

目 录

第 1 章 VRRP配置	1-1
1.1 VRRP简介	1-1
1.2 VRRP配置	1-1
1.3 VRRP典型案例	1-3
1.4 VRRP排错帮助	1-4
第 2 章 IPv6 VRRPv3 配置	2-1
2.1 VRRPv3 简介.....	2-1
2.1.1 VRRPv3 报文结构.....	2-2
2.1.2 VRRPv3 工作原理.....	2-2
2.2 VRRPv3 配置.....	2-3
2.2.1 配置任务序列.....	2-3
2.3 VRRPv3 典型案例	2-5
2.4 VRRPv3 排错帮助	2-6
第 3 章 MRPP配置	3-1
3.1 MRPP简介	3-1
3.1.1 概念介绍	3-1
3.1.2 MRPP协议报文类型	3-2
3.1.3 MRPP协议运行机制	3-3
3.2 MRPP配置任务序列.....	3-3
3.3 MRPP典型案例	3-5
3.4 MRPP排错帮助	3-7
第 4 章 ULPP配置.....	4-1
4.1 ULPP简介	4-1
4.2 ULPP配置任务序列	4-2
4.3 ULPP典型案例.....	4-4
4.3.1 ULPP典型案例 1	4-4

4.3.2 ULPP典型案例 2	4-6
4.4 ULPP排错帮助.....	4-8
第 5 章 ULSM配置	5-1
5.1 ULSM简介	5-1
5.2 ULSM配置任务序列	5-2
5.3 ULSM典型案例	5-3
5.4 ULSM排错帮助	5-4
第 6 章 HA配置	6-1
6.1 HA简介	6-1
6.2 HA配置任务序列	6-2
6.3 HA典型案例	6-3

第1章 VRRP配置

1.1 VRRP简介

VRRP (Virtual Router Redundancy Protocol, 虚拟路由器冗余协议) 是一种容错协议, 其目的是利用备份机制来提高路由器 (或三层以太网交换机) 与外界连接的可靠性。它是为具有多播或广播能力的局域网 (最明显的例子就是以太网) 而设计的, 由 IETF 提出, 目前应用比较广泛。

通常, 一个局域网内的所有主机都会设置一条缺省路由以指明缺省网关, 主机发出的那些目的地址不在本网段的报文将通过该缺省路由发往缺省网关, 从而实现了局域网内各主机与外部网络的通信。然而, 当作为缺省网关的路由器与外部网络相连的通信链路出现故障后, 本网段内所有以该网关为缺省路由下一跳的各主机将被迫中断与外部网络的通信。

VRRP 就是为解决上述问题而提出的。VRRP 运行于局域网的多台路由器上, 它将这几台路由器组织成一台“虚拟”路由器, 或称为一个备份组。在这个备份组中, 有一个活动路由器 (被称为 Master) 和一个或多个备份路由器 (被称为 Backup)。活动路由器将实际承担这个“虚拟”路由器的工作任务 (如负责转发各主机送给“虚拟”路由器的报文), 而备份路由器则作为活动路由器的备份。

在运行的时候, 这个“虚拟”路由器拥有自己的“虚拟”IP 地址, 备份组内的路由器也有自己的 IP 地址。但是, 由于 VRRP 只在路由器或以太网交换机上运行, 所以对于该网段上的各主机来说, 这个备份组是透明的, 它们仅仅知道这个“虚拟”路由器的“虚拟”IP 地址, 而并不知道 Master 以及 Backup 的实际 IP 地址, 因此它们将把自己的缺省网关地址设置为该“虚拟”路由器的“虚拟”IP 地址。于是, 本局域网内的各主机就通过这个“虚拟”路由器来与其它网络进行通信。而实际上, 它们是通过 Master 在与其它网络进行通信。而一旦备份组内的 Master 发生故障, Backup 将会接替其工作, 成为新的 Master, 继续为本局域网内的各主机提供服务, 从而保障本局域网内的各主机可以不间断与外部网络的通信。

我们可以总结一下: 在 VRRP 备份组内, 总有一台路由器或以太网交换机是活动路由器 (Master), 它完成“虚拟”路由器的工作; 该备份组中其它的路由器或以太网交换机作为备份路由器 (Backup, 可以不只一台), 随时监控 Master 的活动。当原有的 Master 出现故障时, 各 Backup 将自动选举出一个新的 Master 来接替其工作, 继续为网段内各主机提供路由服务。由于这个选举和接替阶段短暂而平滑, 因此, 网段内各主机仍然可以正常地使用虚拟路由器, 实现不间断地与外界保持通信。

1.2 VRRP配置

配置任务序列:

1. 创建/删除虚拟路由器 (必须)

2. 配置 VRRP 虚拟 IP 和接口（必须）
3. 启动/关闭虚拟路由器（必须）
4. 配置 VRRP 辅助参数（可选）
 - （1）配置 VRRP 抢占模式
 - （2）配置 VRRP 优先级
 - （3）配置 VRRP 定时器时间间隔
 - （4）配置 VRRP 对接口的监控
 - （5）配置 VRRP 会话监控端口的状态

1. 创建/删除虚拟路由器

命令	解释
全局配置模式	
router vrrp <vrid> no router vrrp <vrid>	创建/删除虚拟路由器。

2. 配置 VRRP 虚拟 IP 和接口

命令	解释
VRRP 协议配置模式	
virtual-ip < ip > no virtual-ip	配置 VRRP 虚拟 IP，no 命令删除虚拟 IP。
interface {IFNAME Vlan <ID>} no interface	配置 VRRP 接口，no 命令删除该接口。

3. 启动/关闭虚拟路由器

命令	解释
VRRP 协议配置模式	
enable	启动该虚拟路由器。
disable	关闭该虚拟路由器。

4. 配置 VRRP 辅助参数

（1）配置 VRRP 抢占模式

命令	解释
VRRP 协议配置模式	
preempt-mode {true false}	配置 VRRP 的抢占模式。

（2）配置 VRRP 优先级

命令	解释
VRRP 协议配置模式	
priority < priority >	配置 VRRP 优先级。

（3）配置 VRRP 定时器时间间隔

命令	解释
VRRP 协议配置模式	

advertisement-interval <time>	配置 VRRP 定时器时间值(单位为秒)。
--	-----------------------

(4) 配置 VRRP 对接口的监控

命令	解释
VRRP 协议配置模式	
circuit-failover {IFNAME Vlan <ID>} <value_reduced> no circuit-failover	配置 VRRP 对接口的监控，no 命令删除对接口的监控。

(5) 配置 VRRP 会话监控端口的状态

命令	解释
VRRP 协议配置模式	
vrrp track interface {ethernet IFNAME IFNAME} priority <priority_value> no vrrp track interface {ethernet IFNAME IFNAME}	配置 VRRP 会话监控端口的状态。

1.3 VRRP典型案例

如下图，SwitchA 和 SwitchB 为在同一组内互为备份的三层以太网交换机。

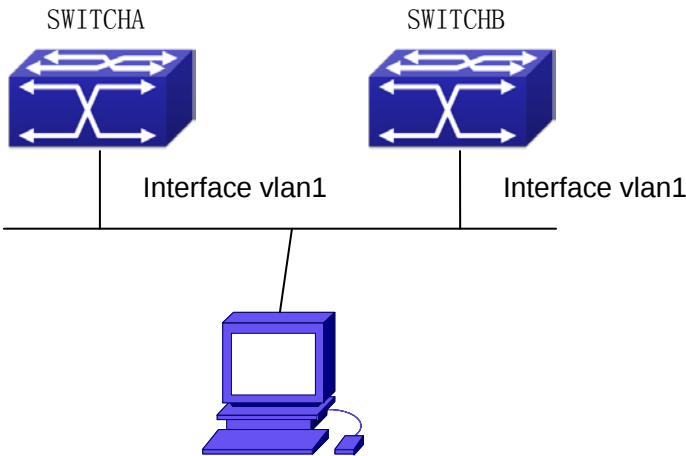


图 1-1 VRRP 网络拓扑示意图

SwitchA 的配置:

```
SwitchA(config)#interface vlan 1
SwitchA(Config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0
SwitchA(config)#router vrrp 1
SwitchA(config-router)#virtual-ip 10.1.1.5
```

```
SwitchA(config-router)#interface vlan 1
```

```
SwitchA(config-router)#enable
```

SwitchB 的配置:

```
SwitchB(config)#interface vlan 1
```

```
SwitchB (Config-if-Vlan1)#ip address 10.1.1.7 255.255.255.0
```

```
SwitchB (config)#router vrrp 1
```

```
SwitchB (config-router)#virtual-ip 10.1.1.5
```

```
SwitchB (config-router)#interface vlan 1
```

```
SwitchB (config-router)#enable
```

