防火墙双机热备技术

www.huawei.com

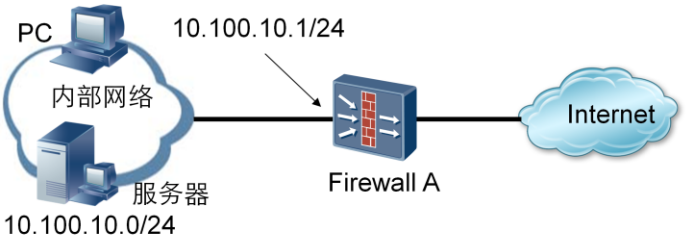
HUAWEI

目标

- 学完本课程后，您将能够:
  - 掌握双机热备技术原理
  - 掌握双机热备基础配置

目录

双机热备份技术产生的原因

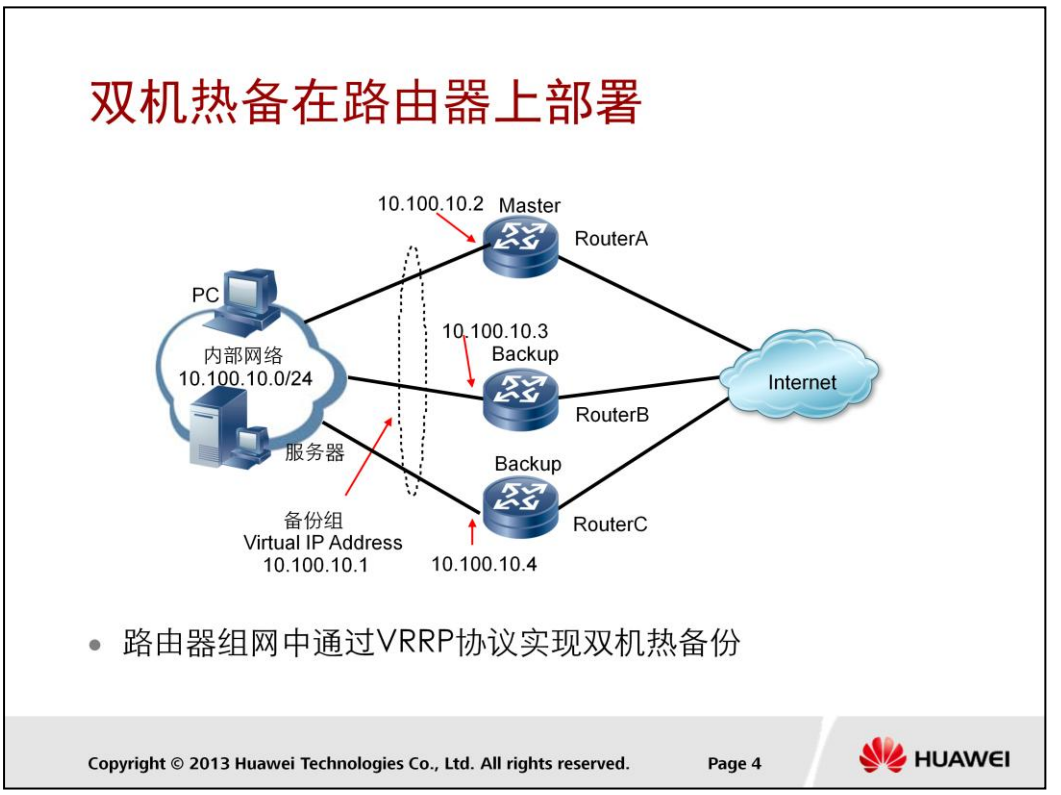


- 传统的组网方式如图所示，内部用户和外部用户的交互报文全部通过Firewall A。如果Firewall A出现故障，内部网络中所有以Firewall A作为默认网关的主机与外部网络之间的通讯将中断，通讯可靠性无法保证。

