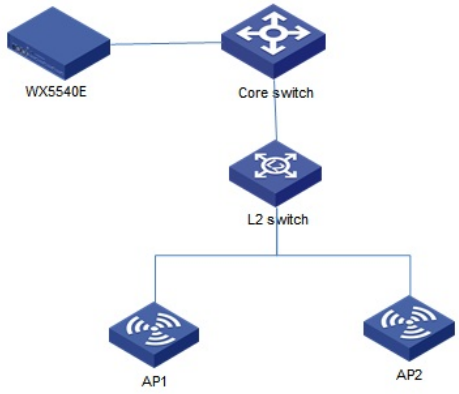
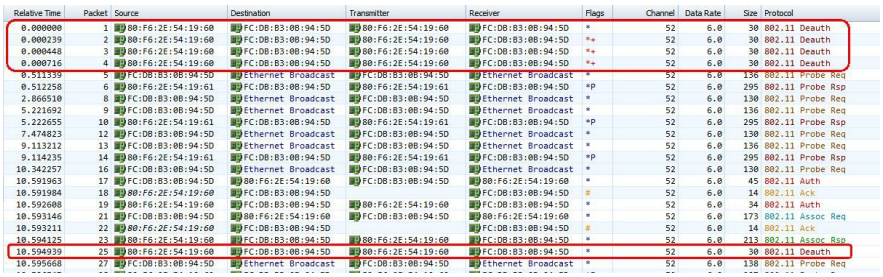
某局点PSK加密大量终端关联失败问题处理经验案例

wlan接入 wlan射频 wlan安全 MAC地址认证 端口安全 **殷俊** 2016-07-09 发表

某局点使用无线控制器WX5540E配置多种款型AP进行无线覆盖，以保证多种环境的用户使用。用户使用场景为大型园区办公网，无线接入采用WPA+TKIP、WPA2+CCMP混合加密PSK认证方式。
无线用户使用时，在某些时间段会出现关联失败，尝试多次关联才可关联上，甚至一直关联不上。不分场景跟AP，所有区域均会出现该问题。



先按照无线的云图之终端关联失败问题排查，排除信号覆盖问题、干扰问题、接入用户数限制问题、误配置问题、个别终端问题等。尝试新增不加密SSID，终端尝试关联正常。
出问题时采集空口抓包信息，分析终端关联失败是终端问题还是无线问题，通过抓包信息来看，终端是被AP踢掉，AP发送deauth报文，强制终端下线。如下所示：



Relative Time	Packet	Source	Destination	Transmitter	Receiver	Flags	Channel	Data Rate	Size	Protocol
0.000000	1	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	*	52	6.0	30	802.11 Deauth
0.000239	2	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	*+	52	6.0	30	802.11 Deauth
0.000448	3	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	*+	52	6.0	30	802.11 Deauth
0.000716	4	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	*+	52	6.0	30	802.11 Deauth
0.511339	5	FC:DB:B3:0B:94:5D	Ethernet Broadcast	FC:DB:B3:0B:94:5D	Ethernet Broadcast	*	52	6.0	136	802.11 Probe Req
0.512258	6	80:F6:2E:54:19:61	FC:DB:B3:0B:94:5D	80:F6:2E:54:19:61	FC:DB:B3:0B:94:5D	*P	52	6.0	295	802.11 Probe Rsp
2.866510	8	FC:DB:B3:0B:94:5D	Ethernet Broadcast	FC:DB:B3:0B:94:5D	Ethernet Broadcast	*	52	6.0	130	802.11 Probe Req
5.221692	9	FC:DB:B3:0B:94:5D	Ethernet Broadcast	FC:DB:B3:0B:94:5D	Ethernet Broadcast	*	52	6.0	136	802.11 Probe Req
5.222655	10	80:F6:2E:54:19:61	FC:DB:B3:0B:94:5D	80:F6:2E:54:19:61	FC:DB:B3:0B:94:5D	*P	52	6.0	295	802.11 Probe Rsp
7.474823	12	FC:DB:B3:0B:94:5D	Ethernet Broadcast	FC:DB:B3:0B:94:5D	Ethernet Broadcast	*	52	6.0	130	802.11 Probe Req
9.113212	13	FC:DB:B3:0B:94:5D	Ethernet Broadcast	FC:DB:B3:0B:94:5D	Ethernet Broadcast	*	52	6.0	136	802.11 Probe Req
9.114235	14	80:F6:2E:54:19:61	FC:DB:B3:0B:94:5D	80:F6:2E:54:19:61	FC:DB:B3:0B:94:5D	*P	52	6.0	295	802.11 Probe Rsp
10.342257	16	FC:DB:B3:0B:94:5D	Ethernet Broadcast	FC:DB:B3:0B:94:5D	Ethernet Broadcast	*	52	6.0	130	802.11 Probe Req
10.591963	17	FC:DB:B3:0B:94:5D	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	80:F6:2E:54:19:60	*	52	6.0	45	802.11 Auth
10.591984	18	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D		FC:DB:B3:0B:94:5D	#	52	6.0	14	802.11 Ack
10.592608	19	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	*	52	6.0	34	802.11 Auth
10.593146	21	FC:DB:B3:0B:94:5D	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	80:F6:2E:54:19:60	*	52	6.0	173	802.11 Assoc Req
10.593211	22	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D		FC:DB:B3:0B:94:5D	#	52	6.0	14	802.11 Ack
10.594125	23	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	*	52	6.0	213	802.11 Assoc Rsp
10.594939	25	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	80:F6:2E:54:19:60	FC:DB:B3:0B:94:5D	*	52	6.0	30	802.11 Deauth
10.595668	27	FC:DB:B3:0B:94:5D	Ethernet Broadcast	FC:DB:B3:0B:94:5D	Ethernet Broadcast	*	52	6.0	138	802.11 Probe Req