1.4 VRRP排错帮助

在配置、使用 VRRP 协议时，可能会由于物理连接、配置错误等原因导致 VRRP 协议未能正常运行。因此，用户应注意以下要点：

- ☞ 首先应该保证物理连接的正确无误；
- ☞ 其次，保证接口和链路协议是 UP（使用 `show interface` 命令）；
- ☞ 然后，确保在接口上已启动了 VRRP 协议；检查同一备份组内的不同路由器（或三层以太网交换机）认证是否相同；
- ☞ 检查同一备份组内的不同路由器（或三层以太网交换机）配置的 timer 时间是否相同；
- ☞ 检查虚拟 IP 地址是否和接口真实 IP 地址在同一网段内；
- ☞ 如果通过上述检查仍无法解决 VRRP 的问题，那么请使用 `debug vrrp` 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

第2章 IPv6 VRRPv3 配置

2.1 VRRPv3 简介

VRRPv3 是针对 IPv6 的虚拟路由冗余协议，它是基于 IPv4 环境下的 VRRP(VRRPv2) 来设计的，下面对其进行简要介绍。

在基于 TCP/IP 协议的网络中，为了保证不直接物理连接的设备之间的通信，必须指定路由。目前常用的指定路由的方法有两种：一种是通过路由协议（比如：内部路由协议 RIP 和 OSPF）动态学习；另一种是静态配置。在每一个终端都运行动态路由协议是不现实的，大多客户端操作系统平台都不支持动态路由协议，即使支持也受到管理开销、收敛度、安全性等许多问题的限制。因此普遍采用对终端 IP 设备静态路由配置，一般是给终端设备指定一个或者多个默认网关(Default Gateway)。静态路由的方法简化了网络管理的复杂度和减轻了终端设备的通信开销，但是它仍然有一个缺点：如果作为默认网关的路由器损坏，所有使用该网关为下一跳主机的通信必然要中断。即便配置了多个默认网关，如不重新启动终端设备，也不能切换到新的网关。采用虚拟路由冗余协议 (VRRP) 可以很好的避免静态指定网关的缺陷。

在 VRRP 协议中，有两组重要的概念：VRRP 路由器和虚拟路由器，主控路由器(Master) 和备份路由器(Backup)。VRRP 路由器是指运行 VRRP 的路由器，是物理实体；虚拟路由器是指 VRRP 协议创建的，是逻辑概念。一组 VRRP 路由器协同工作，共同构成一台虚拟路由器。该虚拟路由器对外表现为一个具有唯一固定 IP 地址和 MAC 地址的逻辑路由器。处于同一个 VRRP 组中的路由器具有两种互斥的角色：主控路由器和备份路由器，一个 VRRP 组中有且只有一台处于主控角色的路由器，可以有一个或者多个处于备份角色的路由器。VRRPv3 协议使用选择策略从路由器组中选出一台作为主控，负责 ND(Neighbor Discovery, 邻居发现)邻居请求消息(IPv4 为 ARP)回应和转发 IP 数据包，组中的其它路由器作为备份的角色处于待命状态。当由于某种原因主控路由器发生故障时，备份路由器能在几秒钟的时延后升级为主路由器。由于此切换非常迅速而且不用改变 IP 地址和 MAC 地址，故对终端使用者系统是透明的。

在 IPv6 环境下，局域网中的主机通常通过邻居发现协议(NDP)而学习到默认网关，这是基于定期接收路由器通告消息来实现的。IPv6 的邻居发现协议中存在一种叫做邻居不可达性检测(Neighbor Unreachability Detection)的机制，该机制通过向邻居节点发送单播的邻居请求消息来检测邻居节点是否失败。为了降低发送邻居请求消息的开销，邻居请求消息只被发送到那些正在发送流量的邻居节点，并且是在一段时间内没有路由器 UP 状态的指示以后才发送的。在邻居不可达性检测机制中，如果采用默认参数，需要花费大约 38 秒才能检测到某个路由器不可达，这种延迟对用户来说非常可观，并且可能引起某些传输协议超时。与 NDP 相比，VRRP 提供了快速的默认网关切换。在 VRRP 中，备份路由器能够在大约 3

秒(默认参数)的时间内接管失效的主控路由器，并且该过程不需要与主机进行任何交互，即对主机是透明的。

2.1.1 VRRPv3 报文结构

VRRPv3 具有自己的报文格式，VRRP 报文用来在备份组内交流路由器的优先级和 Master 的状态，VRRPv3 报文是封装在 IPv6 报文中来发送的，它们被发送到指定的 IPv6 组播地址。VRRPv3 的报文格式如图 1 所示。其中封装 VRRPv3 报文的 IPv6 报文中的源地址为报文出接口的 IPv6 链路本地地址，目的地址为 IPv6 组播地址(分配给 VRRPv3 的组播地址为 FF02:0:0:0:0:0:0:12)，跳数限制必须为 255，下一报头为 112(表示 VRRP 报文)。

- VRRPv3 报文的各个域所代表的含义如下：
- Version: VRRPv3 版本，值为 3；
 - Type: VRRP 报文类型，只有一种类型 ADVERTISEMENT，值为 1；
 - Virtual Rtr ID: 虚拟路由器 ID；
 - Priority: 优先级，取值范围为 0~255；
 - Count IPv6 Addr: VRRPv3 报文中包含的 IPv6 地址个数，最小值为 1；
 - Rsvd: 保留域，值为 0；
 - Adver Int: VRRPv3 报文通告时间间隔，单位为厘秒；
 - Checksum: 校验和，计算范围为整个 VRRPv3 报文和一个 IPv6 伪头(具体请参考 RFC2460)；
- IPv6 Address(es): 一个或多个关联于虚拟路由器的 IPv6 地址,地址个数和“Count IPv6 Addr”相同，其中第一个地址必须为虚拟路由器的虚拟 IPv6 地址。

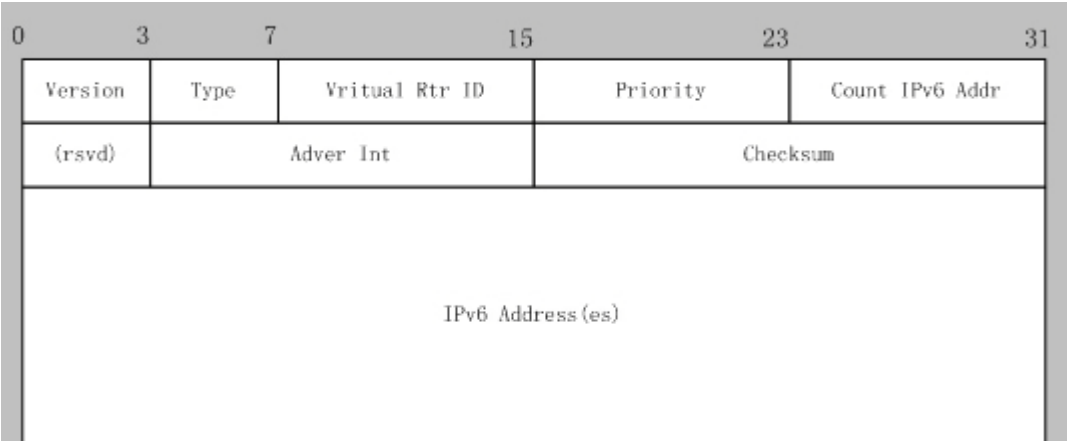


图 2-1 VRRPv3 报文

2.1.2 VRRPv3 工作原理

VRRPv3 的工作原理和 VRRPv2 的工作原理基本相同，主要是通过 VRRP 通告报文的交互来进行的，现简要描述如下。

一个 VRRP 路由器有唯一的标识：VRID，范围为 1-255。该路由器对外表现为唯一的虚拟 MAC 地址，VRRPv3 的虚拟 MAC 地址的格式为 00-00-5E-00-02-{VRID}(VRRPv2 的

虚拟 MAC 地址格式为 00-00-5E-00-01-{VRID})。主控路由器负责对 ND 邻居请求(VRRPv2 为 ARP 请求)用该 MAC 地址做应答。这样，无论如何切换，保证给终端设备的是唯一一致的 IP 和 MAC 地址，减少了切换对终端设备的影响。

VRRP 控制报文只有一种：VRRP 通告(advertisement)。它使用 IP 组播数据包进行封装，组地址格式为 FF02:0:0:0:0:0:XXXX:XXXX。为了保持与 VRRPv2 中组地址(224.0.0.18)的一致性，VRRPv3 通告报文所使用的组播地址可以为 FF02:0:0:0:0:0:0:12，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。为了减少网络带宽消耗，只有主控路由器才可以周期性的发送 VRRP 通告报文。备份路由器在连续 3 个通告间隔内收不到 VRRP 通告或收到优先级为 0 的通告后启动新一轮的 VRRP 选举。

在 VRRP 路由器组中，按优先级选举主控路由器，VRRP 协议中优先级范围是 0-255。若 VRRP 路由器的 IP 地址和虚拟路由器的接口 IP 地址相同，则称该虚拟路由器作 VRRP 组中的 IP 地址所有者；IP 地址所有者自动具有最高优先级：255。优先级 0 一般用在 IP 地址所有者主动放弃主控者角色时使用。可配置的优先级范围为 1-254。优先级的配置原则可以依据链路的速度和成本、路由器性能和可靠性以及其它管理策略设定。主控路由器的选举中，高优先级的虚拟路由器获胜，因此，如果在 VRRP 组中有 IP 地址所有者，则它总是作为主控路由的角色出现。对于相同优先级的候选路由器，按照 IP 地址大小顺序选举(地址大者优先)。VRRP 还提供了优先级抢占策略，如果配置了该策略，高优先级的备份路由器便会剥夺当前低优先级的主控路由器而成为新的主控路由器。

