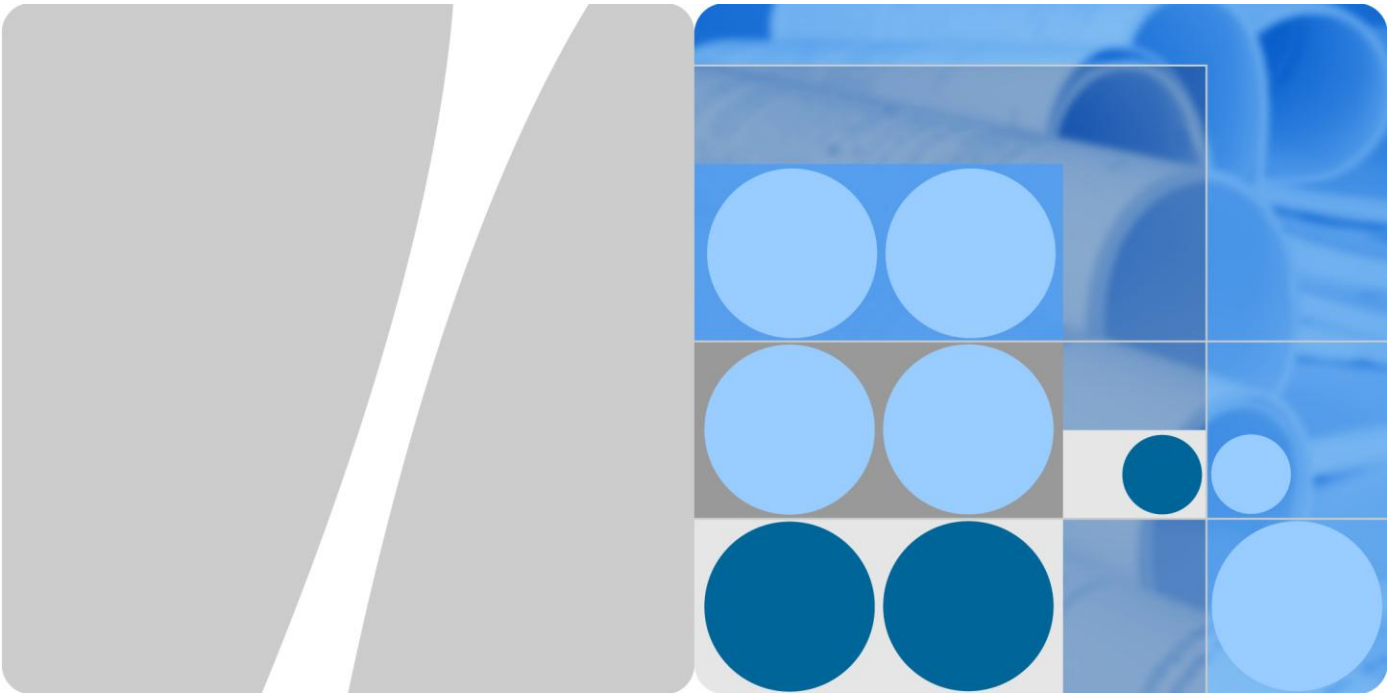


VRRP 技术白皮书

文档版本 01

发布日期 2012-8-31

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

1 VRRP

关于本章

1.1 介绍

定义

虚拟路由冗余协议 VRRP（Virtual Router Redundancy Protocol）通过把几台路由设备联合组成一台虚拟的路由设备，使用一定的机制保证当主机的下一跳路由器出现故障时，及时将业务切换到备份路由器，从而保持业务的连续性和可靠性。

目的

随着网络的快速普及和相关应用的日益深入，各种增值业务（如 IPTV、视频会议等）已经开始广泛部署，基础网络的可靠性日益成为用户关注的焦点，能够保证网络传输不中断对于终端用户非常重要。

现网中，主机一般使用缺省网关与外部网络联系，如果缺省网关发生故障，主机与外部网络的通信将被中断。配置动态路由协议如 RIP、OSPF 或 ICMP 路由发现协议等可以提高系统可靠性，但是需要复杂的配置，而且并不能保证每台主机都支持配置动态路由协议。

VRRP 的出现很好的解决了这个问题。VRRP 能够在不改变组网的情况下，将多台设备组成一个虚拟路由器，通过配置虚拟路由器的 IP 地址为缺省网关，实现缺省网关的备份。当网关设备发生故障时，VRRP 机制能够选举新的网关设备承担数据流量，从而保障网络的可靠通信。

受益

使用 VRRP 功能，可以为用户带来以下的收益：

- 简化网络管理：在具有多播或广播能力的局域网（如以太网）中，借助 VRRP 能在网关设备出现故障时仍然提供高可靠的缺省链路，无需修改动态路由协议、路由发现协议等配置信息便可有效避免单一链路发生故障后的网络中断问题。
- 适应性强：VRRP 报文封装在 IP 报文中，支持各种上层协议。
- 网络开销小：VRRP 只定义了一种报文——VRRP 协议报文，有效减轻了网络设备的负担。

1.2 参考标准和协议

本特性的参考资料清单如下：

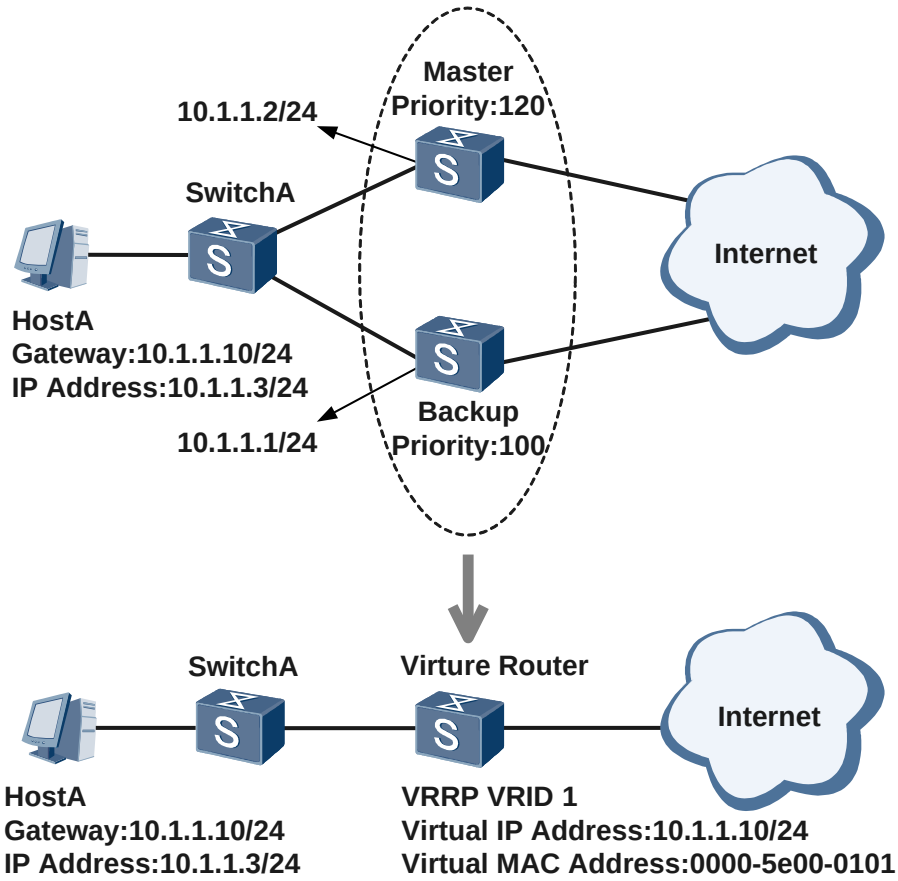
文档	描述	备注
RFC2281	Hot Standby Router Protocol（HSRP）	-
RFC2338	Virtual Router Redundancy Protocol（version number One1998）	-
RFC2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol	-
RFC3768	Virtual Router Redundancy Protocol（version number Two 2004）	-
RFC5798	Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6	-

