

知 某局点7503E-M直连规律性丢包问题

转发不通 ARP ARP攻击防御 许鹏鹏 2020-03-16 发表

组网及说明

S7503E-M交换机TG1/0/27 --- S125X交换机

问题描述

S7503E-M业务转发均正常，但和125X直连的地址时断时续，从流统信息看，报文进入S75E，但驱动没打印出来

源地址：10.0.0.126 目的地址：10.0.0.254

过程分析

查看arp学习正常

```
[TuShuGuan_HuiJu-probe]display arp 10.0.0.254
```

Type: S-Static D-Dynamic O-Openflow R-Rule M-Multiport I-Invalid

IP address	MAC address	VLAN/VSI	Interface	Aging Type
10.0.0.254	542b-de10-6c01	1000	BAGG6	1197 D

端口聚合状态也正常

```
[TuShuGuan_HuiJu-probe]display link-aggregation verbose Bridge-Aggregation 6
```

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Port Status: S -- Selected, U -- Unselected, I -- Individual

Port: A -- Auto port, M -- Management port, R -- Reference port

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,

D -- Synchronization, E -- Collecting, F -- Distributing,

G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation6

Aggregation Mode: Static

Loadsharing Type: Shar

Management VLANs: None

Port	Status	Priority	Oper-Key
XGE1/0/27(R)	S	32768	1

流统结果正常，但是debug看没有replay报文上送CPU

//本地带源ping 10.0.0.254，发出5个，收到5个，但debug ip icmp无reply报文上送

```
dis qos policy interface Ten-GigabitEthernet 1/0/27
```

Interface: Ten-GigabitEthernet1/0/27

Direction: Inbound

Policy: liutong

Classifier: liutong

Operator: AND

Rule(s) :

If-match acl 3005

Behavior: liutong

Accounting enable:

5 (Packets)

0 (pps)

Interface: Ten-GigabitEthernet1/0/27

Direction: Outbound

Policy: liutong

Classifier: liutong

Operator: AND

Rule(s) :

If-match acl 3005

Behavior: liutong

Accounting enable:

5 (Packets)

0 (pps)

发现现场时断时续很有规律，连续通15个包，然后一段时间不通，后面继续连续通15个包后不通，如此循环，检查配置发现，现场配置了arp攻击检测。

设备上配置有源MAC地址固定的ARP攻击检测，怀疑可能由于攻击导致报文可能被丢弃了

```
arp source-mac filter
```

```
arp source-mac aging-time 60
```

```
arp source-mac threshold 15
```

```
arp active-ack enable
```

```
#
```

打开设备debug arp packet，发现确实存在该源MAC发送大量ARP报文的情况。

设备检测到 542b-de10-6c01 (vlan 1000)存在ARP攻击，单板上将该MAC设置为丢弃。

该功能不仅会丢弃arp攻击报文，ip报文也会被丢弃。

解决方法

现场删除该命令后，验证可以ping通。同时也可以选择将arp防攻击检测阈值调大来解决。