某局点S10508X Leaf三层转发不通问题

IP Source Guar | EVPN | VxLAN | ADCampus解决方案 | 张猛 | 2022-09-13 发表

组网及说明

设备型号：S10508X

版本：E7634P03

组网环境：ADCampus 6.2方案组网

问题描述

现场新开局，一组10508X堆叠作为leaf设备，作为分布式网关，当前发现该leaf下挂所有终端访问外网不通

过程分析

源地址为10.193.144.144的终端，通过leaf以及spine访问外网，目的ip地址为10.193.57.253，都位于vpn1中

现场流统发现报文进入leaf设备后未从上行口转出，确认报文丢在了leaf设备上，在leaf设备上查看vpn路由表项正常：

```
[Tao_Zyyjy_1F_Leaf-probe]dis ip routing-table vpn-instance vpn1 10.193.57.253
 Summary count : 1
 Destination/Mask Proto Pre Cost NextHop Interface
10.193.57.252/30 BGP 255 0 10.193.57.1 Vsi3
```

leaf与spine之间的隧道正常：

```
[Tao_Zyyjy_1F_Leaf]dis int Tunnel 1
Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 10.193.57.4, destination 10.193.57.1
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 753 bytes/sec, 6024 bits/sec, 7 packets/sec
Last 300 seconds output rate: 2668 bytes/sec, 21344 bits/sec, 8 packets/sec
Input: 2124068 packets, 199668763 bytes, 0 drops
Output: 2274182 packets, 1022333768 bytes, 0 drops
```

将报文入方向mirror-to cpu后打印，报文的封装正常。

进一步查看连接终端的BAGG1024接口配置，发现接口下启用了ip source guard

```
interface Bridge-Aggregation1024
 port link-type trunk
 port trunk permit vlan 1 101 to 3000 4094
 link-aggregation mode dynamic
 stp instance 0 port priority 16
 stp instance 0 cost 1
 stp tc-restriction
 ip verify source ip-address mac-address
 mac-based ac
 dot1x
 undo dot1x handshake
 undo dot1x multicast-trigger
 dot1x unicast-trigger
 mac-authentication
 mac-authentication domain eia
 mac-authentication parallel-with-dot1x
 port-security free-vlan 1 4094
```

查看生成的绑定表项发现终端对应的vlan为vlan102：

```
[Tao_Zyyjy_1F_Leaf]dis ip source binding | in 144.144
10.193.144.144  642f-c743-47da BAGG1024                102  ARP snooping vsi
```

而实际该终端认证完成后下发了授权vsi为vsi13：

```
<Tao_Zyyjy_1F_Leaf>dis arp 10.193.144.144
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI name Interface              Aging Type
10.193.144.144  642f-c743-47da vsi13         BAGG1024               957   D
```

因此导致报文到达leaf后ip source guard检查不通过被丢弃

解决方法

当前该配置方案不建议配置，删除后恢复正常。

interface_ipv4_binding：配置应用于Leaf接口组，应用于端口安全，配置策略后会下发ip verify source ip-address mac-address，当前方案不建议配置。