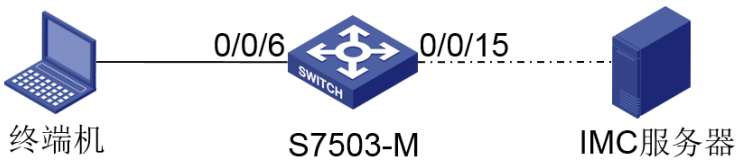
某局点使用S7503E-M 结合IMC做portal认证异常

Radius Portal 徐猛 2019-03-25 发表

组网及说明

现场使用我司的S7503E-M设备，作为下联终端的网关，同时在我们设备上起了portal认证，之前使用正常，后来设备发生了一次异常断电，后来portal就出现了异常情况。

组网说明：



测试终端地址为：10.51.8.216
终端网关为：vlan interface 200：10.51.8.254
IMC服务器地址为：10.51.1.211

问题描述

S7503E-M设备上作为下联终端的网关，起了portal认证，现场配置完portal认证后，portal认证的过程出现了一些异常，现场使用终端进行测试，测试终端ip地址为10.51.8.216，进过测试发现：
（1） 终端接入0/0/6口以后，在vlan 200接口下使能portal相关配置，然后进行portal认证，正常。
（2） 先在vlan 200接口使能portal相关配置，然后接入终端，终端无法进行portal认证，终端ping不通网关vlan 200：10.51.8.254以及portal服务器地址：10.51.1.211。但是配置中网关和IMC地址都是放通的。
portal free-rule 0 source ip any destination ip 10.51.1.211 255.255.255.255
portal free-rule 11 source ip any destination ip 10.51.8.254 255.255.255.255

过程分析

（1）首先我们对设备的配置做了检查：
测试开启portal认证的接口为vlan 200（实际设备上有32个vlan接口下都启用了portal认证）：
interface Vlan-interface200
ip address 10.51.8.254 255.255.255.0
portal enable method direct
portal domain portal
portal bas-ip 10.255.26.62
portal apply web-server imc
#
radius scheme imc
primary authentication 10.51.1.211
primary accounting 10.51.1.211
accounting-on enable
accounting-on extended
key authentication cipher c3$JzyST6WtawaCoKwAXIGeKFSm/Zfi/h0=
key accounting cipher c3$UkIY0qs2bndJY9wqxcFI2W+MX2olleM=
user-name-format without-domain
#
domain portal
authentication portal radius-scheme imc
authorization portal radius-scheme imc
accounting portal radius-scheme imc
#
以及多达69条的portal free-rule的规则，均未发现配置存在问题：

（2）由于portal free-rule规则中去往网关和 IMC服务器的地址都是放通了的，正常终端应该是能ping通网关和IMC服务器的，但是现场终端ping不通网关地址和IMC服务器地址。

测试终端接在6口上，检查设备arp学习正常；
==========display arp all==========

Type: S-Static D-Dynamic O-Openflow R-Rule M-Multiport I-Invalid
10.51.8.216 0016-d3b1-d202 200 GE0/0/6 1123 D

终端网关S7503E-M设备上到IMC的路由正常，能ping通IMC：
dis ip routing-table 10.51.1.211
Summary count : 1
Destination/Mask Proto Pre Cost NextHop Interface
10.51.0.0/16 O_ASE2 150 1 10.255.26.61 Vlan916

从设备上直接ping IMC服务器正常：
ping -a 10.51.8.254 10.51.1.211
Ping 10.51.1.211 (10.51.1.211) from 10.51.8.254: 56 data bytes, press CTRL_C to break
56 bytes from 10.51.1.211: icmp_seq=0 ttl=126 time=1.831 ms
56 bytes from 10.51.1.211: icmp_seq=1 ttl=126 time=1.686 ms
56 bytes from 10.51.1.211: icmp_seq=2 ttl=126 time=1.679 ms
56 bytes from 10.51.1.211: icmp_seq=3 ttl=126 time=1.684 ms
56 bytes from 10.51.1.211: icmp_seq=4 ttl=126 time=1.628 ms

