新IT解决方案领导者

RBM技术专题课程

目录

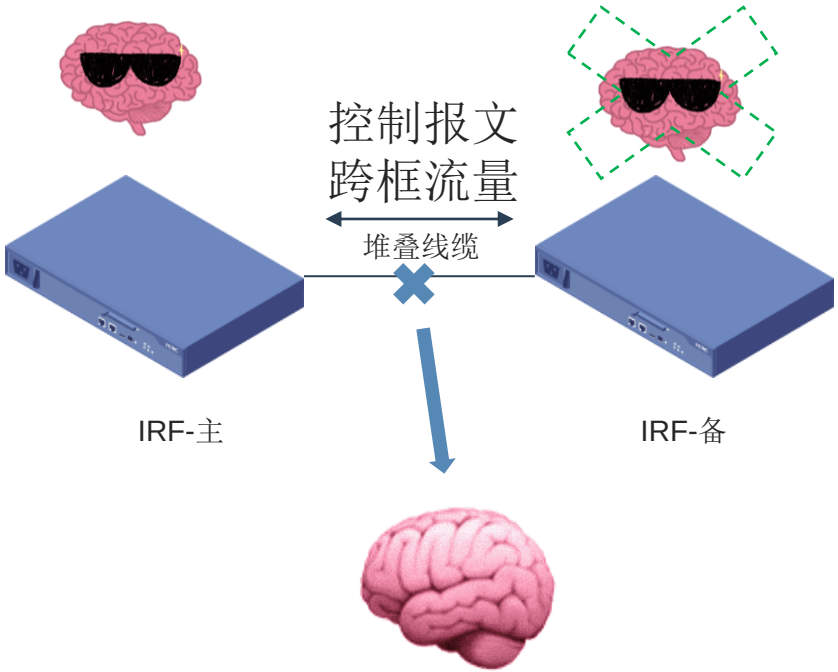
RBM背景

--为什么首选RBM

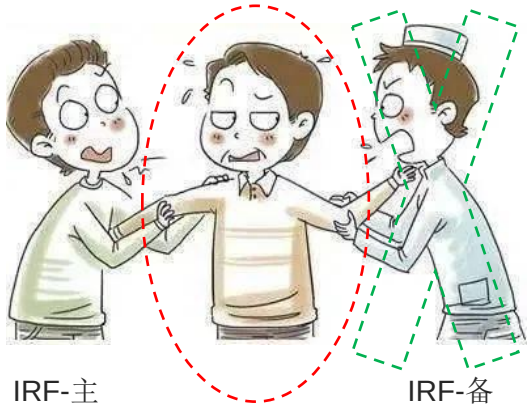
RBM简介

RBM（Remote Backup Management，远端备份管理）提供了一种设备之间备份关键配置信息和业务表项的解决方案。可以实现网络中主设备发生故障时，备设备能够平滑地接替主设备工作，保证用户业务数据的不间断传输，从而实现双机热备。目前安全只支持在两台设备进行双机热备。

RBM VS IRF

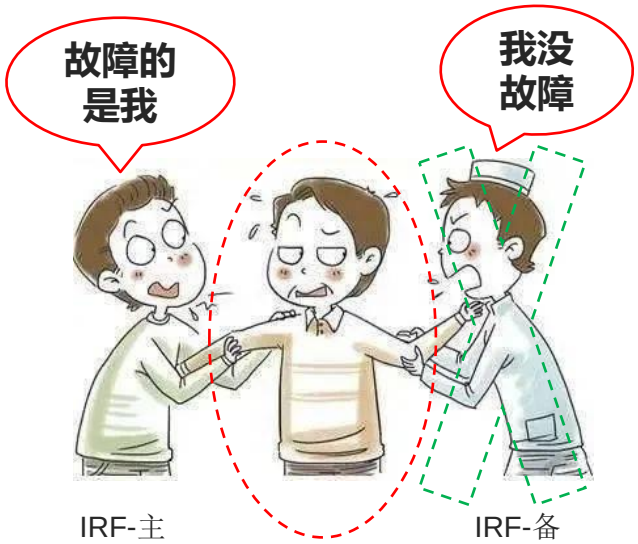


堆叠分裂
俗称：脑裂



MAD检测

RBM VS IRF



MAD检测

MAD“好心办坏事”：

- **MAD工作原理：**IRF分裂后，MAD检测模块会将IRF Member ID号大的成员设备置为Recovery状态，并MAD down该成员设备上除了系统保留接口外的所有接口。

- **堆叠双杀场景：**若IRF分裂原因是IRF Member ID号小的成员设备故障，此时IRF Member ID号大的成员设备接口置down，影响业务。

新华三集团

技术服务部 技术支持中心

【代理商级别】 新华三技支函【2021】161号

【重要】

关于安全高端产品“堆叠双杀”问题的技术公告

公告类别	强制立即整改
整改完成期限	2022/4/30
操作要求	版本升级、组网整改

【产品型号】

涉及安全高端产品系列，具体型号见下表：

【涉及版本】

产品型号	存在问题版本号	规避问题版本号
M9014 M9010 M9006 M9016-V	R9153P3001（不含）之前版本	R9153P3001或更新版本
M9012-S M9008-S M9008-S-V	R9724P3001（不含）之前版本	R9724P3001或更新版本
M9000-AI-E8 M9000-AI-E16	R9001P3001（不含）之前版本	R9001P3001或更新版本
T9006 T9010 T9014	R9136P3001（不含）之前版本	R9136P3001或更新版本
T9008-S T9012-S	R9823P3001（不含）之前版本	R9823P3001或更新版本
T9000-E8	R9001P3001（不含）之前版本	R9001P3001或更新版本

【问题描述】

新华三集团

技术服务部 技术支持中心

【代理商级别】 新华三技支函【2021】088号

【重要】

关于Comware V7平台安全产品推荐采用RBM特性部署HA组网的技术公告

公告类别	预警
操作要求	学习预防

【产品型号】

涉及Comware V7平台全系列高端、中低端、负载均衡安全产品。

【推荐版本】

产品型号	推荐RBM特性的软件版本号
M9014 M9010 M9006 M9016-V	R9153P2412或更新
M9012-S M9008-S M9008-S-V	R9724P2412或更新
M9000-AI-E8 M9000-AI-E16	R9001P2411或更新
T9008-S T9012-S	R9823P2411或更新
T9000-E8	R9001P2411或更新
T9006 T9010 T9014	E9136P22或更新
SecBlade IV NGFW	R8536P24或更新
F5080-D F5060-D F5030-D F5000-AK525 F5000-AK515	R9620P2410或更新
F5080 F5060 F5030 F5000-A F5000-M F5030-6GW F5000-AI-40 F5000-AI-20 F5000-V30	R9628P2412或更新

RBM VS IRF

IRF

需要考虑横穿流量，堆叠开销量大

控制平面统一

以不间断业务方式升级时，操作难度大

RBM

减少了横向链路的带宽限制

控制平面分离

升级方案灵活、简单，对业务无感知

RBM工作原理

RBM技术包含的基本概念—配置角度

远端备份组

remote-backup group

承担备份任务的两台设备组成一个远端备份组，统一管理多个备份组状态的切换，以及两台设备之间关键配置信息和业务表项的备份。

主从管理设备

device-role primary/secondary

俗称“管理的主备” 用于控制设备之间关键配置信息的同步。

选举产生

运行的主备

也称“业务的主备”

默认**主备模式**下运行的主处理业务，并向备设备实时备份业务表项信息；运行的备除接收主的业务表项备份信息外，时刻准备无缝衔接。**双主模式**下（backup-mode dual-active）两边都是运行的主。

RBM技术包含的基本概念—配置角度

RBM通道

用于两台设备之间交互远端备份组的运行状态信息，关键配置信息和业务表信息。

- **控制通道**：可传输的报文类型包括远端备份组的运行状态报文、一致性检查报文和同步配置信息的报文等。控制通道利用TCP建立连接，基于TCP协议自身的保活机制来监测链路的连通性。因此两端设备三层可达即可建立控制通道。（基于TCP的保活机制来监测链路的连通性，五次重连失败断开）
- **数据通道**：仅用于传输设备之间的热备报文和透传报文，不用于传输RBM的其他报文。数据通道直接使用底层驱动进行数据传输，因此不可以跨三层通信。

注意事项：

- 数据通道二层可达、控制通道三层可达；
- 数据、控制通道不允许配置VRF，MTU等参数，要求保持默认参数；
- 控制通道不允许对60063、60064（默认端口）、60065（sslvpn备份通道端口）端口做限制。

