

## H3C 交换机 VRRP 配置与管理

在网络的核心层，为了避免单点故障，提高网络的可用性，核心层的网络设备通常采用以下几种解决方案：设备集群、每个汇聚层设备与每个核心层设备之间的冗余连接，以及设备备份。在本书的第 1 章和第 3 章分别对 Cisco 交换机和 H3C 交换机的集群解决方案进行了详细介绍。冗余连接没有特别的技术，只需要将汇聚层的设备与每个核心层设备连接，然后启用对应的生成树协议，以确保没有网络环路的情况下，提供核心层设备的容错功能。设备备份解决方案就是通常见到的 HSRP（主机冗余路由器协议）和 VRRP（虚拟路由器冗余协议）方案。HSRP 是 Cisco 专用的协议，VRRP 则是通用协议。在本书的第 2 章已对 Cisco 交换机的 HSRP 协议方案的配置与管理方法做了全面介绍，本章要对 H3C 交换机的 VRRP 方案的配置与管理方法进行详细介绍。

在 VRRP 解决方案中，既可以实现在一个备份组中多个交换机的主备备份模式应用，还可以通过创建多个备份组实现备份组中的多个交换机的负载分担应用，以及在一个备份组中的多个交换机间实现负载均衡模式应用。



## 4.1 H3C 交换机 VRRP 基础

VRRP (Virtual Router Redundancy Protocol, 虚拟路由器冗余协议) 可以说是一种设备虚拟化的技术, 把多个路由器 (同样适用于支持路由功能的三层交换机) 虚拟成一个虚拟路由器。其中有一台路由器称之为主路由器 (Master), 其他的都称之为从路由器 (或者备份路由器, Backup)。当主路由器出现故障时, VRRP 可以指定其他从路由器中的一台接替原来主路由器的工作, 以实现不间断路由功能。它与我们在本书第 2 章中介绍的 Cisco 交换机中的 HSRP 协议的功能是类似的, 但实现机制有些区别, 具体将在本章后面介绍。

### 4.1.1 VRRP 简介

VRRP 是将可以承担网关功能的一组路由器加入到一个备份组中, 形成一台虚拟路由器, 由 VRRP 的选举机制决定哪台路由器承担转发任务。在具有多播或广播能力的局域网 (如以太网) 中, 借助 VRRP 能在某设备故障时提供高利用率的默认链路, 而无需修改动态路由协议、路由发现协议的配置信息。通过 VRRP 建立备份链路, 提高了网络的安全性, 能有效避免单一链路发生故障后网络中断问题出现。

在 VRRP 组网应用环境中, 局域网内的主机只需将虚拟路由器的 IP 地址配置为默认网关即可, 而不用配置某台物理路由器的 IP 地址作为网关。VRRP 是一种容错协议, 在提高可靠性的同时, 简化了主机的配置, 是为消除在静态默认路由环境下的默认路由器单点故障引起的网络失效而设计的主、备模式的协议, 使得在发生故障而进行设备功能切换时可以不影响内外数据通信, 不需要再修改内部网络的网络参数。目前, VRRP 协议的实现有 VRRPv2 和 VRRPv3 两个版本。其中, VRRPv2 基于 IPv4, VRRPv3 基于 IPv6。VRRPv2 和 VRRPv3 在功能实现上并没有区别, 只是应用的网络环境不同。本章仅介绍基于 IPv4 的 VRRPv2 应用配置与管理方法。

VRRP 协议将两台或多台路由器设备虚拟成一个设备, 对外提供虚拟路由器 IP (一个或多个) 地址, 而在路由器备份组内部, 如果某个路由器的实际 IP 地址与虚拟路由器 IP 地址一样, 且这台路由器工作正常, 则自动成为 Master 路由器 (主路由器), 或者是通过算法选举产生, 备份组中的其他路由器称之为 Backup 路由器 (备份路由器)。Master 路由器实现针对虚拟路由器 IP 的各种网络功能, 如 ARP 请求、ICMP 消息和数据的转发等; Backup 路由器不拥有该 IP, 除了接收 Master 路由器发送的 VRRP 通告信息外, 不执行对外的网络功能。仅当主机失效时, Backup 路由器接管原先 Master 路由器的网络功能。

VRRP 备份组具有以下特点:

- 虚拟路由器具有 IP 地址, 称为虚拟 IP 地址。局域网内的主机仅需要知道这个虚拟路由器的 IP 地址, 并将其设置为默认路由的下一跳地址。
- 网络内的主机通过这个虚拟路由器与外部网络进行通信。
- 备份组内的路由器根据优先级, 选举出 Master 路由器, 承担网关功能。其他路由器作为 Backup 路由器, 当 Master 路由器发生故障时, 取代 Master 路由器继续履行网关职责, 从而保证网络内的主机不间断地与外部网络进行通信。

如图 4-1 所示, Router A、Router B 和 Router C 组成一个虚拟路由器。此虚拟路由器有自己的 IP 地址。局域网内的主机将虚拟路由器设置为默认网关。Router A、Router B 和 Router C 中优先级最高的路由器作为 Master 路由器, 承担网关的功能。其余两台路由器作为 Backup 路由器。

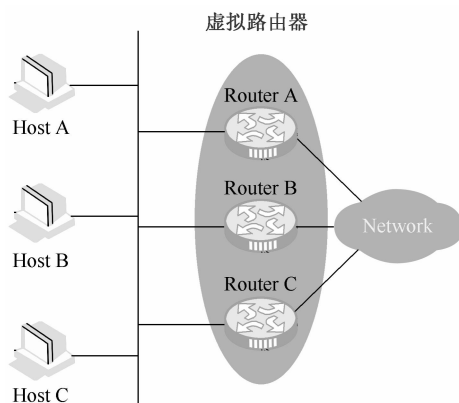


图 4-1 VRRP 组网示例

### 4.1.2 VRRP 的路由器标识、控制报文、认证和 Master 选举

在理解 VRRP 工作原理之前，先来了解一下 VRRP 的虚拟路由器标识、VRRP 控制报文、Master 路由器选举方法和 VRRP 备份组中路由器加入的认证方法。

#### 1. VRRP 虚拟路由器标识

在 VRRP 虚拟路由器有唯一的标识：VRID，范围为 0~255。该路由器对外表现为唯一的虚拟 MAC 地址，地址的格式为 00-00-5E-00-01-[VRID]。VRRP 协议使用多播数据来传输 VRRP 数据，Master 路由器转发数据时所使用的就是这个特殊的虚拟源 MAC 地址，负责源 MAC 地址为虚拟 MAC 地址的 ARP 请求应答，而不是自身网卡的 MAC 地址。这样无论备份组中担当转发任务的实际路由器如何切换，都可保证呈现终端设备的是唯一一致的 IP 和 MAC 地址，减少了网关路由器切换对终端设备的影响。

#### 2. VRRP 控制报文

VRRP 控制报文只有一种，那就是 VRRP 通告（Advertisement）。VRRP 备份组中的 Master 路由器会定时发送 VRRP 通告报文，通知备份组内的路由器自己工作正常。它使用 IP 多播数据包进行封装，使用的组播 IP 地址为 224.0.0.18（IP 协议号为 112；IP 包的 TTL 值必须为 255），发布范围只限于同一局域网内。这保证了 VRID 在不同网络中可以重复使用。用户可以通过设置 VRRP 定时器来调整 Master 路由器发送 VRRP 通告报文的时间间隔。如果 Backup 路由器在等待了三个间隔时间后仍然没有收到 Master 路由器发送的 VRRP 通告报文，则认为原来的 Master 路由器失效，把自己当成 Master 路由器，并对外发送 VRRP 通告报文，重新进行 Master 路由器的选举。

#### 3. Master 路由器选举

VRRP 根据优先级来确定备份组中每台路由器的角色（Master 路由器或 Backup 路由器）。优先级越高，则越有可能成为 Master 路由器。在 VRRP 路由器组中，按优先级选举 Master 路由器，VRRP 协议中优先级范围是 0~255 的正整数。优先级 0 一般用在 IP 地址所有者主动放弃 Master 路由器角色时使用，所以实际可配置的优先级范围为 1~254。若 VRRP 路由器的 IP 地址和虚拟路由器的 IP 地址相同，则称该路由器为 VRRP 组中的 IP 地址所有者，具有最高优先级（255），自动成为 Master 路由器，无需进行选举。

如果 VRRP 备份组中没有具备虚拟路由器 IP 地址的路由器，则要进行 Master 路由器选举。首先各路由器都宣告自己是 Master，发送 VRRP 通告信息，如果收到的其他机器发来的通告信息的优先级比自己高，自己将转换为 Backup 角色；如果相等的话，将比较两个路由器的实际 IP 地址，IP

值较大的优先级高，成为 Master 角色。另外，备份组中的路由器具有以下两种工作方式：

- 非抢占方式：如果备份组中的路由器工作在非抢占方式下，则只要 Master 路由器没有出现故障，Backup 路由器即使随后被配置了更高的优先级也不会成为 Master 路由器。
- 抢占方式：如果备份组中的路由器工作在抢占方式下，它一旦发现自己的优先级比当前的 Master 路由器的优先级高，就会对外发送 VRRP 通告报文，导致备份组内路由器重新选举 Master 路由器，并最终取代原有的 Master 路由器。相应地，原来的 Master 路由器将会变成 Backup 路由器。

为了避免备份组内的成员频繁进行主备状态转换，让 Backup 路由器有足够的时间搜集必要的信息（如路由信息），Backup 路由器接收到优先级低于本地优先级的通告报文后，不会立即抢占成为 Master 路由器，而是等待一定时间——抢占延迟时间后，才会对外发送 VRRP 通告报文取代原来的 Master 路由器。

#### 4. VRRP 认证

为了防止非法用户构造报文攻击备份组，VRRP 通过在 VRRP 报文中增加认证字的方式，验证接收到的 VRRP 报文。VRRP 提供了两种认证方式：

- **simple**：简单字符认证。发送 VRRP 报文的路由器将认证字填入到 VRRP 报文中，而收到 VRRP 报文的路由器会将收到的 VRRP 报文中的认证字和本地配置的认证字进行比较。如果认证字相同，则认为接收到的报文是真实、合法的 VRRP 报文；否则认为接收到的报文是一个非法报文。
- **md5**：MD5 认证。发送 VRRP 报文的路由器利用认证字和 MD5 算法对 VRRP 报文进行摘要运算，运算结果保存在 Authentication Header（认证头）中。收到 VRRP 报文的路由器会利用认证字和 MD5 算法进行同样的运算，并将运算结果与认证头的内容进行比较。如果相同，则认为接收到的报文是真实、合法的 VRRP 报文；否则认为接收到的报文是一个非法报文。

在一个安全的网络中，用户也可以不设置认证方式。

#### 4.1.3 VRRP 工作原理

通常，在如图 4-2 所示网络内的所有主机都设置同一个网关作为报文转发的下一跳，这个网关的 IP 地址又被称为默认路由的下一跳地址（如图中的 10.100.10.1）。图中 Switch 作为网络内主机的网关，对主机发往其他网段的报文进行转发，从而实现了主机与外部网络的通信。当 Switch 发生故障时，本网段内所有以 Switch 为默认网关的主机将无法与外部网络进行通信。VRRP 就是为解决上述问题而提出的，通过物理设备和逻辑设备的分离，很好地解决了上述问题。

图 4-3 所示就是图 4-2 所示网络的一个 VRRP 组网示例。在这个示例中，虚拟路由器拥有自己的虚拟 IP 地址 10.100.10.1（这个 IP 地址可以和备份组内的某个路由器的接口地址相同，注意，Cisco 中的 HSRP 就不能这样，虚拟路由器必须有单独的 IP 地址），备份组内的路由器也有自己的实际 IP 地址（如 Master 路由器的 IP 地址为 10.100.10.2，Backup 路由器的 IP 地址为 10.100.10.3）。局域网内的主机仅仅知道这个虚拟路由器的 IP 地址 10.100.10.1，而并不知道具体的 Master 路由器的 IP 地址 10.100.10.2 以及 Backup 路由器的 IP 地址 10.100.10.3，它们将自己的默认路由由下一跳地址设置为该虚拟路由器的 IP 地址 10.100.10.1。于是，网络内的主机就通过这个虚拟的路由器来与其他网络进行通信。如果备份组内的 Master 路由器出现了故障，Backup 路由器将会通过选举策略选出一个新的 Master 路由器，继续向网络内的主机提供路由服务。从而实现网络内的主机不间断地与外部网络进行通信。

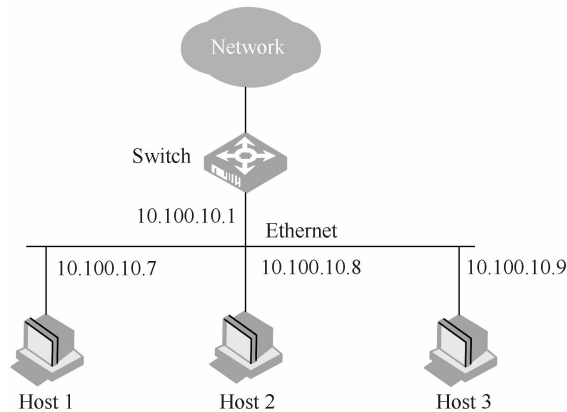


图 4-2 单一网关设备的局域网示例

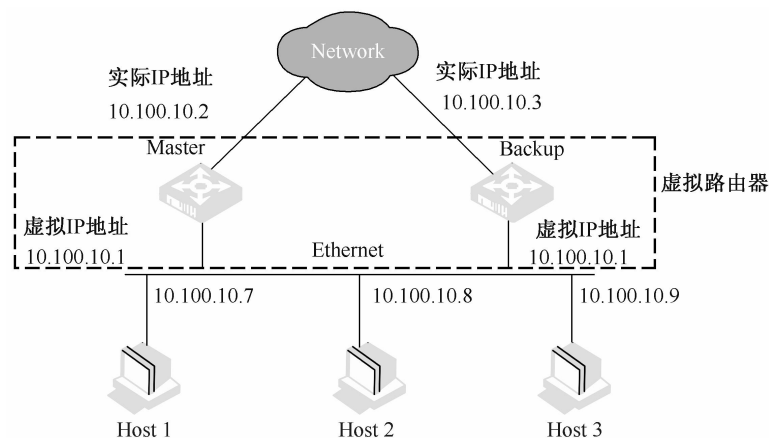


图 4-3 VRRP 网络示例

VRRP 的工作过程如下：

（1）路由器启用 VRRP 功能后，会根据优先级确定自己在备份组中的角色。优先级高的路由器成为 Master 路由器，优先级低的成为 Backup 路由器。Master 路由器定期发送 VRRP 通告报文，通知备份组内的其他路由器自己工作正常；Backup 路由器则启动定时器等待通告报文的到来。

（2）在抢占方式下，当 Backup 路由器收到 Master 路由器发送的 VRRP 通告报文后，会将自己的优先级与通告报文中的优先级进行比较。如果大于通告报文中的优先级，则成为 Master 路由器；否则将保持 Backup 状态。

