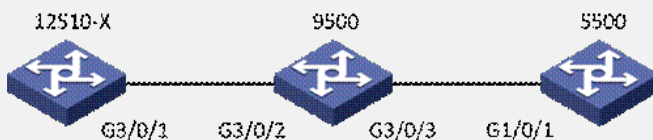


知 S12500-X交换机本地地址无法访问故障案例

MIB 丁犁 2014-07-28 发表

S12500-X交换机本地地址无法访问故障案例

一、组网图：



二、组网及故障描述：

12510-X交换机与5500交换机通过三层路由转发数据。

12510-X G3/0/1接口所属VLAN地址为202.117.104.254/25。

9500 G3/0/2接口所属VLAN地址为202.117.104.253/25； G3/0/3接口所属VLAN地址为202.117.104.80/25

5500 G1/0/1接口所属VLAN地址为202.117.104.79/25。

在5500交换机上ping 12510-X G3/0/1接口所属VLAN地址202.117.104.254无法PING通

```
[5500]ping -a 202.117.104.79 202.117.104.254
```

```
Ping 202.117.104.254 (202.117.104.254) from 202.117.104.79: 56 data bytes, press CTRL_C to break
```

```
--- Ping statistics for 202.117.104.254 ---
```

```
1 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

三、问题分析：

在12510-X上开启debug ip icmp信息，发现12510-X CPU能够正常接收和回应5500交换机的ICMP报文。

```
*Jun 23 18:00:46:174 2014 12510-X SOCKET/7/ICMP: -MDC=1-Chassis=1-Slot=1;
```

```
Time(s):1403546446 ICMP Input:
```

```
ICMP Packet: src = 202.117.104.79, dst = 202.117.104.254
```

```
type = 8, code = 0 (echo)
```

```
*Jun 23 18:00:46:174 2014 12510-X SOCKET/7/ICMP: -MDC=1-Chassis=1-Slot=1;
```

```
Time(s):1403546446 ICMP Output:
```

```
ICMP Packet: src = 202.117.104.254, dst = 202.117.104.79
```

```
type = 0, code = 0 (echo-reply)
```

在12510-X上，通过打印上送CPU的报文，观察发送和接收ICMP报文信息

```
[12500-probe]debug rxtx pkt 1
```

```
.....
```

```
*Jun 23 16:25:11:270 2014 12510-X DRVPLAT/7/RxTxDebug: -MDC=1-Chassis=1-Slot=3;
```

```
0000 0c da 41 b6 77 4d 0c da 41 b6 5e cb 81 00 00 6a
```

```
0010 08 00 45 00 00 3c 52 cd 00 00 01 01 02 6b ca 75
```

```
0020 68 fe ca 75 68 4f 00 00 3d 12 04 21 14 29 61 62
```

```
0030 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72
```

```
0040 73 74 75 76 77 61 62 63 64 65 66 67 68 69
```

.....

通过查看ICMP报文信息，发现12510-X CPU发出的ICMP回应报文TTL=1（上述红色字段）。由于ICMP回应报文TTL=1，当该报告到达9500后，9500作为三层设备将TTL减1后，无法将该报文传递给5500交换机，因此出现无法PING通的故障。

四、解决方法

在12510-X交换机上通过强制ttl数值后，PING 5500 G1/0/1接口地址测试

```
[12510-X]ping -h 2 -a 202.117.104.254 202.117.104.79
```

```
Ping 202.117.104.79 (202.117.104.79) from 202.117.104.254: 56 data bytes, press CTRL_C to break
```

```
56 bytes from 202.117.104.79: icmp_seq=0 ttl=254 time=2.441 ms
```

```
56 bytes from 202.117.104.79: icmp_seq=1 ttl=254 time=2.998 ms
```

```
56 bytes from 202.117.104.79: icmp_seq=2 ttl=254 time=2.261 ms
```

```
56 bytes from 202.117.104.79: icmp_seq=3 ttl=254 time=21.116 ms
```

```
56 bytes from 202.117.104.79: icmp_seq=4 ttl=254 time=74.306 ms
```

```
--- Ping statistics for 202.117.104.79 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
```

```
round-trip min/avg/max/std-dev = 2.261/20.624/74.306/27.787 ms
```

通过测试，验证故障确实是由于12510-X CPU在默认回应请求报文时，将回应报文的TTL置为1导致。

对于该故障情况的出现，怀疑12510-X存在被SNMP攻击，将交换机默认TTL MIB节点修改的情况。读取12510-X相关节点信息，发现默认的TTL数值已被篡改。

```
Name:      ipDefaultTTL
Type:      OBJECT-TYPE
OID:       1.3.6.1.2.1.4.2
Full path: iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).ip(4).ipDefaultTTL(2)
Module:    IP-MIB
```

```
Parent:    ip
Prev sibling: ipForwarding
Next sibling: ipInReceives
```

```
Numerical syntax: Integer (32 bit)
Base syntax:      INTEGER
Composed syntax:  INTEGER
Status:           current
Max access:       read-write
Size list:        1: 1..255
```

```
Description:  The default value inserted into the Time-To-Live field of
               the IP header of datagrams originated at this entity,
               whenever a TTL value is not supplied by the transport layer
               protocol.
```

此时通过SNMP协议将该TTL MIB节点Size list信息修改回255后，12510-X与5500设备之间可以正常互通。

```
Size list:    255: 1..255
```

同时修改12510-X SNMP读写团体字口令强度，防止设备被非法攻击篡改信息。

五、总结

通过该案例，对于PING 12500-X本地地址不通故障时，建议通过debug命令查看设备CPU是否可接收和发送ICMP报文，同时观察CPU处理的报文结构，以便发现异常。