HCIE-Security 备考指南

双机热备

HCIE 只是一个开始….

HCIE 仅是一个证书…懂得做人和处事比证书和技能更重要…

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security 双机热备需要掌握的知识点.....1
双机热备简介.....1
原理描述.....2
应用场景——主备备份.....10
应用场景——负载分担.....13
使用限制和注意事项.....16
典型组网一：业务接口工作在三层，上下行连接交换机.....18
典型组网二：业务接口工作在三层，上下行连接路由器.....22
典型组网三：业务接口工作在二层，上下行连接交换机.....24
典型组网四：业务接口工作在二层，上下行连接路由器.....25
双机热备 FAQ-故障类.....27
双机热备 FAQ-配置类.....30
双机热备 FAQ-原理类.....32
双机热备 FAQ-规格类.....33
双机热备 FAQ-其他类.....35
配置双机热备-Web.....35
配置流程-CLI.....40
配置 VRRP 备份组-CLI.....41
配置接口监控.....46
配置 VLAN 监控.....48
配置心跳接口.....51
启用双机热备.....54
配置备份方式.....57
双机热备配置检查和结果验证.....60
双机热备常用检查命令——display hrp.....62
命令功能.....62
命令格式.....63
参数说明.....63
使用实例.....63
双机热备常用检查命令——display vrrp.....65
命令功能.....65
命令格式.....65
参数说明.....65
使用指南.....65
使用实例.....65
举例：业务接口工作在三层，上行连接路由器，下行连接交换机的主备备份组网.....68
HCIE-Security 模拟面试问题及面试建议.....75

HCIE-Security 双机热备需要掌握的知识点

- VRRP/VGMP/HRP 基本知识；
- 双机热备组网方案；
- 双机热备定位手段

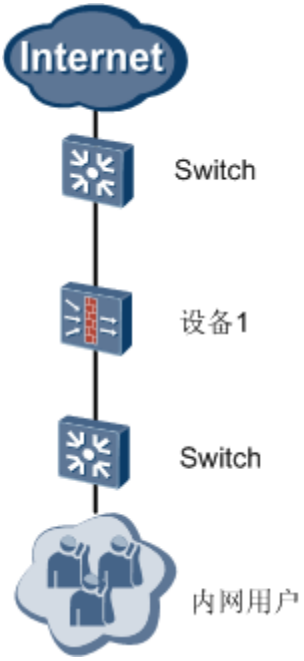
双机热备简介

介绍了双机热备的产生背景以及基本的功能。

如今各种各样的业务广泛部署在网络上，网络带宽也以指数级增长，网络短时间的中断就可能影响大量业务，造成重大损失。高可靠性成为网络建设的关键因素。

如图 1 所示，设备 1 部署在网络节点处，内网用户的业务流量都通过设备 1 进行转发。如果设备 1 出现故障，内外网之间的网络业务将会全部中断。

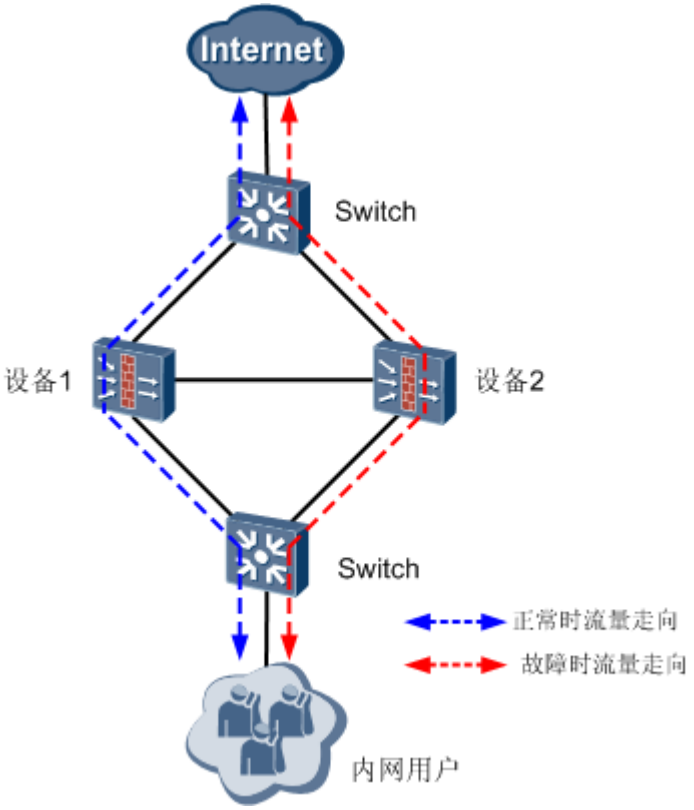
图 1 单条链路网络基本组网图



为了规避一台设备故障导致网络业务中断的风险，可以在网络节点处同时部署两台设备，形成双机热备组网。当其中一台设备出现故障时，业务流量能平滑地切换到备用设备上，保证业务不中断，使内外网用户交互的时候感知不到曾经出现过网络故障。

如图 2 所示，网络正常时业务流量通过设备 1 转发。当设备 1 发生故障时，业务流量切换到设备 2，通过设备 2 转发，从而保证了业务的正常转发，增强了网络的可靠性。

图 2 双机热备基本组网图



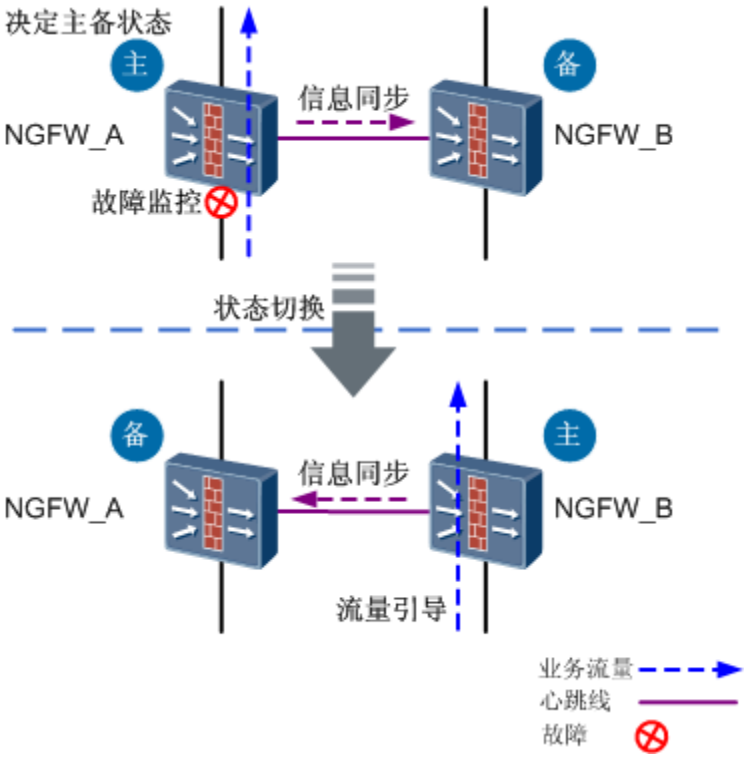
原理描述

介绍了双机热备中常用的协议及概念。

如图 1 所示，双机热备组网的建立和运行需要解决以下五个关键问题：

- 设备的主备状态是如何决定的？
- 如何监控并发现接口或设备故障？
- 发现故障后，如何保证设备的主备状态切换？
- 正常情况和故障后，流量是如何引导的？
- 如何进行信息同步，保证主备切换后业务不中断？

图 1 双机热备关键问题



下面将通过回答这五个关键问题来介绍双机热备的实现原理。

VGMP 决定主备状态

VGMP 管理组是双机热备的核心，它决定了设备的主备状态。

如图 2 所示，NGFW 提供两个 VGMP 管理组：Active 组和 Standby 组。缺省情况下，Active 组的优先级为 65001，Standby 组的优先级为 65000。

两台设备的 VGMP 管理组之间通过心跳接口交互 VGMP Hello 报文，从而比较优先级，协商出自己的 VGMP 管理组状态。

VGMP 管理组有三种状态：initialize、Active 和 Standby。

- initialize：VGMP 管理组处于未启用状态。
- Active：本端 VGMP 管理组的优先级比对端的 VGMP 管理组优先级高。
- Standby：本端 VGMP 管理组的优先级比对端的 VGMP 管理组优先级低。

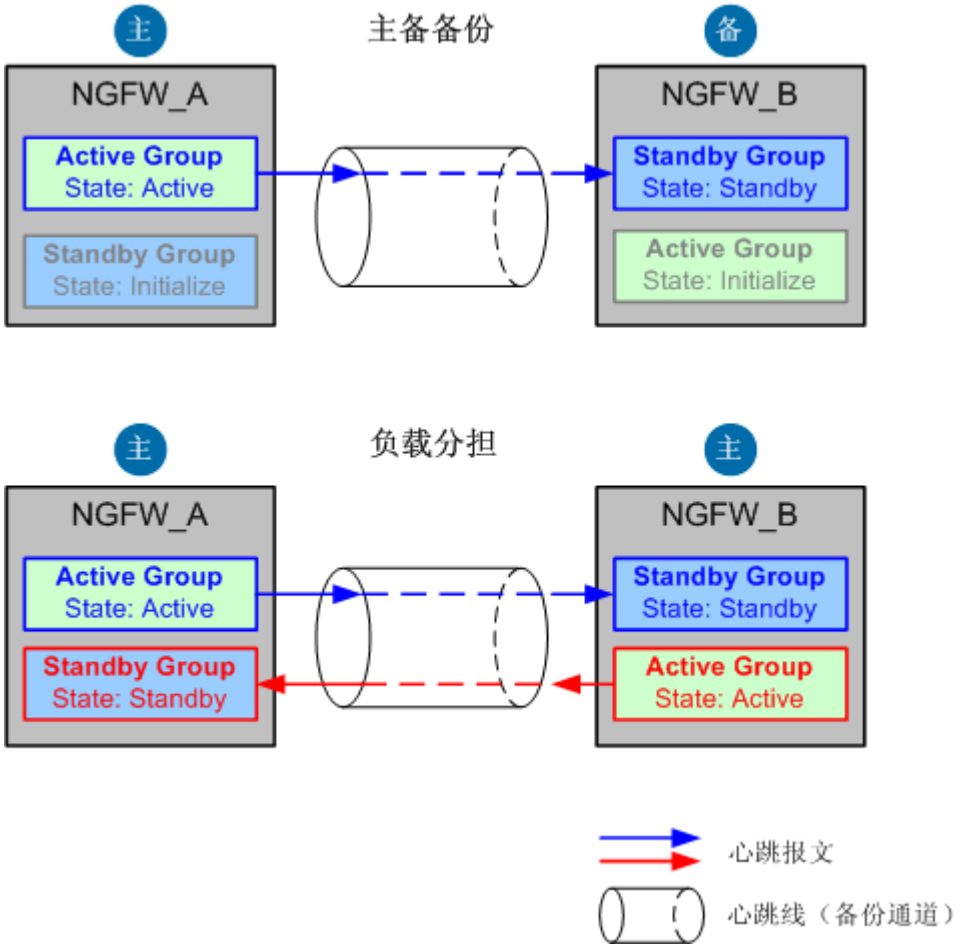
VGMP 管理组的状态决定了设备的主备状态，具体如下：

- 主备备份方式下，主用设备的 VGMP 管理组状态为 Active，备用设备的 VGMP 管理组状态为 Standby。

- 负载分担方式下，两台设备都存在状态为 Active 的 VGMP 管理组，都认为自身是主用设备，形成“双主”的情况。

  这时我们称先启动双机热备功能的设备为配置主设备，后启动双机热备功能的设备为配置备设备。

图 2 VGMP 管理组决定主备状态



VGMP 实现故障监控

VGMP 管理组能够监控接口或整机故障。接口或整机故障会影响 VGMP 管理组的优先级，从而影响 VGMP 管理组的主备状态，进而影响设备的主备状态。

监控接口故障

当 VGMP 管理组监控的接口故障时，VGMP 管理组优先级降低。一个接口故障，优先级降低 2。VGMP 管理组优先级=缺省情况优先级-2*N（注：N 为接口故障个数）

如表 1 所示，VGMP 管理组能够通过以下四种方式监控接口故障。

表 1 VGMP 管理组监控接口故障		
方式	适用的组网	操作
通过 VRRP 备份组监控接口	设备的业务接口工作在三层且连接交换机，设备与交换机后的设备（例如路由器或 PC）之间运行静态路由。	配置 VRRP 备份组。关于 VRRP 备份组的概念请参见通过 VRRP 备份组监控接口。
直接监控接口	设备的业务接口工作在三层连接路由器，设备与路由器间运行 OSPF。	配置 VGMP 管理组监控接口。
通过监控 VLAN 来监控接口	设备的业务接口工作在二层。	配置将接口加入 VLAN，VGMP 管理组监控 VLAN。VLAN 中每个接口故障，VGMP 管理组优先级降低 2。
监控远端接口	监控的不是设备上的，也不是与设备直连的接口，而是同一线路上更远端的接口。	配置 VGMP 管理组监控远端 IP 地址/域名。

监控整机故障

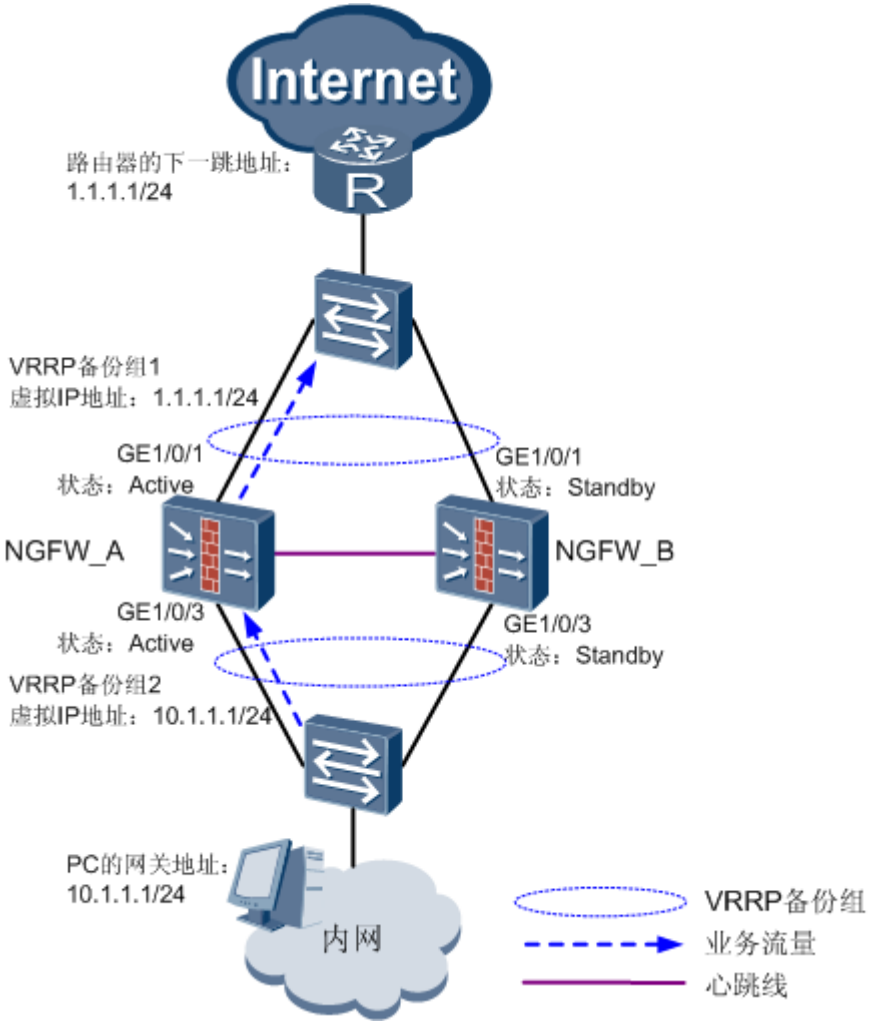
备用设备如果在三个周期内没有收到主用设备发送的 VGMP Hello 报文，则认为主用设备出现故障。这时，备用设备会将本端的 VGMP 管理组状态切换为 Active，从而成为主用设备。

当心跳线或者心跳接口故障时，两台设备都不能收到对方的 VGMP Hello 报文，都会切换成主用设备。但这时两台设备间无法进行配置和会话的备份，因此需要管理员及时处理。

通过 VRRP 备份组监控接口

如图 3 所示，VRRP 将同一个广播域的一组接口组织成一个 VRRP 备份组。在同一个 VRRP 备份组中，只有一个接口处于 Active 状态，其余接口都处于 Standby 状态。同一个 VRRP 备份组中的所有接口一起对外提供一个虚拟 IP 地址，只有状态为 Active 的接口能转发以虚拟 IP 地址作为下一跳的报文，从而转发业务流量。

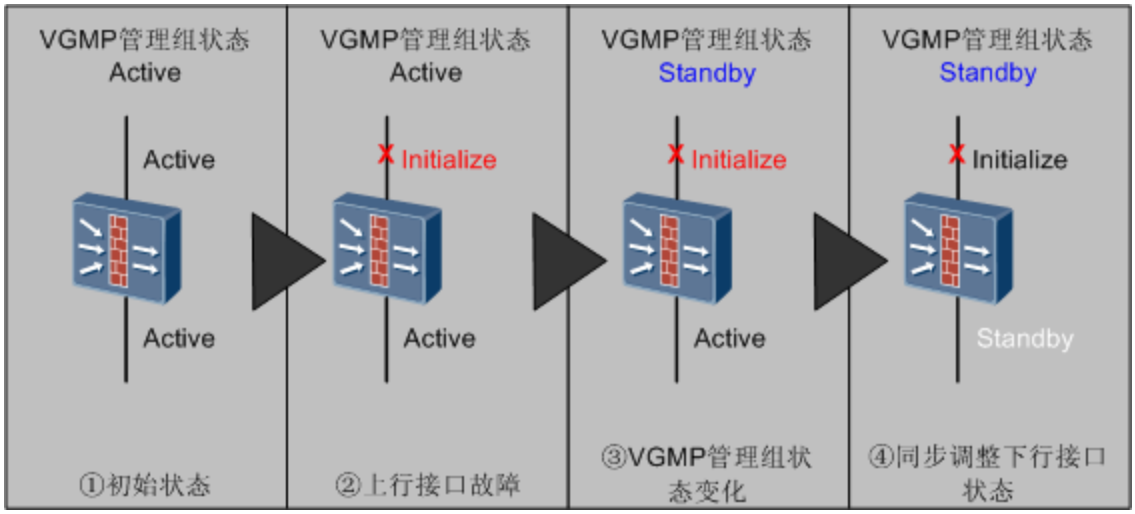
图 3 VRRP 备份组



每一个接口加入 VRRP 备份组时都需要指定其加入的 VGMP 管理组。VGMP 管理组的状态决定了组内的 VRRP 备份组成员接口的状态：当 VGMP 管理组的状态为 Active 时，组内成员接口状态为 Active，当 VGMP 管理组的状态为 Standby 时，组内成员接口状态为 Standby。

如图 4 所示，VGMP 管理组状态切换时，会强制组内所有 VRRP 备份组的成员接口统一切换状态。这样就能保证上下行业务接口同步切换状态，从而保证业务的来回流量都通过备用设备转发，业务不中断。

图 4 VGMP 管理组控制 VRRP 备份组成员接口状态



VGMP 控制状态切换

由于 VGMP 管理组能够决定设备主备状态和实现故障监控，因此 VGMP 管理组能够控制故障时设备状态的切换。

如图 5 所示，VGMP 管理组控制设备状态切换的具体过程如下：

- **主备备份**

  正常运行时，NGFW_A 的 Active 组的优先级为 65001，状态为 Active，因此 NGFW_A 为主用设备。

  当 NGFW_A 的一个监控接口故障时，NGFW_A 的 Active 组的优先级降低到 64999，低于 NGFW_B 的 Standby 组的优先级，因此 NGFW_A 的 Active 组的状态切换为 Standby，NGFW_A 切换成备用设备。NGFW_B 的 Standby 组切换到 Active 状态，NGFW_B 成为新的主用设备。

  NGFW_A 的故障恢复后，Active 组的优先级恢复到 65001，重新高于 NGFW_B 的 Standby 组的优先级 65000，因此 NGFW_A 会重新“抢占”成为主用设备。