RBM技术包含的基本概念—配置角度

RBM通道

用于两台设备之间交互远端备份组的运行状态信息，关键配置信息和业务表信息。

- **控制通道**：可传输的报文类型包括远端备份组的运行状态报文、一致性检查报文和同步配置信息的报文等。控制通道利用TCP建立连接，基于TCP协议自身的保活机制来监测链路的连通性。因此两端设备三层可达即可建立控制通道。（基于TCP的保活机制来监测链路的连通性，五次重连失败断开）
- **数据通道**：仅用于传输设备之间的热备报文和透传报文，不用于传输RBM的其他报文。数据通道直接使用底层驱动进行数据传输，因此不可以跨三层通信。

注意事项：

- 数据通道二层可达、控制通道三层可达；
- 数据、控制通道不允许配置VRF，MTU等参数，要求保持默认参数；
- 控制通道不允许对60063、60064（默认端口）、60065（sslvpn备份通道端口）端口做限制。

RBM技术包含的基本概念—配置角度

[DeviceA] remote-backup group

RBM通道

用于两台设备之间交互远端备份组的运行状态信息，关键配置信息和业务表信息。

- **控制通道**：可传输的报文类型包括远端备份组的运行状态报文、一致
CP建立连接，
因此两端设备三
监测链路的连通

```
[DeviceA] remote-backup group
[DeviceA-remote-backup-group] remote-ip 10.2.1.2
[DeviceA-remote-backup-group] local-ip 10.2.1.1
```

- **数据通道**：仅用于传输设备之间的热备报文和透传报文，不用于传输

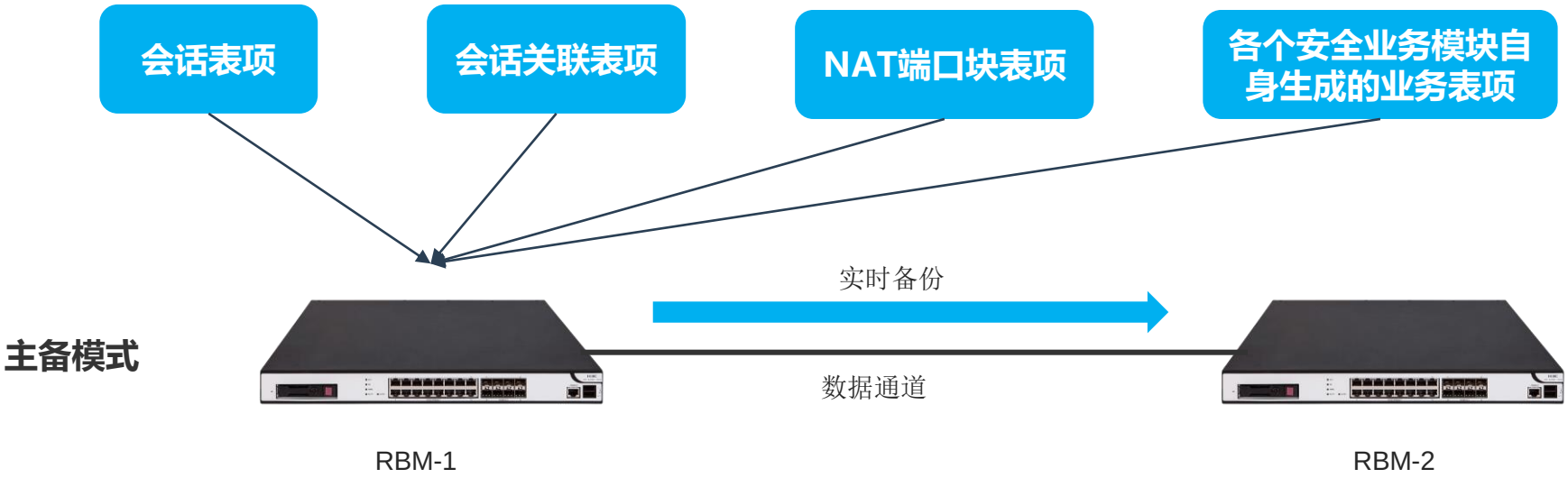
```
[DeviceA] remote-backup group
[DeviceA-remote-backup-group] data-channel interface gigabitethernet 1/0/3
```

注意事项：

- 数据通道二层可达、控制通道三层可达；
- 数据、控制通道不允许配置VRF，MTU等参数，要求保持默认参数；
- 控制通道不允许对60063、60064（默认端口）、60065（sslvpn备份通道端口）端口做限制。

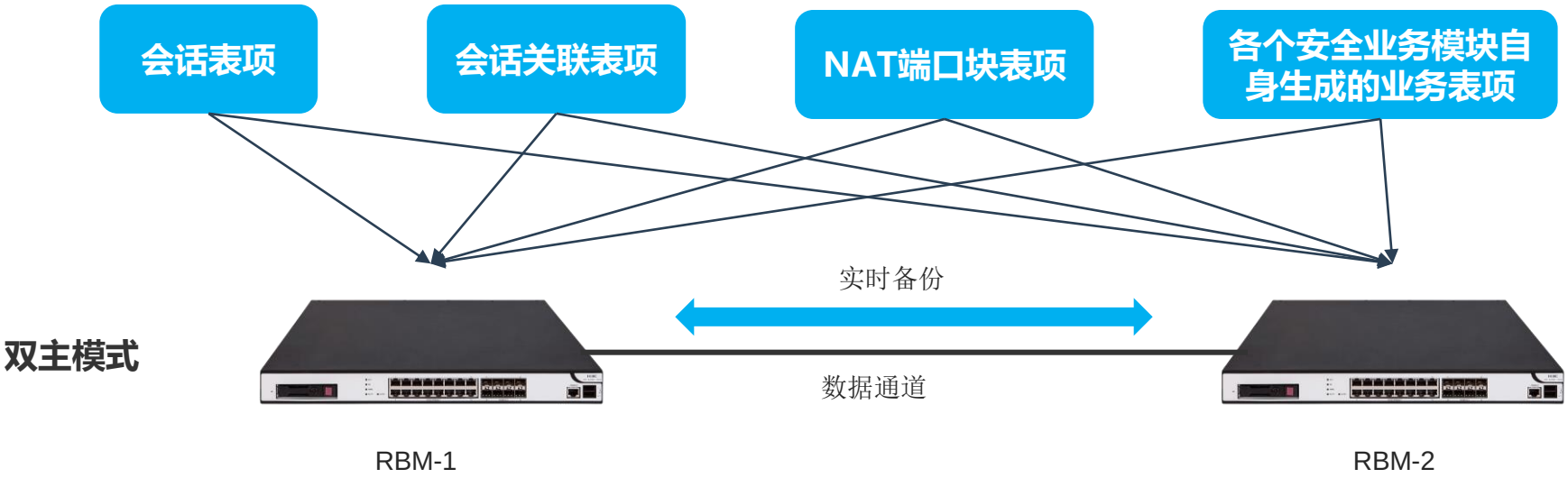
业务表项备份---走数据通道

- **目前支持备份的表项**



业务表项备份---走数据通道

- **目前支持备份的表项**



双主模式

- **功能简介**

保证RBM双机之间配置同步，避免了主备设备切换时因备设备上缺失对应的配置信息而造成的业务中断问题。

要点：

- HA正常时的同步方向：配置信息只能从“主管理设备”同步到“从管理设备”，因此开局后不建议在从管理设备上进行配置
- 实时备份：主管理设备上新增、删除或修改的配置信息将实时备份到从管理设备，保证这些变化的配置信息在主从管理设备上的一致
- 批量备份：主管理设备上的关键配置信息全部备份到从管理设备，从管理设备上会删除与主管理设备上不一致的配置，保证关键配置信息在主从管理设备上的完全一致

• 批量备份的场景

- 主备设备都是第一次建立RBM，通道建立后，主向备进行一次批备，并且后续配置主向备同步
- 主备设备都是第一次建立RBM，先建立RBM通道，然后再开启configuration auto-sync enable（此命令默认开启，即先关闭，然后建立通道，然后再开启），主向备进行一次批备，并且后续配置主向备同步
- 主设备第一次建立RBM，备设备已经建立过RBM，通道建立后，备向主进行批备，并且后续主向备同步
- 主设备建立过RBM，备设备第一次建立RBM，主向备批备，后续配置主向备同步
- 主设备建立过RBM，备设备第一次建立RBM，先关闭configuration auto-sync enable，建立通道，再开启configuration auto-sync enable的情况下，主向备批备，后续配置主向备同步。