为了避免 Ping 虚拟 IP 时返回物理 MAC 地址的错误，这里规定虚拟 IP 不能为接口的真实 IP。这样，所有参与备份组选举的接口默认都是 Backup。

2.2 VRRPv3 配置

2.2.1 配置任务序列

- 1. 创建/删除虚拟路由器（必须）
- 2. 配置 VRRPv3 的虚拟 IPv6 地址和接口（必须）
- 3. 启动/关闭虚拟路由器（必须）
- 4. 配置 VRRPv3 辅助参数（可选）
 - (1) 配置 VRRPv3 抢占模式
 - (2) 配置 VRRPv3 优先级
 - (3) 配置 VRRPv3 通告时间间隔
 - (4) 配置 VRRPv3 的监控接口

1. 创建/删除虚拟路由器

命令	解释
全局配置模式	
router ipv6 vrrp <vrid> no router ipv6 vrrp <vrid>	创建/删除 VRRPv3 虚拟路由器。

2. 配置 VRRPv3 虚拟 IPv6 地址和接口

命令	解释
VRRPv3 协议配置模式	
virtual-ipv6 <ipv6-address> Interface {Vlan <ID> IFNAME } no virtual-ipv6 interface	配置 VRRPv3 虚拟 IPv6 地址和接口，no 命令删除虚拟 IPv6 地址和接口。

3. 启动/关闭虚拟路由器

命令	解释
VRRPv3 协议配置模式	
enable	启动该虚拟路由器。
disable	关闭该虚拟路由器。

4. 配置 VRRPv3 辅助参数

(1) 配置 VRRPv3 抢占模式

命令	解释
VRRPv3 协议配置模式	
preempt-mode {true false}	配置 VRRPv3 的抢占模式。

(2) 配置 VRRPv3 优先级

命令	解释
VRRPv3 协议配置模式	
priority < priority >	配置 VRRPv3 优先级。

(3) 配置 VRRPv3 通告时间间隔

命令	解释
VRRPv3 协议配置模式	
advertisement-interval <time>	配置 VRRPv3 通告时间间隔(单位为厘秒)。

(4) 配置 VRRPv3 的监控接口

命令	解释
VRRPv3 协议配置模式	
circuit-failover {vlan <ID> IFNAME} <value_reduced> no circuit-failover	配置 VRRPv3 的监控接口，no 命令删除监控接口。

2.3 VRRPv3 典型案例

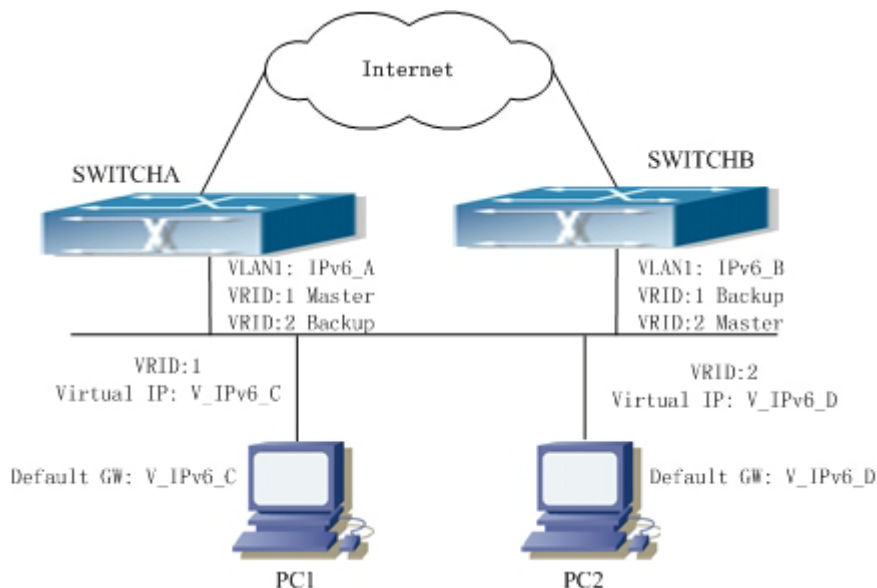


图 2-2 VRRPv3 典型网络拓扑

如图所示，其中交换机 A 和交换机 B 互为备份，交换机 A 为备份组 1 的 Master，同时是备份组 2 的 Backup，交换机 B 为备份组 2 的 Master，同时是备份组 1 的 Backup。交换机 A 和交换机 B 的 VLAN1 接口 IPv6 地址分别为“IPv6_A”和“IPv6_B”(IPv6_A 和 IPv6_B 建议为同一个网段)，备份组 1 和备份组 2 的虚拟 IPv6 地址分别为“V_IPv6_C”和“V_IPv6_D”，主机 1 和主机 2 的缺省 IPv6 网关地址分别配置为“V_IPv6_C”和“V_IPv6_D”(在实际应用当中，主机的 IPv6 网关地址通常是通过路由公告而自动学习到的，这样主机的 IPv6 下一跳地址就具有一定的随机性)。这样不仅实现了路由备份，还具有局域网内的流量分担功能。

SwitchA 的配置：

```
SwitchA(config)#interface vlan 1
SwitchA(config)#router ipv6 vrrp 1
SwitchA(config-router)#virtual-ipv6 fe80::2 interface vlan 1
SwitchA(config-router)#priority 150
SwitchA(config-router)#enable
SwitchA(config)#router ipv6 vrrp 2
SwitchA(config-router)#virtual-ipv6 fe80::3 interface vlan 1
SwitchA(config-router)#enable
```

SwitchB 的配置：

```
SwitchB(config)#interface vlan 1
SwitchB(config)#router ipv6 vrrp 2
SwitchB(config-router)#virtual-ipv6 fe80::3 interface vlan 1
```

```
SwitchB(config-router)#priority 150
SwitchB(config-router)#enable
SwitchB(config)#router ipv6 vrrp 1
SwitchB(config-router)#virtual-ipv6 fe80::2 interface vlan 1
SwitchB(config-router)#enable
```

2.4 VRRPv3 排错帮助

在配置、使用 VRRPv3 协议时，可能会由于物理连接、配置错误等原因导致 VRRPv3 协议未能正常运行。因此，用户应注意以下要点：

- ☞ 首先应该保证物理连接的正确无误；
- ☞ 其次，保证接口和链路协议是 UP（使用 `show ipv6 interface` 命令）；
- ☞ 然后，确保开启了 IPv6 转发功能(使用 `ipv6 enable` 命令)；
- ☞ 另外，确保在接口上已启动了 VRRPv3 协议；
- ☞ 检查同一备份组内的不同路由器（或三层以太网交换机）配置的 timer 时间是否相同；
- ☞ 检查同一备份组内的虚拟 IPv6 地址是否相同。

第3章 MRPP配置

3.1 MRPP简介

MRPP (Multi-layer ring protection protocol, 多环路自动保护协议) 是一个用于以太网环路保护的链路层协议。它在以太网环完整时能够防止数据环路引起的广播风暴, 而当以太网环上一条链路断开时能迅速恢复环网上各个节点之间的通信通路。

MRPP协议功能上类似于STP协议。同STP协议相比, MRPP具有以下特点:

<1>MRPP专用于以太网环型拓扑环境

<2>收敛速度快, 通常小于1秒。理想状况下可以达到100-50毫秒。

3.1.1 概念介绍

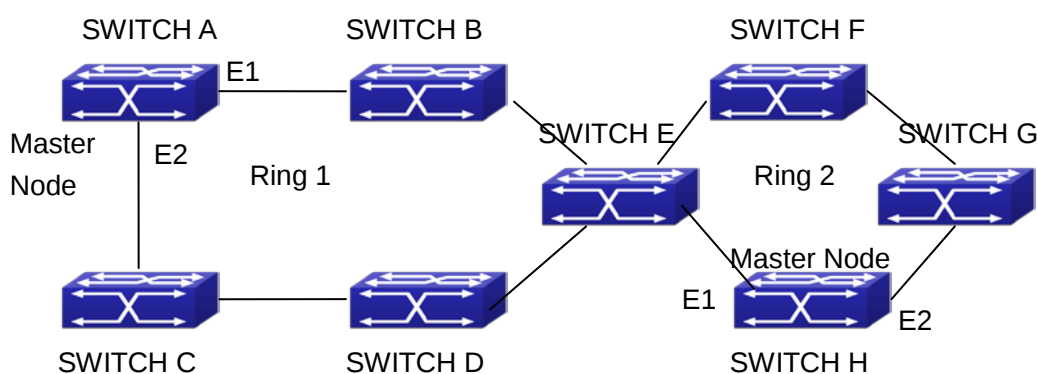


图 3-1 MRPP 示意图

1. 控制VLAN

控制 VLAN 是一个虚拟的 VLAN, 仅仅用来区分链路上传递的 MRPP 协议报文。为了避免引起同其它已经配置的 VLAN 的混淆, 应尽量避免将控制 VLAN ID 配置为其它已经配置的 VLAN ID。不同的 MRPP 环上应该配置不同的控制 VLAN ID。