（3）在非抢占方式下，只要 Master 路由器没有出现故障，备份组中的路由器始终保持 Master 或 Backup 状态，Backup 路由器即使随后被配置了更高的优先级也不会成为 Master 路由器。

（4）如果 Backup 路由器的定时器超时后仍未收到 Master 路由器发送来的 VRRP 通告报文，则认为 Master 路由器已经无法正常工作，此时 Backup 路由器会认为自己是 Master 路由器，并对外发送 VRRP 通告报文。

备份组内的路由器根据优先级选举出 Master 路由器，承担报文的转发功能。有关 Master 路由器的选举原理，参见 4.1.2 节。

#### 4.1.4 VRRP 的两种应用模式

本节仅以基于 IPv4 的 VRRP 为例介绍 VRRP 的两种主要应用模式：主备备份和负载分担。

## 1. 主备备份方式

VRRP 的主备备份方式表示转发任务仅由 Master 路由器承担，仅当 Master 路由器出现故障时，才会从其他 Backup 路由器选举出一个新的 Master 路由器接替工作。主备备份方式仅需要一个备份组，不同路由器在该备份组中拥有不同优先级，优先级最高的路由器将成为 Master 路由器，如图 4-4 所示。

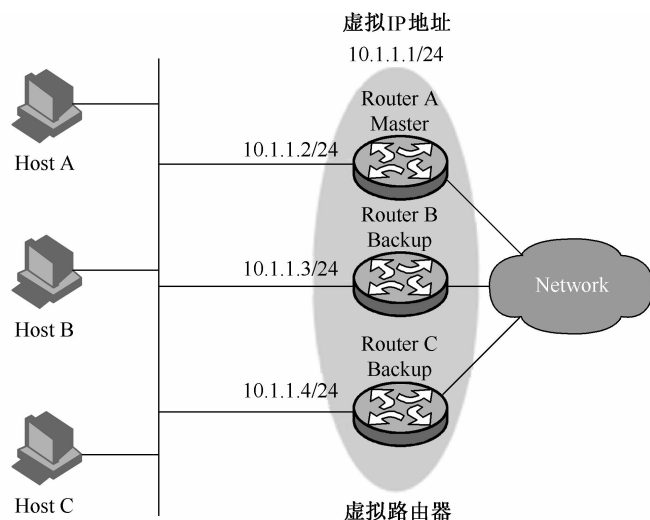


图 4-4 主备备份方式下的 VRRP 应用示例

在本示例中，初始情况下，Router A 为 Master 路由器并承担转发任务，Router B 和 Router C 是 Backup 路由器且都处于就绪监听状态。如果 Router A 发生故障，则备份组内处于 Backup 状态的 Router B 和 Router C 路由器将根据优先级选出一个新的 Master 路由器，这个新 Master 路由器继续向网络内的主机提供路由服务。

## 2. 负载分担方式

在前面介绍的主备备份方式中，我们可以看到，在同一时间实际上使用的只有一台路由器，对于这样价格昂贵的路由器或三层交换机设备来说，这显然代价有点过高。为了克服这一不足，同时又可以实现主备备份方式，通过创建多个备份组可实现多个路由器的负载分担。这就是此处所介绍的负载分担方式。

负载分担方式是指多台路由器同时承担业务，因此负载分担方式需要两个或者两个以上的备份组，每个备份组都包括一个 Master 路由器和若干个 Backup 路由器，各备份组的 Master 路由器各不相同。VRRP 的负载分担方式是在路由器的一个接口上创建多个备份组，并使该路由器在一个备份组中作为 Master 路由器，在其他的备份组中作为 Backup 路由器。同一台路由器可同时加入多个 VRRP 备份组，在不同备份组中有不同的优先级。

如在图 4-5 所示的负载分担方式 VRRP 应用中，有三个备份组存在：

- 备份组 1：对应虚拟路由器 1。Router A 作为 Master 路由器，Router B 和 Router C 作为 Backup 路由器。
- 备份组 2：对应虚拟路由器 2。Router B 作为 Master 路由器，Router A 和 Router C 作为 Backup 路由器。
- 备份组 3：对应虚拟路由器 3。Router C 作为 Master 路由器，Router A 和 Router B 作为 Backup 路由器。

为了实现业务流量在 Router A、Router B 和 Router C 之间进行负载分担，需要将局域网内的主

机的默认网关分别设置为虚拟路由器 1、2 和 3。在配置优先级时，需要确保三个备份组中各路由器的 VRRP 优先级形成一一对应。

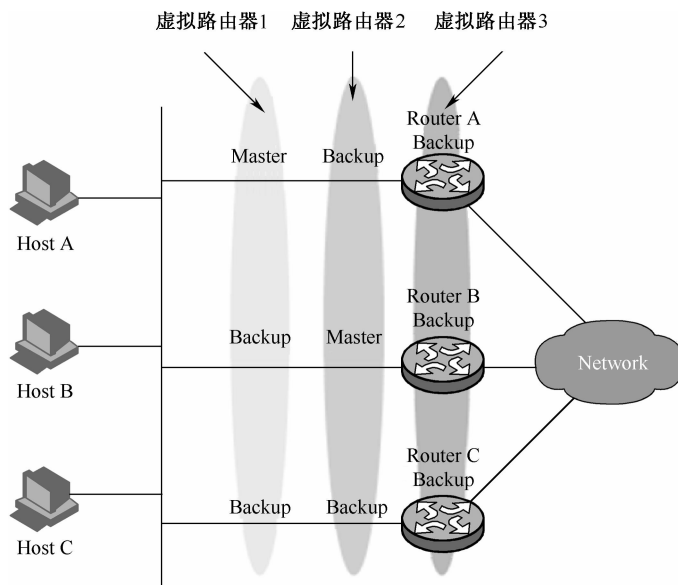


图 4-5 负载分担方式的 VRRP 应用示例

#### 4.1.5 VRRP 与 HSRP 的比较

一说起 VRRP，大家自然就想到了 Cisco 专用的 HSRP（Hot Standby Router Protocol，热备份路由器协议）。在功能上，VRRP 和 HSRP 非常相似，具体的比较如表 4-1 所示。

表 4-1 VRRP 与 HSRP 的比较

比较项目	VRRP	HSRP
是否通用	是	否（Cisco 专用）
虚拟路由器 IP 地址	可以是路由器接口的实际 IP 地址	不能是路由器接口的实际 IP 地址
路由器特征	一个备份组中只能有一个活动路由器和一个备份路由器	一个备份组中只能有一个主路由器和一个或多个备份路由器
认证机制	包括无认证、明文认证和 MD5 消息认证三种方式	明文认证（IOS 12.3 及以上系统软件版本中支持 MD5 消息认证方式）
状态类型	三种（Initialize、Master 和 Backup）	六种（Initial、Learn、Listen、Speak、Standby 和 Active）
报文类型	一种（VRRP 通告）	三种（Hello、Resign 和 Coup）
采用的通信协议	IP（协议号为 112）	UDP（端口号为 1985）
采用的组播 IP 地址	224.0.0.18	HSRPv1: 224.0.0.2, HSRPv2: 224.0.0.102
虚拟路由器的 MAC 地址	00-00-5e-00-01-VRID	00-00-0c-07-ac-xx（xx 为备份组 ID）

## 4.2 H3C 交换机的 VRRP 负载均衡模式

在一些 H3C 交换机中同时支持以下两种模式的 VRRP：

- 标准协议模式：基于 RFC 实现的 VRRPv2 和 VRRPv3。其中，VRRPv2 基于 IPv4，VRRPv3 基于 IPv6。VRRPv2 和 VRRPv3 在功能实现上并没有区别，只是应用的网络环境不同。前面各小节所介绍的都是针对标准协议模式进行的。下面将要介绍的 VRRP 负载均衡模式以 VRRP 标准协议模式为基础，VRRP 标准协议模式中的工作机制（如 Master 路

由器的选举、抢占、监视功能等), VRRP 负载均衡模式均支持。

- 负载均衡模式: 它是在标准协议模式的基础上进行了扩展, 实现了负载均衡功能。支持负载均衡模式的 H3C 交换机主要包括 S58、S9500E 系列, 但 S5600、S7500、7500E 系列不支持。但要注意的是, 这里的“负载分担”与“负载均衡”是不同意义的, 具体将在本节后面介绍。

在 VRRP 标准协议模式中, 只有 Master 路由器可以转发报文, Backup 路由器处于监听状态, 无法转发报文。虽然创建多个备份组可以实现多个路由器之间的负载分担, 但是局域网内的主机需要设置不同的网关, 增加了配置的复杂性。

VRRP 负载均衡模式在 VRRP 提供的虚拟网关冗余备份功能基础上, 增加了负载均衡功能。其实现原理为: 将一个虚拟 IP 地址与多个虚拟 MAC 地址对应, VRRP 备份组中的每个路由器都对应一个虚拟 MAC 地址, 这样就可以使用不同的虚拟 MAC 地址应答主机的 ARP (IPv4 网络中) /ND (IPv6 网络中) 请求, 从而使得不同主机的流量发送到不同的路由器, 备份组中的每个路由器都能转发流量。

在 VRRP 负载均衡模式中, 只需创建一个备份组, 就可以实现备份组中多个路由器之间的负载分担, 避免了 VRRP 备份组中 Backup 路由器始终处于空闲状态、网络资源利用率不高的问题。但在 IRF 堆叠模式下使用 VRRP 负载均衡功能时, 须配置 IRF 的桥 MAC 地址为永久保留 (默认情况下, IRF 的桥 MAC 地址为永久保留)。

#### 4.2.1 负载均衡模式下的虚拟 MAC 地址分配

在 VRRP 负载均衡模式中, Master 路由器负责为备份组中的路由器分配虚拟 MAC 地址, 并为来自不同主机的 ARP/ND 请求应答不同的虚拟 MAC 地址, 从而实现流量在多个路由器之间分担。备份组中的 Backup 路由器不会应答主机的 ARP/ND 请求。

以图 4-6 所示的 IPv4 网络为例, VRRP 负载均衡模式的具体工作过程为:

(1) Master 路由器为备份组中的路由器 (包括 Master 路由器自身) 分配虚拟 MAC 地址。在虚拟 IP 地址为 10.1.1.1/24 的备份组中, Router A 作为 Master 路由器, Router B 作为 Backup 路由器。Router A 为自己分配的虚拟 MAC 地址为 000f-e2ff-0011, 为 Router B 分配的虚拟 MAC 地址为 000f-e2ff-0012。

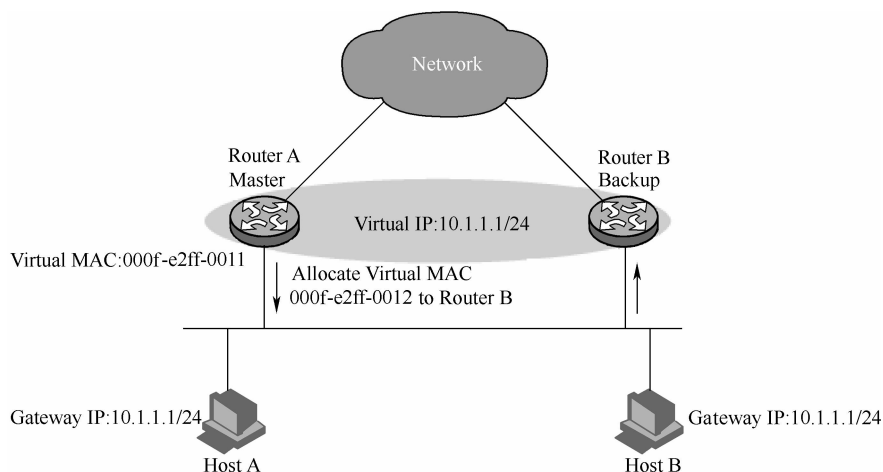


图 4-6 负载均衡模式下的 VRRP 组网示例

(2) Master 路由器接收到主机发送的目标 IP 地址为虚拟 IP 地址的 ARP 请求后, 根据负载均衡算法使用不同的虚拟 MAC 地址应答主机的 ARP 请求。如图 4-7 所示, Host A 发送 ARP 请求获



取网关 10.1.1.1 对应的 MAC 地址时，Master 路由器（即 Router A）使用 Router A 的虚拟 MAC 地址应答该请求；Host B 发送 ARP 请求获取网关 10.1.1.1 对应的 MAC 地址时，Master 路由器使用 Router B 的虚拟 MAC 地址应答该请求。

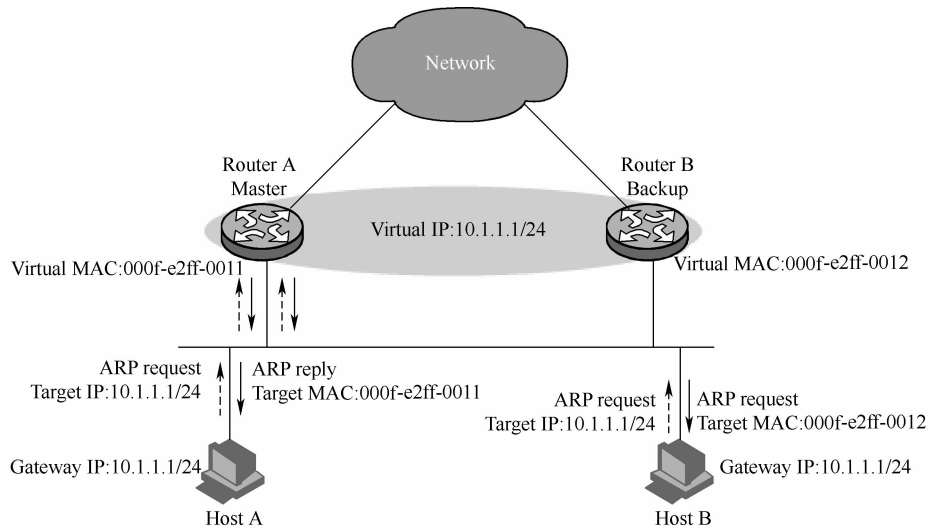


图 4-7 负载均衡模式下 Master 路由器应答 ARP 请求的示例

（3）Master 路由器通过使用不同的虚拟 MAC 地址应答主机的 ARP 请求，可以实现不同主机的流量发送给不同的路由器。如图 4-8 所示，Host A 认为网关的 MAC 地址为 Router A 的虚拟 MAC 地址，从而保证 Host A 的流量通过 Router A 转发；Host B 认为网关的 MAC 地址为 Router B 的虚拟 MAC 地址，从而保证 Host B 的流量通过 Router B 转发。

