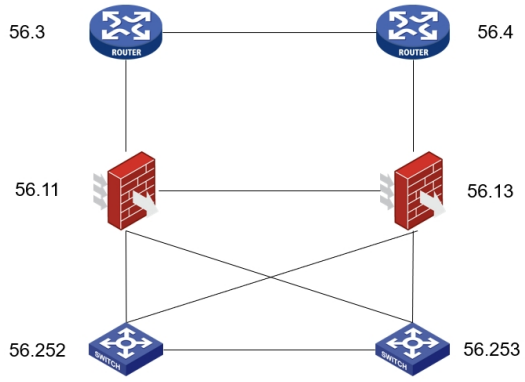
某局点F1090 RBM透明双主 管理备上下行不通问题处理经验案例

双机热备 透明模式 刁勇 2024-05-30 发表

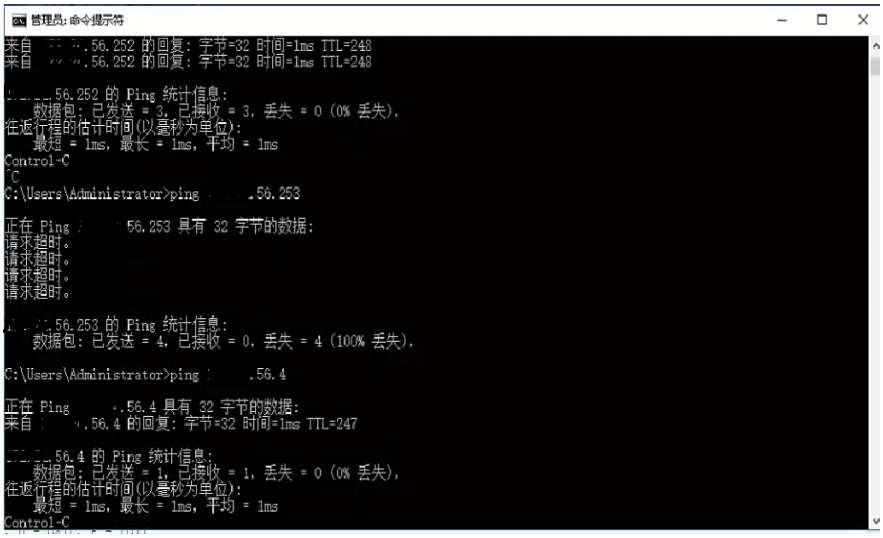
组网及说明

拓扑如下，两台F1090RBM透明双主，上行出口路由器，下行核心交换机，防火墙上下行分别是聚合口1和聚合口2：



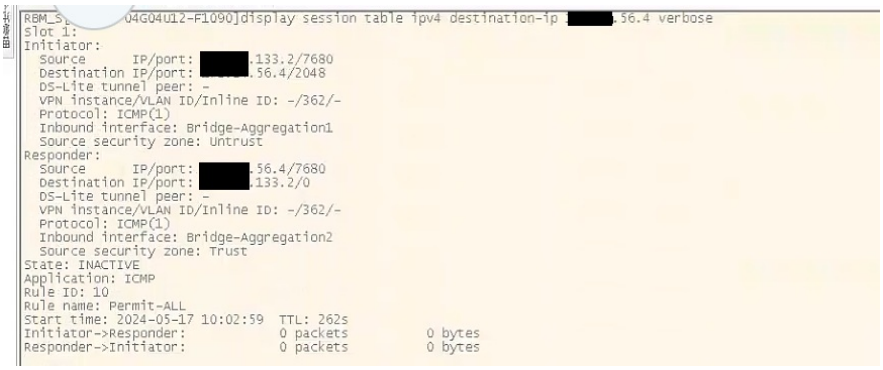
问题描述

ping管理备（56.13）的上下行不通：



过程分析

以56.4为例，查看会话：



debug查看发现反向报文被ASPF策略丢弃了：

May 17 16:02:50:211 2024 CZ-CJ-F04G04U12-F1090 FILTER/7/PACKET: -COntext=1; The packet is permitted. Src-ZOne=Trust, Dst-ZOne=Untrust;If-In=Bridge-Aggregation2(328), If-Out=Bridge-Aggregation1(327), VLAN-In=364, VLAN-Out=364; Packet Info:Src-IP=X.X.56.4, Dst-IP=X.X.133.2, VPN-I

nstance=, Src-MacAddr=X-X-X,Src-Port=0, Dst-Port=0, Protocol=ICMP(1), Application=invalid(0),Terminal=invalid(0), SecurityPolicy=Permit-ALL, Rule-ID=10.
*May 17 16:02:50:211 2024 CZ-CJ-F04G04U12-F1090 ASPF/7/PACKET: -COntext=1;The first packet was dropped by ASPF for invalid status. Src-ZOne=Trust, Dst-ZOne=Untrust;If-In=Bridge-Aggregation2(328), If-Out=Bridge-Aggregation1(327), VLAN-In=364, VLAN-Out=364; Packet Info:Src-IP=X.X.56.4, Dst-IP=X.X.133.2, VPN-Instance=none, Src-Port=7680, Dst-Port=0. Protocol=ICMP(1).
查看debug回显信息，确认不存在来回流量转发方式不同，尝试修改会话模式为宽松模式依旧不行
再次对比发现来回VLAN不一致，会话中正向报文vlan362，debug中反向报文vlan364
设备上聚合口是放通了vlan361 to 370：

```
interface Bridge-Aggregation1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 361 to 370
 link-aggregation mode dynamic
#
interface Bridge-Aggregation2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 361 to 370
 link-aggregation mode dynamic
```

解决方法

使用undo mac fast-forwarding check-vlan-id 命令关闭快速二层转发时对VLAN ID字段的检查功能

1.2.4 mac fast-forwarding check-vlan-id

mac fast-forwarding check-vlan-id命令用来开启快速二层转发时对VLAN ID字段的检查功能。

undo mac fast-forwarding check-vlan-id命令用来关闭快速二层转发时对VLAN ID字段的检查功能。

【命令】

mac fast-forwarding check-vlan-id

undo mac fast-forwarding check-vlan-id

【缺省情况】

快速二层转发时对VLAN ID字段的检查功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

本功能处于开启状态时，二层转发在查找快速转发表时将检查VLAN ID是否匹配，数据流的VLAN ID与快速转发表中不一致时则判定为与表项不匹配。

报文携带的VLAN ID是设备判断其所属TCP会话的依据之一。在防火墙双机热备的组网环境下，有时需要报文在主备设备间传递后仍可以匹配到同一个会话中，而主备设备上报文入接口所属VLAN可能不同，此时可以关闭对VLAN ID的检查以保证报文在主备设备之间传递之后能够匹配到同一会话。

【举例】

开启快速二层转发时对VLAN ID字段的检查功能。

```
<Sysname> system-view
[Sysname] mac fast-forwarding check-vlan-id
```