2. 以太网环(MRPP环)

环形连接的以太网网络拓扑。

每个 MRPP 环有两种状态。

健康状态: 整个环网物理链路是连通的

断裂状态: 环网中一处或者多处物理链路断开

3. 节点

以太网环网上每个交换机都称为一个节点。节点由如下角色:

主节点：每个环上有一个主节点，它是发起环路探测和进行环路预防的主要操作节点。

传输节点：每个环上除了主节点外的其他所有节点为传输节点。

节点角色由用户的配置决定。如图 3-1 所示，Switch A 是 Ring 1 的主节点，Switch B、Switch C，Switch D 和 Switch E 为 Ring 1 的传输节点。

4. 主端口和副端口

主节点和传输节点分别有两个端口接入以太网环，其中一个为主端口，另一个为副端口。端口的角色由用户的配置决定。

主节点的主端口和副端口。

主节点的主端口用来发送环路健康检查报文（Hello），副端口用来接收主节点发出的 Hello 报文。当以太网环处在健康状态时，主节点的副端口在逻辑上阻塞其它数据，只允许 MRPP 的报文通过。当以太网环处在断裂状态时，主节点的副端口将解除阻塞状态，转发数据报文。

传输节点的主端口和副端口在功能上没有区别。

端口的角色由用户的配置决定。如图 3-1 所示，Switch A 的 E1 为主端口，E2 为副端口。

5. 定时器

主节点在发送和接收 MRPP 协议报文时用到两个定时器：Hello 定时器和 Fail 定时器。

Hello 定时器：定义主节点主端口发送健康检测报文的时间间隔的定时器。

Fail 定时器：定义主节点副端口接收健康检测报文的超时时间的定时器。Fail 定时器的值必须大于或等于 Hello 定时器值的 3 倍。

3.1.2 MRPP协议报文类型

报文类型	说明
Hello 报文（健康检查报文）	由主节点的主端口发起，对环路进行检测，如果主节点的副端口能够在配置的超时时间内接收到 Hello 报文，则说明环路正常
LINK-DOWN(链路 Down 事件报文)	传输节点在检测在端口发生 Down 事件后，立即向主节点发送 LINK-DOWN 报文，以通告主节点环路发生故障
LINK-DOWN-FLUSH-FDB 报文	主节点在检测到环路发生故障或者接收到 LINK-DOWN 报文后，打开阻塞的副端口，然后利用两个端口发送该报文，通知各传输节点更新自己的 MAC 地址表

LINK-UP-FLUSH-FDB 报文	由主节点在检测到环路发生故障恢复正常后，利用主端口发出的报文，通知各传输节点更新自己的 MAC 地址表
----------------------	---

3.1.3 MRPP协议运行机制

1. 链路Down告警机制

当传输节点发现自己任何一个属于 MRPP 环的端口 Down 时，都会立刻发送链路 Down 报文给主节点。主节点收到链路 Down 报文后立刻解除其副端口的阻塞状态，并发送 LINK-DOWN-FLUSH-FDB 报文通知所有传输节点，使其更新各自的 MAC 地址转发表。

2. 轮询机制

主节点的主端口根据配置的 Hello-timer,定时向其邻居发送 Hello 报文。如果环路是健康的，主节点的副端口将收到健康检测报文，主节点将保持副端口的阻塞状态。

如果环路是断裂的，主节点的副端口在超时定时器超时后也无法收到健康检测报文。主节点将解除副端口的阻塞状态，同时发送 LINK-DOWN-FLUSH-FDB 报文通知所有传输节点，使其更新各自的 MAC 地址转发表。

3. 环路恢复

主节点在环路故障后，如果副端口收到了主节点发出的 Hello 报文，则证明环路已经恢复，这时主节点阻塞自己的副端口，并向其邻居发送 LINK-UP-FLUSH-FDB 报文。

传输节点上属于 MRPP 环的端口重新 UP 后，主节点可能在过了一段时间后才能发现环路恢复。这段时间对于正常的数据 VLAN 来说，网络有可能形成一个临时的环路，从而产生广播风暴。为了防止临时环路的产生，传输节点发现自己接入环网的端口重新 UP 后，立即将其临时阻塞（只允许控制 VLAN 的报文通过），只有收到主节点发送的 LINK-UP-FLUSH-FDB 报文之后，才解除该端口的阻塞状态。

3.2 MRPP配置任务序列

- 1) 全局启动 MRPP
- 2) 配置 MRPP 环
- 3) 配置 MRPP 端口查询时间
- 4) 配置兼容模式
- 5) 显示和调试 MRPP 相关信息

1) 全局启动 MRPP

命令	解释
全局配置模式	

mrpp enable no mrpp enable	全局启动和关闭 MRPP。
---	---------------

2) 配置 MRPP 环

命令	解释
全局配置模式	
mrpp ring <ring-id> no mrpp ring <ring-id>	创建 MRPP 环，本命令的 NO 操作删除 MRPP 环及其配置。
MRPP 环配置模式	
control-vlan <vid> no control-vlan	配制控制 VLAN ID，本命令的 NO 操作删除配置的控制 VLAN ID。
node-mode {master transit}	配置 MRPP 环的节点类型（主节点或者是副节点）。
hello-timer <timer> no hello-timer	配置 MRPP 环的主节点发送 Hello 报文定时器，本命令的 NO 操作恢复缺省的定时器值。
fail-timer <timer> no fail-timer	配置 MRPP 环的主节点接收 Hello 报文超时定时器，本命令的 NO 操作恢复缺省的定时器值。
enable no enable	使能 MRPP 环，本命令的 NO 操作关闭使能的 MRPP 环。
端口配置模式	
mrpp ring <ring-id> primary-port no mrpp ring <ring-id> primary-port	指定 MRPP 环的主端口。
mrpp ring <ring-id> secondary-port no mrpp ring <ring-id> secondary-port	指定 MRPP 环的副端口。

3) 配置 MRPP 端口查询时间

命令	解释
全局配置模式	
mrpp poll-time <20-2000>	配置 mrpp 端口状态查询时间间隔。

4) 配置兼容模式

命令	解释
全局配置模式	
mrpp errp compatible no mrpp errp compatible	使能 ERRP 的兼容模式，本命令的 no 操作关闭 ERRP 的兼容模式。
mrpp eaps compatible no mrpp eaps compatible	使能 EAPS 的兼容模式，本命令的 no 操作关闭 EAPS 的兼容模式。

errp domain <domain-id>	创建 ERRP 域，本命令的 no 操作删除已经配置的 ERRP 域。
no errp domain <domain-id>	

5) 显示和调试 MRPP 相关信息

命令	解释
特权配置模式	
debug mrpp no debug mrpp	打开 MRPP 模块的调试信息，本命令的 NO 操作关闭 MRPP 调试信息输出。
show mrpp [<ring-id>]	显示 MRPP 环的配置信息。
show mrpp statistics [<ring-id>]	显示 MRPP 环的接收数据包统计信息。
clear mrpp statistics [<ring-id>]	清除 MRPP 环的接收数据包统计信息。

3.3 MRPP典型案例

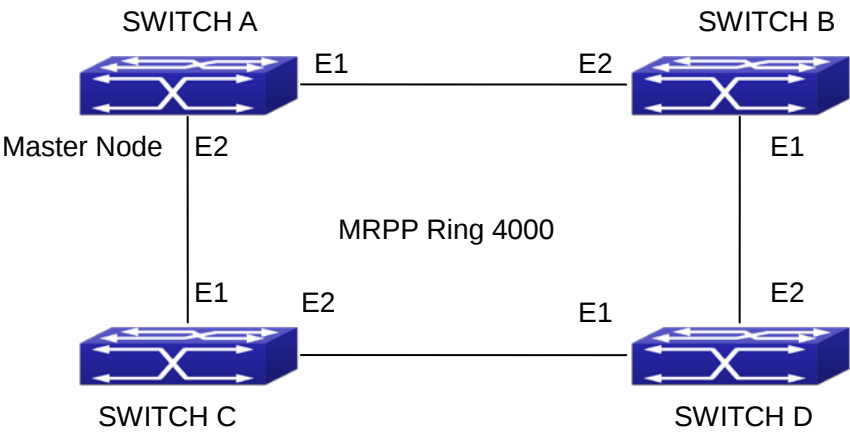


图 3-2 MRPP 典型配置案例

上面的拓扑是大多数情况下使用 MRPP 协议的情形。多个交换机组成一个单一的 MRPP 环，所有的交换机都只配置了一个 MRPP 环 4000，从而组成一个单一的 MRPP 环。

在上面的配置中，SWITCH A 配置为 MRPP 环 4000 的主节点，并且配置 E1/1 为主端口，E1/2 为副端口。其它交换机为 MRPP 环的副节点，分别配置了主端口和副端口。