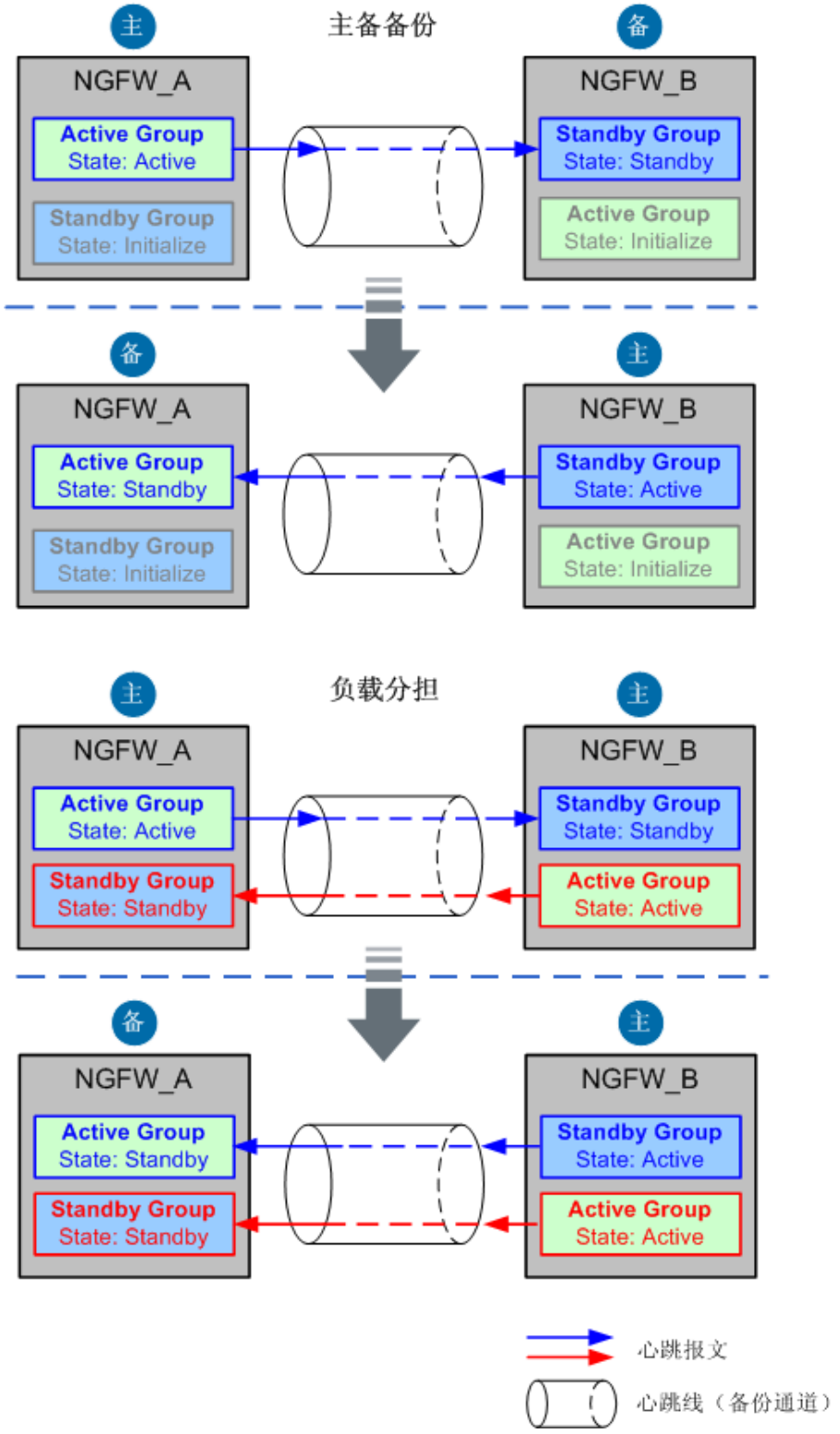
  但是如果关闭了抢占功能，则 NGFW_A 故障恢复后，仍是备用设备，不处理业务。

- **负载分担**

  正常运行时，NGFW_A 的 Active 组与 NGFW_B 的 Standby 组构成一组“主备”，NGFW_B 的 Active 组与 NGFW_A 的 Standby 组也构成一组“主备”。这样 NGFW_A 与 NGFW_B 就都认为自己是主用设备，形成“双主”组网。这时流量通过哪台设备转发是由上下行设备的路由决定的。

当 NGFW_A 的监控接口故障时，NGFW_A 的 Active 组与 Standby 组的优先级都降低，分别低于 NGFW_B 的 Standby 组和 Active 组，状态都切换成 Standby。这样 NGFW_A 就成为了备用设备，所有流量都通过 NGFW_B 转发了。

图 5 VGMP 管理组控制状态切换



流量引导

双机热备组网中，无论正常运行时还是发生故障状态切换后，都需要将流量引导到主用设备上转发。

不同组网下流量引导的实现方式不同，具体如表 2 所示。

表 2 不同组网下流量引导的实现方式

组网	实现方式
设备的业务接口工作在三层且连接交换机，设备与交换机后的设备（例如路由器或 PC）之间运行静态路由。	只有主用设备能够转发下一跳为虚拟 IP 地址的报文，因此流量通过主用设备转发。
设备的业务接口工作在三层连接路由器，设备与路由器间运行 OSPF。	主用设备正常发布路由，备用设备发布的路由 Cost 值增加 65500，因此流量通过主用设备转发。
设备的业务接口工作在二层，加入到同一个 VLAN。	主用设备的 VLAN 能够转发流量，备用设备的 VLAN 不能转发流量，因此流量通过主用设备转发。

HRP 实现信息同步

NGFW 通过执行命令（通过 Web 配置实际上也是在执行命令）来实现用户所需的各种功能。如果备用设备切换为主用设备前，配置命令没有备份到备用设备，则备用设备无法实现主用设备的相关功能，从而导致业务中断。

NGFW 属于状态检测防火墙，对于每一个动态生成的会话连接，都有一个会话表项与之对应。主用设备处理业务过程中创建了很多动态会话表项；而备用设备没有流量经过，因此没有创建会话表。如果备用设备切换为主用设备前，会话表项没有备份到备用设备，则会导致先前经过主用设备的业务流量因为无法匹配会话表而中断，从而影响业务正常进行。

为了实现主用设备出现故障时备用设备能平滑地接替工作，必须在主用和备用设备之间备份关键配置命令和会话表状态信息。为此，NGFW 引入 HRP 备份功能。启动 HRP 备份功能后，关键配置命令和会话表状态信息会实时同步备份到备用设备。

在双机热备组网中，指定心跳线作为专门的备份通道，用于备份配置命令和状态信息。

主备设备通过心跳线交互报文了解对方状态，以及实现配置命令和状态信息的备份。心跳线两端的设备上的接口称为心跳接口。

应用场景——主备备份

当您需要所有业务流量通过一台设备转发，而另一台设备作为备份保证业务不中断时，建议您使用主备备份的双机热备。

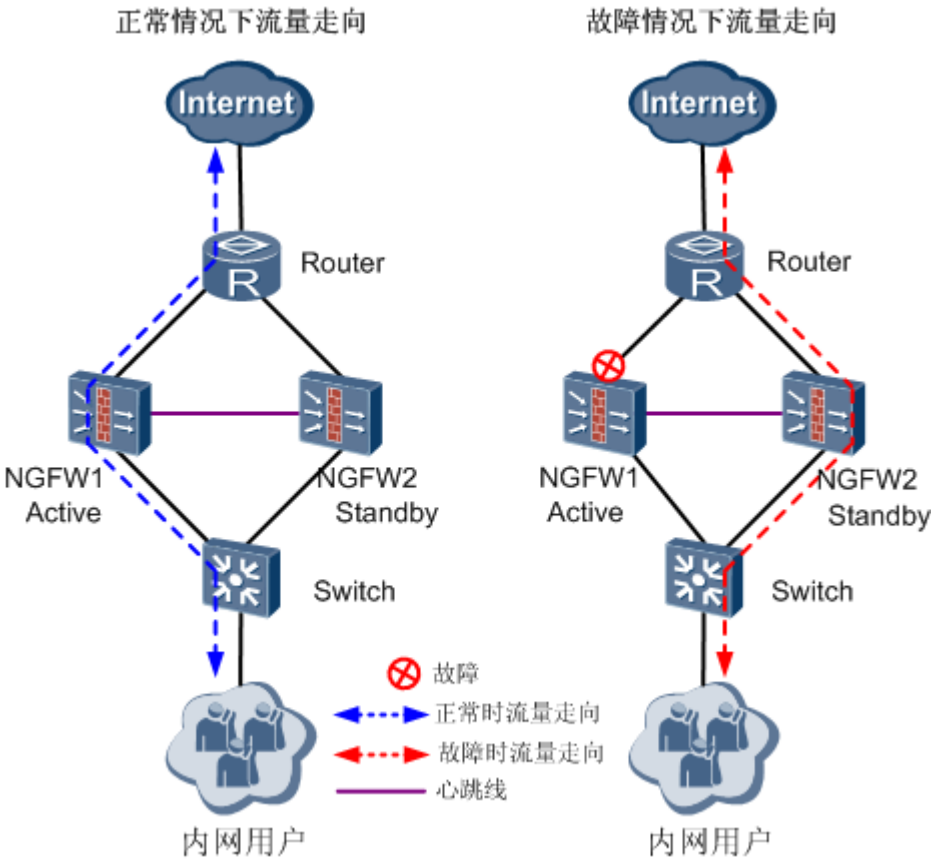
定义

主备备份指正常情况下仅由主用设备处理业务，备用设备空闲；当主用设备接口、链路或整机故障时，备用设备切换为主用设备，接替主用设备处理业务。

主备备份可以有效防止一台设备出现故障导致的网络中断，大大提高了网络的可靠性，常用于重点业务的入口或接入点上，像企业的 Internet 接入点，银行的数据库服务器等。

如图 1 所示，在网络入口处同时部署两台 NGFW 设备，NGFW1 为主用设备，处理业务；NGFW2 为备用设备，不处理业务，只通过心跳线同步 NGFW1 的配置命令和状态信息。当 NGFW1 的接口、链路或整机发生故障时，NGFW2 立即切换为主用设备接替 NGFW1 处理业务，从而保证业务的不中断。

图 1 主备备份应用场景



典型组网

根据主备设备的上下行业务接口类型，以及上下行设备的类型，主备备份的双机热备场景可以分成以下三种组网。

- **业务接口工作在三层，上下行连接交换机**

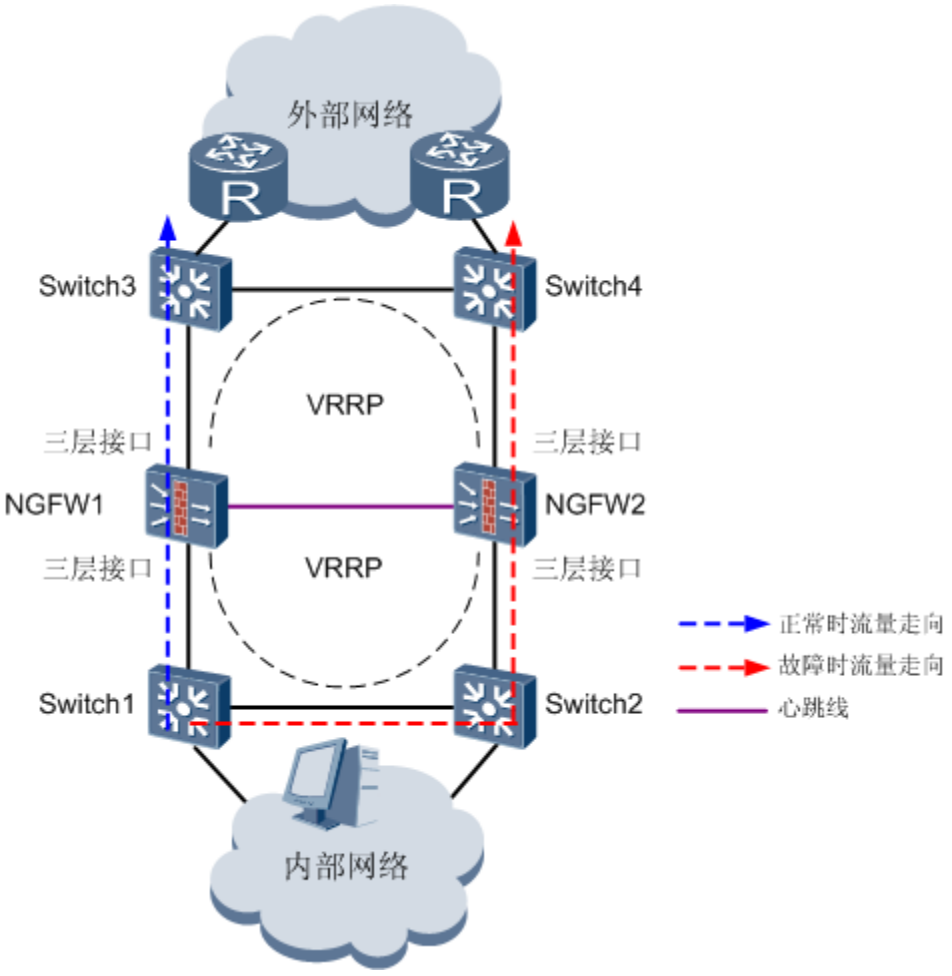
  如图 2 所示，NGFW 的上、下行业务接口工作在三层，与二层交换机直连。NGFW 与交换机后的路由器或者 PC 之间运行静态路由。

  此组网是 NGFW 推荐的典型双机热备组网，是已经应用得很成熟的组网方式，广泛适用于中小型网络或 NGFW 作网关的网络。

  说明：

  与图 1 相比，图 2 中上下行各部署两台设备，可以进一步提升网络可靠性。

  图 2 业务接口工作在三层，上下行连接交换机的组网

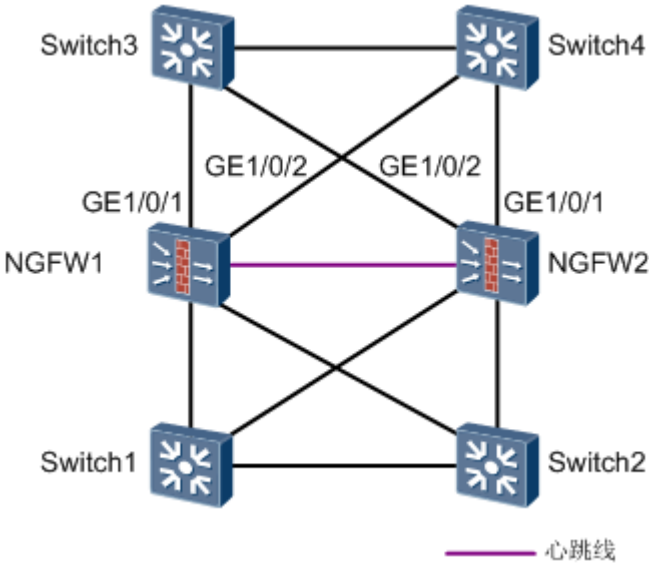


在图 2 的基础上，将 NGFW1 的上行接口与 Switch4 相连，下行接口与 Switch2 相连；将 NGFW2 的上行接口与 Swith3 相连，下行接口与 Swith1 相连。

这样就组成了双机热备的全冗余组网，如图 3 所示。

双机热备的全冗余组网能够进一步提升网络可靠性，避免多条链路故障时业务中断。例如，当 NGFW1 的 GE1/0/1、GE1/0/2 和 NGFW2 的 GE1/0/1 这三个接口都故障时，业务流量依然能够通过 NGFW2 的 GE1/0/2 接口转发。

图 3 双机热备全冗余组网



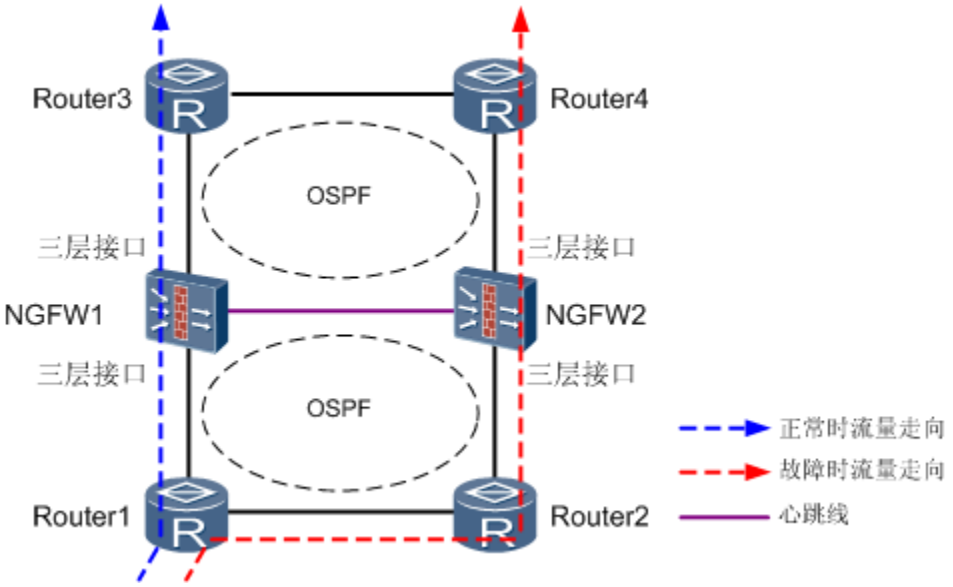
- **业务接口工作在三层，上下行连接路由器**

如图 4 所示，NGFW 的上、下行业务接口工作在三层，与路由器直连。NGFW 与上、下行路由器之间运行 OSPF 协议。

此组网也是 NGFW 推荐的典型双机热备组网，是已经应用得很成熟的组网方式，广泛适用于大中型网络。

此组网可以与业务接口工作在三层，上下行连接交换机的组网结合使用，即组成上行连接路由器，下行连接交换机的组网。

图 4 业务接口工作在三层，上下行连接路由器的组网



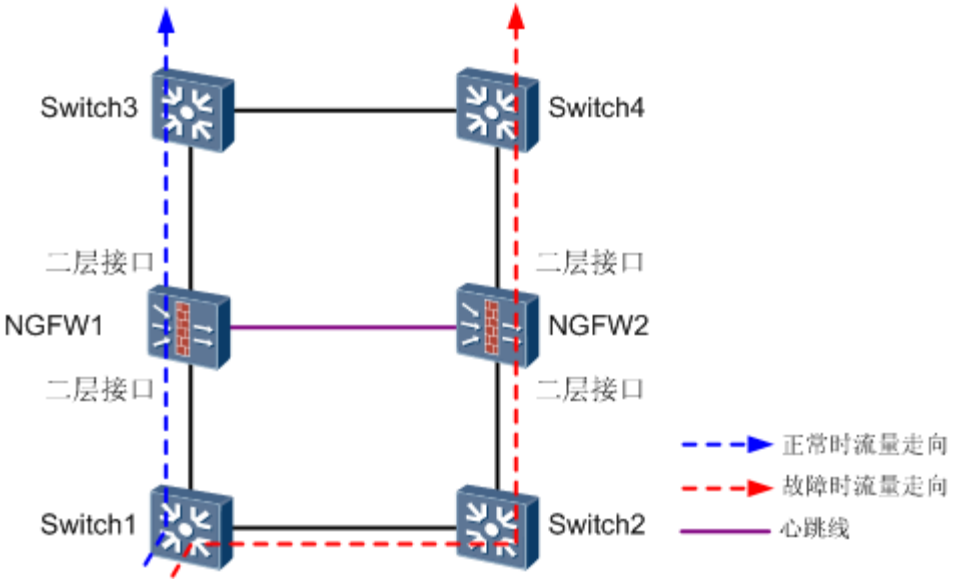
- **业务接口工作在二层，上下行连接交换机**

  如图 5 所示，NGFW 的上、下行业务接口工作在二层，与二层交换机直连。每台 NGFW 的上下行业务接口加入到同一个 VLAN。

  在此组网中，NGFW 透明接入到原有交换机网络，不改变网络拓扑。

  由于 NGFW 的业务接口工作在二层，因此不能运行与 IP 地址相关的业务，例如 VPN。

  图 5 业务接口工作在二层，上下行连接交换机的组网



应用场景——负载分担

当业务流量较大，需要两台设备共同处理并且互为备份时，建议您使用负载分担的双机热备。

定义

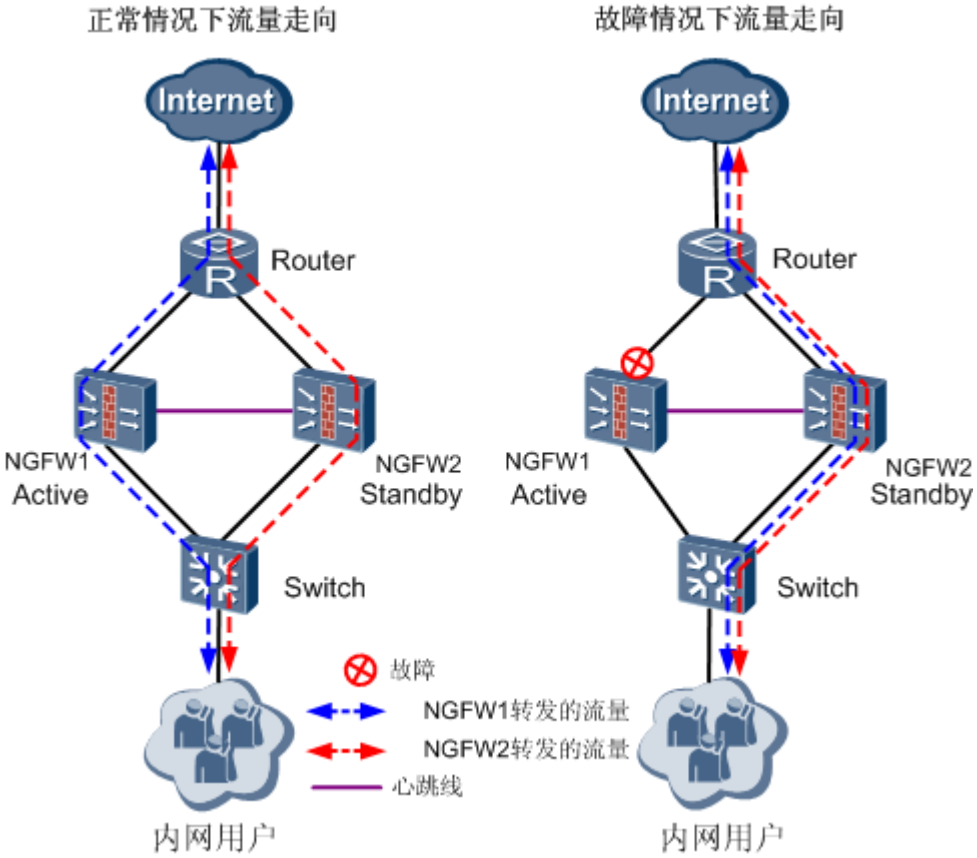
所谓负载分担，也可以称为“互为主备”，即两台设备同时处理业务。当其中一台设备发生故障时，另外一台设备会立即承担其业务，保证原来需要通过这台设备转发的业务不中断。在网络规划时，请保证经过两台设备的总流量不超过单台设备的处理能力。

