某局点Portal对接失败问题经验案例

Portal wlan接入 樊昊 2015-07-29 发表

某客户反馈与我司进行Portal对接开发，发送REQ_CHALLENGE报文我司设备无响应，超时。

通过一线反馈现场AC在设置正确的情况下，第三方平台开发人员与我司设备对接，发送Portal一号报文发送至我司设备无响应。

查看AC配置：

```
#
radius scheme h3cimc
 server-type extended
 primary authentication 192.168.0.161
 primary accounting 192.168.0.161
 user-name-format without-domain
 nas-ip 192.168.0.151
 accounting-on enable
#
domain system
 authentication portal radius-scheme h3cimc
 authorization portal radius-scheme h3cimc
 accounting portal radius-scheme h3cimc
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
#
 portal server CESHI ip 10.63.101.20 url http://10.63.101.20:8088/wifi/login server-type cmcc
 portal free-rule 1 source ip any destination ip 10.65.1.1 mask 255.255.255.255
 portal free-rule 2 source ip any destination ip 10.65.50.1 mask 255.255.255.255
 portal free-rule 3 source ip any destination ip 192.168.0.0 mask 255.255.255.0
 portal free-rule 4 source ip any destination ip 219.235.1.2 mask 255.255.255.255
 portal free-rule 5 source ip 10.63.101.20 mask 255.255.255.255 destination ip any
 portal mac-trigger server ip 192.168.0.161
 portal url-param include user-mac
 portal url-param include nas-ip
 portal url-param include ap-mac
 portal url-param include user-url
 portal url-param include user-ip
 portal url-param include ac-name
#
```

配置正常，且该AC是从正常使用环境中取出进行开发对接的，之前搭配IMC工作正常，且切换后修改了Portal 服务器类型为CMCC，故排除配置问题。

开启debug信息，

```
debugging portal packet interface xxx
debugging portal error
debugging portal tcp-cheat
```

debugging portal acl interface xxx

debugging radius packet

根据输出：

IfName=Vlan-interface55, PortName=WLAN-DBSS0:60, SrcIP=10.63.55.120, DstIP=123.125.125.86, Flow=-1415335965!

*Jun 30 17:30:50:897 2015 XXJS-AC PORTAL/7/PORTAL_DEBUG: Mac trigger permit HTTP-Redirect MAC:9C4E-3672-8A70, IP:0xa3f3778.

*Jun 30 17:30:50:898 2015 XXJS-AC TCPCHEAT/7/TCPCHEAT_DEBUG: Source MAC = 9c4e-3672-8a70 VLAN = 55

45 00 00 34 7e a1 40 00 40 06 81 98 0a 3f 37 78

7b 7d 7d 56 dd 79 00 50 fd 56 11 9c 00 00 00 00

80 02 20 00 27 cf 00 00 02 04 05 b4 01 03 03 02

01 01 04 02

*Jun 30 17:30:50:898 2015 XXJS-AC TCPCHEAT/7/TCPCHEAT_DEBUG: A connection of 10.63.55.120 added!

*Jun 30 17:30:50:898 2015 XXJS-AC TCPCHEAT/7/TCPCHEAT_DEBUG: State of connection with source IP 10.63.55.120 is LISTEN!

*Jun 30 17:30:50:898 2015 XXJS-AC DPPORTAL/7/DP_PORTAL_DEBUG:

Info: Find the freerule result (1)

*Jun 30 17:30:50:898 2015 XXJS-AC TCPCHEAT/7/TCPCHEAT_DEBUG: State of connection with source IP 10.63.55.120 changed from LISTEN to SYN_RECVD!

*Jun 30 17:30:50:899 2015 XXJS-AC DPPORTAL/7/DP_PORTAL_DEBUG:

Matched Redirect ACL.

IfName=Vlan-interface55, PortName=WLAN-DBSS0:60, SrcIP=10.63.55.120, DstIP=123.125.125.86, Flow=-1415335965!

*Jun 30 17:30:50:899 2015 XXJS-AC PORTAL/7/PORTAL_DEBUG: Mac trigger permit HTTP-Redirect MAC:9C4E-3672-8A70, IP:0xa3f3778.

*Jun 30 17:30:50:899 2015 XXJS-AC DPPORTAL/7/DP_PORTAL_DEBUG:

Matched Redirect ACL.

