logical Link Control (LLC) Header
  Dest. SAP: 0xAA SNAP [26]
  Source SAP: 0xAA SNAP [27]
  Command: 0x03 Unnumbered Information [28]
  Vendor ID: 0x000000 XEROX CORPORATION [29-31]
  Protocol Type: 0x88BE IEEE Std 802.1X - Port-based network access control [32-33]
802.1x Authentication
  Protocol Version: 1 [34]
  Packet Type: 3 EAPOL - Key [35]
  Body Length: 95 [36-37]
  EAPOL - Key
    Type: 2 RSN key descriptor [38]
    Key Information: %000000010001010 [39-40]
      Reserved
      0... SHK Handshake is not supported
      0... Key Data Not Encrypted
      0... No Request to Initiate Handshake
      0... No Error
      0... Not Secure
      0... Message does NOT contain Key MIC
      0... Key ACK
      0... Install: 802.1X component shall not configure the temporal key
      0... Reserved
      0... Key Type: Pairwise Key
      0... 010 Vers: HMAC-SHA1-128 is the EAPOL-Key MIC / NIST AES key wrap is the EAPOL-key enc
    Key Length: 16 CCMP [41-42]
    Replay Counter: 1 [43-50]
    Key Nonce: 0x50B23506EAE27317A1404FC5ED7A0520B4A4EF29540394CD75A8904886CF7 [51-62]
    EAPOL-Key IV: 0x00000000000000000000000000000000 [63-98]
    Key RSC: 0x0000000000000000 [99-106]
    Key ID: 0x0000000000000000 [107-114]
    Key MIC: 0x00000000000000000000000000000000 [115-130]
    Key Data Len: 0 [131-132]
  FCS - Frame Check Sequence
    FCS: 0xCDF48B8 [133-136]

```

(2) STA 发出 EAPOL-Key(SNonce, Unicast, MIC)

```

Packet Info Packet Number=20 Flags=0x00000000 Status=0x00000000 Packet Length=159 Timestamp=14:35:55.734240200 08/12/20
802.11 MAC Header
  Version: 0 [0 Mask 0x03]
  Type: %10 Data [0 Mask 0x0C]
  Subtype: %1000 QoS Data [0 Mask 0xF0]
  Frame Control Flags: %00000001 [1]
    0... Non-strict order
    0... Non-Protected Frame
    0... No More Data
    0... Power Management - active mode
    0... This is not a Re-Transmission
    0... Last or Unfragmented Frame
    0... Not an Exit from the Distribution System
    0... To the Distribution System
  Duration: 202 Microseconds [2-3]
  Destination: 80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [4-9]
  Source: 18:8B:86:1D:B9:49 [10-15]
  Seq Number: 0 [22-23 Mask 0xFFF0]
  Frag Number: 0 [24 Mask 0x0F]
  QoS Control Field: %0000000000000000 [24-25]
    AP PS Buffer State: 0
    A-MSDU: Not Present
    Ack: Normal Acknowledge
    EOSP: Not End of Triggered Service Period
    0000 UP: 0 - Best Effort
802.2 Logical Link Control (LLC) Header
  Dest. SAP: 0xAA SNAP [26]
  Source SAP: 0xAA SNAP [27]
  Command: 0x03 Unnumbered Information [28]
  Vendor ID: 0x000000 XEROX CORPORATION [29-31]
  Protocol Type: 0x88BE IEEE Std 802.1X - Port-based network access control [32-33]
802.1x Authentication
  Protocol Version: 1 [34]
  Packet Type: 3 EAPOL - Key [35]
  Body Length: 117 [36-37]
  EAPOL - Key
    Type: 2 RSN Key descriptor [38]
    Key Information: %000000010001010 [39-40]
      Reserved
      0... SHK Handshake is not supported
      0... Key Data Not Encrypted
      0... No Request to Initiate Handshake
      0... No Error
      0... Not Secure
      0... Message contains Key MIC
      0... No Key ACK
      0... Install: 802.1X component shall not configure the temporal key
      0... Reserved
      0... Key Type: Pairwise Key
      0... 010 Vers: HMAC-SHA1-128 is the EAPOL-Key MIC / NIST AES key wrap is the EAPOL-key enc
    Key Length: 0 [41-42]
    Replay Counter: 1 [43-50]
    Key Nonce: 0x35EAD4A85040F7590AA3468C18870E1C3870571932D3A64C2FE965CA9428E7CE [51-82]
    EAPOL-Key IV: 0x00000000000000000000000000000000 [83-98]
    Key RSC: 0x0000000000000000 [99-106]
    Key ID: 0x0000000000000000 [107-114]
    Key MIC: 0x7F1676E75D2AC36CDA2282A4EE37687 [115-130]
    Key Data Len: 22 [131-132]
  RSN: ID=4RSN: Len=20 Version=1 Group Cipher OUI=00-0F-ACIEEE 802.11 Group Cipher Type=4CCMP - default in an RSN Pairw
  FCS - Frame Check Sequence
    FCS: 0x7A83A829 [133-158]

```


(3) AP 发出 EAPOL-Key(Install PTK, Unicast, MIC, Encrypted GTK)

Packet Info Packet Number=22 Flags=0x00000000 Status=0x00000000 Packet Length=193 Timestamp=14:35:55.737092200 08/12/20	
802.11 MAC Header	
Version:	0 [0 Mask 0x03]
Type:	%10 Data [0 Mask 0x0C]
Subtype:	%1000 QoS Data [0 Mask 0xF0]
