S1850 802.1x 重复认证，等待重连

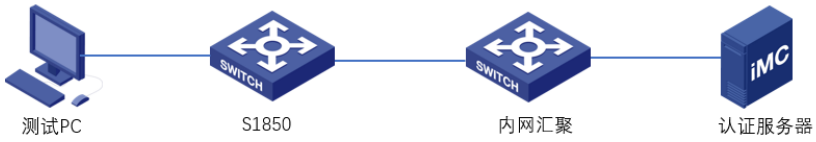
802.1X　李发展1　2022-11-30 发表

组网及说明

设备型号：H3C S1850-52P

设备版本：Version 5.20.99, Release 1102

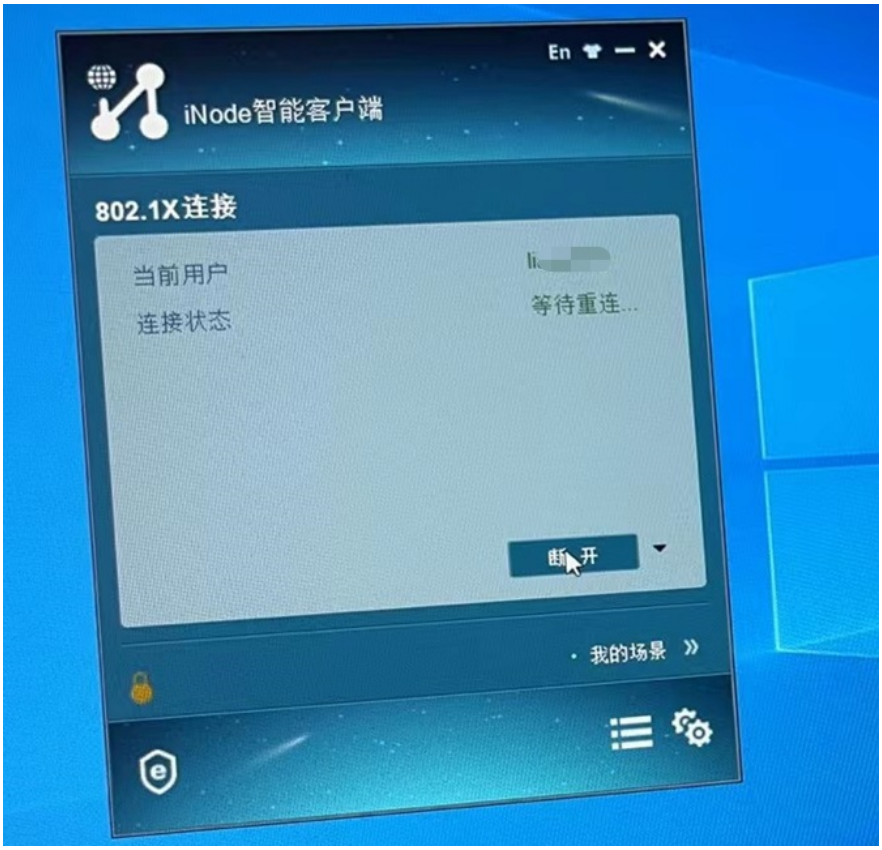
组网如下：

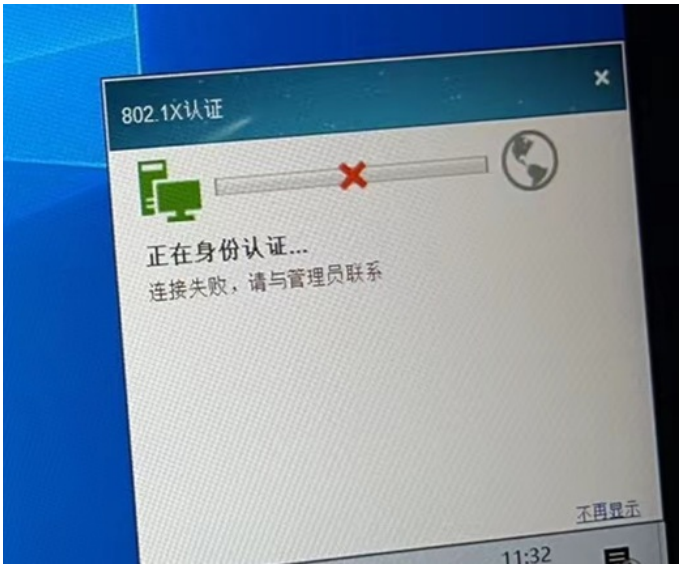


测试PC　S1850　内网汇聚　认证服务器

问题描述

现场终端进行1x认证，发现1x等待重连，最后提示“连接失败，请于管理员联系”





