S5120交换机与NPS服务器配合做802.1x认证失败问题

802.1X Radius 孔天娇 2014-10-22 发表

某客户使用我司交换机S5120结合NPS服务器做802.1x认证，客户发现如果在NPS服务器上配置vlan下发，可以认证成功；取消vlan下发，则不能认证成功。

收集认证失败的debug信息

Debug dot1x all

Debug sc all

Debug radius packet

分析认证报文交互过程

*Sep 1 05:33:12:177 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:Receive:IP=[10.1.5.248],Code=[2],Length=[368]

*Sep 1 05:33:12:179 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:

[8 Framed-Address] [6] [255.255.255.255]

[7 Framed-Protocol] [6] [1]

[6 Service-Type] [6] [2]

[65 Tunnel-Medium-Type] [6] [6]

[64 Tunnel-Type] [6] [13]

[79 EAP-Message] [6] [030C0004]

*Sep 1 05:33:12:180 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:

[25 Class] [46] [691306FD0000013700010200 0A0105F80000000000000000000000001CFC2F350F8FEBF000000000000002F]

[MS-26 MS-CHAP2-Success] [45] [01533D3239393346453531423545374434413931443236353946414343364136303941463636463144142]

[MS-17 MS-MPPE-Recv-Key] [52] [8008D75718C4F3EC4A03C74E2663928FFCF26C04AB299384AC5255C60D88CBF39F1EFAEE97D12AF784ADAD0CD3BFB084F407]

[80 Message-Autheticator] [18] [431E003DC6A4239F561D6FB5E9F80669]

*Sep 1 05:33:12:182 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:Info: RD received MS-CHAP2-Success

*Sep 1 05:33:12:183 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:Info: RD received radius key, Decrypt user Authenticator is:

*Sep 1 05:33:12:184 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:

2a 19 00 00 59 00 00 00 5a 75 00 00 58 15 00 00

*Sep 1 05:33:12:185 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:Info: Decrypt MS-MPPE-Recv-Key with radius authen authenticator is:

*Sep 1 05:33:12:187 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:

20 75 0e c6 84 dc ee 79 20 40 d0 6d 0b 7b 70 e3

03 7d 7e 2b 3c 83 03 f9 34 19 46 8e 32 da 9b 54

1e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

*Sep 1 05:33:12:188 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:Reject, Message=[Vlan value that the server assigns is invalid!]

*Sep 1 05:33:12:189 2014 H3C5120-G5/5F-A1 8021X/7/EVENT:Auth:481,Msg: Auth request ack for failure, ACM->1X.

*Sep 1 05:33:12:190 2014 H3C5120-G5/5F-A1 8021X/7/EVENT:Port:GigabitEthernet1/0/26,Auth:481,Received Msg:261, Current state:14

*Sep 1 05:33:12:192 2014 H3C5120-G5/5F-A1 8021X/7/EVENT:Auth:481,Processing node FAILURE...

从以上radius报文交互过程可以看到设备从NPS服务器侧收到认证响应报文，设备拒绝该报文，因为服务器分配的vlan id无效。怀疑是服务器和设备的配合问题。对比取消下发vlan和下发vlan服务器的响应报文：

取消vlan下发：

*Sep 1 05:33:12:177 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:Receive:IP=[10.1.5.248],Code=[2],Length=[368]

*Sep 1 05:33:12:179 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:

[8 Framed-Address] [6] [255.255.255.255]

[7 Framed-Protocol] [6] [1]

[6 Service-Type] [6] [2]

[65 Tunnel-Medium-Type] [6] [6]

[64 Tunnel-Type] [6] [13]

[79 EAP-Message] [6] [030C0004]

*Sep 1 05:33:12:180 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:

[25 Class] [46] [691306FD000001370001020000A0105F80000000000000000000000001CFC2F350F8FEBF000000000000002F]

[MS-26 MS-CHAP2-Success] [45] [01533D32393933464535314235453744344139314432363539464143433641363039414636364631444142]

[MS-17 MS-MPPE-Recv-Key] [52] [8008D75718C4F3EC4A03C74E2663928FFCF26C04AB299384AC5255C60D88CBF39F1EFAEE97D12AF784ADAD0CD3BFB084F407]

[80 Message-Autheticator] [18] [431E003DC6A4239F561D6FB5E9F80669]

Vlan下发:

*Sep 1 05:37:53:635 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:

[64 Tunnel-Type] [6] [13]

[65 Tunnel-Medium-Type] [6] [6]

[81 Tunnel_Private_Group_ID] [4] [3135]

[1 User-name] [46] [host/Laptop-G56.resourcepro0.resourcepro.com]

[32 NAS-Identifier] [18] [H3C5120-G5/5F-A1]

[5 NAS-Port] [6] [16883727]

*Sep 1 05:37:53:636 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:

[61 NAS-Port-Type] [6] [15]

[31 Caller-ID] [16] [373834352D633463352D30366462]

[40 Acct-Status-Type] [6] [1]

[45 Acct-Authentic] [6] [1]

[44 Acct-Session-Id] [15] [1140801053720]

[4 NAS-IP-Address] [6] [10.1.5.131]

*Sep 1 05:37:53:637 2014 H3C5120-G5/5F-A1 RDS/7/DEBUG:

[55 Event-Timestamp] [6] [1409549873]

[25 Class] [46] [693B0725000001370001020000A0105F80000000000000000000000001CFC2F350F8FEBF0000000000000057]

查看服务器应答报文携带的属性发现虽然取消了vlan数值下发（81号属性），但在设备侧还是收到vlan下发属性（64、65号属性），但是这个值为空，导致设备无法识别。报Vlan value that the server assigns is invalid!

不下发vlan的情况下可以在服务器侧取消64、65、81属性下发。

[65 Tunnel-Medium-Type] [6] [6]

[81 Tunnel_Private_Group_ID] [4] [3135]

[64 Tunnel-Type] [6] [13]

取消64、65、81号属性下发。