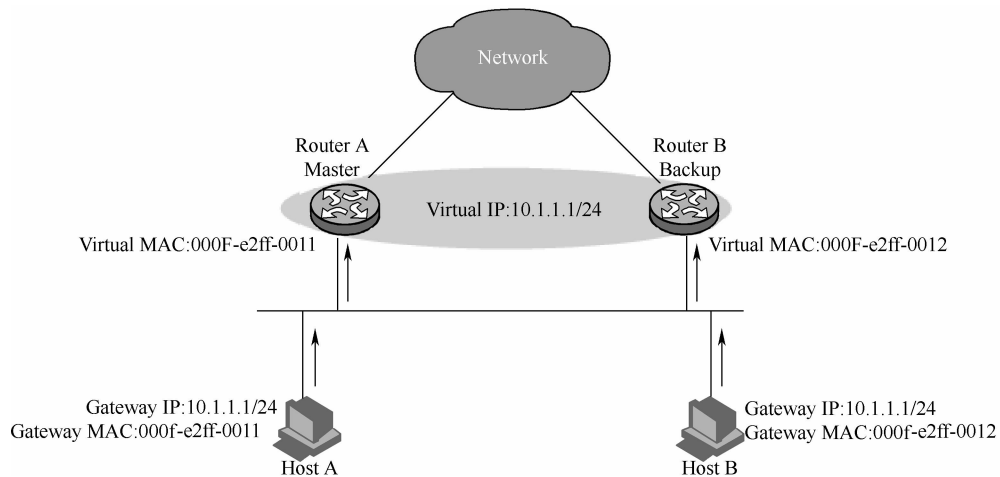


图 4-8 负载均衡模式下主机通过不同路由器转发流量的示例

#### 4.2.2 负载均衡模式下的虚拟转发器

通过前面介绍的 Master 路由器虚拟 MAC 地址的分配功能实现了不同主机将流量发送给备份组中不同的路由器。但为了使备份组中的路由器能够转发主机发送的流量，还需要在路由器上创建虚拟转发器。每个虚拟转发器都对应备份组的一个虚拟 MAC 地址，负责转发目的 MAC 地址为该虚拟 MAC 地址的流量。

## 1. 虚拟转发器的创建

虚拟转发器的创建过程如下：

(1) 备份组中的路由器获取到 Master 路由器为其分配的虚拟 MAC 地址后，创建该 MAC 地址对应的虚拟转发器，该路由器称为此虚拟 MAC 地址对应的虚拟转发器的 VF Owner (Virtual Forwarder Owner，虚拟转发器拥有者)。

(2) 该路由器将虚拟转发器的信息通告给备份组内其他的路由器。

(3) 备份组内的其他路由器接收到该路由器发送的虚拟转发器信息后，会在本地创建该虚拟 MAC 地址对应的虚拟转发器。

由此可见，备份组中的路由器上不仅需要创建 Master 路由器为其分配的虚拟 MAC 地址对应的虚拟转发器，还需要创建其他路由器通告的虚拟 MAC 地址对应的虚拟转发器。

## 2. 虚拟转发器的权重和优先级

虚拟转发器的权重标识了路由器的转发能力。权重值越高，路由器的转发能力越强。当权重低于一定的值——失效下限时，路由器无法再为主机转发流量。

虚拟转发器的优先级用来决定虚拟转发器的状态：不同路由器上同一个虚拟 MAC 地址对应的虚拟转发器中，优先级最高的虚拟转发器处于 Active 状态，称为 AVF (Active Virtual Forwarder)，负责转发流量；其他虚拟转发器处于 Listening 状态，称为 LVF (Listening Virtual Forwarder)，监听 AVF 的状态。虚拟转发器的优先级取值范围为 0~255，其中，255 保留给 VF Owner 使用。如果 VF Owner 的权重高于或等于失效下限，则 VF Owner 的优先级为最高值 255。

设备根据虚拟转发器的权重计算虚拟转发器的优先级的规则如下：

- 如果权重高于或等于失效下限，且设备为 VF Owner，则虚拟转发器的优先级为最高值 255。
- 如果权重高于或等于失效下限，且设备不是 VF Owner，则虚拟转发器的优先级为权重/（本地 AVF 的数目+1）。
- 如果权重低于失效下限，则虚拟转发器的优先级为 0。

## 3. 虚拟转发器备份

备份组中不同路由器上同一个虚拟 MAC 地址对应的多个虚拟转发器之间形成备份关系。在如图 4-9 所示的示例中，说明了备份组中每个路由器上的虚拟转发器信息及其备份关系。

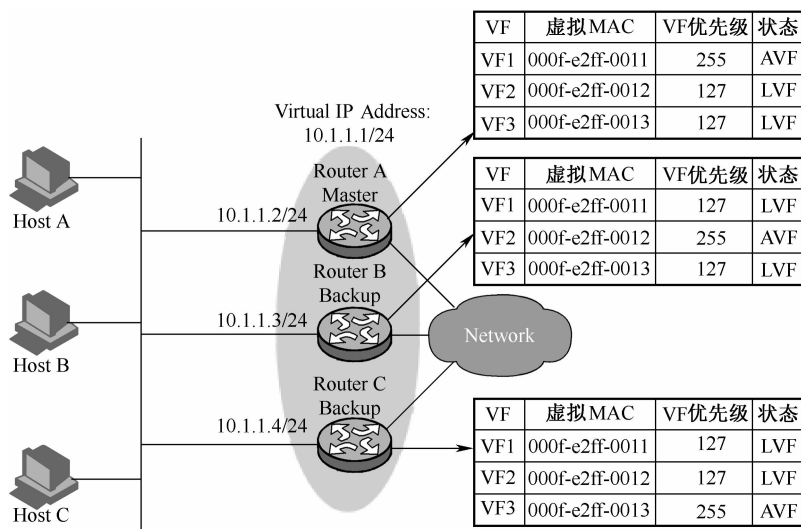


图 4-9 负载均衡模式下的虚拟转发器备份

在本示例中，Master 路由器 Router A 为自己、Router B、Router C 分配的虚拟 MAC 地址分别为 000f-e2ff-0011、000f-e2ff-0012 和 000f-e2ff-0013。虚拟 MAC 地址对应的虚拟转发器分别为 VF 1、VF 2 和 VF 3。在 Router A、Router B 和 Router C 上都创建了这三个虚拟转发器，并形成备份关系。例如，Router A、Router B 和 Router C 上的 VF 1 互相备份：

- Router A 为 VF 1 的 VF Owner，Router A 上 VF 1 的虚拟转发器优先级为最高值 255。因此，Router A 上的 VF 1 作为 AVF，负责转发目的 MAC 地址为虚拟 MAC 地址 000f-e2ff-0011 的流量。
- Router B 和 Router C 上 VF 1 的虚拟转发器优先级为：权重 255/（本地 AVF 数目+1）=127，低于 Router A 上 VF 1 的优先级。因此，Router B 和 Router C 上的 VF 1 作为 LVF，监视 Router A 上 VF 1 的状态。
- 在 Router A 上的 VF 1 出现故障时，将从 Router B 和 Router C 上的 VF 1 中选举出虚拟转发器优先级最高的 LVF 作为 AVF，负责转发目的 MAC 地址为虚拟 MAC 地址 000f-e2ff-0011 的流量。

**【说明】**虚拟转发器始终工作在抢占模式。对于不同路由器上互相备份的 LVF 和 AVF，如果 LVF 接收到 AVF 发送的虚拟转发器信息中虚拟转发器优先级低于本地虚拟转发器优先级，则 LVF 将会抢占成为 AVF。

#### 4. 虚拟转发器的定时器

虚拟转发器的 AVF 出现故障后，接替其工作的新的 AVF 将为该 VF 创建 Redirect Timer 和 Timeout Timer 两个定时器。

- Redirect Timer：VF 重定向定时器。该定时器超时前，Master 路由器还会采用该 VF 对应的虚拟 MAC 地址应答主机的 ARP/ND 请求；该定时器超时后，Master 路由器不再采用该 VF 对应的虚拟 MAC 地址应答主机的 ARP/ND 请求。如果 VF Owner 在 Redirect Timer 超时前恢复，则 VF Owner 可以迅速参与流量的负载分担。
- Timeout Timer：VF 生存定时器，即 AVF 接替 VF Owner 工作的期限。该定时器超时前，备份组中的路由器上都保留该 VF，AVF 负责转发目的 MAC 地址为该 VF 对应虚拟 MAC 地址的报文；该定时器超时后，备份组中的路由器上都删除该 VF，不再转发目的 MAC 地址为该 VF 对应虚拟 MAC 地址的报文。

#### 5. 虚拟转发器的监视功能

AVF 负责转发目的 MAC 地址为虚拟转发器 MAC 地址的流量，当 AVF 连接的上行链路出现故障时，如果不能及时通知 LVF 接替其工作，局域网中以此虚拟转发器 MAC 地址为网关 MAC 地址的主机将无法访问外部网络。

虚拟转发器的监视功能可以解决上述问题。利用 NQA（Network Quality Analyzer，网络质量分析）、BFD（Bidirectional Forwarding Detection，双向转发检测）等监测 AVF 连接的上行链路的状态，并通过 Track 功能在虚拟转发器和 NQA/BFD 之间建立联动。当上行链路出现故障，Track 项的状态变为 Negative，虚拟转发器的权重将降低指定的数额，以便虚拟转发器优先级更高的路由器抢占成为 AVF，接替其转发流量。

虚拟转发器监视功能还可以用来在 LVF 上通过 Track 监视 AVF 的状态，当 AVF 出现故障时，工作在虚拟转发器快速切换模式的 LVF 能够迅速成为 AVF，以保证通信不会中断。

### 4.2.3 VRRP 负载均衡模式的报文

VRRP 标准协议模式中只定义了一种报文——VRRP 通告报文，且只有 Master 路由器周期性发

送该报文，Backup 路由器不会发送 VRRP 通告报文。

为了实现负载均衡，VRRP 负载均衡模式中定义了四种报文：

- **Advertisement 报文：**不仅用于通告本路由器上备份组的状态，还用于通告本路由器上处于 Active 状态的虚拟转发器信息。Master 路由器和 Backup 路由器均周期性发送该报文。
- **Request 报文：**处于 Backup 状态的路由器如果不是 VF Owner，则发送 Request 报文，请求 Master 路由器为其分配虚拟 MAC 地址。
- **Reply 报文：**Master 路由器接收到 Request 报文后，将通过 Reply 报文为 Backup 路由器分配虚拟 MAC 地址。收到 Reply 报文后，Backup 路由器会创建虚拟 MAC 地址对应的虚拟转发器，该路由器称为此虚拟转发器的拥有者。
- **Release 报文：**VF Owner 的失效时间达到一定值后，接替其工作的路由器将发送 Release 报文，通知备份组中的路由器删除 VF Owner 对应的虚拟转发器。

上述报文的格式与 VRRP 标准协议模式中定义的报文格式类似，只是在其基础上增加了选项字段，用来携带实现负载均衡所需要的信息。

## 4.3 H3C 交换机 VRRP 配置

在支持标准协议 VRRP 模式的 H3C 交换机中配置 VRRP 功能，主要包括创建备份组、添加虚拟路由器 IP 地址、启用虚拟路由器 IP 地址、配置备份组优先级等基本功能，以及包括配置备份组成员交换机的抢占方式、VRRP 认证方式、VRRP 定时器和 VRRP 监视功能等高级配置。在支持负载均衡 VRRP 模式的 H3C 交换机中，首先还要配置 VRRP 的工作模式。下面分别予以介绍。

### 4.3.1 VRRP 工作模式配置

本节仅适用于同时支持标准协议 VRRP 模式和负载均衡 VRRP 模式的 H3C 交换机，如 58 系列和 S9500E 系列交换机。配置 VRRP 的工作模式后，路由器上所有的 VRRP 备份组都工作在该模式。VRRP 工作模式的配置步骤如表 4-2 所示。

表 4-2 VRRP 工作模式的配置步骤

步骤	命令	说明	
1	<b>system-view</b> 例如：<Sysname> <b>system-view</b>	进入系统视图	
2	<b>undo vrrp mode</b> 例如：[Sysname] <b>undo vrrp mode</b>	配置 VRRP 工作在标准协议模式	(二者选择其一)，默认情况下，VRRP 工作在标准协议模式
	<b>vrrp mode load-balance</b> 例如：[Sysname] <b>vrrp mode load-balance</b>	配置 VRRP 工作在负载均衡模式	

**【注意】**通过本命令配置 VRRP 的工作模式后，基于 IPv4 和 IPv6 的备份组均工作在指定的模式。VRRP 工作在负载均衡模式时，要求备份组虚拟 IP 地址和 VRRP 备份组中交换机物理端口的 IP 地址不能相同，且虚拟 IP 地址需要与虚拟 MAC 地址对应，也不能采用 VRRP 备份组中交换机物理端口上的实际 MAC 地址。否则，VRRP 负载均衡功能将无法正常工作。

创建 VRRP 备份组后，仍然可以修改 VRRP 的工作模式。修改 VRRP 的工作模式后，路由器上所有的备份组都工作在该模式。

以下示例是配置 VRRP 工作在负载均衡模式。

```
<Sysname> system-view
[Sysname] vrrp mode load-balance
```

### 4.3.2 H3C 交换机 VRRP 基本功能配置

在标准协议模式下配置 H3C 交换机的 VRRP 基本功能，涉及到一个重要的知识点，那就是 VRRP 备份控制 VLAN。也就是 VRRP 报文终结的 VLAN。VLAN 终结是指某个端口在接收到 VLAN 报文后去掉报文中的 VLAN 标记，再进行三层转发或其他处理。VLAN 终结分为：

- 明确终结：终结特定的 VLAN。某端口在接收到特定 VLAN 的报文后去掉该报文中的 VLAN 标记。
- 模糊终结：终结某个范围的 VLAN。某端口在接收到 VLAN 报文后，如果该报文属于指定的 VLAN 范围，则去掉该报文中的 VLAN 标记。

默认情况下，三层以太网端口或 VLAN 接口上配置 VLAN 模糊终结后，该接口不支持发送广播或组播报文。只有启用了 VLAN 终结支持广播/组播报文功能，该接口才可以正常发送广播/组播报文，且广播/组播报文需要在所有终结的 VLAN 内发送。

在如图 4-10 所示的网络中，在 VRRP 备份组中三个路由器的三层以太网接口上配置了模糊 VLAN 终结，要求终结 VLAN 10 和 VLAN 20。为了保证 Master 路由器可以周期性地向 Backup 路由器发送 VRRP 通告报文（组播报文），需要在三层以太网接口上启用 VLAN 终结支持广播/组播功能。启用该功能后，VRRP 通告报文将发送给所有终结的 VLAN。但三层以太网接口上模糊终结的 VLAN 较多时，会导致发送的 VRRP 通告报文数量过多，严重影响设备的性能。为了解决这个问题，就诞生了 VRRP 控制 VLAN 功能。只需关闭 VLAN 终结支持广播/组播功能，然后配置 VRRP 控制 VLAN，就可以使得 Master 路由器仅在控制 VLAN 内发送 VRRP 通告报文，避免发送过多的 VRRP 通告报文。