过程分析

1.排查配置发现无问题

#

radius scheme pd

primary authentication 172.16.20.240 key cipher c3$n8qzDyWpUIPDCPkXtkvetv74l/BrHA==

primary accounting 172.16.20.240 key cipher c3$1vqKY7buBmVCiPwx8k14Txg4Q/GJhw==

key authentication cipher c3$yaGOWMPtsdnewho4A1y8L/D+g9vnpg==

key accounting cipher c3$xW0sbNMIhC99nmBsLsQH9PU4OdAo9A==

user-name-format without-domain

nas-ip 172.16.98.131

#

domain pd

 authentication lan-access radius-scheme pd

 authorization lan-access radius-scheme pd

 accounting lan-access radius-scheme pd

2.让现场从新配置1850和IMC上radius的认证和计费密码

3.从debug dot1x all、debugging radius packet来看出现很多计费无响应报文。

（RADIUS计费开始报文中CODE值为4，计费结束报文中CODE值为5。）

[11:30:01]*Nov 11 11:30:00:322 2022 13-1 RDS/7/DEBUG: Recv MSG,[MsgType=PKT acct_timeout Index = 1048, ulParam3=0]

[11:30:01]*Nov 11 11:30:00:322 2022 13-1 RDS/7/DEBUG: [11:30:01]Error: **Accounting server no response.**(AAAID = 1048, Req-ID = 0)

[11:30:01]*Nov 11 11:30:00:323 2022 13-1 RDS/7/DEBUG: Recv MSG,[MsgType=Account off request Index = 1048, ulParam3=0]

[11:30:01]*Nov 11 11:30:00:324 2022 13-1 RDS/7/DEBUG: Send: IP=[172.16.20.240], UserIndex=[1048], ID=[66], RetryTimes=[0], **Code=[4]**, Length=[226]

[11:30:01]*Nov 11 11:30:00:324 2022 13-1 RDS/7/DEBUG: [11:30:01]Event: Set socket VPN attribute, VPN index=0, Result=0!

[11:30:01]*Nov 11 11:30:00:325 2022 13-1 RDS/7/DEBUG: Send bufferred acct-stop packet.The Raw Packet is: [11:30:01]*Nov 11 11:30:00:325 2022 13-1 RDS/7/DEBUG:

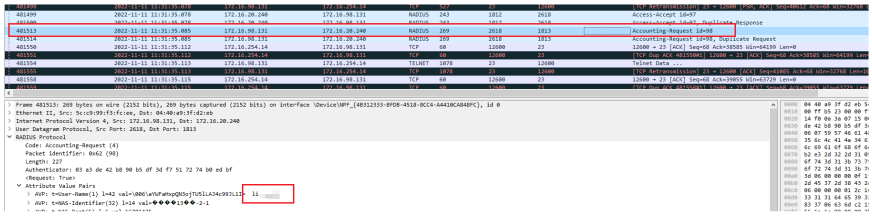
从debug中可以分析出，设备已经发出了计费报文。但是未收到回复报文。

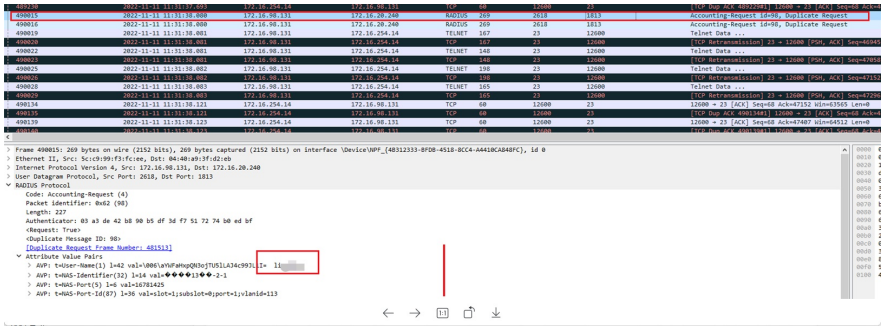
4.在内网汇聚上抓包也可以看到：

NO. 481513 是有抓到accept后的开始计费报文请求的， 但服务器未回应答

NO.490015 设备重传计费报文，仍未收到应答

以此可以得出S1850设备上是没有问题的，内网汇聚也没有问题 ，需要排查imc侧是否有问题。



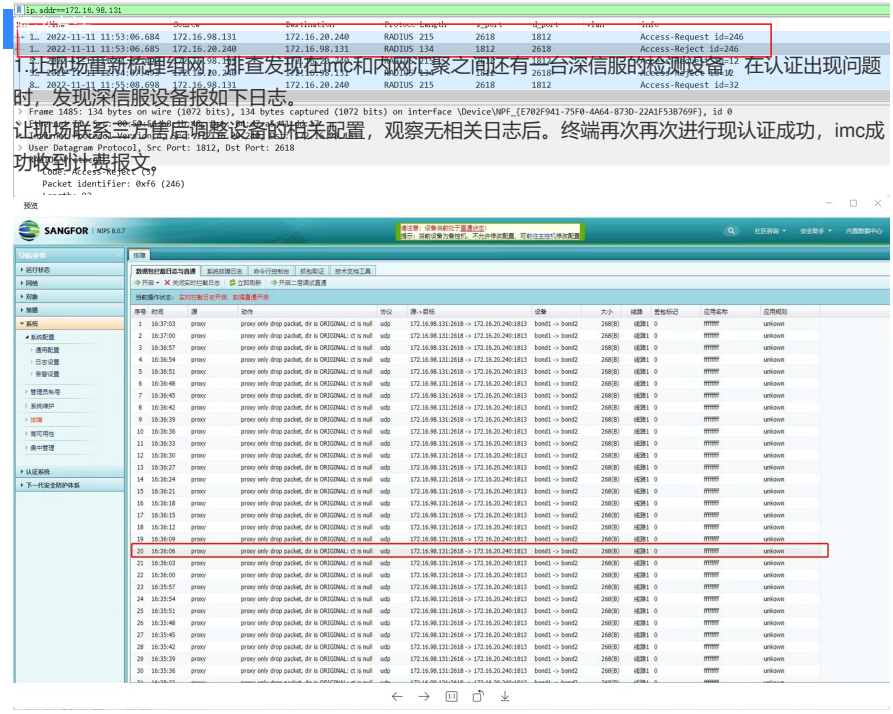


5.联系imc侧发现1x有请求报文，但是报文回应时被拒绝。排查配置发现接口配置1x认证和mac认证。原因就是1x认证成功之后设备又发送了mac认证请求 然后Mac认证的话对应的mac在imc上又没有配置哑终端用户，所以有reject报文。

在端口及配置了1x又配置了mac时：

802.1X认证优先于MAC认证。端口上同时仅使能了802.1X和MAC地址认证的情况下，首次接入的802.1X用户将直接进行802.1X认证，非802.1X用户的报文将在30秒之后触发MAC地址认证。802.1X认证

失败后可以通过MAC认证上线，所以该现象是正常现象。



1.让现场重新梳理组网，排查发现在ac和内网汇聚之间还有一台深信服的检测设备，在认证出现问题时，发现深信服设备报如下日志。

让现场联系工程师配置调整设备的相关配置，观察无相关日志后。终端再次再次进行现认证成功，imc成功收到计费报文。

2.如果客户不进行radius计费，可以把计费配置关闭掉测试，测试发现，终端也可以认证成功。

配置如下：

domain pd

authentication lan-access radius-scheme pd

authorization lan-access radius-scheme pd

accounting lan-access none