为了避免环路，在使能整个 MRPP 环的各 MRPP 环时，应该暂时关闭其中主节点的一个端口，等到所有节点配置完成后，再打开该端口。

在关闭 MRPP 环时，需要确保该 MRPP 环没有环路。

SWITCH A 配置任务序列：

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#fail-timer 18
```

```
Switch(mrpp-ring-4000)#hello-timer 5
Switch(mrpp-ring-4000)#node-mode master
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/1
Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/1)#interface ethernet 1/2
Switch(config-If-Ethernet1/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/2)#exit
Switch(Config)#
```

SWITCH B 配置任务序列:

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/1
Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/1)#interface ethernet 1/2
Switch(config-If-Ethernet1/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/2)#exit
Switch(Config)#
```

SWITCH C 配置任务序列:

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/1
Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/1)#interface ethernet 1/2
Switch(config-If-Ethernet1/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/2)#exit
Switch(Config)#
```

SWITCH D 配置任务序列:

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/1
Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/1)#interface ethernet 1/2
Switch(config-If-Ethernet1/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/2)#exit
Switch(Config)#
```

3.4 MRPP排错帮助

MRPP 协议的正常运行非常依赖于对 MRPP 环上各个交换机的正常配置，否则极有可能形成环路和广播风暴：

- ☞ 在配置 MRPP 环路时。最好先断开该环路，等待各个交换机配置完毕后再打开该环路。
- ☞ 在关闭 MRPP 环路上一个使能的交换机的 MRPP 环的时候，应确保该 MRPP 环所在的环路已经断开。
- ☞ 在 MRPP 环上出现广播风暴时，首先断开该环路，并确定环上的各个交换机 MRPP 环配置是否正确，如果配置正确，恢复该环路，然后观察环路是否正常。
- ☞ MRPP 环网的收敛时间和端口 up/down 的响应方式有关。若使用查询方式，在简单环网内，MRPP 收敛时间为几百毫秒；若使用中断方式，收敛时间在 50 毫秒以内。
- ☞ 一般情况下，端口扫描配置为查询方式即可。中断方式仅适用于对性能要求较高的环境。相比于中断，查询方式的安全性更高。具体参考端口配置命令 `port-scan-mode {interrupt | poll}`。
- ☞ 如果在正常配置下，仍然形成了环路的广播风暴或者环路不通，请打开主节点的 MRPP 的调试功能，并且利用 `show mrpp statistics` 命令观察主节点和传输节点的状态和统计信息是否正常，并将结果发送给本公司技术服务中心。

第4章 ULPP配置

4.1 ULPP简介

每个ULPP组包括两个上行链路端口，一个主端口(master)，另一个为副端口(slave)。这里的端口可以是物理端口，也可以是port channel。ULPP组成员端口有三种状态：Forwarding，Standby，Down。正常情况下，只有一个端口处于转发(Forwarding)状态，另一个端口阻塞，处于待命(Standby)状态。当主端口发生链路故障时，主端口变为Down状态，原来处于Standby状态的副端口切换到Forwarding状态。

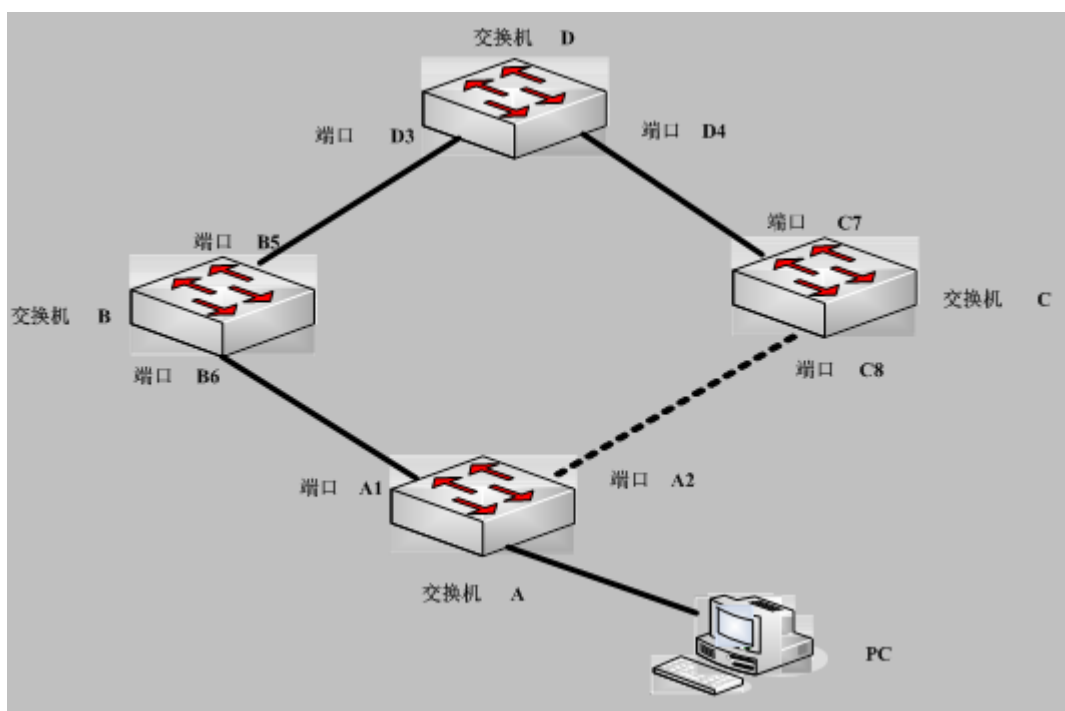


图 4-1 ULPP 使用场景

图 4-1 中使用了双上行组网，这是 ULPP 的典型应用场景。交换机 A 通过 B 和 C 双上行到 D，端口 A1 和 A2 为上行端口。交换机 A 上配置了 ULPP，其中端口 A1 设置为主端口，端口 A2 设置为副端口。当处于 Forwarding 状态的端口 A1 发生故障时，立即进行链路切换，端口 A2 进入 Forwarding 状态。此后，当主端口恢复时，如果没有配置抢占模式，则端口 A2 继续保持 Forwarding 状态，端口 A1 进入 Standby 状态。

通过开启抢占模式，使得主端口从故障恢复时可以对副端口进行抢占。为了避免异常故障导致的频繁链路切换，引入了抢占延时机制，主端口抢占副端口前需要等待一定的时间。为了保持流量的稳定，默认情况下主端口不进行抢占，而是进入 Standby 状态。

对 ULPP 配置时，需要通过 MSTP 实例的方式指定该 ULPP 组所保护的 VLAN，对保护 VLAN 之外的其它 VLAN，ULPP 不提供保护。

当发生链路切换时，网络中设备上原有的转发表项将不适用于新的拓扑。在图 4-1 所

示拓扑中，交换机 A 上配置了 ULPP，作为主端口的端口 A1 处于 Forwarding 状态，此时交换机 D 会从端口 D3 上学习到 PC 的 MAC 地址。此后端口 A1 发生故障，流量切换到端口 A2 进行转发，此时如果有通过交换机 D 发往 PC 的数据，仍然会从端口 D3 进行转发，造成数据包的丢失。因此，链路切换时，配置了 ULPP 的设备需要通过切换变为 Forwarding 状态的端口发送 flush 报文，更新网络中其他设备的 MAC 地址表和 ARP 表。ULPP 分别使用两种 flush 报文对表项进行更新：MAC 地址更新报文和 ARP 删除报文。

为了充分利用带宽资源，ULPP 通过配置可以实现 VLAN 负载均衡。如 4-2 所示，交换机 A 上配置了两个 ULPP 组：组 1 中端口 A1 做为主端口，端口 A2 为副端口，组 2 中端口 A2 为主端口，端口 A1 为副端口，组 1 和组 2 保护的 VLAN 分别为 1-100 和 101-200。此时端口 A1 和端口 A2 同时处于转发状态，主端口和副端口互为备份，分别转发不同范围 VLAN 的报文。端口 A1 发生故障时，VLAN 1-200 的流量都会由端口 A2 进行转发。此后当端口 A1 恢复正常时，端口 2 继续转发 VLAN 101-200 的数据，VLAN 1-100 的数据切换到端口 A1 转发。