备注：第一次建立RBM指的是rbmd进程重启，用户态数据丢失，例如重启设备、新到货设备等。

配置表项备份

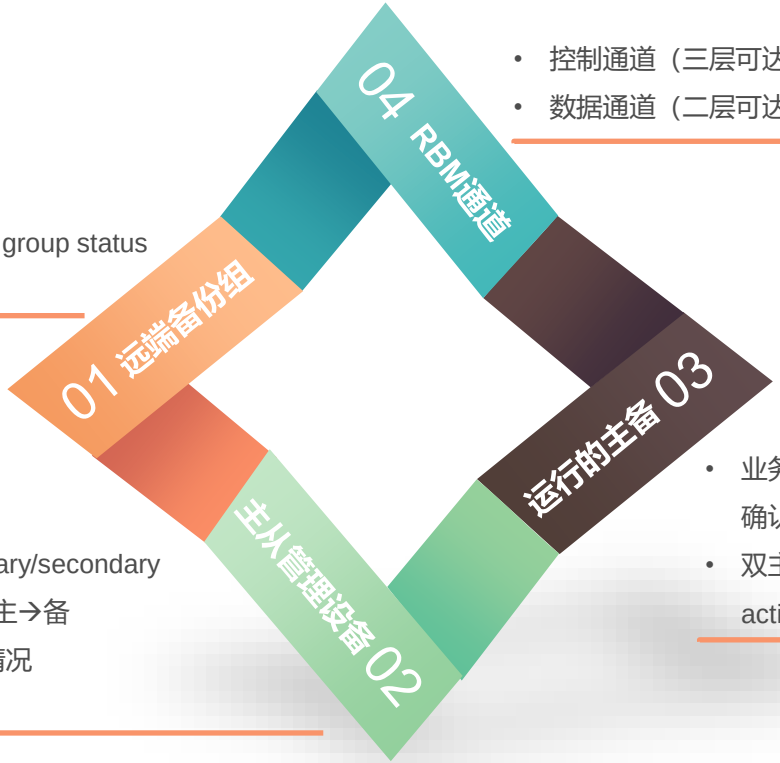
- **目前支持配置信息备份的模块**

策略类	资源类	DPI模块	日志类	VPN类
对象策略	VPN实例	应用层检测引擎	快速日志	SSL VPN
安全策略	ACL	IPS	Flow日志	
ASPF	对象组	URL过滤		
攻击检测与防范	时间段	数据过滤		
连接数限制	安全域	文件过滤		
NAT	会话管理	防病毒		
AFT	APR	数据分析中心		
负载均衡	AAA			
带宽管理	NQA			
应用审计与管理				
共享上网管理				
代理策略				

触发RBM业务主备角色改变的情况

- 控制通道断开：两台设备正常运行情况下，当控制通道断开后会进行主备切换。这时两台设备都变为主设备，进行业务处理，但是两台设备不再是HA状态，对后续的非对称流量会有影响。
- 主设备整机故障。
- 主设备上**所有**主用主控板故障。
- 主设备上HA监控的接口故障（VRRP成员口、track）。
- 主设备上任意业务板故障。
- 主设备上所有交换网板故障。

RBM几个重要概念--复习



- remote-backup group
- 通过display remote-backup group status 查看设备当前的运行状态

- device-role primary/secondary
- 配置同步只能从主→备
- 配置批备的5中情况

- 控制通道（三层可达，TCP三个端口要放通）
- 数据通道（二层可达）

- 业务的主备，通过display remote-backup group 确认状态
- 双主模式需要额外配置backup-mode dual-active

RBM典型组网

--深入理解RBM运行原理

RBM工作在2层

track vlan

双主：两台设备上RBM所监控VLAN的状态均为Active

主备：备设备上RBM所监控VLAN的状态为Inactive

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] track vlan 10
```

track interface:当设备的上下行业务接口为二层接口，上下行连接路由器三层接口组网时，可以通过track interface命令监控二层以太网接口的状态

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] track interface gigabitethernet 1/0/1
[Sysname-remote-backup-group] track interface gigabitethernet 1/0/2
```

RBM工作在3层

track interface

- **双主**：联动静态路由
- **主备**：联动静态路由

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] track interface gigabitethernet 1/0/1
[Sysname-remote-backup-group] track interface gigabitethernet 1/0/2
```

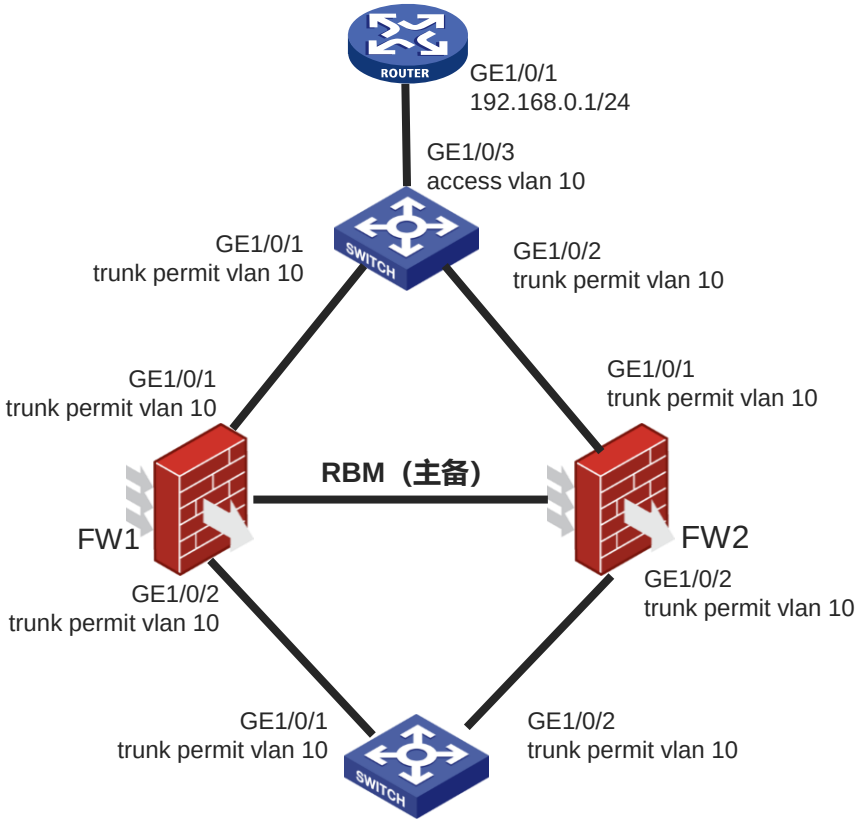
track id:当RBM联动的其中一个Track项的状态为Negative状态时，RBM将进行设备的主备切换，将上下行流量同时切换到新的主设备，保证业务不中断。

```
<Sysname>system-view
[Sysname]track 1 interface GigabitEthernet 1/0/1 physical
[Sysname-track-1]quit
[Sysname]remote-backup group
[Sysname-remote-backup-group]track 1
```

VRRP:不需要配置任何track,RBM自动监控VRRP成员口的状态

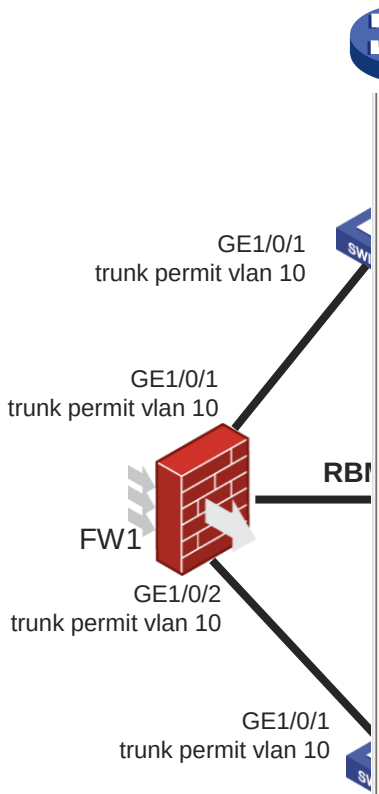
注意：RBM使用track interface时，不支持和其他RBM联动模块共同配置，如track vlan、vrrp、track id、adjust cost

二层场景：主备/双主组网，track vlan



- 两台FW主备二层部署, remote-backup group里track vlan 10。
- 运行的主处理vlan10标签的报文，备不处理vlan10标签的报文。
- 主切备：当FW1的设备故障或上下行接口故障时，FW1会down/up所有的vlan10接口，让上下行二层设备的mac表项刷，并且主不再处理vlan10的报文。保证业务能切换到FW2.
- 备切主：当FW1故障恢复后，经过delay-time后，FW2会down/up所有vlan10的接口，保证上下行二层设备刷新mac表项，并且不再处理vlan10报文，业务正常切换到FW1。

二层场景：主备/双主组网，track vlan