（3）在交换机上针对终端ping IMC服务器的流量做流量统计：
终端ping portal服务器的流量统计情况如下，根据流量统计结果看，报文上到我们设备上，未进行转发。根据和现场工程师沟通，关闭vlan 200接口上的portal功能后，能正常ping通 IMC服务器，但是portal free 规则中相应地址都已经放通，应该不存在该现象，软件版本说明书中也未发现类似问题。
dis qos policy interface
Interface: GigabitEthernet0/0/6
Direction: Inbound
Policy: 1
Classifier: 1
Operator: AND
Rule(s) :
If-match acl 3001
Behavior: 1
Accounting enable:
4 (Packets)
Interface: GigabitEthernet0/0/6
Direction: Outbound
Policy: 2
Classifier: 2
Operator: AND
Rule(s) :
If-match acl 3002
Behavior: 2
Accounting enable:
0 (Packets)
Interface: GigabitEthernet0/0/15
Direction: Inbound
Policy: 2
Classifier: 2
Operator: AND
Rule(s) :
If-match acl 3002
Behavior: 2
Accounting enable:
0 (Packets)
Interface: GigabitEthernet0/0/15
Direction: Outbound
Policy: 1
Classifier: 1
Operator: AND
Rule(s) :
If-match acl 3001
Behavior: 1
Accounting enable:
0 (Packets)

根据上述定位，能断定问题出在我们交换机上，而且和接口上使能的portal认证直接相关，后来经协调产品线专家定位发现：
单板的ACL资源很小，只有3K，32个vlan使能Portal，配置了69条free规则，Portal free就需要下发32*69=2208条，用户上线后底层由于要匹配更多的字段会切成double模式，就会出现资源不足底层无法切成double模式的情况，acl资源早已经超出了，建议优化vlan及Portal free规则，尽可能降低资源占用，优化后请将vlan下的Portal配置全部删除后，再重新配置：

```
Interfaces: GE1/0/1 to GE1/0/24, XGE1/0/25 to XGE1/0/28 (slot 1)
------------------------------------------------------------------------
Type            Total     Reserved   Configured Remaining  Usage
------------------------------------------------------------------------
VFP ACL         2048      1024       0          1024       50%
IFP ACL         4096      1024       2351       721        82%
IFP Meter       2048      512        0          1536       25%
IFP Counter     2048      512        0          1536       25%
EFP ACL         1024      0          0          1024       0%
EFP Meter       512       0          0          512        0%
EFP Counter     512       0          0          512        0%

 Pri 12, Group  5,usedEntries 2270,mode Single, physlice 4/5/6/7/8/9/10/11/12/
 ========================================
  acl type                 usedEntries[2270]
 ========================================
  [35 ]Portal Free                2208
  [37 ]Portal Redirect            62
```

解决方法

S7503E-M的单板的ACL资源很小，只有3K，32个vlan使能Portal，配置了69条free规则，Portal free就需要下发32*69=2208条，用户上线后底层由于要匹配更多的字段会切成double模式，就会出现资源不足底层无法切成double模式的情况，acl资源早已经超出了，建议优化vlan及Portal free规则，尽可能降低资源占用，优化后请将vlan下的Portal配置全部删除后，再重新配置：

```
Interfaces: GE1/0/1 to GE1/0/24, XGE1/0/25 to XGE1/0/28 (slot 1)
------------------------------------------------------------------------
Type            Total     Reserved   Configured Remaining  Usage
------------------------------------------------------------------------
VFP ACL         2048      1024       0          1024       50%
IFP ACL         4096      1024       2351       721        82%
IFP Meter       2048      512        0          1536       25%
IFP Counter     2048      512        0          1536       25%
EFP ACL         1024      0          0          1024       0%
EFP Meter       512       0          0          512        0%
EFP Counter     512       0          0          512        0%

 Pri 12, Group  5,usedEntries 2270,mode Single, physlice 4/5/6/7/8/9/10/11/12/
 ========================================
  acl type                 usedEntries[2270]
 ========================================
  [35 ]Portal Free                2208
  [37 ]Portal Redirect            62
```