HUAWEI

双机热备份技术的出现改变了可靠性难以保证的尴尬状态，通过在网络出口位置部署两台或多台网关设备，保证了内部网络于外部网络之间的通讯畅通。

USG防火墙作为安全设备，一般会部署在需要保护的网络和不受保护的网络之间，即位于业务接口点上。在这种业务点上，如果仅仅使用一台USG防火墙设备，无论其可靠性多高，系统都可能会承受因为单点故障而导致网络中断的风险。为了防止一台设备出现意外故障而导致网络业务中断，可以采用两台防火墙形成双机备份。



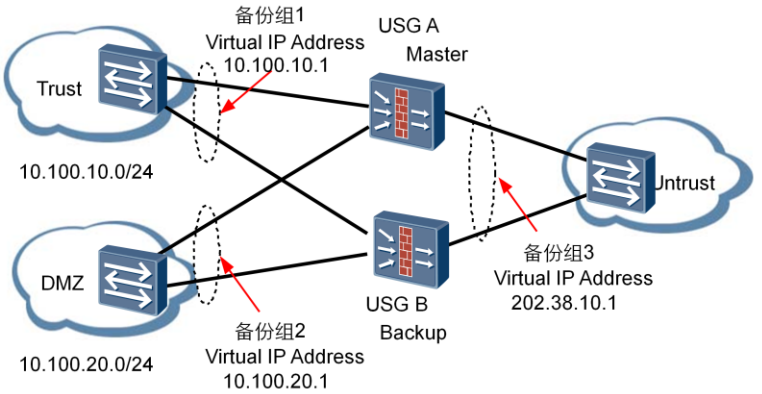
为了避免路由器传统组网所引起的单点故障的发生，通常情况可以采用多条链路的保护机制，依靠动态路由协议进行链路切换。但这种路由协议来进行切换保护的方式存在一定的局限性，当不能使用动态路由协议时，仍然会导致链路中断的问题，因此推出了另一种保护机制VRRP（虚拟路由冗余协议）来进行。采用VRRP的链路保护机制比依赖动态路由协议的广播报文来进行链路切换的时间更短，同时弥补了不能使用动态路由情况下的链路保护。

VRRP（Virtual Router Redundancy Protocol）是一种基本的容错协议。

- 备份组：同一个广播域的一组路由器组织成一个虚拟路由器，备份组中的所有路由器一起，共同提供一个虚拟IP地址，作为内部网络的网关地址。
- 主（Master）路由器：在同一个备份组中的多个路由器中，只有一台处于活动状态，只有主路由器能转发以虚拟IP地址作为下一跳的报文。
- 备份（Backup）路由器：在同一个备份组中的多个路由器中，除主路由器外，其他路由器均为备份路由器，处于备份状态。

主路由器通过组播方式定期向备份路由器发送通告报文（HELLO），备份路由器则负责监听通告报文，以此来确定其状态。由于VRRP HELLO报文为组播报文，所以要求备份组中的各路由器通过二层设备相连，即启用VRRP时上下行设备必须具有二层交换功能，否则备份路由器无法收到主路由器发送的HELLO报文。如果组网条件不满足，则不能使用VRRP。