两台设备共同处理业务，可以提高网络的转发效率，减轻单台设备的处理压力。

如图 1 所示，在网络入口处同时部署两台 NGFW 设备。正常情况下，业务流量分别送到两台 NGFW 上进行处理。每台 NGFW 既作为主用设备处理业务，也作为备用设备通过心跳线同步另外一台 NGFW 的配置及状态信息。

如果 NGFW1 的接口、链路或整机发生故障，NGFW2 会立即承担全部业务流量的转发。

图 1 负载分担应用场景



典型组网

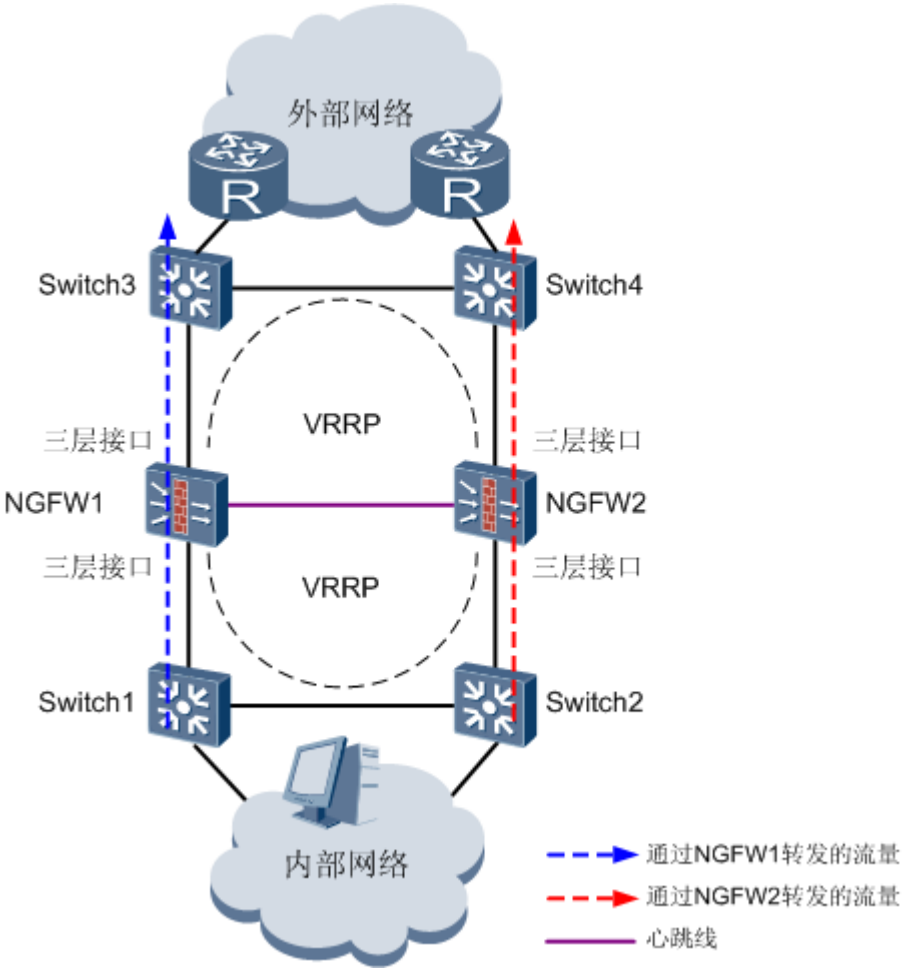
根据两台设备的上下行业务接口类型，以及上下行设备的类型，负载分担的双机热备场景可以分成以下三种组网。

- **业务接口工作在三层，上下行连接交换机**

如图 2 所示，NGFW 的上、下行业务接口工作在三层，与二层交换机直连。NGFW 与交换机后的路由器或者 PC 之间运行静态路由。

此组网的两台 NGFW 共同处理业务，广泛适用于中小型网络或 NGFW 作网关的网络。

图 2 业务接口工作在三层，上下行连接交换机的组网

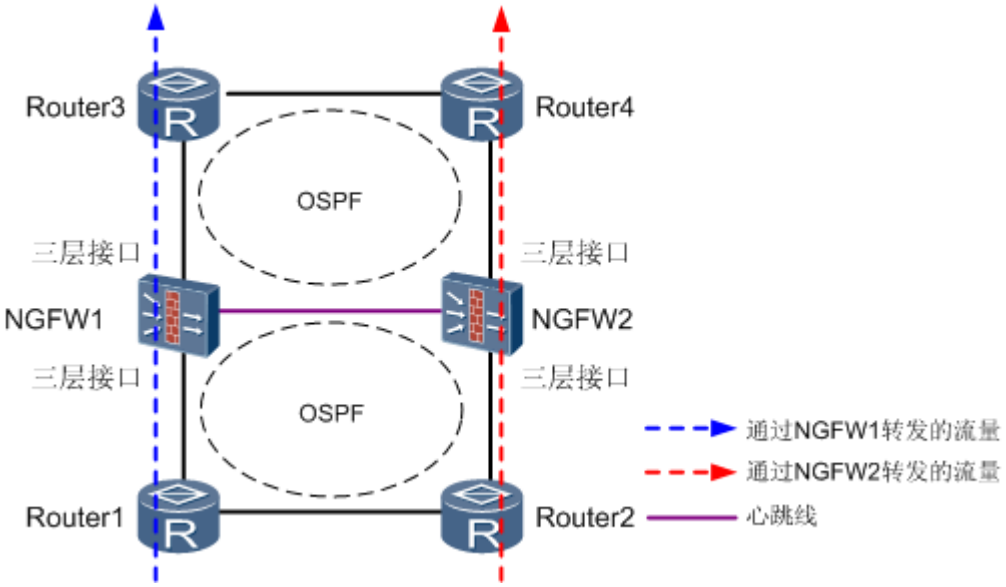


- **业务接口工作在三层，上下行连接路由器**

如图 3 所示，NGFW 的上、下行业务接口工作在三层，与路由器直连。NGFW 与上、下行路由器之间运行 OSPF 协议。

此组网的两台 NGFW 共同处理业务，广泛适用于大中型网络。

图 3 业务接口工作在三层，上下行连接路由器的组网



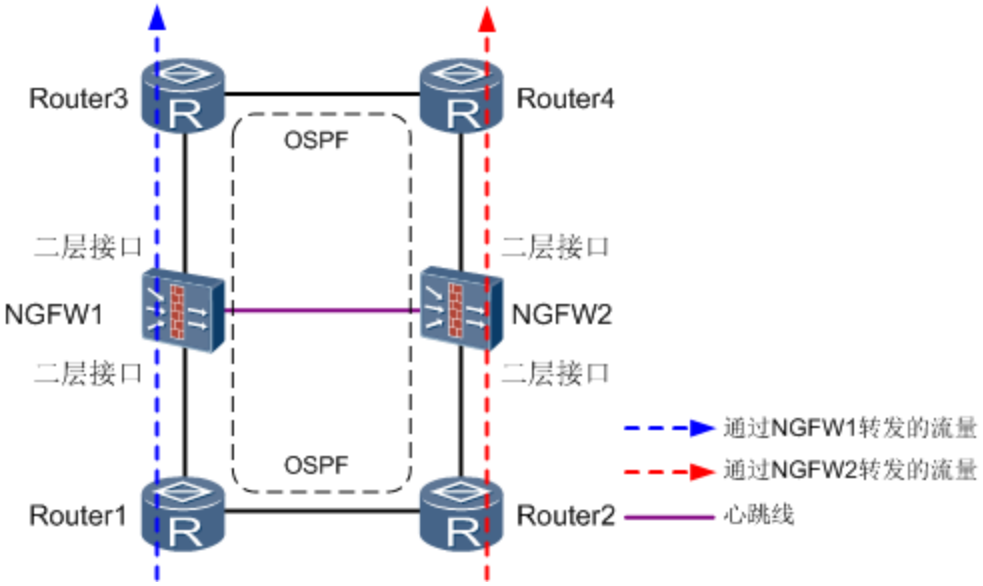
- **业务接口工作在二层，上下行连接路由器**

  如图 4 所示，NGFW 的上、下行业务接口工作在二层，与路由器直连。上、下行路由器之间运行 OSPF 动态路由协议。每台 NGFW 的上下行业务接口加入到同一个 VLAN。

  在此组网中，两台 NGFW 共同处理业务，而且 NGFW 透明接入到原有路由器网络，不改变网络拓扑。

  由于 NGFW 的业务接口工作在二层，因此不能运行与 IP 地址相关的业务，例如 VPN。

  图 4 业务接口工作在二层，上下行连接路由器的组网



使用限制和注意事项

介绍双机热备中的使用限制，包括硬件限制、软件限制、与 NAT 结合使用的限制和与 IPSec 结合使用的限制。

硬件限制

- 目前只支持两台设备进行双机热备。
- 主备设备的产品型号和版本必须相同。
- 主备设备接口卡的位置、类型和数目都必须相同，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。
- 如果使用二层接口作为心跳口，需要将二层接口加入 VLAN，创建 Vlanif 并配置 Vlanif 的 IP 地址。然后使用 Vlanif 接口作为心跳口，并配置 **remote** 参数来指定对端设备心跳口的 IP 地址。

软件限制

- 主备设备的软件版本必须一致。否则，不同版本的软件的某些配置命令或会话表结构可能不同，从而导致主备设备在备份配置命令和状态时产生错误。
- 主备设备的 Bootrom 版本必须一致。
- 建议主备设备的配置文件均为初始文件。否则，可能由于两台设备的配置冲突导致主备切换后出现问题。
- 主备设备需要选择相同的业务接口和心跳口。例如主用设备选择 GigabitEthernet1/0/1 作为业务接口，选择 GigabitEthernet1/0/7 作为心跳口，那么备用设备也需要这样选择。
- 主备设备的对应接口必须加入到相同的安全区域。如主用设备的 GigabitEthernet1/0/1 接口加入了 Trust 区域，那么备用设备的 GigabitEthernet1/0/1 接口也必须加入 Trust 区域。
- 心跳口的 MTU 值必须是缺省值 1500。
- 主备设备业务接口的 IP 地址必须固定，因此双机热备特性不能与 PPPoE 拨号、DHCP Client 等自动获取 IP 地址的特性结合使用。
- 双机热备成功建立后，如果希望使用 Web 界面更改“运行模式”（从“主备备份”切换成“负载分担”，或者从“负载分担”切换成“主备备份”），则必须先清空所有双机热备的配置。

与 NAT 结合使用的限制

- 双机热备与 NAT 结合使用时，主备设备的上下行业务接口必须为三层接口。
- 双机热备的负载分担场景下，当两台 NGFW 上都需要配置 NAT 地址池时，为避免出现 NAT 地址池的端口冲突问题，需要在一台 NGFW 上配置 hrp nat ports-segment primary 命令，另外一台 NGFW 上配置 hrp nat ports-segment secondary 命令。

- 在负载分担方式的双机热备组网中，配置地址池方式的源 NAT 策略时，如果只配置一个 NAT 地址池且不允许端口转换，两台 NGFW 可能会将不同主机发来的流量的源 IP 地址转换成同一个 IP 地址，导致冲突。

  此时，建议您创建两个 NAT 地址池，针对不同源 IP 的流量使用不同的地址池进行 NAT 转换。例如，双机热备的两台设备为 NGFW_A 和 NGFW_B，NGFW_A 和 NGFW_B 分别处理 10.1.1.1～10.1.1.128 和 10.1.1.129～10.1.1.254 网段主机的流量。配置不允许端口转换的地址池方式源 NAT 时，需要创建两个 NAT 地址池 addressgroup1 和 addressgroup2，并配置两条源 NAT 策略，将 10.1.1.1～10.1.1.128 网段主机发来流量的源地址转换为 addressgroup1 中的地址、将 10.1.1.129～10.1.1.254 网段主机发来流量的源地址转换为 addressgroup2 中的地址。

与 IPSec 结合使用的限制

- 双机热备与 IPSec 结合使用时，主备设备的建立隧道的业务接口必须为三层接口。
- 双机热备与 IPSec 结合使用时，双机热备和 IPSec 的配置与单独使用时没有区别。
- 主用设备配置的 IPSec 策略会备份到备用设备上，但是由于接口上的配置不会备份到备用设备，因此需要在备用设备的出接口上应用备份过来的 IPSec 策略。
- 如果设备作为 IPSec 隧道发起方，则必须要执行命令 **local-address** *ip-address*，设置本端发起协商的地址为 VRRP 备份组的虚拟 IP 地址。

典型组网一：业务接口工作在三层，上下行连接交换机

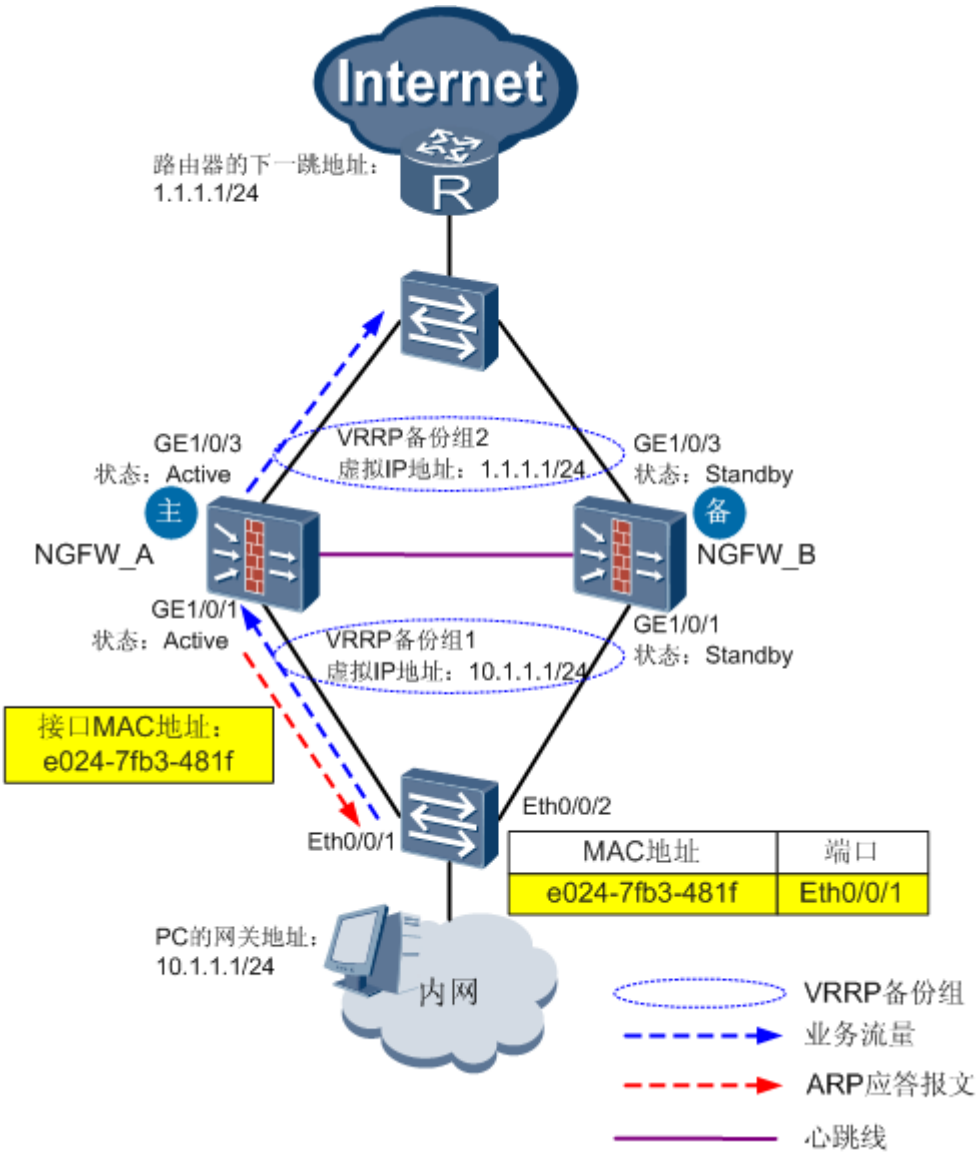
介绍设备的业务接口工作在三层，上下行连接交换机的组网。

如图 1 所示，NGFW 的上、下行业务接口工作在三层，分别与二层交换机直连。

此组网既可以用于主备备份方式，又可以用于负载分担方式的双机热备。

主备备份

图 1 业务接口工作在三层，上下行连接交换机的主备备份组网



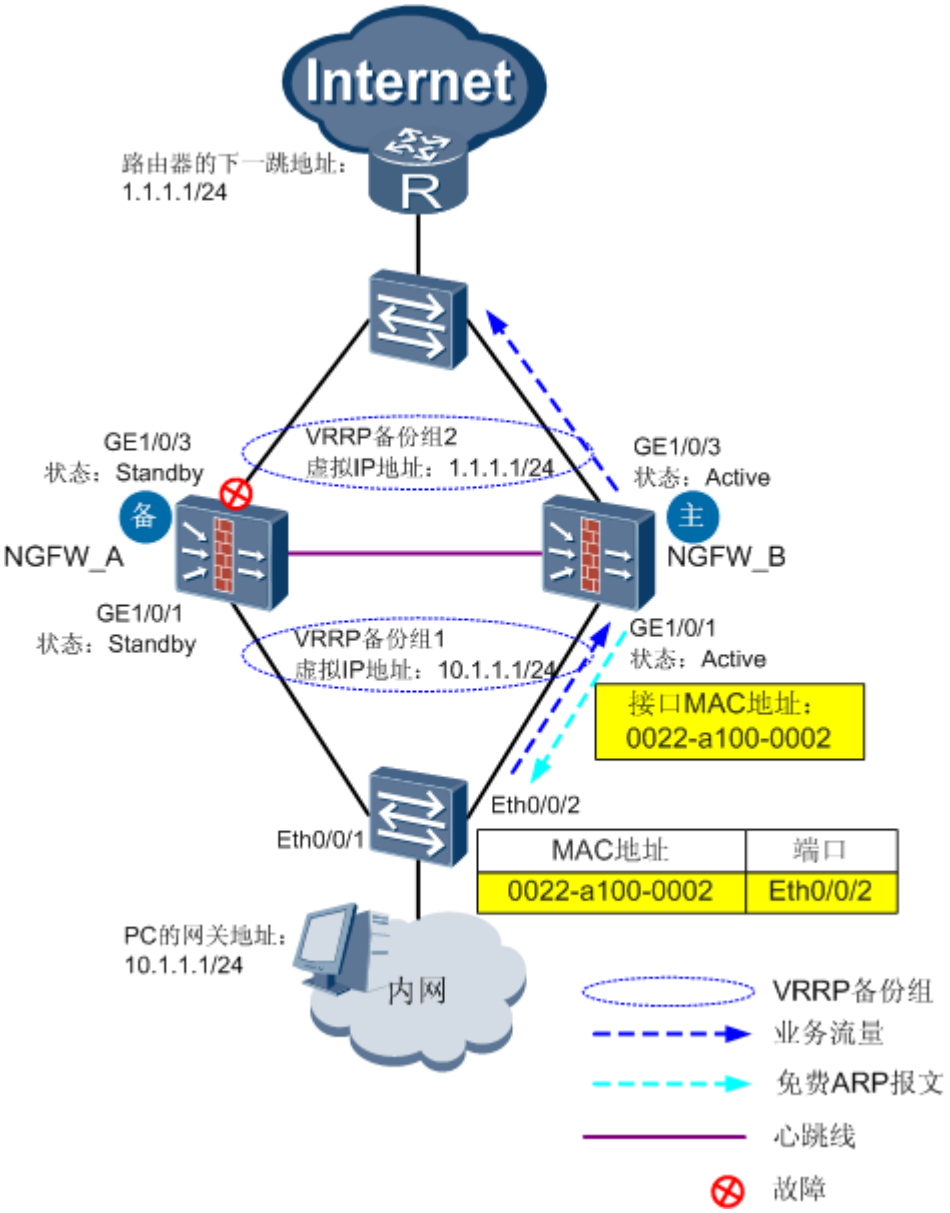
如图 1 所示，在 NGFW_A 的业务接口上配置 VRRP 备份组，并加入 Active 组。在 NGFW_B 的业务接口上配置 VRRP 备份组，并加入 Standby 组。将内网 PC 的网关设置为 VRRP 备份组的虚拟 IP 地址。

正常情况下，网络运行情况分析如下：

1. PC 将用于请求网关 MAC 地址的 ARP 报文发送给交换机。交换机在网络中广播此 ARP 报文。
2. 只有状态为 Active 的接口（NGFW_A 的 GE1/0/1）才会应答 ARP 报文，反馈接口的 MAC 地址。
3. 交换机会记录接口 MAC 地址与端口 Eth0/0/1 的关系，然后将 MAC 地址发送给 PC。
4. PC 将业务报文发送给交换机，业务报文的目的 MAC 地址为 NGFW_A 的 GE1/0/1 接口 MAC 地址。
5. 交换机根据记录的 MAC 地址与端口的关系，将报文从端口 Eth0/0/1 转发，发送给 NGFW_A。

这样在正常情况下，内网 PC 发出的流量就都通过主用设备 NGFW_A 转发了。

图 2 发生故障后



如图 2 所示，当 NGFW_A 发生故障后，网络运行情况分析如下：

1. 当 NGFW_A 的业务接口故障时，NGFW_A 切换成备用设备，NGFW_B 成为主用设备。
2. 新主用设备 NGFW_B 会对外发送免费 ARP，更新上下行交换机的 MAC 地址与端口的对应关系（将 NGFW_B 的 GE1/0/1 接口 MAC 地址与端口 Eth0/0/2 对应）。
3. 当 PC 将业务报文发送给交换机时，报文将从交换机的端口 Eth0/0/2 转发，发送给 NGFW_B。

