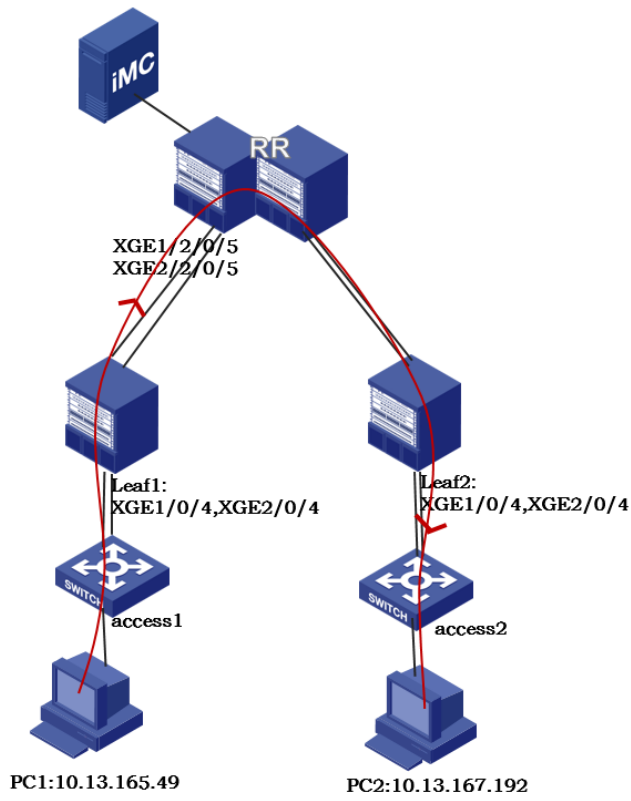


某局点adcampus 5.0方案下东西向流量不通的经验案例

ADCampus解决方案 VxLAN EVPN SNA Center 王燕 2021-03-14 发表

组网及说明

组网如下:



问题描述

#背景摘要

Adcampus5.0, 分布式网关, arp代理方式, 终端mac认证, 南北向已实现互通, 局点想实现东西向互通的精细化控制, 通过SNA下发策略路由方式; 方案部署后未测试过东西向互通情况, 目前arp, 路由学习正常, 但是互访不通;

	ARP代答	ARP代理
响应设备	L2/L3网关	L3网关
ARP 回应的MAC	主机MAC	网关MAC
报文转发方式	二层流量查MAC 三层流量查FIB	全三层转发
MAC地址学习	学习	可以不学习

#需求&策略路由配置

22段的不互访, 25到22段互访, 5期方案通过SNA下发PBR方式控制

```
acl advanced name SDN_ACL_SC_00000k_7_7
rule 0 permit ip source 10.13.167.128 0.0.0.127 destination 10.13.164.0 0.0.3.255
acl advanced name SDN_ACL_SC_00000l_7_7
rule 0 permit ip source 10.13.164.0 0.0.3.255 destination 10.13.167.128 0.0.0.127
acl advanced name SDN_ACL_SC_000002_7_7
rule 0 permit ip destination 10.13.164.0 0.0.3.255 //匹配22位, 丢弃
policy-based-route SDN_SC_7 permit node 0
if-match acl name SDN_ACL_SC_00000k_7_7 //查表转发
policy-based-route SDN_SC_7 permit node 2
if-match acl name SDN_ACL_SC_00000l_7_7 //查表转发
policy-based-route SDN_SC_7 permit node 14
if-match acl name SDN_ACL_SC_000002_7_7
apply output-interface NULL0 //丢弃
```

过程分析

1、#上行spine流统未统计到上来流量，在access上行口抓包有相关流量发到leaf1

```
<Spine>dis lldp neighbor-information list
```

```
Chassis ID : * -- -- Nearest nontpmr bridge neighbor
```

```
# -- -- Nearest customer bridge neighbor
```

```
Default -- -- Nearest bridge neighbor
```

```
Local Interface Chassis ID Port ID System Name
XGE1/2/0/5 6ce5-f76b-22b8 Ten-GigabitEthernet1/0/46 Leaf1
XGE2/2/0/5 6ce5-f76b-22b8 Ten-GigabitEthernet2/0/46 Leaf1 //互联接口
```

```
acl number 3010 //VXLAN内存流统
```

```
description liutong
```

```
rule 15 permit vxlan inner-protocol icmp inner-source 10.13.165.49 0 inner-destination 10.13.167.192 0
```

```
rule 25 permit vxlan inner-protocol icmp inner-source 10.13.167.192 0 inner-destination 10.13.165.49 0
```

```
rule 30 permit vxlan inner-protocol icmp inner-source 10.13.167.254 0 inner-destination 10.13.167.192 0
```

```
<Spine>dis qos policy interface Ten-GigabitEthernet 1/2/0/5
```

```
Interface: Ten-GigabitEthernet1/2/0/5
```

```
Direction: Inbound
```

```
Policy: liutong
```

```
Classifier: liutong
```

```
Operator: AND
```

```
Rule(s) :
```

```
If-match acl 3010
```

```
Behavior: liutong
```

```
Accounting enable:
```

```
0 (Packets)
```

```
0 (pps)
```

```
<Spine>dis qos policy interface Ten-GigabitEthernet 2/2/0/5
```

```
Interface: Ten-GigabitEthernet2/2/0/5
```

```
Direction: Inbound
```

```
Policy: liutong
```

```
Classifier: liutong
```

```
Operator: AND
```

```
Rule(s) :
```

```
If-match acl 3010
```

```
Behavior: liutong
```

```
Accounting enable:
```

```
0 (Packets)
```

```
0 (pps)
```