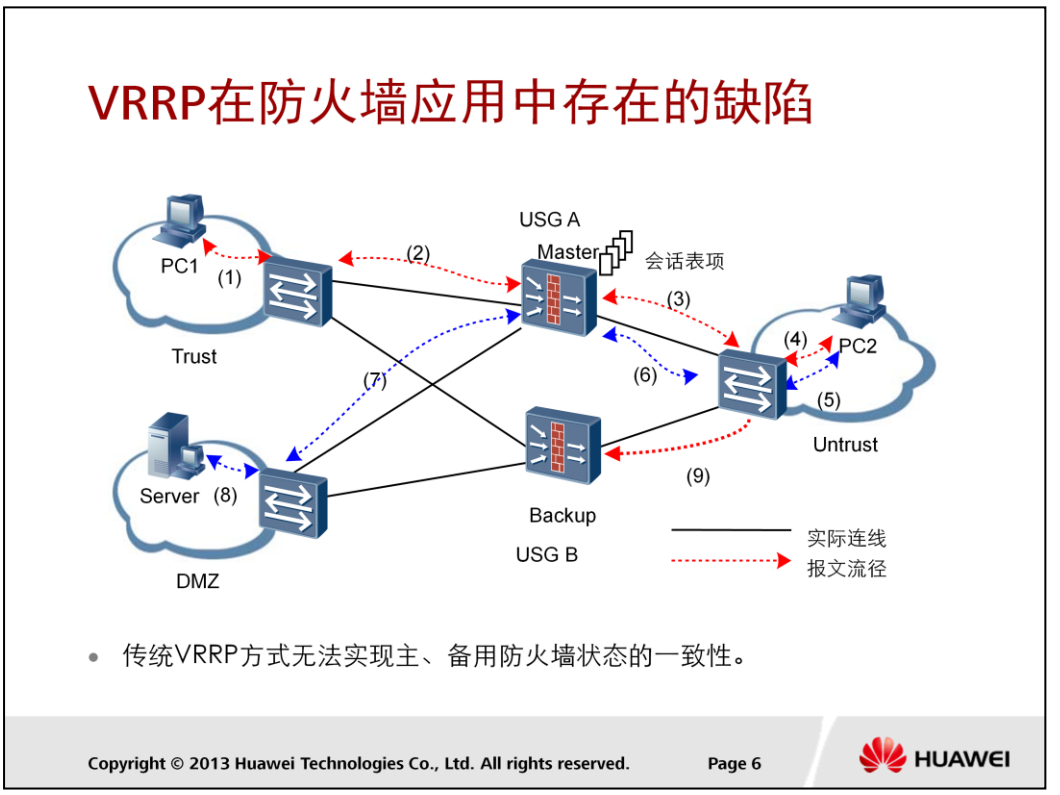
VRRP在多区域防火墙组网中的应用



- 为防火墙上多个区域提供双机备份功能时，需要在每一台防火墙上配置多个VRRP备份组。

当防火墙上多个区域需要提供双机备份功能时，需要在一台防火墙上配置多个VRRP备份组。

由于USG防火墙是状态防火墙，它要求报文的来回路径通过同一台防火墙。为了满足这个限制条件，就要求在同一台防火墙上的所有VRRP备份组状态保持一致，即需要保证在主防火墙上所有VRRP备份组都是主状态，这样所有报文都将从此防火墙上通过，而另外一台防火墙则充当备份设备。



如图所示，假设USG A和USG B的VRRP状态一致，即USG A的所有接口均为主用状态，USG B的所有接口均为备用状态。

此时，Trust区域的PC1访问Untrust区域的PC2，报文的转发路线为(1)-(2)-(3)-(4)。USG A转发访问报文时，动态生成会话表项。当PC2的返回报文经过(4)-(3)到达USG A时，由于能够命中会话表项，才能再经过(2)-(1)到达PC1，顺利返回。同理，当PC2和DMZ区域的Server也能互访。

假设USG A和USG B的VRRP状态不一致，例如，当USG B与Trust区域相连的接口为备用状态，但与Untrust区域的接口为主用状态，则PC1的报文通过USG A设备到达PC2后，在USG A上动态生成会话表项。PC2的返回报文通过路线(4)-(9)返回。此时由于USG B上没有相应数据流的会话表项，在没有其他报文过滤规则允许通过的情况下，USG B将丢弃该报文，导致会话中断。