这样在 NGFW_A 故障时，内网 PC 发出的流量就都通过新主用设备 NGFW_B 转发了。

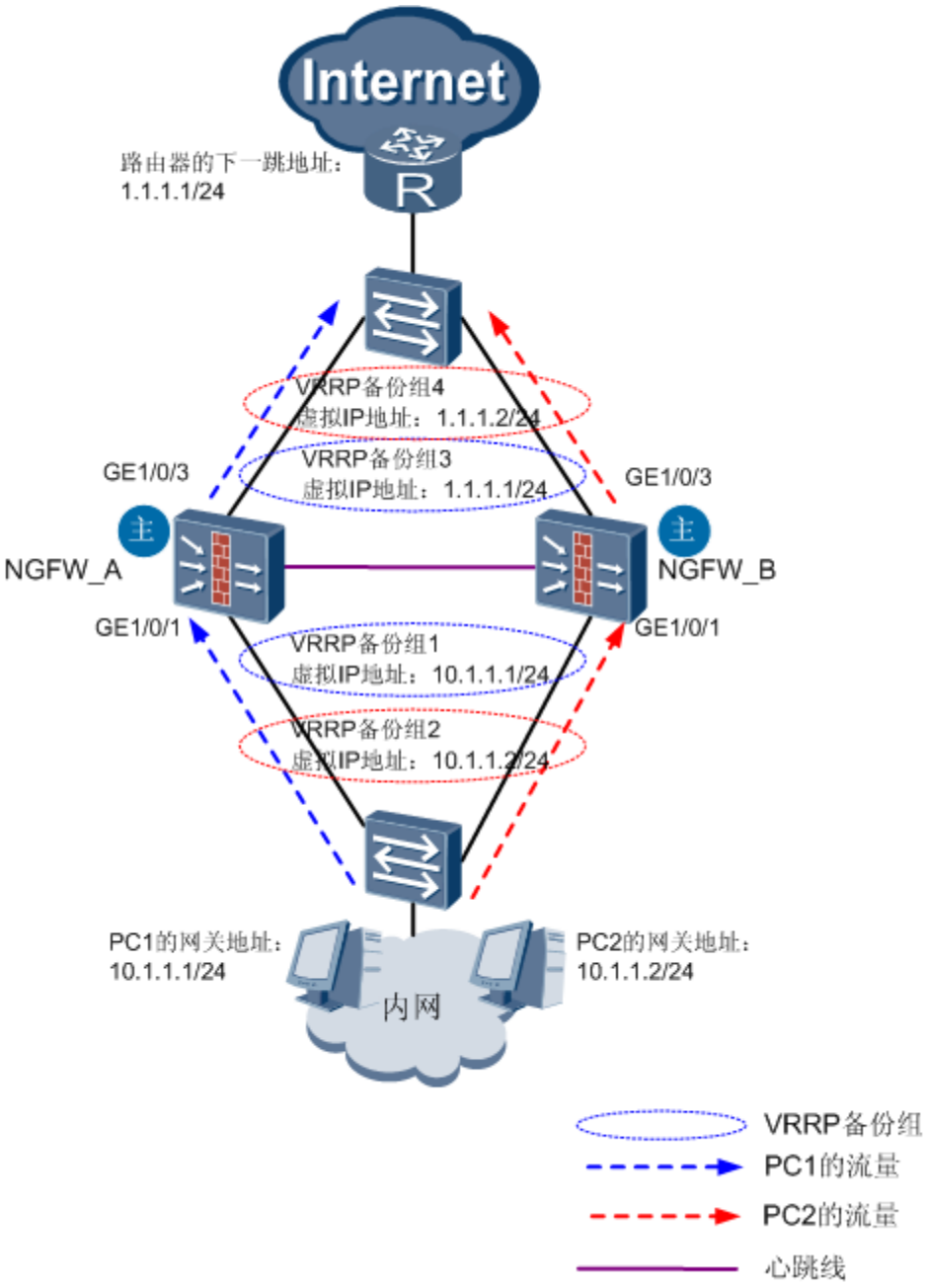
负载分担

如图 3 所示，按照如下配置部署负载分担组网：

- 在 NGFW_A 的 GE1/0/1 上配置 VRRP 备份组 1，加入 Active 组；配置 VRRP 备份组 2，加入 Standby 组。
- 在 NGFW_B 的 GE1/0/1 上配置 VRRP 备份组 1，加入 Standby 组；配置 VRRP 备份组 2，加入 Active 组。
- 将内网一部分 PC 的网关设置为 VRRP 备份组 1 的虚拟 IP 地址，另一部分 PC 的网关设置为 VRRP 备份组 2 的虚拟 IP 地址。
- 在 NGFW_A 的 GE1/0/3 上配置 VRRP 备份组 3，加入 Active 组；配置 VRRP 备份组 4，加入 Standby 组。
- 在 NGFW_B 的 GE1/0/3 上配置 VRRP 备份组 3，加入 Standby 组；配置 VRRP 备份组 4，加入 Active 组。
- 在 Router 上配置两条静态路由，下一跳分别为 VRRP 备份组 3 的虚拟 IP 地址和 VRRP 备份组 4 的虚拟 IP 地址。

这样正常情况下，NGFW_A 的接口 GE1/0/1 转发下一跳为 VRRP 备份组 1 的虚拟 IP 地址的报文，NGFW_B 的接口 GE1/0/1 转发下一跳为 VRRP 备份组 2 的虚拟 IP 地址的报文。一部分 PC 的流量通过 NGFW_A 转发，另一部分 PC 的流量通过 NGFW_B 转发，形成负载分担。

图 3 业务接口工作在三层，上下行连接交换机的负载分担组网



典型组网二：业务接口工作在三层，上下行连接路由器

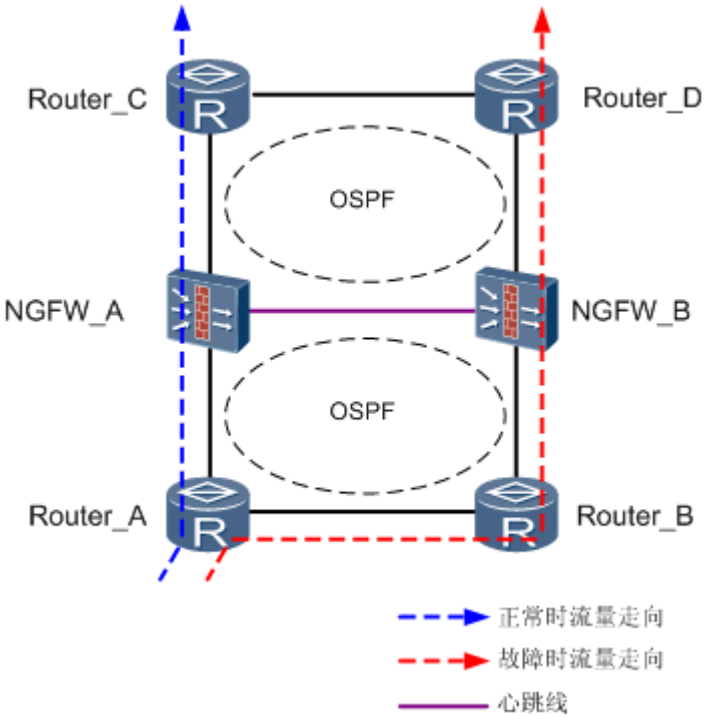
介绍了设备的业务接口工作在三层，上下行连接路由器的组网。

如图 1 所示，NGFW 上、下行业务接口工作在三层，与路由器直连。NGFW 与上、下行路由器之间运行 OSPF 协议。

此组网既可以用于主备备份方式，又可以用于负载分担方式的双机热备。

主备备份

图 1 业务接口工作在三层，上下行连接路由器的主备备份组网



如图 1 所示，主用设备 NGFW_A 正常对外发布路由，备用设备 NGFW_B 发布的路由 Cost 值增加 65500（缺省值，可调整）。

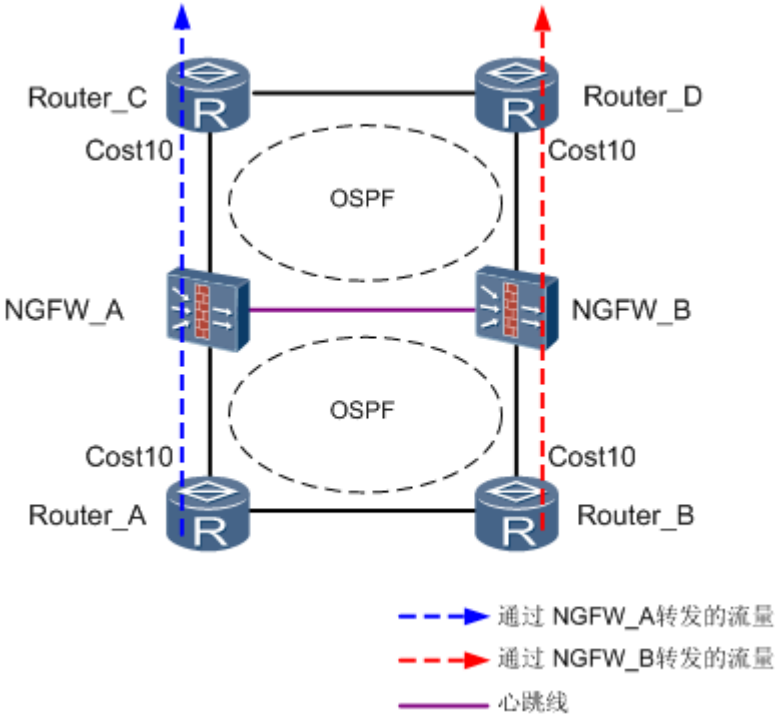
上下行路由器在转发流量时会选择开销（Cost 值）更小的路径，因此流量通过主用设备 NGFW_A 转发。

当 NGFW_A 的业务接口故障时，NGFW_A 切换成备用设备，NGFW_B 成为主用设备。

这时 NGFW_B 正常对外发布路由，NGFW_A 发布的路由 Cost 值增加 65500。这样路由重新收敛后，流量通过 NGFW_B 转发。

负载分担

图 2 业务接口工作在三层，上下行连接路由器的负载分担组网



如图 2 所示，负载分担方式下，NGFW_A 与 NGFW_B 都是主用设备，都正常对外发布路由。

因此需要在 Router_A(C)连接 NGFW_A 和 Router_B(D)连接 NGFW_B 的接口上配置相同的 Cost 值，保证流量通过 NGFW_A 与 NGFW_B 共同转发。

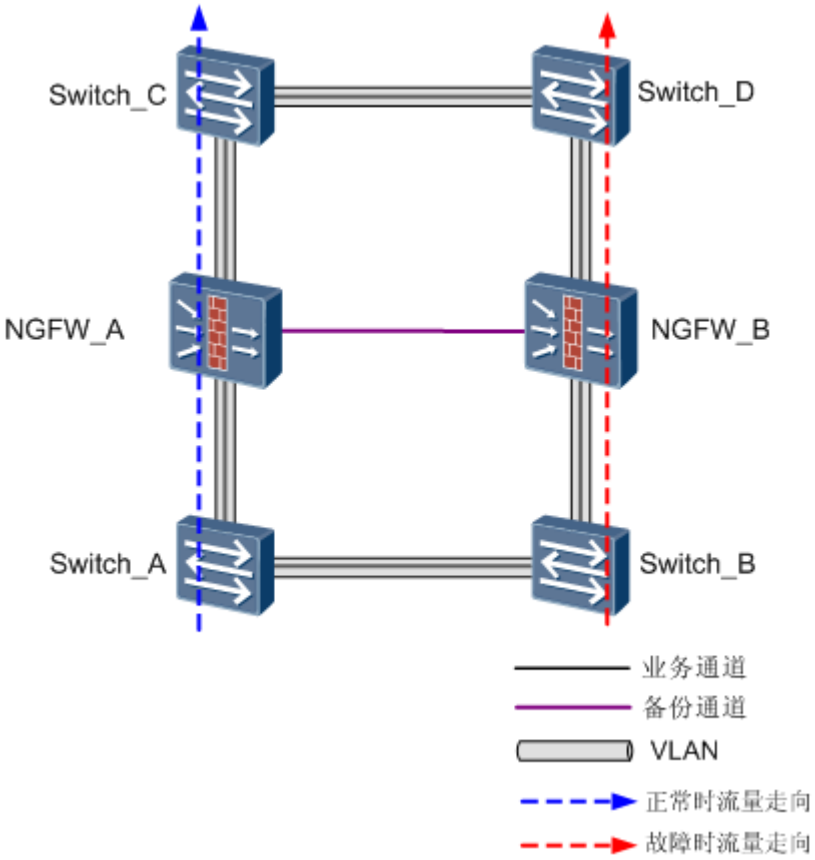
典型组网三：业务接口工作在二层，上下行连接交换机

介绍了设备的业务接口工作在二层，上下行连接交换机的组网。

如图 1 所示，NGFW 的上、下行业务接口工作在二层，分别与二层交换机直连。每台 NGFW 的上下行业务接口加入到同一个 VLAN。

此组网只支持主备备份方式的双机热备。

图 1 业务接口工作在二层，上下行连接交换机组网图



主备备份

如图 1 所示，主用设备 NGFW_A 上的 VLAN 被启用，能够转发流量。备用设备 NGFW_B 上的 VLAN 被禁用，不能转发流量。因此流量都从主用设备 NGFW_A 转发。

注意：

此种组网不支持负载分担方式。因为如果工作于负载分担方式，则两台设备上的 VLAN 都被启用，都能够转发流量，整个网络就会形成环路。

当 NGFW_A 发生故障时，NGFW_A 切换成备用设备，NGFW_B 成为主用设备。

NGFW_A 切换成备用设备时，VLAN 内所有接口都会 Down 然后 Up 一次。这会导致上下行交换机更新自身 MAC 转发表，重新学习 MAC 地址，将流量引导到 NGFW_B 上。

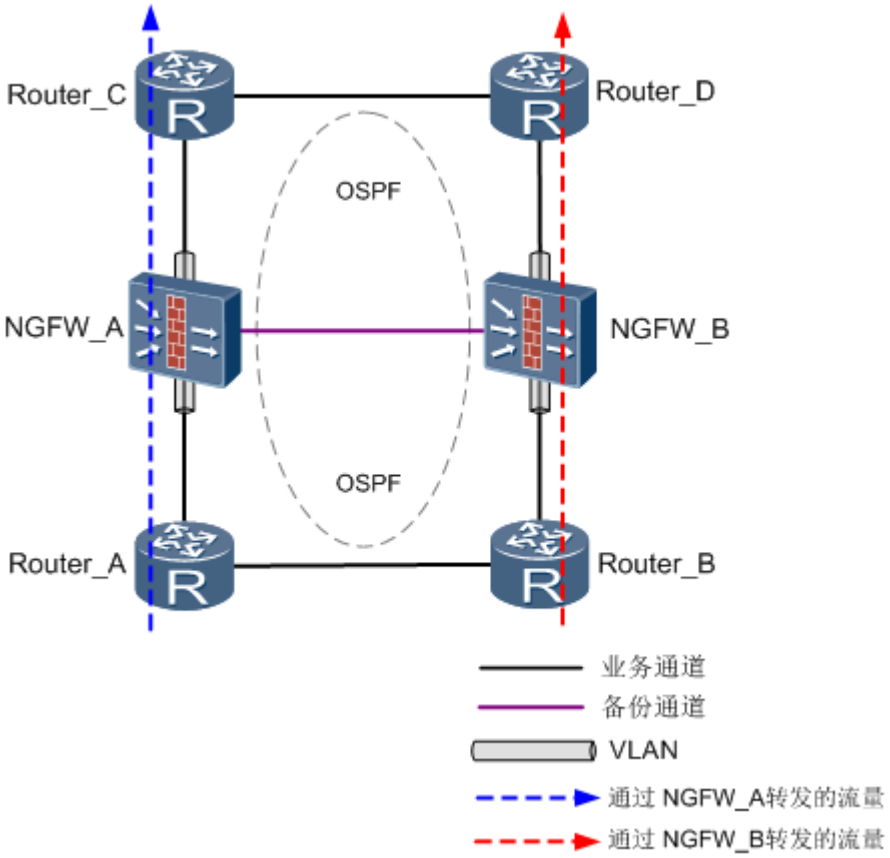
典型组网四：业务接口工作在二层，上下行连接路由器

介绍了设备的业务接口工作在二层，上下行连接路由器的组网。

如图 1 所示，NGFW 上、下行业务接口工作在二层，与路由器直连。上、下行路由器之间运行 OSPF 动态路由协议。每台 NGFW 的上下行业务接口加入到同一个 VLAN。

此组网只支持负载分担方式的双机热备。

图 1 NGFW 业务接口工作在二层，上下行连接路由器组网图



负载分担

NGFW_A 与 NGFW_B 上的 VLAN 都被启用，都能够转发流量。这时需要依靠上下行路由器运行的 OSPF 来实现流量的引导。

因此需要在 Router_A(C)连接 NGFW_A 和 Router_B(D)连接 NGFW_B 的接口上配置相同的 Cost 值，保证流量通过 NGFW_A 与 NGFW_B 共同转发。

注意：

此种组网不支持主备备份方式。因为如果工作于主备备份方式，备用设备上的 VLAN 被禁用，它的上下行路由器就无法进行通信，无法建立路由。这样主备切换时，备用设备就无法及时接替主用设备处理业务，导致业务中断。

NGFW_A 发生故障时，NGFW_A 切换成备用设备，NGFW_B 成为主用设备。

NGFW_A 切换成备用设备时，VLAN 内所有接口都会 Down 然后 Up 一次。这会导致上下行路由器重新计算路由。由于此时 NGFW_A 的 VLAN 已被禁用，链路 COST 值增大，因此流量全部从 NGFW_B 转发。

双机热备 FAQ-故障类

为什么原主用防火墙抢占后业务中断？

如果主备切换后业务正常，原主用防火墙抢占后业务中断，通常是因为路由尚未收敛，或者会话表备份不完整。另外，某些交换机整机故障后，在重新启动的过程中，接口可能反复 Up/Down。如果在此过程中抢占，也会导致业务中断。

请调整原主用防火墙的抢占延时。

为什么双机热备反复切换状态？

请先检查业务接口状态，如果业务接口反复 Down/Up，必然触发双机热备反复切换状态。如果业务接口正常，通常是因为两台防火墙的心跳报文发送间隔不一致，请修改。

为什么原主用防火墙的故障恢复后不抢占？

可能原因如下：

- 关闭了抢占功能。
- 尚未满足抢占延时。原主用防火墙故障恢复后，并不会立即抢占。设置抢占延时是为了避免主用防火墙状态不稳定引起的反复切换。

为什么主备防火墙的配置文件上，相同配置项的顺序不同？

通常是因为两台防火墙的初始配置不一致。需要把顺序不同的配置（如安全区域、虚拟系统）全部删除，重新配置。

强烈建议使用缺省配置开始配置双机热备。

为什么主用防火墙和备用防火墙的会话表不一致？

请先检查备份通道状态。如果备份通道故障，主用防火墙的会话不能备份到备用防火墙。

如果关闭了会话自动备份功能，两台防火墙的会话表必然不一致。在开启会话自动备份的情况下，会话也不是实时备份的。只有当会话老化线程扫描到会话、且此会话需要备份，才会备份到备用防火墙上。因此，会话建立一段时间（10 秒左右）之后才会备份到备用防火墙上。

另外，在开启会话自动备份的情况下，如下类型的会话不备份。

- 到防火墙自身的会话
- 未完成 3 次握手的 TCP 半连接会话
- 只有首包为 UDP 报文、后续包未命中的 UDP 报文（BT 协议）

会话自动备份和会话快速备份有什么区别，为什么来回路径不一致必须启用会话快速备份？

会话快速备份和传统的会话实时备份的区别是：

- 会话快速备份是在会话建立的时候立即备份到备用防火墙上；会话实时备份只有当会话老化线程扫描到会话、且此会话需要备份，才会备份到备用防火墙上。
- 会话快速备份能备份 TCP 半连接会话和到防火墙自身的会话。

来回路径不一致时，必须保证两台防火墙的会话表完全相同，必须启用会话快速备份。

来回路径不一致组网，为什么启用了会话快速备份 TCP 业务仍然有时候不通？

来回路径不一致组网下，防火墙启动了会话快速备份，如果业务流量很大，需要备份的状态信息比较多。可能会由于备份不及时使部分业务有延时甚至不通。例如，TCP 业务的 SYN 报文由一台防火墙转发，而 ACK 报文由另一台防火墙转发，若会话表还未备份过来，将导致 ACK 报文因状态错误被丢弃。

如果对业务的影响较大，可以关闭防火墙的链路状态检测。

防火墙主备切换后，为什么当前的主用防火墙上有带 remote 标志的会话？

带 remote 标志的会话是由原主用防火墙备份过来的。防火墙主备切换后，原先备份过来的会话表项还是会带有 remote 标志，直到该会话老化。

为什么备用防火墙上不能配置命令？

两台防火墙建立主备状态后，可以自动备份的命令不能在备用防火墙上手动配置，在主用防火墙上配置命令后会自动同步到备用防火墙。

如果需要在备用防火墙上手动配置这类命令，需要先取消配置的自动备份功能（undo hrp auto-sync config）。

为什么在主用防火墙上配置的命令没有备份到备用防火墙？

如果关闭了配置自动备份功能，则配置命令不会备份。另外，不是所有的命令都备份，如接口和路由相关的配置不会备份。

具体哪些命令可以备份，请参考支持备份的命令和状态信息。

为什么日志服务器会收到主用防火墙和备用防火墙的 NAT 会话日志？

主用防火墙的日志配置自动同步到备用防火墙。备用防火墙上有此配置就会向日志服务器发送日志。

您可以参考如下步骤，删除备用防火墙上的日志配置，来规避此问题。

1. 关闭配置命令的自动备份功能（**undo hrp auto-sync config**）。
2. 删除日志服务器配置。
3. 打开配置命令的自动备份功能，保证后续新执行的配置命令可以自动备份到备用防火墙（**hrp auto-sync config**）。