```
RBM_P<FW1>
RBM_P<FW1>
RBM_P<FW1>*May  3 16:32:58:496 2023 FW1 MACFW/7/MACFW_PACKET: -Context
=1;
Receiving, vlan = 10, interface = GigabitEthernet1/0/1, payload =
 FF FF FF FF FF FF 14 80 17 BB 01 02 81 00 00 0A
 08 06 00 01 08 00 06 04 00 01 14 80 17 BB 01 02
 C0 A8 00 01 00 00 00 00 00 00 C0 A8 00 02 00 00
 00 00 00 00 00 00 00 00 00 00 00 00
Receiving an Ethernet frame.
VsysID = 1

*May  3 16:32:58:496 2023 FW1 MACFW/7/MACFW_PACKET: -Context=1;
Delivering, vlan = 10, interface = GigabitEthernet1/0/1, payload =
 FF FF FF FF FF FF 14 80 17 BB 01 02 81 00 00 0A
 08 06 00 01 08 00 06 04 00 01 14 80 17 BB 01 02
 C0 A8 00 01 00 00 00 00 00 00 C0 A8 00 02 00 00
 00 00 00 00 00 00 00 00 00 00 00 00
Delivering an Ethernet frame to layer 2.
VsysID = 1

*May  3 16:32:58:496 2023 FW1 MACFW/7/MACFW_PACKET: -Context=1;
Sending, vlan = 10, interface = GigabitEthernet1/0/2, payload =
 FF FF FF FF FF FF 14 80 17 BB 01 02 81 00 00 0A
 08 06 00 01 08 00 06 04 00 01 14 80 17 BB 01 02
 C0 A8 00 01 00 00 00 00 00 00 C0 A8 00 02 00 00
 00 00 00 00 00 00 00 00 00 00 00 00
Sending an Ethernet frame.
VsysID = 1

*May  3 16:32:58:496 2023 FW1 MACFW/7/MACFW_PACKET: -Context=1;
Receiving, vlan = 10, interface = GigabitEthernet1/0/2, payload =
 14 80 17 BB 01 02 14 80 27 74 02 02 81 00 00 0A
 08 06 00 01 08 00 06 04 00 02 14 80 27 74 02 02
 C0 A8 00 02 14 80 17 BB 01 02 C0 A8 00 01 00 00
 00 00 00 00 00 00 00 00 00 00 00 00
Receiving an Ethernet frame.
VsysID = 1

*May  3 16:32:58:497 2023 FW1 MACFW/7/MACFW_PACKET: -Context=1;
Sending, vlan = 10, interface = GigabitEthernet1/0/1, payload =
 14 80 17 BB 01 02 14 80 27 74 02 02 81 00 00 0A
 08 06 00 01 08 00 06 04 00 02 14 80 27 74 02 02
 C0 A8 00 02 14 80 17 BB 01 02 C0 A8 00 01 00 00
 00 00 00 00 00 00 00 00 00 00 00 00
Sending an Ethernet frame.
```

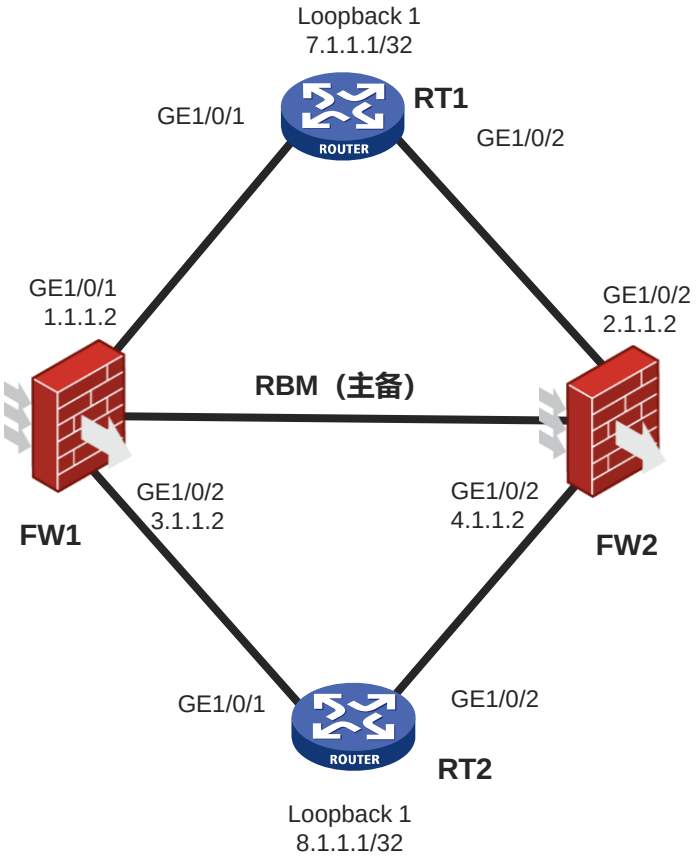
处理vlan10标签的arp

```
RBM_S<FW2>
RBM_S<FW2>
RBM_S<FW2>
RBM_S<FW2>
RBM_S<FW2>*May  3 16:31:40:088 2023 FW2 MACFW/7/MACFW_PACKET: -Context=
1;
Receiving, vlan = 10, interface = GigabitEthernet1/0/1, payload =
 FF FF FF FF FF FF 14 80 17 BB 01 02 81 00 00 0A
 08 06 00 01 08 00 06 04 00 01 14 80 17 BB 01 02
 C0 A8 00 01 00 00 00 00 00 00 C0 A8 00 02 00 00
 00 00 00 00 00 00 00 00 00 00 00 00
Receiving an Ethernet frame.
VsysID = 1

*May  3 16:31:40:089 2023 FW2 MACFW/7/MACFW_PACKET: -Context=1;
Receiving, vlan = 10, interface = GigabitEthernet1/0/2, payload =
 FF FF FF FF FF FF 14 80 17 BB 01 02 81 00 00 0A
 08 06 00 01 08 00 06 04 00 01 14 80 17 BB 01 02
 C0 A8 00 01 00 00 00 00 00 00 C0 A8 00 02 00 00
 00 00 00 00 00 00 00 00 00 00 00 00
Receiving an Ethernet frame.
VsysID = 1
```

不处理任何vlan10标签的报文

```
RBM_S<FW2>
RBM_S<FW2>u t m
The current terminal is disabled to display logs.
RBM_S<FW2>
RBM_S<FW2>
RBM_S<FW2>dis int brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description