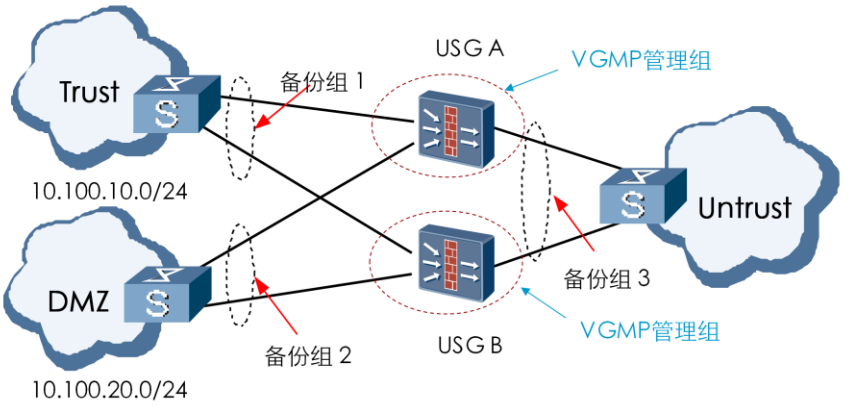
问题产生的原因：报文的转发机制不同。

- 路由器：每个报文都会查路由表当匹配上后才进行转发，当链路切换后，后续报文不会受到影响，继续进行转发。
- 状态检测防火墙：如果首包允许通过会建立一条五元组的会话连接，只有命中该会话表项的后续报文（包括返回报文）才能够通过防火墙；如果链路切换后，后续报文找不到正确的表项，会导致业务中断。

注意：当路由器配置NAT后也会存在同样的问题，因为在进行NAT后会形成一个NAT转换后的表项。

VRRP用于防火墙多区域备份

- 为了保证所有VRRP备份组切换的一致性，在VRRP的基础上进行了扩展，推出了VGMP（VRRP Group Management Protocol）来弥补此局限。

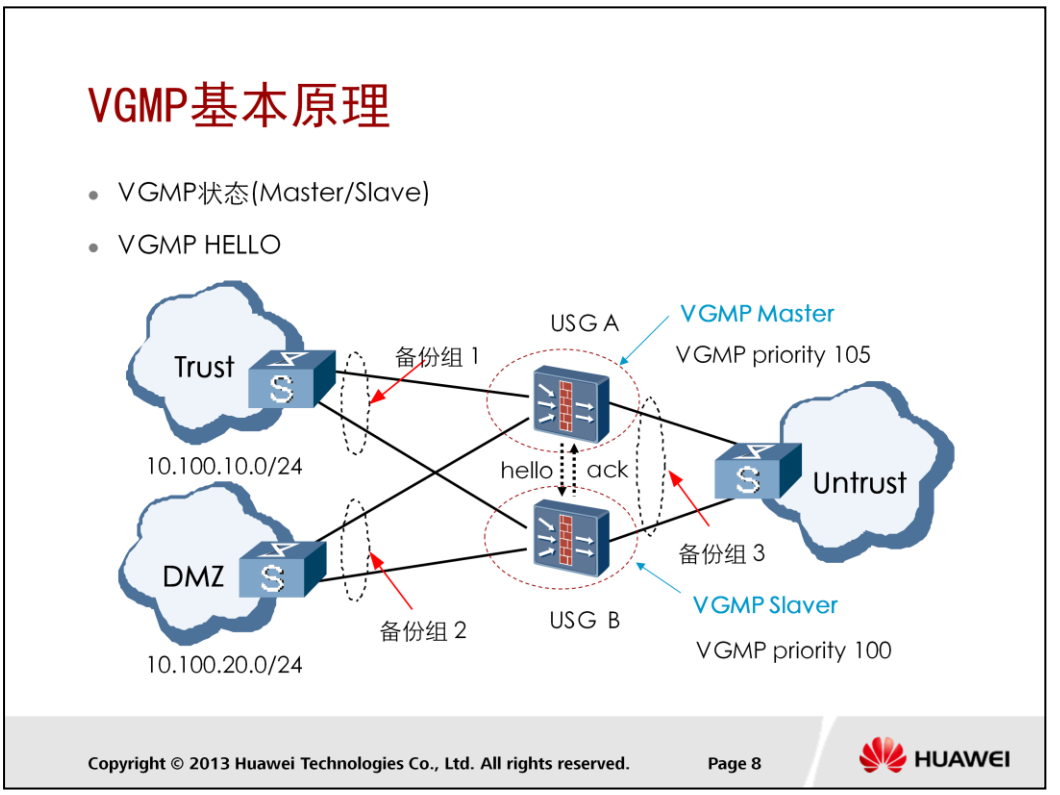


HUAWEI

VRRP在防火墙中应用的要求：

- VRRP状态的一致性
- 会话表状态备份

VGMP提出VRRP管理组的概念，将同一台防火墙上的多个VRRP备份组都加入到一个VRRP管理组，由管理组统一管理所有VRRP备份组。通过统一控制各VRRP备份组状态的切换，来保证管理组内的所有VRRP备份组状态都是一致的。



