某局点使用iNode结合锐捷交换机（等第三方）802.1x认证提示用户不存在的原因分析

寻尚岩 2017-08-14 发表

现场使用iNode结合锐捷交换机做802.1x认证，终端使用静态IP地址，勾选了上传客户端版本号和IP地址两个选项，服务器使用EIA。用户认证时提示用户名为空或者用户不存在或者没有申请该服务。

用户认证时提示用户不存在或者没有申请该服务。

分析服务器UAM调试日志，发现Radius报文里面User-Name为空，如下图所示，所以用户认证时会提示用户不存在。

CODE = 1.

ID = 109.

ATTRIBUTES:

User-Name(1) = "..".

Service-Type(6) = 2.

Framed-MTU(12) = 1500.

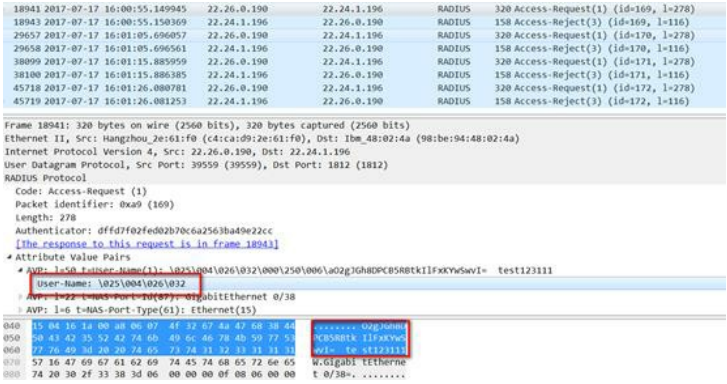
EAP-Message(79) = "0202002904107a641759202816286f66b03f37153b237a68616e676a696e6775616e5f776c406f7072".

Message-Authenticator(80) = "9fd0dd61cc66689a282c6329429921e6".

Attribute (0-102) is not defined in dic file r2.

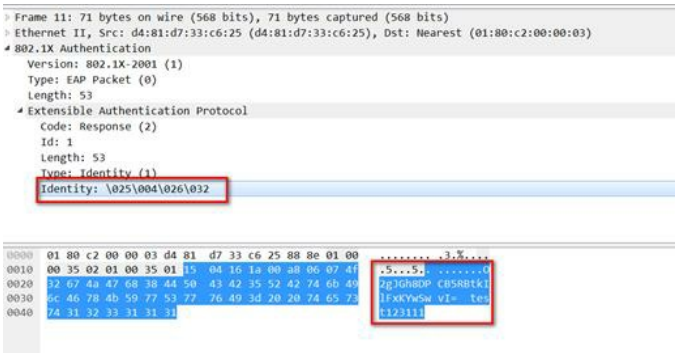
NAS-Port-Type(61) = 15.

继续分析服务器抓包，发现接入设备传过来的user-name里面是有值的，具体值为：15 04 16 1a 00 a8 06.....，UAM发现该字节流里面有00,00在编程语言表示结束的意思，所以UAM会截取15 04 16 1a为用户名，而15 04 16 1a为不可见字符，所以最终UAM提示用户名为空。



现场接入设备是第三方设备，配置的EAP模式，EAP模式下设备仅仅透传客户端的认证报文，所以该字节流应该是客户端传过来的。

分析客户端侧抓包，发现客户端封装的EAP报文的identity字段就是以15 04开头的，所以可以明确原始报文是iNode生成的。iNode在填充identity字段时为何不直接填充用户名而是要以15 04开头呢，这是因为为了实现我司的一些私有功能而设置的特殊标识，目的就是告诉交换机后面紧跟的一些字节是iNode上传的一些用户属性。比如以15 04开头时就表示后面紧跟的4字节是用户IP地址；以06 07开头时表示后面紧跟的30字节是客户端版本号，设备发现以1504开头或者0607开头就知道后面紧跟的是IP地址和客户端版本号了，同时交换机会提取出相关属性后重新封装到Radius报文转给UAM，而现场的第三方交换机不识别该标识，所以把EAP报文整体传给了UAM，最终导致出问题。



为了进一步确认问题，再看iNode封装的报文顺序，发现data部分是按照IP地址、客户端版本号、账号名的顺序封装的。IP地址以15 04开头，后面的16 1a 00 a8就是22.26.0.168.再往后是0607,0607后面的4f开头的就是客户端版本号。

Code (1): Response ---- 02

Id (1): 1 ---- 01

Length (2): 53 ---- 00 35
Data Type (1): ID ---- 01
IPv4 (4): 22.26.0.168
CliVer (30):
4f 32 67 4a 47 68 38 44 50 43 42 35 52 42 74 6b
49 6c 46 78 4b 59 77 53 77 76 49 3d 20 20
O2gJGh8DPCB5RBtkIlFxKYwSwvI=
Username (10):
74 65 73 74 31 32 33 31 31 31
test123111

iNode去勾选“上传IP地址”；
更换我司交换机；
终端侧IP地址不要包含0段。
以上三选一即可

1504后面的4个字节标识ip地址；0607（0608是针对域账号）后面的30个字节是客户端版本号。