为什么 Ping 不通 VRRP 虚拟 IP 地址？

可能原因如下：

- VRID 冲突。
- 关闭了虚拟 IP 地址的 Ping 开关。根据 RFC3768，不能使用 Ping 命令检测虚拟 IP 地址的连通性。华为提供了虚拟 IP 地址的 Ping 开关，以方便监控。此开关默认开启，如被禁用，请执行 **vrrp virtual-ip ping enable** 命令开启。

为什么原配置主设备故障恢复后，仍然是配置从设备？

防火墙要想成为配置主设备，必须具备如下条件：

- 只有 VGMP 管理组状态为 Active 的防火墙才有机会成为配置主设备。（主备备份方式下，主用防火墙即配置主设备）
- 在负载分担方式下，按照 VGMP 管理组优先级、心跳口的 IP 地址从大到小的顺序选择配置主设备。

除非配置主设备出现故障或者退出 VRRP 备份组，否则配置主设备与配置从设备不转换角色，以保证配置主设备的稳定。

因此，在负载分担方式下，配置主设备故障后，原配置从设备变成配置主设备。原配置主设备故障恢复后，VGMP 管理组抢占，但是配置主设备不会抢占。

双机热备 FAQ-配置类

上下行接口配置了 VRRP 虚拟 IP 地址，还需要配置实 IP 地址吗？

在配置 VRRP 虚拟 IP 地址前，必须先配置接口的 IP 地址。VRRP 虚拟 IP 地址和接口 IP 地址可以在同一个网段，也可以不在同一个网段。

为什么主用防火墙需要配置较长的抢占延时，而备用防火墙可以配置很短的抢占延时？

抢占操作总是在主用防火墙故障恢复后启动。如果主用防火墙的抢占延时太短，则主用防火墙很快完成状态切换，但备用防火墙上的会话表项可能还没有完全备份过来，导致主用防火墙上会话表项不全，部分业务中断。因此主用防火墙要配置较长的抢占延时。

备用防火墙故障恢复后不会启动抢占操作，抢占延时没有意义，可以使用缺省值。

主用防火墙配置了较长的抢占延时后，会不会影响故障响应速度？

不会。主用防火墙出现故障时，业务很快切换到备用防火墙。主用防火墙的抢占延时只在其故障恢复时起作用，即故障恢复后，再经过抢占延时时间，才会启动抢占操作。这时备用防火墙是正常工作的，不会影响故障响应速度。

调整 VGMP Hello 报文的发送间隔，对组网有何影响？

VGMP Hello 报文即心跳报文，用于检测主备防火墙的连接状态。状态为 Standby 的 VGMP 管理组连续 3 个报文发送周期没有收到对端发送的 VGMP Hello 报文，认为对端出现故障，将自己切换到 Active 状态。因此，设置较短的 VGMP Hello 报文发送间隔可以提高对防火墙整机故障的响应速度。

但是，如果 VGMP Hello 报文发送间隔太小，可能会影响双机热备状态的稳定。当防火墙的 CPU 负荷较大时，发送 VGMP Hello 报文的任务得不到调度，会导致防火墙误切换。因此一般推荐使用缺省值（1 秒）。

双机热备组网时，配置 IPSec VPN 需要注意什么？

- 只支持主备备份方式的 IPSec VPN。
- 防火墙的上下行业务接口必须为三层接口（包括 VLANIF 接口）。
- 先建立双机热备状态，再配置 IPSec VPN。在主用防火墙上配置的 IPSec 策略会自动备份到备用防火墙上。在备用防火墙上，只需要在出接口上应用备份过来的 IPSec 策略即可。
- 如果防火墙作为 IPSec 隧道的发起方，必须执行命令 **local-address ip-address**，设置本端发起协商的地址为 VRRP 备份组的虚拟 IP 地址。
- 配置 DPD，在状态倒换后自动删除主用防火墙上已建立的隧道，以免业务被丢弃。

心跳接口是否一定需要直连？

不一定。心跳接口可以直连，也可以通过中间设备，如交换机或路由器连接。推荐直连。

当心跳接口通过中间设备连接时，配置心跳接口时需要配置 **remote** 参数指定对端心跳接口的 IP 地址。这主要是因为：

不配置 **remote** 参数，NGFW 发送的心跳报文使用 VRRP 协议封装，VRRP 报文是组播报文，部分交换机和路由器对于该类型的组播报文会上送自身处理，占用其自身的 CPU 资源。NGFW 上心跳报文随着业务的增加而增多，导致交换机和路由器 CPU 的负载过高，对交换机和路由器处理其它组播报文（如 OSPF）产生冲击。交换机和路由器对 VRRP 报文的限制，也会引起 NGFW 心跳报文的丢弃，导致 NGFW 状态的不稳定。

配置 **remote** 参数后，NGFW 将心跳报文封装成 UDP 报文，交换机和路由器对 UDP 报文不会上送自身处理，不会影响交换机和路由器的性能以及网络业务。

是否需要配置心跳接口所在域与 Local 域之间的安全策略？

- 配置心跳接口时如果不配置 **remote** 参数，心跳报文被封装成 VRRP 报文，此时不配置安全策略设备也能正常处理。
- 配置心跳接口时如果配置 **remote** 参数，心跳报文被封装成 UDP 报文，此时需要正确配置心跳接口所在安全区域和 Local 之间的域间安全策略，设备才能正常接收和发送心跳报文。

双机热备 FAQ-原理类

负载分担方式下，防火墙的主备关系如何确定？

在负载分担方式下，最先建立主备状态的防火墙成为配置主设备。

双机热备组网中，配置主设备和配置从设备是什么意思？

负载分担工作方式下，两台防火墙都有状态为 Active 的 VGMP 管理组，如何在这两台防火墙之间备份信息、需要备份哪些命令以及备份方向都是需要考虑的问题。

为了避免备份时混乱，防火墙引入了配置主设备和配置从设备的概念。发送配置备份内容的防火墙称为配置主设备（命令行提示符前有 HRP_A 前缀），接收配置备份内容的防火墙称为配置从设备（命令行提示符前有 HRP_S 前缀）。

可以自动备份的配置命令，只能在配置主设备上执行。

防火墙双机热备组网时，上下行二层设备通过什么报文学习到虚拟 MAC 地址表项？

主用防火墙定期发送 VRRP 通告报文，其源 MAC 以虚拟 MAC 地址填充（只有主用防火墙才会发送 VRRP 通告报文）。上下行二层设备通过 VRRP 通告报文学习到虚拟 MAC 地址对应的出接口。

防火墙双机热备组网时，上下行三层设备通过什么报文学习到虚拟 IP 地址的 ARP 表项？

上下行三层设备转发报文时，查询路由表获取下一跳，找到 VRRP 备份组的虚拟 IP 地址，然后据此查询 ARP 表。如果找不到虚拟 IP 地址的 ARP 表项则发送 ARP 请求。主用防火墙收到 ARP 请求后应答（只有主用防火墙才会应答）。

此 ARP 应答报文的二层报文头的源 MAC 地址以接口的实 MAC 地址填充，ARP 应答数据的源 MAC 地址以虚拟 MAC 地址填充。上下行三层设备通过 ARP 应答数据中的源 MAC 地址学习到虚拟 IP 地址对应的虚拟 MAC 地址。

上下行三层设备用虚拟 MAC 地址填充收到的报文的二层报文头的目的 MAC 地址字段，然后转发给防火墙。

hrp auto-sync 和 hrp sync 有什么区别？

hrp auto-sync 是自动备份，默认启用，表示后续配置和状态表项将备份到备用防火墙上。该命令对当前已存在的配置和状态表项没有影响。

hrp sync 则把主用防火墙当前的配置和状态表项立即备份到备用防火墙上。该命令立即生效，对后续配置和状态表项没有影响。

各种接口的优先级如何计算？

防火墙默认有两个 VGMP 管理组，分别为 Active 和 Standby。缺省情况下，Active VGMP 管理组的优先级为 65001，Standby VGMP 管理组的优先级为 65000。

VGMP 管理组优先级的计算方法如下：

- 对于普通接口，每一个接口故障，VGMP 管理组的优先级减 2。
- 对于 Eth-Trunk 接口，逻辑接口故障，VGMP 管理组的优先级减 2，成员接口故障不影响 VGMP 管理组的优先级。
- 对于 VLAN，每一个成员接口故障，VGMP 管理组的优先级减 2。
- 对于 IP-Link 监视的接口，如果 IP-Link 检测失败，VGMP 管理组的优先级减 2。

为什么双机热备组网不支持 Easy IP？

在 Easy IP 的配置中，无法指定 VRID。正常情况下，主用防火墙使用自身的出接口的 IP 地址作为公网地址，建立会话。在主备切换后，备用防火墙也采用自身的出接口的 IP 地址作为公网地址。这时，主用防火墙备份过来的会话，与备用防火墙的出接口 IP 地址不能匹配，导致业务中断。

双机热备 FAQ-规格类

主备切换的时间多长？

主备切换的时间与其触发条件有关。

- 如果由接口或链路故障触发主备切换，切换时间为毫秒级。
- 如果由整机故障触发切换，切换时间为 3 个心跳报文的发送间隔。

VRRP 虚拟 IP 地址能否做为 NAT 地址池的地址？

可以。如果只有一个公网地址，可以使用 VRRP 虚拟 IP 地址作为 NAT 地址池地址。

哪些类型的接口可以用做业务接口，哪些类型的接口可以用做心跳口？

常见接口对业务接口和心跳口的支持情况如表 1。

表 1 常见接口

接口类型	业务接口	心跳口
10GE 接口	支持，推荐	支持，推荐
GE 接口	支持，推荐	支持，推荐
Eth-Trunk 接口	支持，推荐	支持，推荐
子接口	支持	支持，不推荐
VLANIF 接口	支持	支持，不推荐

如果以子接口作为业务接口，必须将子接口加入 VRRP 备份组或者 VGMP 管理组，不能用物理接口。

防火墙是否支持使用虚拟 MAC 地址作为源 MAC 地址封装报文？

支持。缺省情况下，防火墙转发三层业务时，使用接口的实际 MAC 地址封装报文。如果需要使用虚拟 MAC 地址封装报文，请在接口视图下执行 **vrrp virtual-mac enable** 命令。

在双机热备组网中，防火墙的上下行设备能否选用四层交换机？

防火墙的上下行设备可以使用四层交换机。在这种组网中，必须使用虚拟 MAC 地址来封装业务报文，否则主备切换后将导致业务中断。

缺省情况下，防火墙使用接口的实际 MAC 地址封装业务报文并转发。在防火墙与四层交换机的组网中，四层交换机建立连接状态表，记录从防火墙转发过来的报文的源 MAC 地址（即主用防火墙业务接口的 MAC 地址）。四层交换机根据连接状态表转发报文。主备切换时，四层交换机不会自动更新连接状态表中的 MAC 地址，因此还会将报文转发至原来的主用防火墙，导致业务中断。

使用虚拟 MAC 地址封装业务报文后，防火墙使用虚拟 MAC 地址封装业务报文并转发，四层交换机的连接状态表中记录的是虚拟 MAC 地址。主备切换后，四层交换机可以转发业务报文到新的主用防火墙上。

虚拟 MAC 地址与虚拟 IP 地址相对应，是防火墙根据 VRID 自动生成的 MAC 地址，其格式为：

- IPv4：00-00-5E-00-01-{VRID}
- IPv6：00-00-5E-00-02-{VRID}

在防火墙业务接口上，启用虚拟 MAC 地址封装业务报文的命令如下：

```
<sysname> system-view
[sysname] interface GigabitEthernet 1/0/1
[sysname-GigabitEthernet1/0/1] vrrp virtual-mac enable
```

双机热备 FAQ-其他类

如何执行主备切换测试？

VGMP 管理组的优先级不能手工修改，为达到相同的效果，有两种方案。

- 手工 shutdown 主用防火墙的 VRRP 备份组接口，降低 VGMP 管理组优先级，触发状态切换。如果状态切换失败，此方案将影响业务。
- 手工 shutdown 主用防火墙上一个未用的接口，并将其加入 Active VGMP 管理组（在此接口下执行 **hrp track active** 命令），降低 VGMP 管理组优先级，触发状态切换。

备用防火墙上的特征库如何升级？

特征库在线升级的配置命令可以自动备份到备用防火墙上。主用防火墙和备用防火墙都可以按照预定的时间，自动从安全服务中心下载最新版本的特征库。另外，在主用防火墙上执行的手动在线升级，会在备用防火墙上同步执行。

双机热备是否需要 License 支持？

双机热备特性本身无须 Lincese 支持。

如果防火墙上其他的业务需要 License 支持，必须保证主用防火墙和备用防火墙都申请和激活了相同规格的 License。如果备用防火墙上没有激活 License，或者 License 规格少于主用防火墙，可能导致业务中断。

配置双机热备-Web

介绍双机热备的 Web 配置方法。

前提条件

1. 根据网络情况和实际需求，确定组网。具体请参见典型组网分析。
2. 根据需求，确定使用主备备份还是负载分担。

3. 完成网络的基本配置，包括接口、路由和安全策略。

背景信息

根据组网不同，双机热备的配置不同。

组网	操作
组网一：业务接口工作在三层，上下行连接交换机	需要配置虚拟 IP 地址，将上下行业务接口加入 VRRP 备份组。
组网二：业务接口工作在三层，上下行连接路由器	需要配置接口监控，监控上下行业务接口。
组网三：业务接口工作在二层，上下行连接交换机	不需要配置虚拟 IP 地址和配置接口监控。 由于 VGMP 管理组默认监控除 VLAN1 外的所有 VLAN，因此只需要将上下行业务接口加入到 VLAN 中即可。
组网四：业务接口工作在二层，上下行连接路由器	不需要配置虚拟 IP 地址和配置接口监控。 由于 VGMP 管理组默认监控除 VLAN1 外的所有 VLAN，因此只需要将上下行业务接口加入到 VLAN 中即可。

管理员需要在双机热备组网的两台 NGFW 上完成下面的操作步骤。

操作步骤

1. 选择“系统 > 高可靠性 > 双机热备”。
2. 单击“配置”。
3. 选中“启用”前的复选框后，配置双机热备基本参数。具体参数解释如下：

参数	说明
运行模式	选择双机的运行模式。 • 主备备份：两台设备处于主备备份运行模式，一台为主用设备，一台为备用设备。 • 负载分担：两台设备处于负载分担运行模式，两台设备互为主备。 **注意：** 业务接口工作在二层且连接交换机时，必须选择“主备备份”。
运行角色	在主备备份运行模式下，选择本设备是做主用设备还是备用设备。当“运行模式”选择“主备备份”时，界面显示此配置项。
心跳接口	选择心跳接口，心跳接口必须已经配置了 IP 地址。心跳接口用于两台设备之间备份配置和状态信息。 当两台设备的心跳接口通过交换机或路由器相连时，必须配置“对端接口 IP”。“对端接口 IP”即为对端设备的心跳接口 IP 地址。 **说明：**

参数	说明
	不配置“对端接口 IP”时，心跳报文为组播报文；配置了“对端接口 IP”后，心跳报文为单播报文。 因此当配置了“对端接口 IP”后，需要配置 local 区域与心跳接口所在区域间的安全策略，保证两台设备能够交互报文。 最多可以配置 16 个心跳接口，但只有最先配置的处于 UP 状态的心跳接口处于使用状态。单击，可以添加心跳接口。
主动抢占	选择是否启用主动抢占功能。设备默认启用此功能，抢占延时为 60 秒。此功能仅在主用设备上生效。 主动抢占是指主用设备故障恢复后，重新切换成主用设备处理业务的过程。如果取消了主动抢占功能的配置，则主用设备故障恢复后，仍是备用设备，不处理业务。 当设备的业务接口工作在二层，上下行连接路由器时，必须启用此功能。
Hello 报文周期	Hello 报文周期默认为 1000 毫秒，建议使用默认值。若要修改此参数，必须保证两台设备配置的取值一致。 • 主备备份运行模式下，Hello 报文周期是指主用设备向备用设备发送 Hello 报文的时间间隔。 • 负载分担运行模式下，Hello 报文周期是指两台设备相互发送 Hello 报文的时间间隔。

4. 配置虚拟 IP 地址（VRRP 备份组）。

说明：

当业务接口工作在三层且连接交换机时，需要配置虚拟 IP 地址。

a. 在“配置虚拟 IP 地址”下单击“新建”。

b. 配置虚拟 IP 地址的参数。具体的配置原则和参数解释如下：

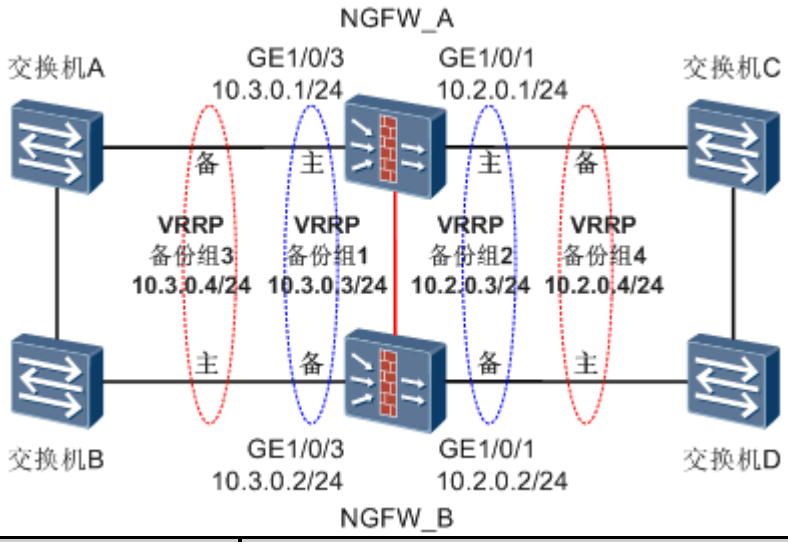
- 如果“运行模式”为“主备备份”，需要在主用设备上将业务接口加入 VRRP 备份组，在备用设备上将相同的业务接口加入相同的 VRRP 备份组。

  如图 1 所示，NGFW_A 的 GE1/0/1 接口加入 VRRP 备份组 2，NGFW_B 的 GE1/0/1 接口也加入 VRRP 备份组 2。

- 如果“运行模式”为“负载分担”，需要在 NGFW_A 上将一个业务接口加入两个 VRRP 备份组（其中一个“角色”为“主”，另一个“角色”为“备”）。在 NGFW_B 上将相同的业务接口加入与 NGFW_A 相同的两个 VRRP 备份组（“角色”需要与 NGFW_A 相反）。

如图 1 所示，NGFW_A 的 GE1/0/1 接口加入 VRRP 备份组 2（角色为主）和 VRRP 备份组 4（角色为备），NGFW_B 的 GE1/0/1 接口也加入 VRRP 备份组 2（角色为备）和 VRRP 备份组 4（角色为主）。

c. **图 1** 配置虚拟 IP 地址



参数	说明
VRID	VRRP 备份组的 ID。两台 NGFW 相同的接口应该配置 VRID 相同的 VRRP 备份组。 例如图 1 中 NGFW_A 与 NGFW_B 的 GE1/0/1 接口上都配置 VRRP 备份组 2，VRID 都为 2。
接口	配置 VRRP 备份组的接口，此接口应该是设备的上下行业务接口。 例如图 1 中两台 NGFW 的 GE1/0/1 和 GE1/0/3 接口。
接口 IP 地址/掩码	选择“接口”后，此处自动显示接口的 IP 地址和掩码。 例如在 NGFW_A 上选择 GE1/0/1，这里显示 10.2.0.1/24。
虚拟 IP 地址/掩码	输入 VRRP 备份组的虚拟 IP，例如图 1 中的 10.2.0.3/24、10.3.0.3/24、10.2.0.4/24、10.3.0.4/24。 虚拟 IP 不能与接口 IP 相同。对于 IPv4 的 VRRP 备份组，如果虚拟 IP 与接口 IP 不在同一网段，则必须输入掩码。 虚拟 IP 是两台 NGFW 共同对外提供的 IP 地址。在上下行设备看来，两台 NGFW 是一台设备，接口 IP 为虚拟 IP。因此当上下行设备配置静态路由时，需要将下一跳设置为虚拟 IP。
Link-Local 地址	对于 IPv6 的 VRRP 备份组，除了配置虚拟 IP 地址，还需要配置 Link-Local 地址。Link-Local 地址是 IPv6 的 VRRP 备份组的链路本地地址。链路本地地址是前缀为 FE80 的 IPv6 的地址（如 FE80::7），用于同一链路的相邻节点间通信，有效域仅限于本地链路。配置 VRRP 备份组的虚拟 IPv6 地址时，必须同时为 VRRP 备份组配置一个 Link-Local 地址。
角色	当“运行模式”选择“负载分担”时，界面显示此配置项。 这时如果一台设备的 VRRP 备份组的角色为主，那么另一台设备的相同 VRRP