当防火墙上的VGMP为Master状态时，组内所有VRRP备份组的状态统一为Master状态，所有报文都将从该防火墙上通过，该防火墙成为主用防火墙。此时另外一台防火墙上对应的VGMP为备状态，该防火墙成为备用防火墙。

通过指定VGMP组的优先级来决定谁将成为主防火墙或备用防火墙。

VGMP的优先级会根据组内的VRRP备份组成员的状态动态调整，以此完成两台防火墙的主备倒换。

与VRRP类似，状态为Master的VGMP也会定期向对端发送HELLO报文，通知Slave端本身的运行状态（包括优先级、VRRP成员状态等）。与VRRP不同的是，Slave端收到HELLO报文后，会回应一个ACK消息，该消息中也会携带本身的优先级、VRRP成员状态等。

VGMP HELLO报文发送周期缺省为1秒。当Slave端三个HELLO报文周期没有收到对端发送的HELLO报文时，会认为对端出现故障，从而将自己切换到Master状态。

- 状态一致性管理

各备份组的主/备状态变化都需要通知其所属的VGMP管理组，由VGMP管理组决定是否允许VRRP备份组进行主/备状态切换。如果需要切换，则VGMP管理组控制所有的VRRP备份组统一切换。VRRP备份组加入到管理组后，状态不能自行单独切换。

- 抢占管理

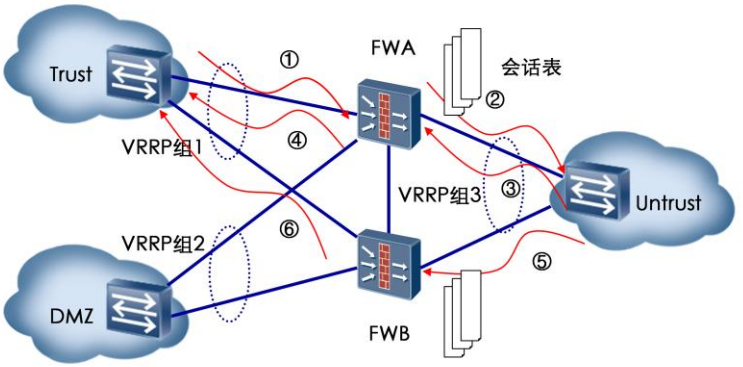
VRRP备份组本身具有抢占功能。即当原来出现故障的主设备故障恢复时，其优先级也会恢复，此时可以重新将自己的状态抢占为主。

VGMP管理组的抢占功能和VRRP备份组类似，当管理组中出现故障的备份组故障恢复时，管理组的优先级也将恢复。此时VGMP可以决定是否需要重新抢占称为主设备。

当VRRP备份组加入到VGMP管理组后，备份组上原来的抢占功能将失效，抢占行为发生与否必须由VGMP管理组统一决定。

HRP基本概念

- HRP（Huawei Redundancy Protocol）协议，用来将主防火墙关键配置和连接状态等数据向备防火墙上同步。



HUAWEI

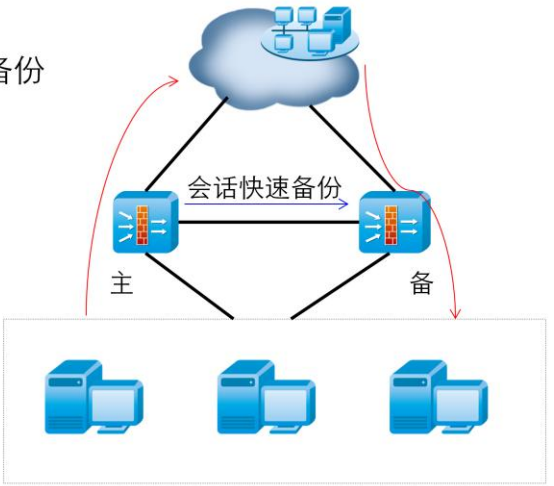
在双机热备组网中，当主防火墙出现故障时，所有流量都将切换到备防火墙。因为USG防火墙是状态防火墙，如果备防火墙上没有原来主防火墙上的会话表等连接状态数据，则切换到备防火墙的流量将无法通过防火墙，造成现有的连接中断，此时用户必须重新发起连接。