1.3 原理描述

1.3.1 VRRP 基本概念

如图 1-1 所示，VRRP 协议的基本概念如下：

图1-1 VRRP 备份组示意图



- 虚拟路由器（Virtual Router）：又称 VRRP 备份组，由一个 Master 设备和多个 Backup 设备组成，被当作一个共享局域网内主机的缺省网关。
- Master 设备（Virtual Router Master）：承担转发报文任务的 VRRP 设备。
- Backup 设备（Virtual Router Backup）：一组没有承担转发任务的 VRRP 设备，当 Master 设备出现故障时，它们将通过竞选成为新的 Master 设备。
- VRID：虚拟路由器的标识。
- 虚拟 IP 地址(Virtual IP Address)：虚拟路由器的 IP 地址，一个虚拟路由器可以有一个或多个 IP 地址，由用户配置。
- IP 地址拥有者（IP Address Owner）：如果一个 VRRP 设备将虚拟路由器 IP 地址作为真实的接口地址，则该设备被称为 IP 地址拥有者。如果 IP 地址拥有者是可用的，通常它将成为 Master。
- 虚拟 MAC 地址（Virtual MAC Address）：虚拟路由器根据虚拟路由器 ID 生成的 MAC 地址。一个虚拟路由器拥有一个虚拟 MAC 地址，格式为：00-00-5E-00-01-{VRID}(VRRP for IPv4)；00-00-5E-00-02-{VRID}(VRRP for IPv6)。当虚拟路由器回应 ARP 请求时，使用虚拟 MAC 地址，而不是接口的真实 MAC 地址。
- 主 IP 地址（Primary IP Address）：从接口的真实 IP 地址中选出来的一个主用 IP 地址，通常选择配置的第一个 IP 地址。VRRP 广播报文使用主 IP 地址作为 IP 报文的源地址。

- 优先级（Priority）：虚拟路由器中 VRRP 设备的优先级。虚拟路由器根据优先级选举出 Master 设备和 Backup 设备。
- 抢占模式：在抢占模式下，如果 Backup 设备的优先级比当前 Master 设备的优先级高，则主动将自己切换成 Master。
- 非抢占模式：在非抢占模式下，只要 Master 设备没有出现故障，Backup 设备即使随后被配置了更高的优先级也不会成为 Master 设备。

1.3.2 VRRP 协议报文

VRRP 协议报文封装在 IP 报文中，发送到分配给 VRRP 的 IP 组播地址。在 IP 报文头中，源地址为发送报文接口的主 IP 地址（不是虚拟 IP 地址），目的地址是 224.0.0.18，TTL 是 255，协议号是 112。

目前，VRRP 协议包括两个版本：VRRPv2 和 VRRPv3，VRRPv2 仅适用于 IPv4 网路，VRRPv3 适用于 IPv4 和 IPv6 两种网络。VRRPv2 和 VRRPv3 的主要区别为：

- 支持的网络类型不同。VRRPv3 适用于 IPv4 和 IPv6 两种网络，而 VRRPv2 仅适用于 IPv4 网络。
- 认证功能不同。VRRPv3 不支持认证功能，而 VRRPv2 支持认证功能。
- 发送通告报文的时间间隔的单位不同。VRRPv3 支持的是厘秒级，而 VRRPv2 支持的是秒级。

基于不同的网络类型，VRRP 还可以分为 VRRP for IPv4 和 VRRP for IPv6（简称 VRRP6）。VRRP for IPv4 支持 VRRPv2 和 VRRPv3，而 VRRP for IPv6 仅支持 VRRPv3。

配置 VRRP 协议的版本示例：

步骤 1 执行命令 system-view，进入系统视图。

```
<Quidway> system-view
```

步骤 2 执行命令 vrrp version { v2 | v3 }，配置当前设备的 VRRP 协议版本号。

#缺省情况下，VRRP 协议版本号为 v2。此处配置 VRRP 协议版本号为 v3。

```
[Quidway] vrrp version v3
```

步骤 3 （可选）如果选择 v3 版本，还可以执行命令 **vrrp version-3 send-packet-mode** { v2-only | v3-only | v2v3-both }，配置 VRRPv3 发送通告报文的模式。

#缺省情况下，VRRPv3 版本备份组发送通告报文的模式为 v3-only。此处配置通告报文发送模式为 v2v3-both。

```
[Quidway] vrrp version-3 send-packet-mode v2v3-both
```

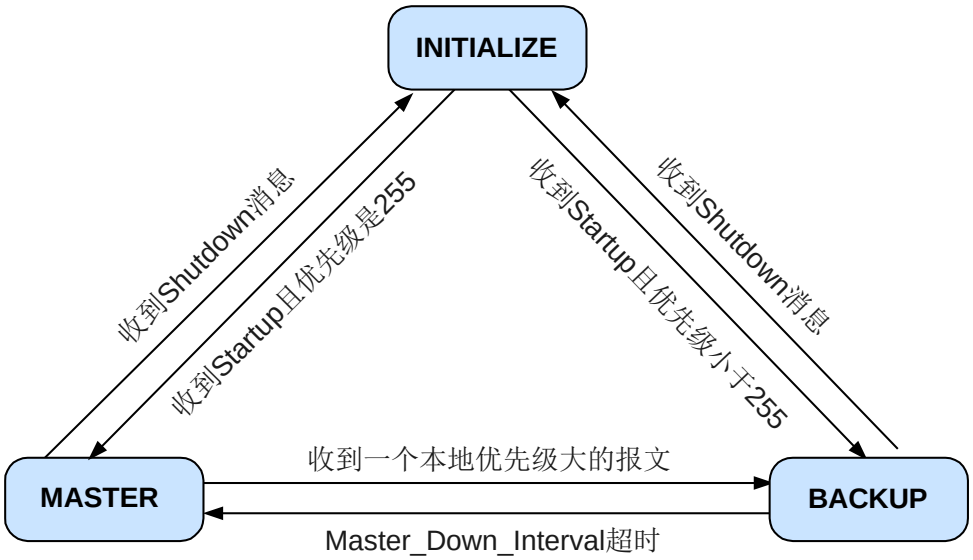
1.3.3 VRRP 工作原理

VRRP 状态机

VRRP 协议中定义了三种状态机：初始状态（Initialize）、活动状态（Master）、备份状态（Backup）。其中，只有处于 Master 状态的设备才可以转发那些发送到虚拟 IP 地址的报文。