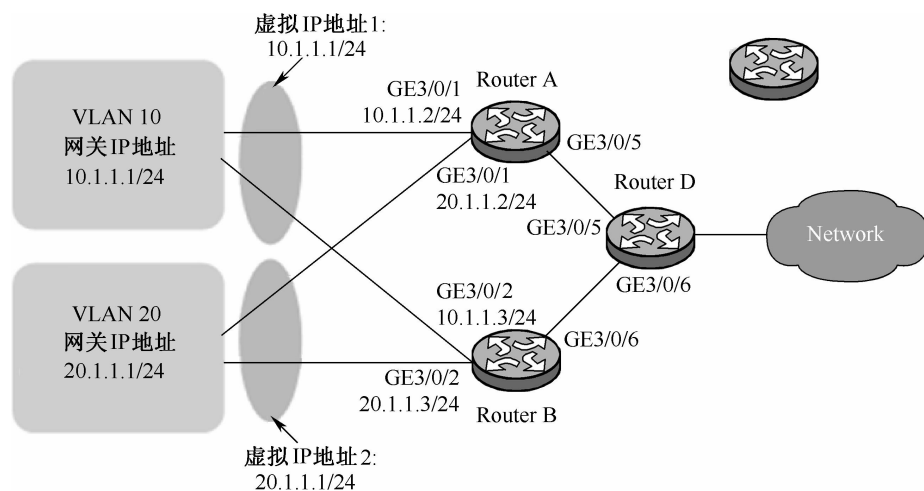


图 4-10 VRRP 控制 VLAN 示意图

VRRP 控制 VLAN 分为两种：

- 只指定一层 VLAN 标记：配置了模糊 Dot1q 终结的子接口上，需要指定此类控制 VLAN。
- 指定两层 VLAN 标记：配置了模糊 QinQ 终结的子接口上，需要指定此类控制 QinQ VLAN。

在支持 VRRP 功能的 H3C 以太网交换机上所需进行的基本功能配置如表 4-3 所示。但要注意，不要在远程镜像 VLAN（Remote-probe VLAN）的三层接口上，进行 VRRP 备份组相关特性的配置，否则可能影响报文镜像效果。

表 4-3 VRRP 基本功能的配置步骤

步骤	命令	说明
1	<b>system-view</b> 例如: <Sysname> system-view	进入系统视图
2	<b>vrrp ping-enable</b> 例如: [Sysname] vrrp ping-enable	(可选) 启用备份组虚拟路由器对 <b>ping</b> 操作的响应功能。默认情况下, 备份组虚拟路由器的 IP 地址不能被 <b>ping</b> 通, 可用 <b>undo vrrp ping-enable</b> 命令恢复为默认情况。如果不想让虚拟 IP 地址可以被 <b>ping</b> 通, 则本步可不执行。 要注意的是, 本命令需要在配置备份组之前执行。在设备上创建了备份组之后, 将不允许执行本命令
3	<b>vrrp method { real-mac   virtual-mac }</b> 例如: [Sysname] vrrp method virtual-mac	(可选) 配置备份组虚拟路由器的 IP 地址和 MAC 地址的对应关系, 可使用路由接口的实际 MAC 地址对应备份组虚拟路由器的 IP 地址, 也可使用虚拟 MAC 地址对应备份组虚拟路由器的 IP 地址。 <ul style="list-style-type: none"> <li><b>real-mac</b>: 二选一选项, 用来指定在 VRRP 进行备份的时候采用交换机路由接口的实际 MAC 地址和备份组的虚拟路由器的 IP 地址对应</li> <li><b>virtual-mac</b>: 二选一选项, 用来指定在 VRRP 进行备份的时候采用虚拟 MAC 地址和备份组的虚拟 IP 地址对应</li> </ul> 默认情况下, 交换机采用备份组的虚拟 MAC 地址和备份组虚拟路由器的 IP 地址对应, 可用 <b>undo vrrp method</b> 命令恢复虚拟路由器 IP 地址与虚拟路由器 MAC 地址的默认对应关系。 <b>【注意】</b> 备份组的 MAC 地址和 IP 地址的对应形式需要在配置备份组之前就设定。如果在交换机上已经创建了备份组, 系统将不允许设置备份组的 MAC 地址和 IP 地址的对应关系。 本配置在负载均衡模式下不会生效。无论如何配置虚拟 IP 地址对应的 MAC 地址的类型, 在负载均衡模式下, 始终是虚拟 IP 地址与虚拟 MAC 地址对应
4	<b>vlan vlan-id</b> 例如: [Sysname] vlan 2	创建备份组对应的控制 VLAN, <i>vlan-id</i> 为 VLAN 接口的 VLAN ID。但要注意, VRRP 工作在负载均衡模式时, 不能配置 VRRP 控制 VLAN
5	<b>quit</b> 例如: [Sysname] quit	退回系统视图
6	<b>interface Vlan-interface vlan-id</b> 例如: [Sysname] interface Vlan-interface 2	进入 VLAN 接口视图
7	<b>vrrp dot1q vid vlan-id</b>	配置了模糊 Dot1q 终结的子接口上, 指定 VRRP 控制 VLAN
	<b>vrrp dot1q vid vlan-id secondary-dot1q secondary-vlan-id</b>	配置了模糊 QinQ 终结的子接口上, 指定 VRRP 控制 VLAN
8	<b>vrrp vrid virtual-router-id virtual-ip virtual-address</b> 例如: [Sysname-Vlan-interface2] vrrp vrid 10 virtual-ip 10.10.0.1	在以上 VLAN 接口上创建备份组, 或为已创建的备份组配置虚拟 IP 地址, 一个备份组最多可以配置 16 个虚拟 IP 地址 <ul style="list-style-type: none"> <li><b>virtual-router-id</b>: 用来指定要创建或者要进入的 VRRP 备份组的组号, 取值范围为 1~255 的正整数</li> <li><b>virtual-address</b>: 用来为指定的备份组虚拟路由器配置虚拟 IP 地址</li> </ul> 可用 <b>undo vrrp vrid virtual-router-id [ virtual-ip virtual-address ]</b> 命令删除一个已经存在的备份组, 或者删除备份组中的某个地址。如果备份组中的虚拟路由器的 IP 地址被删除完, 则系统会自动将这个备份组删除。 <b>【注意】</b> 虚拟路由器的 IP 地址必须和备份组中成员交换机使用的真实 IP 地址在同一网段, 如果配置了不在同网段的虚拟路由器的 IP 地址, 该备份组会处于 VRRP 尚未配置的初始状态, 此状态下, VRRP 不起作用。 当 VRRP 工作在负载均衡模式时, 虚拟 IP 地址不能与 VRRP 备份组中路由器的接口 IP 地址相同, 即负载均衡模式的 VRRP 备份组中不能存在 IP 地址所有者 (二者可选其一) 仅适用于 S9500E 系列交换机。默认情况下, 没有指定 VRRP 控制 VLAN, 即 Master 路由器在所有模糊终结的 VLAN 内发送 VRRP 通告报文
9	<b>vrrp vrid virtual-router-id priority priority</b> 例如: vrrp vrid 10 priority 100	(可选) 设置当前交换机在备份组中的优先级。优先级决定交换机在备份组中的地位, 优先级越高, 越有可能成为 Master 路由器。优先级 0 为系统保留给特殊用途来使用, 255 则是系统保留给 IP 地址所有者, 当交换机为 IP 地址所有者时, 其优先级始终为 255, 不允许对其进行优先级的配置 <ul style="list-style-type: none"> <li><b>virtual-router-id</b>: 用来指定当前交换机配置的优先级所在的 VRRP 备份组号, 取值范围为 1~255</li> <li><b>priority</b>: 设置当前交换机在指定的备份组中的优先级, 取值范围为 1~254</li> </ul> 默认情况下, 备份组的优先级为 100, 可用 <b>undo vrrp vrid priority</b> 命令恢复交换机在备份组的优先级为默认值

【示例 1】启用备份组的虚拟路由器 IP 地址的被 ping 功能。

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] vrrp ping-enable
```

【示例 2】指定当前交换机的备份组虚拟路由器 IP 地址和交换机的路由接口实际 MAC 地址对应，也就是使用交换机的路由接口 MAC 地址。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] vrrp method real-mac
```

【示例 3】在 VLAN2 接口上创建一个备份组 1，并配置虚拟 IP 地址为 10.10.0.1。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] interface Vlan-interface 2
[H3C-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.0.1
```

【示例 4】在 VLAN2 接口上删除虚拟路由器的 IP 地址 10.10.10.10。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] interface Vlan-interface 2
[H3C-Vlan-interface2] undo vrrp vrid 1 virtual-ip 10.10.10.10
```

【示例 5】在 VLAN2 接口上删除备份组 1。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] interface Vlan-interface 2
[H3C-Vlan-interface2] undo vrrp vrid 1
```

【示例 6】在 VLAN2 接口上设置当前交换机在备份组 1 中的优先级为 100。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] interface Vlan-interface 2
[H3C-Vlan-interface2] vrrp vrid 1 priority 100
```

### 4.3.3 H3C 交换机 VRRP 高级功能配置

在支持 VRRP 功能的 H3C 以太网交换机上所需进行的高级配置任务如下（均为可选配置）：

- 备份组中成员交换机抢占方式和抢占延时时间配置
- 备份组中成员交换机的 VRRP 认证方式以及认证字配置
- VRRP 定时器配置
- VRRP 监视功能配置

这些高级功能的配置均需要在进行上节介绍的一些必选基本功能配置后进行，特别是需要先为备份组配置虚拟路由器 IP 地址。

#### 1. 备份组中成员交换机抢占方式和抢占延时时间配置

在本章前面已介绍到，H3C 以太网交换机的 VRRP 有抢占方式和非抢占方式之分。如果需要优先级高的交换机能够主动抢占成为 Master，就需要将这台交换机设置为抢占方式；如果需要将抢占的时间延长，还可以设置延迟时间。在非抢占方式的备份组中，一旦某台交换机成为 Master，只要它没有出现故障，即使在备份组中的其他交换机的优先级被配置成高于它，也不会成为 Master。相反，如果为抢占方式，则一旦备份组内的 Backup 交换机发现自己的优先级比当前的 Master 交换机的优先级高，就会抢占 Master 角色，成为 Master 交换机，这样原来的 Master 交换机将会变成 Backup 角色。

在设置抢占的同时，还可以设置延迟时间，使得优先级较高的 Backup 交换机延迟一段时间再成为 Master 交换机。其目的在于：在性能不够稳定的网络中，Master 交换机正常工作时，也可能由于网络堵塞导致 Backup 交换机收不到原来 Master 交换机发来的 VRRP 通告报文，使得备份组内

的成员频繁地进行主备状态转换。设置延迟时间后, Backup 交换机没有按时收到来自 Master 交换机的 VRRP 通告报文时, 会再等待一段时间, 只有在这段等待时间过后 Backup 交换机还没有收到来自原 Master 交换机的 VRRP 通告报文, Backup 交换机才会转换为 Master 角色。

备份组中成员交换机抢占方式和抢占延时时间的配置方法是在配置了虚拟 IP 地址的 VLAN (备份组中的交换机接口属于这个 VLAN) 接口视图下使用 **vrp vrid virtual-router-id preempt-mode [ timer delay delay-value ]** 命令。参数 *virtual-router-id*: 用来设置要配置抢占方式的 VRRP 备份组号, 取值范围为 1~255 的正整数, 参数 *delay-value*: 用来设置 Backup 交换机抢占 Master 角色前所需等待的时间, 取值范围为 0~255 秒。

默认情况下, 备份组内的交换机被设置为抢占方式, 延迟时间为 0 秒。可用 **undo vrrp vrid preempt-mode** 命令取消备份组的抢占方式。

【示例 1】设置备份组 1 为抢占方式。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] interface Vlan-interface 2
[H3C-Vlan-interface2] vrrp vrid 1 preempt-mode
```

【示例 2】设置备份组 1 的 Backup 交换机抢占 Master 角色时的等待时间为 5 秒。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] interface Vlan-interface 2
[H3C-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

【示例 3】取消备份组 1 中交换机的抢占方式设置。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] interface Vlan-interface 2
[H3C-Vlan-interface2] undo vrrp vrid 1 preempt-mode
```

## 2. 备份组中成员交换机的 VRRP 认证方式以及认证字配置

在本章前面 4.1.3 节中介绍了 VRRP 支持三种认证方式: 无认证、明文认证和 MD5 消息摘要认证, 默认方式为无认证, 也就是要加入到 VRRP 备份组的交换机无需认证就可以加入到 VRRP 备份组中。VRRP 认证方式和认证字 (也就是认证密码) 的配置方法是直接在虚拟路由器所在 VLAN 的 VLAN 接口下使用 **vrp vrid virtual-router-id authentication-mode authentication-type authentication-key** 命令。命令中的三个参数说明如下:

- *virtual-router-id*: 用于指定要配置认证方式的 VRRP 备份组编号, 取值范围为 1~255。
- *authentication-type*: 用于指定以上备份组的认证方式, 主要有以下两种: 可选值有两种  
① **simple**: 表示进行简单字符认证; ② **md5**: 表示用 MD5 算法进行认证。
- *authentication-key*: 用于指定所选认证方式的认证字。当采用 **simple** 认证方式时, 为明文验证字, 长度为 1~8 个字符; 当采用 **md5** 认证方式时, 为明文验证字或者 MD5 密文验证字。如果以明文形式输入, 长度为 1~8 个字符, 如: 1234567; 如果以密文形式输入, 长度必须为 24, 并且必须是密文形式 (只能通过从其他加密的密文复制得到, 不能直接输入)。

【注意】认证字区分大小写, 但在进行配置前, 需要先在接口上创建备份组并配置虚拟 IP 地址。而且, 这里所配置的 VRRP 认证适用于同一个接口上的所有 VRRP 备份组, 也就是在同一个接口上只需进行一次 VRRP 认证即可, 无论它加入了多少个备份组, 该接口上的所有备份组都使用相同的 VRRP 认证和认证字。另外, 加入同一备份组的所有成员也要设置相同的认证方式和认证字。

下面的示例是设置 VRRP 备份组 1 的认证方式为 **simple** 方式, 认证字为 123456。注意, 这是在对的备份组所在 VLAN 的 VLAN 接口中配置的, 所以需要先确保该 VLAN 接口上已配置虚拟 IP 地址, 并且所指定的 VRRP 备份组已创建。



```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.0.1
[Sysname-Vlan-interface2] vrrp vrid 1 authentication-mode simple 123456
```

### 3. VRRP 定时器配置

在 VRRP 中因为只有一种报文，那就是 VRRP 通告报文，向组内的成员交换机通知自己工作正常，所以在 VRRP 的配置中仅需要配置 Master 交换机 VRRP 通告报文发送的定时器（也就是报文发送的时间间隔）。如果 Backup 交换机在等待了 3 个间隔时间后，依然没有收到 VRRP 通告报文，则认为自己是 Master 交换机，并对外发送 VRRP 通告报文，进行 Master 交换机重新选举。VRRP 报文发送定时器也需要在配置好 VRRP 备份组和所属的 VLAN 的 VLAN 接口上的虚拟路由器 IP 地址后进行，就是在对应的 VLAN 接口下使用 **vrrp vrid virtual-router-id timer advertise adver-interval** 命令进行 VRRP 报文发送定时器配置。命令中的两个参数说明如下：

