

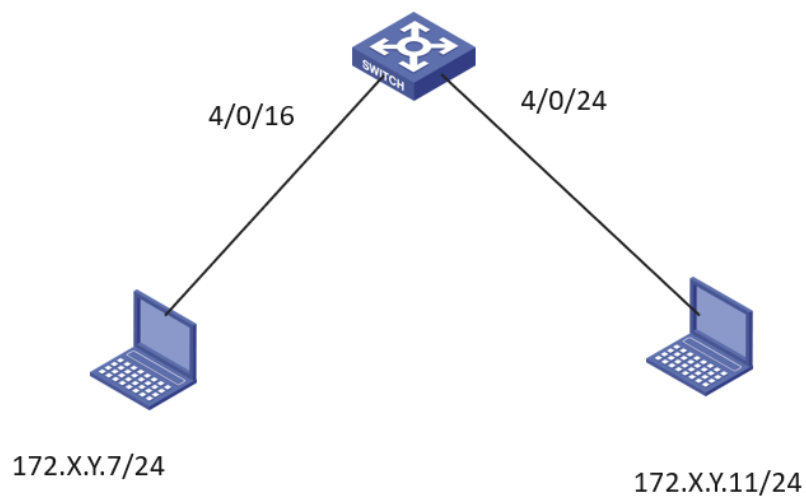
知 某局点S12508X-AF出方向包过滤不生效的经验案例

packet-filter

徐玉娟

2023-06-25 发表

组网及说明



问题描述

在交换机端口XGE4/0/16出方向做包过滤，放通同网段以及个别网段。配置包过滤后同网段终端172.X.Y.11无法与172.X.Y.7通信

配置包过滤前后的ping测试结果

```
[h3c@~]$ ping 172.25.28.7
PING 172.25.28.7 (172.25.28.7) 56(84) bytes of data:
64 bytes from 172.25.28.7: icmp_seq=15 ttl=64 time=0.158 ms
64 bytes from 172.25.28.7: icmp_seq=16 ttl=64 time=0.162 ms
64 bytes from 172.25.28.7: icmp_seq=17 ttl=64 time=0.114 ms
64 bytes from 172.25.28.7: icmp_seq=18 ttl=64 time=0.150 ms
^C
--- 172.25.28.7 ping statistics ---
18 packets transmitted, 4 received, 77% packet loss, time 16995ms
rtt min/avg/max/mdev = 0.114/0.146/0.162/0.019 ms
[h3c@vcfc1 ~]$ di ip int brief
-bash: di: command not found
[h3c@vcfc1 ~]$ ping 172.25.28.7
PING 172.25.28.7 (172.25.28.7) 56(84) bytes of data:
^P^C
--- 172.25.28.7 ping statistics ---
529 packets transmitted, 0 received, 100% packet loss, time 528141ms
```

过程分析

1, 检查配置没有问题, 没有配置其他包过滤, 且只有 acl 2002中匹配了该网段

```
interface Ten-GigabitEthernet4/0/16
port link-mode bridge
port access vlan 4094
packet-filter 2002 outbound
#
acl basic 2002
rule 25 permit source 172.X.Y.0 0.0.0.255
rule 100 deny
```

2, 删除包过滤之后就可以互通

改成入方向包过滤也可以互通

```
interface Ten-GigabitEthernet4/0/16
port link-mode bridge
description license-server1
port access vlan 4094
packet-filter 2002 inbound
```

3, 配置出方向包过滤, 查看acl下发情况有报错

```
Acl-Type PktFilter IP on PORT, Stage EFP, SinglePort, Installed, Active
L2 PROGRAM : Prio Mjr/Sub 8/2113798118, Group 15 [0], enRtnHealth 1, Entry 202, Mdc 1
ACL GroupNo : 2002, RuleID : 25 V4v6 1
Rule Match -----
    Out Port: 11
    Source IP: 172.X.Y.0, 255.255.255.0
    IP Type: Any IPv4 packet EFP Arad Don't Set
    Not mirror copy
    Forwarding Type: ipv4_uc
```

Actions -----

Permit

L2 PROGRAM : Bank 10 Location 10 HIT(read-clear): NO

经过确认, 125X设备针对二层转发报文出方向的ACL无法匹配源目IP, 只可以匹配IP协议类型, 所以报文都匹配上rule 100被deny掉了, 测试去掉rule 100就可以通:

```
acl basic 2002
rule 25 permit source 172.X.Y.0 0.0.0.255
rule 100 deny  删除此条规则之后可以通
```

底层acl下发时, 匹配源目ip的规则报错"Any IPv4 packet EFP Arad Don't Set"说明出方向不支持

```
[H3C-probe]debug qacl show slot 4 chip 0 verbose 7 acl-type 95
```

```
Acl-Type PktFilter IP on PORT, Stage EFP, SinglePort, Installed, Active
L2 PROGRAM : Prio Mjr/Sub 8/2113798118, Group 15 [0], enRtnHealth 1, Entry 202, Mdc 1
ACL GroupNo : 2002, RuleID : 25 V4v6 1
Rule Match -----
    Out Port: 11
    Source IP: 172.X.Y.0, 255.255.255.0
    IP Type: Any IPv4 packet EFP Arad Don't Set----EFP即出方向, 说明出方向不支持
    Not mirror copy
    Forwarding Type: ipv4_uc
```

Actions -----

Permit

L2 PROGRAM : Bank 10 Location 10 HIT(read-clear): NO

解决方法

入方向不存在该限制，建议把包过滤下在入方向解决：

=====

Acl-Type PktFilter IP on PORT, Stage IFP, SinglePort, Installed, Active

L2 PROGRAM : Prio Mjr/Sub 8/2113798112, Group 16 [0], enRtnHealth 1, Entry 208, Mdc 1

ACL GroupNo : 2002, RuleID : 31 V4v6 1

Rule Match -----

In Port: 11

EtherType: 0x800, 0xffff

Source IP: 172.X.Y.0, 255.255.255.0

Actions -----

Permit

L2 PROGRAM : Bank 12 Location 11 HIT(read-clear): YES

=====

