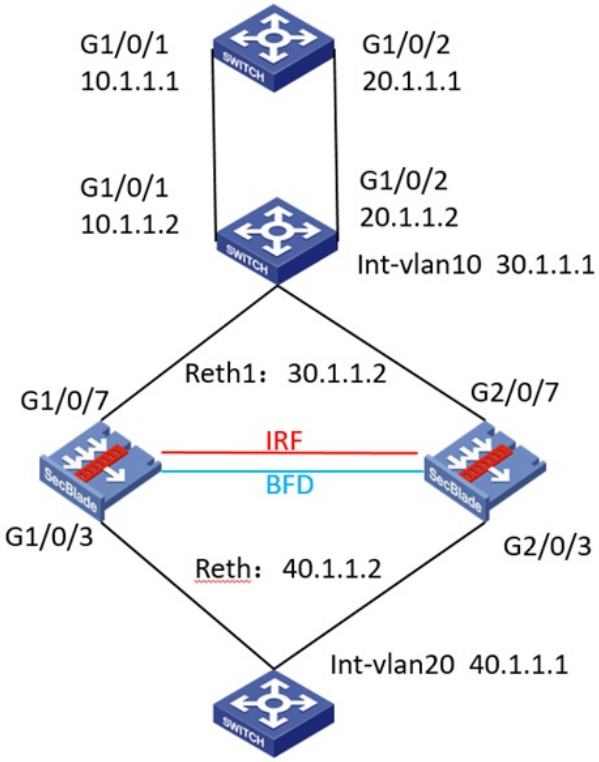
nqa+track下一跳实现防火墙主备切换

冗余组 IRF NQA Track **陈启敏** 2021-02-28 发表

组网及说明

组网以及说明：



问题描述

组网要求：客户现网是F1070的防火墙做了IRF，双出口电信、联通接在堆叠防火墙上行交换机上，现在想配置冗余组实现主备切换，另外客户反馈想通过对上行检测下一跳地址来切换而不仅仅是接口物理状态。

过程分析

1、防火墙堆叠配置，交换机上的ip地址、vlan接口配置、路由等自行配置

2、在防火墙上下行各自配置冗余口，放入冗余组中，以便进行track联动实现主备切换

3、track项为track下一跳的地址，连续四次不可达则启动链路切换

解决方法

配置如下

```
#堆叠防火墙上配置
#track项配置
track 1 nqa entry admin test1 reaction 1  //nqa与track 联动，检测上行链路下一跳是否可达
#
track 2 interface GigabitEthernet1/0/3 physical  //track防火墙下行链路物理状态
#
track 3 nqa entry admin test2 reaction 2 //nqa与track 联动，检测上行链路下一跳是否可达
#
track 4 interface GigabitEthernet2/0/3 physical  //track防火墙下行链路物理状态
#

#
nqa entry admin test1 //配置nqa检测项，检测下一跳地址为电信网段地址，频率为100ms一次，连续探测失败达到4次阈值时，就触track模块联动。
 type icmp-echo
  destination ip 10.1.1.1
  frequency 100
  reaction 1 checked-element probe-fail threshold-type consecutive 4 action-type trigger-only
#
nqa entry admin test2
 type icmp-echo
  destination ip 20.1.1.1
  frequency 100
  reaction 2 checked-element probe-fail threshold-type consecutive 4 action-type trigger-only
#
 nqa schedule admin test1 start-time now lifetime forever  /用来配置测试组的启动时间为当前和持续时间为永久。
 nqa schedule admin test2 start-time now lifetime forever
#
interface Reth1    //配置防火墙上下行冗余口与其成员接口
 ip address 30.1.1.2 255.255.255.0
 member interface GigabitEthernet1/0/7 priority 255
 member interface GigabitEthernet2/0/7 priority 50
#
interface Reth2
 ip address 40.1.1.2 255.255.255.0
 member interface GigabitEthernet1/0/3 priority 255
 member interface GigabitEthernet2/0/3 priority 50

#安全域配置
security-zone name Trust
 import interface Reth1
 import interface Reth2

#路由配置
 ip route-static 0.0.0.0 0 30.1.1.1
 ip route-static 40.1.1.0 24 40.1.1.1

#冗余组配置
redundancy group aaa
 member interface Reth1
 member interface Reth2
 node 1
  bind slot 1
  priority 100
  track 1 interface GigabitEthernet1/0/7
  track 2 interface GigabitEthernet1/0/3
 node 2
  bind slot 2
```

```
priority 50
track 3 interface GigabitEthernet2/0/7
```