VRRP 状态转换如图 1-2 所示：

图1-2 VRRP 状态机转换示意图



VRRP 状态的详细介绍请参见表 1-1。

表1-1 VRRP 协议状态

状态	说明
Initialize	该状态为 VRRP 不可用状态，在此状态时设备不会对 VRRP 报文做任何处理。 通常设备刚启动时或设备检测到故障时会进入 Initialize 状态。
Master	当 VRRP 设备处于 Master 状态时，它将会做下列工作： • 定时（Advertisement_Interval）发送 VRRP 通告报文。 • 以虚拟 MAC 地址响应对虚拟 IP 地址的 ARP 请求。 • 转发目的 MAC 地址为虚拟 MAC 地址的 IP 报文。 • 如果它是这个虚拟 IP 地址的拥有者，则接收目的 IP 地址为这个虚拟 IP 地址的 IP 报文。否则，丢弃这个 IP 报文。
Backup	当 VRRP 设备处于 Backup 状态时，它将会做下列工作： • 接收 Master 设备发送的 VRRP 通告报文，判断 Master 设备的状态是否正常。

状态	说明
	• 对虚拟 IP 地址的 ARP 请求，不做响应。 • 丢弃目的 MAC 地址为虚拟 MAC 地址的 IP 报文。 • 丢弃目的 IP 地址为虚拟 IP 地址的 IP 报文。 • 如果收到比自己优先级小的报文时，丢弃报文，不重置 Master_Down_Interval 定时器；如果收到优先级和自己相同的报文，则重置 Master_Down_Interval 定时器，不进一步比较 IP 地址。 说明： Master_Down_Interval 定时器：Backup 设备在该定时器超时后仍未收到通告报文，则会转换为 Master 状态。计算公式如下：Master_Down_Interval=(3* Advertisement_Interval) + Skew_time（偏移时间）。其中，Skew_Time=(256–Priority)/256。

VRRP 工作过程

VRRP 的工作过程如下：

VRRP 备份组中的交换机根据优先级选举出 Master。Master 交换机通过发送免费 ARP 报文，将虚拟 MAC 地址通知给与它连接的设备或者主机，从而承担报文转发任务。

Master 交换机周期性向备份组内所有 Backup 交换机发送 VRRP 通告报文，以公布其配置信息（优先级等）和工作状况。

如果 Master 交换机出现故障，VRRP 备份组中的 Backup 交换机将根据优先级重新选举新的 Master。

VRRP 备份组状态切换时，Master 交换机由一台设备切换为另外一台设备，新的 Master 交换机会立即发送携带虚拟路由器的虚拟 MAC 地址和虚拟 IP 地址信息的免费 ARP 报文，刷新与它连接的主机或设备中的 MAC 表项，从而把用户流量引到新的 Master 交换机上来，整个过程对用户完全透明。

原 Master 交换机故障恢复时，若该设备为 IP 地址拥有者（优先级为 255），将直接切换至 Master 状态。若该设备优先级小于 255，将首先切换至 Backup 状态，且其优先级恢复为故障前配置的优先级。

Backup 交换机的优先级高于 Master 交换机时，由 Backup 交换机的工作方式（抢占方式和非抢占方式）决定是否重新选举 Master。

由此可见，为了保证 Master 交换机和 Backup 交换机能够协调工作，VRRP 需要实现以下功能：

- Master 交换机的选举；
- Master 交换机状态的通告。

下面将从上述两个方面详细介绍 VRRP 的工作过程。

- **Master 交换机的选举**

VRRP 根据优先级来确定虚拟路由器中每台交换机的角色（Master 交换机或 Backup 交换机）。优先级越高，则越有可能成为 Master 交换机。

初始创建的 VRRP 交换机工作在 Initialize 状态，收到接口 Up 的消息后，若此交换机的优先级小于 255，则会先切换至 Backup 状态，待 Master_Down_Interval 定时器超时后再切换至 Master 状态。首先切换至 Master 状态的 VRRP 交换机通过 VRRP 通告报文的交互获知虚拟交换机中其他成员的优先级，进行 Master 的选举：

- 如果 VRRP 报文中 Master 交换机的优先级高于或等于自己的优先级，则 Backup 交换机保持 Backup 状态；
- 如果 VRRP 报文中 Master 交换机的优先级低于自己的优先级，采用抢占方式的 Backup 交换机将切换至 Master 状态，采用非抢占方式的 Backup 交换机仍保持 Backup 状态。

说明：

- 如果多个 VRRP 交换机同时切换到 Master 状态，通过 VRRP 通告报文的交互进行协商后，优先级较低的 VRRP 交换机将切换成 Backup 状态，优先级最高的 VRRP 交换机成为最终的 Master 设备；优先级相同时，VRRP 交换机上 VRRP 备份组所在接口主 IP 地址较大的成为 Master 设备。
- 如果创建的 VRRP 交换机为 IP 地址拥有者，收到接口 Up 的消息后，将会直接切换至 Master 状态。

- **Master 交换机状态的通告**

Master 交换机周期性地发送 VRRP 通告报文，在 VRRP 备份组中公布其配置信息（优先级等）和工作状况。Backup 交换机通过接收到 VRRP 报文的情况来判断 Master 交换机是否工作正常。

- 当 Master 交换机主动放弃 Master 地位（如 Master 交换机退出备份组）时，会发送优先级为 0 的通告报文，用来使 Backup 交换机快速切换成 Master 交换机，而不用等到 Master_Down_Interval 定时器超时。这个切换的时间称为 Skew time，计算方式为：（256－Backup 交换机的优先级）/256，单位为秒。
- 当 Master 交换机发生网络故障而不能发送通告报文的时候，Backup 交换机并不能立即知道其工作状况。等到 Master_Down_Interval 定时器超时后，才会认为 Master 交换机无法正常工作，从而将状态切换为 Master。其中，Master_Down_Interval 定时器取值为：（3×Advertisement_Interval）＋Skew_time，单位为秒。

说明：

在性能不稳定的网络中，网络堵塞可能导致 Backup 交换机在 Master_Down_Interval 期间没有收到 Master 交换机的报文，Backup 交换机则会主动切换为 Master。如果此时原 Master 交换机的报文又到达了，新 Master 交换机将再次切换回 Backup。如此则会出现 VRRP 备份组成员状态频繁切换的现象。为了缓解这种现象，可以配置抢占延时，使得 Backup 交换机在等待了 Master_Down_Interval 后，再等待抢占延迟时间。如在此期间仍没有收到通告报文，Backup 交换机才会切换为 Master 交换机。

VRRP 认证

对于安全程度不同的网络环境，VRRP 支持在通告报文中设定不同的认证方式和认证字。

在安全程度高的网络中，可以采用无认证方式。设备对要发送的 VRRP 通告报文不进行任何认证处理，收到通告报文的设备也不进行任何认证，认为收到的都是真实的、合法的 VRRP 报文。

在有可能受到安全威胁的网络中，可以采用简单字符（Simple）认证方式或 MD5 认证方式。

- 简单字符（Simple）认证：发送 VRRP 通告报文的交换机将认证方式和认证字填充到通告报文中，而收到通告报文的交换机则会将报文中的认证方式和认证字与本端配置的认证方式和认证字进行匹配。如果相同，则认为接收到的报文是合法的 VRRP 通告报文；否则认为接收到的报文是一个非法报文，并丢弃这个报文。
- MD5 认证：发送 VRRP 通告报文的交换机利用 MD5 算法对认证字进行加密，加密后保存在 Authentication Data 字段中。收到通告报文的交换机会对报文中的认证方式和解密后的认证字进行匹配，检查该报文的合法性。