IfName=Vlan-interface55, PortName=WLAN-DBSS0:60, SrcIP=10.63.55.120, DstIP=123.125.125.86, Flow=-1415335965!

*Jun 30 17:30:50:899 2015 XXJS-AC PORTAL/7/PORTAL_DEBUG: Mac trigger permit HTTP-Redirect MAC:9C4E-3672-8A70, IP:0xa3f3778.

*Jun 30 17:30:50:900 2015 XXJS-AC TCPCHEAT/7/TCPCHEAT_DEBUG: Source MAC = 9c4e-3672-8a70 VLAN = 55

45 00 00 28 7e a2 40 00 40 06 81 a3 0a 3f 37 78

7b 7d 7d 56 dd 79 00 50 fd 56 11 9d 30 73 b3 0b

50 10 fb 90 a9 7c 00 00

*Jun 30 17:30:50:900 2015 XXJS-AC TCPCHEAT/7/TCPCHEAT_DEBUG: State of connection with source IP 10.63.55.120 is SYN_RECVD!

*Jun 30 17:30:50:900 2015 XXJS-AC TCPCHEAT/7/TCPCHEAT_DEBUG: State of connection with source IP 10.63.55.120 changed from SYN_RECVD to ESTABLISHED!

*Jun 30 17:30:50:900 2015 XXJS-AC TCPCHEAT/7/TCPCHEAT_DEBUG: State of connection with source IP 10.63.55.120 is ESTABLISHED!

*Jun 30 17:30:50:901 2015 XXJS-AC TCPCHEAT/7/TCPCHEAT_DEBUG: Source MAC = 9c4e-3672-8a70 VLAN = 55

该终端（MAC:9C4E-3672-8A70，IP:10.63.55.120）,关联上AP之后，AC mac-trigger功能对其进行放行，当流量触发阈值之后成功发起重定向，将终端请求重定向至第三方Portal 服务器。根据第三方Port

al后台确认，设备确实重定向到了设备，Portal服务器也收到了重定向的页面请求，Portal服务器在获取到页面的账号密码之后向设备发起认证请求出现问题，遂协调平台方抓包排查。

420	3.60297000	10.63.55.120	10.63.101.20	TCP	66 56654 > radan-http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
421	3.60304800	10.63.101.20	10.63.55.120	TCP	66 radan-http > 56654 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=
422	3.60466600	10.63.55.120	10.63.101.20	TCP	60 56654 > radan-http [ACK] Seq=1 Ack=1 Win=65700 Len=0
423	3.60593100	10.63.55.120	10.63.101.20	HTTP	992 POST /wifi/login HTTP/1.1 (application/x-www-form-urlencoded)
424	3.61333800	10.63.101.20	192.168.0.151	PORTAL	58 Portal type REQ_CHALLENGE
425	3.61403700	192.168.0.151	10.63.101.20	PORTAL	60 Portal type ACK_CHALLENGE
426	3.63617400	10.63.101.20	10.63.55.120	TCP	285 [TCP segment of a reassembled PDU]

抓包可以看出Portal服务器发起了REQ_CHANLLAGE报文，按照《中国移动WLAN业务PORTAL协议规范》中的报文类型表：

Type	值	方向	含义
REQ_CHALLENGE	0x01	Client----->服务器	Portal 服务器 向AC设备发送的请求Challenge报文
ACK_CHALLENGE	0x02	Client<-----服务器	AC设备对Portal 服务器请求Challenge报文的响应报文
REQ_AUTH	0x03	Client----->服务器	Portal 服务器向AC设备发送的请求认证报文
ACK_AUTH	0x04	Client<-----服务器	AC设备对Portal 服务器请求认证报文的响应报文
REQ_LOGOUT	0x05	Client----->服务器	若ErrCode字段值为0x00，表示此报文是Portal 服务器向AC设备发送的请求用户下线报文；若ErrCode字段值为0x01，表示该报文是Portal 服务器发送的超时报文，其原因是Portal 服务器发出的各种请求在规定时间内没有收到响应报文。
ACK_LOGOUT	0x06	Client<-----服务器	AC设备对Portal 服务器请求下线报文的响应报文
AFF_ACK_AUTH	0x07	Client----->服务器	Portal 服务器对收到的认证成功响应报文的确认报文；
NTF_LOGOUT	0x08	服务器 --> Client	用户被强制下线通知报文
REQ_INFO	0x09	Client --> 服务器	信息询问报文
ACK_INFO	0x0a	服务器 --> Client	信息询问的应答报文
REQ_CHALLENGE	0x01	Client----->服务器	Portal 服务器 向AC设备发送的请求Challenge报文
ACK_CHALLENGE	0x02	Client<-----服务器	AC设备对Portal 服务器请求Challenge报文的响应报文
REQ_AUTH	0x03	Client----->服务器	Portal 服务器向AC设备发送的请求认证报文
ACK_AUTH	0x04	Client<-----服务器	AC设备对Portal 服务器请求认证报文的响应报文

