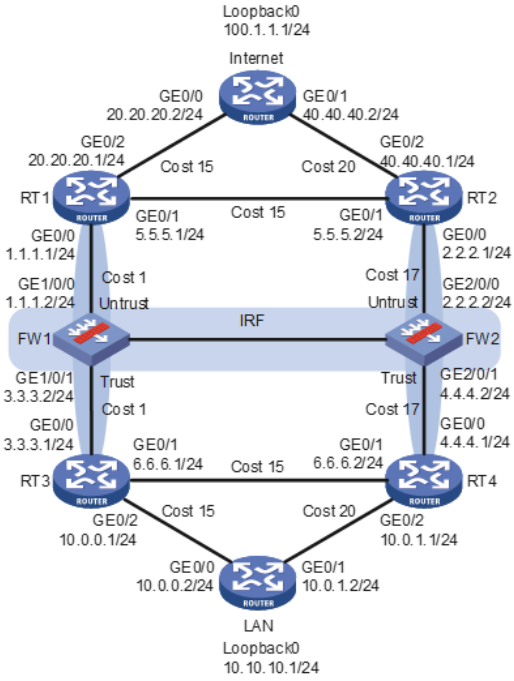
V7防火墙冗余组结合OSPF实现主备切换的典型配置案例

冗余组 冗余口 **孙轶宁** 2020-08-29 发表

组网及说明



防火墙主备组网，使用冗余组，保证10.10.10.1与100.1.1.1互通，图中防火墙的接口除IRF线路外，断一条线，或者故障一个设备都能保持流量不跨框。

配置步骤

FW配置

```
irf member 1 priority 32
 irf member 2 priority 1
#
 router id 1.1.1.1
#
track 1 interface GigabitEthernet1/0/0 physical
#
track 2 interface GigabitEthernet2/0/0 physical
#
track 3 interface GigabitEthernet1/0/1 physical
#
track 4 interface GigabitEthernet2/0/1 physical
#
ospf 1
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
  network 2.2.2.0 0.0.0.255
  network 3.3.3.0 0.0.0.255
  network 4.4.4.0 0.0.0.255
#
irf-port 1/1
 port group interface GigabitEthernet1/0/23
#
irf-port 2/2
 port group interface GigabitEthernet2/0/23
#
interface GigabitEthernet1/0/0
 port link-mode route
 combo enable copper
 ip address 1.1.1.2 255.255.255.0
 ospf network-type p2p
```

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 ip address 3.3.3.2 255.255.255.0
 ospf network-type p2p
#
interface GigabitEthernet2/0/0
 port link-mode route
 combo enable copper
 ip address 2.2.2.2 255.255.255.0
 ospf cost 17
 ospf network-type p2p
#
interface GigabitEthernet2/0/1
 port link-mode route
 combo enable copper
 ip address 4.4.4.2 255.255.255.0
 ospf cost 17
 ospf network-type p2p
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
 import interface GigabitEthernet2/0/1
#
security-zone name Untrust
 import interface GigabitEthernet1/0/0
 import interface GigabitEthernet2/0/0
#
redundancy group int1
 node 1
  bind slot 1
  priority 100
  track 1 interface GigabitEthernet1/0/0
  track 3 interface GigabitEthernet1/0/1
  node-member interface GigabitEthernet1/0/0
  node-member interface GigabitEthernet1/0/1
 node 2
  bind slot 2
  priority 50
  track 2 interface GigabitEthernet2/0/0
  track 4 interface GigabitEthernet2/0/1
  node-member interface GigabitEthernet2/0/0
  node-member interface GigabitEthernet2/0/1
#
 session synchronization enable
 session synchronization dns http
#
security-policy ip
 rule 10 name permit
  action pass
  source-zone Local
  source-zone Trust
  source-zone Untrust
  destination-zone Local
  destination-zone Trust
  destination-zone Untrust
RT1配置
router id 2.2.2.2
#
ospf 1
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
  network 5.5.5.0 0.0.0.255
```