参数	说明
	备份组（VRID 相同）的角色必须为备。反之亦然，如图 1 所示。

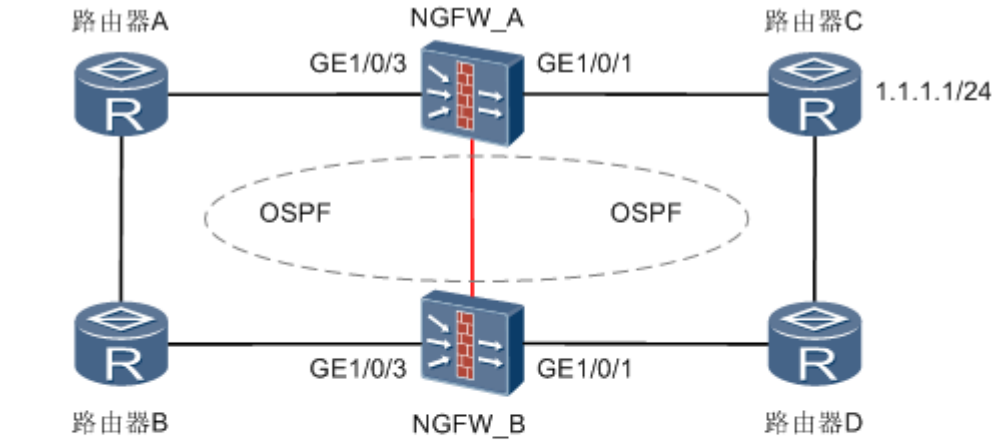
d. 单击“确定”。

5. 配置接口监控，如图 2 所示。

说明：

当业务接口工作在三层且连接路由器时，需要配置接口监控。选择的监控接口应该是设备的业务接口。

图 2 配置接口监控



具体参数解释如下：

参数	说明
监控接口	选择需要监控的上行和下行业务接口。例如图 2 中的 GE1/0/1 和 GE1/0/3。
监控远程探测地址/域名	输入需要监控的非直连接口的 IP 地址或域名。例如图 2 中的公网地址“1.1.1.1”。 在哪个接口后输入“监控远程探测地址/域名”就代表探测报文从哪个接口发出。

参数	说明
将所选监控接口加入到监控组	选中此复选框后，设备会将之前所选的“监控接口”加入到监控组中。 当监控组中的一个接口 down 时，所有接口状态都变成 down。例如图 2 中接口 GE1/0/1 故障，GE1/0/3 的状态也变成 down。

6. 单击“确定”。

后续处理

配置完成后，选择“系统 > 高可靠性 > 双机热备”，查看双机热备的运行情况。具体参数解释如下：

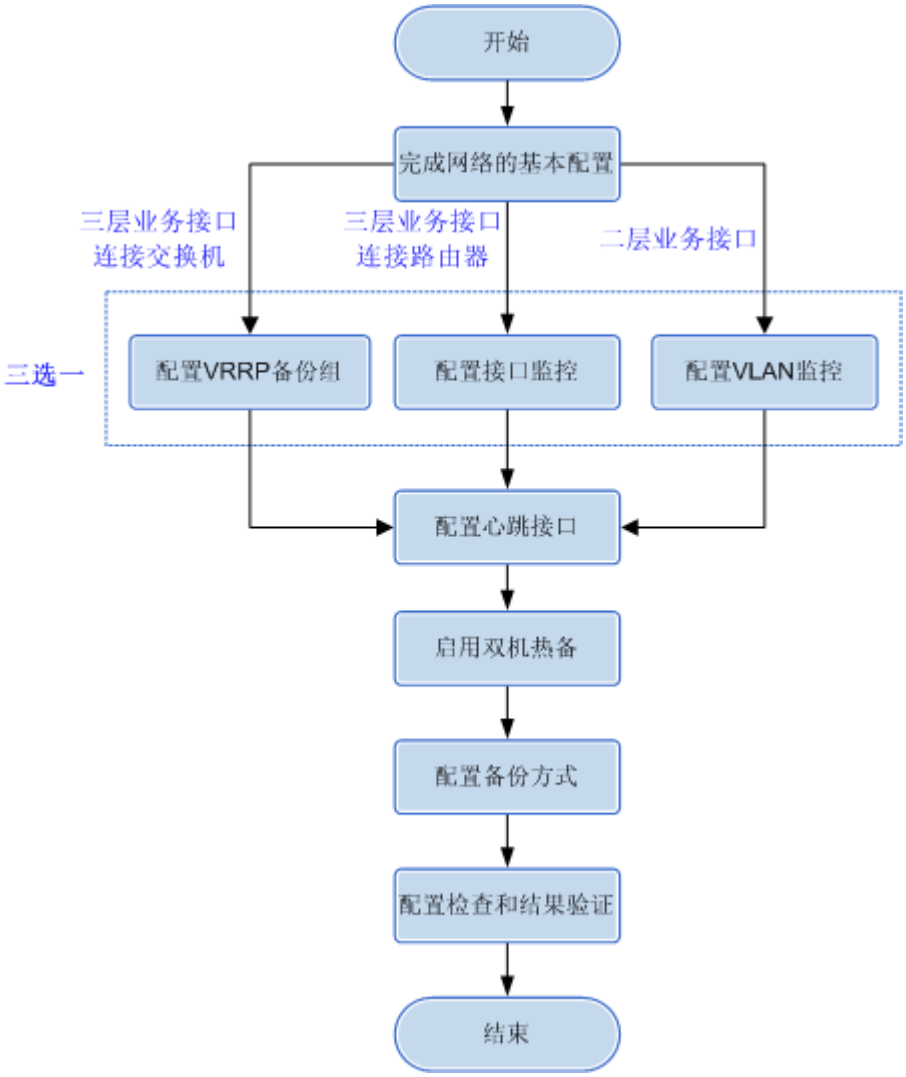
参数	说明
当前运行模式	• 单机：没有运行双机热备时，显示此参数。 • 主备备份：运行在主备备份工作模式时，显示此参数。 • 负载分担：运行在负载分担工作模式时，显示此参数。
当前运行角色	• 初始化：配置完成后，双机热备状态尚未建立时，设备显示此参数。 • 主用：双机热备状态正常建立后，主用设备显示此参数。 • 备用：双机热备状态正常建立后，备用设备显示此参数。 单击“详细”，查看设备主备状态切换的记录信息，包括：切换时间、切换内容和原因。 单击“手动切换”，可以手动选择设备的运行角色。
当前心跳接口	显示当前正在使用的心跳接口以及心跳接口的带宽使用率。
主动抢占	显示是否启用主动抢占功能。
配置一致性	显示两台设备的配置是否一致。 单击“配置一致性检查”，对两台设备的配置一致性进行检查。 单击“详细”，显示总体检查结果、检查日期以及各个模块的检查结果。 在“一致性检查”界面单击“同步配置”，可以同步两台设备的配置。 单击“重新检查”，重新检查两台设备配置的一致性。
虚拟 IP	显示监控的 VRRP 备份组的状态。
接口	显示监控的接口的状态。
远端监控 IP/域名	显示监控的远端监控 IP/域名的状态。

配置流程-CLI

介绍双机热备的配置流程，您可以参照本节的流程图阅读下面的章节。

双机热备的配置流程请参见图 1。

图 1 配置流程



配置 VRRP 备份组-CLI

当业务接口工作在三层且连接交换机时，需要配置 VRRP 备份组。

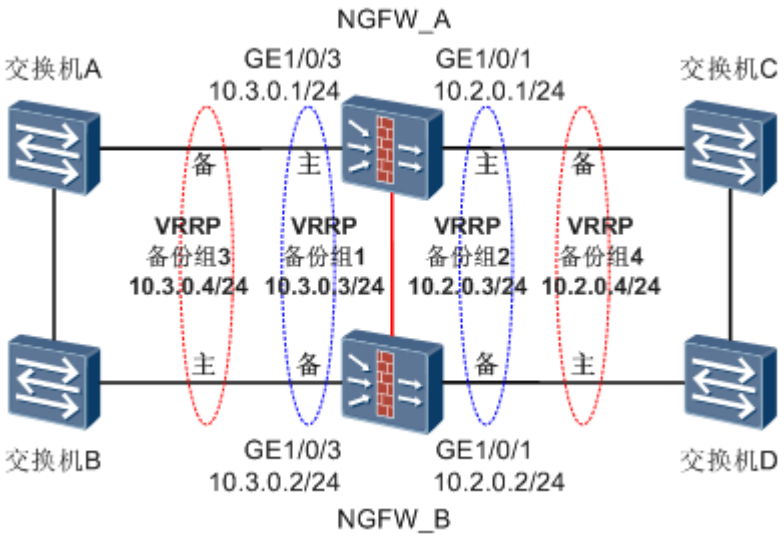
前提条件

1. 完成业务接口的配置，包括接口 IP 地址和加入安全区域的配置。
2. 配置安全策略，允许流量正常通过设备。

背景信息

配置 VRRP 备份组的思路如下所示：

图 1 配置 VRRP 备份组



- 主备备份

  1. 在主用设备的业务接口上配置 VRRP 备份组，将 VRRP 备份组加入状态为 Active 的 VGMP 管理组。

     如图 1 所示，在 NGFW_A 的 GE1/0/1 接口上配置 VRRP 备份组 2，加入状态为 Active 的 VGMP 管理组；在 GE1/0/3 接口上配置 VRRP 备份组 1，加入状态为 Active 的 VGMP 管理组。

  2. 在备用设备的业务接口上配置 VRRP 备份组，将 VRRP 备份组加入状态为 Standby 的 VGMP 管理组。

     如图 1 所示，在 NGFW_A 的 GE1/0/1 接口上配置 VRRP 备份组 2，加入状态为 Standby 的 VGMP 管理组；在 GE1/0/3 接口上配置 VRRP 备份组 1，加入状态为 Standby 的 VGMP 管理组。

  3. 在上下行网络的主机或设备上将静态路由下一跳或出口网关设置为 VRRP 备份组的虚拟 IP 地址。

- 负载分担

  1. NGFW_A 的上下行业务接口上分别配置两个 VRRP 备份组，其中一个加入状态为 Active 的 VGMP 管理组，另外一个加入状态为 Standby 的 VGMP 管理组。

     如图 1 所示，在 NGFW_A 的下行接口上配置 VRRP 备份组 1（加入状态为 Active 的 VGMP 管理组）和 VRRP 备份组 3（加入状态为 Standby 的 VGMP 管理组）；在上行接口上配置 VRRP 备份组 2（加入状态为 Active 的 VGMP 管理组）和 VRRP 备份组 4（加入状态为 Standby 的 VGMP 管理组）。

  2. 在 NGFW_B 的业务接口上配置与 NGFW_A 相同的 VRRP 备份组，但分别加入与 NGFW_A 状态相反的 VGMP 管理组。

如图 1 所示，在 NGFW_A 的下行接口上配置 VRRP 备份组 1（加入状态为 Standby 的 VGMP 管理组）和 VRRP 备份组 3（加入状态为 Active 的 VGMP 管理组）；在上行接口上配置 VRRP 备份组 2（加入状态为 Standby 的 VGMP 管理组）和 VRRP 备份组 4（加入状态为 Active 的 VGMP 管理组）。

3. 在上下行网络的主机或设备（如 PC）上配置两条静态路由，下一跳分别指向两个 VRRP 备份组的虚拟 IP 地址。

操作步骤

1. 在系统视图下进入接口视图。

   interface *interface-type interface-number*

   支持配置 VRRP 备份组的接口类型包括：三层以太网接口及其子接口，三层 Eth-Trunk 接口和 Vlanif 接口。

2. 根据实际组网情况，执行如下命令配置 IPv4 或 IPv6 的 VRRP 备份组。

   - 配置 IPv4 的 VRRP 备份组。

     vrrp vrid *virtual-router-id* **virtual-ip** *virtual-address* [*ip-mask* | *ip-mask-length*] { **active** | **standby** }

   - 配置 IPv6 的 VRRP 备份组。

     a. 配置 Link-Local 地址。

        vrrp6 vrid *virtual-router-id* **virtual-ip** *FE80::X:X* **link-local** { **active** | **standby** }

     b. 配置虚拟 IPv6 地址。

        vrrp6 vrid *virtual-router-id* **virtual-ip** *virtual-ipv6-address*

3. 以上命令中参数的配置注意事项如下：

   - *virtual-router-ID* 是 VRRP 备份组的 ID。双机热备的两台 NGFW 相同的接口应该配置 VRID 相同的 VRRP 备份组。

- *FE80::X:X* link-local 用来指定 IPv6 的 VRRP 备份组的链路本地地址。链路本地地址是前缀为 FE80 的 IPv6 的地址，用于同一链路的相邻节点间通信，有效域仅限于本地链路。配置 VRRP 备份组的虚拟 IPv6 地址时，必须先为 VRRP 备份组配置一个链路本地地址。
- *virtual-address* 和 *virtual-ipv6-address* 是 VRRP 备份组的虚拟 IP 地址，虚拟 IP 地址不能与接口的实际 IP 地址相同。

  虚拟 IP 是两台 NGFW 共同对外提供的 IP 地址。在上下行设备看来，两台 NGFW 是一台设备，接口 IP 为虚拟 IP。因此当上下行设备配置静态路由时，需要将下一跳设置为虚拟 IP。

- *ip-mask* | *ip-mask-length* 是 IPv4 的 VRRP 备份组虚拟 IP 地址的掩码。当虚拟 IP 地址与接口的 IP 地址不在同一网段时，需要配置掩码。

4. **可选**：在接口视图下配置 VRRP 报文认证。

   vrrp vrid *virtual-router-ID* authentication-mode { simple | md5 } *key*

   缺省情况下，不进行 VRRP 报文认证。在一个安全的网络中，可以采用缺省设置，NGFW 对发送和收到的 VRRP 报文不会进行认证。

   在有可能受到安全威胁的网络中，建议配置 VRRP 认证。NGFW 只支持简单字符认证方式（参数为 simple）和 md5 认证。

   说明：

   主备设备加入同一 VRRP 备份组的接口需要配置相同的 VRRP 认证字。

   IPv6 的 VRRP 备份组不支持配置 VRRP 报文认证。

5. **可选**：在接口视图下启用虚拟 MAC 地址功能。

   vrrp virtual-mac enable

   当 NGFW 的上下行设备存在四层交换机时，需要在接口上启用虚拟 MAC 地址功能。

6. **可选**：在系统视图下配置主用设备发送免费 ARP 报文的时间间隔。

   vrrp gratuitous-arp timeout *time*

   缺省情况下，主用设备每隔 300 秒（5 分钟）发送一次免费 ARP 报文。

time 的取值需要小于上下行交换机的 MAC 转发表老化时间。*time* 的取值越小，发生主备设备切换时，上下行交换机的 MAC 转发表更新就越快。

任务示例

如图 1 所示，主备备份时，VRRP 备份组的配置如下：

```
[NGFW_A] interface GigabitEthernet 1/0/1
[NGFW_A-GigabitEthernet1/0/1] ip address 10.2.0.1 24
[NGFW_A-GigabitEthernet1/0/1] vrrp vrid 2 virtual-ip 10.2.0.3 active
[NGFW_A-GigabitEthernet1/0/1] quit
[NGFW_A] interface GigabitEthernet 1/0/3
[NGFW_A-GigabitEthernet1/0/3] ip address 10.3.0.1 24
[NGFW_A-GigabitEthernet1/0/3] vrrp vrid 1 virtual-ip 10.3.0.3 active
[NGFW_A-GigabitEthernet1/0/3] quit
[NGFW_B] interface GigabitEthernet 1/0/1
[NGFW_B-GigabitEthernet1/0/1] ip address 10.2.0.2 24
[NGFW_B-GigabitEthernet1/0/1] vrrp vrid 2 virtual-ip 10.2.0.3 standby
[NGFW_B-GigabitEthernet1/0/1] quit
[NGFW_B] interface GigabitEthernet 1/0/3
[NGFW_B-GigabitEthernet1/0/3] ip address 10.3.0.2 24
[NGFW_B-GigabitEthernet1/0/3] vrrp vrid 1 virtual-ip 10.3.0.3 standby
[NGFW_B-GigabitEthernet1/0/3] quit
```

如图 1 所示，负载分担时，VRRP 备份组的配置如下：

```
[NGFW_A] interface GigabitEthernet 1/0/1
[NGFW_A-GigabitEthernet1/0/1] ip address 10.2.0.1 24
[NGFW_A-GigabitEthernet1/0/1] vrrp vrid 2 virtual-ip 10.2.0.3 active
[NGFW_A-GigabitEthernet1/0/1] vrrp vrid 4 virtual-ip 10.2.0.4 standby
[NGFW_A-GigabitEthernet1/0/1] quit
[NGFW_A] interface GigabitEthernet 1/0/3
[NGFW_A-GigabitEthernet1/0/3] ip address 10.3.0.1 24
[NGFW_A-GigabitEthernet1/0/3] vrrp vrid 1 virtual-ip 10.3.0.3 active
[NGFW_A-GigabitEthernet1/0/3] vrrp vrid 3 virtual-ip 10.3.0.4 standby
[NGFW_A-GigabitEthernet1/0/3] quit
[NGFW_B] interface GigabitEthernet 1/0/1
[NGFW_B-GigabitEthernet1/0/1] ip address 10.2.0.2 24
[NGFW_B-GigabitEthernet1/0/1] vrrp vrid 2 virtual-ip 10.2.0.3 standby
[NGFW_B-GigabitEthernet1/0/1] vrrp vrid 4 virtual-ip 10.2.0.4 active
[NGFW_B-GigabitEthernet1/0/1] quit
[NGFW_B] interface GigabitEthernet 1/0/3
[NGFW_B-GigabitEthernet1/0/3] ip address 10.3.0.2 24
[NGFW_B-GigabitEthernet1/0/3] vrrp vrid 1 virtual-ip 10.3.0.3 standby
```

```
[NGFW_B-GigabitEthernet1/0/3] vrrp vrid 3 virtual-ip 10.3.0.4 active
[NGFW_B-GigabitEthernet1/0/3] quit
```

配置接口监控

当业务接口工作在三层且连接路由器时，需要配置接口监控。

前提条件

1. 完成业务接口的配置，包括接口 IP 地址和加入安全区域的配置。
2. 在 NGFW 和上下行路由器上配置 OSPF，保证网络连通。
3. 配置安全策略，允许流量正常通过设备。

操作步骤

1. 在系统视图下进入接口视图。

   interface *interface-type interface-number*

   支持的接口类型包括：三层以太网接口及其子接口和三层 Eth-Trunk 接口。

2. 在接口视图下配置由状态为 Active 或 Standby 的 VGMP 管理组监控接口。

   hrp track { active | standby }

   主备备份方式下，需要在主用设备的上下行业务接口上配置 **hrp track active**，备用设备的上下行业务接口上配置 **hrp track standby**。

   负载分担方式下，需要在两台设备的上下行业务接口上配置 **hrp track active** 和 **hrp track standby**。

3. 在系统视图下启用根据 VGMP 管理组状态调整 OSPF 的 COST 值功能。

   - IPv4 网络：

     hrp ospf-cost adjust-enable [*standby-cost*]

   - IPv6 网络：

hrp ospfv3-cost adjust-enable [*standby-cost*]

注意：

业务接口工作在三层且连接路由器的主备备份组网必须配置该命令，负载分担组网可以不配置此命令。

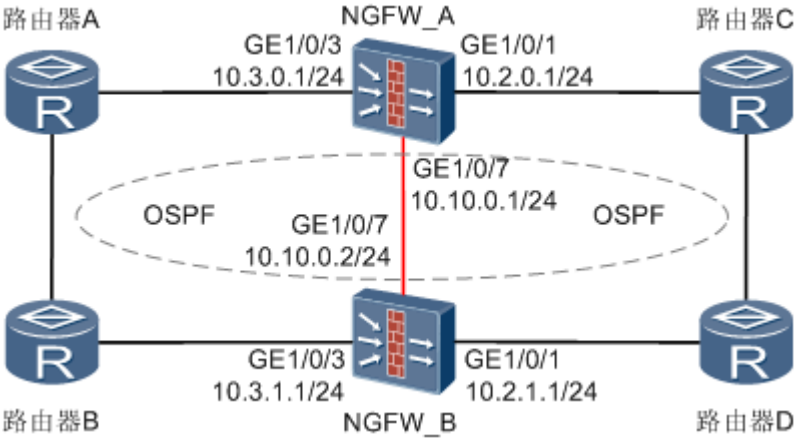
缺省情况下，此功能处于启用状态，Cost 值（*standby-cost*）为 65500。

standby-cost 的取值与上下游路由器设定的 OSPF Cost 值有关。要求 *standby-cost* 的取值大于备用设备上下游路由器的 Cost 值。

配置这个命令后，NGFW 发布 OSPF 路由时，会判断自身是主用设备还是备用设备。如果是主用设备，NGFW 把学习到的路由直接发布出去；如果是备用设备，NGFW 发布 Cost 值为 *standby-cost* 的路由。这样上下行路由器在计算路由的时候，就能将下一跳指向主用设备，并把报文转发到主用设备上。

任务示例

图 1 配置接口监控



如图 1 所示，主备备份时，接口监控的配置如下：

```
[NGFW_A] interface GigabitEthernet 1/0/1
[NGFW_A-GigabitEthernet1/0/1] ip address 10.2.0.1 24
[NGFW_A-GigabitEthernet1/0/1] hrp track active
[NGFW_A-GigabitEthernet1/0/1] quit
[NGFW_A] interface GigabitEthernet 1/0/3
[NGFW_A-GigabitEthernet1/0/3] ip address 10.3.0.1 24
[NGFW_A-GigabitEthernet1/0/3] hrp track active
[NGFW_A-GigabitEthernet1/0/3] quit
[NGFW_B] interface GigabitEthernet 1/0/1
[NGFW_B-GigabitEthernet1/0/1] ip address 10.2.1.1 24
[NGFW_B-GigabitEthernet1/0/1] hrp track standby
[NGFW_B-GigabitEthernet1/0/1] quit
```

```
[NGFW_B] interface GigabitEthernet 1/0/3
[NGFW_B-GigabitEthernet1/0/3] ip address 10.3.1.1 24
[NGFW_B-GigabitEthernet1/0/3] hrp track standby
[NGFW_B-GigabitEthernet1/0/3] quit
```

