

### 802.1x无线接入服务正常上线过程报文简析

1.这个接入过程中参与的功能模块有WMAC (802.11链路协商模块)、端口安全 (接入认证的统一管理模块)、802.1x模块 (802.1x认证报文处理模块)、AAA模块 (认证处理模块)、Radius模块 (和Radius server的认证处理模块), 即收集上述几个方面的调试信息, 如下:

```
debugging wlan mac all
```

```
debugging port-security all
```

```
debugging dot1x all
```

```
debugging radius packet
```

2.客户端和设备的WMAC进行链路协商, 当设备确认协商成功, 也就是成功给客户端发送了Association response报文 (通过调试信息可以看到“WMAC/7/EVENT : ACK received for association response”), 则说明802.11链路已经建立成功, 之后WMAC会通知端口安全进行802.1x认证;

3.端口安全的调试信息“PORTSEC/7/Event: Port:WLAN-DBSS1:2,Receive PORTSEC\_RCVMSG\_AU THREQ\_1X\_11KEY msg” (例如\_1X\_11KEY) 表明端口安全已经接收到了WMAC触发认证的认证请求;

4.端口安全直接通知802.1x模块启动认证, 通过调试信息“8021X/7/EVENT: Port:WLAN-DBSS1:2,Port sec received the 802.1x authenticate request from WLAN.”可以确认;

5.802.1x模块首先会发送一个Packet Type: 0和Packet Length: 5的报文 (EAP request报文) 给客户端, 此后通常802.1x模块会收到来自于客户端的一个“EAPOL-START”报文, 通常会有下面的提示信息“8021X/7/PACKET: Port:WLAN-DBSS1:2,Auth:36,Received EAPOL-Start but user has online.”。该信息对协商没有影响, 而且802.1x模块会直接再次发送一个EAP Request报文。 报文如下:

```
---Verbose information of the packet---
```

```
Destination Mac Address: 6c88-1459-898c
```

```
Source Mac Address: 5866-ba5e-c6f0
```

```
Mac Frame Type: 888e.
```

```
Protocol Version ID: 1.
```

```
Packet Type: 0.
```

```
Packet Length: 5.
```

```
-----Packet Body-----
```

```
Code: 1.
```

```
Identifier: 1.
```

```
Length: 5.
```

6.当802.1x模块在发送了第一个EAPOL-Request之后, 接收到无线客户端的EAPOL-Response报文, 如果一切正常就会触发radius认证报文“8021X/7/EVENT: Auth:36,Processing node EAP relay...”。如果没有收到response或者没有发送radius认证报文, 则很大程度上说明客户端配置有问题或者携带的用户名、域名信息可能存在错误;

7.Radius模块发送认证报文的调试信息通常为“RDS/7/DEBUG: Recv MSG:[MsgType=Auth request Index = 36, ulParam3=3437348848]”, 随后跟随一个radius报文的发送过程, 包

```
括“Send attribute list”和“Send Raw Packet is.”;
```

```
WX3010E RDS/7/DEBUG: Send attribute list:
```

```
WX3010E RDS/7/DEBUG:
```

```
[1 User-name          ] [7] [dot1x]
[12 Framed-MTU       ] [6] [1450]
[79 EAP-Message      ] [12] [0201000A01646F743178]
[80 Message-Authenticator ] [18] [00000000000000000000000000000000]
[89 Chargeable_user_identity ] [3] []
[4 NAS-IP-Address    ] [6] [10.153.43.141]
```

8.之后, Radius模块会等待服务器的回应报文“RDS/7/DEBUG: Recv MSG,[MsgType=PKT response Index = 80, ulParam3=3437728656]”, 并且由802.1x模块转化为802.1x报文“8021X/7/EVENT:Auth:164,Msg: ACM eap relay.”发送到无线客户端;

9.之后的所有的认证报文都继续上面的过程, 当设备radius接收到认证服务器的回应, 就会relay转化为EAPOL-Request报文发送给客户端, 同时等待客户端的相应; 此时如果接收到客户端的EAPOL-Response报文, 则802.1x通过relay处理后通过radius模块发送认证报文给认证服务器;