说明：

目前仅 VRRPv2 版本支持认证，VRRPv3 版本不支持认证。

MD5 认证能够提供比简单字符（Simple）认证更高的安全保障。

配置 VRRP 报文的认证方式示例：

步骤 1 执行命令 system-view，进入系统视图。

```
<Quidway> system-view
```

步骤 2 执行命令 interface interface-type interface-number，进入接口视图。

#进入配置了 VRRP 功能的 VLANIF100 的接口视图。

```
[Quidway] interface vlanif 100
```

步骤 3 执行命令 **vrrp vrid virtual-router-id authentication-mode** { **simple** { key | plain key | cipher cipher-key } | **md5** md5-key }，配置 VRRP 报文认证方式。

#配置备份组 1 的认证方式为 MD5 认证，认证字为 hello。

```
[Quidway-Vlanif100] vrrp vrid 1 authentication-mode md5 hello
```

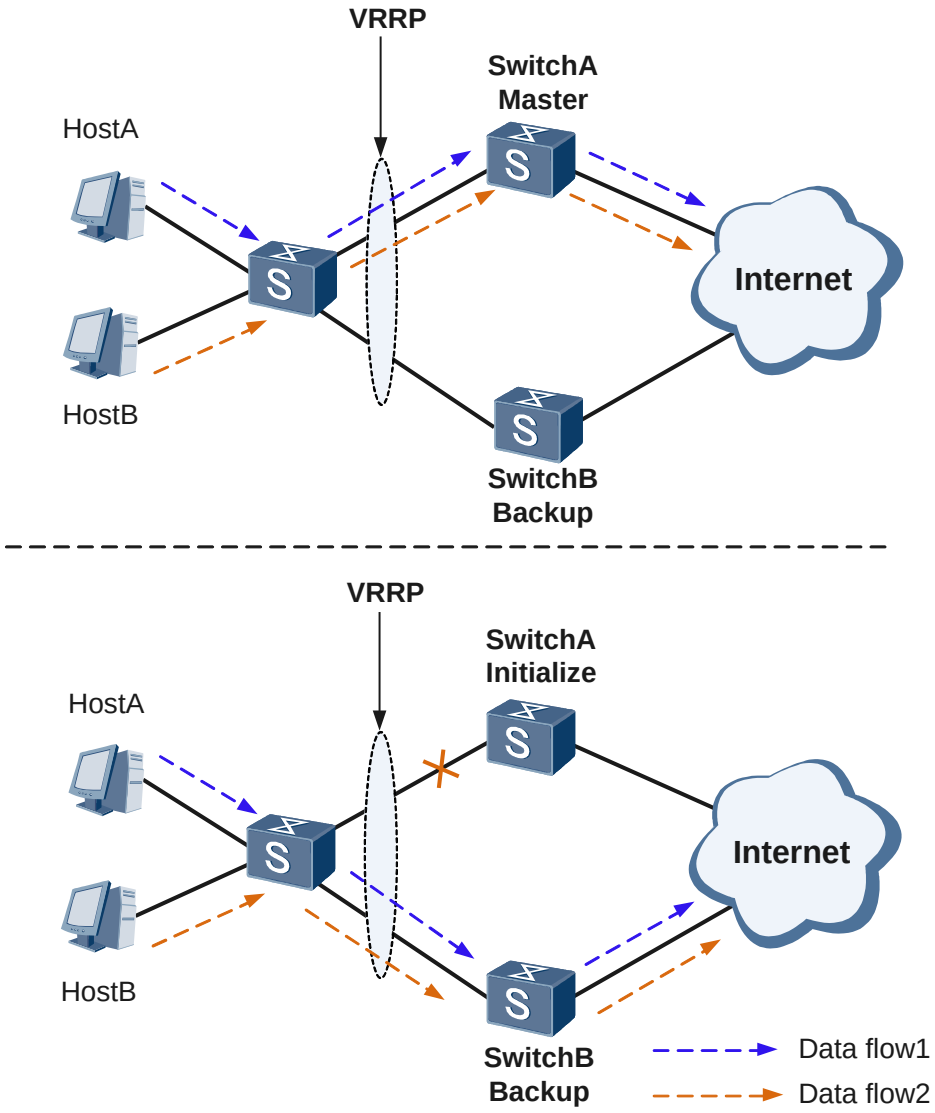
说明：

同一 VRRP 备份组配置的认证方式和认证字必须相同，否则 Master 设备和 Backup 设备无法协商成功。

1.3.4 VRRP 主备备份

主备备份是 VRRP 提供备份功能的基本方式，如图 1-3 所示。该方式需要建立一个虚拟路由器，该虚拟路由器可以包括一个 Master 设备和若干 Backup 设备。

图1-3 VRRP 主备备份示意图



正常情况下，SwitchA 为 Master 设备并承担业务转发任务，SwitchB 为 Backup 设备且不承担业务转发。SwitchA 定期发送 VRRP 通告报文通知 SwitchB 自己工作正常。如果 SwitchA 发生故障，SwitchB 会根据优先级选举成为新的 Master 设备，继续为主机转发数据，实现网关备份的功能。

SwitchA 故障恢复后，在抢占方式下，将重新选举成为 Master；在非抢占方式下，将保持在 Backup 状态。

配置 VRRP 主备备份关键步骤示例：

说明：

这里列举的仅是关键步骤，并非是全部步骤。

在 SwitchA 上创建 VRRP 备份组 1，配置 SwitchA 在该备份组中的优先级为 120，在该备份组中优先级最高，将作为 Master。

```
[SwitchA] interface vlanif 100
```

```
[SwitchA-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchA-Vlanif100] vrrp vrid 1 priority 120
[SwitchA-Vlanif100] vrrp vrid 1 preempt-mode timer delay 20
[SwitchA-Vlanif100] quit
```

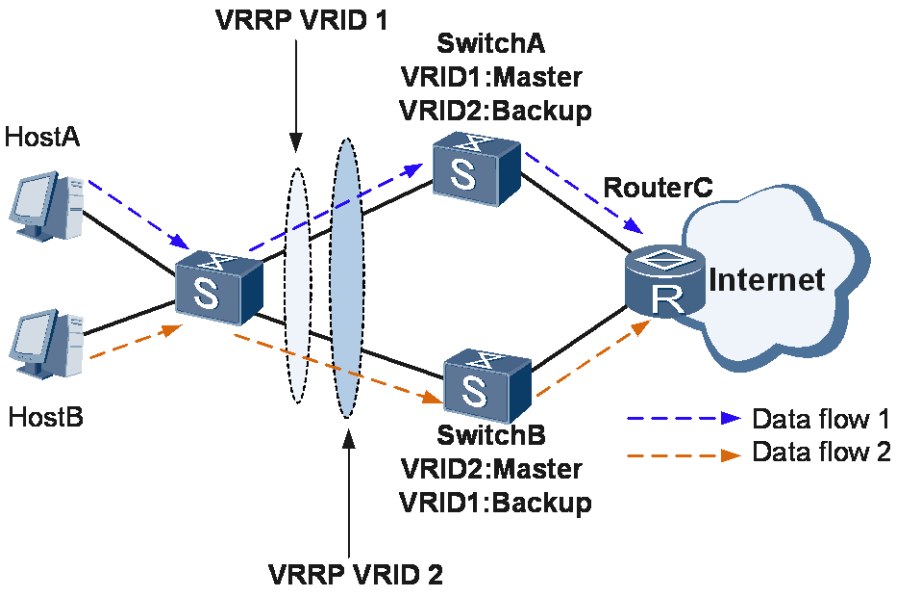
在 SwitchB 上创建 VRRP 备份组 1，其在该备份组中的优先级为缺省值 100。由于优先级使用缺省值，无需再对优先级进行配置。当 Master 出现故障时，将变为 Master，承担流量转发。

