

知 S1850 802.1x 重复认证, 等待重连

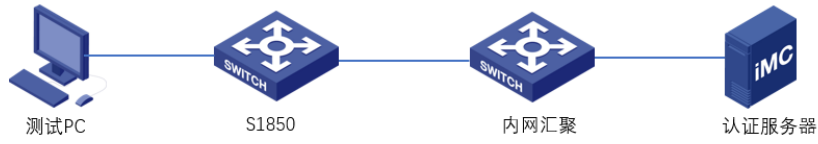
802.1X 李发展1 2022-11-30 发表

组网及说明

设备型号: H3C S1850-52P

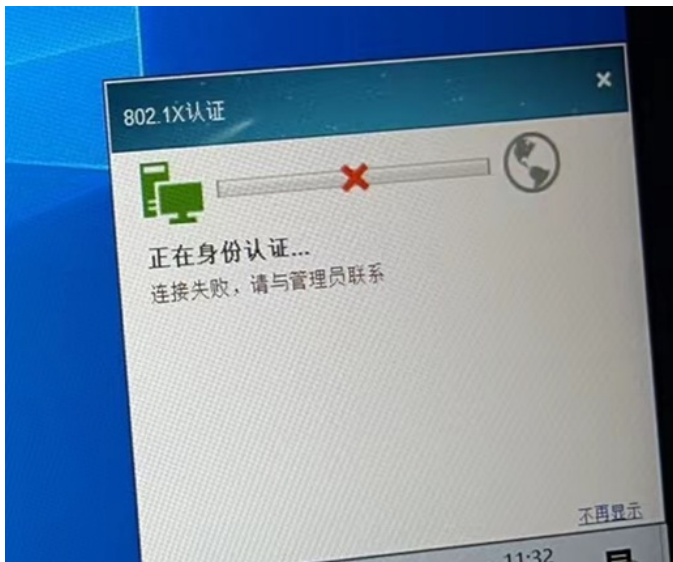
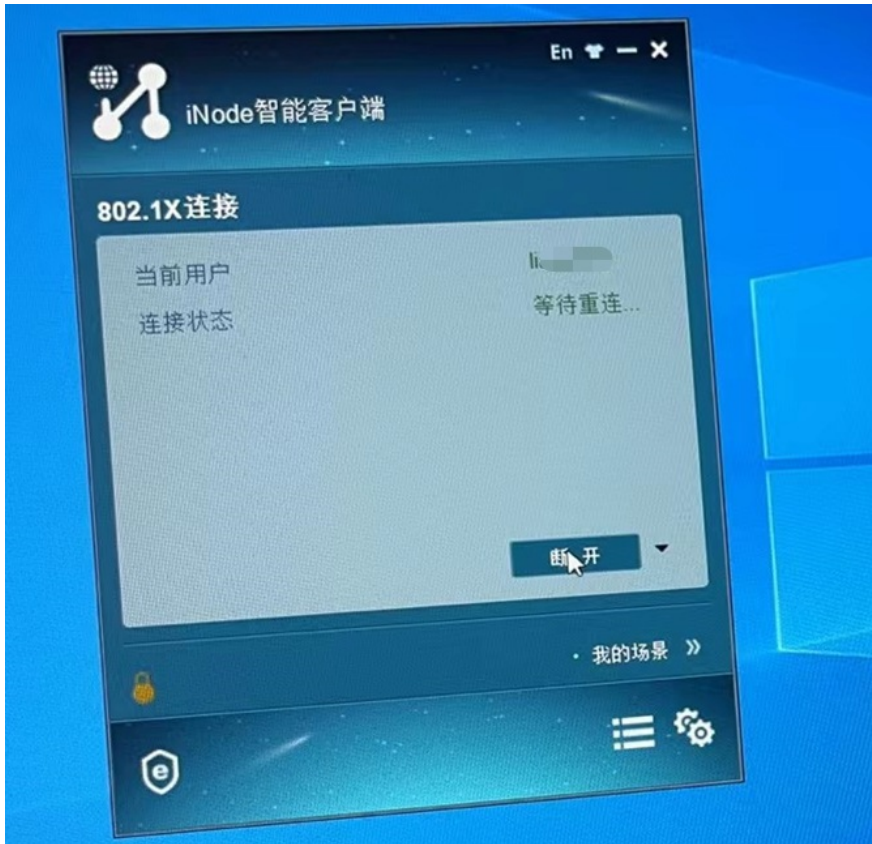
设备版本: Version 5.20.99, Release 1102

组网如下:



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 $c$3$n8qzDyWpUIPDCPkXtkvetv74l/BrHA==
primary accounting 172.16.20.240 key cipher $c$3$1vqKY7buBmVCiPwx8k14Txg4Q/GJhw==
key authentication cipher $c$3$yaGOWMPtsdnewho4A1y8L/D+g9vnpvg==
key accounting cipher $c$3$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 r
esponse.(AAAIID = 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 buffered acct-stop packet.The Ra
w 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。

The image displays two screenshots of network traffic analysis. The top screenshot shows a list of captured packets with details for packet 481513, which is an Accounting-Request (RADIUS) with Code 4. The bottom screenshot shows a list of captured packets with details for packet 490015, which is an Accounting-Request (RADIUS) with Code 4, identified as a duplicate request. Both screenshots include detailed protocol information such as Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and RADIUS Protocol, along with hex and ASCII data views.

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。

The image displays two screenshots from a network analysis tool. The top screenshot shows a packet capture for RADIUS traffic. A red box highlights the 'Access-Request id=246' and 'Access-Request id=32' entries. Below the capture, there is a text overlay in Chinese: '1.让现场重新梳理组网，排查发现在核心和内网汇聚之间还有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。让现场联系厂商调整设备的相关配置，观察无相关日志后。终端再次进行认证成功，imc成功收到计费报文。' The bottom screenshot shows the 'SANGFOR' configuration interface for RADIUS. A table lists various RADIUS services and their configurations.

序号	时间	源	动作	协议	源IP	源端口	设备	大小	结果	告警标记	应用名称	应用规则
1	16:37:03	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
2	16:37:00	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
3	16:36:57	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
4	16:36:54	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
5	16:36:51	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
6	16:36:48	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
7	16:36:45	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
8	16:36:42	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
9	16:36:39	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
10	16:36:36	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
11	16:36:33	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
12	16:36:30	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
13	16:36:27	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
14	16:36:24	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
15	16:36:21	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
16	16:36:18	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
17	16:36:15	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
18	16:36:12	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
19	16:36:09	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
20	16:36:06	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
21	16:36:03	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
22	16:36:00	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
23	16:35:57	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
24	16:35:54	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
25	16:35:51	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
26	16:35:48	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
27	16:35:45	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
28	16:35:42	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
29	16:35:39	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	
30	16:35:36	proxy	proxy only drop packet, dir is ORIGINAL: ct is null	udp	172.16.98.131	2618	bond2 -> bond2	260(0)	成功	0	unKnown	

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