```
  network 20.20.20.0 0.0.0.255
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 1.1.1.1 255.255.255.0
 ospf network-type p2p
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 5.5.5.1 255.255.255.0
 ospf cost 15
 ospf network-type p2p
#
interface GigabitEthernet0/2
 port link-mode route
 combo enable copper
 ip address 20.20.20.1 255.255.255.0
 ospf cost 15
 ospf network-type p2p
```

RT2配置

```
router id 3.3.3.3
#
ospf 1
 area 0.0.0.0
  network 2.2.2.0 0.0.0.255
  network 5.5.5.0 0.0.0.255
  network 40.40.40.0 0.0.0.255
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 2.2.2.1 255.255.255.0
 ospf cost 17
 ospf network-type p2p
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 5.5.5.2 255.255.255.0
 ospf cost 15
 ospf network-type p2p
#
interface GigabitEthernet0/2
 port link-mode route
 combo enable copper
 ip address 40.40.40.1 255.255.255.0
 ospf cost 20
 ospf network-type p2p
```

RT3配置

```
router id 4.4.4.4
#
ospf 1
 area 0.0.0.0
  network 3.3.3.0 0.0.0.255
  network 6.6.6.0 0.0.0.255
  network 10.0.0.0 0.0.0.255
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 3.3.3.1 255.255.255.0
 ospf network-type p2p
```

#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 6.6.6.1 255.255.255.0
 ospf cost 15
 ospf network-type p2p
#
interface GigabitEthernet0/2
 port link-mode route
 combo enable copper
 ip address 10.0.0.1 255.255.255.0
 ospf cost 15
 ospf network-type p2p
RT4配置
router id 5.5.5.5
#
ospf 1
 area 0.0.0.0
  network 4.4.4.0 0.0.0.255
  network 6.6.6.0 0.0.0.255
  network 10.0.1.0 0.0.0.255
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 4.4.4.1 255.255.255.0
 ospf cost 17
 ospf network-type p2p
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 6.6.6.2 255.255.255.0
 ospf cost 15
 ospf network-type p2p
#
interface GigabitEthernet0/2
 port link-mode route
 combo enable copper
 ip address 10.0.1.1 255.255.255.0
 ospf cost 20
 ospf network-type p2p
LAN配置
router id 6.6.6.6
#
ospf 1
 silent-interface LoopBack0
 area 0.0.0.0
  network 10.0.0.0 0.0.0.255
  network 10.0.1.0 0.0.0.255
  network 10.10.10.1 0.0.0.0
#
interface LoopBack0
 ip address 10.10.10.1 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 10.0.0.2 255.255.255.0
 ospf cost 15
 ospf network-type p2p
#
interface GigabitEthernet0/1

```
 port link-mode route
 combo enable copper
 ip address 10.0.1.2 255.255.255.0
 ospf cost 20
 ospf network-type p2p
Internet配置
router id 7.7.7.7
#
ospf 1
 silent-interface LoopBack0
 area 0.0.0.0
  network 20.20.20.0 0.0.0.255
  network 40.40.40.0 0.0.0.255
  network 100.1.1.1 0.0.0.0
#
interface LoopBack0
 ip address 100.1.1.1 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 20.20.20.2 255.255.255.0
 ospf cost 15
 ospf network-type p2p
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 40.40.40.2 255.255.255.0
 ospf cost 20
 ospf network-type p2p
```

测试结果：

切换前冗余组的状态，可以看到node1的两条链路即左边的链路为主链路。

```
<FW-IRF>dis redundancy group int1
Redundancy group int1 (ID 1):
  Node ID      Slot          Priority   Status        Track weight
  1            Slot1         100        Primary       255
  2            Slot2         50         Secondary     255

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

Member interfaces:

Node 1:
  Node member     Physical status
    GE1/0/0       UP
    GE1/0/1       UP
  Track info:
    Track    Status          Reduced weight     Interface
    1        Positive        255                GE1/0/0
    3        Positive        255                GE1/0/1
Node 2:
  Node member     Physical status
    GE2/0/0       UP
    GE2/0/1       UP
  Track info:
    Track    Status          Reduced weight     Interface
    2        Positive        255                GE2/0/0
    4        Positive        255                GE2/0/1
```

切换前LAN的路由以及Internet的路由，可以看到路由的出接口都是左边的接口。

<LAN>dis ip ro

Destinations : 26 Routes : 26

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.0/24	O_INTRA	10	17	10.0.0.1	GE0/0
2.2.2.0/24	O_INTRA	10	33	10.0.0.1	GE0/0
3.3.3.0/24	O_INTRA	10	16	10.0.0.1	GE0/0
4.4.4.0/24	O_INTRA	10	33	10.0.0.1	GE0/0
5.5.5.0/24	O_INTRA	10	32	10.0.0.1	GE0/0
6.6.6.0/24	O_INTRA	10	30	10.0.0.1	GE0/0
10.0.0.0/24	Direct	0	0	10.0.0.2	GE0/0
10.0.0.0/32	Direct	0	0	10.0.0.2	GE0/0
10.0.0.2/32	Direct	0	0	127.0.0.1	InLoop0
10.0.0.255/32	Direct	0	0	10.0.0.2	GE0/0
10.0.1.0/24	Direct	0	0	10.0.1.2	GE0/1
10.0.1.0/32	Direct	0	0	10.0.1.2	GE0/1
10.0.1.2/32	Direct	0	0	127.0.0.1	InLoop0
10.0.1.255/32	Direct	0	0	10.0.1.2	GE0/1
10.10.10.1/32	Direct	0	0	127.0.0.1	InLoop0
20.20.20.0/24	O_INTRA	10	32	10.0.0.1	GE0/0
40.40.40.0/24	O_INTRA	10	52	10.0.0.1	GE0/0
100.1.1.1/32	O_INTRA	10	32	10.0.0.1	GE0/0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

<Internet>dis ip ro

Destinations : 26 Routes : 26

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.0/24	O_INTRA	10	16	20.20.20.1	GE0/0
2.2.2.0/24	O_INTRA	10	33	20.20.20.1	GE0/0
3.3.3.0/24	O_INTRA	10	17	20.20.20.1	GE0/0
4.4.4.0/24	O_INTRA	10	33	20.20.20.1	GE0/0
5.5.5.0/24	O_INTRA	10	30	20.20.20.1	GE0/0
6.6.6.0/24	O_INTRA	10	32	20.20.20.1	GE0/0
10.0.0.0/24	O_INTRA	10	32	20.20.20.1	GE0/0
10.0.1.0/24	O_INTRA	10	52	20.20.20.1	GE0/0
10.10.10.1/32	O_INTRA	10	32	20.20.20.1	GE0/0
20.20.20.0/24	Direct	0	0	20.20.20.2	GE0/0
20.20.20.0/32	Direct	0	0	20.20.20.2	GE0/0
20.20.20.2/32	Direct	0	0	127.0.0.1	InLoop0
20.20.20.255/32	Direct	0	0	20.20.20.2	GE0/0
40.40.40.0/24	Direct	0	0	40.40.40.2	GE0/1
40.40.40.0/32	Direct	0	0	40.40.40.2	GE0/1
40.40.40.2/32	Direct	0	0	127.0.0.1	InLoop0
40.40.40.255/32	Direct	0	0	40.40.40.2	GE0/1
100.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