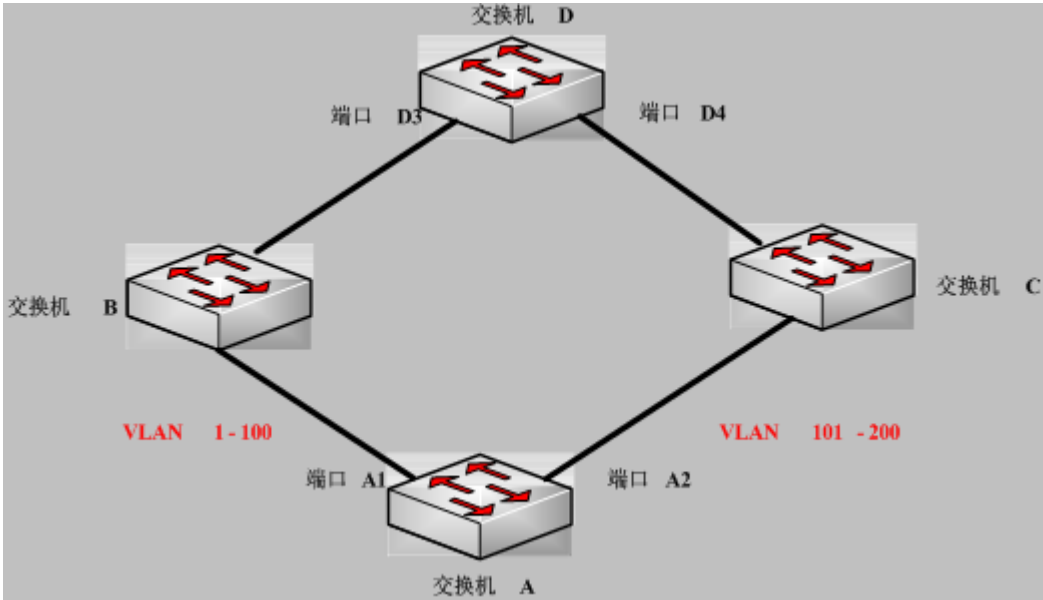


图 4-2 VLAN 负载均衡

4.2 ULPP配置任务序列

- 1) 全局创建 ULPP 组
- 2) 配置 ULPP 组
- 3) 显示和调试 ULPP 相关信息

1) 全局创建 ULPP 组

命令	解释
全局配置模式	

ulpp group <integer> no ulpp group <integer>	全局配置和删除 ULPP 组。
---	-----------------

2) 配置 ULPP 组

命令	解释
ULPP 组配置模式	
preemption mode no preemption mode	配置 ULPP 组的抢占模式，no 操作为删除抢占模式。
preemption delay <integer> no preemption delay	配置抢占时延，no 操作恢复默认值 30s。
control vlan <integer> no control vlan	配置发送控制 VLAN，no 操作恢复发送控制 VLAN 的默认值 1。
protect vlan-reference-instance <instance-list> no protect vlan-reference-instance <instance-list>	配置保护 VLAN，no 操作为删除保护 VLAN。
flush enable mac flush disable mac	使能或者关闭 MAC 地址更新的 flush 报文的发送功能。
flush enable arp flush disable arp	使能或者关闭 ARP 删除的 flush 报文的发送功能。
flush enable mac-vlan flush disable mac-vlan	使能或关闭根据 vlan 删除动态单播 mac 的 flush 报文发送功能
description <string> no description	配置或者删除 ULPP 组描述。
端口配置模式	
ulpp control vlan <vlan-list> no ulpp control vlan <vlan-list>	配置接收控制 VLAN，no 操作恢复接收控制 VLAN 的默认值 1。
ulpp flush enable mac ulpp flush disable mac	使能或者关闭 MAC 地址更新的 flush 报文的接收功能。
ulpp flush enable arp ulpp flush disable arp	使能或者关闭 ARP 删除的 flush 报文的接收功能。
ulpp flush enable mac-vlan ulpp flush disable mac-vlan	使能或关闭 mac-vlan 类型的 flush 报文接收功能
ulpp group <integer> master no ulpp group <integer> master	配置或者删除 ULPP 组的主端口。
ulpp group <integer> slave no ulpp group <integer> slave	配置或者删除 ULPP 组的副端口。

3) 显示和调试 ULPP 相关信息

命令	解释
特权配置模式	
show ulpp group [group-id]	显示已配置的 ULPP 组的配置信息。
show ulpp flush counter interface {ethernet <IFNAME> <IFNAME>}	显示 flush 报文统计信息。
show ulpp flush-receive-port	显示端口接收 flush 类型和 control vlan。
clear ulpp flush counter interface <name>	清除 flush 报文统计信息。
debug ulpp flush {send receive} interface <name> no debug ulpp flush {send receive} interface <name>	显示收发 flush 报文信息，no 操作为关闭显示收发 flush 报文信息。
debug ulpp flush content interface <name> no debug ulpp flush content interface <name>	显示接收到的 flush 报文内容，no 操作为关闭显示 flush 报文内容。
debug ulpp error no debug ulpp error	显示 ULPP 错误信息，no 操作为关闭显示 ULPP 错误信息。
debug ulpp event no debug ulpp event	显示 ULPP 事件信息，no 操作为关闭显示 ULPP 事件信息。

4.3 ULPP 典型案例

4.3.1 ULPP 典型案例 1

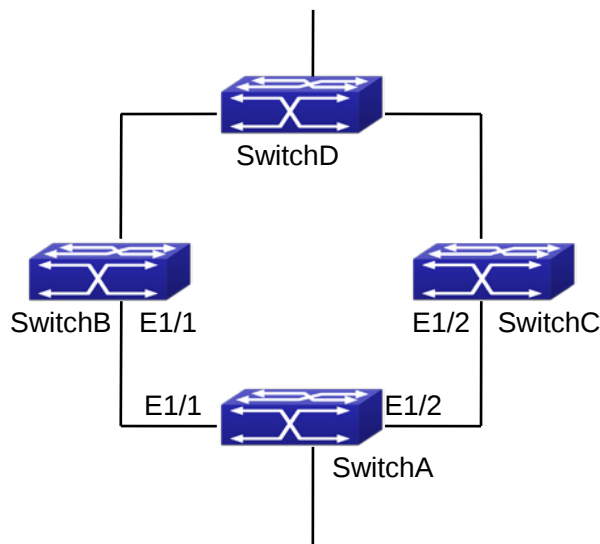


图 4-3 ULPP 典型配置案例 1

上面的拓扑是 ULPP 协议的典型应用环境。

SwitchA 有两条上行链路，分别连接 SwitchB 和 SwitchC，当不开启任何协议的时候，该拓扑成环。为了避免环路，可以在 SwitchA 上配置 ULPP 协议，配置 ULPP 组的主副端口，在主副端口都 up 的情况下，会将副端口置为 standby 状态，即不再转发数据报文，在主端口 down 掉的情况下，会将副端口置为 forwarding 状态，从而实现了链路的切换。SwitchB 和 SwitchC 上也可以开启接收 flush 报文的命令，用来配合 SwitchA 上的 ULPP 协议的运行，从而达到快速切换链路的目的，尽可能的减少了切换时延。

在配置 SwitchA 上的 ULPP 协议时，首先创建一个 ULPP 组，配置该组的保护 VLAN 为 vlan10，然后配置 interface Ethernet 1/1 为该 ULPP 组的主端口，interface Ethernet 1/2 为该 ULPP 组的副端口，控制 VLAN 为 10。在 SwitchB 和 SwitchC 上配置接收 ULPP 的 flush 报文。

SwitchA 配置任务序列：

```
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/1; 1/2
Switch(Config-vlan10)#exit
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 10
Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#control vlan 10
Switch(ulpp-group-1)#exit
Switch(Config)#interface ethernet 1/1
```

```
Switch(config-If-Ethernet1/1)# ulpp group 1 master
Switch(config-If-Ethernet1/1)#exit
Switch(Config)#interface Ethernet 1/2
Switch(config-If-Ethernet1/2)# ulpp group 1 slave
Switch(config-If-Ethernet1/2)#exit
```

SwitchB 配置任务序列:

```
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/1
Switch(Config-vlan10)#exit
Switch(Config)#interface ethernet 1/1
Switch(config-If-Ethernet1/1)# ulpp flush enable mac
Switch(config-If-Ethernet1/1)# ulpp flush enable arp
Switch(config-If-Ethernet1/1)# ulpp control vlan 10
```

SwitchC 配置任务序列:

```
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/2
Switch(Config-vlan10)#exit
Switch(Config)#interface ethernet 1/2
Switch(config-If-Ethernet1/2)# ulpp flush enable mac
Switch(config-If-Ethernet1/2)# ulpp flush enable arp
Switch(config-If-Ethernet1/2)# ulpp control vlan 10
```

4.3.2 ULPP典型案例 2

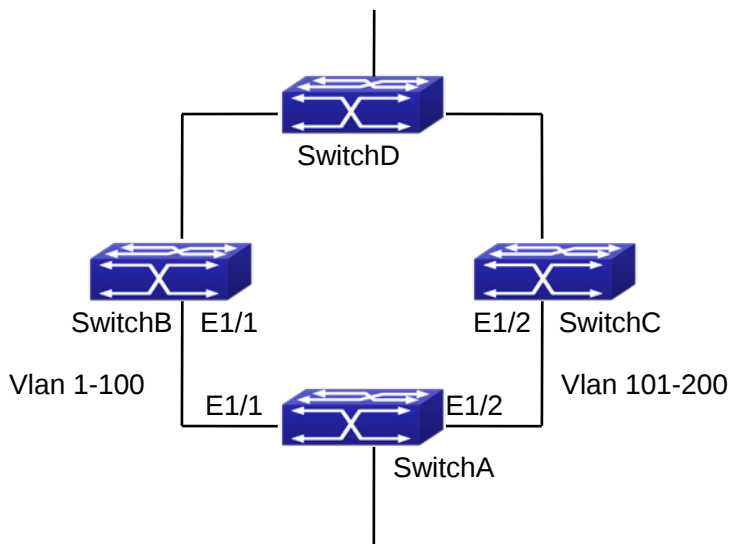


图 4-4 ULPP 典型配置案例 2

ULPP 可以通过配置来实现 VLAN 负载均衡。如图 4-4 所示，switchA 上配置了两个 ULPP 组：组 1 中端口 E1/1 做为主端口，端口 E1/2 为副端口，组 2 中端口 E1/2 为主端口，端口 E1/1 为副端口，组 1 和组 2 保护的 VLAN 分别为 1-100 和 101-200。此时端口 E1/1 和端口 E1/2 同时处于转发状态，主端口和副端口互为备份，分别转发不同范围 VLAN 的报文。端口 E1/1 发生故障时，VLAN 1-200 的流量都会由端口 E1/2 进行转发。此后当端口 E1/1 恢复正常时，端口 E1/2 继续转发 VLAN 101-200 的数据，VLAN 1-100 的数据切换到端口 E1/1 转发。

