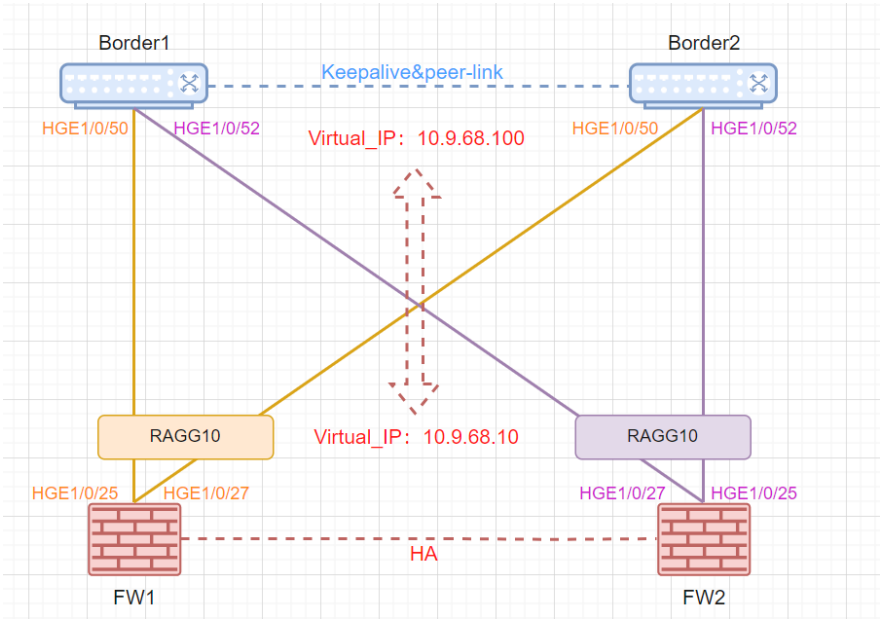
防火墙RBM对接交换机M-LAG典型配置

双机热备 VRRP 孔凡安 2024-01-18 发表

组网及说明



FW配置：FW1与FW2采用RBM组网，M-LAG Border的跨设备二层聚合口与RBM FW设备的设备内三层聚合口对接。FW主设备的设备内三层聚合口编号应与备设备的设备内三层聚合口编号保持一致。防火墙省略安全域和安全策略配置。

Border设备配置：采用M-LAG组网，Border1与Border2之间一条直连链路聚合作为peer-link链路，一条直连链路作为M-LAG MAD链路。

配置步骤

FW配置如下：

	FW1	FW2
HA接口配置	# interface Route-Aggregation1024 ip address 192.168.1.1 255.255.255.252 link-aggregation mode dynamic # 	# interface Route-Aggregation1024 ip address 192.168.1.2 255.255.255.252 link-aggregation mode dynamic #
业务接口配置	# interface HundredGigE1/0/25 port link-mode route port link-aggregation group 10 # interface HundredGigE1/0/27 port link-mode route port link-aggregation group 10 # interface Route-Aggregation10 link-aggregation mode dynamic # interface Route-Aggregation10.10 ip address 10.9.68.1 255.255.255.0 vrrp vrid 10 virtual-ip 10.9.68.10 active vlan-type dot1q vid 10 # 	# interface HundredGigE1/0/25 port link-mode route port link-aggregation group 10 # interface HundredGigE1/0/27 port link-mode route port link-aggregation group 10 # interface Route-Aggregation10 link-aggregation mode dynamic # interface Route-Aggregation10.10 ip address 10.9.68.2 255.255.255.0 vrrp vrid 10 virtual-ip 10.9.68.10 stand by vlan-type dot1q vid 10 #
RBM配置	# remote-backup group backup-mode dual-active data-channel interface Route-Aggregation1024 delay-time 5 local-ip 192.168.1.1 remote-ip 192.168.1.2 device-role primary # 	# remote-backup group backup-mode dual-active data-channel interface Route-Aggregation1024 delay-time 5 local-ip 192.168.1.2 remote-ip 192.168.1.1 device-role secondary #