10.在进行802.1x的调试信息分析的时候可以关注“Port:WLAN-DBSS1:27, Auth:164”两个信息, 根据端口号和Auth的编号可以和具体的一个用户产生对应关系; 而在radius报文中可能会携带无线客户端的MAC地址, 有可能更方便的分析报文;

11.当Radius模块完成无线客户端的认证之后, 会通知802.1x认证成功并将radius key传递给802.1x模块。“WX3010E 8021X/7/EVENT: Port:WLAN-DBSS1:2,Auth:36,Received Msg:0x104,Msg: Auth request ack for succeed, ACM->1X., Current state:14 ”调试信息表明802.1x已经接收到认证成功消息, 之后的调试信息会给出一些该用户的授权信息 (例如VLAN或者User profile) ;

12.WLAN模块成功接收到端口安全 (802.1x认证成功以后会通知WLAN) 的密钥协商触发消息WLAN/7/EVENT : 11Key trigger event received from PORTSEC”之后开始进行4-way handshake协商过程;

4-way handshake协商过程如下:

```
WX3010E PORTSEC/7/Event: Port:WLAN-DBSS1:2,PORTSEC EAPOL-Key Send Mbuf to Ethernet Success.
```

```
WX3010E WMAC/7/EVENT : Sent 4-way handshake message1 to station 6c88-1459-898c
```

```
WX3010E WMAC/7/EVENT : 4-way handshake FSM changes state, idle -> ptkstart for client 6c88-1459-898c
```

```
WX3010E 8021X/7/PACKET: Port:WLAN-DBSS1:2,Received an EAPOL packet.
```

```
WX3010E 8021X/7/PACKET: Port:WLAN-DBSS1:2,Received Packet Type: EAPOL-KEY.
```

```
WX3010E 8021X/7/EVENT: Port:WLAN-DBSS1:2, Send key packet to WLAN.
```

```
WX3010E WMAC/7/EVENT : Received valid 4-way handshake message2 from client 6c88-1459-898c
```

```
WX3010E PORTSEC/7/Event: Port:WLAN-DBSS1:2,PORTSEC EAPOL-Key Send Mbuf to Ethernet Success.
```

```
WX3010E WMAC/7/EVENT : Sent 4-way handshake message3 to station 6c88-1459-898c successfully
```

```
WX3010E WMAC/7/EVENT : 4-way handshake FSM changes state, ptkstart -> ptkinitnegotiating for client 6c88-1459-898c
```

```
WX3010E WMAC/7/EVENT : Received EAPOL-KEY frame from client 6c88-1459-898c is successfully handled
```

13.“WLAN/7/EVENT : Sent 4-way handshake message1 to station 6c88-1459-898c successfully”调试信息表明WLAN已经向无线客户端发送了第一个协商报文, 如果没有接收到回应的第二个协商报文, WLAN会定时进行重传, 相关的调试信息为“WLAN/7/EVENT : 4-way handshake message resend timer expired for client 6c88-1459-898c”;

14.WLAN之后会和无线客户端进行一系列的key协商, 当Key协商成功以后会通知802.1x和端口安全“8021X/7/EVENT: Port:WLAN-DBSS1:2,Auth:36,DOT1X Auth SuccessTrans Received an 11key succe

ss msg.”;

15.WMAC会再次从端口安全接收到整个认证彻底成功的消息（11key协商实际上是端口安全的802.1x认证的一部分），“WMAC/7/EVENT : WMAC/7/EVENT : Authorization event received from PORTSEC.”；稍后，WMAC会下发该无线客户端相关的各种信息“WX3010E WMAC/7/EVENT : RT backup sta when sta up or GTK/PTK update.

WX3010E WMAC/7/EVENT : Add mobile (6c88-1459-898c) sent”;

16.说明：如果在802.1x认证过程出现了任何的失败，802.1x模块会向无线客户端发送一个EAPOL-Failure报文，该报文最典型的调试信息“8021X/7/EVENT:Auth:3422,Sending EAPoL-Failure”;