Deauth报文中reason code为1：

```
Packet Info
    Packet Number:          25
    Flags:                  0x00000000
    Status:                 0x00000000
    Packet Length:          30
    Timestamp:              16:08:46.808235200 05/05/2016
    Data Rate:              12  6.0 Mbps
    Channel:                52  5260MHz  802.11a
    Signal Level:           83%
    Signal dBm:             -57
    Noise Level:            31%
    Noise dBm:              -82
802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %00  Management [0 Mask 0x0C]
    Subtype:                %1100  Deauthentication [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:               60  Microseconds [2-3]
    Destination:            FC:DB:B3:0B:94:5D [4-9]
    Source:                 80:F6:2E:54:19:60 [10-15]
    BSSID:                  80:F6:2E:54:19:60 [16-21]
    Seq Number:             3413 [22-23 Mask 0xFFF0]
    Frag Number:            0 [22 Mask 0x0F]
802.11 Management - Deauthentication
    Deauthentication Reason Code: 1  Unspecified reason [24-25]
FCS - Frame Check Sequence
    FCS:                    0xFDEA2F32  Calculated
```

同时在AC上打开debug调试信息，采集终端关联失败详细信息，相关调试信息如下：

debugging wlan mac all

debugging wlan mac error

debugging port-security error

问题复现时采集debug关键信息如下：

InspurAC_Master WMAC/6/WMAC_CLIENT_GOES_OFFLINE: Client fcdb-b30b-945d disconnected from WLAN Inspur-L. Reason code is 1.

InspurAC_Master PORTSEC/7/Error: port-security PSK user up to limits

该信息表示AC上PSK认证用户已达到上限，超过设备规格。V5平台无线控制器PSK认证用户规格限制为4K。

由于该局点接入认证全部用的是PSK加密，查看当前在线用户数已超过4K，如下：

dis wlan client

Total Number of Clients : 4103

目前V5平台所有无线控制器的PSK认证用户规格都是4K，但不同款型的AC对接入用户数的规格又不一样，该局点WX5540E完全可以满足4K以上用户接入。所以不建议新增设备扩容，通过mac-and-psk的认证方式可以解决该问题，扩展规格。 具体配置方法如下：

配置AC

启用端口安全。

system-view

[AC] port-security enable

配置无线端口安全，使用MAC-and-PSK认证。

[AC] interface wlan-ess 2

[AC-WLAN-ESS2] port-security port-mode mac-and-psk

[AC-WLAN-ESS2] port-security tx-key-type 11key

[AC-WLAN-ESS2] port-security preshared-key pass-phrase 12345678

[AC-WLAN-ESS2] quit

创建服务模板2（加密类型服务模板），配置SSID为mactest，将WLAN-ESS2接口绑定到服务模板2。

[AC] wlan service-template 2 crypto

[AC-wlan-st-2] ssid mactest

[AC-wlan-st-2] bind wlan-ess 2

[AC-wlan-st-2] cipher-suite ccmp

[AC-wlan-st-2] security-ie rsn

[AC-wlan-st-2] service-template enable

[AC-wlan-st-2] quit

创建AP 1的模板，名称为ap1，型号名称选择WA3628i-AGN，并配置AP 1的序列号为210235A29G007C000020。

[AC] wlan ap ap1 model WA3628i-AGN

[AC-wlan-ap-ap1] serial-id 210235A29G007C000020

将服务模板2绑定到AP 1的radio 1口。

[AC-wlan-ap-ap1] radio 1 type dot11an

[AC-wlan-ap-ap1-radio-1] service-template 2

[AC-wlan-ap-ap1-radio-1] radio enable

[AC-wlan-ap-ap1-radio-1] quit

[AC-wlan-ap-ap1] quit

添加认证域cams，都配为“none”。

[AC] domain cams

[AC-isp-cams] authentication none

[AC-isp-cams] authorization none

[AC-isp-cams] accounting none

[AC-isp-cams] quit

指定MAC认证域为cams。

[AC] mac-authentication domain cams