- **virtual-router-id**：用于指定要设置 VRRP 报文发送定时器的 VRRP 备份组编号，取值范围为 1~255。
- **adver-interval**：用于指定备份组中的 Master 交换机发送 VRRP 报文的定时器，取值范围为 1~255 秒。

默认情况下，备份组中的 Master 交换机发送 VRRP 报文的定时器为 1 秒，可用 **undo vrrp vrid virtual-router-id timer advertise** 命令来恢复为默认值。

**【注意】**同一备份组内的交换机要配置相同的定时器值，否则导致配置错误。

下面的示例是设置备份组 1 中 Master 交换机发送 VRRP 报文的定时器为 15 秒。

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 timer advertise 15
```

### 4. VRRP 监视功能配置

通过本章前面的学习我们已经知道，VRRP 备份组中的 Backup 交换机会在 Master 交换机出现故障时重新选举新的 Master 交换机。这就涉及到一个如何识别 Master 交换机出现故障的问题了。这就是此处所要介绍的 VRRP 监视功能，它是监视 Master 交换机在备份组中的接口状态，VRRP 协议一旦发现该接口 Down 了，立即降低 Master 主机的优先级，这样就可以重新进行 Master 交换机选举。

其实这里的 VRRP 端口监视包括两个方面，一是监视 VRRP 备份组中 VLAN 接口状态，另一个是监视某个 VLAN 中的交换机物理端口状态。VRRP 的 VLAN 接口监视功能更好地扩充了备份功能，即不仅能在备份组所在的接口出现故障时提供备份功能，而且在交换机的其他接口不可用时，也可以使用备份功能。当被监视的接口 Down 掉时，拥有这个接口的交换机的优先级会自动降低一个数额，可能导致备份组内其他交换机的优先级高于这个交换机的优先级，从而使得其他优先级高的交换机转变为 Master。启动 VRRP 备份组端口监视功能后，将对物理端口进行链路状态监视，在物理端口发生故障时，会降低所在交换机的优先级。如果备份组内管理交换机（Master）与上游连接的物理端口发生故障时，管理交换机的优先级按照设定的优先级降低值自动降低，从而促使备份组内重新选举管理交换机。

这两种监视功能的具体步骤如表 4-4 所示。

**【注意】**当备份组内存在“IP 地址拥有者”（也就是 VRRP 备份组中某个交换机的物理端口 IP 地址与 VRRP 虚拟 IP 地址相同的交换机）时，IP 地址拥有者上配置的 VRRP 备份组的监视端口功能不生效，因为该交换机永久是 VRRP 备份组的 Master，具有最高优先级 255，不可改变。监视物

理端口时，该端口可以包含在备份组所在 VLAN 接口的 VLAN 中，但最多只可以对 8 个物理端口进行监控。

表 4-4 VRRP 监视功能的配置步骤

步骤	命令	说明
1	<b>system-view</b> 例如：<Sysname> <b>system-view</b>	进入系统视图
2	<b>interface Vlan-interface vlan-id</b> 例如：[Sysname] <b>interface Vlan-interface 1</b>	进入 VLAN 接口视图
3	<b>vrrp vrid virtual-router-id virtual-ip virtual-address</b> 例如：[Sysname-Vlan-interface1] <b>vrrp vrid 1 virtual-ip 10.10.0.1</b>	添加备份组虚拟路由器的 IP 地址，参见 4.2.1 节介绍
4	<b>vrrp vrid virtual-router-id track interface vlan-interface vlan-id [ reduced value-reduced ]</b> 例如：[Sysname-Vlan-interface1] <b>vrrp vrid 1 track interface vlan-interface 1 reduced 30</b>	<p>（可选）启用 VRRP 备份组 VLAN 接口监视功能。参数说明如下：</p> <ul style="list-style-type: none"> <li><b>virtual-router-id</b>：用来指定要启用备份组 VLAN 接口监视功能的 VRRP 备份组编号，取值范围为 1~255</li> <li><b>vlan-id</b>：用来指定要监视的 VLAN 接口（不一定是属于 VRRP 备份组所加入的 VLAN）</li> <li><b>reduced value-reduced</b>：可选参数，在指定的 VLAN 接口上出现 Down 状态后，指定交换机的优先级降低的数额，取值范围为 1~255。默认情况下，出现这种情况时对应 VLAN 接口的交换机的优先级降低数额为 10，若未输入 <b>value-reduced</b> 参数，则表示使用默认值</li> </ul> <p>可用 <b>undo vrrp vrid virtual-router-id track interface vlan-interface vlan-id</b> 命令取消监视接口</p>
5	<b>quit</b> 例如：[Sysname-Vlan-interface1] <b>quit</b>	退出
6	<b>interface interface-type interface-number</b> 例如：[Sysname] <b>interface GigabitEthernet 1/0/1</b>	进入以太网端口视图
7	<b>vrrp vlan-interface vlan-id vrid virtual-router-id track [ reduced value-reduced ]</b> 例如：[Sysname-GigabitEthernet1/0/1] <b>vrrp vlan-interface 1 vrid 1 track reduced 50</b>	<p>启用 VRRP 备份组物理端口监视功能。命令中的参数说明如下：</p> <ul style="list-style-type: none"> <li><b>vlan-id</b>：指定要监视的物理端口所属 VLAN 的 VLAN 编号（不一定是属于 VRRP 备份组所加入的 VLAN）</li> <li><b>virtual-router-id</b>：指定要启用物理端口监视功能的 VRRP 备份组编号，取值范围为 1~255</li> <li><b>reduced value-reduced</b>：监视到指定 VLAN 的物理端口处于 Down 状态时指定对应以太网端口的优先级降低的数额，取值范围为 1~255。默认情况下，以太网端口优先级降低的数额为 10，若未输入 <b>value-reduced</b> 参数则表示使用该默认值</li> </ul> <p>可用 <b>undo vrrp vlan-interface vlan-id vrid virtual-router-id track</b> 命令关闭 VRRP 备份组物理端口的监视功能</p>

【示例 4】在启用了 VRRP 功能的 VLAN2 接口上设置监视 VLAN1 接口，当 VLAN1 接口 Down 掉时，VLAN2 上的备份组 1 的 Master 交换机优先级降低 50。

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 track interface vlan-interface 1 reduced 50
```

【示例 5】监视 VLAN2 中以太网端口 GigabitEthernet1/0/1，在出现 Down 状态时，该端口优先级降低 50。

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port GigabitEthernet1/0/1
[Sysname-vlan2] quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vrrp vlan-interface 2 vrid 1 track reduced 50
```

## 5. 虚拟转发器监视配置

在配置虚拟转发器监视功能之前，需要先在接口上创建备份组并配置虚拟 IP 地址。在 VRRP 标准协议模式和负载均衡模式下均可配置虚拟转发器监视功能，但只有在 VRRP 负载模式下虚拟转

发器监视功能才会起作用。

在这里先来简单介绍 Track 功能。

为了避免报文转发失败，提高通信的可靠性，一些模块需要及时感知接口的状态、链路的状态、网络的可达性或网络的性能。例如，静态路由需要及时感知路由下一跳是否可达。当下一跳不可达时，报文无法通过该静态路由到达目的网络。此时，应该将静态路由置为无效，确保报文不再通过该静态路由转发。需要感知接口状态、网络可达性等的模块，称为应用模块。

设备可以通过多种方式监测接口状态、链路状态、网络可达性和网络性能，如 NQA（Network Quality Analyzer，网络质量分析）、BFD（Bidirectional Forwarding Detection，双向转发检测）和接口管理。负责监测接口状态、网络可达性等的模块，称为监测模块。

应用模块可以直接与监测模块关联。监测模块负责监测接口状态、链路状态、网络可达性或网络性能，并将监测结果通知给应用模块；应用模块根据监测结果，进行相应的处理，例如，将静态路由置为无效。应用模块支持与多种监测模块关联时，由于不同监测模块通知给应用模块的监测结果形式各不相同，应用模块需要分别处理不同形式的监测结果。

在应用模块和监测模块之间增加 Track 模块，可以屏蔽不同监测模块的差异，简化应用模块的处理。Track 模块中可以创建多个 Track 对象，分别与不同的应用模块和监测模块关联。该 Track 对象称为 Track 项，通过编号来标识。Track 项的状态包括以下三种：

- **Positive**: 表示监测的对象正常工作，如接口处于 Up 状态、网络可达。
- **Negative**: 表示监测的对象出现异常，如接口处于 Down 状态、网络不可达。
- **Invalid**: 表示监测结果无效，如 NQA 作为监测模块时，与 Track 项关联的 NQA 测试组不存在。

配置虚拟转发器监视 Track 项的方法是在 VRRP 备份所属 VLAN 的 VLAN 接口（先要为该 VLAN 接口配置 VRRP 虚拟 IP 地址）视图下使用 **vrrp vrid virtual-router-id weight track track-entry-number [ reduced weight-reduced ]** 命令。VRRP 工作在负载均衡模式时，如果配置虚拟转发器监视 Track 项，则当 Track 项状态为 Negative 时，路由器上所有虚拟转发器的权重都将降低指定的数额；被监视的 Track 项状态由 Negative 变为 Positive 或 Invalid 后，路由器中所有虚拟转发器的权重会自动恢复。命令中的参数说明如下：

- **virtual-router-id**: 指定要配置虚拟转发器监视功能的 VRRP 备份组号，取值范围为 1~255。
- **track track-entry-number**: 指定被监视的 Track 项序号，**track-entry-number** 取值范围为 1~1024。
- **reduced weight-reduced**: 可选参数，指定当 Track 项状态为 Negative 时，虚拟转发器的权重降低的数额，**weight-reduced** 取值范围为 1~255，默认值为 30。

默认情况下，没有指定虚拟转发器监视的 Track 项，可用 **undo vrrp vrid weight track** 命令取消虚拟转发器监视指定的 Track 项。

**【注意】**只有 VRRP 工作在负载均衡模式时，执行本命令才会生效。

在进行本配置之前，需要先在 VLAN 接口上创建备份组并配置虚拟 IP 地址。

被监视的 Track 项可以是未创建的 Track 项。可以通过 **vrrp vrid weight track** 命令指定监视的 Track 项后，再通过 **track** 命令创建该 Track 项。

默认情况下，虚拟转发器的权重为 255；虚拟转发器的失效下限为 10。

由于 VF Owner 的权重高于或等于失效下限时，它的优先级始终为 255，不会根据虚拟转发器的权重改变，因此只有配置的权重降低数额能够保证监视的上行链路出现故障时 VF Owner 的权重低于失效下限，即权重降低的数额大于 245，其他的虚拟转发器才能接替 VF Owner 成为 AVF。

下面的示例是在 VLAN 接口 2 上配置虚拟转发器权重监视 Track 项 1，当 Track 项 1 状态为 Negative 时，VLAN 接口 2 上备份组 1 所有虚拟转发器的权重都降低 50。

```

<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 weight track 1 reduced 50

```

## 4.4 H3C 交换机 VRRP 管理

可在任意视图下执行表 4-5 所示的 **display** 命令查看配置 VRRP 功能后的运行情况，验证配置的效果。还可在用户视图下执行表 4-5 中的 **reset** 命令清除 VRRP 的统计信息。

表 4-5 VRRP 配置的显示与维护命令

命令	说明
<b>S58 及以前系列支持 VRRP 的交换机（分两条命令）：</b> <b>display vrrp [ verbose ] [ interface vlan-interface vlan-id [ vrid virtual-router-id ] ]</b> <b>display vrrp statistics [ interface vlan-interface vlan-id [ vrid virtual-router-id ] ]</b> <b>S7500 及以后系列交换机（仅一条命令）：</b> <b>display vrrp [ interface Vlan-interface vlan-id   statistics [ Vlan-interface vlan-id ] ] [ virtual-router-id ]</b>	显示 VRRP 的状态信息和统计信息。 <b>display</b> 命令可以在任意视图下执行
<b>S58 及以前系列支持 VRRP 的交换机：</b> <b>reset vrrp statistics [ interface vlan-interface vlan-id [ vrid virtual-router-id ] ]</b> <b>S7500 及以后系列交换机：</b> <b>reset vrrp statistics [ vlan-interface vlan-id ] [ virtual-router-id ]</b>	清除 VRRP 的统计信息。 <b>reset</b> 命令可以在用户视图下执行

### 1. display vrrp 命令

**display vrrp [ verbose ] [ interface vlan-interface vlan-id [ vrid virtual-router-id ] ]** 用来显示 VRRP 备份组的状态信息，该命令仅适用于 S58 及以前支持 VRRP 功能的 H3C 交换机系列。命令中的可选项和参数说明如下：

- **verbose**：可选项，指定显示 VRRP 状态的详细信息。
- **vlan-interface vlan-id**：可选参数，显示指定 VLAN 接口对应的 VRRP 备份组状态信息，其中，*vlan-id* 为 VLAN 接口的编号。
- **vrid virtual-router-id**：可选参数，指定仅显示指定备份组的 VRRP 状态信息。其中，*virtual-router-id* 为 VRRP 备份组号，取值范围为 1~255。

如果不输入接口号和备份组号，将显示该设备上所有备份组的状态信息；如果只输入接口号，不输入备份组号则显示该接口上所有备份组的状态信息；如果同时输入接口号和备份组号，则仅显示指定接口上的指定备份组的状态信息。

【示例 1】显示当前交换机上的所有 VRRP 备份组信息。输出信息中各字段的描述如表 4-6 所示。

```

<Sysname> display vrrp
Run Method      : VIRTUAL-MAC
Virtual Ip Ping : Disable
The total number of the virtual routers:  1

```

Interface	VRID	State	Run Pri	Adver. Time	Auth Type	Virtual IP
Vlan2	2	Initialize	100	1	NONE	173.160.0.1

【示例 2】显示当前交换机 VRRP 功能运行状态的详细信息。输出信息中各字段的描述如表 4-7 所示。

表 4-6 display vrrp 输出信息字段说明

字段	说明
Run Method	VRRP 当前的运行模式，包括： <ul style="list-style-type: none"> <li>● REAL-MAC：采用 VRRP 备份组中设备的实际 MAC 地址</li> <li>● VIRTUAL-MAC：采用 VRRP 备份组虚拟 MAC 地址</li> </ul>
Virtual IP ping	备份组的虚拟 IP 地址能否被 ping 通
Interface	当前交换机上启用 VRRP 功能的 VLAN 接口
VRID	当前交换机的 VRID
State	当前交换机在备份组中的状态，包括 Master、Backup 和 Initialize 三种状态
Run Pri	当前交换机在 VRRP 备份组中的运行优先级
Adver.Timer	所设置的 VRRP 通告报文发送时间间隔
Auth Type	所设置的 VRRP 认证类型，包括无认证（NONE）、SIMPLE 和 MD5
Virtual IP	VRRP 备份组的虚拟 IP 地址

<Sysname> **display vrrp verbose**