GE1/0/0              DOWN DOWN     --
GE1/0/3              DOWN DOWN     --
GE1/0/4              DOWN DOWN     --
GE1/0/5              DOWN DOWN     --
GE1/0/6              DOWN DOWN     --
GE1/0/7              DOWN DOWN     --
GE1/0/8              DOWN DOWN     --
GE1/0/9              DOWN DOWN     --
GE1/0/10             DOWN DOWN     --
GE1/0/11             DOWN DOWN     --
GE1/0/12             DOWN DOWN     --
```

三层场景0：主备/双主组网，联动静态路由（不推荐）



- 假设业务：7.1.1.1 →ping→ 8.1.1.1
- RT1静态路由：

ip route-static 0.0.0.0 0 1.1.1.2 preference 70

ip route-static 0.0.0.0 0 2.1.1.2 preference 80

- RT2静态路由：

ip route-static 0.0.0.0 0 3.1.1.2 preference 70

ip route-static 0.0.0.0 0 4.1.1.2 preference 80

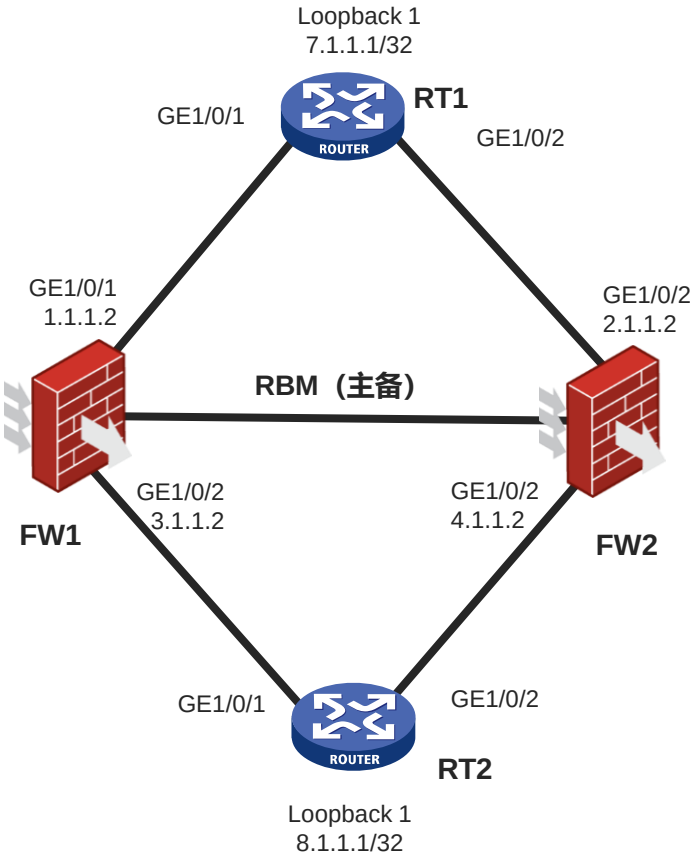
- remote-backup group配置：

track interface GigabitEthernet1/0/1

track interface GigabitEthernet1/0/2

- 切换机制：FW1→FW2，FW1上的GE1/0/1和GE1/0/2口down，此时RT1和RT2优先级较小的路由生效，实现流量的切换
- 回切机制： FW2→FW1，倒计时结束后，FW1的业务口恢复UP，优先级较高的路由恢复，实现流量回切

三层场景0：主备/双主组网，联动静态路由（不推荐）



◆ 存在双备的问题：

双备---现场RBM下配置了track 聚合口联动静态路由，主墙的某一个被track的接口down，恢复UP之后启动倒计时，并把这个接口down，此时如果备墙被track的接口也down了，随后up恢复，此时主墙和备墙都是RBM运行的备，等待主墙的回切倒计时结束，主墙恢复RBM运行的主，主墙接口up，但是由于倒回定时器的问题，备墙还是认为自己有问题，接口都是备RBMdown的状态（undo shutdown也无法恢复）。后续如果主墙被track的接口再down一次，就会导致双备发生。

该问题目前版本未解决，所以此组网不推荐。

静态路由联动及RBM新增说明

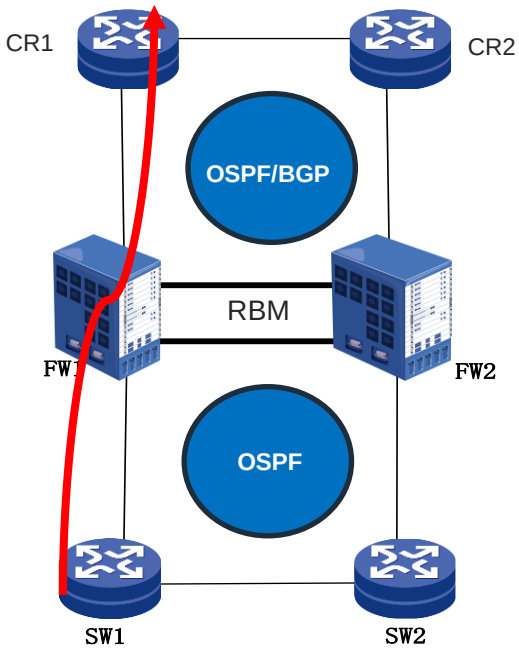
静态路由联动

- RBM视图下，配置track interface 监控上下行接口状态，保证可以联动静态路由进行主备切换，保证业务的无缝连接。

RBM使用说明

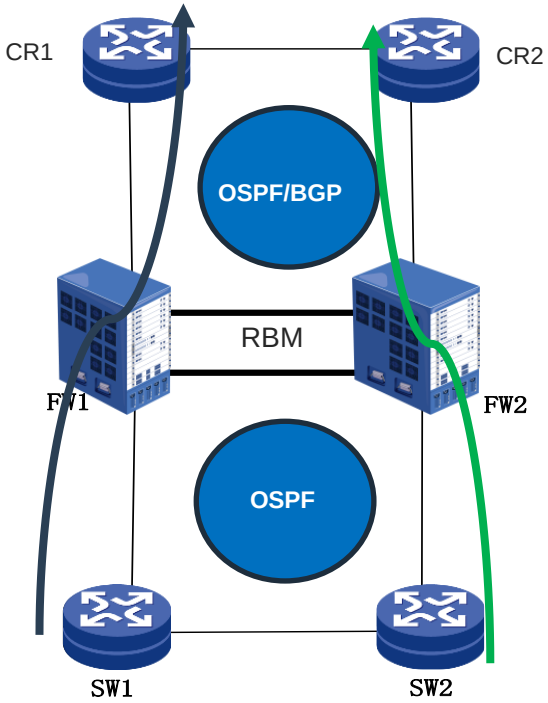
- M9000系列从R9153P3001开始支持静态路由联动，监控上下行接口的状态；M9000-S系列R9724P3001开始支持。
- 中低端防火墙需要B64D060分支R版本开始支持RBM+静态路由联动

三层场景1：主备组网，防火墙三层，上下行连接路由器组网



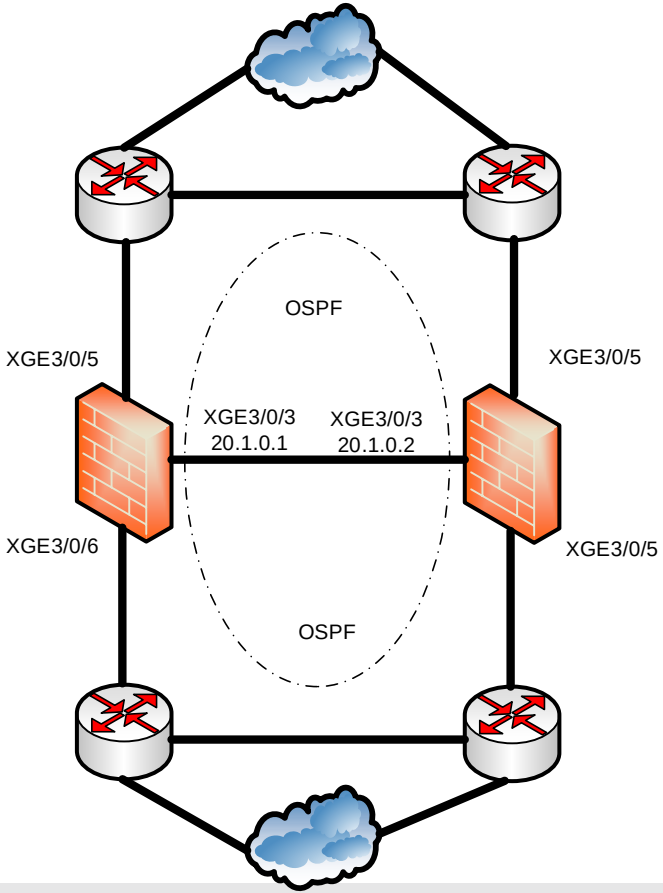
- 两台FW的业务接口都工作在三层，上下行分别连接路由器。FW与上下行路由器之间运行OSPF/BGP协议。
- 两台FW以主备备份方式工作。
- 正常流量从**SW1-FW1-CR1**。
- 当FW1的设备故障或上下行接口故障时FW1对外发布的路由开销值被调整，原本通向FW1的所有流量都指向了FW2
- 接口类故障 业务板故障，主控故障，切换丢包时延百毫秒级(4层报文场景)。

三层场景2：双主组网，防火墙三层，上下行连接路由器组网



- 两台FW的业务接口都工作在三层，上下行分别连接路由器。FW与上下行路由器之间运行OSPF/BGP协议。
- 两台FW以负载分担方式工作。
- 正常流量可以从**SW1-FW1-CR1**，同样流量也可以从**SW2-FW2-CR2**
- 当FW1设备故障或上下行接口故障时，FW1对外发布的路由开销值被调整，**原本通向FW1的所有流量都指向了FW2**
- 接口类故障 业务板故障，主控故障，切换丢包时延百毫秒级(4层报文场景)。

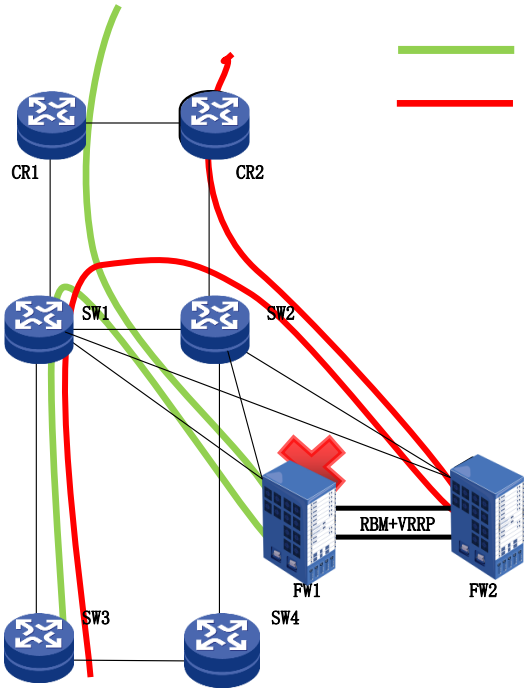
以RBM+OSPF 双主组网配置举例



主管理设备配置命令如下：