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchB-Vlanif100] quit
```

1.3.5 VRRP 负载分担

负载分担是指多个 VRRP 备份组同时承担业务，如图 1-4 所示。VRRP 负载分担与 VRRP 主备备份的基本原理和报文协商过程都是相同的。同样对于每一个 VRRP 备份组，都包含一个 Master 设备和若干 Backup 设备。与主备备份方式不同点在于：负载分担方式需要建立多个 VRRP 备份组，各备份组的 Master 设备可以不同；同一台 VRRP 设备可以加入多个备份组，在不同的备份组中具有不同的优先级。

图1-4 VRRP 负载分担示意图



如图 1-4 所示，配置两个 VRRP 备份组：

- VRRP 备份组 1：SwitchA 为 Master 设备，SwitchB 为 Backup 设备。
- VRRP 备份组 2：SwitchB 为 Master 设备，SwitchA 为 Backup 设备。

一部分用户将 VRRP 备份组 1 作为网关，另一部分用户将 VRRP 备份组 2 作为网关。

这样即可实现对业务流量的负载分担，同时，也起到了相互备份的作用。

配置 VRRP 负载分担关键步骤示例：

说明：

这里列举的仅是关键步骤，并非是全部步骤。

在 SwitchA 和 SwitchB 上创建 VRRP 备份组 1，配置 SwitchA 的优先级为 120，抢占延时为 20 秒，作为 Master 设备，一部分流量将通过 SwitchA 进行转发；SwitchB 的优先级为缺省值，作为 Backup 设备。

```
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchA-Vlanif100] vrrp vrid 1 priority 120
[SwitchA-Vlanif100] vrrp vrid 1 preempt-mode timer delay 20
[SwitchA-Vlanif100] quit
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchB-Vlanif100] quit
```

在 SwitchA 和 SwitchB 上创建 VRRP 备份组 2，配置 SwitchB 的优先级为 120，抢占延时为 20 秒，作为 Master 设备，一部分流量将通过 SwitchB 进行转发；SwitchA 的优先级为缺省值，作为 Backup 设备。

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 2 virtual-ip 10.1.1.112
[SwitchB-Vlanif100] vrrp vrid 2 priority 120
[SwitchB-Vlanif100] vrrp vrid 2 preempt-mode timer delay 20
[SwitchB-Vlanif100] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] vrrp vrid 2 virtual-ip 10.1.1.112
[SwitchA-Vlanif100] quit
```

1.3.6 VRRP 平滑倒换

VRRP 备份组中，Master 设备进行主控板的主备倒换时，从发生主备倒换到新的主控板正常工作期间，Master 设备可能无法正常发送 VRRP 协议报文。Backup 设备在 Master_Down_Interval 定时器超时后，由于未收到 VRRP 通告报文而切换为 Master。当原 Master 设备完成主备倒换后，由于原 Master 设备的优先级高于新 Master 设备，抢占模式下，会重新抢占成为 Master，从而引起链路两次切换，导致系统业务流量的不稳定。

为了避免主备倒换对业务流量的影响，可以在 Master 设备上使能 VRRP 平滑倒换功能。在 VRRP 平滑倒换的过程中，Master 和 Backup 分工不同，相互配合，共同保证业务的平滑传输。

平滑倒换前，必须在 Backup 设备上使能 VRRP 协议报文时间间隔学习功能。使能后，Backup 设备收到通告报文时，会检查报文中的发送时间间隔值，如果和自己的不同，Backup 设备就会学习到报文中的时间间隔，并调整自己的协议报文时间间隔值，与报文中的值保持一致。

Master 设备主控板的主备倒换启动时，首先保存当前配置的 VRRP 通告报文发送间隔，然后调整 VRRP 通告报文发送间隔（一般远大于倒换前的发送间隔），并以新的时间间隔发送通告报文。

Backup 设备收到通告报文后，学习报文中的时间间隔值，并调整自己的定时器，与其保持一致。

倒换结束后，Master 设备恢复倒换前的报文发送间隔，并以新的时间间隔发送通告报文。Backup 设备收到报文后会再一次学习时间间隔。

说明：

- 在平滑倒换的过程中，VRRP 的报文时间间隔学习功能优先于抢占功能，即如果 Backup 状态的 VRRP 收到的协议报文里面的时间间隔和自己当前配置的不一致，并且报文中携带的优先级低于自己当前的配置优先级，这种情况 VRRP 首先考虑的是学习这个时间间隔并重置超时定时器，而后才会考虑是否抢占。
- VRRP 平滑倒换功能还依赖于系统本身，如果设备自身从主备倒换一开始系统便非常繁忙，无法调度 VRRP 模块运行的情况，VRRP 平滑倒换功能无效。

配置 VRRP 平滑倒换关键步骤示例：

说明：

这里列举的仅是关键步骤，并非是全部步骤。

#使能 VRRP 整机平滑倒换功能并配置平滑倒换期间 VRRP 报文中携带的时间间隔。此处配置 VRRP 协议报文发送的时间间隔为 80 秒。

```
<Quidway> system-view
[Quidway] vrrp smooth-switching timer 20
```

说明：

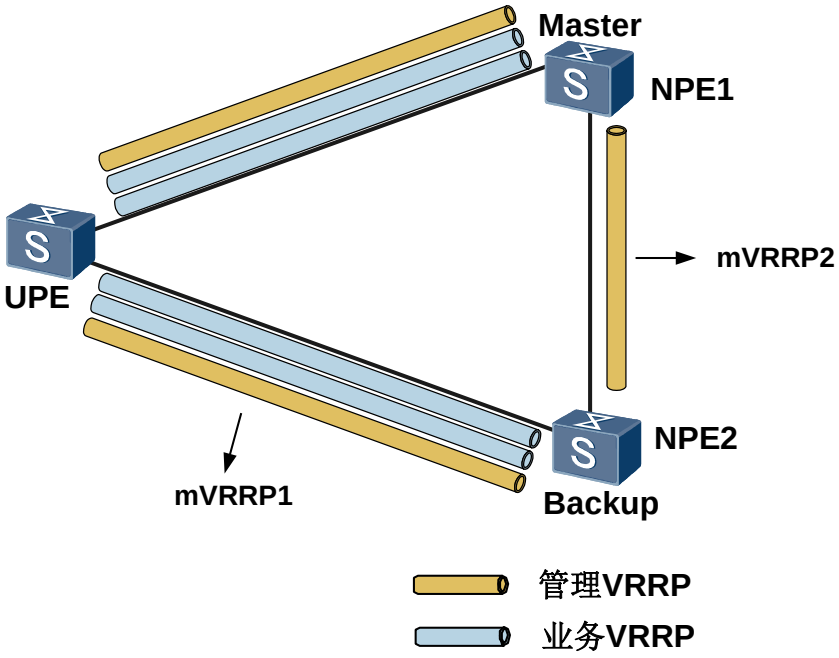
默认情况下，VRRP 整机平滑倒换功能处于使能状态，并且 VRRP 报文携带的默认时间间隔为 100 秒。