switchA 配置任务序列：

```
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1-100
Switch(Config-Mstp-Region)#instance 2 vlan 101-200
Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#preemption mode
Switch(ulpp-group-1)#exit
Switch(Config)#ulpp group 2
Switch(ulpp-group-2)#protect vlan-reference-instance 2
Switch(ulpp-group-2)#preemption mode
Switch(ulpp-group-2)#exit
Switch(Config)#interface ethernet 1/1
Switch(config-if-Ethernet1/1)#switchport mode trunk
Switch(config-if-Ethernet1/1)#ulpp group 1 master
```

```
Switch(config-If-Ethernet1/1)#ulpp group 2 slave
Switch(config-If-Ethernet1/1)#exit
Switch(Config)#interface Ethernet 1/2
Switch(config-If-Ethernet1/2)#switchport mode trunk
Switch(config-If-Ethernet1/2)# ulpp group 1 slave
Switch(config-If-Ethernet1/2)# ulpp group 2 master
Switch(config-If-Ethernet1/2)#exit
```

switchB 配置任务序列:

```
Switch(Config)#interface ethernet 1/1
Switch(config-If-Ethernet1/1)#switchport mode trunk
Switch(config-If-Ethernet1/1)# ulpp flush enable mac
Switch(config-If-Ethernet1/1)# ulpp flush enable arp
```

switchC 配置任务序列:

```
Switch(Config)#interface ethernet 1/2
Switch(config-If-Ethernet1/2)# switchport mode trunk
Switch(config-If-Ethernet1/2)# ulpp flush enable mac
Switch(config-If-Ethernet1/2)# ulpp flush enable arp
```

4.4 ULPP排错帮助

- ☞ 目前对于超过双上行的多上行，可以允许配置，但是会出现环路，所以不建议在超过双上行的链路上配置 ULPP。
- ☞ 如果在正常配置下，仍然形成了环路的广播风暴或者环路不通，请打开 ULPP 的调试功能，复制 3 分钟内的 debug 信息以及配置信息，并将结果发送给本公司技术服务中心。

第5章 ULSM配置

5.1 ULSM简介

ULSM (Uplink State Monitor) 用来进行端口状态同步。每个 ULSM 组由上行端口和下行端口组成，上行端口和下行端口都可以为多个。端口可以是物理端口，也可以是 port channel，但不能是 port channel 的成员端口，每个端口只能属于一个 ULSM 组。

上行端口是 ULSM 组中被监控的端口。当 ULSM 组中的所有上行端口都为 Down 或 ULSM 组不存在上行端口时，ULSM 组的状态为 Down。只要有一个上行端口为 Up，ULSM 组的状态就为 Up。

下行端口是 ULSM 组中的受控端口。下行端口的状态会随着 ULSM 组 Up/Down 状态而改变，并保持与 ULSM 组的状态一致。

ULSM 主要与 ULPP 配合使用，使得下游设备可以快速感知上游设备链路故障，并做出相应处理。在图 5-1 中所示环境中，交换机 A 上配置了 ULPP，此时通过端口 A1 转发流量，如果交换机 B 与交换机 D 间链路发生故障，由于交换机 A 无法感知上游链路的故障，继续从端口 A1 转发，从而造成流量的丢失。

可以通过在交换机 B 上配置 ULSM 解决上述问题。步骤为：将交换机 B 上的端口 B5 设置为 ULSM 组上行端口，端口 B6 设置为下行端口。当交换机 B 与交换机 D 间链路发生故障时，下行端口 B6 与 ULSM 组状态同步为 Down，从而引发配置了 ULPP 的交换机 A 发生链路切换，避免数据的丢失。

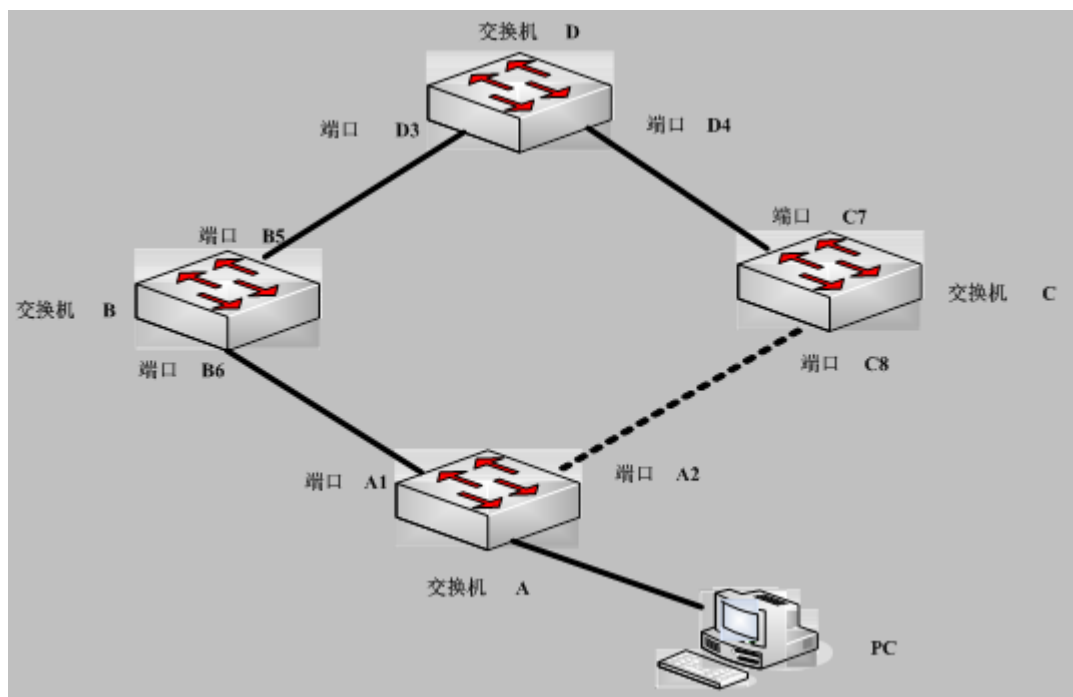


图 5-1 ULSM 使用场景

5.2 ULSM配置任务序列

- 1) 全局创建 ULSM 组
- 2) 配置 ULSM 组
- 3) 显示和调试 ULSM 相关信息

1) 全局创建 ULSM 组

命令	解释
全局配置模式	
ulsm group <group-id> no ulsm group <group-id>	全局配置和删除 ULSM 组。

2) 配置 ULSM 组

命令	解释
端口配置模式	
ulsm group <group-id> {uplink downlink} no ulsm group <group-id> {uplink downlink}	配置 ULSM 组的上行/下行端口，no 命令 删除上行/下行端口。

3) 显示和调试 ULSM 相关信息

命令	解释
特权配置模式	
show ulsm group [group-id]	显示已配置的 ULSM 组的配置信息。
debug ulsm event no debug ulsm event	显示 ULSM 事件信息，no 操作关闭显示 ULSM 事件信息。

5.3 ULSM 典型案例

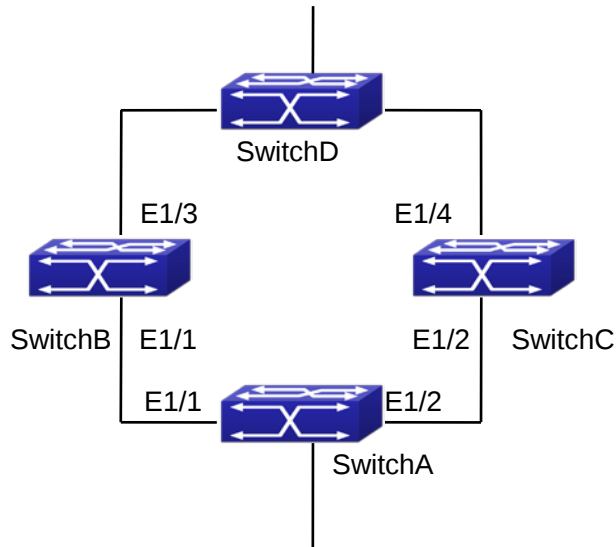


图 5-2 ULSM 典型配置案例

上面的拓扑是 ULSM 和 ULPP 协议配合使用的典型应用环境。

ULSM 本身是用来进行端口状态同步的，该功能单独使用并没有太大的意义，所以一般情况下是和 ULPP 协议结合使用的。在拓扑中，SwitchA 上开启 ULPP 协议，用来进行链路的切换，SwitchB 和 SwitchC 上开启 ULSM 协议，用来监听上行的链路是否 down，如果 down 掉，则 ULSM 会对下行端口执行 down 操作，从而使下行链路 down 掉，此时 ULPP 协议就相应的执行链路切换操作。

