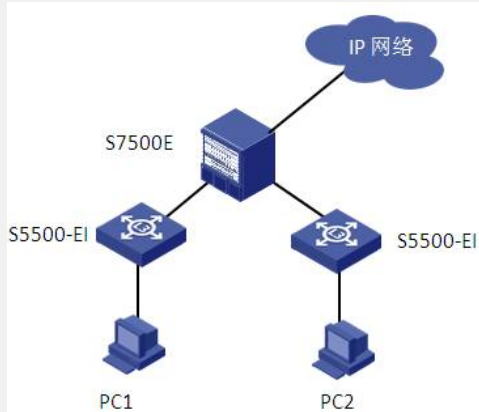


## 某局点S7500E Portal认证失败原因为Admin Reset故障处理案例分析

### 一、组网：



客户组网拓扑示意图如上，采用S7500E做核心网关，S5500-EI设备作为汇聚上行连接到S7500E的Slot 0槽位，在S7500E上做Portal认证。

PC上采用iNode作为Portal客户端，Portal服务器采用iMC。

### 二、问题描述：

客户反馈近期网络内随机出现部分用户无法认证的情况。iNode客户端提示“收到下线请求报文，用户离线”。有时候多次尝试之后又能认证成功。

### 三、过程分析：

首先在iMC侧查看认证失败用户的失败原因，发现失败原因都是“Admin reset”

用户详情			
基本信息			
帐号名	chengzq	用户名	程志清
昵称	非研发2600	用户分组	非研发
登录名	chengzq@sany		
接入信息			
接入开始时间	2012-06-05 11:11:34	接入结束时间	2012-06-05 11:11:42
接入时长	8	下线原因	Admin Reset
设备IP地址	10.11.35.254	设备端口号	5
设备槽号	0	设备子槽号	0
进入字节数	0	流出字节数	0
VLAN名称	VLAN ID	外层VLAN ID	0
无线用户SSID		认证方式	不使用混合组网
用户IP地址	10.11.35.157	用户MAC地址	00:16:41:2D:C0:A0
设备NAT IP地址	10.11.35.254		
绑定域		登录域	
代理类型	设备至本地	计费会话标识	112005510306187050

从这个下线原因来分析，此认证失败与portal设备相关。

紧接着在设备上开启debug对认证失败的用户认证过程进行跟踪，

Debug 信息里有下面的信息(这里跟踪的认证失败用户是chengzq@sany)

```
%Jun 5 10:38:37:685 2012 SYZJ-ZXJF-SW-S7510E-01 RDS/6/RDS_SUCC: -IfName=Vlan-interface35-VlanId=0-MACAddr=00:16:41:2D:C0:A0-IPAddr=10.11.35.157-IPv6Addr=N/A-UserName=chengzq@sany; User got online successfully.
```

// 这里说明用户认证通过。后续将进行ACL资源分配操作。

```
*Jun510:38:37:6872012SYZJ-ZXJF-SW-S7510E-01PORTAL/7/PORTAL_DEBUG: Processing NOTIFY user index 4509 IP 10.11.35.157, user's state is not WAIT_AUTHEN_ACK!
```

```
*Jun510:38:37:6872012SYZJ-ZXJF-SW-S7510E-01 PORTAL/7/PORTAL_DEBUG: Stop state timer: user index 4509 IP 10.11.35.157 state WAIT_LOGIN_ACK!
```

```
*Jun 5 10:38:37:687 2012 SYZJ-ZXJF-SW-S7510E-01 PORTAL/7/PORTAL_DEBUG: Processing LOGIN-ACK user 4509 IP 10.11.35.157 recv LOGIN-SUCC from ACM!!
```

```
*Jun 5 10:38:37:688 2012 SYZJ-ZXJF-SW-S7510E-01 PORTAL/7/PORTAL_DEBUG: State WAIT_LOGIN_ACK change to ONLINE,ID 4509 IP 10.11.35.157
```

\*Jun 5 10:38:44:802 2012 SYZJ-ZXJF-SW-S7510E-01 PORTAL/7/PORTAL\_DEBUG: Portal send packet length:82

Portal packet head:

SN:2307 Type:8 AttrNum:4 ErrCode:0 UserIP:10.11.35.157

Portal packet attribute list:

[ 10 BAS-IP ] [ 6 ] [10.11.35.254]

[ 11 Session-ID ] [ 8 ] [0016412dc0a0]

[ 5 TextInfo ] [ 30 ] [Send NTF\_LOGOUT when online!]

[ 38 DeviceStartTime ] [ 6 ] [1335981184]

Portal raw packet:

02 08 01 00 09 03 00 00 0a 0b 23 9d 00 00 00 04

5b 66 70 c7 12 cc d7 90 ee 8a ca d0 26 42 91 13

0a 06 0a 0b 23 fe 0b 08 00 16 41 2d c0 a0 05 1e

53 65 6e 64 20 4e 54 46 5f 4c 4f 47 4f 55 54 20

77 68 65 6e 20 6f 6e 6c 69 6e 65 21 26 06 4f a1

74 80

\*Jun 5 10:38:44:804 2012 SYZJ-ZXJF-SW-S7510E-01 PORTAL/7/PORTAL\_DEBUG: -Slot=0 ; Add ACL driver return:11

// 返回值11表示acl资源不足，这里在给用户申请ACL资源时，失败，返回错误。并最终导致了用户的下线。

最终结果导致用户以Admin reset下线。

[48 Acct-Output-Packets ] [6 ] [0]

[52 Acct\_Input\_Gigawords ] [6 ] [0]

[53 Acct\_Output\_Gigawords ] [6 ] [0]

[49 Terminate-Cause ] [6 ] [6]

//这里Terminate-Cause下线原因6表示Admin reset。

最终导致出现了客户网络中随机出现认证失败的情况。

另外从S7500E的日志里，也可以看到对应的Slot 0槽位ACL资源不足的信息

\*Jun 5 10:38:44:803 2012 SYZJ-ZXJF-SW-S7510E-01 PORTAL/5/PORTAL\_ACL\_FAILURE: -Slot=0; The number of ACLs on the device has reached the maximum.

// 这里报了Slot 0的ACL资源占用已经到达最大值。

从设备配置来看，设备上添加了很多portal free-rule以及安全和隔离ACL，这样会占用大量的ACL资源，确实容易导致出现ACL资源不足的情况。

#### 四、 解决方法：

对于此类情况，因为单板硬件ACL资源是固定的，只能考虑下面几种解决方案：

- 1) 优化设备配置，减少安全ACL、隔离ACL、Portal free-rule的数量；
- 2) 更换ACL规格更高的业务板或者新增业务板将认证用户均匀分布到多个业务单板上；
- 3) 对于此案例中的组网，因为S7500E下挂设备S5500-EI也支持portal认证，可以考虑将部分portal用户下移到S5500-EI设备上。