1.3.7 管理 VRRP

为了提高网络可靠性，通常部署 NPE 主备双归属。为了满足不同的业务需要，NPE 之间可以运行多个 VRRP 备份组。此时每个 VRRP 备份组都需要维护自己的状态机，这样 NPE 之间就会存在大量的 VRRP 协议报文。

如图 1-5 所示，为了减少协议报文对带宽的占用及 CPU 资源的消耗，可以将其中一个 VRRP 备份组配置为管理 VRRP 备份组（mVRRP），其余的业务 VRRP 备份组与管理 VRRP 备份组进行绑定。此时，管理 VRRP 负责发送协议报文来协商设备的主备状态；业务 VRRP 不发送协议报文，其主备状态与管理 VRRP 的主备保持一致，以此减少协议报文对 CPU 与带宽资源的消耗。

图1-5 管理 VRRP 示意图



管理 VRRP 备份组有两种角色：

- 当管理 VRRP 备份组作为网关使用时（如图 1-5 中的 mVRRP1），管理 VRRP 既负责协商设备的主备状态，也承担业务流量。此时在配置管理 VRRP 之前必须先创建普通 VRRP 备份组并配置虚拟 IP 地址，该虚拟 IP 地址即为用户设置的网关地址。
- 当管理 VRRP 备份组不作为网关使用时（如图 1-5 中的 mVRRP2），管理 VRRP 只负责协商设备的主备状态，不承担业务流量。因此管理 VRRP 不需要具有虚拟 IP 地址，用户可以直接在接口上创建管理 VRRP 备份组。该配置在一定程度上降低了用户维护的复杂度。

配置管理 VRRP 关键步骤示例：

说明：

这里列举的仅是关键步骤，并非是全部步骤。

#将 VRRP 备份组 1 配置为管理 VRRP。

```
[Quidway-Vlanif10] admin-vrrp vrid 1
```

#（可选）配置业务 VRRP 备份组 2 与管理 VRRP 备份组 1 绑定。

```
[Quidway-Vlanif20] vrrp vrid 2 track admin-vrrp interface vlanif 20 vrid 1
unflowdown
```

1.4 应用

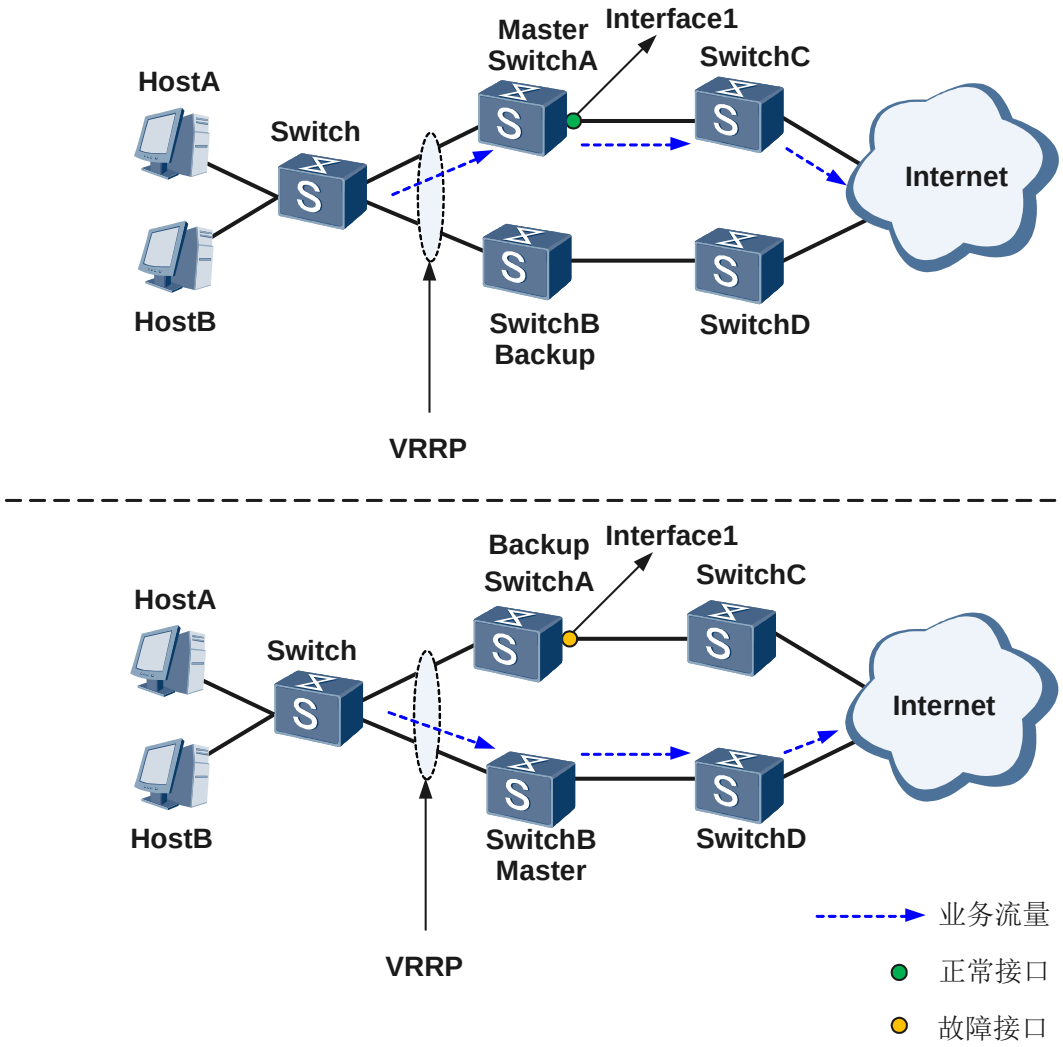
1.4.1 VRRP 与接口状态联动监视上行接口

VRRP 备份组只能感知其所在接口状态的变化，当 VRRP 交换机上行接口或直连链路发生故障时，VRRP 无法感知，此时会引起业务流量中断。通过部署 VRRP 与接口状态联动监视上行接口可以有效地解决上述问题，当 Master 设备的上行接口或直连链路发生故障时，通过调整自身优先级，触发主备切换，确保流量正常转发。

VRRP 可以通过 Increased 和 Reduced 方式来监视接口状态：

- 如果 VRRP 交换机上配置以 Increased 方式监视一个接口，当被监视的接口状态变成 Down 后，该 VRRP 交换机的优先级增加指定值（该值由用户指定）。
- 如果 VRRP 交换机上配置以 Reduced 方式监视一个接口，当被监视的接口状态变为 Down 后，该 VRRP 交换机的优先级降低指定值（该值可由用户指定，缺省值为 10）。