可以看到Portal 服务器发送的报文中User IP字段未填入有效内容，全为0，但是实际该值我们设备已经通过重定向URL上报给了服务器（配置中有portal url-param include user-ip）。下面是该字段的详细说明：

UserIP

UserIP字段为Portal用户的IP地址，长度为 4 字节，其值由Portal 服务器根据其获得的IP地址填写，在所有的报文中此字段都要有具体的值；

UserPort:

UserPort字段目前没有用到，长度为 2 字节，在所有报文中其值为0；

故AC回复的报文为：

```
] User Datagram Protocol, Src Port: cisco-sccp (2000)
    Source port: cisco-sccp (2000)
    Destination port: 6576 (6576)
    Length: 24
  ⊞ Checksum: 0x2b96 [validation disabled]
] PORTAL Protocol
    VERSION: 1
    Type: ACK_CHALLENGE (0x02)
    Pap/Chap: 0x00
    Reserve: 0
    Serial Number: 32787
    Reqest ID: 0
    User IP: 0.0.0.0 (0.0.0.0)
    User Port: 0
    Error Code: 0x01
    Attribute Number: 0x00
```

ErrorCode为1，表示AC设备告诉Portal 服务器请求Challenge被拒绝，AC拒绝是合理的。协调Portal服务器开发人员修改。此次回复正常。

```
⊟ PORTAL Protocol
    VERSION: 1
    Type: ACK_CHALLENGE (0x02)
    Pap/Chap: 0x00
    Reserve: 0
    Serial Number: 32775
    Reqest ID: 8685
    User IP: 10.63.55.120 (10.63.55.120)
    User Port: 0
    Error Code: 0x00
    Attribute Number: 0x01
  ⊟ Attribute: Challenge
      Type: Challenge (0x03)
      Length: 18
      Value: \002⊠x|\033x⊠⊠⊠s⊠\a⊠⊠\003\206
```

但在3号报文REQ_AUTH又出现问题。

根据抓包：

```
⊟ PORTAL Protocol
    VERSION: 1
    Type: REQ_AUTH (0x03)
    Pap/Chap: 0x00
    Reserve: 0
    Serial Number: 32776
    Reqest ID: 8685
    User IP: 10.63.55.120 (10.63.55.120)
    User Port: 0
    Error Code: 0x00
    Attribute Number: 0x02
  ⊟ Attribute: UserName
      Type: UserName (0x01)
      Length: 7
      Value: admin
  ⊟ Attribute: ChapPassword
      Type: ChapPassword (0x04)
      Length: 18
      Value: ⊠\f⊠\224⊠⊠⊠\017⊠⊠⊠⊠\006
```

遂对照协议，发现该报文问题错在长度不对。

协议中要求

Attr(属性字段)	AttrType	属性值长度	属性含义
UserName	0x01	<=253 （可变）	随e行用户名，具体为：“用户手机号码”； 全国/省内预付费卡用户名称：13位数字； 为满足国际漫游的需要，支持253字节的长用户名。
PassWord	0x02	<=16（可变）	用户提交的明文密码
Challenge	0x03	16（固定）	Chap方式加密的魔术字
ChapPassWord	0x04	16（固定）	经过Chap方式加密后的密码

按照上面表格可以发现ChapPassword字段（0X04）长度应该为固定的16位，而第三方Portal服务器发送的报文该字段长度为18，不符合要求，遂与服务器方确认，该处错误是由于服务器在计算CHAPPASSWORD时，算出的值采用了整型保存，在封装协议时转为字符串型，转换之后出现异常，导致该字段长度变长，且数值错误。安排Portol服务器方修改，修改后，交互正常，终端能够上线，计费正常。

填充1号报文中的User IP字段为正确值；

3号报文中的ChapPassWord保证字段填充正确，长度为固定的16位。