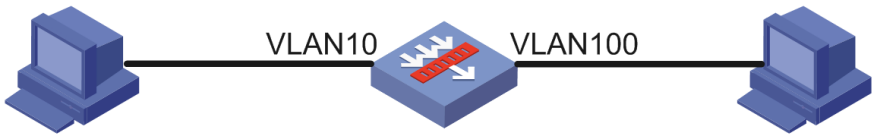
某局点F5060跨VLAN模式Bridge转发不通处理经验案例

二层转发 孙轶宁 2018-11-08 发表

组网及说明



如上图，F5060两边是两台终端，分别属于VLAN10和100，配置跨VLAN模式Bridge使VLAN10和100互通

问题描述

F5060配置如下

```
bridge 1 inter-vlan
 add vlan 10 100
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
#
security-zone name Trust
 import interface GigabitEthernet1/0/1 vlan 10
#
security-zone name Untrust
 import interface GigabitEthernet1/0/2 vlan 100
#
security-policy ip
 rule 10 name permit
  action pass ‘
  source-zone trust
  source-zone untrust
  destination-zone trust
  destination-zone untrust
```

发现两台PC互ping不通

过程分析

1、首先确认两边PC有没有学到ARP，发现两边都有对方的ARP表项。

2、检查设备上面是否有会话，发现设备没有会话。

3、在设备上面deb aspf packet，发现没有源目安全域。

*Nov 8 19:18:03:646 2018 H3C ASPF/7/PACKET: -COntext=1; The packet was dropped by ASPF for nonexistent zone pair. **Src-ZOne=-, Dst-ZOne=-**;If-In=GigabitEthernet1/0/1(2), If-Out=(0), VLAN-In=10, VLAN-Out=100; Packet Info:Src-IP=192.168.1.10, Dst-IP=192.168.1.100, VPN-Instance=none,Src-Port=2731, Dst-Port=2048. Protocol=ICMP(1).

4、经确认，跨VLAN模式Bridge需要将VLAN加入安全域，而不是接口带VLAN加安全域，配置如下

```
security-zone name Trust
 import vlan 10
#
security-zone name Untrust
 import vlan 100
```

解决方法

将VLAN加入安全域，不需要将接口带VLAN加安全域

```
security-zone name Trust
 import vlan 10
#
security-zone name Untrust
 import vlan 100
```