Border配置：

	Border1	Border2
M-LAG系统参数	m-lag system-mac 0068-0068-0068 m-lag system-number 1 m-lag system-priority 68 m-lag keepalive ip destination 192.168.68.2 source 192.168.68.1	m-lag role priority 65535 m-lag system-mac 0068-0068-0068 m-lag system-number 2 m-lag system-priority 68 m-lag keepalive ip destination 192.168.68.1 source 192.168.68.2
peer-link配置	# interface Bridge-Aggregation1024 port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 20 link-aggregation mode dynamic port m-lag peer-link 1 undo mac-address static source-check enable # 	# interface Bridge-Aggregation1024 port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 20 link-aggregation mode dynamic port m-lag peer-link 1 undo mac-address static source-check enable #

m-lag接口	# vlan 10 # interface HundredGigE1/0/50 port link-mode bridge port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 port link-aggregation group 10 # interface HundredGigE1/0/52 port link-mode bridge port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 port link-aggregation group 20 # interface Bridge-Aggregation10 port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 link-aggregation mode dynamic port m-lag group 10 # interface Bridge-Aggregation20 port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 link-aggregation mode dynamic port m-lag group 20 #	# vlan 10 # interface HundredGigE1/0/50 port link-mode bridge port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 port link-aggregation group 10 # interface HundredGigE1/0/52 port link-mode bridge port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 port link-aggregation group 20 # interface Bridge-Aggregation10 port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 link-aggregation mode dynamic port m-lag group 10 # interface Bridge-Aggregation20 port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 10 link-aggregation mode dynamic port m-lag group 20 #
VRRP配置	# interface Vlan-interface10 ip address 10.9.68.11 255.255.255.0 vrrp vrid 1 virtual-ip 10.9.68.100 vrrp vrid 1 priority 254 #	# interface Vlan-interface10 ip address 10.9.68.12 255.255.255.0 vrrp vrid 1 virtual-ip 10.9.68.100 #

配置完成后，测试FW1以自身虚地址ping对端Border虚地址，对应测试如下：

```
RBM_P<M9K-L>ping -a 10.9.68.10 10.9.68.100
Ping 10.9.68.100 (10.9.68.100) from 10.9.68.10: 56 data bytes, press CTRL+C to bre
ak
56 bytes from 10.9.68.100: icmp_seq=0 ttl=255 time=1.678 ms
56 bytes from 10.9.68.100: icmp_seq=1 ttl=255 time=1.227 ms
56 bytes from 10.9.68.100: icmp_seq=2 ttl=255 time=1.366 ms
56 bytes from 10.9.68.100: icmp_seq=3 ttl=255 time=1.370 ms
56 bytes from 10.9.68.100: icmp_seq=4 ttl=255 time=1.316 ms
```

会话信息：

```
Initiator:
  Source      IP/port: 10.9.68.10/11567
  Destination IP/port: 10.9.68.100/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: InLoopBack0
  Source security zone: Local
Responder:
  Source      IP/port: 10.9.68.100/11567
  Destination IP/port: 10.9.68.10/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Route-Aggregation10.10
  Source security zone: Trust
State: ICMP_REPLY
Application: ICMP
Rule ID: 100
Rule name: CMNET-WAIN-03
```

```
Start time: 2024-01-18 12:06:17  TTL: 23s
Initiator->Responder:          5 packets        420 bytes
Responder->Initiator:          5 packets        420 bytes
```

FW1对应ARP表项：

```
RBM_P<M9K-L>disp arp int ro10.10
  Type: S-Static    D-Dynamic    O-Openflow   R-Rule   I-Invalid
IP address      MAC address    SVLAN/VSI  Interface/Link ID       Aging Type
10.9.68.2       743a-2021-eddc --          RAGG10.10               14    D
10.9.68.11      703a-a677-0279 --          RAGG10.10               15    D
10.9.68.12      703a-a676-fe77 --          RAGG10.10               16    D
10.9.68.100     0000-5e00-0101 --          RAGG10.10               8     D
```

Border1对应ARP表项：

```
<S68-L2>disp arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI name Interface             Aging Type
192.168.68.2    703a-a676-fe8c --          XGE1/0/3                1107  D
10.158.3.1      40fe-9555-84e8 20          BAGG30                  611   D
10.9.68.2       743a-2021-eddc 10          BAGG20                  426   D
10.158.3.12     0068-0012-0030 20          BAGG1024                614   D
10.9.68.12      703a-a676-fe77 10          BAGG1024                1180  D
10.9.68.1       98f1-81b5-1fb5 10          BAGG10                  836   D
10.9.68.10      0000-5e00-010a 10          BAGG10                  851   D
```

配置关键点

1. FW无需配置track，接口下配置VRRP之后，RBM会自动关注接口状态。
2. Border peer-link链路两端端口上关闭报文入接口与静态MAC地址表项匹配检查功能，以确保三层单播流量转发正常。
3. 同一个广播域下VRRP对应的VRID不要冲突，参考案例：某局点comwareV7 配置VRRP之后报VRRP VRID冲突
4. 以上案例仅供探究，实际组网参考客户实际需求。