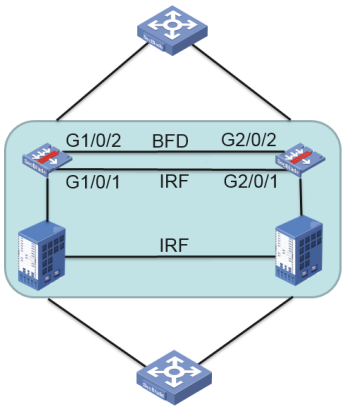
SecBlade III FW使用面板口做BFD MAD检测CPU利用率高经验案例

IRF BFD **茆新楼** 2018-12-11 发表

组网及说明



问题描述

两台S7510E上分别插了一块SecBlade III FW板卡，S7510E之间做了IRF，SecBlade III FW之间做了IRF。SecBlade III FW的面板口G1/0/1作为 IRF端口，G1/0/2作为BFD MAD检测口。

部署完成后，发现无业务情况下插卡的CPU利用率很高：

==========display cpu==========

Slot 1 CPU 0 CPU usage:

86% in last 5 seconds

85% in last 1 minute

85% in last 5 minutes

过程分析

1、通过display process slot 1发现CPU主要被如下进程所使用：

==========display process slot 1==========

JID	PID	%CPU	%MEM	STAT	PRI	TTY	HH:MM:SS	COMMAND
350	350	**3.0**	0.0	R	100	-	03:14:45	[kdrvdp4]
351	351	**3.0**	0.0	R	100	-	03:16:20	[kdrvdp5]
……								
376	376	**2.5**	0.0	R	100	-	02:49:13	[kdrvdp30]

可以看出转发进程高，但是现场目前处于测试阶段，没有大规模业务。

此时检查插卡的IRF端口发现广播报文占总报文数100%：

GigabitEthernet1/0/1

Current state: UP

IP packet frame type: Ethernet II, hardware address: dcda-XXXX-6e58

Description: GigabitEthernet1/0/1 Interface

Bandwidth: 1000000 kbps

Last 300 second input: 103393 packets/sec 38166431 bytes/sec 32%

Last 300 second output: 102988 packets/sec 38102748 bytes/sec 32%

Input (total): **1337338548 packets**, 491039513185 bytes

0 unicasts, **1337338548 broadcasts**, 0 multicasts, 0 pauses

Output (total): **1343436141 packets**, 494919527158 bytes

0 unicasts, **1343436141 broadcasts**, 0 multicasts, 0 pauses

将G1/0/2口shutdown后，CPU立刻恢复正常，一般情况下接口广播包多可能是设备上出现了环路。

查看BFD MAD接口相关配置如下：

```
interface Vlan-interface4090
 mad bfd enable
 mad ip address 1.1.1.17 255.255.255.0 member 1
 mad ip address 1.1.1.18 255.255.255.0 member 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 4090
 undo stp enable
```

```
#
interface GigabitEthernet2/0/2
 port link-mode bridge
 port access vlan 4090
 undo stp enable
```

通过检查以上配置，按照交换机的BFD MAD检测配置思路来看是没有问题的。经确认，目前防火墙插卡配置BFD MAD检测较为特殊，MAD检测的物理端口需要使用三层聚合口的方式：将MAD检测的物理口加入到三层聚合口中，并将三层聚合口放入安全域，放通该安全域到local域以及local域到该安全域。

解决方法

将BFD MAD检测物理端口加入三层聚合口，并将聚合口加入安全域：

```
#
interface route-aggregation 3
#
interface gigabitethernet 1/0/2
  port link-aggregation group 3
interface gigabitethernet 2/0/2
  port link-aggregation group 3
#
interface route-aggregation 3
  mad bfd enable
  mad ip address 1.1.1.17 24 member 1
  mad ip address 1.1.1.18 24 member 2
#
security-zone name trust
  import interface route-aggregation 3
#
acl number 2000
  rule 0 permit source 1.1.1.0 0.0.0.255
#
zone-pair security source trust destination loacl
  packet-filter 2000
#
zone-pair security source local destination trust
  packet-filter 2000
```