防火墙二层部署冗余组切换无法实现回切问题分析

冗余组 **孔凡安** 2022-08-10 发表

组网及说明

不涉及

问题描述

防火墙组网二层部署，堆叠+冗余组配置，利用二层聚合配置最大选中数实现业务主备处理。

关键配置如下：

```
#
track 1 interface Ten-GigabitEthernet1/1/0 physical
#
track 2 interface Ten-GigabitEthernet2/1/0 physical
#
track 3 interface Ten-GigabitEthernet1/1/1 physical
#
track 4 interface Ten-GigabitEthernet2/1/1 physical
#
#
interface Bridge-Aggregation6
 port access vlan 10
 link-aggregation mode dynamic
 link-aggregation selected-port maximum 1
#
interface Bridge-Aggregation16
 port access vlan 10
 link-aggregation mode dynamic
 link-aggregation selected-port maximum 1
#
interface Ten-GigabitEthernet1/1/0
 port link-mode bridge
 port access vlan 10
  link-aggregation port-priority 50
 port link-aggregation group 6
#
interface Ten-GigabitEthernet1/1/1
 port link-mode bridge
 port access vlan 10
 link-aggregation port-priority 50
 port link-aggregation group 16
#
interface Ten-GigabitEthernet2/1/0
 port link-mode bridge
 port access vlan 10
 link-aggregation port-priority 100
 port link-aggregation group 6
#
interface Ten-GigabitEthernet2/1/1
 port link-mode bridge
 port access vlan 10
 link-aggregation port-priority 100
 port link-aggregation group 16
#
#
redundancy group aaa
 node 1
  bind slot 1
  priority 100
  track 1 interface Ten-GigabitEthernet1/1/0
  track 3 interface Ten-GigabitEthernet1/1/1
  node-member interface Ten-GigabitEthernet1/1/0
  node-member interface Ten-GigabitEthernet1/1/1
 node 2
  bind slot 2
  priority 50
```

```
 track 2 interface Ten-GigabitEthernet2/1/0
 track 4 interface Ten-GigabitEthernet2/1/1
 node-member interface Ten-GigabitEthernet2/1/0
 node-member interface Ten-GigabitEthernet2/1/1
#
```

过程分析

初始的状态组网正常，当1框的接口恢复UP后，冗余组1 min缺省实现回切，但是查看聚合口的成员接口，发现还是2框的接口被选中。

```
[H3C]display redundancy group aaa
Redundancy group aaa (ID 1):
 Node ID    Slot        Priority  Status     Track weight
 1          Slot1       100       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
 Track info:
  Track   Status      Reduced weight   Interface
  1       Positive    255              XGE1/1/0
  3       Positive    255              XGE1/1/1
 Node 1:
  Node member     Physical status
  XGE1/1/0        UP
  XGE1/1/1        UP
 Node 2:
  Node member     Physical status
  XGE2/1/0        UP
  XGE2/1/1        UP
```

当把1框的某一个接口down掉后，冗余组主切换到2框：

```
[H3C]display redundancy group aaa
Redundancy group aaa (ID 1):
 Node ID    Slot        Priority  Status     Track weight
 1          Slot1       100       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:
 Node 1:
  Node member     Physical status
  XGE1/1/0        UP
  XGE1/1/1        DOWN(redundancy down)
 Track info:
  Track   Status      Reduced weight   Interface
  1       Negative(Faulty) 255         XGE1/1/0
  3       Negative    255              XGE1/1/1
 Node 2:
  Node member     Physical status
  XGE2/1/0        UP
  XGE2/1/1        UP
 Track info:
  Track   Status      Reduced weight   Interface
  2       Positive    255              XGE2/1/0
  4       Positive    255              XGE2/1/1
```

```
[H3C-Ten-GigabitEthernet1/1/0]display link-aggregation verbose
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

Node 1:
Aggregate Interface: Bridge-Aggregation6
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 782c-29c4-0800
Local:
  Port            Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  XGE1/1/0        U       50       5         {ACD}
  XGE2/1/0        S       100      5         {ACDEF}
```

Remote:
XGE2/1/1 UP
Actor Partner Priority Oper-Key SystemID Flag
Track info:

Track Status Reduced weight Interface
XGE1/1/0 1 10 321 0x8000, 9c52-f882-7f51 {AC}
XGE2/1/0 2 100 321 0x8000, 9c52-f882-7f51 {ACDEF}
Positive 295
Positive 285
XGE2/1/1

解决方法

链路聚合没有抢占机制，1框的接口UP后，不会参与抢占，所以聚合选中接口还在2框。
需要人工干预，使聚合组选中接口回到1框。

Aggregate Interface: Bridge-Aggregation1.6
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 782c-29c4-0800
Local:
Port Status Priority Oper-Key Flag

XGE1/1/1 U 50 4 {ACD}
XGE2/1/1 S 100 4 {ACDEF}
Remote:
Actor Partner Priority Oper-Key SystemID Flag

XGE1/1/1 3 10 577 0x8000, 9c52-f882-7f51 {AC}
XGE2/1/1 4 100 577 0x8000, 9c52-f882-7f51 {ACDEF}