HRP模块提供了基础的数据备份机制和传输功能。各个应用模块收集本模块需要备份的数据，提交给HRP模块，HRP模块负责将数据发送到对端防火墙的对应模块，应用模块需要再将HRP模块提交上来的数据进行解析，并加入到防火墙的动态运行数据池中。

- 备份内容：要备份的连接状态数据包括TCP/UDP的会话表、ServerMap表项、动态黑名单、NO-PAT表项、ARP表项等。
- 备份方向:防火墙上有状态为主的VGMP管理组，向对端备份。
- 备份方式：分为三种
  - 批量备份：在两台设备第一次协商完成后，批量备份所有信息
  - 实时备份：在设备运行过程中，新建或者刷新的数据实时备份
  - 配置批量备份需要消耗较多的资源，缺省情况下是关闭的。
- 备份通道：一般情况下，在两台设备上直连的端口作为备份通道，有时也称为“心跳线”（VGMP也通过该通道进行通信）。

HRP会话快速备份

- 首包会话快速备份
- 更新报文会话快速备份



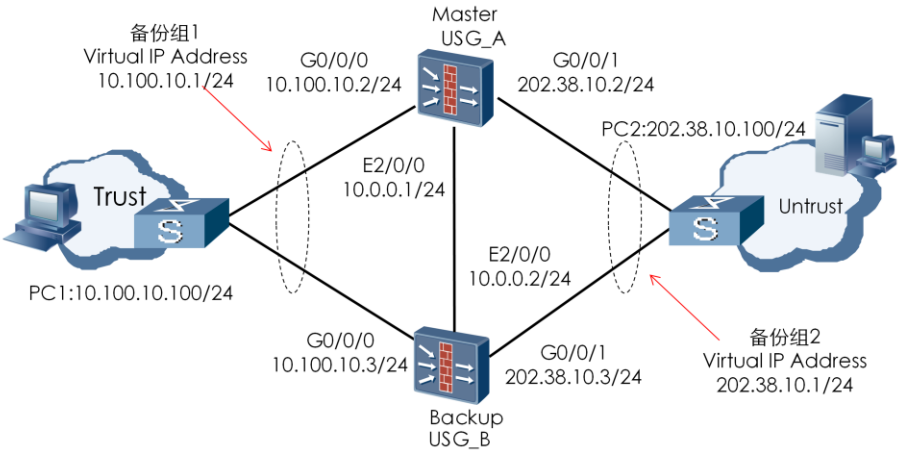
在来回路径不一致的组网中，业务流的来回报文有可能不会从同一个防火墙上经过。为了支持来回路径不一致的组网，防火墙增加了会话快速备份功能。即在首包创建会话时，立即将会话数据打包备份到对端，然后再将报文转发出去，保证了当回应的报文到达对端防火墙时，对端防火墙上已经接收到备份过来的会话数据并加入到会话表中。比如对于TCP三次握手的报文，SYN+ACK报文从另一台设备回来时，由于查不到会话，报文会被丢弃，导致连接建立失败。对于UDP会话，第一个反向报文过来时，在另一台上也会因为查不到会话，需要走包过滤流程，有可能会被丢弃。

通常情况下，对于TCP连接、状态改变的报文命中会话之后立即备份到对端，包括三次握手报文和fin、rst报文；对于UDP会话，快速备份是创建会话之后立即备份到对端，后续报文也进行备份以避免会话信息的老化。

目录

双机热备基本组网

- 上下行业务接口工作在三层模式，连接二层设备时，需要在上下行的业务接口上配置VRRP备份组，使VGMP管理组能够通过VRRP备份组监测三层业务接口。



双机热备组网最常见的是防火墙采用路由模式，下行交换机双线上联到防火墙，正常情况下防火墙A作为主，当防火墙A上行或下行链路down掉后，防火墙B自动切换为主设备，交换机流量走向防火墙B。