图1-6 VRRP 监视上行接口的组网示意图

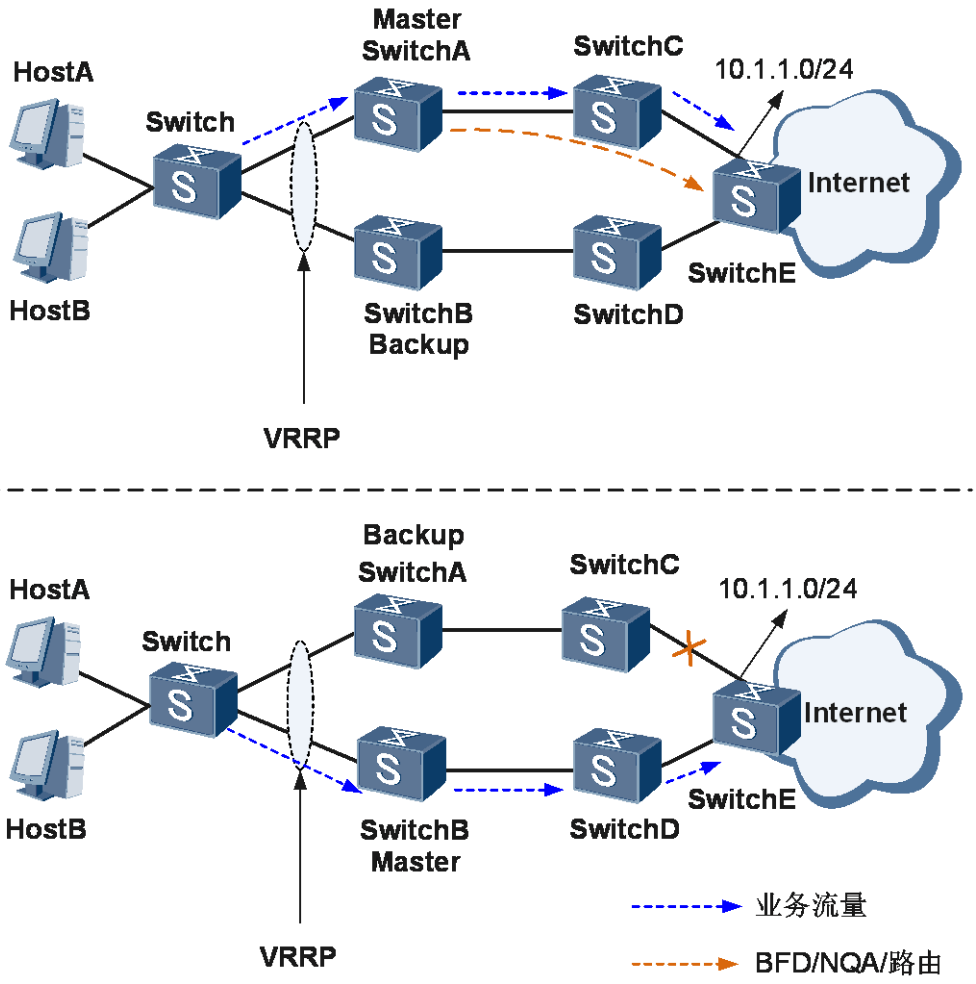


如图 1-6 所示，SwitchA 和 SwitchB 之间配置 VRRP 备份组，其中 SwitchA 为 Master 设备，SwitchB 为 Backup 设备，SwitchA 和 SwitchB 皆工作在抢占方式下。在 SwitchA 上配置以 Reduced 方式监视上行接口 Interface1，当 Interface1 故障时，SwitchA 降低自身优先级，通过报文协商，SwitchB 抢占成为 Master，确保用户流量正常转发。

1.4.2 VRRP 与 BFD/NQA/路由联动监视上行链路

VRRP 只能感知 VRRP 备份组之间的故障，而配置 VRRP 监视上行接口仅能感知 Master 设备上行接口或直连链路的故障，当 Master 设备上行非直连链路故障时，VRRP 无法感知，此时会导致用户流量丢失。通过部署 VRRP 与 BFD/NQA/路由联动监视上行链路，可以有效地解决上述问题。通过配置 BFD/NQA/路由检测 Master 上行链路的连通状况，当 Master 设备的上行链路发生故障时，BFD/NQA/路由可以快速检测故障并通知 Master 设备调整自身优先级，触发主备切换，确保流量正常转发。

图1-7 VRRP 与 BFD/NQA/路由联动监视上行链路典型组网图



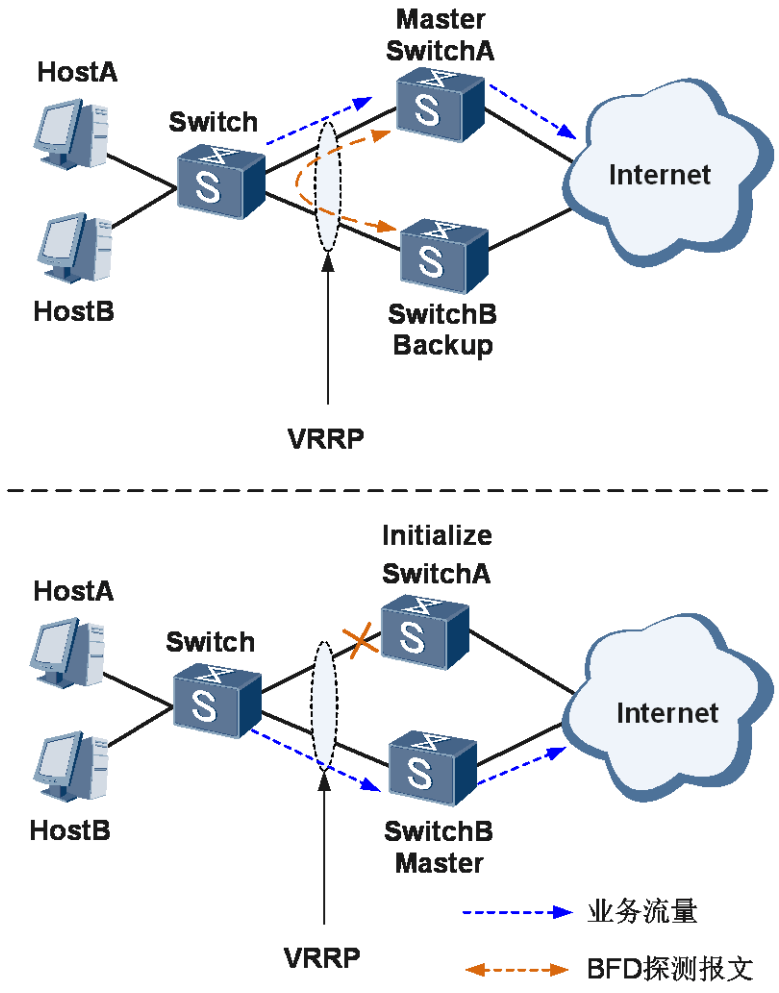
如图 1-7 所示，SwitchA 和 SwitchB 之间配置 VRRP 备份组，其中 SwitchA 为 Master 设备，SwitchB 为 Backup 设备，SwitchA 和 SwitchB 皆工作在抢占方式下。配置 BFD/NQA/路由监测 SwitchA 到 SwitchE 之间的链路，并在 SwitchA 上配置以 VRRP 与 BFD/NQA/路由联动。当 BFD/NQA/路由检测到 SwitchC 到 SwitchE 之间的链路故障

