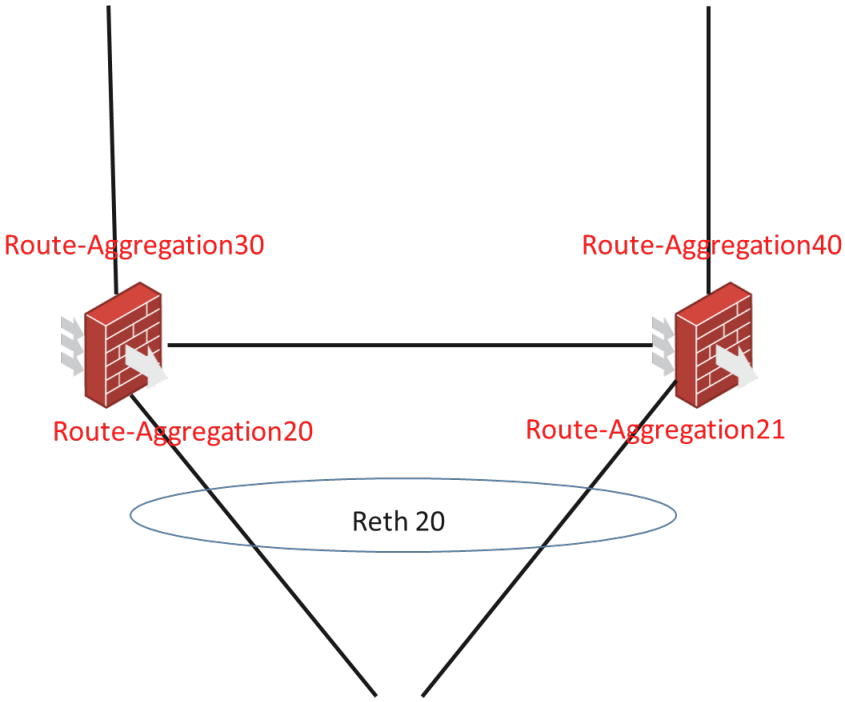
防火墙冗余组不回切典型案例分析

IRF 冗余组 Track 孔凡安 2022-09-27 发表

组网及说明



如图所示，两台防火墙堆叠+冗余主备部署。上行依靠路由优先级实现主备，下行依靠冗余口实现流量主备。

上下行均为单框聚合，每个聚合口的成员口均为两个。

问题描述

测试冗余组切换情况时，shutdown、undo shutdown主框接口，冗余组主备切换以及回切正常。
重启1框后，1框接口无法UP，冗余组不回切。
关键配置：

```
#
redundancy group aaa
 member interface Reth20
 node 1
  bind slot 1
  priority 255
  track 11 interface Route-Aggregation30
  track 12 interface Route-Aggregation20
  node-member interface Ten-GigabitEthernet1/2/4
  node-member interface Ten-GigabitEthernet1/2/5
 node 2
  bind slot 2
  priority 50
  track 21 interface Route-Aggregation40
  track 22 interface Route-Aggregation21
  node-member interface Ten-GigabitEthernet2/2/4
  node-member interface Ten-GigabitEthernet2/2/5
#
```

注：Ten-GigabitEthernet1/2/4与 Ten-GigabitEthernet1/2/5为Route-Aggregation30的成员口，Ten-GigabitEthernet2/2/4与Ten-GigabitEthernet2/2/5为 Route-Aggregation40的成员口

过程分析

slot1重启后，冗余组状态：

```
Redundancy group aaa (ID 1):
  Node ID      Slot          Priority   Status        Track weight
  1            Slot1         255        Secondary     -255
  2            Slot2         50         Primary       255

Preempt delay time remained     : 0    sec
Preempt delay timer setting     : 60   sec
Remaining hold-down time        : 0    sec
Hold-down timer setting         : 1    sec
Manual switchover request       : No

Member interfaces:
    Reth20

Node 1:
  Node member     Physical status
    XGE1/2/4      DOWN(redundancy down)
  Track info:
    Track    Status          Reduced weight     Interface
    11       Negative(Faulty) 255               RAGG30
    12       Negative         255               RAGG20
Node 2:
  Node member     Physical status
    XGE2/2/4      UP
  Track info:
    Track    Status          Reduced weight     Interface
    21       Positive        255               RAGG40
    22       Positive        255               RAGG21
```

发现slot1的权值为负值，然后查看上下行物理接口状态，发现被冗余down了。

例如：

```
Ten-GigabitEthernet1/2/2
Current state: ETH-rddc Shutdown
Line protocol state: DOWN(LAGG)
Description: TO_HW_S6800
Maximum transmission unit: 1500
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: c4c0-6317-54c6
IPv6 packet frame type: Ethernet II, hardware address: c4c0-6317-54c6
Media type is optical fiber, loopback not set, promiscuous mode not set
Speed Negotiation, Duplex Negotiation, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
Last link flapping: Never
Last clearing of counters: Never
Current system time:2022-09-06 09:50:37 BeiJing+08:00:00
Last time when physical state changed to up:-
Last time when physical state changed to down:2022-09-06 09:45:37 BeiJing+08:00:00
 Peak input rate: 0 bytes/sec, at 00-00-00 00:00:00
 Peak output rate: 0 bytes/sec, at 00-00-00 00:00:00
 Last 300 second input: 0 packets/sec 0 bytes/sec -%
[ZWY-F08-F5030-INTERNET-1]disp link-a v ro30
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
```

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

原因分析：slot 1重启以后，如果1/2/4和1/2/5口up了，但是聚合口由于动态聚合，没有及时up，聚合口就作为故障口，触发冗余组主备切换，1/2/4和1/2/5就作为成员接口被冗余down，导致Route-Aggregation30永远无法up，无法触发主备倒回。track故障口应该配置1/2/4和1/2/5，不能配置聚合口

解决方法

上行接口配置track物理口，而不是聚合口。

```
redundancy group aaa
member interface Reth20
node 1
  bind slot 1
  priority 255
 track 11 reduced 150 interface Ten-GigabitEthernet1/2/4
   track 12 interface Route-Aggregation20
   track 13 reduced 150 interface Ten-GigabitEthernet1/2/5
   node-member interface Ten-GigabitEthernet1/2/4
   node-member interface Ten-GigabitEthernet1/2/5
node 2
  bind slot 2
  priority 50
  track 21 reduced 150 interface Ten-GigabitEthernet2/2/4
  track 22 interface Route-Aggregation21
  track 23 reduced 150 interface Ten-GigabitEthernet2/2/5
  node-member reduced 150 interface Ten-GigabitEthernet2/2/4
  node-member reduced 150 interface Ten-GigabitEthernet2/2/5
```