2、PBR配置无问题，下面是底层下发情况：

```
[Leaf1-probe]debug qacl show acl-resc slot 1 chip 0
```

```
-----Qacl VTCam UsedResc Info-----
```

```
Acl Hw Resource: Group 0, VTCamId 0, Client TTI 0
```

```
-----
```

```
Pri 7, usedEntries 177, mode Double
```

```
=====
```

```
acl type usedEntries[177]
```

```
=====
```

```
[10:07:33] [134]Policy Based Routing V4 175
```

```
[10:07:33] [275]Policy Based Routing V4 Global 2
```

```
[Leaf1-probe]debug qacl show slot 1 chip 0 verbose (acl-type 134
```

```
[Leaf1-probe]debug qacl show slot 1 chip 0 verbose 20 acl-type 134
```

```
[Leaf1-probe]debug qacl show slot 1 chip 0 verbose 40 acl-type 134
```

```
[Leaf1-probe]debug qacl show slot 1 chip 0 verbose 60 acl-type 134
```

```
[Leaf1-probe]debug qacl show slot 1 chip 0 verbose 80 acl-type 134
```

```
:
```

```
:
```

ACL-Type Policy Based Routing V4, Stage IPCL 0, NoExpand, Installed, Active
Prio Mjr/Sub 0x207/0x3, RuleFormat INGRESS_EXT_NOT_IPV6, Vtcame/Idx 4/678,
PBRV4 Policy SDN_SC_7, VlanIntf 812, Node 2, ApplyIdx 0, Match ACI 1(Yes 1: No 0)

解决方法
ACL GroupNo : 637534211, RuleID : 0

interface LoopBack0

ip address 10.13.132.5 255.255.255.255/环回口地址配置改成32位掩码, 各表项下发正常

ospf source-ip 10.13.167.128, 255.255.255.128

Dest IP: 10.13.164.0, 255.255.252.0

IP Type: Any IPv4 packet

Mac to me: 1

Evlan: 4098

Actions -----

Account mode packets, green and non-green

Permit

Accounting: Hi 0, Lo 1818

:

ACL-Type Policy Based Routing V4, Stage IPCL 0, NoExpand, Installed, Active

Prio Mjr/Sub 0x207/0x3, RuleFormat INGRESS_EXT_NOT_IPV6, Vtcame/Idx 4/679,

PBRV4 Policy SDN_SC_7, VlanIntf 812, Node 3, ApplyIdx 0, Match ACI 1(Yes 1: No 0)

ACL GroupNo : 637534213, RuleID : 0

Rule Match -----

Global range

Source IP: 10.13.164.0, 255.255.252.0

Dest IP: 10.13.167.128, 255.255.255.128

IP Type: Any IPv4 packet

Mac to me: 1

Evlan: 4098

Actions -----

Account mode packets, green and non-green

Permit

Accounting: Hi 0, Lo 23422

3、#本端leaf 终端arp学习正常

<Leaf1>dis arp 10.13.165.49

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

IP address	MAC address	VLAN/VSI name	Interface	Aging Type
------------	-------------	---------------	-----------	------------

10.13.165.49	9c7b-ef4a-9e34	vsi7	BAGG4	1198 D
--------------	----------------	------	-------	--------

#mac表项学习正常

[Leaf1]dis l2vpn mac-address | be 9c7b-ef4a-9e34

MAC Address : 9c7b-ef4a-9e34

VSI Name : vsi7

State : Mac-auth

Link ID/Name Aging

BAGG4 NotAging

#两端隧道正常自动建立, 互ping隧道地址测试正常

<Leaf1>dis interface Tunnel 3

Tunnel3

Current state: UP

Line protocol state: UP

Description: Tunnel3 Interface

Bandwidth: 64 kbps

Maximum transmission unit: 1500

Internet protocol processing: Disabled

Last clearing of counters: Never

Tunnel source 10.13.132.5, destination 10.13.132.4

Tunnel protocol/transport UDP_VXLAN/IP

Last 300 seconds input rate: 2818 bytes/sec, 22544 bits/sec, 11 packets/sec

Last 300 seconds output rate: 3 bytes/sec, 24 bits/sec, 0 packets/sec

Input: 90877343 packets, 19193532346 bytes, 0 drops

Output: 4161 packets, 1501415 bytes, 0 drops

#ARP代理方式, 跨leaf二层互通查看对端PC2 32位主机路由学习正常

[Leaf1-probe]dis ip routing-table vpn-instance Production 10.13.167.192

Summary count : 3

Destination/Mask	Proto	Pre Cost	NextHop	Interface
------------------	-------	----------	---------	-----------

0.0.0.0/0	BGP	255 2	10.13.132.254	Vsi3
10.13.164.0/22	Direct	0 0	10.13.167.254	Vsi7
10.13.167.192/32	BGP	255 0	10.13.132.4	Vsi3