切换过程前后的ping包，在ping过程中shutdown RT1的G0/0口，可以看到切换成功，切换过程中存在

少量丢包。
[RT1]int g0/0
[RT1-GigabitEthernet0/0]sh
[RT1-GigabitEthernet0/0]%Aug 12 16:32:10:186 2018 RT1 OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 1.1.1.2(GigabitEthernet0/0) changed from FULL to DOWN.
%Aug 12 16:32:10:187 2018 RT1 IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet0/0 changed to down.
%Aug 12 16:32:10:187 2018 RT1 IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet0/0 changed to down.
切换后的冗余组状态，可以看到主链路已经切换到node2即右边的链路，node1的链路已被down。
<FW-IRF>%Aug 12 16:38:44:713 2018 FW-IRF IFNET/3/PHY_UPDOWN: -COntext=1; Physical state on the interface GigabitEthernet1/0/0 changed to down.
%Aug 12 16:38:44:713 2018 FW-IRF IFNET/5/LINK_UPDOWN: -COntext=1; Line protocol state on the interface GigabitEthernet1/0/0 changed to down.
%Aug 12 16:38:44:715 2018 FW-IRF RDDC/5/RDDC_ACTIVENODE_CHANGE: -COntext=1; Redundancy group int1 active node changed to node 2 (slot 2), because of node's weight changed.
%Aug 12 16:38:44:717 2018 FW-IRF OSPF/5/OSPF_NBR_CHG: -COntext=1; OSPF 1 Neighbor 1.1.1.1(GigabitEthernet1/0/0) changed from FULL to DOWN.
%Aug 12 16:38:44:722 2018 FW-IRF IFNET/3/PHY_UPDOWN: -COntext=1; Physical state on the interface GigabitEthernet1/0/1 changed to down.
%Aug 12 16:38:44:722 2018 FW-IRF IFNET/5/LINK_UPDOWN: -COntext=1; Line protocol state on the interface GigabitEthernet1/0/1 changed to down.
%Aug 12 16:38:44:722 2018 FW-IRF OSPF/5/OSPF_NBR_CHG: -COntext=1; OSPF 1 Neighbor 3.3.3.1(GigabitEthernet1/0/1) changed from FULL to DOWN.

<FW-IRF>dis redundancy group int1
Redundancy group int1 (ID 1):
 Node ID Slot Priority Status Track weight
 1 Slot1 100 Secondary -255
 2 Slot2 50 Primary 255

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

Member interfaces:

Node 1:
 Node member Physical status
  GE1/0/0 DOWN
  GE1/0/1 DOWN(redundancy down)
 Track info:
  Track Status Reduced weight Interface
  1 Negative(Faulty) 255 GE1/0/0
  3 Negative 255 GE1/0/1
Node 2:
 Node member Physical status
  GE2/0/0 UP
  GE2/0/1 UP
 Track info:
  Track Status Reduced weight Interface
  2 Positive 255 GE2/0/0
4 Positive 255 GE2/0/1
此时LAN的路由以及Internet的路由已经切换到右边的链路
<LAN>dis ip ro

Destinations : 24 Routes : 24

Destination/Mask Proto Pre Cost NextHop Interface
0.0.0.0/32 Direct 0 0 127.0.0.1 InLoop0
2.2.2.0/24 O_INTRA 10 54 10.0.1.1 GE0/1
4.4.4.0/24 O_INTRA 10 37 10.0.1.1 GE0/1

