S7502E IP Source Guard 匹配 DHCP Snooping表项案例

IP Source Guar DHCP Snooping 许家豪 2021-12-14 发表

组网及说明

设备及版本：S7502E 7624P01 ADCampus 五期B03

组网：leaf-access-pc 全部直连

问题描述

问题描述：leaf上开启了IP Source Guard 功能，当leaf口UP/DOWN后，出现部分PC ping通网关，但是无法跨三层访问

过程分析

10.68.101.128和10.68.101.133 是两台PC 的ip，当出现问题时（ 10.68.101.133网络不通）使用 Display ip source binding 命令查看，如下图所示

发现 10.68.101.133 没有对应的DHCP snooping 表项，但是有ARP snooping表项。

```
10.68.98.106    d43d-7e60-cfbc XGE2/0/35                667  DHCP snooping
<XZZX-EX-HJ1>dis ip source binding ip-address 10.68.101.128
Total entries found: 2
IP address      MAC address    Interface               VLAN Type
10.68.101.128   b07b-2520-3929 XGE2/0/3                619  DHCP snooping
10.68.101.128   b07b-2520-3929 XGE2/0/3                619  ARP snooping vsi
<XZZX-EX-HJ1>dis ip source binding ip-address 10.68.101.133
Total entries found: 1
IP address      MAC address    Interface               VLAN Type
10.68.101.133   540d-f92b-1586 XGE2/0/3                650  ARP snooping vsi
```

经核实ARP Snooping 的生产只有符合ARP特征即可，一条报文即可生成，安全性不高，因此并不用于过滤报文。

表1-1 IPv4动态绑定功能信息表

接口类型	表项来源模块	用途
二层以太网接口	DHCP Snooping、802.1X	报文过滤
	ARP Snooping	配合其它模块（例如MFF）提供相关的安全服务，而不直接用于过滤报文
三层以太网接口/VLAN接口	DHCP中继	报文过滤
	DHCP服务器	配合其它模块（例如授权ARP）提供相关的安全服务，而不直接用于过滤报文

leaf下行口UP/down后，DHCP Snooping 表项消失是因为，用户被下线了。DHCP Snooping表项消失，IP Source Guard 无法根据DHCP Snooping表项动态生成ip source binding表项，因此无法跨三层访问

如下图所示，在leaf下行口shutdown后的动作（保持在线或者下线）是由MAC认证服务器设置的，如果下图中的Port-down keep online 如果是enable，在shutdown动作后，用户仍会在线，否则用户会被踢下线。

```
[XZZX-EX-HJ1-Ten-GigabitEthernet2/0/34]dis mac-authentication connection user-ma
c 8089-17ad-235d
Total connections: 1
Slot ID: 2
User MAC address: 8089-17ad-235d
Access interface: Ten-GigabitEthernet2/0/34
Username: 808917ad235d
User access state: Successful
Authentication domain: bl
IPv4 address: 10.68.99.10
IPv4 address source: IP Source Guard
Initial VLAN: 621
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: vsi3
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: 86400 sec
Offline detection: Ignore (server-assigned)
Online from: 2021/10/22 20:05:09
Online duration: 800h 57m 49s
Port-down keep online: Enabled

[XZZX-EX-HJ1-Ten-GigabitEthernet2/0/34]dis mac-authentication connection user-ma
c 6c4b-90bb-7846
Total connections: 1
Slot ID: 2
User MAC address: 6c4b-90bb-7846
Access interface: Ten-GigabitEthernet2/0/34
Username: 6c4b90bb7846
User access state: Successful
Authentication domain: bl
IPv4 address: 10.68.99.11
IPv6 address: 240B:8044:106E:0:9C04:CBEC:2D27:708A
IPv4 address source: IP Source Guard
IPv6 address source: IP Source Guard
Initial VLAN: 655
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: vsi3
Authorization microsegment ID: N/A
Authorization ACL number/name: 3001
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: http://192.168.248.10:30004/byod/index.html?usermac=%m&userip=%c&userurl=%o&original=%o
Authorization IPv6 URL: N/A
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: 86400 sec
Online from: 2021/11/24 20:59:18
Online duration: 0h 4m 17s
Port-down keep online: Disabled (offline)
```

解决方法

在控制器侧，修改服务器下发授权信息时携带端口down后所采取的动作为enable。