```
#
track 1 interface Ten-GigabitEthernet 3/0/5 physical
#
track 2 interface Ten-GigabitEthernet 3/0/6 physical
#
nat remote-backup port-alloc primary
#
remote-backup group
 local-ip 20.1.0.1
 remote-ip 20.1.0.2
 device-role primary
 backup-mode dual-active
 data-channel interface Ten-GigabitEthernet 3/0/3
 delay-time 1
 adjust-cost ospf enable increment 1000
 adjust-cost ospfv3 enable absolute 60000
 track 1
 track 2
```

三层场景3：防火墙旁挂部署，VRRP主备组网



场景：双机旁挂VRRP+RBM主备部署，上下行接口本框聚合或单链路，上下行不同子接口各配一组VRRP，FW1为主，FW2为备。

流量走向：

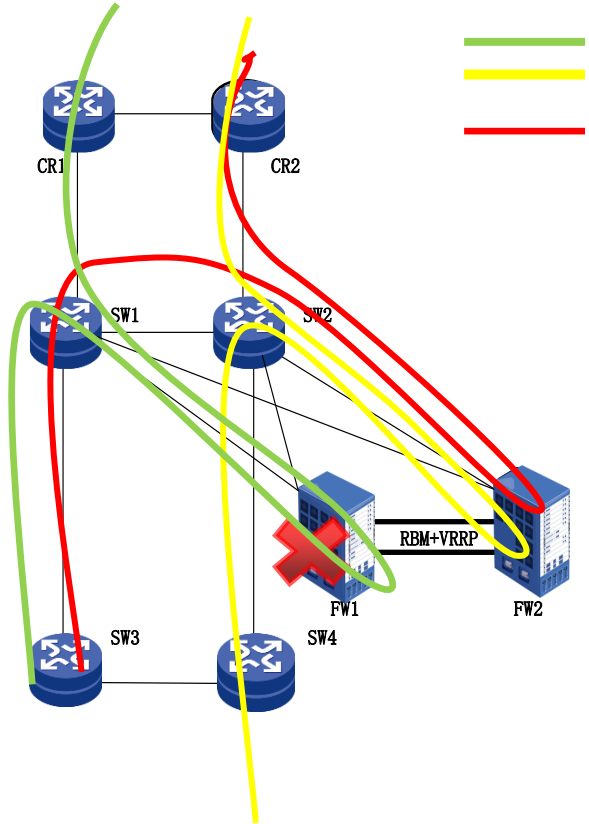
正常流量从**SW3-SW1-FW1-CR1**。

当FW1的设备故障时，使用RBM +VRRP联动机制实现主备切换，原本通向FW1的所有流量都指向了**FW2**

故障切换：

接口类故障 业务板故障，主主控故障，切换丢包时延百毫秒级(4层报文场景)。

三层场景4：防火墙旁挂部署，VRRP双主组网



FW1正常时，流量走向

FW1故障时，流量走向

场景：双机旁挂VRRP+RBM主主部署，上下行接口本框聚合或单链路，上下行不同子接口各配两组VRRP，互为主备。

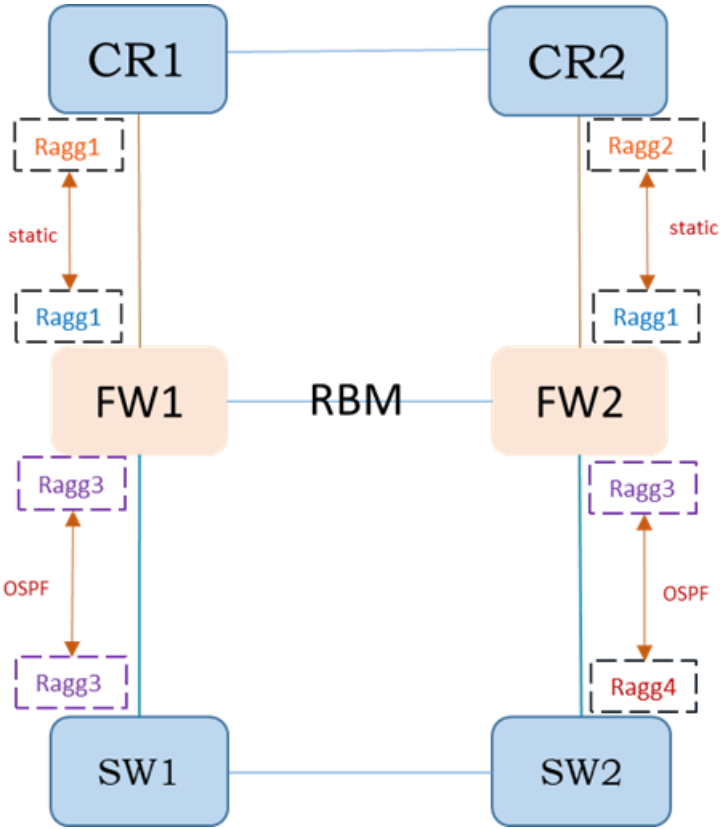
流量走向：

正常流量可以从**SW3-SW1-FW1-CR1**，同样流量也可以从**SW4-SW2-FW2-CR2**。当FW1的设备故障时，使用RBM +VRRP联动机制实现主备切换，原本通向FW1的所有流量都指向了**FW2**

故障切换：

接口类故障 业务板故障，主主控故障，切换丢包时延百毫秒级(4层报文场景)。

三层场景5：EAA联动，上行静态，下行ospf



组网：

上行设备写静态路由指到FW的地址池地址，防火墙对上接口做snat转换。

防火墙RBM主备部署，下行ospf，两台防火墙对上写默认路由出公网，并且将默认路由引入ospf进程，向下发布。

下行设备的明细路由通过ospf发布到FW。

切换效果：

RBM视图下只track监控下行聚合口Ragg3,EAA监控syslog，一旦RBM切换，EAA检测到日志关键词就会执行动作down掉上行Ragg1的接口。

工作原理：

如果FW1上行Ragg1接口down，CR1上配置的静态路由失效，FW1上的默认路由也会失效，导致下行设备学不到FW1的默认路由。这样就可以保证上行设备和下行设备都不会网FW1上送流量。

如果FW1下行接口down，EAA检测到RBM切换后把上行口down，这样就可以保证上行设备和下行设备都不会网FW1上送流量。

三层场景5：EAA联动，上行静态，下行ospf

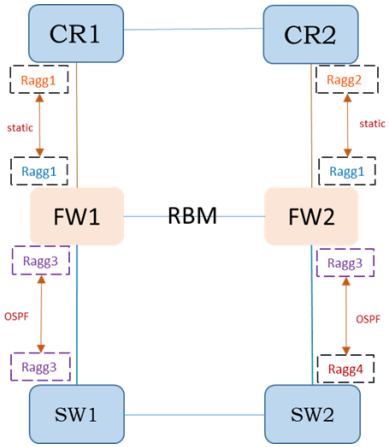
关键配置：

RBM切换的日志

十秒内产生一次日志就触发

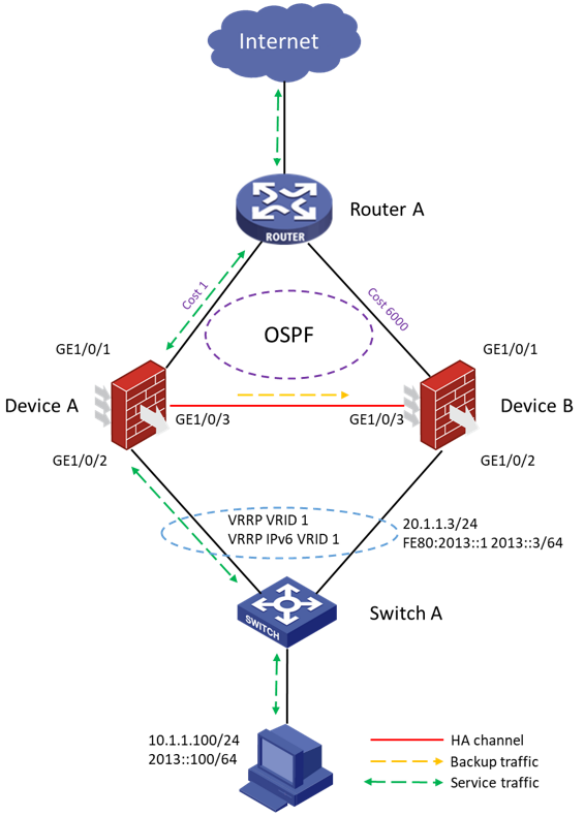
```
undo info-center enable
#
rtm cli-policy shutdown
event syslog priority all msg "RBM running status changed to standby" occurs 1 period 10
action 1 cli system-view
action 2 cli interface Route-Aggregation 1
action 3 cli shutdown
user-role level-3
user-role network-operator
user-role network-admin
commit
#
#
rtm cli-policy shutdown
event syslog priority all msg "RBM running status changed to active" occurs 1 period 10
action 1 cli system-view
action 2 cli interface Route-Aggregation 1
action 3 cli undo shutdown
user-role level-3
user-role network-operator
user-role network-admin
commit
#
info-center enable
```

回切日志