```
5.5.5.0/24         O_INTRA 10  69          10.0.1.1        GE0/1
6.6.6.0/24         O_INTRA 10  30          10.0.0.1        GE0/0
10.0.0.0/24        Direct  0   0           10.0.0.2        GE0/0
10.0.0.0/32        Direct  0   0           10.0.0.2        GE0/0
10.0.0.2/32        Direct  0   0           127.0.0.1       InLoop0
10.0.0.255/32      Direct  0   0           10.0.0.2        GE0/0
10.0.1.0/24        Direct  0   0           10.0.1.2        GE0/1
10.0.1.0/32        Direct  0   0           10.0.1.2        GE0/1
10.0.1.2/32        Direct  0   0           127.0.0.1       InLoop0
10.0.1.255/32      Direct  0   0           10.0.1.2        GE0/1
10.10.10.1/32      Direct  0   0           127.0.0.1       InLoop0
20.20.20.0/24      O_INTRA 10  84          10.0.1.1        GE0/1
40.40.40.0/24      O_INTRA 10  74          10.0.1.1        GE0/1
100.1.1.1/32       O_INTRA 10  74          10.0.1.1        GE0/1
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
<Internet>dis ip ro

Destinations : 24       Routes : 24

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
2.2.2.0/24         O_INTRA 10  37          40.40.40.1      GE0/1
4.4.4.0/24         O_INTRA 10  54          40.40.40.1      GE0/1
5.5.5.0/24         O_INTRA 10  30          20.20.20.1      GE0/0
6.6.6.0/24         O_INTRA 10  69          40.40.40.1      GE0/1
10.0.0.0/24        O_INTRA 10  84          40.40.40.1      GE0/1
10.0.1.0/24        O_INTRA 10  74          40.40.40.1      GE0/1
10.10.10.1/32      O_INTRA 10  74          40.40.40.1      GE0/1
20.20.20.0/24      Direct  0   0           20.20.20.2      GE0/0
20.20.20.0/32      Direct  0   0           20.20.20.2      GE0/0
20.20.20.2/32      Direct  0   0           127.0.0.1       InLoop0
20.20.20.255/32    Direct  0   0           20.20.20.2      GE0/0
40.40.40.0/24      Direct  0   0           40.40.40.2      GE0/1
40.40.40.0/32      Direct  0   0           40.40.40.2      GE0/1
40.40.40.2/32      Direct  0   0           127.0.0.1       InLoop0
40.40.40.255/32    Direct  0   0           40.40.40.2      GE0/1
100.1.1.1/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
再将RT1的G0/0口undo shutdown，可以看到冗余组以及路由又切换回去了
[RT1-GigabitEthernet0/0]un sh
[RT1-GigabitEthernet0/0]%Aug 12 16:45:46:685 2018 RT1 IFNET/3/PHY_UPDOWN: Physical state
on the interface GigabitEthernet0/0 changed to up.
%Aug 12 16:45:46:686 2018 RT1 IFNET/5/LINK_UPDOWN: Line protocol state on the interface Giga
bitEthernet0/0 changed to up.
%Aug 12 16:45:46:698 2018 RT1 OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 1.1.1.2(GigabitEther
net0/0) changed from LOADING to FULL.

<FW-IRF>%Aug 12 16:53:12:538 2018 FW-IRF IFNET/3/PHY_UPDOWN: -COntext=1; Physical stat
e on the interface GigabitEthernet1/0/0 changed to up.
%Aug 12 16:53:12:538 2018 FW-IRF IFNET/5/LINK_UPDOWN: -COntext=1; Line protocol state on
the interface GigabitEthernet1/0/0 changed to up.
%Aug 12 16:53:12:552 2018 FW-IRF OSPF/5/OSPF_NBR_CHG: -COntext=1; OSPF 1 Neighbor 1.1.
```

1.1(GigabitEthernet1/0/0) changed from LOADING to FULL.
%Aug 12 16:53:12:552 2018 FW-IRF IFNET/3/PHY_UPDOWN: -COntext=1; Physical state on the int
erface GigabitEthernet1/0/1 changed to up.
%Aug 12 16:53:12:553 2018 FW-IRF IFNET/5/LINK_UPDOWN: -COntext=1; Line protocol state on
the interface GigabitEthernet1/0/1 changed to up.
%Aug 12 16:53:12:555 2018 FW-IRF OSPF/5/OSPF_NBR_CHG: -COntext=1; OSPF 1 Neighbor 3.3.
3.1(GigabitEthernet1/0/1) changed from LOADING to FULL.
%Aug 12 16:54:13:082 2018 FW-IRF RDDC/5/RDDC_ACTIVENODE_CHANGE: -COntext=1;Redun
dancy group int1 active node changed to node 1 (slot 1), because of node's weight changed.

<FW-IRF>dis redundancy group int1
Redundancy group int1 (ID 1):
 Node ID Slot Priority Status Track weight
 1 Slot1 100 Primary 255
 2 Slot2 50 Secondary 255

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

Member interfaces:

Node 1:
 Node member Physical status
  GE1/0/0 UP
  GE1/0/1 UP
 Track info:
  Track Status Reduced weight Interface
  1 Positive 255 GE1/0/0
  3 Positive 255 GE1/0/1
Node 2:
 Node member Physical status
  GE2/0/0 UP
  GE2/0/1 UP
 Track info:
  Track Status Reduced weight Interface
  2 Positive 255 GE2/0/0
4 Positive 255 GE2/0/1

配置关键点

1. 合理规划OSPF的cost值，确保冗余组切换时路由能够正常切换，并避免跨框流量。
2. 每一个冗余组的节点需要绑定其接口所在的slot。
3. 使用Track跟踪物理接口时务必加上physical。
4. 会话同步开启后dns与http的会话需单独开启。