时，通知 SwitchA 降低自身优先级，通过报文协商，SwitchB 抢占成为 Master，确保用户流量正常转发。

1.4.3 VRRP 与 BFD 联动实现快速切换

VRRP 备份组通过收发 VRRP 协议报文进行主备状态的协商，以实现设备的冗余备份功能。当 VRRP 备份组之间的链路出现故障时，Backup 设备需要等待 Master_Down_Interval 后才能感知故障并切换为 Master 设备，切换时间通常在 3 秒以上。在等待切换期间内，业务流量仍会发往 Master 设备，此时会造成用户数据丢失。通过部署 VRRP 与 BFD 联动功能，可以有效解决上述问题。通过在 Master 设备和 Backup 设备之间建立 BFD 会话并与 VRRP 备份组进行绑定，快速检测 VRRP 备份组之间的连通状态，并在出现故障时及时通知 VRRP 备份组进行主备切换，实现了毫秒级的切换速度，减少了流量丢失。

图1-8 VRRP 与 BFD 联动实现快速切换的组网示意图



如图 1-8 所示，SwitchA 和 SwitchB 之间配置 VRRP 备份组，SwitchA 为 Master 设备，SwitchB 为 Backup 设备，用户侧的流量通过 SwitchA 转发。SwitchA 和 SwitchB 皆工作在抢占方式下，其中 SwitchA 为延时抢占，SwitchB 为立即抢占。在 SwitchA 和 SwitchB 两端配置 BFD 会话，并在 SwitchB 上配置 VRRP 与 BFD 联动。

当 VRRP 备份组间出现故障时，BFD 快速检测故障并通知 SwitchB 增加指定的优先级（此时 SwitchB 的优先级须高于 SwitchA 的优先级），SwitchB 立即抢占为 Master，用户侧流量通过 Switch 转发，实现了主备的快速切换。

1.5 故障处理案例

1.5.1 同一个备份组内出现多个 Master 设备

故障现象

一个 VRRP 备份组内，长时间存在多个 Master 设备。

处理步骤

步骤 1 在多个 Master 设备间执行 ping 操作，检查各 Master 设备之间的网络连接情况

如果无法 ping 通，请检查网络连接是否正确。

如果可以 ping 通，请执行步骤 2。

步骤 2 在任意视图下执行 **display vrrp protocol-information** 命令，检查各 Master 设备配置的 VRRP 版本和报文发送方式是否兼容

如果各 Master 设备配置的版本和发送方式不能兼容，请在系统视图下执行 **vrrp version** { v2 | v3 }命令更改为相同的版本。

如果各 Master 设备配置的版本和发送方式可以兼容，请执行步骤 3。

说明：

- v2 版本的 VRRP 备份组，只能发送和接收 v2 版本的 VRRP 通告报文，如果接收到 v3 版本的 VRRP 通告报文，则该备份组将此报文丢弃。
- v3 版本的 VRRP 备份组，可以接收 v2 和 v3 版本的 VRRP 通告报文，支持配置报文发送方式为 v2–only、v3–only 或 v2v3–both。

步骤 3 在任意视图下执行 **display vrrp virtual-router-id** 命令，检查各 Master 设备配置的虚拟 IP 地址、通告报文发送间隔、认证方式及认证字是否一致

- 如果配置的虚拟 IP 地址不一致，请执行 **vrrp vrid** virtual-router-id virtual-ip virtual-address 命令更改为一致的虚拟 IP 地址。
- 如果配置的通告报文发送间隔不一致，请执行 **vrrp vrid** virtual-router-id **timer advertise** advertise-interval 命令更改为一致的发送间隔。
- 如果配置的认证方式及认证字不一致，请执行 **vrrp vrid** virtual-router-id **authentication-mode** { **simple** { key | plain key | cipher cipher-key } | **md5** md5-key } 命令更改为一致的认证方式及认证字。

1.5.2 VRRP 主备状态频繁切换

故障现象

VRRP 备份组中，设备主备状态频繁切换。

处理步骤

步骤 1 在任意视图下执行 **display vrrp** virtual-router-id 命令，查看当前 VRRP 备份组有无联动接口、BFD 及 NQA 等

- 如果配置了联动接口、BFD 及 NQA 等，接口、BFD 及 NQA 状态的震荡会引起 VRRP 主备状态震荡，请排除所联动模块的故障。
- 如果没有配置联动功能，请执行步骤 2。

步骤 2 在任意视图下执行 **display vrrp** virtual-router-id 命令，查看当前 VRRP 备份组配置的抢占延迟时间

- 如果配置的抢占延迟时间为 0，请在 VRRP 备份组所在的接口视图下执行 **vrrp vrid** virtual-router-id **preempt-mode timer delay** delay-value 命令配置非 0 的抢占延迟时间。
- 如果配置的抢占时间为非 0，请执行步骤 3。

步骤 3 在当前 VRRP 备份组所在的接口视图下执行 **vrrp vrid** virtual-router-id **timer advertise** advertise-interval 命令配置更大的通告报文发送间隔，或执行 **vrrp vrid** virtual-router-id **preempt-mode timer delay** delay-value 命令配置更大的抢占延迟时间。

1.6 FAQ

1.6.1 VRRP 备份组虚拟 IP 地址为何无法 ping 通？

为了防止 VRRP 备份组可能遭受 ICMP 攻击的隐患，有的时候会执行命令 **undo vrrp virtual-ip ping enable** 关闭虚拟 IP 地址的 ping 功能，这样将无法 ping 通 VRRP 备份组的虚拟 IP 地址。如果需要 ping 通 VRRP 备份组的虚拟 IP 地址，可以在系统视图下执行 **vrrp virtual-ip ping enable** 命令，开启 VRRP 组虚拟 IP 地址 ping 功能。

1.6.2 如何来调整 VRRP 的免费 ARP 发送的频率？

缺省情况下，Master 每 2 分钟发送一次免费 ARP 报文。可以通过命令 **vrrp gratuitous-arp timeout** 来调整免费 ARP 报文的发送频率。

1.6.3 VRRP 报文在 Super-VLAN 中发送时，为什么在 VRRP 主备间的链路上不让第一个子 VLAN 通过，则 VRRP 报文收发不正常？

缺省情况下，Super-VLAN 仅向自己的状态为 Up 的 VLAN ID 最小的 Sub-VLAN 发送 VRRP 通告报文。可以通过 **vrrp advertise send-mode** 来取消或设置 Super-VLAN 中的 VRRP 通告报文的发送方式。

1.6.4 交换机的 RRPP 和 VRRP 功能可以同时使用吗？

交换机可以同时配置 RRPP 和 VRRP 功能。

1.7 术语与缩略语

术语与缩略语	英文全称	中文全称
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议
ARP	Address Resolution Protocol	地址解析协议
BFD	Bidirectional Forwarding Detection	双向转发检测
L2VPN	Layer 2 virtual private network	二层虚拟专用网
PW	Pseudo Wire	虚电线
VSI	Virtual Switching Instance	虚拟交换实例
QinQ	802.1Q in 802.1Q	802.1Q 嵌套 802.1Q
ME	Metro Ethernet	城域以太
mVRRP	Manage Virtual Router Redundancy Protocol	管理 VRRP
mVPLS	Manage Virtual Private LAN Service	管理 VPLS
mVSI	Manage Virtual Switching Instance	管理 VSI