```
#
track 1 interface Route-Aggregation 3 physical
#
remote-backup group
 data-channel interface Ten-GigabitEthernet1/0/15
 delay-time 1
 adjust-cost ospf enable absolute 6000
 track 1
 local-ip 99.99.99.1
 remote-ip 99.99.99.2
 device-role primary
```

关于虚墙：RBM支持context



场景：两台FW的业务接口都工作在三层，上下行分别连接三层交换机。FW与上下行三层设备之间运行静态路由，无VRRP。两台FW以RBM的负载均衡方式工作。SW1，SW2，SW3，SW4为三层交换机。

配置关键：

- VRRP、ospf等动态路由协议在虚墙配置
- track 、remote-backup group视图下的所有配置都在根墙配

故障切换：

- 当RBM整机切换的时候，context虚墙中的vrrp或ospf等动态路由协议会一起切换，从而实现context和根墙状态保持一致。

注意事项：

高端D045P3001开始，中低端D060分支开始支持RBM+context

记忆口诀：

- RBM视图下的配置都在根墙配，业务相关在虚墙配。

RBM特性相关命令介绍

RBM特性命令-1

#本端控制通道IP地址：local-ip x.x.x.x

配置用于建立控制通道的本端IP地址，Server端将使用此Local IP提供TCP监听服务

#对端控制通道IP地址： remote-ip x.x.x.x port x

配置用于建立控制通道的对端IP地址

#对端控制通道端口号

配置用于建立控制通道的对端端口号，在主备设备上配置的对端端口号必须一致，缺省为60064

#运行角色: device-role primary/secondary

RBM双机热备中的设备分为主 从两种管理角色，用于控制设备之间关键配置信息的同步。配置信息只能从“主管理设备”同步到“从管理设备”，并覆盖从管理设备上的相关配置信息

RBM特性命令-2

#运行模式：backup-mode dual-active

RBM双机热备的运行模式包括如下两种：

主备模式：正常情况下仅由主设备处理业务，备设备处于空闲状态，实时待命

双主模式：两台设备同时处理业务，充分利用设备资源，提高系统负载能力，此模式通过“互为主备”方法实现。

缺省为主备模式，双主模式需要配置backup-mode dual-active。

#数据通道：data-channel interface

主/备设备使用此功能配置的接口建立RBM双机热备的数据通道，此数据通道仅用于传输设备之间的热备报文和透传报文，不用于传输主/备设备之间的其他报文。

#业务表项热备： hot-backup enable

开启此功能后，主设备会将其生成的业务表项实时同步到备设备，当主设备发生故障时备设备可以能平滑地接替主设备的工作，保证业务不中断。

缺省为打开状态。

RBM特性命令-3

#自动同步配置信息： configuration auto-sync enable

开启此功能前，主管理设备上已经配置的命令，将会在开启此功能后进行一次批备，之后新增的命令将实时备份到从管理设备。

配置信息很多时批备时间会很长，可能需要一到两个小时。因此在初始规划网络配置时，建议先开启此功能，以减少后面配置信息进行批备的时间。缺省为开启状态。

#配置信息一致性检查：configuration sync-check interval

此功能用于检测双机热备状态下的两台设备的配置信息是否一致，用于防止发生两台设备配置信息不一致，导致主备切换后业务不通的情况。当配置信息不一致时，会发送日志信息，以提示管理员进行配置信息的手动同步。

缺省检查周期为24小时。

#流量回切延迟时间：delay-time

RBM双机热备组网中的主设备发生故障后，流量自动切换到对端设备。当原来的主设备恢复为主后，流量会进行回切。由于业务表项在主/备设备之间进行备份需要一定的时间，为了保证业务能够平滑切换，所以需要延迟流量的回切。如果不配置表示永不回切，如果要回切只能手工回切。

RBM特性命令-4

#联动动态路由：adjust-cost enable bgp|isis|ospf|ospfv3 increment|absolute

目前支持联动ospfv2、ospfv3、bgp和isis。主备模式下，备设备发布的动态路由cost值会做相应增加；双主模式下，正常运行时两台设备发布的路由都不加cost值，主备设备都处理业务流量且相互备份，当一台设备故障时，故障设备发布的路由cost值会做相应增加，所有流量在未故障的设备中处理。

#联动Track项

Track是全局配置，可以RBM视图下只配置相关的track项，当track项状态发生变化时，会触发RBM备份组进行重新主备选举。

由于RBM模块本身已经在检测业务板状态，因此建议只配置track接口项。

RBM特性命令-5

#VRRP备份组配置：vrrp vrid x virtual-ip x.x.x.x+掩码长度 +active|standby

在接口下创建vrrp备份组并添加虚地址，指定接口属于active或standby组

RBM主备模式，每个接口下添加一个VRRP备份组。

RBM双主模式，每个接口下添加两个VRRP备份组。

#nat端口块分配：nat remote-backup port-alloc primary|secondary

双主模式下，两台设备共用同一个nat资源池，为避免端口块分配冲突，在配置主设备上配置nat remote-backup port-alloc primary，配置备设备会自动下发nat remote-backup port-alloc secondary，配置主使用端口块前半段，配置备使用端口块后半段。

主备模式下，无需配置此命令。

#配置SNAT地址池绑定VRRP备份组：vrrp vrid x

当VRRP的虚拟IP地址与NAT地址组/NAT端口块组中公网地址成员**处于同一网段时**，设备无法判断是否需要对NAT地址组/NAT端口块组中公网地址成员的ARP请求进行响应。如果两台设备都回应ARP响应报文，则无法保证响应报文中MAC地址的正确性，也无法保证与HA相连的三层设备上ARP表项的正确性。为了避免上述情况的发生，需要将Master设备发送的ARP报文中携带的MAC地址改为VRRP备份组的虚拟MAC地址。当Master设备收到ARP请求时，回应的ARP响应报文中携带的MAC地址为此VRRP备份组的虚拟MAC地址。

```
#
nat address-group 1
 address 1.0.0.1 1.0.0.100
 vrrp vrid 7
```

如果地址池地址与VRRP虚拟IP不同网段，则不需要为地址池绑定VRRP备份组。

RBM技术维护手段介绍

配置RBM的注意事项：

- 主/备设备的型号必须一致。
- 主/备设备的软件版本必须一致。
- 主/备设备之间建立控制通道的接口必须一致。
- 主/备设备之间建立数据通道的接口必须一致。
- 主/备设备对应槽位上的接口必须加入到相同的安全域(会同步)。
- 主/备设备业务板的位置 数量和类型一致。
- 主/备设备接口板的位置 数量和类型一致。

热备功能规格说明

- 要求进行双机热备份的两台设备主控板的数量相同，接口板的位置 类型和数量都相同，业务板的数量和位置相同，否则会出现主用设备备份过去的信息，与备用设备的物理配置无法兼容，导致主备切换后出现问题。
- 要求主备设备的HASH选板模式 HASH因子配置一致。

RBM使用说明

- RBM热备开关hot-backup enable默认开启。
- 配置同步功能只在主上生效，所以建议相关配置操作都在配置主上进行。

RBM技术维护手段介绍

RBM_P<M9010_1>display remote-backup-group status
Remote backup group information:
  Backup mode: Active/standby----------业务运行模式
  Device management role: Primary----------管理主备角色
  Device running status: Standby----------当前设备运行状态
  Data channel interface: Route-Aggregation1----------数据通道
  Local IP: 192.168.2.2
  Remote IP: 192.168.2.1   Destination port: 60064
  Control channel status: Connected----------控制通道连接状态
  Keepalive interval: 1s
  Keepalive count: 10
  Configuration consistency check interval: 24 hour
  Configuration consistency check result: Inconsistent(2021-08-13 13:59:20)
  Configuration backup status: Auto sync enabled
  Session backup status: Hot backup enabled
  Delay-time: 1 min----------倒回延迟时间
  Uptime since last switchover: 1 days, 6 hours, 3 minutes
  Switchover records:----------切换记录
    Time   Status change   Cause
    2021-09-22 09:59:46 Standby to Active   Switchover request
    2021-09-22 09:59:17 Active to Standby   Switchover request

RBM技术维护手段介绍

- Switchover request可以实现RBM主备状态的切换，该命令只在RBM主备场景下生效，并且需要在设备运行状态为主设备（active）上执行。如果执行该命令后，只能通过在运行状态为主的设备上再次执行该命令或者有业务板重启、track项生效才会倒回。