```

Run Method      : VIRTUAL-MAC
Virtual Ip Ping : Disable
Interface       : Vlan-interface1
VRID            : 1
Adver. Timer    : 1
Admin Status    : UP
State           : Master
Config Pri      : 120
Run Pri         : 100
Preempt Mode    : YES
Delay Time      : 0
Auth Type       : NONE
Virtual IP      : 192.168.0.100
Virtual MAC     : 0000-5e00-0101
Master IP       : 192.168.0.18

```

表 4-7 display vrrp verbose 输出信息字段说明

字段	说明
Run Method	VRRP 当前的运行模式，包括： <ul style="list-style-type: none"> <li>● REAL-MAC：采用 VRRP 备份组中设备的实际 MAC 地址</li> <li>● VIRTUAL-MAC：采用 VRRP 备份组虚拟 MAC 地址</li> </ul>
Virtual Ip Ping	备份组的虚拟 IP 地址能否被 ping 通
Interface	当前交换机上启用 VRRP 功能的 VLAN 接口
VRID	当前交换机的 VRID
Adver. Timer	所设置的 VRRP 通告报文发送时间间隔
Admin Status	当前交换机的可管理状态，包括 UP 和 DOWN 两种状态
State	当前交换机在备份组中的状态，包括 Master、Backup 和 Initialize 三种状态
Config Pri	当前交换机所配置的 VRRP 优先级
Run Pri	当前交换机在 VRRP 备份组中的运行优先级
Preempt Mode	当前交换机上所配置的抢占模式
Delay Time	当前交换机上所配置的抢占延迟
Auth Type	当前交换机上所配置的认证类型，包括无认证（NONE）、SIMPLE 和 MD5
Virtual IP	VRRP 备份组的虚拟 IP 地址
Virtual MAC	备份组虚拟 IP 地址对应的虚拟 MAC 地址，只在交换机为 Master 状态时，才显示此表项
Master IP	处于 Master 状态的交换机所对应接口的主 IP 地址

## 2. display vrrp statistics 命令

**display vrrp statistics [ interface vlan-interface *vlan-id* [ vrid *virtual-router-id* ] ]** 命令用来显示 VRRP 备份组的统计信息。本命令也仅适用于 S58 及以前系列支持 VRRP 的 H3C 交换机，不适用于 S7500 及以后系列支持 VRRP 的 H3C 交换机。命令中的参数说明如下：

- **vlan-interface *vlan-id***：可选参数，指定显示指定 VLAN 接口中所有 VRRP 备份组统计信息。其中，*vlan-id* 为 VLAN 接口的编号。
- **vrid *virtual-router-id***：可选参数，指定显示 *vlan-id* 参数所对应 VLAN 接口中指定的备份组

VRRP 统计信息。其中, *virtual-router-id* 为 VRRP 备份组号, 取值范围为 1~255 的正整数。

如果不输入 VLAN 接口号和备份组号, 将显示该设备上所有备份组的统计信息; 如果只输入 VLAN 接口号, 不输入备份组号, 则显示该 VLAN 接口上所有备份组的统计信息; 如果同时输入接口号和备份组号, 则显示该接口上指定备份组的统计信息。

【示例 3】显示当前交换机上所有 VRRP 备份组的统计信息。输出信息中各字段的说明如表 4-8 所示。

```
<Sysname> display vrrp statistics
Interface          : Vlan-interface1
VRID               : 1
Checksum Errors    : 0          Version Errors          : 0
VRID Errors        : 0          Advertisement Interval Errors : 0
IP TTL Errors      : 0          Auth Failures        : 0
Invalid Auth Type  : 0          Auth Type Mismatch   : 0
Packet Length Errors : 0       Address List Errors   : 0
Become Master      : 1          Priority Zero Pkts Rcvd : 0
Advertise Rcvd     : 0          Priority Zero Pkts Sent  : 0
Invalid Type Pkts Rcvd : 0
```

表 4-8 display vrrp statistics 输出信息字段说明

字段	说明
Interface	虚拟路由器所在的 VLAN 接口
VRID	备份组号
Checksum Errors	校验和发生错误的次数
Version Errors	版本号错误次数
VRID Errors	虚拟路由器的 VRID 错误次数
Advertisement Interval Errors	VRRP 通告报文发送时间间隔错误的次数
IP TTL Errors	TTL 错误的次数
Auth Failures	认证错误的次数
Invalid Auth Type	认证类型无效的次数
Auth Type Mismatch	认证类型不匹配的次数
Packet Length Errors	VRRP 报文长度错误的次数
Address List Errors	虚拟 IP 地址列表错误的次数
Become Master	当前交换机在 VRRP 备份组中充当 Master 的次数
Priority Zero Pkts Rcvd	收到的优先级为 0 的 VRRP 通告报文的数目
Advertise Rcvd	收到的 VRRP 通告报文的数目
Priority Zero Pkts Sent	发送的优先级为 0 的 VRRP 通告报文的数目
Invalid Type Pkts Rcvd	报文类型错误的次数

【说明】以上两条命令在 S7500 及以后支持 VRRP 的 H3C 交换机系列中就合并成了一条命令, 那就是 **display vrrp [ interface Vlan-interface vlan-id | statistics [ Vlan-interface vlan-id ] ] [ virtual-router-id ]**。该命令只是不支持前面 S58 及以前系列交换机所支持的 **verbose** 可选项, 但包括了上面两条命令的功能。参数说明也可参见以上两条命令中的对应参数。

### 3. reset vrrp statistics 命令

**reset vrrp statistics [ interface vlan-interface vlan-id [ vrid virtual-router-id ] ]** 命令用来清除当前交换机上的 VRRP 统计信息。它是在用户视图下执行的。命令中的参数说明如下:

- **vlan-interface vlan-id**: 可选参数, 指定清除指定 VLAN 接口中所有 VRRP 备份组统计信息。其中, *vlan-id* 为 VLAN 接口的编号。
- **vrid virtual-router-id**: 可选参数, 指定清除 *vlan-id* 参数所对应 VLAN 接口中指定的备份组 VRRP 统计信息。其中, *virtual-router-id* 为 VRRP 备份组号, 取值范围为 1~255 的正整数。

如果不输入接口号和备份组号，则清除该交换机上所有备份组的统计信息；如果只输入接口号，不输入备份组号，则清除该接口上所有备份组的统计信息；如果同时输入接口号和备份组号，则清除该接口上指定备份组的统计信息。

【示例 4】清除当前交换机所有接口上所有备份组的 VRRP 统计信息。

```
<Sysname> reset vrrp statistics
```

## 4.5 H3C 交换机 VRRP 配置示例

在本章前面已介绍到 H3C 交换机支持标准协议和负载均衡两种 VRRP 工作模式。在标准协议工作模式中，又有主备备份和负载分担两种应用模式。下面分别用一个示例进行介绍。但与前面一样，此处也仅介绍基于 IPv4 协议的这些 VRRP 应用示例。

### 4.5.1 简单主备备份模式的 VRRP 应用配置示例

VRRP 的最简单应用就是主备备份模式，就是创建一个 VRRP 备份组，然后在这个备份组中指定或选举一个 Master 交换机，备份组中的其他交换机均为 Backup 交换机。平时只有 Master 交换机担当数据转发任务，只有在 Master 交换机失效，或者重新选择新的 Master 交换机时，Backup 交换机中的一台才可能接替原来 Master 交换机的工作。但任一时刻实际上都只有 Master 一台交换机担当数据转发任务，备份组中的其他交换机只是起到一个备份的作用。

本示例拓扑如图 4-11 所示。Host A 需要访问位于 Internet 上的 Host B，Host A 的默认网关为 210.110.10.1/24。Switch A 和 Switch B 共同组成一个 VRRP 备份组 1，虚拟 IP 地址为 210.110.10.1/24。要求当 Switch A 正常工作时，Host A 发送给 Host B 的报文通过 Switch A 转发；当 Switch A 出现故障时，Host A 发送给 Host B 的报文通过 Switch B 转发。

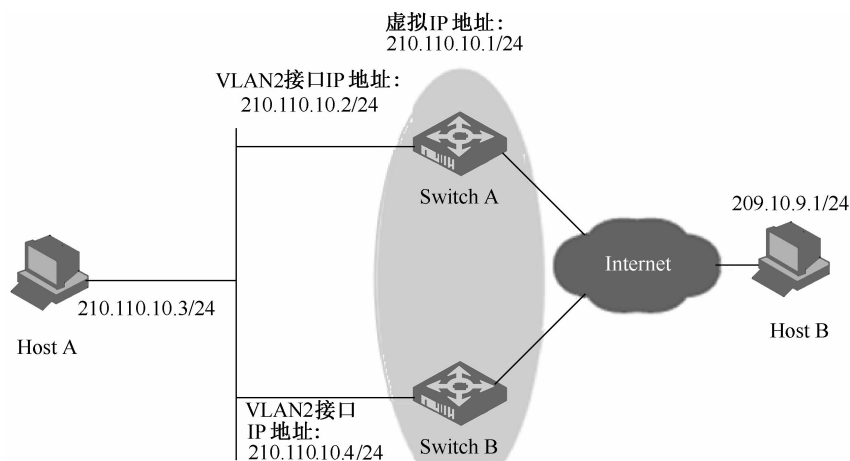


图 4-11 主备备份方式 VRRP 应用示例

下面是具体的配置步骤。

#### 1. Switch A 上的配置

(1) 创建 VRRP 备份组所属的 VLAN2（不是固定的，可以是其他任一 VLAN），为这个 VLAN 接口配置 IP 地址（注意，不是 VRRP 备份组的虚拟 IP 地址），并把交换机的 Gigabitethernet 1/0/5 接口加入到这个 VLAN 中。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 210.110.10.2 255.255.255.0
```

## (2) 配置 VRRP 属性。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 210.110.10.1 !---创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 210.110.10.1
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 120 !---设置 Switch A 在备份组 1 中的优先级为 120，高于 Switch B 所采用的默认的优先级 100，以保证 Switch A 成为 Master，负责转发流量
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5 !---设置 Switch A 工作在抢占方式，以保证 Switch A 故障恢复后，能再次抢占成为 Master，即只要 Switch A 正常工作，就由 Switch A 负责转发流量。为了避免频繁地进行状态切换，配置抢占延迟时间为 5 秒
```

## 2. Switch B 上的配置

(1) 创建与 Switch A 相同的 VRRP 备份组所属的 VLAN2，为该 VLAN 的 VLAN 接口配置 IP 地址（VRRP 组中的所有 IP 地址必须在同一个网段），并把交换机的 Gigabitethernet 1/0/5 接口加入到这个 VLAN 中。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-Vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 210.110.10.4 255.255.255.0
```

## (2) 配置 VRRP 属性。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 210.110.10.1 !---创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 210.110.10.1
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 7 !---设置 Switch B 工作在抢占方式，抢占延迟时间为 7 秒
```

## 3. 验证配置结果

配置完成后，在 Host A 上可以 ping 通 Host B。通过 **display vrrp verbose** 命令查看配置后的结果。在 Switch A 上的备份组 1 信息如下（注意输出信息中粗体字部分所显示的 Master 交换机的 VLAN 接口 IP 地址）。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
  Run Mode       : Standard
  Run Method     : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID           : 1
  Admin Status   : Up
  Config Pri     : 120
  Preempt Mode   : Yes
  Auth Type      : None
  Virtual IP     : 210.110.10.1
  Virtual MAC    : 0000-5e00-0101
  Master IP      : 210.110.10.2
  Adver Timer    : 1
  State          : Master
  Running Pri    : 120
  Delay Time     : 5
```

Switch B 上的备份组 1 的详细信息如下。

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
  Run Mode       : Standard
  Run Method     : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID           : 1
  Admin Status   : Up
  Config Pri     : 100
  Preempt Mode   : Yes
  Adver Timer    : 1
  State          : Backup
  Running Pri    : 100
  Delay Time     : 5
```



```
Auth Type      : None
Virtual IP     : 210.110.10.1
Master IP    : 210.110.10.2
```

对比两个交换机上的 VRRP 备份组 1 信息可以看出，在备份组 1 中 Switch A 为 Master 路由器，Switch B 为 Backup 路由器，Host A 发送给 Host B 的报文通过 Switch A 转发。

在 Switch A 出现故障后，在 Host A 上仍然可以 ping 通 Host B，此时通过 **display vrrp verbose** 命令查看 Switch B 上的备份组 1 的详细信息（注意输出信息中粗体字部分所显示的 Master 交换机的 VLAN 接口 IP 地址）。

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
  Run Mode      : Standard
  Run Method    : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID          : 1
  Admin Status  : Up
  Config Pri    : 100
  Preempt Mode  : Yes
  Auth Type     : None
  Virtual IP    : 210.110.10.1
  Virtual MAC   : 0000-5e00-0101
Master IP    : 210.110.10.4
  Adver Timer   : 1
  State         : Master
  Running Pri   : 100
  Delay Time    : 7
```

以上显示信息表示 Switch A 出现故障后，Switch B 成为 Master 路由器，Host A 发送给 Host B 的报文通过 Switch B 转发。

当 Switch A 故障恢复后，再使用 **display vrrp verbose** 命令查看 Switch A 上的 VRRP 备份组 1 的详细信息，如下所示（注意输出信息中粗体字部分所显示的 Master 交换机的 VLAN 接口 IP 地址）。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
  Run Mode      : Standard
  Run Method    : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID          : 1
  Admin Status  : Up
  Config Pri    : 120
  Preempt Mode  : Yes
  Auth Type     : None
  Virtual IP    : 210.110.10.1
  Virtual MAC   : 0000-5e00-0101
Master IP    : 210.110.10.2
  Adver Timer   : 1
  State         : Master
  Running Pri   : 120
  Delay Time    : 7
```

以上显示信息表示 Switch A 故障恢复后，Switch A 会抢占成为 Master，Host A 发送给 Host B 的报文仍然通过 Switch A 转发。

#### 4.5.2 综合主备备份模式的 VRRP 应用配置示例

在上一示例中只配置了最基本的 VRRP 属性，利用了 VRRP 的最基本的功能，没有配置 VRRP 认证，也没有配置 VRRP 接口/端口监视功能。本示例包括了 VRRP 主备备份模式应用中以上这些比较高级的功能配置。本示例的网络拓扑参见图 4-11。

Host A 需要访问位于 Internet 上的 Host B，Host A 的默认网关为 210.110.10.1/24。Switch A 和 Switch B 共同组成一个 VRRP 备份组 1，虚拟 IP 地址为 210.110.10.1/24。要求当 Switch A 正常工作时，Host A 发送给 Host B 的报文通过 Switch A 转发；当 Switch A 连接 Internet 的 VLAN3 接口不可用时，Host A 发送给 Host B 的报文通过 Switch B 转发。另外，为了防止非法用户构造报文攻击备

份组，通过简单字符认证方法验证备份组 1 中的 VRRP 报文，认证字为 123456。

下面是具体的配置步骤。

### 1. Switch A 上的配置

(1) 配置 VRRP 备份组所属的 VLAN2（上节已解释的配置此处不再重复说明）。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 210.110.10.2 255.255.255.0
```