Frame Control Flags: %00000010 [1]	
0... Non-strict order 0... Non-Protected Frame 0... No More Data 0... Power Management - active mode 0... This is not a Re-Transmission 0... Last or Unfragmented Frame 1... Exit from the Distribution System 0... Not to the Distribution System	
Duration:	314 Microseconds [2-3]
Destination:	18:BB:86:6D:B9:49 [4-9]
BSSID:	80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [10-15]
Source:	80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [16-21]
Seq Number:	1 [22-23 Mask 0xFFF0]
Frag Number:	0 [22 Mask 0x0F]
QoS Control Field: %0000000000000000 [24-25]	
AP PS Buffer State: 0 A-MSDU: Not Present Ack: Normal Acknowledge EOSP: Not End of Triggered Service Period 0000 UP: 0 - Best Effort	
802.2 Logical Link Control (LLC) Header	
Dest. SAP:	0xAA SNAP [26]
Source SAP:	0xAA SNAP [27]
Command:	0xB3 Unnumbered Information [28]
Vendor ID:	0x000000 XEROX CORPORATION [29-31]
Protocol Type:	0x88BE IEEE Std 802.1X - Port-based network access control [32-33]
802.1x Authentication	
Protocol Version:	1 [34]
Packet Type:	3 EAPOL - Key [35]
Body Length:	151 [36-37]
EAPOL - Key	
Type:	2 RSN key descriptor [38]
Key Information: %000100111001010 [39-40]	
XX... Reserved 0... SMK Handshake is not supported 1... Key Data Encrypted 0... No Request to Initiate Handshake 0... No Error 1... Secure 1... Message contains Key MIC 1... Key ACK 1... Install: 802.1X component shall configure the temporal key XX... Reserved 1... Key Type: Pairwise Key 010 Vers: HMAC-SHA1-128 is the EAPOL-Key MIC / NIST AES key wrap is the EAPOL-key enc	
Key Length:	16 CCMP [41-42]
Replay Counter:	2 [43-50]
Key Nonce:	0x5006235086EA1E2737A1484FCE07A052084A4EF29540394CD75A8904886CF7 [51-82]
EAPOL-Key IV:	0x00000000000000000000000000000000 [83-98]
Key RSC:	0xE601010000000000 [99-106]
Key ID:	0x0000000000000000 [107-114]
Key MIC:	0x3EAB07217FCAC02688937CC45676BACC [115-130]
Key Data Len:	56 [131-132]
Key Data:	(56 bytes) [133-188]
FCS - Frame Check Sequence	
FCS:	0x263161AA [189-192]

(4) STA 发出 EAPOL-Key(Unicast,MIC)

Packet Info Packet Number=23 Flags=0x00000000 Status=0x00000000 Packet Length=137 Timestamp=14:35:55.740476200 08/12/20	
802.11 MAC Header	
Version:	0 [0 Mask 0x03]
Type:	%10 Data [0 Mask 0x0C]
Subtype:	%1000 QoS Data [0 Mask 0xF0]
Frame Control Flags: %00000001 [1]	
0... Non-strict order 0... Non-Protected Frame 0... No More Data 0... Power Management - active mode 0... This is not a Re-Transmission 0... Last or Unfragmented Frame 0... Not an Exit from the Distribution System 1... To the Distribution System	
Duration:	202 Microseconds [2-3]
BSSID:	80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [4-9]
Source:	18:BB:86:6D:B9:49 [10-15]
Destination:	80:3F:5D:A9:A0:4E WinstarsTe:A9:A0:4E [16-21]
Seq Number:	1 [22-23 Mask 0xFFF0]
Frag Number:	0 [22 Mask 0x0F]
QoS Control Field: %0000000000000000 [24-25]	
AP PS Buffer State: 0 A-MSDU: Not Present Ack: Normal Acknowledge EOSP: Not End of Triggered Service Period 0000 UP: 0 - Best Effort	
802.2 Logical Link Control (LLC) Header	
Dest. SAP:	0xAA SNAP [26]
Source SAP:	0xAA SNAP [27]
Command:	0xB3 Unnumbered Information [28]
Vendor ID:	0x000000 XEROX CORPORATION [29-31]
Protocol Type:	0x88BE IEEE Std 802.1X - Port-based network access control [32-33]
802.1x Authentication	
Protocol Version:	1 [34]
Packet Type:	3 EAPOL - Key [35]
Body Length:	95 [36-37]
EAPOL - Key	
Type:	2 RSN key descriptor [38]
Key Information: %000000100001010 [39-40]	
XX... Reserved 0... SMK Handshake is not supported 0... Key Data Not Encrypted 0... No Request to Initiate Handshake 0... No Error 1... Secure 0... Message contains Key MIC 0... No Key ACK 0... Install: 802.1X component shall not configure the temporal key XX... Reserved 1... Key Type: Pairwise Key 010 Vers: HMAC-SHA1-128 is the EAPOL-Key MIC / NIST AES key wrap is the EAPOL-key enc	
Key Length:	0 [41-42]
Replay Counter:	2 [43-50]
Key Nonce:	0x00 [51-82]
EAPOL-Key IV:	0x00000000000000000000000000000000 [83-98]
Key RSC:	0x0000000000000000 [99-106]
Key ID:	0x0000000000000000 [107-114]
Key MIC:	0x142A998E14076458CF14DF1FFF5BCF3 [115-130]
Key Data Len:	0 [131-132]
FCS - Frame Check Sequence	
FCS:	0xE2992A99 [133-136]