Master管理组默认情况下会每隔1秒发送一次vrrp报文，可以在接口视图下调整vrrp报文发送间隔。接口视图下修改vrrp报文发送时间：

vrrp vrid virtual-router-ID timer advertise adver-interval

vrrp也可以与ip-link进行配合，当上行链路断掉后使vrrp能够进行主备切换。在接口视图下配置ip-link：

vrrp vrid virtual-router-id ip-link link-id

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30s。配置VGMP管理组的抢占延迟时间命令如下：

hrp preempt [delay interval]

HRP两台USG心跳口的接口类型和编号必须相同，且心跳口不能为二层以太网接口。USG支持使用Eth-Trunk接口做为心跳口，既提高了可靠性，又增加了备份通道的带宽。主备USG的心跳口可以直接相连，也可以通过中间设备，如交换机或路由器连接。当心跳口通过中间设备相连时，需要配置remote参数来指定对端IP地址。

当两台设启用备HRP备份功能之后，会进行主备状态的协商，最后得到一个主用设备（显示时以HRP_M表示），一个备用设备（显示时以HRP_S表示）。两端首次协商出主备后，主用设备将向备用设备备份配置和连接状态等信息。

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。

USG工作于负载分担组网时，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USG的会话信息立即同步至另一台USG，保证内外部用户的业务不中断。

VRRP配置举例

- USG_A关于VRRP组1配置：

  [USG_A]interface GigabitEthernet 0/0/0

  [USG_A-GigabitEthernet 0/0/0]ip address 10.100.10.2 24

  [USG_A-GigabitEthernet 0/0/0]vrrp vrid 1 10.100.10.1 master

- USG_B关于VRRP组1的配置：

  [USG_B]interface GigabitEthernet 0/0/0

  [USG_B-GigabitEthernet0/0/0]ip address 10.100.10.3 24

  [USG_B-GigabitEthernet 0/0/0]vrrp vrid 1 virtual-ip 10.100.10.1 slave

HRP配置举例

- USG_A关于HRP配置：

  [USG_A]hrp enable

  [USG_A]hrp mirror session enable

  [USG_A]hrp interface Ethernet 2/0/0

  [USG_A]hrp interface GigabitEthernet 0/0/0

  [USG_A]hrp interface GigabitEthernet0/0/1

USG_B关于HRP的配置：

[USG_B]hrp enable

[USG_B]hrp mirror session enable

[USG_B]hrp interface Ethernet 2/0/0

[USG_B]hrp interface GigabitEthernet 0/0/0

[USG_B]hrp interface GigabitEthernet 0/0/1

查看VRRP状态

```
HRP_M<USG_A>display vrrp int G0/0/1
    16:13:46  2013/06/08
     GigabitEthernet0/0/1 | Virtual Router 2
       VRRP Group : Master
       state : Master
       Virtual IP : 202.38.10.1
       Virtual MAC : 0000-5e00-0102
       Primary IP : 202.38.10.2
       PriorityRun : 120
       PriorityConfig : 100
       MasterPriority : 120
       Preempt : YES   Delay Time : 0
       Advertisement Timer : 1
       Auth Type : NONE
       Check TTL : YES
```

查看HRP状态

- 查看处于Master状态防火墙的状态信息如下：

```
HRP_M<USG_A>dis hrp state
16:15:31  2013/06/08
The firewall's config state is: MASTER

Current state of virtual routers configured as master:
        GigabitEthernet0/0/1    vrid   2 : master
        GigabitEthernet0/0/0    vrid   1 : master
```


查看处于Slave状态防火墙的状态信息如下：

```
HRP_S[USG_B] display hrp state
  16:40:13  2010/11/29
  The firewall's config state is: SLAVE
  Current state of virtual routers configured as slave:
      GigabitEthernet0/0/0    vrid   1 : slave
      GigabitEthernet0/0/1    vrid   2 : slave
```

总结

- 双机热备技术原理
- 双机热备基本组网及配置

Thank you

www.huawei.com