(2) 配置 VRRP 属性（上节已解释的配置此处不再重复说明）。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 210.110.10.1
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
[SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple 123456 !---设置备份组的认证方式为 simple 认证，认证字为 123456
[SwitchA-Vlan-interface2] vrrp vrid 1 timer advertise 4 !---设置 Master 发送 VRRP 报文的间隔时间为 4 秒
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
[SwitchA-Vlan-interface2] vrrp vrid 1 track interface vlan-interface 3 reduced 30 !---配置 Switch A 监视上行接口——VLAN3 接口，
当 VLAN3 接口不可用时，降低 Switch A 在备份组 1 中的优先级。降低后的优先级应低于 Switch B 的优先级 100，即优先级降低数额应大
于 20，以保证 Switch B 能够抢占成为 Master。本例中，配置优先级降低数额为 30
```

### 2. Switch B 上的配置

(1) 配置 VRRP 备份组所属的 VLAN2（上节已解释的配置此处不再重复说明）。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 210.110.10.4 255.255.255.0
```

(2) 配置 VRRP 属性（上节已解释的配置此处不再重复说明）。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 210.110.10.1
[SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple 123456 !---设置备份组的认证方式为 simple 认证，认证字为
123456（备份组中的所有交换机的认证方式和认证字配置必须一致）
[SwitchB-Vlan-interface2] vrrp vrid 1 timer advertise 5 !---设置 Master 发送 VRRP 报文的间隔时间为 5 秒
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 7 !---设置 Switch B 工作在抢占方式，以保证 Switch A 的优先级降
低后，Switch B 可以抢占成为 Master。为了避免频繁地进行状态切换，配置抢占延迟时间为 7 秒
```

### 3. 验证配置结果

配置完成后，在 Host A 上可以 ping 通 Host B。通过 **display vrrp verbose** 命令查看配置后的结果。Switch A 上显示的备份组 1 的详细信息如下（注意输出信息中粗体字部分所显示的 Master 交换机的 VLAN 接口 IP 地址）。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
  Run Mode       : Standard
  Run Method     : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID           : 1                Adver Timer   : 5
  Admin Status   : Up               State          : Master
  Config Pri     : 120              Running Pri    : 120
  Preempt Mode   : Yes              Delay Time     : 7
  Auth Type      : Simple           Key            : hello
  Virtual IP     : 210.110.10.1
  Virtual MAC    : 0000-5e00-0101
Master IP      : 210.110.10.2
VRRP Track Information:
  Track Interface: Vlan3            State : Up      Pri Reduced : 30
```

Switch B 上显示的备份组 1 的详细信息如下（注意输出信息中粗体字部分所显示的 Master 交换机的 VLAN 接口 IP 地址）。

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
  Run Mode      : Standard
  Run Method    : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID          : 1
  Admin Status  : Up
  Config Pri    : 100
  Preempt Mode  : Yes
  Auth Type     : Simple
  Virtual IP    : 210.110.10.1
  Master IP     : 210.110.10.2
  Adver Timer   : 5
  State         : Backup
  Running Pri   : 100
  Delay Time    : 7
  Key           : hello
```

以上显示信息表示在备份组 1 中 Switch A 为 Master 路由器，Switch B 为 Backup 路由器，Host A 发送给 Host B 的报文通过 Switch A 转发。

当 Switch A 连接 Internet 的 VLAN3 接口不可用时，在 Host A 上仍然可以 ping 通 Host B。通过 **display vrrp verbose** 命令查看备份组的信息。此时在 Switch A 上显示的备份组 1 的详细信息如下（注意输出信息中粗体字部分所显示的 Master 交换机的 VLAN 接口 IP 地址）。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
  Run Mode      : Standard
  Run Method    : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID          : 1
  Admin Status  : Up
  Config Pri    : 120
  Preempt Mode  : Yes
  Auth Type     : Simple
  Virtual IP    : 210.110.10.1
  Master IP     : 210.110.10.4
  Adver Timer   : 5
  State         : Backup
  Running Pri   : 90
  Delay Time    : 7
  Key           : hello
VRRP Track Information:
  Track Interface: Vlan3
  State          : Down
  Pri Reduced    : 30
```

在 Switch A 的 VLAN3 接口不可用时，Switch B 上显示的备份组 1 的详细信息如下（注意输出信息中粗体字部分所显示的 Master 交换机的 VLAN 接口 IP 地址）。

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
  Run Mode      : Standard
  Run Method    : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID          : 1
  Admin Status  : Up
  Config Pri    : 100
  Preempt Mode  : Yes
  Auth Type     : Simple
  Virtual IP    : 210.110.10.1
  Virtual MAC   : 0000-5e00-0101
  Master IP     : 210.110.10.4
  Adver Timer   : 5
  State         : Master
  Running Pri   : 100
  Delay Time    : 7
  Key           : hello
```

以上显示信息表示 Switch A 的 VLAN3 接口不可用时，Switch A 的优先级降低为 90，成为 Backup 路由器，Switch B 成为 Master 路由器，Host A 发送给 Host B 的报文通过 Switch B 转发。

### 4.5.3 负载分担模式 VRRP 应用配置示例

本示例是 VRRP 的负载分担应用配置示例，通过在一个 VRRP 备份组中创建多个 VRRP 备份组（分属于不同 VLAN），在实现主备备份 VRRP 应用的同时实现 VRRP 备份组中交换机的负载分担。

本示例拓扑如图 4-12 所示。VLAN 2 内主机的默认网关为 210.110.10.100/24；VLAN 3 内主机的默认网关为 210.110.10.200/24；Switch A 和 Switch B 同时属于虚拟 IP 地址为 210.110.10.100/24 的备份组 1 和虚拟 IP 地址为 210.110.10.200/24 的备份组 2。在备份组 1 中 Switch A 的优先级高于 Switch B，在备份组 2 中 Switch B 的优先级高于 Switch A，从而保证 VLAN 2 和 VLAN 3 内的主机分别通过 Switch A 和 Switch B 通信，当 Switch A 或 Switch B 出现故障时，主机可以通过另一台设备继续通信，避免通信中断。

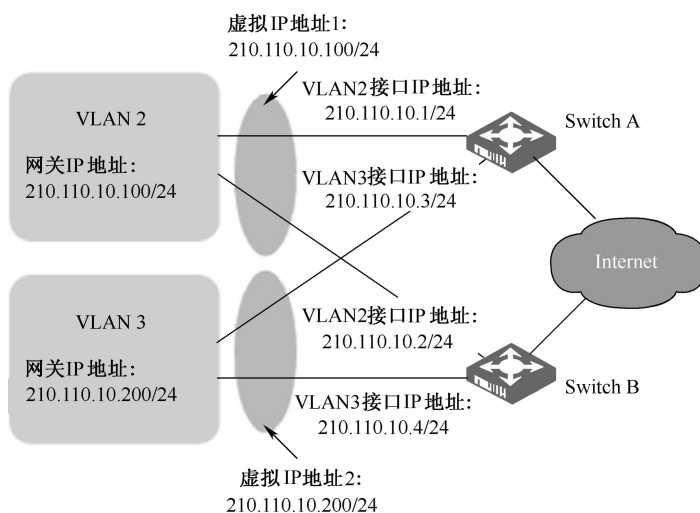


图 4-12 负载分担 VRRP 应用示例

下面是具体的配置步骤。

#### 1. Switch A 上的配置

（1）创建 VRRP 备份组 1 所属的 VLAN 2，VRRP 备份组 2 所属的 VLAN 3，并分别为 VLAN2 和 VLAN3 接口配置 IP 地址，然后把 Switch A 的 GigabitEthernet 1/0/5 端口加入到 VLAN 2 中，把 Switch A 的 GigabitEthernet 1/0/6 端口加入到 VLAN 3 中。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitEthernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 210.110.10.1 255.255.255.0
[SwitchA-Vlan-interface2] quit
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitEthernet 1/0/6
[SwitchA-vlan3] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 210.110.10.3 255.255.255.0
```

#### （2）配置 VRRP 属性。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 210.110.10.100 !---创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 210.110.10.100
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 120 !---设置 Switch A 在备份组 1 中的优先级为 120，高于 Switch B 所采用的默认优先级 100，以保证在备份组 1 中 Switch A 成为 Master，负责转发流量
```

```
[SwitchA-Vlan-interface2] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] vrrp vrid 2 virtual-ip 210.110.10.200 !---创建备份组 2，并配置备份组 2 的虚拟 IP 地址为 210.110.10.200
```

## 2. Switch B 上的配置

(1) 创建 VRRP 备份组 1 所属的 VLAN 2，VRRP 备份组 2 所属的 VLAN 3，并分别为 VLAN2 和 VLAN3 接口配置 IP 地址，然后把 Switch B 的 Gigabitethernet 1/0/5 端口加入到 VLAN 2 中，把 Switch B 的 Gigabitethernet 1/0/6 端口加入到 VLAN 3 中。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 210.110.10.2 255.255.255.0
[SwitchB-Vlan-interface2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/6
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 210.110.10.4 255.255.255.0
```

(2) 配置 VRRP 属性。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 210.110.10.100 !---创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 210.110.10.100
[SwitchB-Vlan-interface2] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] vrrp vrid 2 virtual-ip 210.110.10.200 !---创建备份组 2，并配置备份组 2 的虚拟 IP 地址为 210.110.10.200
[SwitchB-Vlan-interface3] vrrp vrid 2 priority 120 !---设置 Switch B 在备份组 2 中的优先级为 120，高于 Switch A 的优先级 100，以
保证在备份组 2 中 Switch B 成为 Master，负责转发流量
```

## 3. 验证配置结果

下面通过 **display vrrp verbose** 命令查看配置后的结果。Switch A 上的备份组详细信息如下（注意输出信息中粗体字部分所显示的 Master 交换机的 VLAN 接口 IP 地址）。

```
[SwitchA-Vlan-interface3] display vrrp verbose
IPv4 Standby Information:
  Run Mode      : Standard
  Run Method    : Virtual MAC
Total number of virtual routers : 2

Interface Vlan-interface2
VRID           : 1                Adver Timer   : 1
Admin Status   : Up              State          : Master
Config Pri     : 120             Running Pri    : 120
Preempt Mode   : Yes            Delay Time     : 0
Auth Type      : None
Virtual IP     : 210.110.10.100
Virtual MAC    : 0000-5e00-0101
Master IP     : 210.110.10.1

Interface Vlan-interface3
VRID           : 2                Adver Timer   : 1
Admin Status   : Up              State          : Backup
Config Pri     : 100             Running Pri    : 100
Preempt Mode   : Yes            Delay Time     : 0
Auth Type      : None
Virtual IP     : 210.110.10.200
Master IP     : 210.110.10.4
```

Switch B 上显示的备份组详细信息如下（注意输出信息中粗体字部分所显示的 Master 交换机

的 VLAN 接口 IP 地址)。

```
[SwitchB-Vlan-interface3] display vrrp verbose
IPv4 Standby Information:
  Run Mode       : Standard
  Run Method     : Virtual MAC
Total number of virtual routers : 2
Interface Vlan-interface2
  VRID          : 1                Adver Timer   : 1
  Admin Status  : Up              State          : Backup
  Config Pri    : 100             Running Pri    : 100
  Preempt Mode  : Yes             Delay Time     : 0
  Auth Type     : None
  Virtual IP    : 210.110.10.100
  Master IP     : 210.110.10.1

Interface Vlan-interface3
  VRID          : 2                Adver Timer   : 1
  Admin Status  : Up              State          : Master
  Config Pri    : 120             Running Pri    : 120
  Preempt Mode  : Yes             Delay Time     : 0
  Auth Type     : None
  Virtual IP    : 210.110.10.200
  Virtual MAC   : 0000-5e00-0102
  Master IP     : 210.110.10.4
```

从以上两台交换机上显示的信息可以看出，在备份组 1 中 Switch A 为 Master 路由器，Switch B 为 Backup 路由器，默认网关为 210.110.10.100/24 的主机通过 Switch A 访问 Internet；备份组 2 中 Switch A 为 Backup 路由器，Switch B 为 Master 路由器，默认网关为 210.110.10.200/24 的主机通过 Switch B 访问 Internet。

#### 4.5.4 VRRP 负载均衡模式配置示例

在本书 4.2 节中专门介绍了 VRRP 负载均衡工作模式，它是 S58 和 S9500E 等少数 H3C 交换机系列支持的一种 VRRP 工作模式。它与前面介绍的负载分担模式不一样，负载分担模式是通过创建多个 VRRP 备份组，对同一交换机指定不同的备份组角色，以此来实现 VRRP 备份组中交换机的负载分担。而负载均衡则是通过在同一个备份组中配置不同的虚拟 MAC 地址，以形成指向不同交换机的虚拟转发器来实现同一备份组中各交换机的负载均衡。

本示例拓扑如图 4-13 所示。Switch A、Switch B 和 Switch C 属于虚拟 IP 地址为 10.1.1.1/24 的备份组 1。10.1.1.0/24 网段内主机的默认网关为 10.1.1.1/24，利用 VRRP 备份组保证某台网关设备（Switch A、Switch B 或 Switch C）出现故障时，局域网内的主机仍然可以通过网关访问外部网络。同时，备份组 1 工作在负载均衡模式，在 Switch A、Switch B 和 Switch C 上分别配置虚拟转发器通过 Track 项监视上行接口（VLAN3 接口）的状态。当上行接口出现故障时，降低 Switch A、Switch B 和 Switch C 上虚拟转发器的权重，以便其他设备接管它的转发任务。这样就可以通过一个备份组实现负载分担，充分利用网关资源。

下面是具体的配置步骤。

##### 1. Switch A 上的配置

(1) 创建 VRRP 备份组 1 和所属的 VLAN 2，指定 VRRP 为负载均衡模式，并为 VLAN2 接口配置 IP 地址，然后把 Switch A 的 GigabitEthernet 1/0/5 端口加入到 VLAN 2 中。

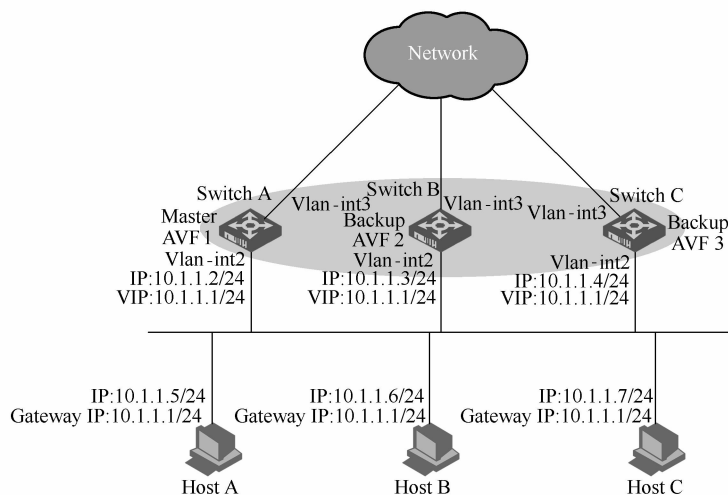


图 4-13 负载均衡模式 VRRP 应用示例

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] vrrp mode load-balance    !---配置 VRRP 工作在负载均衡模式
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.2 24
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1    !---创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.1
```

