

# 知 S10508 Portal认证不成功经验案例

Portal 林洪宇 2017-08-24 发表

某局点交换机S10508配合我司IMC认证服务器和iNode客户端为接入用户终端提供Portal认证,需求: 用户在认证前通过DHCP直接获取一个IP地址, 可以访问Portal Web服务器, 以及设定部分免认证地址用户可以直接访问; 其余地址需要认证通过后才可访问网络资源。

当前局点Portal认证测试过程中, 发现终端无法正常成功认证, 故障现象是终端可以获取DHCP分配的地址, 可以访问Web服务器, 但是始终无法通过Portal认证, 无法访问网络资源。

查看设备相关配置:

```
radius scheme youxian  
primary authentication 192.168.180.200 1812
```

```
primary accounting 192.168.180.200 1813
```

```
key authentication simple youxian
```

```
key accounting simple youxian
```

```
user-name-format with-domain
```

```
nas-ip 192.168.216.254
```

```
domain youxian
```

```
authentication portal radius-scheme youxian
```

```
authorization portal radius-scheme youxian
```

```
accounting portal radius-scheme youxian
```

```
portal server youxian
```

```
ip 192.168.180.200 key simple youxian
```

```
portal web-server youxian
```

```
url http://192.168.180.200:8080/portal
```

```
interface Vlan-interface216
```

```
description iNode测试
```

```
ip address 192.168.216.254 255.255.255.0
```

```
dhcp select relay
```

```
dhcp relay server-address 192.1.1.240
```

```
dhcp relay server-address 192.1.1.244
```

```
portal enable method direct
```

```
portal bas-ip 192.168.216.254
```

```
portal apply web-server youxian
```

查看交换机配置, Portal和Radius相关配置完整。

根据认证过程整理分析:

客户端侧发起Portal认证, 认证不通过, 提示认证不成功报错, 从IMC认证服务器查看日志:

看认证不成功的原因是因为设备没有回应ack-auth报文:

```
device response time out, stop send packet to device success, device ip is 192.168.216.254
```

交换机S10508侧开启debug分析:

```
debug radius all
```

```
debug portal all
```

```
*Aug 24 10:30:57:992 2017 S105-IRF PORTAL/7/EVENT: -MDC=1; User-SM[192.168.216.12]: Notified Auth-SM to process the REQ_AUTH packet.
```

```
*Aug 24 10:30:57:992 2017 S105-IRF PORTAL/7/FSM: -MDC=1; Auth-SM: Started to run.
```

```
*Aug 24 10:30:57:992 2017 S105-IRF PORTAL/7/FSM: -MDC=1; Auth-SM [192.168.216.12]: Entered state Authenticating.
```

```
*Aug 24 10:30:57:995 2017 S105-IRF PORTAL/7/EVENT: -MDC=1; User-SM[192.168.216.12]: AAA processed authentication request and returned error.
```

```
*Aug 24 10:30:57:995 2017 S105-IRF PORTAL/7/EVENT: -MDC=1; User-SM[192.168.216.12]: Auth-SM logged out the user and notified User-SM to process.
```

```
*Aug 24 10:30:57:995 2017 S105-IRF PORTAL/7/FSM: -MDC=1; User-SM[192.168.216.12]: Begin to run.
```

\*Aug 24 10:30:57:995 2017 S105-IRF PORTAL/7/FSM: -MDC=1; User-SM [192.168.216.12]: State changed from Authenticating to Done.  
\*Aug 24 10:30:57:996 2017 S105-IRF PORTAL/7/FSM: -MDC=1; User-SM[192.168.216.12]: User was destroyed.  
\*Aug 24 10:30:57:997 2017 S105-IRF PORTAL/7/EVENT: -MDC=1; User-SM[192.168.216.12]: Added ARP rule.  
\*Aug 24 10:30:57:997 2017 S105-IRF PORTAL/7/EVENT: -MDC=1; User-SM[192.168.216.12]: Notified User-Detect-SM to stop detection.

从debug信息可以看到

AAA processed authentication request and returned error

终端用户进行AAA认证请求失败，导致认证不成功。

通过打印的Portal报文查看：

Portal received 152 bytes of packet: Type=req\_auth(3), ErrCode=0, IP=192.168.216.12

```
*Aug 24 10:30:57:992 2017 S105-IRF PORTAL/7/PACKET: -MDC=1;
[ 1 USERNAME      ][ 46] [aWwNHBkHOnlrQBljLIV1e4QS5jk= test1@portal]
[ 4 CHAPPWD       ][ 18] [cde737f65b1f0d5d1ef066dc3faa5dd8]
[ 3 CHALLENGE     ][ 18] [1adee11491dcfb79fd094a517fb1674]
[ 10 BASIP        ][ 6] [192.168.216.254]
[ 33 RELAYMSG     ][ 32] [MGkLSk8BPtyRR81eFNwlnzwHOA=]
```

根据客户端发送的Portal报文，查看用户名为 test1@portal；

根据Portal认证的原理：每个Portal用户都属于一个认证域，且在其所属的认证域内进行认证/授权/计费，认证域中定义了一套认证/授权/计费的策略。

通过在指定接口上配置Portal用户使用的认证域，使得所有从该接口接入的Portal用户被强制使用指定的认证域来进行认证、授权和计费。即使Portal用户输入的用户名中携带的域名相同，接入设备的管理员也可以通过该配置使得不同接口上接入的Portal用户使用不同的认证域，从而增加管理员部署Portal接入策略的灵活性。

从指定接口上接入的Portal用户将按照如下先后顺序选择认证域：接口上指定的Portal用户使用的ISP域-->用户名中携带的ISP域-->系统缺省的ISP域。

用户带着@portal的域名触发认证，首先设备接口下没有指定终端用户使用的ISP域，则按照Portal用户选择认证域的顺序，根据用户名中携带的ISP域进行AAA认证，设备上没有配置关于portal的domain，自动转为系统缺省的ISP域进行AAA认证，而设备上调用radius scheme为domain youxian，系统缺省的ISP域system域没有相关AAA策略，

因此终端Portal用户并没有找到正确的认证域，无法进行认证域中的认证/授权/计费策略，从而无法通过Portal认证。

1、修改用户客户端携带的ISP域为设备上配置的youxian域；

2、将设备上系统缺省的ISP域设置为youxian域。