```
RBM_P<M9010-1>display  remote-backup-group  status
Remote backup group information:
  Backup mode: Active/standby
  Device management role: Primary
  Device status: Active
  Data channel interface: Route-Aggregation1
  Local IP: 192.168.168.1
  Remote IP: 192.168.168.2    Destination port: 60064
  Control channel status: Connected
  Keepalive interval: 1s
  Keepalive count: 10
  Configuration consistency check interval: 24 hour
  Configuration consistency check result: Not Performed
  Configuration backup status: Auto sync enabled
  Session backup status: Hot backup enabled
  Delay-time: 1 min
[M9010-1]remote-backup  group
[M9010-1-remote-backup-group]switchover request
```

RBM技术维护手段介绍

- 当主备设备上存在不一致的配置时，可以通过如下命令进行手工同步

  RBM_P[M9010_1-remote-backup-group]configuration manual-sync

  %Aug 13 16:51:33:659 2021 M9010_1 SHELL/6/SHELL_CMD: -Line=vty0-IPAddr=10.88.32.123-User=admin; Command is configuration manual-sync

  %Aug 13 16:51:33:666 2021 M9010_1 RBM/6/RBM_CFG_BATCH_SYNC_START: Started batch configuration synchronization.

  %Aug 13 16:51:36:822 2021 M9010_1 RBM/6/RBM_CFG_BATCH_SYNC_FINISH: Finished batch configuration synchronization.

主

```
#
object-group ip address test
 0 network host address 1.1.1.1
 10 network host address 1.1.1.2
#
```

备

```
#
object-group ip address test
 0 network host address 1.1.1.1
 10 network host address 1.1.1.3
#
```

RBM技术维护手段介绍

- 正常情况下，我们配置的delay-time为30分钟或者50分钟，如果需要做主备倒换测试，我们可以先将主备设备上的delay-time设置的时间短一些，这样可以加快设备的倒回，注意改了delay-time之后要保存配置，否则测试整机重启时，设备起来后delay-time会恢复原来的配置，造成两边delay-time不一致。所有倒换测试完成后，将delay-time改回30分钟或者50分钟，并保存配置。
- 双主场景下，假如未配置delay-time或者配置的delay-time时间较长，当做了倒换测试、升级之类的操作后，两台墙为主备状态，如何快速恢复为双主状态？通常是给两边配上或调整delay-time 1，然后在运行状态为主的墙上shut/undo shut接口触发下，等1分钟后恢复双主，恢复后重新调回原有delay-time。

- RBM无法回切的情况举例：

1. 联想RBM切换的触发条件，检查备上边的触发条件是否恢复；

2. 更换故障板卡后发现故障设备状态一直为standby不回切，查看系统健康状态有故障信息：

```
RBM_S[FW]display system health
Health: Faulty(1)
    HgPort check: Faulty(1)
PacketLoss check: Normal(0)
RBM_S[FW]display system health history
Health: Faulty(1)
    HgPort check:
        Faulty(1) 2021-03-18 20:43:20 on slot 13
        Faulty(1) 2021-03-18 20:43:14 on slot 11
        Faulty(1) 2021-03-18 20:43:14 on slot 10
        Faulty(1) 2021-03-18 20:43:13 on slot 12
```

必须要在清除故障信息之后在经过delay-time后才能回切：

```
RBM_S[FW]reset-health-value hgportdown slot 10
RBM_S[FW]reset-health-value hgportdown slot 11
RBM_S[FW]reset-health-value hgportdown slot 12
RBM_S[FW]reset-health-value hgportdown slot 13
```

RBM升级&换备件

--细节决定成败
万变不离其宗

RBM技术维护手段介绍-软件版本升级（主备）

1. 保存主墙和备墙的配置，备份到本地

2.通过display remote-backup-group status中device running status的active和standby字段确认业务运行的主备，通过display system stable state和display device确认备墙状态正常后，升级备墙

3.备墙重启完成后，通过display system stable state和display device确认备墙状态正常，通过display session statistics summary确认主备墙的会话量级一致后，在主墙的remote-backup group视图下执行switchover request，使得RBM业务主备状态切换，当前主墙变为备墙，备墙切换为主墙，测试业务

4.业务测试正常后，升级备墙，备墙重启完后，通过确认备墙状态正常，确认主备墙的会话量级一致后，在当前主墙的remote-backup group视图下执行switchover request，使得RBM业务主备状态再次切换，测试业务

5.业务测试正常后，保存主备墙配置

注意：步骤中的主墙和备墙，指的是配置主墙和配置备墙

RBM技术维护手段介绍-软件版本升级（双主）

1. 保存主墙和备墙的配置，备份到本地

2.通过display system stable state和display device确认主备墙状态正常后，在主备墙的remote-backup group视图下执行**undo backup-mode**，使RBM双主变为主备模式，此时业务切换到主墙，测试业务

3.测试业务正常后，保存主备墙配置，升级备墙

4.备墙重启完成后，通过display system stable state和display device确认备墙状态正常，通过display session statistics summary确认主备墙的会话量级一致后，在主墙的remote-backup group视图下执行**switchover request**，RBM业务主备状态切换，测试业务

5.业务测试正常后，升级主墙，主墙重启完后，确认备墙状态正常，确认主备墙的会话量级一致，在备墙的remote-backup group视图下执行switchover request，RBM业务主备状态再次切换，测试业务

6. 务测试正常后，在主备墙的remote-backup group视图下配置**backup-mode dual-active**

注意：步骤中的主墙和备墙，指的是配置主墙和配置备墙

RBM技术维护手段介绍-拆堆叠升级对比

升级操作步骤：

1. 首先断开BFD MAD检测线缆.
2. 手工shutdown 一框业务端口，进入冗余组，手工使用命令switchover request切换防火墙业务板备份组至2框，此时2框承载流量，测试2框业务，业务正常。
3. save保存配置。
4. shutdown 2框IRF端口（console FW2），手工拔出无法shutdown的IRF端口(手工拔剩余最后一个IRF端口)，开始重启1框reboot chassis 1（此时2框独立承载业务）。
5. 等待一框防火墙业务板加载成功后，dis device/display system stable state查看设备状态正常，shutdwon 2框业务端口，undo shutdown 1框业务端口，开始进行业务验证。
6. 一框业务测试正常，重启2框（及时插入拔出的IRF） reboot chassis 2 。
7. 2框重启直接合并，合并成功，测试业务正常，插入MAD BFD线缆，升级完成。
8. save保存配置

RBM技术维护手段介绍-M/T9K系列更换备件

■ 更换主控：

1）单框主控冗余的情况下更换单块主控，直接执行更换操作即可，更换过程中RBM不会发生切换；

2）单框主控无冗余的情况下更换主控，需要先把业务切换到另外一边，将故障一侧的业务口全down，隔离后再执行更换操作（单框主控全down的时候，RBM通道会断）；

■ 更换业务板：

1）运行主更换业务板：调整delay-time到合适的时间，先切业务到另一边，然后执行更换操作，更换完毕后恢复delay-time；

2）运行的备更换业务板：确认业务后直接执行更换操作；

注意事项：

① 由于业务板更换需要主控板版本校验，所以更换故障业务板卡之前，需要先确认主控板中是否有主控的版本，如果没有的话业务板会起不来；

② 在更换的业务板重启完毕后，业务回切之前（如果有回切动作的话），建议在管理主上手工批备一次配置configuration manual-sync，保证主备流表一致。

RBM技术维护手段介绍- M/T9K更换备件

■ 更换接口板或交换网板：

接口板的更换会导致接口down，建议更换前先保证RBM切换到另一边；

接口板及交换网板与主控板共用版本，均不涉及版本升级等操作；

需要保证设备主控板中存在当前主控运行版本BIN文件；

接口子卡不支持热插拔，详情请见安装手册；

接口板更换完毕后，建议管理主上进行一次配置手工批备configuration manual-sync，保证主备流表一致。

更换操作过程参考链接：

M9000系列防火墙硬件更换操作指导——风扇

M9000系列防火墙硬件更换操作指导——主控板

M9000系列防火墙硬件更换操作指导——业务板

M9000系列防火墙硬件更换操作指导——接口板&交换网板

THANKS

www.h3c.com