SwitchA 配置任务序列：

```
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1
Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#exit
Switch(Config)#interface ethernet 1/1
Switch(config-If-Ethernet1/1)# ulpp group 1 master
Switch(config-If-Ethernet1/1)#exit
Switch(Config)#interface Ethernet 1/2
Switch(config-If-Ethernet1/2)# ulpp group 1 slave
Switch(config-If-Ethernet1/2)#exit
```

SwitchB 配置任务序列：

```
Switch(Config)#ulsm group 1
```

```
Switch(Config)#interface ethernet 1/1
Switch(config-If-Ethernet1/1)#ulsm group 1 downlink
Switch(config-If-Ethernet1/1)#exit
Switch(Config)#interface ethernet 1/3
Switch(config-If-Ethernet1/3)#ulsm group 1 uplink
Switch(config-If-Ethernet1/3)#exit
```

SwitchC 配置任务序列:

```
Switch(Config)#ulsm group 1
Switch(Config)#interface ethernet 1/2
Switch(config-If-Ethernet1/2)#ulsm group 1 downlink
Switch(config-If-Ethernet1/2)#exit
Switch(Config)#interface ethernet 1/4
Switch(config-If-Ethernet1/4)#ulsm group 1 uplink
Switch(config-If-Ethernet1/4)#exit
```

5.4 ULSM排错帮助

- ☞ 如果在正常配置下，下行端口没有响应上行端口的 **down** 事件，请打开 ULSM 的调试功能，复制 3 分钟内的 **debug** 信息以及配置信息，并将结果发送给本公司技术服务中心。

第6章 HA配置

6.1 HA简介

随着网络的发展，用户对于网络的可靠性提出了越来越高的要求，那么向用户提供“高可用性(High Availability)”数据通讯设备，逐渐成为各个数据通信设备商追求的目标，是其保持核心竞争力的重要保证。

HA 是一种系统设计和实现方式，它保证我们的设备能够向用户提供持续的服务。如果因为某种原因，我们提供的网络通信设备“Down 机”，那么这种不可访问性，对某些用户来说可能是无法接受的。

在数据通信中可以使用的 HA 技术很多，针对不同的问题，可能有不同的处理方式。传统高可用技术主要包括：

- 1) 物理设备：冗余电源、冗余风扇、冗余主控、板卡支持热插拔；
- 2) 链路层面：以太网链路聚合（手工聚合、LACP）；
- 3) 二层多路径：STP、MSTP、SmartLink；
- 4) 三层多路径：VRRP、ECMP、动态路由协议多路径；
- 5) 故障 检测：NQA、BFD、OAM、DLDP；
- 6) 不间断转发：GR、热补丁升级；
- 7) L4-L7 多路径：状态热备、非对称路径转发；
- 8) NSF/SSO：不间断转发的主备控制板倒换。

HA（High Availability，高可靠性）特性用于实现系统的高可靠性。支持 HA 特性的设备有两块单板，一块为主用板，工作在 Master 模式；另一块为备用板，工作在 Slave 模式。备用板通过同步功能，来保持与主用板当前配置的一致。

HA 主要体现在以下两个方面：

当主用板发生故障或者被拔出时，备用板将迅速自动取代主用板成为新的主用板（下面简称该过程为主备倒换），以保证设备的继续运行。

当升级设备的时候，可以先升级备用板，再手工执行主备倒换，主备倒换时，原主用板会使用配置的新的下次启动文件重新启动，从而达到升级原主用板的效果。相比整机重启的方式，大大减少了升级过程业务中断的时间。

当使用主备倒换方式升级设备的时候，要求新的软件版本和当前的软件版本能够实现平滑升级（即版本间的差异较小），否则，可能会导致备用板不能启动。这种升级方式的步骤如下：

- (1) 将最新的软件版本分别下载到主用板和备用板；
- (2) 分别指定主用板和备用板的下次启动文件为新版本的软件；
- (3) 手工重启备用板；
- (4) 手动进行主备倒换。

用户不能直接对备用板进行命令行操作，需要通过主用板的命令行界面进行配置，然后主用板会将配置同步给备用板。当备用板启动时，主用板会对备用板进行初始同步（即批量

备份)。在这个过程中，系统将不会响应用户的输入。初始同步完成后，用户可以在主用板上正常执行命令、进行配置，此时，主用板和备用板将保持实时同步，即用户对主用板的配置将同步到备用板上，以保证主备板当前配置的一致。

6.2 HA配置任务序列

1. 配置同步 running-config
2. 手动进行主备切换
3. 配置指定板卡复位
4. 配置 running-config 同步间隔时间

1. 配置同步 running-config

命令	解释
全局配置模式	
force runcfg-sync	手动配置主控与备份主控的配置同步。

2. 手动进行主备切换

命令	解释
全局配置模式	
force switchover	手动进行主备切换。

3. 配置指定板卡复位

命令	解释
全局配置模式	
reset slot <slot no>	独立模式下，复位指定板卡（包括备份主控）。
reset member <member ID> slot <slotID>	堆叠模式下，复位指定板卡。

4. 配置 running-config 同步间隔时间

命令	解释
全局配置模式	
runcfg-sync [<interval>]	配置 running-config 同步间隔时间。

6.3 HA 典型案例

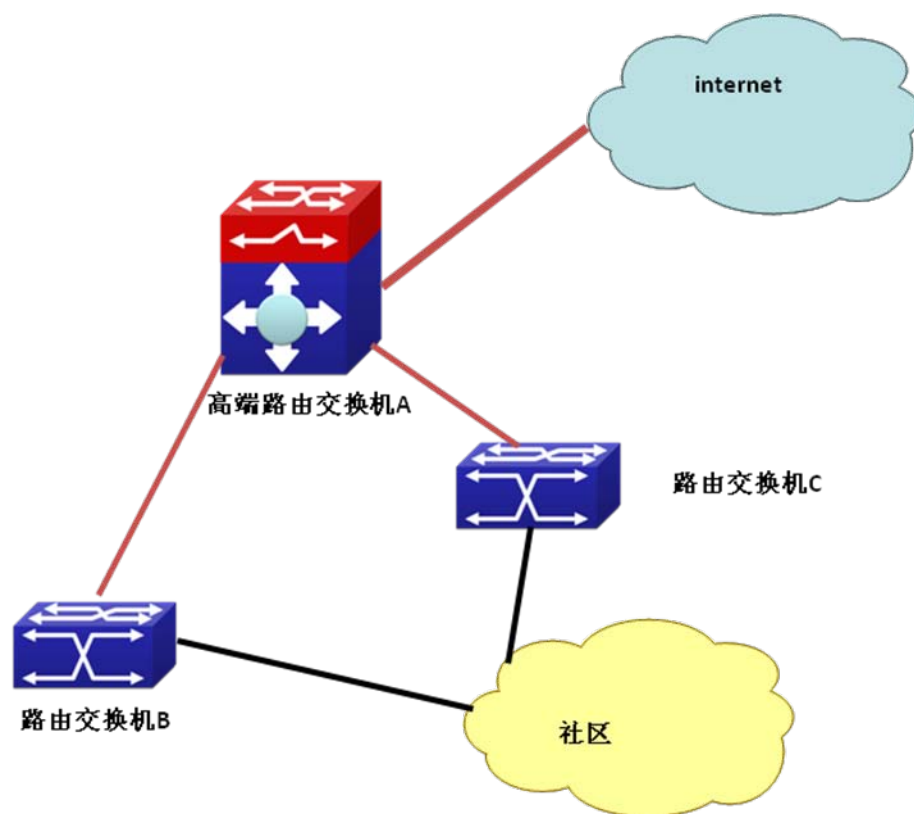


图 6-1 HA 典型应用

一种企业网的典型拓扑如图所示，高端路由交换机 A，通过两台普通路由交换机 B，C 向企业提供 internet 访问服务，尽管其提供 B 和 C 路由交换机作为负载分担和冗余备份链路，当其某一台发生故障的时候，企业依然可以正常的访问网络。但是当 A 节点发生故障的时候，整个企业与 internet 分离，无法提供 internet 访问服务。那么对于 A 设备，当其发生故障的时候，如何支持 NSF/SSO 技术，那么当高端路由交换机 A 的主控板发生故障的时候，其可以在不间断转发的前提下，倒换到备用主控，然后从故障中热恢复过来。在故障恢复的过程中整个数据转发层面没有任何的动荡，而企业内部用户根本无法感知到 A 节点的故障。

当然，在实际的部署中可以采用链路冗余等手段，向用户提供可靠的 internet 访问，但是其他技术都需要其他的冗余链路或者冗余设备，设置需要多态冗余网络设备。相比之下，支持 NSF/SSO 的设备，一台就可以满足用户的需求，这不失为一种选择。