## (2) 配置 VRRP 属性。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 120    !---配置 Switch A 在备份组 1 中的优先级为 120，高于 Switch B 的优先级 110 和 Switch C 的优先级 100，以保证 Switch A 成为 Master
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5    !---配置 Switch A 工作在抢占方式，以保证 Switch A 故障恢复后，能再次抢占成为 Master，即只要 Switch A 正常工作，Switch A 就会成为 Master。为了避免频繁地进行状态切换，配置抢占延迟时间为 5 秒
[SwitchA-Vlan-interface2] quit
```

## (3) 配置 VRRP 的 VLAN 接口监视功能。

```
[SwitchA] track 1 interface vlan-interface 3    !---创建和 VLAN3 接口物理状态关联的 Track 项 1。如果 Track 项的状态为 Negative，则说明 Switch A 的上行接口出现故障
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp vrid 1 weight track 1 reduced 250    !---配置虚拟转发器监视 Track 项 1。Track 项的状态为 Negative 时，降低 Switch A 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Switch A 的转发任务。本例中，配置虚拟转发器权重降低数额为 250
```

## 2. Switch B 上的配置

Switch B 上的配置与 Switch A 配置基本一样。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] vrrp mode load-balance    !---配置 VRRP 工作在负载均衡模式
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.1.1.3 24
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1    !---创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.1
[SwitchB-Vlan-interface2] vrrp vrid 1 priority 110    !---配置 Switch B 在备份组 1 中的优先级为 110，高于 Switch C 的优先级，以保证 Switch A 出现故障时，Switch B 成为 Master
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5    !---配置 Switch B 工作在抢占方式，抢占延迟时间为 5 秒
[SwitchB-Vlan-interface2] quit
[SwitchB] track 1 interface vlan-interface 3    !---创建和 VLAN3 接口物理状态关联的 Track 项 1。如果 Track 项的状态为 Negative，则说明 Switch B 的上行接口出现故障
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 weight track 1 reduced 250    !---配置虚拟转发器监视 Track 项 1。Track 项的状态为 Negative 时，降低 Switch B 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Switch B 的转发任务。本例中，配置虚拟转发器权重降低数额为 250
```

### 3. Switch C 上的配置

Switch C 上的配置基本上与 Switch B 一样。

```
<SwitchC> system-view
[SwitchC] vlan 2
[SwitchC-vlan2] port gigabitethernet 1/0/5
[SwitchC-vlan2] quit
[SwitchC] vrrp mode load-balance
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ip address 10.1.1.4 24
[SwitchC-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[SwitchC-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
[SwitchC-Vlan-interface2] quit
[SwitchC] track 1 interface vlan-interface 3
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] vrrp vrid 1 weight track 1 reduced 250
```

### 4. 验证配置结果

对以上三台交换机都配置完后，在 Host A 上可以 ping 通外网了。可通过 **display vrrp verbose** 命令查看配置后的结果。Switch A 上的备份组 1 的详细信息如下（注意输出信息中的粗体字部分）。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
  Run Mode       : Load Balance
  Run Method     : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID          : 1
  Admin Status  : Up
  Config Pri    : 120
  Preempt Mode  : Yes
  Auth Type     : None
  Virtual IP    : 10.1.1.1
  Adver Timer   : 1
  State        : Master
  Running Pri   : 120
  Delay Time    : 5
Member IP List : 10.1.1.2 (Local, Master)
10.1.1.3 (Backup)
10.1.1.4 (Backup)
Forwarder Information: 3 Forwarders 1 Active
Config Weight : 255
Running Weight : 255
Forwarder 01
  State      : Active
  Virtual MAC : 000f-e2ff-0011 (Owner)
  Owner ID   : 0000-5e01-1101
  Priority    : 255
  Active     : local
Forwarder 02
  State      : Listening
  Virtual MAC : 000f-e2ff-0012 (Learnt)
  Owner ID   : 0000-5e01-1103
  Priority    : 127
  Active     : 10.1.1.3
Forwarder 03
  State      : Listening
  Virtual MAC : 000f-e2ff-0013 (Learnt)
  Owner ID   : 0000-5e01-1105
  Priority    : 127
  Active     : 10.1.1.4
Forwarder Weight Track Information:
  Track Object : 1
  State        : Positive
  Weight Reduced : 250
```

Switch B 上的备份组 1 的详细信息如下（注意输出信息中的粗体字部分）。

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
  Run Mode       : Load Balance
  Run Method     : Virtual MAC
Total number of virtual routers : 1
```



```

Interface Vlan-interface2
  VRID          : 1                      Adver Timer   : 1
  Admin Status  : Up                     State          : Backup
  Config Pri    : 110                    Running Pri    : 110
  Preempt Mode  : Yes                    Delay Time     : 5
  Auth Type     : None
  Virtual IP    : 10.1.1.1
Member IP List : 10.1.1.3 (Local, Backup)
10.1.1.2 (Master)
10.1.1.4 (Backup)
Forwarder Information: 3 Forwarders 1 Active
Config Weight : 255
Running Weight : 255
Forwarder 01
  State          : Listening
  Virtual MAC    : 000f-e2ff-0011 (Learnt)
  Owner ID       : 0000-5e01-1101
  Priority        : 127
  Active         : 10.1.1.2
Forwarder 02
State          : Active
  Virtual MAC    : 000f-e2ff-0012 (Owner)
  Owner ID       : 0000-5e01-1103
  Priority        : 255
  Active         : local
Forwarder 03
  State          : Listening
  Virtual MAC    : 000f-e2ff-0013 (Learnt)
  Owner ID       : 0000-5e01-1105
  Priority        : 127
  Active         : 10.1.1.4
Forwarder Weight Track Information:
  Track Object   : 1                      State : Positive Weight Reduced : 250

```

Switch C 上的备份组 1 的详细信息如下（注意输出信息中的粗体字部分）。

```

[SwitchC-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
  Run Mode       : Load Balance
  Run Method     : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID          : 1                      Adver Timer   : 1
  Admin Status  : Up                     State          : Backup
  Config Pri    : 100                    Running Pri    : 100
  Preempt Mode  : Yes                    Delay Time     : 5
  Auth Type     : None
  Virtual IP    : 10.1.1.1
Member IP List : 10.1.1.4 (Local, Backup)
10.1.1.2 (Master)
10.1.1.3 (Backup)
Forwarder Information: 3 Forwarders 1 Active
Config Weight : 255
Running Weight : 255
Forwarder 01
  State          : Listening
  Virtual MAC    : 000f-e2ff-0011 (Learnt)
  Owner ID       : 0000-5e01-1101
  Priority        : 127
  Active         : 10.1.1.2
Forwarder 02
  State          : Listening
  Virtual MAC    : 000f-e2ff-0012 (Learnt)
  Owner ID       : 0000-5e01-1103
  Priority        : 127
  Active         : 10.1.1.3
Forwarder 03
State          : Active

```

```
Virtual MAC      : 000f-e2ff-0013 (Owner)
Owner ID        : 0000-5e01-1105
Priority         : 255
Active          : local
Forwarder Weight Track Information:
Track Object    : 1          State : Positive   Weight Reduced : 250
```

以上显示信息表示在备份组 1 中 Switch A 为 Master 路由器，Switch B 和 Switch C 为 Backup 路由器。Switch A、Switch B 和 Switch C 上各有一个 AVF（活跃转发器），并有两个作为备份的 LVF。

当 Switch A 的上行接口（VLAN 接口 3）出现故障后，同样可以通过 **display vrrp verbose** 命令查看 Switch A 上备份组的详细信息，具体如下（注意输出信息中的粗体字部分）。信息表示 Switch A 的上行接口出现故障后，Switch A 上虚拟转发器的权重降低为 5，低于失效下限。Switch A 上所有虚拟转发器的状态均变为 Initialize，不能再用于转发。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
  Run Mode      : Load Balance
  Run Method    : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID          : 1          Adver Timer : 1
  Admin Status  : Up         State      : Master
  Config Pri    : 120        Running Pri : 120
  Preempt Mode  : Yes        Delay Time  : 5
  Auth Type     : None
  Virtual IP    : 10.1.1.1
Member IP List : 10.1.1.2 (Local, Master)
10.1.1.3 (Backup)
10.1.1.4 (Backup)
Forwarder Information: 3 Forwarders 0 Active
  Config Weight : 255
Running Weight : 5
Forwarder 01
  State      : Initialize
  Virtual MAC : 000f-e2ff-0011 (Owner)
  Owner ID   : 0000-5e01-1101
  Priority    : 0
  Active     : 10.1.1.4
Forwarder 02
  State      : Initialize
  Virtual MAC : 000f-e2ff-0012 (Learnt)
  Owner ID   : 0000-5e01-1103
  Priority    : 0
  Active     : 10.1.1.3
Forwarder 03
  State      : Initialize
  Virtual MAC : 000f-e2ff-0013 (Learnt)
  Owner ID   : 0000-5e01-1105
  Priority    : 0
  Active     : 10.1.1.4
Forwarder Weight Track Information:
Track Object : 1          State : Negative   Weight Reduced : 250
```

此时再通过 **display vrrp verbose** 命令查看 Switch C 上备份组的详细信息，得到结果如下（注意输出信息中的粗体字部分）。从输出信息可以看出，Switch C 已成为虚拟 MAC 地址 000f-e2ff-0011 对应的虚拟转发器的 AVF，接管 Switch A 的转发任务，同时还有一个虚拟 MAC 地址 000f-e2ff-0013 对应的虚拟转发器的 AVF。

```
[SwitchC-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
  Run Mode      : Load Balance
  Run Method    : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID          : 1          Adver Timer : 1
```

```

Admin Status : Up                      State : Backup
Config Pri   : 100                     Running Pri : 100
Preempt Mode : Yes                     Delay Time : 5
Auth Type    : None
Virtual IP    : 10.1.1.1
Member IP List : 10.1.1.4 (Local, Backup)
                  10.1.1.2 (Master)
                  10.1.1.3 (Backup)
Forwarder Information: 3 Forwarders 2 Active
Config Weight : 255
Running Weight : 255
Forwarder 01
  State : Active
  Virtual MAC : 000f-e2ff-0011 (Take Over)
  Owner ID : 0000-5e01-1101
  Priority : 85
  Active : local
  Redirect Time : 93 secs
  Time-out Time : 1293 secs
Forwarder 02
  State : Listening
  Virtual MAC : 000f-e2ff-0012 (Learnt)
  Owner ID : 0000-5e01-1103
  Priority : 85
  Active : 10.1.1.3
Forwarder 03
  State : Active
  Virtual MAC : 000f-e2ff-0013 (Owner)
  Owner ID : 0000-5e01-1105
  Priority : 255
  Active : local
Forwarder Weight Track Information:
Track Object : 1          State : Positive   Weight Reduced : 250

```

在超时计时器超时后（约 1800 秒后），再查看 Switch C 上备份组的详细信息，得到如下结果（注意输出信息中的粗体字部分）。从输出信息可以看出，在超时计时器超时后，删除虚拟 MAC 地址 000f-e2ff-0011 对应的虚拟转发器，不再转发目的 MAC 地址为该 MAC 地址的报文。此时 VRRP 备份组中就相当于只有 Switch B 和 Switch C 这两台交换机。

```

[SwitchC-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
  Run Mode : Load Balance
  Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID : 1                      Adver Timer : 1
  Admin Status : Up              State : Backup
  Config Pri : 100               Running Pri : 100
  Preempt Mode : Yes            Delay Time : 5
  Auth Type : None
  Virtual IP : 10.1.1.1
  Member IP List : 10.1.1.4 (Local, Backup)
                    10.1.1.2 (Master)
                    10.1.1.3 (Backup)
Forwarder Information: 2 Forwarders 1 Active
Config Weight : 255
Running Weight : 255
Forwarder 02
  State : Listening
  Virtual MAC : 000f-e2ff-0012 (Learnt)
  Owner ID : 0000-5e01-1103
  Priority : 127
  Active : 10.1.1.3
Forwarder 03

```

```

State          : Active
Virtual MAC    : 000f-e2ff-0013 (Owner)
Owner ID      : 0000-5e01-1105
Priority       : 255
Active        : local
Forwarder Weight Track Information:
Track Object   : 1          State : Positive   Weight Reduced : 250

```

在 Switch A 出现故障后，通过 **display vrrp verbose** 命令查看 Switch B 上备份组的详细信息，结果如下（注意输出信息中的粗体字部分）。从输出信息可以看出，在 Switch A 出现故障后，备份组中只有 Switch B 和 Switch C 两台交换机了，它们原来都是 Backup 角色，现在要重新选举 Master 角色。因为 Switch B 的优先级高于 Switch C，将抢占成为 Master 路由器。

```

[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
Run Mode       : Load Balance
Run Method     : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
VRID           : 1                      Adver Timer   : 1
Admin Status   : Up                     State         : Master
Config Pri     : 110                    Running Pri    : 110
Preempt Mode   : Yes                    Delay Time    : 5
Auth Type      : None
Virtual IP     : 10.1.1.1
Member IP List : 10.1.1.3 (Local, Master)
10.1.1.4 (Backup)
Forwarder Information: 2 Forwarders 1 Active
Config Weight  : 255
Running Weight : 255
Forwarder 02
State          : Active
Virtual MAC    : 000f-e2ff-0012 (Owner)
Owner ID      : 0000-5e01-1103
Priority       : 255
Active        : local
Forwarder 03
State          : Listening
Virtual MAC    : 000f-e2ff-0013 (Learnt)
Owner ID      : 0000-5e01-1105
Priority       : 127
Active        : 10.1.1.4
Forwarder Weight Track Information:
Track Object   : 1          State : Positive   Weight Reduced : 250

```



#### 经验之谈

如果频频出现配置错误提示，这表明交换机收到了错误的 VRRP 报文。一种可能是备份组内的另一台交换机配置不一致，另一种可能是有的设备试图发送非法的 VRRP 报文。对于第一种可能，可以通过修改配置来解决。对于第二种可能，则是有些设备有不良企图，应当通过非技术手段来解决。

如果在同一个备份组内出现多个 Master 交换机，则可能有两种原因，一种是多个 Master 并存时间较短，属于正常情况，无需进行人工干预；另一种是多个 Master 长时间共存，有可能是备份组内成员之间收不到 VRRP 报文，或者收到的报文不合法。解决方法是在多个 Master 之间互相 ping，如果 ping 不通，先检查设备连通性。如果能 ping 通，检查 VRRP 的配置。对于同一个 VRRP 备份组的配置，必须保证虚拟路由器的 IP 地址个数、每个虚拟路由器的 IP 地址、定时器间隔时间和认证方式完全一样。

如果出现 VRRP 状态频繁转换，则一般是由于备份组的定时器间隔时间设置太短造成的，加大这个时间间隔或者设置抢占延迟都可以解决这种故障。