如图 1 所示，负载分担时，接口监控的配置如下：

```
[NGFW_A] interface GigabitEthernet 1/0/1
[NGFW_A-GigabitEthernet1/0/1] ip address 10.2.0.1 24
[NGFW_A-GigabitEthernet1/0/1] hrp track active
[NGFW_A-GigabitEthernet1/0/1] hrp track standby
[NGFW_A-GigabitEthernet1/0/1] quit
[NGFW_A] interface GigabitEthernet 1/0/3
[NGFW_A-GigabitEthernet1/0/3] ip address 10.3.0.1 24
[NGFW_A-GigabitEthernet1/0/3] hrp track active
[NGFW_A-GigabitEthernet1/0/3] hrp track standby
[NGFW_A-GigabitEthernet1/0/3] quit
[NGFW_B] interface GigabitEthernet 1/0/1
[NGFW_B-GigabitEthernet1/0/1] ip address 10.2.1.1 24
[NGFW_B-GigabitEthernet1/0/1] hrp track active
[NGFW_B-GigabitEthernet1/0/1] hrp track standby
[NGFW_B-GigabitEthernet1/0/1] quit
[NGFW_B] interface GigabitEthernet 1/0/3
[NGFW_B-GigabitEthernet1/0/3] ip address 10.3.1.1 24
[NGFW_B-GigabitEthernet1/0/3] hrp track active
[NGFW_B-GigabitEthernet1/0/3] hrp track standby
[NGFW_B-GigabitEthernet1/0/3] quit
```

配置 VLAN 监控

当业务接口工作在二层时，需要配置 VLAN 监控。缺省情况下，启用双机热备后，VGMP 管理组会监控除 VLAN1 外的所有 VLAN。

前提条件

1. 完成业务接口的配置，包括将三层接口转换成二层接口和加入安全区域的配置。
2. 将上下行业务接口加入到同一 VLAN（不能是 VLAN1）中。
3. 配置安全策略，允许流量正常通过设备。

背景信息

配置 VLAN 监控的注意事项如下：

- 当上下行业务接口工作在二层，连接交换机时，只支持主备备份方式。
- 当上下行业务接口工作在三层，连接路由器时，只支持负载分担方式。这时需要在防火墙的上下行路由器上配置相同 COST 值的 OSPF 路由。

操作步骤

1. 在系统视图下进入 VLAN 视图。

   vlan *vlan-id*

2. 在 VLAN 视图下配置由状态为 Active 或 Standby 的 VGMP 管理组监控 VLAN。

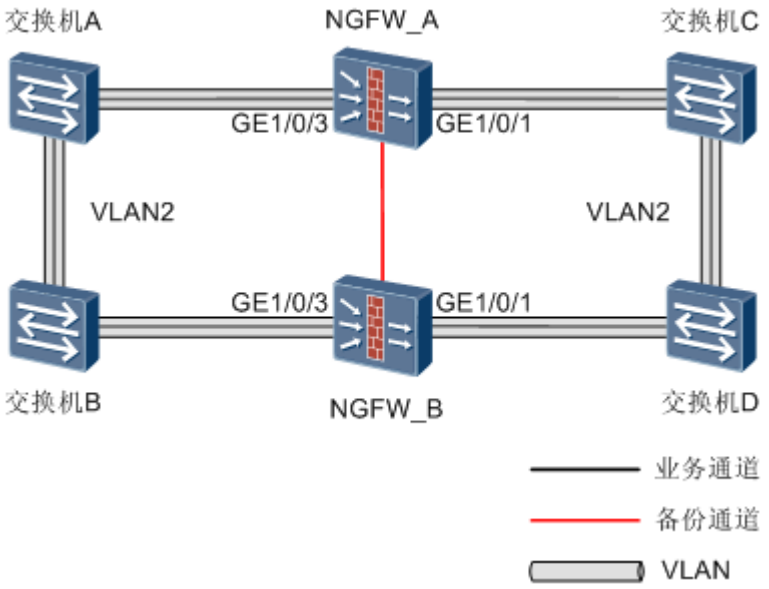
   hrp track { active | standby }

   主备备份方式下，需要在主用设备的业务接口所在 VLAN 配置 **hrp track active**，备用设备的业务接口所在 VLAN 配置 **hrp track standby**。

   负载分担方式下，需要在两台设备的业务接口所在 VLAN 配置 **hrp track active** 和 **hrp track standby**。

任务示例

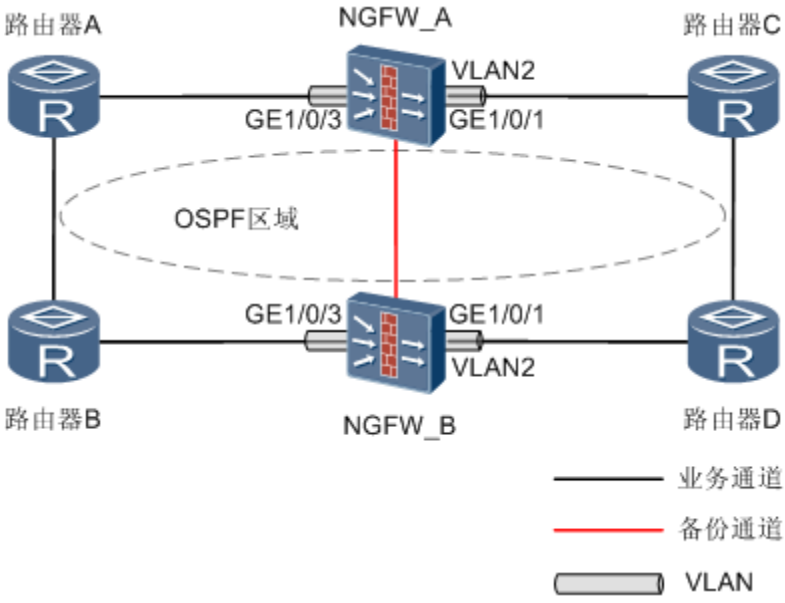
图 1 配置 VLAN 监控（连接交换机）



如图 1 所示，当业务接口工作在二层且连接交换机时（主备备份），VLAN 监控的配置如下：

```
[NGFW_A] VLAN 2
[NGFW_A-vlan-2] port GigabitEthernet 1/0/1
[NGFW_A-vlan-2] port GigabitEthernet 1/0/3
[NGFW_A-vlan-2] hrp track active
[NGFW_B] VLAN 2
[NGFW_B-vlan-2] port GigabitEthernet 1/0/1
[NGFW_B-vlan-2] port GigabitEthernet 1/0/3
[NGFW_B-vlan-2] hrp track standby
```

图 2 配置 VLAN 监控（连接路由器）



如图 2 所示，当业务接口工作在二层且连接路由器时（负载分担），VLAN 监控的配置如下：

```
[NGFW_A] VLAN 2
[NGFW_A-vlan-2] port GigabitEthernet 1/0/1
[NGFW_A-vlan-2] port GigabitEthernet 1/0/3
```

```
[NGFW_A-vlan-2] hrp track active
[NGFW_A-vlan-2] hrp track standby
[NGFW_B] VLAN 2
[NGFW_B-vlan-2] port GigabitEthernet 1/0/1
[NGFW_B-vlan-2] port GigabitEthernet 1/0/3
[NGFW_B-vlan-2] hrp track active
[NGFW_B-vlan-2] hrp track standby
```

配置心跳接口

双机热备组网中，管理员需要在两台设备上分别配置心跳接口，并通过心跳线将两台设备的心跳接口相连。

背景信息

双机热备的两台设备通过心跳接口交互报文了解对方状态，以及实现配置命令和状态信息的备份。

建议两台设备间的心跳接口直接相连。

NGFW 支持使用 Eth-Trunk 接口做为心跳接口，既提高了可靠性，又增加了备份通道的带宽。

操作步骤

1. 配置心跳接口的 IP 地址。

   a. 在系统视图下进入接口视图。

      interface *interface-type interface-number*

      支持做心跳接口的接口类型包括：三层以太网接口及其子接口，三层 Eth-Trunk 接口和 Vlanif 接口。

   b. 在接口视图下配置心跳接口的 IP 地址。

      ip address *ip-address net-mask*

      心跳接口不对外发布路由，不处理业务，可以配置为私网 IP 地址。

2. 将心跳接口加入安全区域。

   a. 在系统视图下进入安全区域视图。

firewall zone *zone-name*

双机热备中两台 NGFW 的心跳接口必须加入相同的安全区域。

b. 将心跳接口加入安全区域。

add interface *interface-type interface-number*

3. 在系统视图下指定心跳接口。

hrp interface *interface-type interface-number* [**remote** *ip-address*]

- 双机热备的两台 NGFW 的心跳接口的接口类型和编号必须相同。例如 NGFW_A 的心跳接口为 GigabitEthernet 1/0/7，那么 NGFW_B 的心跳接口也必须为 GigabitEthernet 1/0/7。
- 双机热备的两台 NGFW 的心跳接口可以直接相连，也可以通过交换机或路由器相连。推荐心跳接口直连。

当心跳接口通过交换机或路由器相连时，必须配置 **remote** *ip-address* 来指定对端心跳接口的 IP 地址。

如果使用二层接口作为心跳接口，需要将二层接口加入 VLAN，创建 Vlanif 并配置 Vlanif 的 IP 地址，然后使用 Vlanif 接口作为心跳口。当心跳接口是 Vlanif 接口时，无论心跳接口是否直连，都需要配置 **remote** 参数来指定对端心跳口的 IP 地址。

4. **可选：**配置 local 区域与心跳接口所在安全区域间的安全策略的动作为允许。

说明：

- 配置心跳接口时如果不配置 **remote** 参数，心跳报文被封装成 VRRP 报文，此时不配置安全策略设备也能正常处理。
- 配置心跳接口时如果配置 **remote** 参数，心跳报文被封装成 UDP 报文，此时需要正确配置心跳接口所在安全区域和 Local 之间的域间安全策略，设备才能正常接收和发送心跳报文。

b. 在系统视图下进入安全策略视图。

security-policy

c. 创建安全策略规则，并进入安全策略规则视图。

rule name *rule-name*

d. 指定源安全区域。

source-zone { *zone-name &<1-6>* | all }

*zone-name&< 1-6>*设置为 local 和心跳接口所在的安全区域。

说明：

source-zone 与 destination-zone 都指定两个安全区域表示允许流量在 local 区域与心跳接口所在安全区域间双向通过。

e. 指定目的安全区域。

destination-zone { *zone-name &<1-6>* | all }

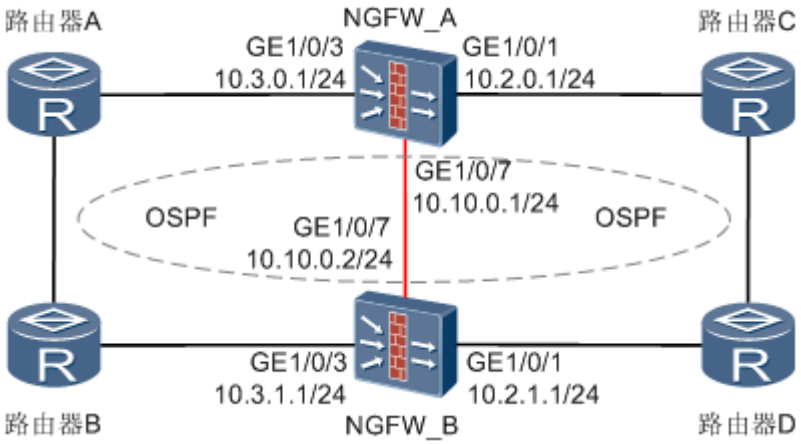
*zone-name&< 1-6>*设置为 local 和心跳接口所在的安全区域。

f. 配置动作为允许。

action permit

任务示例

图 1 配置心跳接口



如图 1 所示，NGFW_A 与 NGFW_B 通过心跳接口 GigabitEthernet1/0/7 相连，GigabitEthernet1/0/7 属于 DMZ 区域。

NGFW_A 上心跳接口的配置如下：

```
[NGFW_A] interface GigabitEthernet 1/0/7
[NGFW_A-GigabitEthernet1/0/7] ip address 10.10.0.1 24
[NGFW_A-GigabitEthernet1/0/7] quit
[NGFW_A] firewall zone dmz
[NGFW_A-zone-dmz] add interface GigabitEthernet 1/0/7
[NGFW_A-zone-dmz] quit
[NGFW_A] security-policy
[NGFW_A-policy-security] rule name ha
[NGFW_A-policy-security-rule-ha] source-zone local dmz
[NGFW_A-policy-security-rule-ha] destination-zone local dmz
[NGFW_A-policy-security-rule-ha] action permit
[NGFW_A-policy-security-rule-ha] quit
[NGFW_A-policy-security] quit
[NGFW_A] hrp interface GigabitEthernet 1/0/7
```

除了接口 IP 地址外，NGFW_B 的心跳接口配置与 NGFW_A 完全相同。

启用双机热备

启用双机热备功能后，双机热备组网建立成功。

前提条件

1. 完成配置 VRRP 备份组、配置接口监控、配置 VLAN 监控三者之一。
2. 完成配置心跳接口。

背景信息

对于主备备份场景，主用设备的命令行上显示 HRP_A，备用设备的命令行上显示 HRP_S。

对于负载分担场景，由于两台设备互为主备，因此先建立起主备关系的设备的命令行上显示 HRP_A，后建立起主备关系的设备的命令行上显示 HRP_S

注意：

正常情况下不会出现两台设备上都显示 **HRP_A** 或 **HRP_S** 的情况。

通常情况下，双机热备关系建立成功后，再进行其他业务的配置（比如 NAT、IPSec 等），这样配置命令和状态信息才可以从主用设备备份到备用设备。

操作步骤

1. **可选：**在系统视图下配置发送 Hello 报文的时间间隔。

   hrp timer hello *interval*

   缺省情况下，状态为 Active 的 VGMP 管理组发送 Hello 报文的时间间隔为 1000ms。

   注意：

   为了避免主备 NGFW 出现误切换，不要轻易将状态为 Active 的 VGMP 管理组发送 VGMP Hello 报文的时间间隔改小。建议采用缺省时间间隔 1000ms。

   若要修改此时间间隔，需保证主备 NGFW 配置的时间间隔一致。否则，可能会导致 NGFW 的主备状态不稳定。

2. **可选：**在系统视图下配置 VGMP 管理组的抢占延迟时间。

   hrp preempt [delay *interval*]

   缺省情况下，VGMP 管理组的抢占功能为启用状态，抢占延迟时间为 60s。

   注意：

   在双机热备组网环境下，如果 NGFW 和上下行设备之间一边运行 VRRP 协议，一边运行动态路由协议，必须配置 VGMP 管理组的抢占延迟时间大于动态路由协议（如 OSPF 协议）的收敛时间或者配置不抢占功能，否则可能会导致业务中断。

3. 在系统视图下配置负载分担场景的双机热备运行模式。

   hrp loadbalance-device

   缺省情况下，NGFW 的双机热备运行模式为主备备份模式，配置此命令可以将双机热备运行模式切换为负载分担模式。

   双机热备的负载分担场景下，需要分别在两台 NGFW 上配置此命令。

主备备份场景不需要配置此命令。

4. 在系统视图下配置主备备份场景的设备运行角色。

   hrp standby-device

   缺省情况下，NGFW 的运行角色为主用。配置此命令可以将 NGFW 的运行角色切换为备用。

   双机热备的主备备份场景下，需要在备用 NGFW 上配置此命令，将其运行角色切换为备用。主用 NGFW 上不需要配置此命令。

   负载分担场景下，不涉及设备运行角色的配置。

5. 在系统视图下配置负载分担场景的 NAT 地址池端口分配功能。

   hrp nat ports-segment { primary | secondary }

   注意：

   双机热备的负载分担场景下，当两台 NGFW 上都需要配置 NAT 地址池时，为避免出现 NAT 地址池的端口冲突问题，需要在一台 NGFW 上配置 **hrp nat ports-segment primary** 命令，另外一台 NGFW 上配置 **hrp nat ports-segment secondary** 命令。

   主备备份场景不需要配置此命令。

6. 在系统视图下启用双机热备功能。

   hrp enable

   此命令需要在双机热备中的两台 NGFW 上分别配置。

7. **可选：** 在系统视图下启用 TCP 会话状态检测延迟功能。

   hrp tcp link-state check delay *delay-time*

   在 NGFW 上、下行业务接口工作在二层的双机热备组网中，如果 NGFW 上启用了 TCP 会话状态检测，则需要分别在主、备设备上执行该命令，启用 TCP 会话状态检测延迟功能。否则，在主备切换时，新的主设备上会因为无法学习到 MAC 地址表而无法建立会话。启用该功能后，在主备切换时，新的主设备上会暂

时禁用 TCP 会话状态检测，在指定的延迟时间（*delay-time*）后再重新启用 TCP 会话状态检测，从而保证新的主设备能学习到 MAC 地址表。

缺省情况下，未启用 TCP 会话状态检测延迟功能。

8. **可选：**在系统视图下启用允许配置备用设备功能。

   hrp standby config enable

   此命令只有在备用设备上配置才生效。

   缺省情况下，未启用允许配置备用设备的功能。所有可以备份的信息都只能在主用设备上配置，不能在备用设备上配置。

   启用允许配置备用设备的功能后，所有可以备份的信息都可以直接在备用设备上进行配置。且备用设备上的配置可以同步到主用设备。

   如果主备设备上都进行了某项配置，则从时间上来说，后配置的信息会覆盖先配置的信息。

9. **可选：**执行命令 **hrp encryption-key**，配置主、备设备间加密特定备份报文（如配置命令）的密钥。

   缺省情况下，备份报文以明文形式传输。当两台 NGFW 的心跳口非直连时，出于安全性考虑，建议使用该命令配置加密密钥。配置密钥时，需要分别在主、备设备上配置，同时两台 NGFW 上的密钥要保持一致，否则会导致主备设备间备份失败。

10. **可选：** 执行命令 **hrp ip-packet priority** *priority-number*，配置心跳报文的 IP 头优先级。

    心跳报文的 IP 头优先级缺省值为 6。

    priority-number 数值越大表示优先级越高。设备转发报文时，优先级高的会被优先转发。

配置备份方式

介绍三种备份方式及配置过程，包括自动备份、手工备份和会话快速备份。

前提条件

启用自动备份或手工备份功能之前，必须先启用双机热备。

背景信息

NGFW 支持三种不同类型的备份方式，如表 1 所示。

表 1 NGFW 支持的 HRP 备份方式

备份方式	配置命令	状态信息	说明
自动备份	在主用设备、备用设备都正常工作的情况下，如果启用自动备份功能，则在主用设备上每执行一条可以备份的命令时，此配置命令就会被同步执行到备用设备。如果在主用设备上执行的命令不在备份范围内，则该命令仅在主用设备上执行。 对于备份范围内的配置命令，只能在主用设备上配置，备用设备不能配置。 对于备份范围外的配置命令，备用设备上可以配置。 当备用设备故障时，配置命令自动备份无法进行。	在主备运行过程中，当主用设备上产生了需要备份的状态信息时，主用设备自动将状态信息同步到备用设备进行备份，备用设备更新状态。 当备用设备故障时，状态信息自动备份无法进行。	此功能在 NGFW 上缺省为开启，即默认自动备份配置命令和状态信息。应用于各种双机热备组网中。
手工批量备份	当主用设备、备用设备都正常工作时，在主用设备上执行手工批量备份命令，则主用设备将备份范围内的配置命令批量发送到备用设备，备用设备同步执行这些配置命令。 当备用设备故障时，配置命令无法手工批量备份。	当主用设备、备用设备都正常工作时，在主用设备上执行手工批量备份命令，则主用设备将备份范围内的状态信息批量发送到备用设备，备用设备更新状态。 当备用设备故障时，状态信息无法手工批量备份。	主要用于主备设备之间配置不同步，需要批量备份的场景。
快速备份	不备份	当 NGFW 工作于负载分担组网环境下，如果报文的来回路径不一致，即来回两个方向的报文分别从不同的 NGFW 经过，如果主用设备的状态信息没有及	为了保证状态信息的及时同步，快速备份功能只是备份状态信息，不备份配置的命令。配置命令的备份由自动备份功能实现。通常用于负载分担组网环

表 1 NGFW 支持的 HRP 备份方式			
备份方式	配置命令	状态信息	说明
		时备份到备用设备，则备用设备会将到达的报文丢弃。 为防止上述现象发生，可以通过快速备份会话，将主用设备相应的状态信息表项快速备份到备用设备，使返回报文在备用设备上能够查找到相应的状态信息表项，从而保证内外部用户的业务不中断。 对于来回路径不一致的组网，需要开启快速备份功能。	境下，主备设备需要同时处理业务的场景。

操作步骤

- 在系统视图下启用命令与状态信息的自动备份。

  hrp auto-sync [config | connection-status]

  缺省情况下，命令与状态信息的自动备份功能处于启用状态。

  使用不带参数的 hrp auto-sync 命令时，表示同时进行配置命令和状态信息的自动备份。

- 在用户视图下启用手工批量备份功能。

  hrp sync [config | connection-status]

  当自动备份功能无法进行或者两台设备之间配置不同步，需要强制进行一次备份完全同步时，启用手工批量备份功能。

- 在系统视图下启用会话快速备份功能。

  hrp mirror session enable，启用会话快速备份。

  NGFW 工作于负载分担方式时，报文的来回路径可能会不一致，务必启用会话快速备份功能，使一台 NGFW 的会话信息立即同步至另一台 NGFW，保证内外部用户的业务不中断。

NGFW 工作于主备备份组网环境下时，可以不启用此功能。

说明：

快速备份功能只是备份状态信息，不备份配置的命令。

双机热备配置检查和结果验证

双机热备配置完成后，请进行配置检查和结果验证。检查配置是否正确，以及主备设备之间是否可以正常切换。

操作步骤

1. 查看命令行提示符显示。

   HRP 主备关系建立成功后，如果命令行上有 HRP_A 的标识，表示此 NGFW 和另外一台 NGFW 进行协商之后成为主用设备；如果命令行上有 HRP_S 的标识，表示此 NGFW 和另外一台 NGFW 进行协商之后成为备用设备。

2. 按照表 1 检查双机热备的配置。

表 1 双机热备配置检查 Checklist

序号	是否必选	检查项	检查方法	检查结果
通用项目				
1	必选	主用防火墙和备用防火墙的产品型号、软件版本一致。	<sysname> **display version**	□通过 □不通过
2	必选	主用防火墙和备用防火墙的接口卡类型和安装位置一致。	<sysname> **display device**	□通过 □不通过
3	必选	主用防火墙和备用防火墙使用相同的业务接口。	<sysname> **display hrp state**	□通过 □不通过
4	必选	主用防火墙和备用防火墙使用相同的心跳口。	<sysname> **display hrp interface**	□通过 □不通过
4.a	可选	如果采用 Eth-Trunk 作为备份通道，主用防火墙和备用防火墙的 Eth-Trunk 成员接口相同。	<sysname> **display eth-trunk** *trunk-id*	□通过 □不通过
4.b	可选	如果使用业务通道作为备份通道，必	<sysname> **display current-**	□通过

表 1 双机热备配置检查 Checklist				
序号	**是否必选**	**检查项**	**检查方法**	**检查结果**
		须在指定心跳口的同时指定对端心跳口的 IP 地址。	**configuration | include hrp interface**	□不通过
5	必选	主用防火墙和备用防火墙的接口加入到相同的安全区域。	<sysname> **display zone**	□通过 □不通过
6	可选	主用防火墙和备用防火墙的业务接口加入相同的 VRRP 备份组、共享一个虚拟 IP 地址。	• IPv4：<sysname> **display vrrp interface** *interface-type interface-number* • IPv6：<sysname> **display vrrp6 interface** *interface-type interface-number*	□通过 □不通过
7	可选	主用防火墙和备用防火墙的业务接口加入不同的 VGMP 管理组。	<sysname> **display hrp state**	□通过 □不通过
8	必选	已关闭主用防火墙的抢占功能，或者抢占延时大于 60 秒。	<sysname> **display hrp group**	□通过 □不通过
9	可选	如果报文的来回路径不一致，必须启用会话快速备份功能。	<sysname> **display current-configuration | include hrp mirror**	□通过 □不通过
业务接口工作在二层				
10	必选	上下行业务接口加入到同一个 VLAN 中。	<sysname> **display port vlan** [*interface-type interface-number*]	□通过 □不通过
11	必选	使用 VGMP 管理组直接监控业务接口的状态。	<sysname> **display hrp state**	□通过 □不通过
12	可选	如果防火墙上下行接口连接交换机，使用主备备份方式。	<sysname> **display hrp group**	□通过 □不通过
13	可选	如果防火墙上下行接口连接路由器，使用负载分担方式。	<sysname> **display hrp group**	□通过 □不通过
业务接口工作在三层				
14	必选	主用防火墙和备用防火墙的接口已经配置 IP 地址。	<sysname> **display ip interface brief**	□通过 □不通过
15	可选	如果防火墙上下行接口连接交换机，防火墙的上下行设备将 VRRP 备份组的虚拟 IP 地址作为自己的下一跳地址。	检查防火墙的上下行设备的静态路由配置。	□通过 □不通过
16	可选	如果防火墙上下行接口连接路由器，防火墙运行 OSPF 协议，且 OSPF 区域不包括心跳口。	<sysname> **display ospf** [*process-id*] **brief**	□通过 □不通过

表 1 双机热备配置检查 Checklist				
序号	**是否必选**	**检查项**	**检查方法**	**检查结果**
17	可选	如果防火墙上下行接口连接路由器，且工作在主备备份方式，必须根据双机热备的状态调整路由的 COST 值。	<sysname> **display current-configuration | include hrp ospf-cost**	□通过 □不通过
负载分担方式				
18	必选	启用会话快速备份功能。	<sysname> **display current-configuration | include hrp mirror**	□通过 □不通过
19	可选	指定 NAT 地址池的端口范围。	<sysname> **display current-configuration | include hrp nat**	□通过 □不通过

3. 在主用设备接口视图下，执行命令 **shutdown**，验证主备设备是否进行切换。

   在主用设备的一个业务接口下执行命令 shutdown 后，主用设备此接口的状态变为 Down，其他接口工作正常。备用设备的标记由 HRP_S 变为 HRP_A，主用设备的标记由 HRP_A 变为 HRP_S，且业务正常转发，说明主备机切换成功。

   在主用设备的相同接口上执行命令 undo shutdown 后，主用设备此接口的状态变为 Up。在经过抢占延迟时间后，主用设备的标记由 HRP_S 变为 HRP_A，备用设备的标记由 HRP_A 变为 HRP_S，且业务正常转发，说明故障恢复时抢占成功。

4. 在主用设备用户视图下，执行命令 **reboot**，通过命令行重启主用设备，验证主备设备是否进行切换。

   在主用设备上执行命令 reboot，如果备用设备的标记由 HRP_S 变为 HRP_A，且业务正常转发，说明主备机切换成功。

   主用设备重启完成后，重新正常工作。在经过抢占延迟时间后，主用设备的标记由 HRP_S 变为 HRP_A，备用设备的标记由 HRP_A 变为 HRP_S，且业务正常转发，说明故障恢复时抢占成功。

双机热备常用检查命令——display hrp

命令功能

display hrp 命令用来显示 HRP 的配置参数和状态信息。

命令格式

```
display hrp { state | interface | statistic | group }
```

参数说明

参数	参数说明	取值
state	显示当前 HRP 的状态，包括管理组的接口和 track 接口等。	-
interface	显示当前 HRP 备份通道的接口及其状态。	-
statistic	显示当前 HRP 的备份统计信息。	-
group	显示当前 VGMP 管理组的信息。	-

使用实例

在 NGFW 启动 HRP 功能之后，显示 HRP 的状态信息。

```
HRP_A<sysname> display hrp state
The firewall's config state is: ACTIVE

 Current state of virtual routers configured as active:
                   GigabitEthernet1/0/2    vrid   2 : active
                   GigabitEthernet1/0/1    vrid   1 : active
```

在 NGFW 启动 HRP 功能之后，显示 HRP 备份通道的接口及其状态。

```
HRP_A<sysname> display hrp interface
GigabitEthernet1/0/2 : running
GigabitEthernet1/0/1 : ready
```

在 NGFW 启动 HRP 功能之后，显示 HRP 的备份统计信息。

```
HRP_A<sysname> display hrp statistic
Current hrp state: backup

 Statistic of hrp messages send queue:
   Number of messages in queue:       0
   Sequence of next new message:      501
   Sequence of next send message:     501
   Sequence of expected ack message:  501

 Statistic of hrp messages receive queue:
```

```
  Number of messages in queue:   0
  Sequence of expected message:  2537
```

表 1 display hrp statistic 命令输出信息描述

项目	描述
Current hrp state	当前的备份状态： • ready：就绪 • backup：备份 • smooth：平滑 • unkown：未知 状态为“backup”时才表示主备设备之间能正常备份，其他状态均为中间状态。
Statistic of hrp messages send queue	设备发送备份报文的队列统计。
Statistic of hrp messages receive queue	设备接收备份报文的队列统计。

在 NGFW 启动 HRP 功能之后，显示当前 VGMP 管理组的信息。

```
HRP_A<sysname> display hrp group
 Active group status:
   Group enabled:         yes
   State:                 active
   Priority running:      65001
   Total VRRP members:    1
   Hello interval(ms):    1000
   Preempt enabled:       yes
   Preempt delay(s):      30
   TCP check delay(s):    60
   Peer group available:  1
   Peer's member same:    yes
 Standby group status:
   Group enabled:         yes
   State:                 standby
   Priority running:      65000
   Total VRRP members:    1
   Hello interval(ms):    1000
   Preempt enabled:       yes
   Preempt delay(s):      0
   TCP check delay(s):    60
   Peer group available:  1
   Peer's member same:    yes
```

双机热备常用检查命令——display vrrp

命令功能

display vrrp 命令用来查看 IPv4 的 VRRP 备份组的状态信息。

命令格式

display vrrp [**interface** *interface-type interface-number* [*virtual-router-id*]]

参数说明

参数	参数说明	取值
interface-type interface-number	接口类型和接口编号。	接口类型为 GigabitEthernet 接口、子接口、Eth-Trunk 接口或 Vlanif 接口。
virtual-router-id	IPv4 的 VRRP 备份组组号。	必须为已经创建的 IPv4 的 VRRP 备份组组号。

使用指南

- 如果不输入接口名和备份组组号，则显示 NGFW 上所有 IPv4 的 VRRP 备份组的状态信息。
- 如果只输入接口名，则显示接口上所有 IPv4 的 VRRP 备份组的状态信息。
- 如果输入接口号和备份组组号，则显示指定 IPv4 的 VRRP 备份组的状态信息。

使用实例

查看 NGFW 上所有 IPv4 的 VRRP 备份组的信息。

```
<sysname> display vrrp
GigabitEthernet1/0/1 | Virtual Router 1
    VRRP Group : Active
    State : Active
    Virtual IP : 10.1.1.99
    Virtual MAC : 0000-5e00-0101
    Primary IP : 10.1.1.100
    Priority Run : 100
    Active Priority : 100
    Preempt : YES   Delay Time : 0
```

```
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES
GigabitEthernet1/0/1 | Virtual Router 3
    VRRP Group : Standby
    State : Active
    Virtual IP : 10.1.1.100
    Virtual MAC : 0000-5e00-0103
    Primary IP : 10.1.1.100
    Priority Run : 100
    Active Priority : 100
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES
GigabitEthernet1/0/2 | Virtual Router 2
    VRRP Group : Active
    State : Active
    Virtual IP : 10.1.2.101
    Virtual MAC : 0000-5e00-0102
    Primary IP : 10.1.2.100
    Priority Run : 100
    Active Priority : 100
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES
```

查看接口上所有 IPv4 的 VRRP 备份组的信息。

```
<sysname> display vrrp interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1 | Virtual Router 1
    VRRP Group : Active
    State : Active
    Virtual IP : 10.1.1.99
    Virtual MAC : 0000-5e00-0101
    Primary IP : 10.1.1.100
    Priority Run : 100
    Active Priority : 100
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
```

```
    Check TTL : YES
GigabitEthernet1/0/1 | Virtual Router 3
    VRRP Group : Standby
    State : Active
    Virtual IP : 10.1.1.100
    Virtual MAC : 0000-5e00-0103
    Primary IP : 10.1.1.100
    Priority Run : 100
    Active Priority : 100
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES
```

查看接口上指定 IPv4 的 VRRP 备份组的信息。

```
<sysname> display vrrp interface GigabitEthernet 1/0/1 1
GigabitEthernet1/0/1 | Virtual Router 1
    VRRP Group : Active
    State : Active
    Virtual IP : 10.1.1.99
    Virtual MAC : 0000-5e00-0101
    Primary IP : 10.1.1.100
    Priority Run : 100
    Active Priority : 100
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES
```

表 1 display vrrp 命令输出信息描述

项目	描述
Virtual Router	VRRP 备份组号。
VRRP Group	VRRP 备份组所处的 VGMP 管理组： • Active：表示该备份组处于 Active 管理组。 • Standby：表示该备份组处于 Standby 管理组。
State	VRRP 状态： • Active：表示设备在该备份组中作为 Active。 • Standby：表示设备在该备份组中作为 Standby。 • Initialize：所有 VRRP 备份组以 Initialize 状态开始。
Virtual IP	VRRP 备份组的虚拟 IP 地址。

表 1 display vrrp 命令输出信息描述	
项目	**描述**
Virtual MAC	虚拟 MAC 地址。 虚拟 MAC 地址是根据 VRID 自动生成的 MAC 地址，其格式为：00-00-5E-00-01-{VRID}。
Primary IP	接口的 IP 地址。
Priority Run	VRRP 备份组的运行优先级，即当前的优先级。
Active Priority	备份组中主设备的优先级。若设备为主设备，则该项的值与 **Priority Run** 的值相同。
Preempt	抢占方式标识： • YES：表示抢占。 • NO：表示不抢占。
Delay Time	采用抢占方式时的延迟时间，单位是秒。
Advertisement Timer	主设备发送广播报文的时间间隔，单位是秒。
Auth Type	VRRP 报文认证方式： • NONE：表示不认证。 • SIMPLE TEXT：表示简单字符认证。 • MD5：表示 MD5 认证。
Auth key	认证字（密文形式）。
Check TTL	是否检测 VRRP 报文的 TTL 值。

举例：业务接口工作在三层，上行连接路由器，下行连接交换机的主备备份组网

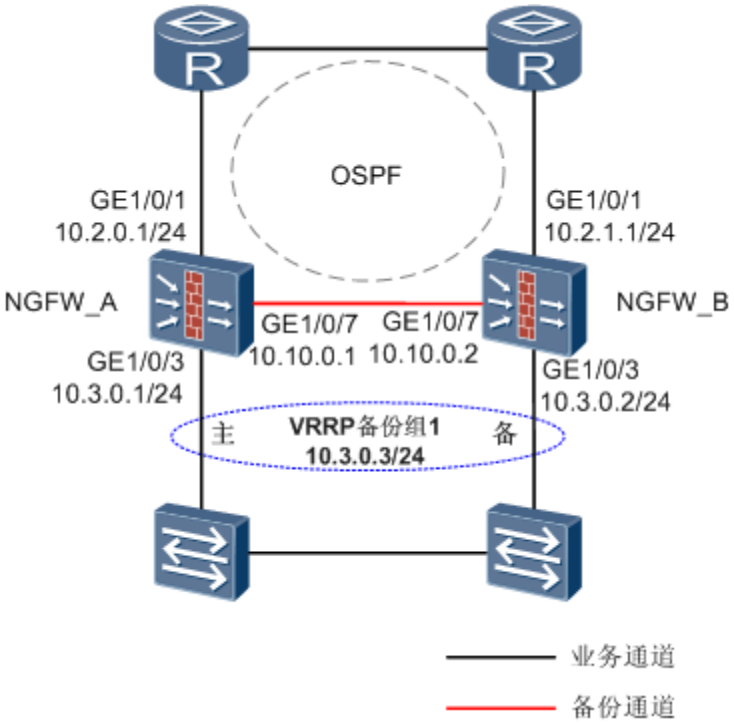
介绍了业务接口工作在三层，上行连接路由器，下行连接交换机的主备备份组网的举例。

组网需求

如图 1 所示，两台 NGFW 的业务接口都工作在三层，上行连接路由器，下行连接二层交换机。NGFW 与路由器之间运行 OSPF 协议。

现在希望两台 NGFW 以主备备份方式工作。正常情况下，流量通过 NGFW_A 转发。当 NGFW_A 出现故障时，流量通过 NGFW_B 转发，保证业务不中断。

图 1 业务接口工作在三层，上行连接路由器，下行连接交换机的主备备份组网



操作步骤

1. 配置接口，完成网络基本配置。

   a. 在 NGFW_A 上配置接口。

      1. 选择“网络 > 接口”。

      2. 单击 GE1/0/1，按如下参数配置。

安全区域	untrust
IPv4	
IP 地址	10.2.0.1/24

      3. 单击“确定”。

      4. 参考上述步骤按如下参数配置 GE1/0/3 接口。

安全区域	trust
IPv4	
IP 地址	10.3.0.1/24

      5. 参考上述步骤按如下参数配置 GE1/0/7 接口。

安全区域	dmz
IPv4	

IP 地址	10.10.0.1/24

b. 在 NGFW_B 上配置接口。

1. 选择“网络 > 接口”。

2. 单击 GE1/0/1，按如下参数配置。

安全区域	untrust
IPv4	
IP 地址	10.2.1.1/24

3. 单击“确定”。

4. 参考上述步骤按如下参数配置 GE1/0/3 接口。

安全区域	trust
IPv4	
IP 地址	10.3.0.2/24

5. 参考上述步骤按如下参数配置 GE1/0/7 接口。

安全区域	dmz
IPv4	
IP 地址	10.10.0.2/24

2. 配置 OSPF，保证路由可达。

a. 在 NGFW_A 上配置 OSPF。

1. 选择“网络 > 路由 > OSPF”。

2. 单击“新建”。

3. 按如下参数新建 OSPF。

类型	OSPF v2
进程 ID	10

4. 单击“确定”。

5. 单击  。

6. 单击“新建”。

7. 按如下参数新建区域。

区域	0.0.0.0
网段 IP	10.2.0.0
正/反掩码	255.255.255.0

8. 单击“确定”。

9. 选择“基本配置 > 网络配置”。

10. 单击“新建”。

11. 按如下参数新建网络。

区域	0.0.0.0
网段 IP	10.3.0.0
正/反掩码	255.255.255.0

12. 单击“确定”。

b. 在 NGFW_B 上配置 OSPF。

1. 选择“网络 > 路由 > OSPF”。

2. 单击“新建”。

3. 按如下参数新建 OSPF。

类型	OSPF v2
进程 ID	10

4. 单击“确定”。

5. 单击。

6. 单击“新建”。

7. 按如下参数新建区域。

区域	0.0.0.0
网段 IP	10.2.1.0
正/反掩码	255.255.255.0

8. 单击“确定”。

9. 选择“基本配置 > 网络配置”。

10. 单击“新建”。

11. 按如下参数新建网络。

区域	0.0.0.0
网段 IP	10.3.0.0
正/反掩码	255.255.255.0

12. 单击“确定”。

3. 配置双机热备。

a. 在 NGFW_A 上配置双机热备功能。

1. 选择“系统 > 高可靠性 > 双机热备”。

2. 单击“配置”。

3. 选中“启用”前的复选框后，按如下参数配置。

4. 单击“确定”。

b. 在 NGFW_B 上配置双机热备功能。

1. 选择“系统 > 高可靠性 > 双机热备”。

2. 单击“配置”。

3. 选中“启用”前的复选框后，按如下参数配置。

4. 单击“确定”。

4. 在内网的设备上配置缺省路由，下一跳为 VRRP 备份组 1 的虚拟 IP 地址 10.3.0.3。

5. 配置安全策略。

在 NGFW_A 上配置的安全策略会自动备份到 NGFW_B 上。

a. 选择“策略 > 安全策略”。

b. 单击“新建”。

c. 按照如下参数配置安全策略。

名称	policy_sec
源安全区域	local,trust,untrust
目的安全区域	local,trust,untrust

动作	允许

d. 单击“确定”。

结果验证

选择“系统 > 高可靠性 > 双机热备”，查看双机热备的运行情况。

- 正常情况下，NGFW_A 的“当前运行模式”为“主备备份”，“当前运行角色”为“主用”；NGFW_B 的“当前运行模式”为“主备备份”，“当前运行角色”为“备用”。这说明流量通过 NGFW_A 转发。
- 当 NGFW_A 出现故障时，NGFW_A 的“当前运行模式”为“主备备份”，“当前运行角色”为“备用”；NGFW_B 的“当前运行模式”为“主备备份”，“当前运行角色”为“主用”。这说明流量通过 NGFW_B 转发。

配置脚本

NGFW_A

```
#
 hrp enable

 hrp ospf-cost adjust-enable
 hrp interface GigabitEthernet 1/0/7
 hrp preempt delay 60
#
interface GigabitEthernet 1/0/1
 ip address 10.2.0.1 255.255.255.0
 hrp track active
#
interface GigabitEthernet 1/0/3
 ip address 10.3.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.3.0.3 active
#
interface GigabitEthernet 1/0/7
 ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet 1/0/3
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet 1/0/1
```

NGFW_B

```
#
 hrp enable
 hrp standby-device
 hrp ospf-cost adjust-enable
 hrp interface GigabitEthernet 1/0/7
 hrp preempt delay 60
#
interface GigabitEthernet 1/0/1
 ip address 10.2.1.1 255.255.255.0
 hrp track standby
#
interface GigabitEthernet 1/0/3
 ip address 10.3.0.2 255.255.255.0
  vrrp vrid 1 virtual-ip 10.3.0.3 standby
#
interface GigabitEthernet 1/0/7
 ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet 1/0/3
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet 1/0/1
```

NGFW_A	NGFW_B

#
firewall zone dmz
 set priority 50
 add interface GigabitEthernet1/0/7
#
ospf 10
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.3.0.0 0.0.0.255
#
security-policy
 rule name policy_sec
  source-zone local
  source-zone trust
  source-zone untrust
  destination-zone local
  destination-zone trust
  destination-zone untrust
  action permit
	#
	firewall zone dmz
	 set priority 50
	 add interface GigabitEthernet1/0/7
	#
	ospf 10
	 area 0.0.0.0
	  network 10.2.1.0 0.0.0.255
	  network 10.3.0.0 0.0.0.255
	#
	security-policy
	 rule name policy_sec
	  source-zone local
	  source-zone trust
	  source-zone untrust
	  destination-zone local
	  destination-zone trust
	  destination-zone untrust
	  action permit

HCIE-Security 模拟面试问题及面试建议

1. VRRP、VGMP、HRP 在双机热备中起到什么作用？
2. 双机热备的组网方式有哪些，分别阐述？

每一章的 FAQ 都是面试考官喜欢追问的地方^_^
每一章的故障排除也是哦……